TEXTBOOKS

Computer Science

Institute for Communications Engineering

Ernst M. Gabidulin

Rank Codes

TUM.University Press

Ernst M. Gabidulin

Rank Codes

The German National Library has registered this publication in the German National Bibliography. Detailed bibliographic data are available on the Internet at https://portal.dnb.de.

Imprint

1. Edition

Editor: Vladimir Sidorenko
Translation: Vladimir Sidorenko
Layout design and typesetting: Vladimir Sidorenko
Cover design: Caroline Ennemoser, Vladimir Sidorenko
Cover illustration: Caroline Ennemoser

TUM.University Press
Technical University of Munich
Arcisstrasse 21
80333 Munich

DOI: 10.14459/2021md1601193
ISBN printed edition: 978-3-95884-062-1

www.tum.de

From the translation editor

It is a pleasure to introduce the book "Rank codes" written by an outstanding Russian scientist, my teacher, Ernst M. Gabidulin. Ernst Mukhamedovich Gabidulin, Honored Scientist of the Russian Federation, is a Professor at the Moscow Institute (National Research University) of Physics and Technology.

The book contains the theory and some applications of the rank metric codes developed by the author and called *Gabidulin codes* by the scientific community. The book can be recommended to students and researchers working with rank metric codes.

A matrix code $\mathcal{C}$ is a set of $m \times n$ matrices (codewords) of fixed size over a finite field $\mathbb{F}_q$ of order q. The matrix codes are considered in the rank metric that is defined as follows. The distance between two matrices is the rank of their difference. The code distance $d(\mathcal{C})$ of a code $\mathcal{C}$ is the minimum distance between different code matrices. Given a metric, the main directions of coding theory are to design codes with a maximum number of codewords for a fixed code distance, to obtain the properties of the codes, to construct efficient decoding algorithms that find a code matrix nearest to a given matrix.

The fundamental results in three mentioned directions were obtained in the famous paper "Theory of Codes with Maximum Rank Distance" by Gabidulin [Gab85]. The author introduced a class of $\mathbb{F}_{q^m}$-linear vector (n, k, d) codes, consisting of vectors of length n over the extension field $\mathbb{F}_{q^m}$. Here k is the code dimension and d is the code distance in the rank metric. Every code vector of length n over $\mathbb{F}_{q^m}$ can be represented as an $m \times n$ matrix over the base field $\mathbb{F}_q$, hence a vector code is simultaneously the matrix code endowed by the rank metric.

The author introduced a subclass of linear vector codes called *Rank codes*. These codes reach the upper Singleton bound in the rank metric and therefore they are called maximum rank distance (MRD) codes. The vector representation of the linear rank metric codes allowed to the author to propose an efficient decoding algorithm, which made the rank codes ready for practical applications.

In recognition of the author's work on rank metric codes, the scientific community named the Rank codes in [Gab85] *Gabidulin codes*.

The rank metric codes were independently introduced by Delsarte in [Del78] and by Gabidulin in [Gab85], and rediscovered by Roth in [Rot91] (see comments in [GR92]) and by Cooperstein in [Coo97]. Current applications of rank-metric codes include network coding, code-based cryptography, criss-cross error correction in memory chips, distributed data storage, space-time codes for MIMO systems, and digital watermarking.

Further theoretical results and potential applications relating to rank codes were obtained by Gabidulin alone [Gab92], [GA86] and with coauthors, see e.g., [GPT92] with Paramonov and Tretjakov, [GP04], [GP08], [GP16], [GP17b] with Pilipchuk, [KG05] with Kshevetskiy, [GB08], [GB09] with Bossert, [GL08] with Loidreau, [GOHA03] with Ourivski, Honary and Ammar, [LGB03] with Lusina and Bossert. Many of these results are included in this book.

Nowadays, the topic of rank metric codes is a subject on which a great deal of research in being carried out. An Internet search for "rank metric code" returns more than 37 millions results. We cannot give an overview of the topic here, but let us mention some of the publications.

The works of Silva, Kschischang and Kötter [KK08], [SKK08] showed that subspace codes based on rank metric codes can be used in random linear network coding. They proposed efficient decoding algorithms correcting errors and erasures in the rank metric. This greatly increased interest in Gabidulin codes. In [GY08], Gadouleau and Yan investigated the packing and covering properties of codes in the rank metric. Augot, Loidreau and Robert [ALR18] generalized Gabidulin codes to the case of infinite fields, eventually with characteristic zero. Cyclic codes over skew polynomial rings were considered in [BU09] by Boucher and Ulmer and in [Mar17] by Martínez-Peñas.

An interesting direction of research is a direct sum of Gabidulin codes also called interleaved Gabidulin codes. Vertical interleaving was introduced by Loidreau and Overbeck [LO06]. Horizontal interleaving by Sidorenko, Jiang and Bossert [SJB11] results in the linear vector codes. An interest in this direction is due to the fact that both types of interleaving give MRD codes and can efficiently correct errors of rank almost up to the code distance.

Recent dissertations, defended in Ulm University and Technical University of Munich, contain interesting results about interleaved Gabidulin codes and give an overview of the topic. These are dissertations [WZ13] by Wachter-Zeh, [Li15] by Li, [Bar17] by Bartz, and [Puc18] by Puchinger.

Another interesting results can be found in [GX12] by Guruswami and Xing, in [LSS14] by Li et al., in [PRLS17] by Puchinger, Rosenkilde, et al., in [HTR18] by Horlemann-Trautmann and Rosenthal, in [GR18] by Gorla and Ravagnani, in [MV19] by Mahdavifar and Vardy, and in [Ner20] by Neri.

I am very grateful to Prof. Gerhard Kramer for his support during preparation and publishing the book.

Vladimir Sidorenko

Preface

Coding theory studies methods of error correcting that occur during transmission over a channel with noise. These methods are based on using discrete signals and on adding artificial redundancy. Discreteness allows us to describe signals in terms of abstract symbols that are not related to their physical implementation. Artificial redundancy makes it possible to correct errors using fairly complex combinatorial signal designs.

In the modern coding theory, one can distinguish several main interrelated areas, which include

- algebraic coding theory;
- classic questions related to proving the existence of encoding and decoding methods;
- finding bounds for error correcting ability;
- creating models of networks and communication channels;
- performance evaluation of special code ensembles for communication channels;
- development of efficient coding and decoding algorithms.

The central place in this theory belongs to the algebraic coding theory, which uses a wide range of mathematical methods from simple binary arithmetic to modern algebraic geometry. The main objects of coding theory are vector spaces with a metric. Subsets of these spaces are called codes. The main task is to build codes of a given cardinality having the maximum possible pairwise distance between the elements. The dual task is to build codes of maximum cardinality for a given minimum pairwise distance.

The most popular metric in coding theory is *the Hamming weight* of a vector, defined as the number of its nonzero components. Most results in algebraic coding theory are obtained for the Hamming metric. Thousands of articles and books have been dedicated to this metric. However, the Hamming metric does not always provide a good fit for the characteristics of real channels; therefore, other metrics are of interest. One such metric is the rank metric, and this book is devoted to coding theory in this metric. The book considers one of the most interesting areas of algebraic coding theory, namely codes with distance in rank metric. Currently, these codes are very popular both from a theoretical point of view and for applications in communications and cryptography. Many articles have been written on these topics. But there are almost no books in which the main ideas and modern results are brought together.

It is worth mentioning two books on rank metric codes. First, “Coding for radio-electronics” [GA86] by Gabidulin and Afanasyev, which was published (in Russian) in 1986, i.e., 30 years ago. It needs to be supplemented with new scientific results obtained in the years since. Second, “Lectures on algebraic coding” by Gabidulin, 2015, is a brief guide, in which, along with the main known codes, only one small chapter is devoted to rank codes, where the basic concepts are introduced and coding and decoding algorithms are given.

This book presents the main scientific results obtained over more than three decades and provides brief information about the pioneers of this direction in coding. Most of the results presented here were obtained by the author alone, while others were co-authored, for which references are given. In the scientific community, these codes are given the name of the author – Gabidulin codes.

Here is a brief guide for the book.

Chapter 1 is an introduction. Here, definitions of groups, rings, fields, basis, trace, degree, and so on are given. The main issues related to finite fields are explained, the Euclidean algorithm is given, and operations with linearized polynomials are described. This chapter contains the necessary information for understanding the rest of the book.

Chapter 2 starts the presentation of the material directly related to the theory of rank coding.

A class of q-cyclic rank codes, which are similar to cyclic codes in the Hamming metric, is introduced in Chapter 3.

Chapter 4 is devoted to one of the main problems – decoding. *Fast* decoding algorithms, i.e., algorithms with a polynomial, rather than an exponential, complexity of decoding, are considered.

Chapter 5 outlines special constructions of rank codes built on symmetric matrices. It is shown that such codes allow us to exceed the existing error-correction bound in certain situations.

Chapters 6, 7, and 8 consider applications of rank codes.

In Chapter 6, rank codes are applied in random network coding. The principles of constructing subspace codes based on the Gabidulin rank codes proposed by Kötter, Kschischang, and Silva are considered.

Chapter 7 is devoted to multicomponent subspace codes. It shows the connection of these codes with random network coding. It gives a description of the constructions involved, and provides an estimate of the cardinality of the codes.

Principles for building multicomponent subspace codes using combinatorial block designs and rank codes are developed in Chapter 8. An iterative decoding algorithm is proposed for the new codes.

Problems and exercises are given in Chapter 9.

The author believes that for young people who intend to master the theory of algebraic coding, in particular in the rank metric, this manual will provide such an opportunity. Specialists in this field can find suggestions for further developments in the ideas presented here.

The author is very grateful to Vladimir Sidorenko for his enormous efforts to create the book in English.

Contents

1

Finite fields, polynomials, vector spaces

1.1 Metrics

Let us recall the definition of a metric space. Let a set $\mathcal{X}$ be an additive group, i.e., the operations of pairwise addition and subtraction are defined on this set. Define the norm function $\mathcal{N} : \mathcal{X} \to R$ on $\mathcal{X}$. This function should satisfy the following axioms:
For all elements $\underline{\mathbf{x}}, \underline{\mathbf{y}} \in \mathcal{X}$,

$$\begin{array}{rcll} \mathcal{N}(\underline{\mathbf{x}}) & \geq & 0 & \text{(non-negativity);} \\ \mathcal{N}(\underline{\mathbf{x}}) & = & 0 \iff \underline{\mathbf{x}} = 0 & \text{(positive definite or point-separating);} \\ \mathcal{N}(\underline{\mathbf{x}} + \underline{\mathbf{y}}) & \leq & \mathcal{N}(\underline{\mathbf{x}}) + \mathcal{N}(\underline{\mathbf{y}}) & \text{(triangle inequality).} \end{array}$$

The norm function allows us to define the pairwise distance between elements $\underline{\mathbf{x}}, \underline{\mathbf{y}} \in \mathcal{X}$:

$$d(\underline{\mathbf{x}}, \underline{\mathbf{y}}) := \mathcal{N}(\underline{\mathbf{x}} - \underline{\mathbf{y}}).$$

An additive group $\mathcal{X}$ equipped with the norm function $\mathcal{N} : \mathcal{X} \to R$ is called a metric space.

1.2 Rank metric

The distance between matrices of the same size over a certain field was introduced by the Chinese mathematician Hua Loo-Keng in 1951 under the name "arithmetic distance" [Hua51]. *Matrix weight (norm)* was defined as the standard algebraic *matrix rank*. The transition from one matrix to another can be made by sequentially adding matrices of rank 1 to the original matrix. The distance is defined as the *minimum* number of matrices required for such a transition. It was shown that the distance is equal to the rank of the difference of these matrices. However, this work did not consider applications of this concept to coding theory.

The rank distance (or q-distance) in the set of bilinear forms was introduced in [Del78]. It is defined as the rank of the difference of two rectangular matrices representing the corresponding bilinear forms. A family of optimal linear *matrix* codes (sets of matrices over a finite field) with a given rank distance was proposed and the number of matrices of a given rank in the code was found.

The rank distance for vector spaces over an extension field was introduced in [Gab85]. The rank norm of a vector with coordinates from an extension field is defined as the *maximum* number of vector coordinates linearly independent over the base field. The rank distance between two vectors is defined as the rank norm of their difference. A rank code in vector representation is a set of vectors over an extension field, where distance between vectors is measured in the rank metric. For all admissible parameters, families of optimal vector codes with a given rank distance were found [Gab85], and fast coding and decoding algorithms were proposed for these codes.

1.3 Finite field constructions

A discrete message is a sequence of symbols selected from a given finite alphabet. The error control coding of discrete messages is a transformation of the message. The transformation may be linear or nonlinear. Further on we consider linear transformations. The requirement of one-to-one encoding and one-to-one decoding in the absence of errors in the channel imposes certain restrictions on the choice of the final alphabet of symbols and their transformations. The most significant successes were achieved when the final alphabet is considered as a finite field.

A set F is called *an additive group* if the following conditions hold.

1. An *addition* operation is given in which two elements a and b from the set F are associated with the third element $a+b$ from the same set, called the sum, and $a+b=b+a$.

2. For any three elements from F, the associativity law $(a+b)+c=a+(b+c)$ holds.

3. There is a *zero element*[1] $0 \in F$ for which the relation $a+0=a$ holds for all $a \in F$.

4. For each element $a \in F$ there is an opposite element, denoted by $-a$, with the property: $-a+a=0$.

Example 1. *The set if integers, including* 0*, is an additive group.*

A set F is called a *multiplicative set* if

1. The *multiplication* operation is given in which two elements a and b from this set are mapped to the third element, denoted by $a \cdot b$ (or ab), from the same set and called the *product*;

2. For any three elements from F the associativity law $(ab)c = a(bc)$ is fulfilled.

A multiplicative set is called a multiplicative group if it contains an *unit element*[2] 1 for which the relation $1 \cdot a = a \cdot 1 = a$ holds for all $a \in F$ and if for any element $a \in F$ there exists a multiplicative inverse element, denoted by a^{-1}, with the property $a \cdot a^{-1} = a^{-1} \cdot a = 1$.
A multiplicative group is called abelian (or commutative) if $a \cdot b = b \cdot a$.

Example 2. *All nonzero* rational *numbers with the identity element* 1 *form a multiplicative abelian group.*

The set of all integers is not a multiplicative group, since the inverse element is not an integer.

[1] the identity element for an additive group

[2] the identity element for a multiplicative group

On the same set, the operations of addition and multiplication can be defined simultaneously. A set that is an additive group with respect to the addition operation in which all nonzero elements form a multiplicative set with respect to the multiplication operation is called a *ring*.

The existence of inverse elements for all nonzero elements of the ring is not required.

Example 3. *All integers form a commutative ring; all even integers form a ring without unity.*

A *field* is a commutative ring with unity, where each non-zero element has a multiplicative inverse. All elements of the field, including 0, form an additive group, and all nonzero elements form a multiplicative group.

Of the above examples, only rational numbers form a field. Fields containing a finite number of elements are called *finite* fields or Galois fields (GF). They are often denoted by $\mathbb{F}_q$ or by $GF(q)$, where q is the number of elements in the field.

Consider some constructions of finite fields.

A *prime* field $\mathbb{F}_p$, where p is a prime. For example, the field of residues of integers modulo a prime, where the *minimum positive residual* A modulo N is the remainder when A is divided by N.

The operations of addition, subtraction, multiplication on the set of residue classes can be introduced through operations with integers. Therefore, the set of residue classes is a commutative ring with zero 0 and one 1. This residue class ring is also known as a quotient ring or a factor ring.

Theorem 1.1. *The ring of residue classes modulo prime p forms a finite field of order p.*

The integers $0, 1, \ldots, p-1$ are usually taken as representatives of elements of the prime field. The operations of addition, subtraction, multiplication in $\mathbb{F}_p$ are defined as standard operations with integers followed by calculation of the residue (remainder) of the operation modulo p. The inverse element a^{-1} is defined as the solution of the equation $a \cdot a^{-1} \equiv 1 \mod p$.

The *extension field* $\mathbb{F}_{p^m}$ is an extension of the prime field of order m. It can be defined as a vector *space of dimension* m. Every element $\mathbf{a} \in \mathbb{F}_{p^m}$ is defined as a linear combination of vectors $\alpha_i \in \mathbb{F}_{p^m}$

$$\mathbf{a} = a_0\alpha_0 + a_1\alpha_1 + \cdots + a_{m-1}\alpha_{m-1} \tag{1.1}$$

with coefficients (coordinates) $a_i \in \mathbb{F}_p$. Linearly independent vectors

$$\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$$

form a basis of the vector space. The number of different elements (1.1) is p^m.

1.4 Multiplicative structure of a finite field

Let a be a nonzero element of the field $\mathbb{F}_q$. Compute sequential powers $1 = a^0, a, a^2, \ldots, a^n, \ldots$. Since every power of a is an element of the field, this series can have at most $q-1$ different nonzero elements of $\mathbb{F}_q$. Hence, there exist two integers i and j such that $a^i = a^{i+j}$ or $a^j = 1$. The set of different sequential powers a^i of the element $a \in \mathbb{F}_q$ for $i = \overline{0, n-1}$ such, that every $a^i \neq 1$ except $a^0 = a^n = 1$, is called a *multiplicative cyclic group* of order n of the field $\mathbb{F}_q$. The element a is called a generator of order n or simply an element of order n, if n is the minimum integer such that $a^n = 1,\ n > 0$.

An element of order $q-1$ is called *a primitive element* of the field $\mathbb{F}_q$.

Let us give the following important theorems without proofs.

Theorem 1.2 (Fermat)**.** *Every element b of the field $\mathbb{F}_q$ satisfies the congruence relation $b^q \equiv b$.*

Theorem 1.3. *Every element of the field $GF(q)$ belongs to a cyclic group of order n, where n divides $q-1$.*

A field $\mathbb{F}_q$ has primitive elements. Indeed, if $q-1$ is prime, then in $\mathbb{F}_q$, all elements except 0 and 1 are primitive, since $q-1$ has only two trivial divisors: 1 and $q-1$.

Let $q-1$ be non-prime. Assume that one primitive element $\alpha \in \mathbb{F}_q$ is known and the decomposition $q-1 = \prod_i p_i^{l_i}$ to prime factors p_i, where l_i are positive integers, is also known.

Consider the element $\beta = a^n$. If n divides $q-1$ then the order of β is at most $\frac{(q-1)}{n}$. If n and $q-1$ are coprime then there exists an integer $N = n^{-1} \pmod{q-1}$. Then the sequence of residuals $k \equiv ni \pmod{q-1}$ for $i = 0, 1, \ldots,$ runs through the full set of residuals from 0 to $q-2$, since $Nk = Nni \equiv i \pmod{q-1}$. Hence, the elements $\beta = a^n$ are primitive if n and $q-1$ are coprime.

The number of primitive elements of the field $\mathbb{F}_q$, i.e., the number of integers n which are coprime to $q-1$, is given by the Euler function

$$\phi(q-1) = \prod_{i=1}^{k} p_i^{l_i-1}(p_i - 1),$$

where $q - 1 = \prod_{i=1}^{k} p_i^{l_i}$.

For practical implementation of a field and algebraic coding methods, at least one primitive element should be found. The following theorem helps to solve this problem.

Theorem 1.4. *Let $q - 1 = \prod_{i=1}^{k} p_i^{l_i}$. The element $\alpha \in \mathbb{F}_q$ is primitive if it satisfies: $\alpha^{\frac{(q-1)}{p_i}} \neq 1$, $i = 1, \ldots, k$.*

It follows from the above theorems that every element of the field $\mathbb{F}_q$ is a root of the equation $x^q - x = 0$. Elements of order n that divides $q-1$ are the roots of $x^n - 1 = 0$.

It follows from the definition of a primitive element $\alpha \in \mathbb{F}_q$ that elements $1, \alpha, \ldots, \alpha^{m-1}$ form a power basis of the field with operations modulo the minimal polynomial of the element α. Also every sequential powers α^l, α^{l+1}, $\ldots, \alpha^{l+m-1}$ form a basis.

Theorem 1.5. *For any elements a and b from $\mathbb{F}_{p^m}$, $m \geq 1$, it holds that*

$$(a+b)^p = a^p + b^p.$$

1.5 Polynomial ring over a finite field

A polynomial $f(x)$ in variable x over a finite field $\mathbb{F}_q$ is the following sum

$$f(x) = \sum_{i=0}^{n} f_i x^i \tag{1.2}$$

with coefficients $f_i \in \mathbb{F}_q$.

Computation of this sum for $x = \gamma$ is called *evaluation of the polynomial* at γ and the result of computation $f(\gamma)$ is called the *value of the polynomial* at the point γ. If $\gamma \in \mathbb{F}_{q^m}$, then $f(\gamma)$ belongs to the field $\mathbb{F}_{q^m}$ or its subfield.

The *degree of the polynomial* $f(x)$ is the maximum index of nonzero coefficient. The degree of polynomial $f(x)$ is denoted by $\deg(f)$. In the above definition, $\deg(f) = n$, if $f_n \neq 0$. If $f_n = 1$, then the polynomial is called *monic*.

For any n, all polynomials of degree up to n form an additive abelian group, for which *the sum* is

$$h(x) = f(x) + g(x) = \sum_{i=0}^{n} (f_i + g_i)x^i,$$

where $\deg(h) \leq max\{\deg(f), \deg(g)\}$. Commutativity of the polynomial addition follows from commutativity of addition in $\mathbb{F}_q$ of the coefficients. The polynomial with all zero coefficients is the zero in the group.

The product of polynomials of arbitrary degrees is as follows

$$h(x) = f(x)g(x) = \sum_{i=0}^{t} x^i f_i \sum_{i=0}^{s} x^i g_i$$

$$= \textstyle\sum_{i=0}^{s+t} x^k \sum_{i=0}^{k} f_i g_{k-i} = \sum_{k=0}^{s+t} x^k h_k,$$

where $h_k = \sum f_i g_{k-i}$. The degree of $h(x)$ is $s + t$, if $f_s \neq 0$ and $g_t \neq 0$. Commutativity of polynomial multiplication follows from commutativity of multiplication of their coefficients. Multiplication of polynomials requires at most: st additions and $(s + 1)(t + 1)$ multiplications of the coefficients.

The set of polynomials of finite degree forms *a commutative ring* with the unit element $e(x) = 1$.

Division with remainder on the set of polynomial of any degree is defined by a division algorithm. Given arbitrary polynomials $f(x)$ and $g(x)$ over $\mathbb{F}_q$, the goal of a division algorithm is to find two polynomials: the quotient $Q(x)$ and the remainder $R(x)$ that satisfy $f(x) = g(x)Q(x)+R(x)$ and $\deg(R) < \deg(g)$. Any polynomial of degree s can be written as $g_s(x^s + \sum g_i)x^i$, where the expression in the brackets is a monic polynomial. With this, let us give a division algorithm for a monic divisor.

Input:

$$f(x) = \sum_{i=0}^{t} f_i x^i, g(x) = \sum_{i=0}^{s} g_i x^i, g_s = 1,\ f_t \neq 0.$$

Begin:

$$F_i = \left\{ \begin{array}{l} f_i,\ \text{if } i = \overline{0,t}, \\ 0,\ i > t; \end{array} \right\} \quad G_i = \left\{ \begin{array}{l} g_i,\ \text{if } i = \overline{0,s}, \\ 0,\ \text{if } i > s. \end{array} \right\}$$

If $t < s$, then set

$$Q(x) = 0, \quad R(x) = f(x)$$

and stop.

If $t \geq s$, then use long division, shown by the following two examples.

1. Polynomials having the same degree:

$$f(x) = f_t x^t + f_{t-1} x^{t-1} + \cdots + f_1 x + f_0, \quad g(x) = x^t + g_{t-1} x^{t-1} + \cdots + g_1 x + g_0.$$

Step 1: Divide the leading coefficient of $f(x)$ by the one of $g(x)$, get f_t, which is one coefficient from $Q(x)$.
Step 2. Multiply $g(x)$ by f_t and subtract the result from $f(x)$:

$$R(x) = f(x) - f_t g(x) = (f_{t-1} - f_t g_{t-1}) x^{t-1} + \cdots + (f_1 - f_t g_1) x + (f_0 - f_t g_0).$$

The degree of $R(x)$ is less than the degree of $g(x)$ and the algorithm stops after two steps with results

$$Q(x) = f_t, \quad R(x) = (f_{t-1} - f_t g_{t-1}) x^{t-1} + \cdots + (f_1 - f_t g_1) x + (f_0 - f_t g_0).$$

2. The degree of $g(x)$ is less than the degree of $f(x)$ by 1:

$$f(x) = f_t x^t + f_{t-1} x^{t-1} + \cdots + f_1 x + f_0, \quad g(x) = x^{t-1} + g_{t-2} x^{t-2} + \cdots + g_1 x + g_0.$$

Step 1. Divide the leading coefficient of $f(x)$ by the one of $g(x)$, obtain f_t, which is a coefficient from $Q(x)$.
Step 2. Multiply $g(x)$ by f_t and subtract the result from $f(x)$:

$$\widehat{f}(x) = f(x) - f_t x g(x) = (f_{t-1} - f_t g_{t-2}) x^{t-1} + \cdots + (f_1 - f_t g_1) x^2 + (f_0 - f_t g_0) x.$$

The degree of $\widehat{f}(x)$ equals the degree of $g(x)$. Hence, we have the case of the first example where the algorithm stops in two steps. The total number of steps is four in this case.

This algorithm requires at most $(t - s + 1)s$ multiplications and the same number of additions in the field of coefficients. This bound can be replaced by $(t - s + 1)w$ if the divisor has only w nonzero coefficients.

If the divider $g(x)$ is not monic then one can use the division algorithm with the monic polynomial $g_s^{-1} g(x)$. This requires computation of the inverse element g_s^{-1} and s multiplications. Then $t - s + 1$ multiplications are required to make corrections of the quotient.

A ring of residue classes modulo a polynomial of degree m, irreducible over $\mathbb{F}_q$, is a field of order q^m. In the general case, any polynomial can be used as a modulo. For example, the theory of cyclic codes over $\mathbb{F}_q$ uses modulo $x^n - 1$ and its factorization, where n is code length. The set of codewords of a length n of a cyclic code forms an ideal in the residue class ring modulo $x^n - 1$, generated by its factor. Every codeword can be written as $c(x) \equiv g(x)u(x)(\mod x^n - 1)$, where $u(x)$ is a polynomial of degree $n - \deg(g) - 1$ representing encoded message.

1.6 Inverse elements

Every nonzero element of a field has the inverse element satisfying $aa^{-1} = 1$. From Fermat's theorem we get $a^{-1} = a^{q-2}$, where $a \in \mathbb{F}_q$. In multiplicative representation we have $a^{-1} = \alpha^{-i}$, for some i, where α is a primitive element of the field.

It is asymptotically faster to compute a^{-1} using the Euclidean algorithm, which for any integers (or polynomials) a and b gives the solution of equation $aQ + bP = d$, where d is the greatest common divisor (GCD) of a, b. Consider the prime field $\mathbb{F}_p$. For any integer $b < p$, GCD of $(b, p) = 1$. From the equation $pQ + bP = 1$ we have $b^{-1} \equiv P \mod p$.

In the case of a residual field $\mathbb{F}_{p^m}$ modulo a non-reducible polynomial $\mu(x)$ of degree m, for any $b(x)$ over $\mathbb{F}_p$ of degree less than m, the GCD of $(b(x), \mu(x)) = \gamma$, where $\gamma \in \mathbb{F}_p$. From the equality $\mu(x)Q(x) + b(x)P(x) = \gamma$ we obtain $b^{-1}(x) = \gamma^{-1}P(x)(\mod \mu(x))$, where γ^{-1} is the inverse element in the prime subfield.

1.7 Division with remainder for integers and polynomials

For integers and polynomials there are algorithms for division with remainder (Euclidean algorithms).

For integers. For any two integers r_0 and r_1 there exist unique integers *quotient* q_1 and *remainder* r_2 such that

$$\begin{aligned}&r_0 = q_1 r_1 + r_2,\\&\text{ where}\\&0 \leq r_2 < |r_1|.\end{aligned}$$

For polynomials. For any two polynomials $r_0(x)$ and $r_1(x)$ over $\mathbb{F}_p$ there exist unique polynomials *quotient* $q_1(x)$ and *remainder* $r_2(x)$ such that

$$\begin{aligned}&r_0 = q_1(x) r_1(x) + r_2(x),\\&\text{ where either } r_2(x) = 0,\\&\text{ or } \deg(r_2(x)) < \deg(r_1(x)).\end{aligned}$$

Algorithms computing division with remainder are used to find the greatest common divisor of two integers or two polynomials.

Let us consider the Euclidean algorithm for polynomials in details.

1.8 Euclidean algorithm for polynomials

For any two polynomials $r_0(x)$ and $r_1(x)$ over $\mathbb{F}_p$ there exists a *monic* polynomial $d(x) = \gcd(r_0(x), r_1(x))$, called *the greatest common divisor* (GCD), which divides both polynomials $r_0(x)$ and $r_1(x)$ and is divisible by any other common divisor of polynomials $r_0(x)$ and $r_1(x)$. The Euclidean algorithm allows us to compute $d(x)$ by using a division algorithm multiple times.

Later on we write f instead of $f(x)$ if it is clear from the context that we mean a polynomial $f(x)$.

First of all, let us introduce two sequences of auxiliary polynomials a_i and b_i:

$$\begin{array}{r|ll} a_i = -q_{i-1} a_{i-1} + a_{i-2}, & a_0 = 1, & a_1 = 0.\\ b_i = -q_{i-1} b_{i-1} + b_{i-2}, & b_0 = 0, & b_1 = 1.\end{array}$$

We will assume that $\deg(r_0) \geq \deg(r_1)$.

Step 1. Divide with remainder $r_0(x)$ by $r_1(x)$. Compute auxiliary polynomials $a_0(x)$ and $b_0(x)$.

$$1.\ \Big|\ r_0 = q_1 r_1 + r_2,\ \Big|\ a_0 = 1,\ \Big|\ b_0 = 0.$$

If $r_2(x) = 0$ then stop. In this case, GCD is $d(x) = r_1(x)$ normalized to the monic form.

If $r_2(x) \neq 0$, then go to the next step.

Step 2. Divide $r_1(x)$ by $r_2(x)$, compute $a_1(x)$ and $b_1(x)$.

$$\begin{array}{r|l|l|l}
1. & r_0 = \ q_1 r_1 + r_2, & a_0 = 1, & b_0 = 0. \\
2. & r_1 \ = q_2 r_2 + r_3, & a_1 = 0, & b_1 = 1.
\end{array}$$

If $r_3(x) = 0$ then stop. In this case $d(x) = r_2(x)$ normalized to the monic form.

If $r_3(x) \neq 0$ then go to the next step.

Step 3. Divide $r_2(x)$ by $r_3(x)$, compute $a_2(x)$ and $b_2(x)$.

$$\begin{array}{r|l|l|l}
1. & r_0 = q_1 r_1 + r_2, & a_0 = 1, & b_0 = 0. \\
2. & r_1 = q_2 r_2 + r_3, & a_1 = 0, & b_1 = 1. \\
3. & r_2 = q_3 r_3 + r_4, & a_2 = -q_1 a_1 + a_0, & b_2 = -q_1 b_1 + b_0.
\end{array}$$

If $r_4(x) = 0$ then stop. In this case $d(x) = r_3(x)$, normalized to the monic form.

If $r_4(x) \neq 0$ then go to the next step. Continue until Step $s + 1$ such that at the previous step s the remainder $r_{s+1}(x) \neq 0$ and at step $s + 1$ the remainder $r_{s+2}(x) = 0$.

Step $s + 1$. Divide $r_s(x)$ by $r_{s+1}(x)$, compute $a_s(x)$ and $b_s(x)$.

$$\begin{array}{r|ll|l|l}
1 & r_0 = & q_1 r_1 + r_2, & a_0 = 1, & b_0 = 0. \\
2 & r_1 = & q_2 r_2 + r_3, & a_1 = 0, & b_1 = 1. \\
3 & r_2 = & q_3 r_3 + r_4, & a_2 = -q_1 a_1 + a_0, & b_2 = -q_1 b_1 + b_0. \\
\vdots & & \vdots & \vdots & \vdots \\
s+1 & r_s \ = & q_{s+1} r_{s+1}, & a_s = -q_{s-1} a_{s-1} + a_{s-2}, & b_s = -q_{s-1} b_{s-1} + b_{s-2}.
\end{array}$$

Since the degree $\deg(r_1)$ is finite and $\deg(r_i)$ is decreasing, the procedure will stop after a finite number of steps. The GCD of $r_0(x)$ and $r_1(x)$ is

$$d(x) = \gcd(r_0(x),\ r_1(x)) = a^{-1} r_{s+1}(x),$$

where a is the leading coefficient of the last nonzero remainder $r_{s+1}(x)$.

On the way, one can observe that

$$r_i = a_i r_0 + b_i r_1, \qquad i = 0,\ 1,\ \dots\ .$$

1.9 Computation of powers and logarithms

Some procedures of algebraic decoding require computation of sequential powers of a field element. Let us consider two methods to compute b^t, where $b \in \mathbb{F}_q$ and the exponent t is any integer.

1. If $t = t_1 t_2$ then $b^t = (b^{t_1})^{t_2}$. This method requires at most $t_1 + t_2$ multiplications in $\mathbb{F}_q$.

2. Let $t = \sum_{i=0}^{m} \tau_i 2^i$, where $\tau_m = 1$, $\tau_i \in 0, 1$, then $t = \tau_0 + 2(\tau_1 + 2(\dots \tau_m))$. Computation using the formula $b^t = (((b^{\tau_m})^2 \dots)^2 b^{\tau_1})^2 b^{\tau_0}$ requires at most $2(m-1)$ multiplications in $\mathbb{F}_q$. More precisely, it requires at most $(m-1)$ multiplications and $(m-1)$ squarings.

The second method is convenient for arbitrary t, while for a given t it is convenient to combine these two methods to compute, e.g., an inverse element of a field.

Computation of a fractional power $\frac{1}{t}$ of an element is connected with solving the polynomial equation $x^t - b = 0$.

Logarithm of $b \in \mathbb{F}_q$ base $\alpha \in \mathbb{F}_q$ is the exponent in multiplicative representation of b: $\log_\alpha b = u$, if $b = \alpha^u$, $u \geq 0$. In general, α is any element of order n of the field $\mathbb{F}_q$, where n divides $q - 1$.

1.10 Trace and normal basis

The trace of an element $a \in \mathbb{F}_{p^m}$ is the sum $Tr(a) = a + a^p + a^{p^2} + \dots + a^{p^{m-1}}$. The main properties of the trace function:

1. $Tr(a) \in \mathbb{F}_p$;
2. $Tr(a + b) = Tr(a) + Tr(b)$;
3. $(Tr(a))^p = Tr(a^p) = Tr(a)$;

4. $Tr(1) = m(\mod p)$;

5. $Tr(0) = 0$;

6. $Tr(\beta) = f_{i-1}\frac{m}{t}(\mod p)$,

where $f(\beta) = 0$, $f(x) = \sum_{i=0}^{t} f_i x^i$ is the minimal polynomial of the element β; t divides m. The trace over any subfield $\mathbb{F}_q$ is defined similarly.

There are many applications of the trace function. The most important are: solving polynomial equations, building Galois fields, construction of sequences over $\mathbb{F}_p$ with good correlation properties.

A basis of a vector space is not unique. The most frequently used are polynomial basis and normal basis. A normal basis is as follows: $\gamma, \gamma^p, \gamma^{p^2}, \ldots, \gamma^{p^{m-1}}$, $\gamma \in \mathbb{F}_{p^m}$. An important property of a normal basis is $Tr(\gamma) \neq 0$. For every field $\mathbb{F}_{p^m}$ there exists a normal basis.

1.11 Ring of linearized polynomials

Denote $[i] = q^{\{i \mod m\}}$. Let q be a prime power. The polynomial

$$F(z) = \sum_{i=0}^{n} F_i z^{[i]},$$

where $F_i \in \mathbb{F}_{q^m}$, $i = 0, 1, \ldots, n$ is called *linearized* over the field $\mathbb{F}_{q^m}$. Denote by $R_m[z]$ the set of all such linearized polynomials. Let us define operations of addition and multiplication on this set.

1. Addition is defined in the same way as for ordinary polynomials: if

$$F(z) = \sum_{i=0}^{n} F_i z^{[i]},\ G(z) = \sum_{i=0}^{n} G_i z^{[i]},$$

then

$$C(z) = F(z) + G(z) = \sum_{i=0}^{n} (F_i + G_i) z^{[i]}. \tag{1.3}$$

The sum of linearized polynomials is a linearized polynomial.

2. The operation of symbolic multiplication, denoted by $*$, differs from multiplication of ordinary polynomials. If $F(z) = \sum\limits_{i=0}^{n_1} F_i z^{[i]}$ and $G(z) = \sum\limits_{k=0}^{n_2} G_k z^{[k]}$, then

$$\begin{aligned} C(z) &= \sum_{i=0}^{n_1+n_2} C_i z^{[i]} = F(z) * G(z) = F(G(z)) \\ &= \sum_{i=0}^{n_1} F_i (G(z))^{[i]} = \sum_{j=0}^{n_1+n_2} \left(\sum_{i+k=j} F_i G_k^{[i]} \right) z^{[i+k]}. \end{aligned} \tag{1.4}$$

Thus, the product $C(z)$ of linearized polynomials is also a linearized polynomial with coefficients $C_j = \sum\limits_{i+k=j} F_i G_k^{[i+k]}$. In contrast to ordinary multiplication, the symbolic multiplication is a non-commutative operation: $F(z) * G(z) \neq G(z) * F(z)$ in general. However the symbolic multiplication is associative:

$$F(z) * (G(z) * H(z)) = (F(z) * G(z)) * H(z).$$

The defined operations are also distributive:

$$(F(z) + G(z)) * H(z) = F(z) * H(z) + G(z) * H(z),$$

$$H(z) * (F(z) + G(z)) = H(z) * F(z) + H(z) * G(z).$$

Hence, the set of linearized polynomials $R_m[z]$ with the operations of addition and (symbolic) multiplication is a non-commutative ring. The unit of the ring $R_m[z]$ is the linearized polynomial $e(z) = z$. Indeed, for any polynomial $F(z) \in R_m[z]$ it holds that $z * F(z) = F(z) * z = F(z)$.

The q-degree of the polynomial $F(z) = \sum_i F_i z^{[i]}$, denoted by $q\deg(F)$, is the maximum index i for which $F_i \neq 0$. This coefficient F_i is called *the leading coefficient.* If $F(z) \neq 0$ and $G(z) \neq 0$, then $q\deg(F * G) \geq q\deg(F)$.

1.11.1 Left and right Euclidean algorithms

There are Euclidean algorithms for left and right divisions in the ring $R_m[z]$. Let us start with the *left* division. Let $F_1(z) = \sum_{i=0}^{n} F_{1i} z^{[i]}$ be any polynomial of

q-degree $q\deg(F_1) = n$ and $F_0(z) = \sum_{k=0}^{m} F_{0k} z^{[k]}$ be any polynomial of q-degree $q\deg(F_0) = m > n$. Subtract from $F_0(z)$ the polynomial $F_{0m} F_{1n}^{[n-m]} z^{m-n} * F_1(z)$. Then the q-degree of the difference $D(z)$ will be less than m. If the $q\deg(D)$ is at least n, then the leading coefficient of $D(z)$ can be removed by subtracting correct left multiple of the polynomial $F_1(z)$. By continuing this procedure, at the end we have $F_0(z) = G_1(z) * F_1(z) + F_2(z)$ where the remainder $F_2(z)$ is either the all zero polynomial or the polynomial of q-degree less than n, i.e., $q\deg(F_2) < q\deg(F_1)$.

The *right* division algorithm can be obtained by subtracting the right multiples of the polynomial $F_1(z)$: $F_0(z) = F_1(z) * Q(z) + f_2(z)$, where either $f_2(z) = 0$, or $q\deg(f_2) < q\deg(F_1)$.

Let us consider the left division in details. The right division is similar. Let us write the sequence of equalities:

$$\begin{array}{l} F_0(z) = G_1(z) * F_1(z) + F_2(z),\ q\deg(F_2) < q\deg(F_1); \\ F_1(z) = G_2(z) * F_2(z) + F_3(z),\ q\deg(F_3) < q\deg(F_2); \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ F_{s-1}(z) = G_s(z) * F_s(z) + F_{s+1}(z),\ q\deg(F_{s+1}) < q\deg(F_s); \\ F_s(z) = G_{s+1}(z) * F_{s+1}(z). \end{array} \tag{1.5}$$

Here, the last nonzero remainder $F_{s+1}(z)$ is the right symbolic GCD of the polynomials $F_0(z)$ and $F_1(z)$. If GCD is cz with $c \in \mathbb{F}_{q^m}$, then the polynomials $F_0(z)$ and $F_1(z)$ are called coprime.

Let us recurrently define polynomials $U_i(z)$, $A_i(z)$, $V_i(z)$, $B_i(z)$, for $i \geq 1$:

$$\begin{array}{ll} U_i(z) = U_{i-1}(z) * G_i(z) + U_{i-2}(z), & U_0(z) = z,\ U_{-1}(z) = 0, \\ A_i(z) = G_i(z) * A_{i-1}(z) + A_{i-2}(z), & A_0(z) = z,\ A_{-1}(z) = 0, \\ V_i(z) = V_{i-1}(z) * G_i(z) + V_{i-2}(z), & V_0(z) = 0,\ V_{-1}(z) = z, \\ B_i(z) = G_i(z) * B_{i-1}(z) + B_{i-2}(z), & B_0(z) = 0,\ B_{-1}(z) = z. \end{array} \tag{1.6}$$

Then

$$\begin{array}{l} F_0(z) = U_i(z) * F_i(z) + U_{i-1}(z) * F_{i+1}(z), \\ F_1(z) = V_i(z) * F_i(z) + V_{i-1}(z) * F_{i+1}(z), \end{array} \tag{1.7}$$

and

$$F_i(z) = (-1)^i (B_{i-1}(z) * F_0(z) - A_{i-1}(z) * F_1(z)). \tag{1.8}$$

1.11.2 Factor ring of linearized polynomials

Together with the ring $R_m[z]$ defined above let us consider its factor ring modulo polynomial $z^{[m]} - z$ consisting of the right residue classes. The elements of the factor ring can be identified with linearized polynomials of q-degree at most $[m-1] = q^{m-1}$.

Let $F(z) = \sum_{i=0}^{m-1} f_i z^{[i]} \in R_m[z]$. Then

$$F^{[1]}(z) = f_{m-1}^{[1]} z^{[0]} + f_0^{[1]} z^{[1]} + \ldots + f_{m-2}^{[1]} z^{[m-1]}.$$

Hence, q-powering of a polynomial in the ring R_m is equivalent to q-powering of its coefficients followed by the right cyclic shift of the coefficients. We call this operation a *q-cyclic shift*. Every ideal in the ring $R_m[z]$ is the main ideal generated by a polynomial $G(z)$, which satisfies $z^{[m]} - z = H(z) * G(z)$, i.e., $G(z)$ is the right divisor of the polynomial $z^{[m]} - z$. Notice, if the leading coefficient of $G(z)$ is 1, then polynomials $G(z)$ and $H(z)$ commute. The ideal $\{G\}$ is invariant with respect to q-cyclic shift, i.e., if $g \in \{G\}$, then $g^{[i]} \in \{G\}$ as well.

The two-sided ideal in the ring $R_m[z]$, generated by $z^{[m]} - z$, splits $R_m[z]$ into the set of residue classes modulo polynomial $z^{[m]} - z$, isomorphic to the facror ring $R_m[z]/(z^{[m]} - z)$. Denote this factor ring by $L_m[z]$. Elements of $L_m[z]$ can be identified with all possible linearized polynomials over the field $\mathbb{F}_{q^m}$ with q-degree at most $m - 1$.

To do this, addition and multiplication of polynomials $F(z) = \sum\limits_{i=0}^{m-1} F_i z^{[i]}$ and $G(z) = \sum\limits_{i=0}^{m-1} G_i z^{[i]}$ from the ring $L_m[z]$ should be defined as follows

$$\begin{aligned} F(z) + G(z) &= \sum_{i=0}^{m-1} (F_i + G_i) z^{[i]} && (1.9) \\ F(z) \circledast G(z) &= F(z) * G(z) \mod z^{[m]} - z. && (1.10) \end{aligned}$$

The ring $L_m[z]$ is a finite non-commutative ring which consists of q^{m^2} linearized polynomials. The Euclidean division algorithms in this ring are induced by the correspondent algorithms in $R_m[z]$. Hence all ideals in $L_m[z]$ are main.

Consider the structure of a left ideal in details. Any such ideal is defined by a *generator* polynomial $G(z)$, where $G(z)$ is a divisor of $z^{[m]} - z$. Elements of the ideal $\{G\}$ are all possible polynomials of the form

$$g(z) = c(z) \circledast G(z), \tag{1.11}$$

where $c(z)$ is any polynomial from $L_m[z]$.

If the generator polynomial has q-degree r, then the dimension of the ideal equals $k = m - r$.

Another way to define the ideal $\{G\}$ uses the polynomial $H(z)$ satisfying $z^{[m]} - z = G(z) * H(z)$ as follows. A polynomial $g(z)$ belongs to the ideal $\{G\}$ if and only if

$$g(z) \circledast H(z) = 0. \tag{1.12}$$

Indeed, if $g(z)$ is the same as in (1.11), then

$$g(z) \circledast H(z) = c(z) \circledast G(z) \circledast H(z) = c(z) \circledast (z^{[m]} - z) = 0. \tag{1.13}$$

Inversely, if (1.12) holds, then

$$g(z) * H(z) = c(z) * (z^{[m]} - z) = c(z) * G(z) * H(z). \tag{1.14}$$

Hence, $g(z) = c(z) \circledast G(z)$.

Consider the polynomial

$$g(z) = g_0 z + g_1 z^{[1]} + \cdots + g_{m-2} z^{[m-2]} + g_{m-1} z^{[m-1]}. \tag{1.15}$$

Recall that q-cyclic shift of the polynomial is

$$\widetilde{g}(z) = g_{m-1}^{[1]} z + g_0^{[1]} z^{[1]} + g_1^{[1]} z^{[2]} + \cdots + g_{m-2} z^{[m-1]}. \tag{1.16}$$

If $g(z) \in \{G(z)\}$ then $z^{[1]} \circledast g(z) \in \{G(z)\}$. Hence, $z^{[1]} \circledast g(z) = g(z)^{[1]}$ mod $(z^{[m]} - z) = \widetilde{g}(z) \in \{G(z)\}$. Thus, if a polynomial belongs to the ideal, then all its q-cyclic shifts also belong to the same ideal.

2

Rank metric codes

Introduction

Denote by $\mathbb{F}_q$ a finite field consisting of q elements, where q is a prime power. Later on, this field is called the *base field*. The extension of the field of degree m consists of q^m elements and is denoted by $\mathbb{F}_{q^m}$.

There are two representations of codes in rank metric: *matrix* representation and *vector* representation.

Matrix representation uses the space $\{\mathbb{F}_q^{m\times n}\}$ of rectangular $m\times n$ matrices over the base field $\mathbb{F}_q$. Dimension of the space is mn.

The *norm* $\mathfrak{N}(M)$ of a matrix $M \in \mathbb{F}_q^{m\times n}$ is its algebraic rank over the field $\mathbb{F}_q$, $\mathfrak{N}(M) = \mathrm{Rk}_{\mathbb{F}_q}(M)$.

The *rank distance* between two matrices $M_1, M_2 \in \mathbb{F}_q^{m\times n}$ is defined as the norm of their difference: $d_r(M_1,\ M_2) = \mathrm{Rk}_{\mathbb{F}_q}(M_1 - M_2)$.

The *matrix code* $\mathcal{M}$ is a subset of the space $\{\mathbb{F}_q^{m\times n}\}$ of matrices.

The *rank code distance* d_r is the minimum rank distance between two different code matrices:

$$d_r = \min\{\mathrm{Rk}_{\mathbb{F}_q}(M_i - M_j) : M_i, M_j \in \mathcal{M},\ i \neq j\}.$$

A matrix code $\mathcal{M}$ with code distance d_r is $\mathbb{F}_q$*-linear* if the code is a k-dimensional subspace of the space $\mathbb{F}_q^{m\times n}$, where $k \in \{1, \ldots, mn\}$. The code is named $[m \times n, k, d_r]$-code.

The cardinality of any matrix code $\mathcal{M}$ with $m \geq n$ and code distance d_r satisfies the Singleton bound:

$$|\mathcal{M}| \leq q^{m(n-d_r+1)}.$$

The dimension k of a $\mathbb{F}_q$-linear $[m \times n, k, d_r]$-code satisfies: $k \leq m(n - d_r + 1)$.

If a matrix code $\mathcal{M}$ reaches the Singleton bound, i.e.

$$|\mathcal{M}| = q^{m(n-d_r+1)},$$

or for a linear code

$$k = m(n - d_r + 1),$$

then the code is called the *maximum rank distance* (MRD) code.

For the **vector representation**, the ambient space is the space $\mathbb{F}_{q^m}^n$ of vectors of length n over the extension field $\mathbb{F}_{q^m}$.

Norm of a vector $\mathbf{v} \in \mathbb{F}_{q^m}^n$ is the *column rank* of the vector

$$N(\mathbf{v}) = \mathrm{Rk}_{\mathbb{F}_q}(\mathbf{v}),$$

which is defined as the *maximum* number of the vector components linearly independent over the base field $\mathbb{F}_q$.

The *rank distance* between two vectors $\mathbf{v}_1,\ \mathbf{v}_2$ is defined as the norm of their difference: $d_r(\mathbf{v}_1,\ \mathbf{v}_2) = \mathrm{Rk}_{\mathbb{F}_q}(\mathbf{v}_1 - \mathbf{v}_2)$.

The *vector code* $\mathcal{V}$ is any subset of the vector space $\{\mathbb{F}_{q^m}^n\}$.

The *rank code distance* d_r is the minimum rank distance between two different code vectors:

$$d_r = \min\{\mathrm{Rk}_{\mathbb{F}_q}(\mathbf{v}_i - \mathbf{v}_j) : \mathbf{v}_i, \mathbf{v}_j \in \mathcal{M},\ i \neq j\}.$$

A vector code $\mathcal{V}$ with rank code distance d_r is $\mathbb{F}_{q^m}$*-linear* if the code $\mathcal{V}$ is a k-dimensional subspace, $k \in \{1,\ 2,\ \ldots, n\}$, of the vector space $\mathbb{F}_{q^m}^n$, where scalars are elements of the extension field $\mathbb{F}_{q^m}$. The code is named $[n, k, d_r]$-code. $\mathbb{F}_q$-linear vector codes can also be defined, where codewords are elements of $\mathbb{F}_{q^m}^n$ and the scalars are elements of the base field $\mathbb{F}_q$.

The cardinality $|\mathcal{V}|$ of any vector code with code distance d_r and with $m \geq n$ satisfies the Singleton bound:

$$|\mathcal{V}| \leq q^{m(n-d_r+1)}.$$

For any $\mathbb{F}_{q^m}$-linear vector $[n, k, d_r]$-code holds $k \leq n - d_r + 1$.

If a code reaches a Singleton bound then it is called an MRD code.

There exists close connection between *vector* and *matrix* codes. Let $\mathbf{\Omega} = \{\omega_1, \omega_2, \ldots, \omega_m\}$ be a basis of the extension field $\mathbb{F}_{q^m}$ considered as a vector space over $\mathbb{F}_q$. Take a vector $\mathbf{v} = (v_1, v_2, \ldots, v_j, \ldots, v_n)$, $v_j \in \mathbb{F}_{q^m}^n$. Every its component can be uniquely written as

$$v_j = a_{1,j}\omega_1 + a_{2,j}\omega_2 + \cdots + a_{i,j}\omega_i + \cdots + a_{m,j}\omega_m,$$

where the coefficients $a_{i,j}$ are taken from the base field $\mathbb{F}_q$. As a result, the vector $\mathbf{v}$ of length n over the extension field $\mathbb{F}_{q^m}$ can be written as the $m \times n$ matrix over the base field $\mathbb{F}_q$ by replacing every component v_j by the column vector $(a_{1,j}, a_{2,j}, \ldots, a_{m,j})^T$ using a fixed basis $\mathbf{\Omega}$ of the extension field. Inverse mapping is also possible.

2.1 Delsarte matrix codes in rank metric

Delsate proposed codes in rank metric in the space of bi-linear forms. Let us describe these codes as matrix codes in the space of rectangular $m \times n$ matrices $\{\mathbb{F}_q^{m\times n}\}$, $n \leq m$. The function $\mathrm{Tr}(x) = \sum\limits_{l=0}^{m-1} x^{q^l}$, $x \in \mathbb{F}_{q^m}$, is the trace function from the extension field $\mathbb{F}_{q^m}$ to the base field $\mathbb{F}_q$.

The Delsarte code is a $\mathbb{F}_q$-linear $[m \times n, k, d_r]$ MRD matrix code of dimension $k = m(n - d_r + 1)$. The code is defined by the following parameters:

1. the rank code distance d_r, $1 \leq d_r \leq n$,
2. the length $k = n - d_r + 1$ of message vectors
$$\mathbf{u} = \begin{bmatrix} u_0 & u_1 & \ldots & u_{n-d_r} \end{bmatrix} \in \mathbb{F}_{q^m}^{n-d_r+1},$$
3. the subspace, spanned by elements $\boldsymbol{N} = \{\nu_1, \nu_2, \ldots, \nu_n\}$ from the extension field $\mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$,
4. a basis $\mathbf{\Omega} = \{\omega_1, \omega_2, \ldots, \omega_m\}$ of the extension field $\mathbb{F}_{q^m}$.

The code $\mathcal{M}$ is a set of $m \times n$ matrices. Every code matrix is defined by a message vector $\mathbf{u}$

$$\mathcal{M} = \left\{ M(\mathbf{u}) : \mathbf{u} \in \mathbb{F}_{q^m}^{n-d_r+1} \right\},$$

where elements $M_{i,j}(\mathbf{u}), \quad i = 1, 2, \dots, m, \quad j = 1, 2, \dots, n$, of the matrix $M(\mathbf{u})$ are given by

$$M_{ij}(\mathbf{u}) = \mathrm{Tr}\left(\omega_i \sum_{s=0}^{n-d_r} u_s \nu_j^{q^s}\right).$$

The code distance d_r of the code $\mathcal{M}$ reaches the Singleton bound. Hence the Delsarte code is an MRD matrix code. General decoding methods for these codes are not described in existing publications in this field.

2.2 Dual bases

Recall, that for $x \in \mathbb{F}_{q^m}$ the map $\sigma(x) = x^q$ is called the Frobenius automorphism. This map preserves the base field: $\sigma(\mathbb{F}_q) = \mathbb{F}_q$. The map for vectors $\mathbf{x}$ and for matrices (M_{ij}) is defined element-vise as follows:

$$\sigma(\mathbf{x}) = \mathbf{x}^q = \sigma(x_1, x_2, \dots, x_n) = (x_1^q, x_2^q, \dots, x_n^q)$$

for $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_{q^m}^n$ and

$$\sigma((M_{ij})) = (M_{ij}^q).$$

To construct MRD vector codes we need some of the properties of dual bases.

Let components of the vector $\boldsymbol{\lambda} = \begin{pmatrix}\lambda_1 & \lambda_2 & \dots & \lambda_m\end{pmatrix}$ form a basis of the extension field $\mathbb{F}_{q^m}$. The Moore matrix [Moo96] for this basis is

$$\boldsymbol{\Lambda} = \begin{pmatrix} \boldsymbol{\lambda} \\ \boldsymbol{\lambda}^q \\ \boldsymbol{\lambda}^{q^2} \\ \dots \\ \boldsymbol{\lambda}^{q^{m-2}} \\ \boldsymbol{\lambda}^{q^{m-1}} \end{pmatrix} = \begin{pmatrix} \lambda_1 & \lambda_2 & \dots & \lambda_m \\ \lambda_1^q & \lambda_2^q & \dots & \lambda_m^q \\ \lambda_1^{q^2} & \lambda_2^{q^2} & \dots & \lambda_m^{q^2} \\ \dots & \dots & \dots & \dots \\ \lambda_1^{q^{m-2}} & \lambda_2^{q^{m-2}} & \dots & \lambda_m^{q^{m-2}} \\ \lambda_1^{q^{m-1}} & \lambda_2^{q^{m-1}} & \dots & \lambda_m^{q^{m-1}} \end{pmatrix}.$$

This matrix is nonsingular [LN83].

There is a unique dual basis $\boldsymbol{\mu} = \begin{pmatrix}\mu_1 & \mu_2 & \dots & \mu_m\end{pmatrix}$ such that the transpose of its Moore matrix

$$\boldsymbol{\mathcal{M}} = \begin{pmatrix} \boldsymbol{\mu} \\ \boldsymbol{\mu}^{q} \\ \boldsymbol{\mu}^{q^2} \\ \dots \\ \boldsymbol{\mu}^{q^{m-2}} \\ \boldsymbol{\mu}^{q^{m-1}} \end{pmatrix} = \begin{pmatrix} \mu_1 & \mu_2 & \dots & \mu_m \\ \mu_1^{q} & \mu_2^{q} & \dots & \mu_m^{q} \\ \mu_1^{q^2} & \mu_2^{q^2} & \dots & \mu_m^{q^2} \\ \dots & \dots & \dots & \dots \\ \mu_1^{q^{m-2}} & \mu_2^{q^{m-2}} & \dots & \mu_m^{q^{m-2}} \\ \mu_1^{q^{m-1}} & \mu_2^{q^{m-1}} & \dots & \mu_m^{q^{m-1}} \end{pmatrix}$$

is inverse to the matrix $\boldsymbol{\Lambda}$:

$$\boldsymbol{\Lambda}\boldsymbol{\mathcal{M}}^{\top} = \begin{pmatrix} \boldsymbol{\lambda} \\ \boldsymbol{\lambda}^{q} \\ \boldsymbol{\lambda}^{q^2} \\ \dots \\ \boldsymbol{\lambda}^{q^{m-2}} \\ \boldsymbol{\lambda}^{q^{m-1}} \end{pmatrix} \left(\boldsymbol{\mu}^{\top} \quad (\boldsymbol{\mu}^{q})^{\top} \quad \dots \quad \left(\boldsymbol{\mu}^{q^{m-2}}\right)^{\top} \quad \left(\boldsymbol{\mu}^{q^{m-1}}\right)^{\top} \right) =$$

$$= \begin{pmatrix} \lambda_1 & \lambda_2 & \dots & \lambda_m \\ \lambda_1^{q} & \lambda_2^{q} & \dots & \lambda_m^{q} \\ \lambda_1^{q^2} & \lambda_2^{q^2} & \dots & \lambda_m^{q^2} \\ \dots & \dots & \dots & \dots \\ \lambda_1^{q^{m-2}} & \lambda_2^{q^{m-2}} & \dots & \lambda_m^{q^{m-2}} \\ \lambda_1^{q^{m-1}} & \lambda_2^{q^{m-1}} & \dots & \lambda_m^{q^{m-1}} \end{pmatrix} \begin{pmatrix} \mu_1 & \mu_1^{q} & \dots & \mu_1^{q^{m-2}} & \mu_1^{q^{m-1}} \\ \mu_2 & \mu_2^{q} & \dots & \mu_2^{q^{m-2}} & \mu_2^{q^{m-1}} \\ \dots & \dots & \dots & \dots & \dots \\ \mu_m & \mu_m^{q} & \dots & \mu_m^{q^{m-2}} & \mu_m^{q^{m-1}} \end{pmatrix} = \boldsymbol{I}_m,$$

or equivalently for $i = 1, 2, \dots, m$ holds

$$\boldsymbol{\lambda}^{q^i} \cdot \left(\boldsymbol{\mu}^{q^j}\right)^{\top} = \sum_{s=1}^{m} \lambda_s^{q^i} \mu_s^{q^j} = \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{if } i \neq j. \end{cases} \tag{2.1}$$

2.3 MRD Gabidulin vector codes

Below we consider $\mathbb{F}_{q^m}$-linear maximum rank distance (MRD) vector codes over the extension field $\mathbb{F}_{q^m}$ of maximal possible length m. Shorter codes of length $n < m$ can be obtained by deleting $m - n$ columns from the generator or from the check matrix.

The rank metric $[m, k, d_r]$ vector code $\mathcal{V}$ can be defined by a full rank generator $k \times m$ matrix $\mathbf{G}_k$ over the extension field $\mathbb{F}_{q^m}$. Code vectors are all possible $\mathbb{F}_{q^m}$-linear combinations of rows of the matrix.

Equivalently, this code can be defined by a full rank check $(m-k) \times m$ matrix $\mathbf{H}_{m-k}$ over the extension field $\mathbb{F}_{q^m}$. The matrices should satisfy $\mathbf{G}_k \mathbf{H}_{m-k}^\top = \mathbf{0}$, where $\mathbf{0}$ is the all-zero $k \times (m-k)$ matrix. A vector code is an MRD code if $d_r = m - k + 1$. The following lemma allows us to verify this property.

Lemma 2.1 ([Gab85])**.** *Let $\mathbf{H}_{m-k} \in \mathbb{F}_{q^m}^{(m-k)\times n}$ be a check matrix of the code $\mathcal{V}$. The code $\mathcal{V}$ is an MRD code if and only if*

$$\mathrm{Rk}_{\mathbb{F}_{q^m}}(Y\mathbf{H}_{m-k}^\top) = m - k$$

for every matrix $Y \in \mathbb{F}_q^{(m-k)\times m}$ over the base field with rank $\mathrm{R}_{\mathbb{F}_q}(Y) = m - k$.

Another test is based on the known property [Gab85] that the dual code $\mathcal{V}^\perp$ is also an MRD code with code distance $d_r^\perp = k + 1$ and the generator matrix of the dual code $\mathcal{V}^\perp$ coincides with the check matrix $\mathbf{H}_{m-k}$ of the code $\mathcal{V}$. Hence the following lemma is true:

Lemma 2.2. *Let $\mathbf{G}_k \in \mathbb{F}_{q^m}^{k\times n}$ be a generator matrix of the code $\mathcal{V}$. The code $\mathcal{V}$ is an MRD code if and only if*

$$\mathrm{Rk}_{\mathbb{F}_{q^m}}(Y\mathbf{G}_k^\top) = k$$

for any matrix $Y \in \mathbb{F}_q^{k\times m}$ over the base field of rank $\mathrm{Rk}_{\mathbb{F}_q}(Y) = k$.

2.3.1 Vector codes based on dual bases

Theorem 2.3 ([Gab85])**.** *Given dual bases $\boldsymbol{\lambda}$ and $\boldsymbol{\mu}$, the code $\mathcal{V}$ with generator and check matrices*

$$\mathbf{G}_k = \begin{pmatrix} \boldsymbol{\lambda} \\ \boldsymbol{\lambda}^{q} \\ \boldsymbol{\lambda}^{q^2} \\ \vdots \\ \boldsymbol{\lambda}^{q^{k-2}} \\ \boldsymbol{\lambda}^{q^{k-1}} \end{pmatrix}, \quad \mathbf{H}_{m-k} = \begin{pmatrix} \boldsymbol{\mu}^{q^k} \\ \boldsymbol{\mu}^{q^{k+1}} \\ \vdots \\ \boldsymbol{\mu}^{q^{m-2}} \\ \boldsymbol{\mu}^{q^{m-1}} \end{pmatrix} \tag{2.2}$$

is an MRD code, i.e., it has cardinality q^{mk} and code distance $d_r = m - k + 1$.

Indeed, both matrices are of full rank. From bases duality and from (2.1) it follows that $\mathbf{G}_k \, \mathbf{H}_{m-k}^{\top} = \mathbf{0}$. Using Lemma 2.1 one can prove that the distance of the code $\mathcal{V}$ is $d_r - 1 = m - k$.

2.3.2 Generalized vector codes

The following theorem shows another class of vector codes.

Theorem 2.4 ([KG05]). *Let s be a positive integer co-prime with the extension degree of the field, $\gcd(s, m) = 1$. Then the code $\mathcal{V}$ with the following generator and check matrices*

$$\mathbf{G}_k = \begin{pmatrix} \boldsymbol{\lambda} \\ \boldsymbol{\lambda}^{q^s} \\ \boldsymbol{\lambda}^{q^{2s}} \\ \vdots \\ \boldsymbol{\lambda}^{q^{(k-2)s}} \\ \boldsymbol{\lambda}^{q^{(k-1)s}} \end{pmatrix}, \quad \mathbf{H}_{m-k} = \begin{pmatrix} \boldsymbol{\mu}^{q^{ks}} \\ \boldsymbol{\mu}^{q^{(k+1)s}} \\ \vdots \\ \boldsymbol{\mu}^{q^{(m-2)s}} \\ \boldsymbol{\mu}^{q^{(m-1)s}} \end{pmatrix}$$

is an MRD code.

These codes are called *generalized* vector codes.

The codes introduced in Theorems 2.3 and 2.4 are $\mathbb{F}_{q^m}$-linear vector codes with the maximum rank distance, i.e., MRD-codes.

2.3.3 Vector codes based on linearized polynomials

Another way to construct rank metric vector codes is to use linearized polynomials. A linearized polynomial is a sum

$$\mathbf{u}(x) = u_0 x + u_1 x^q + u_2 x^{q^2} + \cdots + u_{k-1} x^{q^{k-1}}, \tag{2.3}$$

where coefficients u_i belong to the field $\mathbb{F}_{q^m}$.

Let us use the polynomial (2.3) to construct a vector code $\mathcal{V}$. In order to do this, select a basis $\boldsymbol{\lambda} = \begin{pmatrix}\lambda_1 & \lambda_2 & \dots & \lambda_m\end{pmatrix}$ and evaluate the polynomial (2.3) "at the point" $x = \boldsymbol{\lambda}$. In this way we obtain the following vector $\mathbf{u}(\boldsymbol{\lambda})$

$$\mathbf{u}(\boldsymbol{\lambda}) = \begin{pmatrix}u_0 & u_1 & \dots & u_{k-1}\end{pmatrix} \begin{pmatrix}\boldsymbol{\lambda} \\ \boldsymbol{\lambda}^q \\ \vdots \\ \boldsymbol{\lambda}^{q^{k-1}}\end{pmatrix},$$

which is a code vector of the code $\mathcal{V}$. Here, one can see the message vector $\mathbf{u} = \begin{pmatrix}u_0 & u_1 & \dots & u_{k-1}\end{pmatrix}$ and the generator matrix $\mathbf{G}_k$ of the vector MRD code.

By evaluation all linearized polynomials of degree at most q^{k-1} at the point $x = \boldsymbol{\lambda}$ we obtain all code vectors of the code $\mathcal{V}$ in Theorem 2.3.

For many years, the only known MRD matrix codes were those of Delsarte [Del78] and the vector MRD codes described in Theorems 2.3 and 2.4. Recently, new classes of vector MRD codes were suggested. In [She16], codes are defined using another type of linearized polynomials:

$$\mathbf{u}(x) = u_0 x + u_1 x^q + u_2 x^{q^2} + \dots + u_{k-1} x^{q^{k-1}} + \eta u_0^{q^h} x^{q^k}, \tag{2.4}$$

where $u_i \in \mathbb{F}_{q^m}$, $i = 0, 1, \dots, k$ and the coefficients u_i belong to the field $\mathbb{F}_{q^m}$. The coefficient η also belong to $\mathbb{F}_{q^m}$, with the restriction that its norm $N(\eta)$ satisfies

$$N(\eta) = \eta^{\frac{q^m-1}{q-1}} \neq 1. \tag{2.5}$$

For a basis $\boldsymbol{\lambda} = \begin{pmatrix}\lambda_1 & \lambda_2 & \dots & \lambda_m\end{pmatrix}$ let us compute the vector

$$\mathbf{u}(\boldsymbol{\lambda}) = u_0 \boldsymbol{\lambda} + u_1 \boldsymbol{\lambda}^q + u_2 \boldsymbol{\lambda}^{q^2} + \dots + u_{k-1} \boldsymbol{\lambda}^{q^{k-1}} + \eta u_0^{q^h} \boldsymbol{\lambda}^{q^k}.$$

This is one of the code vectors. By considering polynomials (2.4) with all possible message coefficients $\{u_0,\ u_1,\ \dots,\ u_{k-1}\}$ we obtain all the code vectors $\mathbf{u}(\boldsymbol{\lambda})$ of the new code. The cardinality of the code is q^{mk} and the rank code distance is $d_r = m - k + 1$, i.e., the new code is an MRD code.

The code construction based on the polynomial (2.4) gives $\mathbb{F}_{q^m}$-linear vector codes if the parameter $h = 0$. Otherwise, if $h \geq 1$ it gives $\mathbb{F}_q$-linear vector codes.

These codes are called *twisted codes.*

Remark 2.5. *This construction can't be used if $q = 2$, since any nonzero element $\eta \in \mathbb{F}_{2^m}$ has norm 1.*

Another class of MDR codes obtained using the linearized polynomials

$$\mathbf{u}(x) = u_0 x + u_1 x^{q^s} + u_2 x^{q^{2s}} + \cdots + u_{k-1} x^{q^{(k-1)s}} + \eta u_0^{q^h} x^{q^{ks}}, \quad u_i \in \mathbb{F}_{q^m} \tag{2.6}$$

is described in the papers [She16, LTZ18]. Here s is a positive integer such that $\gcd(s,m) = 1$ and the parameter η satisfies (2.5). These codes are called *generalized twisted codes.*

The generator and check matrices of $\mathbb{F}_{q^m}$-linear twisted codes [She16] are as follows

$$\widetilde{\mathbf{G}}_k = \begin{pmatrix} \boldsymbol{\lambda} + \eta\boldsymbol{\lambda}^{q^k} \\ \boldsymbol{\lambda}^q \\ \boldsymbol{\lambda}^{q^2} \\ \vdots \\ \boldsymbol{\lambda}^{q^{k-2}} \\ \boldsymbol{\lambda}^{q^{k-1}} \end{pmatrix}, \quad \widetilde{\mathbf{H}}_{m-k} = \begin{pmatrix} \boldsymbol{\mu}^{q^k} - \eta\boldsymbol{\mu} \\ \boldsymbol{\mu}^{q^{k+1}} \\ \vdots \\ \boldsymbol{\mu}^{q^{m-2}} \\ \boldsymbol{\mu}^{q^{m-1}} \end{pmatrix}. \tag{2.7}$$

Similarly, the generator and check matrices of $\mathbb{F}_{q^m}$-linear generalized twisted codes [LTZ18, She16] can be written as

$$\widetilde{\mathbf{G}}_k = \begin{pmatrix} \boldsymbol{\lambda} + \eta\boldsymbol{\lambda}^{q^{ks}} \\ \boldsymbol{\lambda}^{q^s} \\ \boldsymbol{\lambda}^{q^{2s}} \\ \vdots \\ \boldsymbol{\lambda}^{q^{(k-2)s}} \\ \boldsymbol{\lambda}^{q^{(k-1)s}} \end{pmatrix}, \quad \widetilde{\mathbf{H}}_{m-k} = \begin{pmatrix} \boldsymbol{\mu}^{q^{ks}} - \eta\boldsymbol{\mu} \\ \boldsymbol{\mu}^{q^{(k+1)s}} \\ \vdots \\ \boldsymbol{\mu}^{q^{(m-2)s}} \\ \boldsymbol{\mu}^{q^{(m-1)s}} \end{pmatrix}, \gcd(s,m) = 1. \tag{2.8}$$

New generalizations of $\mathbb{F}_{q^m}$-linear codes are proposed in the paper [PRS17]. It is shown that such MRD codes exist for the code length $n = 2^{-l}m$, where l is an integer and $2^l|m$. Explicit code construction uses the polynomials

$$\mathbf{u}(x) = u_0 x + u_1 x^q + \cdots + u_{k-1} x^{q^{k-1}} + \eta u_0 x^{q^{k-1+t}} : u_i \in \mathbb{F}_{q^m}, 1 < t < s-1. \tag{2.9}$$

Among other recent constructions of MDR codes let us mention the codes described in [OÖ16, OÖ17]. The paper [OÖ16] proposes (independently of

[She16]) $\mathbb{F}_q$-linear MRD codes for the cases $m = 3$, $d_r = 2$ and $m = 4$, $d_r = 3$. The authors of [OÖ17] suggest a class of MRD codes under the name *additive generalized twisted codes*. If the base field is $\mathbb{F}_q = \mathbb{F}_{p^u}$, where p is prime and $u \geq 2$ is integer, then additive generalized twisted MRD codes are $\mathbb{F}_p$-linear, but not necessarily F_q- or $\mathbb{F}_{q^m}$-linear.

The papers [She16, LTZ18, OÖ16, OÖ17, PRS17] do not consider any decoding methods to correct errors of restricted rank.

3

q-cyclic rank metric codes

In this chapter, we introduce a code class that is similar to cyclic codes in the Hamming metric.

Definition 1. *A code $\mathcal{M}$ is called* q-cyclic *if together with any code vector* $\mathbf{g} = \begin{pmatrix} g_0 & g_1 & \dots & g_{n-1} \end{pmatrix}$ *it contains the vector* $\widehat{\mathbf{g}} = \begin{pmatrix} g_{n-1}^{[1]} & g_0^{[1]} & \dots & g_{n-2}^{[1]} \end{pmatrix}$*, obtained from* $\mathbf{g}$ *by the cyclic shift of its components by one position to the right with raising them to the q-th power.*

Later on, we consider only linear q-cyclic rank metric codes. For simplicity, we will restrict ourselves to the case when $n = m$, i.e., when the code length n coincides with the extension degree m of the field $\mathbb{F}_{q^m}$.

3.1 q-cyclic codes as ideals

Denote by $L_m[z]$ the ring of linearized polynomials modulo $z^{[m]} - z$.

A linear (m, k)-code $\mathcal{M}$ is q-cyclic if and only if it is a left ideal of the ring $L_m[z]$. Since all ideals are principal in this ring, a q-cyclic (m, k)-code can be defined by a *generator* polynomial $G(z)$ of q-degree $r = m - k$. The polynomial $G(z)$ divides $z^{[m]} - z$:

$$H(z) * G(z) = z^{[m]} - z. \tag{3.1}$$

Given the polynomial $G(z)$, all code polynomials $g(z)$ can be obtained using the rule

$$g(z) = \left(\sum_{i=0}^{k-1} c_i z^{[i]} \right) * G(z) = \sum_{i=0}^{k-1} c_i G^{[i]}(z), \tag{3.2}$$

where the coefficients $c_i,\ i = 0, 1, \ldots, k-1$, independently take values from the field $\mathbb{F}_{q^m}$.

3.2 Check polynomials

Another way to define a q-cyclic code is to use a *check* polynomial $H(z) = H_0 z + \cdots + H_k z^{[k]},\ H_k = 1$, obtained from (3.1). Code polynomials $g(z)$ are all the solutions in the ring $L_m[z]$ of the equation

$$g(z) \circledast H(z) = 0. \tag{3.3}$$

Encoding using the check polynomial is based on the relation (3.3), which can be rewritten as

$$\left(\sum_{i=0}^{m-k-1} g_i z^{[i]} \right) \circledast H(z) = - \left(\sum_{i=m-k}^{m-1} g_i z^{[i]} \right) * H(z). \tag{3.4}$$

The q-degree of the polynomial in the left part of the equation is at most $m-1$. Hence, the operation of multiplication $\circledast$ in the ring $L_m(z)$ can be replaced by the operation of multiplication $*$ in the ring $R_m(z)$.

The encoding algorithm is as follows. We right multiply the "information part" of a code polynomial

$$G_0(z) = g_{m-k} z^{[m-k]} + \cdots + g_{m-1} z^{[m-1]}$$

by $H(z)$ in the ring $L_m(z)$, i.e., we reduce the product modulo $z^{[m]} - z$. Having obtained the polynomial we left divide by $H(z)$ in the ring $R_m(z)$. The remainder gives "the check" part $g_0 z + g_1 z^{[1]} + \cdots + g_{[m-k-1]} z^{[m-k-1]}$ of the code polynomial.

3.3 Defining q-cyclic codes by roots

Let $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ be a set of $\mathbb{F}_q$-linear independent elements of the field $\mathbb{F}_{q^m}$. A q-cyclic code can be defined by these elements as follows.

The polynomial $g(z)$ belongs to a q-cyclic (m, k)-code if and only if the roots of the polynomial are all linear combinations $u_1\alpha_1 + u_2\alpha_2 + \cdots + u_r\alpha_r$ with coefficients u_i from $\mathbb{F}_q$:

$$g(u_1\alpha_1 + u_2\alpha_2 + \cdots + u_r\alpha_r) = 0. \tag{3.5}$$

In fact, it is enough to require that

$$g(\alpha_s) = 0, \quad s = 1, 2, \ldots, r, \tag{3.6}$$

since the polynomial $g(z)$ is linearized and hence $g(u_1\alpha_1 + u_2\alpha_2 + \cdots + u_r\alpha_r) = \sum\limits_{s=1}^{r} u_s g(\alpha_s)$ for $u_s \in \mathbb{F}_q$. So, if $g(z) = g_0 z + \cdots + g_{m-1} z^{[m-1]}$ is a code polynomial, then

$$\sum_{i=0}^{m-1} g_i \alpha_s^{[i]} = 0, \quad s = 1, 2, \ldots, r. \tag{3.7}$$

From here it follows that a check matrix of the q-cyclic code defined by the roots can be written as

$$H = \begin{bmatrix} \alpha_1^{[0]} & \alpha_1^{[1]} & \ldots & \alpha_1^{[m-1]} \\ \alpha_2^{[0]} & \alpha_2^{[1]} & \ldots & \alpha_2^{[m-1]} \\ \vdots & \vdots & \ldots & \vdots \\ \alpha_r^{[0]} & \alpha_r^{[1]} & \ldots & \alpha_r^{[m-1]} \end{bmatrix}. \tag{3.8}$$

In this case, the generator polynomial $G(z)$ is the linearized polynomial of minimal q-degree that has $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ as the roots.

Example 4. *Let $r = 2$. Let $\alpha_1 = \gamma, \alpha_2 = \gamma^{[1]}$, where γ is an element of a normal basis of the field F_{q^m}. Then*

$$H = \begin{bmatrix} \gamma & \gamma^{[1]} & \ldots & \gamma^{[m-2]} & \gamma^{[m-1]} \\ \gamma^{[1]} & \gamma^{[2]} & \ldots & \gamma^{[m-1]} & \gamma \end{bmatrix}.$$

The code defined by the check matrix H has distance 3 in rank metric.

3.4 Generator matrices

In coordinate vector representation, a q-cyclic code can be defined by a generator matrix G. Denote by $\mathbf{c} = (c_0,\ c_1, \dots,\ c_{k-1})$ a vector of *information* symbols. Then the correspondent code vector g is

$$g = \mathbf{c}G. \tag{3.9}$$

Sometimes it is convenient to have a systematic encoding, where components of the information vector $\mathbf{c}$ can be found at fixed positions of the code vector. In a q-cyclic code, the information symbols can be placed at any k sequential position. It is convenient to place the information symbols to k leading positions $m-1,\ m-2, \dots,\ m-k$. In this case, the generator matrix can be obtained as follows. Divide in the ring $R_m[z]$ the monomial $z^{[i]}$ by the generator polynomial $G(z)$:

$$z^{[i]} = Q_i(z) * G(z) + R_i(z). \tag{3.10}$$

Then

$$z^{[i]} - R_i(z) = Q_i(z) * G(z) \tag{3.11}$$

are code polynomials. For $i = \{m-1,\ m-2,\ \dots,\ m-k\}$, these polynomials and correspondent vectors are linearly independent. These vectors form the rows of the generator matrix:

$$G = (-R\ I_k). \tag{3.12}$$

Here I_k is the identity matrix of order k, and R is the $k \times (m-k)$ matrix in which i-th row is the remainder $R_{m-i}(z)$ in the vector representation.

This encoding of a q-cyclic code can be implemented using the Euclidean algorithm as follows. Denote the information symbols

$$c_{r-1} = g_{m-1},\ c_{k-2} = g_{m-2}, \dots,\ c_0 = g_{m-k}$$

and the polynomial

$$G_0(z) = g_{m-1}z^{[m-1]} + g_{m-2}z^{[m-2]} + \cdots + g_{m-k}z^{[m-k]}.$$

Using right division of this polynomial by the generator polynomial $G(z)$ obtain

$$G_0(z) = Q(z) * G(z) + F(z), \quad q\text{deg}(F) < q\text{deg}(G) = m-k. \tag{3.13}$$

Then the coefficients $g_{m-i},\ i = k+1,\ \ldots,\ m$ of the remainder $F(z)$ give the remaining (check) symbols of the code vector:

$$\mathbf{g} = \left(\underbrace{g_0,\ g_1,\ \ldots,\ g_{m-k-1}},\ \overbrace{g_{m-k},\ \ldots,\ g_{m-1}} \right).$$

3.5 Check matrices

The check matrix H is defined by the check polynomial $H(z) = \sum\limits_{i=0}^{k} H_i z^{[i]}$ and has the form

$$\begin{aligned} H &= \begin{bmatrix} H_k & H_{k-1}^{[1]} & \ldots & H_0^{[k]} & 0 & \ddots & 0 \\ 0 & H_k^{[1]} & \ldots & H_1^{[k]} & H_0^{[k+1]} & 0 & 0 \\ \ddots & \ddots & \ddots & \ddots\ \ddots & \ddots & 0 & \\ 0 & 0 & \ldots & 0 & H_k^{[r-1]} & \ldots & H_0^{[m-1]} \end{bmatrix} \\ &= \begin{bmatrix} h_k & h_{k-1} & \ldots & h_0 & 0 & \ddots & 0 \\ 0 & h_k^{[1]} & \ldots & h_1^{[1]} & h_0^{[1]} & 0 & 0 \\ \ddots & \ddots & \ddots & \ddots\ \ddots & \ddots & 0 & \\ 0 & 0 & \ldots & 0 & h_k^{[r-1]} & \ldots & h_0^{[r-1]} \end{bmatrix}, \end{aligned} \tag{3.14}$$

where we denote $h_i = H_i^{[k-i]}, \quad i = 0, 1, \ldots, k.$

4

Fast algorithms for decoding rank codes

4.1 Error correction in rank metric

Codes with check matrix (2.2) allows error correction using the algorithms similar to decoding algorithms for generalized Reed–Solomon codes.

Let $\mathbf{g} = (g_1, \ldots, g_n)$ be a code vector, $\mathbf{e} = (e_1, \ldots, e_n)$ an error vector, and $\mathbf{y} = \mathbf{g} + \mathbf{e}$ the received vector. Compute the syndrome

$$\mathbf{s} = (s_0, s_1, \ldots, s_{d-2}) = \mathbf{y}\mathbf{H}^T = \mathbf{e}\mathbf{H}^T. \tag{4.1}$$

The task of the decoder: given the syndrome $\mathbf{s}$ find an error vector. Let the rank norm of the error vector be t. Then it can be written as

$$\mathbf{e} = \mathbf{E}\mathbf{Y} = (E_1, \ldots, E_t)\mathbf{Y}, \tag{4.2}$$

where $E_1, \ldots, E_t$ are linearly independent over $\mathbb{F}_q$, and $\mathbf{Y} = (Y_{ij})$ is an $(t \times n)$-matrix of rank t with elements from $\mathbb{F}_q$. Then (4.1) can be rewritten as

$$\mathbf{s} = \mathbf{E}\mathbf{Y}\mathbf{H}^T = \mathbf{E}\mathbf{X}, \tag{4.3}$$

where the matrix $\mathbf{X} = \mathbf{Y}\mathbf{H}^T$ has the form

$$\mathbf{X} = \begin{bmatrix} x_1 & x_1^{[1]} & \dots & x_1^{[d-2]} \\ x_2 & x_2^{[1]} & \dots & x_2^{[d-2]} \\ \dots & \dots & \dots & \dots \\ x_t & x_t^{[1]} & \dots & x_t^{[d-2]} \end{bmatrix},$$

where

$$x_p = \sum_{j=1}^{n} Y_{pj} h_j,\ p = 1, \dots, t, \tag{4.4}$$

are linearly independent over $\mathbb{F}_q$. Equation (4.1) is equivalent to the following system of equations with unknowns $E_1, \dots, E_t, x_1, x_2, \dots, x_t$:

$$\sum_{i=1}^{t} E_i x_i^{[p]} = s_p,\ p = 0, 1, \dots, d-2. \tag{4.5}$$

Let a solution of the system be found. Then from (4.4) a matrix $\mathbf{Y}$ can be calculated, and from (4.2) an error vector $\mathbf{e}$ can be obtained. Note that the system (4.5) for a given t has many solutions, however for $t \le \frac{(d-1)}{2}$ all solutions lead to the same vector $\mathbf{e}$.

So, the decoding problem is reduced to solving system (4.5) for the minimal t.

Define the polynomial $S(z) = \sum_{j=0}^{d-2} s_j z^{[j]}$. Let $\Delta(z) = \sum_{p=0}^{t} \Delta_p z^{[p]}$, $\Delta_t = 1$, denote a polynomial that has all possible $\mathbb{F}_q$-linear combinations of $E_1, E_2, \dots, E_t$ as roots. Let $F(z) = \sum_{i=0}^{t-1} F_i z^{[i]}$, where $F_i = \sum_{p=0}^{i} \Delta_p s_{i-p}^{[p]}$, $i = 0, 1, \dots, t-1$.

Lemma 4.1. *The following equality holds*

$$F(z) = \Delta(z) * S(z) \mod z^{[d-1]}. \tag{4.6}$$

Indeed,

$$\Delta(z) * S(z) = \sum_{p=0}^{t} \Delta_p (S(z))^{[p]} = \sum_{i=0}^{t+d-2} z^{[i]} \left(\sum_{p+j=i} \Delta_p s_j^{[p]} \right).$$

For $t \le i \le d-2$ we have

$$\textstyle\sum_{p+j=i} \Delta_p s_j^{[p]} = \sum_{p=0}^{t} \Delta_p s_{i-p}^{[p]} = \sum_{p=0}^{t} \Delta_p \left(\sum_{j=1}^{t} E_j x_j^{[j-p]} \right)^{[p]} =$$

$$= \textstyle\sum_{j=1}^{t} x_j^{[i]} \Delta(E_j) = 0$$

since $\Delta(E_j) = 0$, $j = 1, 1, \dots, t$.

If the coefficients of $F(z)$ are known, then the coefficients of the polynomial $\Delta(z)$ can be found recurrently as follows. Let $s_0 = \dots = s_{j-1} = 0$, $s_j \neq 0$. Then

$$\begin{aligned} \Delta_0 &= \tfrac{F_j}{s_j}, \\ \Delta_p &= \frac{\left(F_{j+p} - \sum_{i=0}^{p-1} \Delta_i s_{p+j-i}^{[i]}\right)}{s_j^{[p]}},\ p = 1, 2, \dots, t, \end{aligned} \tag{4.7}$$

where for $j + p \geq t$ we set $F_{j+p} = 0$.

Now assume that $E_1, \dots, E_t$ and the polynomial Δ_z are known. Consider the "shortened" system of equations

$$\sum_{j=1}^{t} E_j x_j^{[p]} = s_p,\ p = 0, 1, \dots, t-1 \tag{4.8}$$

with unknowns $x_1, x_2, \dots, x_t$.

Let us solve (4.8) by sequential exclusion of variables. Denote $A_{1j} = E_j$, $Q_{1p} = s_p$. Multiply the $(p+1)$-th equation of the system by A_{11}^{q-1}, take the root of order q and subtract it from p-th equation. As a result, obtain a system without x_1:

$$\sum_{j=2}^{p} A_{2j} x_j^{[p]} = Q_{2p},\ p = 0, 1, \dots, m-2, \tag{4.9}$$

where

$$\begin{aligned} A_{2j} &= A_{1j} - \left(\tfrac{A_{1j}}{A_{11}}\right)^{[-1]} A_{11},\ j = 2, \dots, t, \\ Q_{2p} &= Q_{1p} - \left(\tfrac{Q_{1p+1}}{A_{11}}\right)^{[-1]} A_{11},\ p = 0, 1, \dots, t-2. \end{aligned} \tag{4.10}$$

By repeating this procedure $t - 1$ times and leaving the first equations in the system at every step we get a system of linear equations with a triangular matrix of coefficients:

$$\sum_{j=1}^{t} A_{ij} x_j = Q_{i0},\ i = 1, 2, \dots, t, \tag{4.11}$$

where

$$A_{1j} = E_j,\ j = 1, \dots, ;$$
$$A_{ij} = \begin{cases} 0, & j < i, \\ A_{i-1,j} - \left(\dfrac{A_{i-1,j}}{A_{i-1,i-1}} \right)^{[-1]} A_{i-1,i-1}, & p = 0, \dots, t-i,\ i = 2, \dots, t. \end{cases} \tag{4.12}$$

$$Q_{1p} = s_p,\ p = 0, \dots, t-1,$$
$$Q_{ip} = Q_{i-1,p} - \left(\tfrac{Q_{i-1,p+1}}{A_{i-1,i-1}} \right)^{[-1]} A_{i-1,i-1},\ p = 0, 1, \dots, t-i,\ i = 2, \dots, t. \tag{4.13}$$

System (4.11) can be solved using the following recurrent formulas

$$x_t = \tfrac{Q_{t0}}{A_{mm}},$$
$$x_{t-i} = \tfrac{\left(Q_{t-i,0} - \sum_{j=t-i+1}^{t} A_{-i,j}\right)}{A_{t-i,t-i}},\ i = 1, \dots, t-1. \tag{4.14}$$

The decoding algorithm is as follows.

I. Compute the syndrome vector $\mathbf{s} = (s_0, \dots, s_{d-2})$ and obtain correspondent polynomial $S(z) = \sum_{i=0}^{d-2} s_i z^{[i]}$.

II. Set $F_0(z) = z^{[i-1]}$, $F_1(z) = S(z)$, and apply the Euclidean algorithm until $F_{t+1}(z)$ is such that

$$\text{qdeg}(F_t(z)) \geq q^{\frac{d-1}{2}}. \tag{4.15}$$

Then

$$\Delta(z) = \gamma A(z),$$
$$F(z) = \gamma(-1)^t F_{t+1}(z), \tag{4.16}$$

where γ is selected such that the coefficient Δ_t is equal to 1.

Indeed, if the number of rank errors is at most $\frac{(d-1)}{2}$, then equalities (4.16) follow from (1.8) and from Lemma 4.1. The uniqueness of polynomials $F(z)$ and $\Delta(z)$ can be proved in the same way as in the case of standard generalized Reed–Solomon codes.

The polynomial $\Delta(z)$ can be found either by the first formula in (4.16), if the polynomials $A_i(z)$, $i = 1, 2, \dots,$ have been computed using the Euclidean algorithm, or using (4.7), where the coefficients of remainders $F_{m+1}(z)$, computed with the algorithm, are required. Then any $\mathbb{F}_q$-linearly independent roots $E_1, \dots, E_m$ of the polynomial $\Delta(z)$ can be found.

III. Using (4.11)-(4.14) and known $E_1, \dots, E_t$ compute $x_1, \dots, x_t$. Find the matrix $\mathbf{Y}$ from decomposition (4.4). Finally, compute the error vector $\mathbf{e}$ from (4.2).

As an example, consider the case $d = 3$, $q = 2$. Here we can correct single rank errors in a field of characteristic 2.

1. Compute the syndrome $\mathbf{s} = (s_0, s_1)$. If $s_0 = 0$ and $s_1 = 0$ then conclude that there were no errors.

2. If $s_0 \neq 0$ and $s_1 \neq 0$ then the Euclidean algorithm gives the polynomial $\Delta(z) = -(\frac{s_0^1}{s_{[1]}})z + z^{[1]}$. Conclude that it was a single error and find E as a nonzero root of the equation $\Delta(z) = 0$, i.e., $E = (\frac{s_0^{[1]}}{s_1})$. In this case, the system (4.10) has a single equation and gives $x = \frac{s_1}{s_0} = y_1 h_1 + y_2 h_2 + \ldots + y_n h_n$, where $y_i = 0$ or 1. The error vector is $\mathbf{e} = (y_1 E, y_2 E, \dots, y_n E)$.

3. If $s_0 = 0$, $s_1 \neq 0$ or $s_0 \neq 0$, $s_1 = 0$, then conclude that the error has a rank at least 2 since the Euclidean algorithm would give the polynomials $\Delta(z) = z^{[1]}$ and $\Delta(z) = z^{[2]}$, which have no roots.

4.2 Error and erasure correction by MRD codes

Assume we need to correct errors and also erasures of columns and rows up to the theoretical bound. If there have been no erasures then the decoding algorithm from Section 4.1 will correct rank errors.

Later we will show that in general the variables corresponding to row erasures can be excluded from the (first) system of syndrome equations, giving the second system, and the decoding problem will be reduced to error and column erasure correction. In turn, the column erasures can be excluded from the second system of syndrome equations in a similar way, and the decoding problem will be reduced to error correction only. After error correction we will return to column erasure correction and then to row erasures. As a result, we will correct all three types of distortions: errors and erasures of both columns and rows.

Before we describe the general decoding algorithm let us recall the construction of the rank distance (n, k, d)-code, where n is the code length, k is the number of information symbols, and d is the code distance.

The *rank* of a vector $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}),\ x_j \in \mathbb{F}_{q^n}$, denoted by $\mathrm{Rk}_{\mathbb{F}_q}(\mathbf{x})$, is the maximum number of components that are linearly independent over $\mathbb{F}_q$.

Let the vector

$$\mathbf{g} = (g_0, g_1, ..., g_{n-1}) \tag{4.17}$$

give a basis of the extension $\mathbb{F}_{q^n}$ of the base field $\mathbb{F}_q$, i.e., components $g_j \in \mathbb{F}_{q^n},\ j = 0, \ldots, n-1$, are linearly independent over the base field $\mathbb{F}_q$. Then any n-vector $\mathbf{x} \in \mathbb{F}_{q^n}^n$ can be uniquely represented as

$$\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) = (g_0, g_1, ..., g_{n-1})A(\mathbf{x}) = \mathbf{g}A(\mathbf{x}), \tag{4.18}$$

where $A(\mathbf{x})$ is a $n \times n$ matrix over the base field $\mathbb{F}_q$.

Equivalently, the rank of a vector $\mathbf{x}$ can be defined as the standard algebraic rank of the matrix $A(\mathbf{x})$, i.e., $\mathrm{Rk}_{\mathbb{F}_q}(\mathbf{x}) = \mathrm{Rk}(A(\mathbf{x}))$.

A code in *vector* representation (vector code) with rank distance d is defined as a set $V \subseteq \mathbb{F}_{q^n}^n$ of vectors $\mathbf{x}_j \in \mathbb{F}_{q^n}^n$ such that $\min\limits_{i \neq j} \mathrm{Rk}_{\mathbb{F}_q}(\mathbf{x}_i - \mathbf{x}_j) = d$.

The same code in *matrix* form (matrix code) is the set of corresponding matrices $A(\mathbf{x}_j),\ j = 1, \ldots, V$.

An $\mathbb{F}_{q^n}$-linear code with rank distance d having $V = (q^n)^k$ code vectors we denote by (n, k, d)-code. An (n, k, d)-code is called the maximum rank distance (MRD) code if $d = n - k + 1$.

An MRD $(n, k, d = n - k + 1)$ code in vector form can be defined by a generator matrix. The standard form of a generator matrix is:

$$\mathbf{G}_k = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-1} \\ g_0^{[1]} & g_1^{[1]} & \cdots & g_{n-1}^{[1]} \\ \cdots & \cdots & \cdots & \cdots \\ g_0^{[k-1]} & g_1^{[k-1]} & \cdots & g_{n-1}^{[k-1]} \end{pmatrix}, \tag{4.19}$$

where $g_j^{[i]} = g_j^{q^{i \bmod n}}$.

The first row of the generator matrix is the vector

$$\mathbf{g} = (g_0, g_1, ..., g_{n-1}),$$

over the extension field $\mathbb{F}_{q^n}$, where the components $g_j \in \mathbb{F}_{q^n},\ j = 0, \ldots, n-1$, are linearly independent over the base field $\mathbb{F}_q$. Hence, the vector $\mathbf{g}$ is a basis of the extension field $\mathbb{F}_{q^n}$ over the base field $\mathbb{F}_q$. Every next row of the generator matrix is the Frobenius power of the previous row.

Denote by $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1})$ the information vector, which has *information symbols*, $u_j \in \mathbb{F}_{q^n}$, $j = 0, 1, \ldots, k-1$ as components. Then the code vector $\mathbf{g}(\mathbf{u})$ corresponding to the information vector $\mathbf{u}$ can be obtained as

$$\mathbf{g}(\mathbf{u}) = \mathbf{u}\mathbf{G}_k. \tag{4.20}$$

The rank norm of any nonzero code vector is at least $n-k+1$, hence the code distance is $d = n-k+1$.

Known fast decoding algorithms use the following check matrix

$$\mathbf{H}_{n-k} = \mathbf{H}_{d-1} = \begin{pmatrix} h_0 & h_1 & \ldots & h_{n-1} \\ h_0^{[1]} & h_1^{[1]} & \ldots & h_{n-1}^{[1]} \\ \ldots & \ldots & \ldots & \ldots \\ h_0^{[n-k+1]} & h_1^{[n-k+1]} & \ldots & h_{n-1}^{[n-k+1]} \end{pmatrix}, \tag{4.21}$$

where elements $h_0, h_1, \ldots, h_{n-1}$ are linearly independent over the base field $\mathbb{F}_q$. The generator and the check matrices satisfy

$$\mathbf{G}_k \mathbf{H}_{n-k}^{\top} = 0. \tag{4.22}$$

4.3 Rank errors and rank erasures

Rank metric codes can be used for telecommunication as follows.

Select an MRD (n, k, d)-code in vector form. The vector form is convenient for coding and decoding. A code word $\mathbf{g}(\mathbf{u})$ to be transmitted is converted using (4.18) to a square q-ary matrix of order n. For definiteness assume that the first row of the generator matrix $\mathbf{G}_k$ is the basis of the extension field.

The code matrix is transmitted over a system of n parallel channels. Elements of the i-th row enter the i-th channel. Elements of the j-th column are transmitted during the j-th time interval.

The code matrix can be distorted during the transmission by adding a noise matrix of order n. Consider three types of distortions.

1. The noise matrix E is added to the code matrix and the receiver does not know which columns or rows are distorted. The received matrix is transformed to a vector using (4.18). Hence, the decoder should process the received vector

$$\mathbf{y} = \mathbf{g}(\mathbf{u}) + \mathbf{e}.$$

We say that there is an error of rank m, or m rank errors, if $\mathrm{Rk}_{\mathbb{F}_q}(\mathbf{e}) = m$. To be corrected, the error of rank m is written as

$$\mathbf{e} = (e_1, e_2, \ldots, e_m)U, \tag{4.23}$$

where the *unknown* elements $e_j \in \mathbb{F}_{q^n}$, are $\mathbb{F}_q$-linearly independent and U is a q-ary $m \times n$ matrix

$$U = \begin{pmatrix} u_{1,1} & u_{1,2} & \ldots & u_{1,n} \\ u_{2,1} & u_{2,2} & \ldots & u_{2,n} \\ \vdots & \vdots & \ldots & \vdots \\ u_{m,1} & u_{m,2} & \ldots & u_{m,n} \end{pmatrix} \tag{4.24}$$

with *unknown* elements.

2. The noise matrix E_{row} is added to the code matrix and the receiver *knows the side information* that the rows $i_1, i_2, \ldots, i_v$ can be distorted. The received matrix is transformed to a vector using (4.18). If only the i-th row $\mathbf{R}$ of E_{row} is nonzero then the code vector is distorted by $g_i\mathbf{R}$, where g_i is a known basis element. Hence, the decoder should work with the vector
$$\mathbf{y} = \mathbf{g}(\mathbf{u}) + \mathbf{e}_{\text{row}},$$
where
$$\mathbf{e}_{\text{row}} = (g_{i_1}, g_{i_2}, \ldots, g_{i_v})R_{\text{row}}. \tag{4.25}$$
Here the elements g_{i_j} *are known*, while the q-ary $v \times n$ matrix
$$R_{\text{row}} = \begin{pmatrix} r_{1,1} & r_{1,2} & \ldots & r_{1,n} \\ r_{2,1} & r_{2,2} & \ldots & r_{2,n} \\ \vdots & \vdots & \ldots & \vdots \\ r_{v,1} & r_{v,2} & \ldots & r_{v,n} \end{pmatrix} \tag{4.26}$$
is unknown. We say that the vector $\mathbf{e}_{\text{row}}$ defines an erasure of v rows.

3. The noise matrix E_{col} is added to the code matrix and the receiver *knows the side information* that the columns $j_1, j_2, \ldots, j_r$ can be distorted. The received matrix is transformed to a vector using (4.18). If only the j-th column of E_{col} is nonzero then E_{col} will be transformed to the vector $w_j c$, where $w_j \in \mathbb{F}_{q^n}$ is *an unknown* while c is a known q-ary n-vector that

has the j-th component 1 and all the rest are zeros. Hence, the decoder should work with the vector

$$\mathbf{y} = \mathbf{g}(u) + \mathbf{e}_{\text{col}},$$

where

$$\mathbf{e}_{\text{col}} = (w_{j_1}, w_{j_2}, \dots, w_{j_r})C_{\text{col}}. \tag{4.27}$$

Here w_{j_k} *are unknown* while the q-ary $r \times n$ matrix

$$C_{\text{col}} = \begin{pmatrix} 0 & \dots & 0 & c_{1,j_1} = 1 & 0 & \dots & 0 \\ 0 & \dots & \dots & 0 & c_{2,j_2} = 1 & \dots & 0 \\ 0 & \dots & \dots & \dots & \dots & \dots & 0 \\ 0 & \dots & \dots & \dots & 0 & c_{r,j_r} = 1 & \dots \end{pmatrix} \tag{4.28}$$

is known. We say that the vector e_{col} defines erasure of r columns.

In the general case, rank errors and erasures can occur simultaneously and a decoder should process the received vector

$$\mathbf{y} = \mathbf{g}(\mathbf{u}) + \mathbf{e} + \mathbf{e}_{\text{row}} + \mathbf{e}_{\text{col}} \tag{4.29}$$

where the error vectors are given in (4.23), (4.25) and (4.27).

Lemma 4.2. *An MRD* $(n, k, d = n-k+1)$ *code corrects simultaneously erasures of* v *rows,* r *columns and errors of rank* m *if*

$$2m + v + r \leq d - 1. \tag{4.30}$$

Proof. Consider all the code matrices of order n. Delete v rows and r columns in all these matrices. We obtain a new code of $(n - v) \times (n - r)$ matrices with rank distance at least $\widetilde{d} = d - v - r$. Hence, this code corrects errors of rank m if $m \leq (d - v - r - 1)/2$, or

$$2m + v + r \leq d - 1.$$

■

Simultaneous error and erasure correction is considered in the next section

4.4 Simultaneous error and erasure correction

Consider an algorithm for error and erasure correction. The algebraic decoding starts with computation of the syndrome vector $\mathbf{s} = (s_0, s_1, \ldots, s_{d-2})$. For a received vector $\mathbf{y}$, given by (4.29), we have

$$\begin{aligned} \mathbf{s}^\top = \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{d-2} \end{pmatrix} &= \mathbf{H}_{d-1}\mathbf{y}^\top \\ &= \mathbf{H}_{d-1}U^\top \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{pmatrix} + \mathbf{H}_{d-1}R_{\mathrm{row}}^\top \begin{pmatrix} g_{i_1} \\ g_{i_2} \\ \vdots \\ g_{i_v} \end{pmatrix} + \mathbf{H}_{d-1}C_{\mathrm{col}}^\top \begin{pmatrix} w_{j_1} \\ w_{j_2} \\ \vdots \\ w_{j_r} \end{pmatrix}. \end{aligned} \tag{4.31}$$

Using (4.24), (4.26) and (4.28) we can rewrite the syndrome as follows

$$\mathbf{s}^\top = \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{d-2} \end{pmatrix} = \sum_{k=1}^{m} e_k \begin{pmatrix} x_k \\ x_k^{[1]} \\ \vdots \\ x_k^{[d-2]} \end{pmatrix} + \sum_{k=1}^{v} g_{i_k} \begin{pmatrix} f_k \\ f_k^{[1]} \\ \vdots \\ f_k^{[d-2]} \end{pmatrix} + \sum_{k=1}^{r} w_{j_k} \begin{pmatrix} h_{j_k} \\ h_{j_k}^{[1]} \\ \vdots \\ h_{j_k}^{[d-2]} \end{pmatrix}. \tag{4.32}$$

Here $x_k = \sum_{p=1}^{n} h_{p-1} u_{k,p}$, $k = 1, \ldots, m$, $f_k = \sum_{p=1}^{n} h_{p-1} r_{k,p}$, $k = 1, \ldots, v$.

Without loss of generality we can assume that the elements of each of the following sets

$$\begin{gathered} \{x_1, \ldots, x_m, f_1, \ldots, f_v, h_{j_1}, \ldots, h_{j_r}\} \\ \text{and} \\ \{e_1, \ldots, e_m, g_{i_1}, \ldots, g_{i_v}, w_{j_1}, \ldots, w_{j_r}\} \end{gathered} \tag{4.33}$$

are linearly independent over $\mathbb{F}_q$. Otherwise the number of unknowns can be decreased. The decoding can be done using the syndrome (4.32) and its modifications.

Together with the syndrome $\mathbf{s}$ let us use the modified syndrome $\mathbf{s}_{\text{mod}}$:

$$\mathbf{s}_{\text{mod}}^\top = \begin{pmatrix} s_0^{[n]} \\ s_1^{[n-1]} \\ \vdots \\ s_{d-2}^{[n-d+2]} \end{pmatrix}$$

$$= \sum_{k=1}^{m} x_k \begin{pmatrix} e_k^{[n]} \\ e_k^{[n-1]} \\ \vdots \\ e_k^{[n-d+2]} \end{pmatrix} + \sum_{k=1}^{v} f_k \begin{pmatrix} g_{i_k}^{[n]} \\ g_{i_k}^{[n-1]} \\ \vdots \\ g_{i_k}^{[n-d+2]} \end{pmatrix} + \sum_{k=1}^{r} h_{j_k} \begin{pmatrix} w_{j_k}^{[n]} \\ w_{j_k}^{[n-1]} \\ \vdots \\ w_{j_k}^{[n-d+2]} \end{pmatrix}. \tag{4.34}$$

The decoder should solve system of equations (4.32) or (4.34) and find unknowns $\{x_k, f_k, e_k, w_{j_k}\}$. After this, rank errors e and rank erasures $e_{\text{row}}, e_{\text{col}}$ should be corrected.

Let us show that it is possible if conditions of Lemma 4.2 are satisfied. The idea is as follows.

First assume that there were no erasures, i.e., $e_{\text{row}} = e_{\text{col}} = 0$ and only rank errors should be corrected. In this case, the syndrome (4.32) contains unknowns $\{x_k, e_k\}$ only. Existing standard algorithms allow rank error correction if the rank m satisfies $2m \le d-1$.

Let us show that in the general case, the unknowns $\{f_k\}$, that define row erasures, can be excluded from the system of equations (4.32). The problem will be reduced to correction of rank errors and *column* erasures. In turn, the column erasures also can be excluded and we only need to correct errors.

4.4.1 Exclusion of row erasures

Row erasures are included in in the syndrome as:

$$\sum_{k=1}^{v} g_{i_k} \begin{pmatrix} f_k \\ f_k^{[1]} \\ \vdots \\ f_k^{[d-2]} \end{pmatrix},$$

where the elements g_{i_k}, $k = 1, \dots, v$, are known while f_k, $k = 1, \dots, v$, are unknown.

Define the linearized polynomial

$$T(z) = \sum_{i=0}^{v} T_i z^{[i]}, \tag{4.35}$$

that has all $\mathbb{F}_q$-linear combinations of g_{i_k}, $k = 1, \dots, v$, as roots. In particular,

$$T(g_{i_k}) = 0, \quad k = 1, 2, \dots, v. \tag{4.36}$$

The coefficients T_i are used to exclude unknowns f_k, $k = 1, \dots, v$, and to modify the syndrome. Denote the modified syndrome by $\tilde{\mathbf{s}} = (\tilde{s}_0 \ \tilde{s}_1 \ \dots \ \tilde{s}_{d-2-v})$. It has dimension $d - 1 - v$ and can be computed as follows:

$$\widetilde{\mathbf{s}}^\top = \begin{pmatrix} \widetilde{s}_0 \\ \widetilde{s}_1 \\ \vdots \\ \widetilde{s}_{d-3-v} \\ \widetilde{s}_{d-2-v} \end{pmatrix} = \begin{pmatrix} s_v & s_{v-1}^{[1]} & \dots & s_1^{[v-1]} & s_0^{[v]} \\ s_{v+1} & s_v^{[1]} & \dots & s_2^{[v-1]} & s_1^{[v]} \\ \vdots & \vdots & \dots & \vdots & \vdots \\ s_{d-3} & s_{d-4}^{[1]} & \dots & s_{d-4-v}^{[v-1]} & s_{d-3-v}^{[v]} \\ s_{d-2} & s_{d-3}^{[1]} & \dots & s_{d-3-v}^{[v-1]} & s_{d-2-v}^{[v]} \end{pmatrix} \begin{pmatrix} T_0 \\ T_1 \\ \vdots \\ T_{v-1} \\ T_v \end{pmatrix}. \tag{4.37}$$

Denote:

$$\begin{array}{lll} \widetilde{e}_k = T(e_k); & \widetilde{x}_k = x_k^{[v]}; & k = 1, 2, \dots, m; \\ \widetilde{w}_{j_k} = T(w_{j_k}); & \widetilde{h}_{j_k} = h_{j_k}^{[v]}; & k = 1, 2, \dots, r. \end{array} \tag{4.38}$$

Lemma 4.3. *The modified syndrome* $\tilde{\mathbf{s}}$ *can be written as:*

$$\widetilde{\mathbf{s}}^\top = \begin{pmatrix} \widetilde{s}_0 \\ \widetilde{s}_1 \\ \vdots \\ \widetilde{s}_{d-2-v} \end{pmatrix} = \sum_{k=1}^{m} \widetilde{e}_k \begin{pmatrix} \widetilde{x}_k \\ \widetilde{x}_k^{[1]} \\ \vdots \\ \widetilde{x}_k^{[d-2-v]} \end{pmatrix} + \sum_{k=1}^{r} \widetilde{w}_{j_k} \begin{pmatrix} \widetilde{h}_{j_k} \\ \widetilde{h}_{j_k}^{[1]} \\ \vdots \\ \widetilde{h}_{j_k}^{[d-2-v]} \end{pmatrix}. \tag{4.39}$$

Proof. From (4.32) and (4.37) we get

$$\begin{aligned}
\widetilde{s}_j = \quad & s_{v+j}T_0 + s_{v+j-1}^{[1]}T_1 + \cdots + s_{j+1}^{[v-1]}T_{v-1} + s_j^{[v]}T_v & = \\
& \left(\sum_{k=1}^{m} e_k x_k^{[v+j]} + \sum_{k=1}^{v} g_{i_k} f_k^{[v+j]} + \sum_{k=1}^{r} w_{j_k} h_{j_k}^{[v+j]}\right) T_0 & + \\
& \left(\sum_{k=1}^{m} e_k^{[1]} x_k^{[v+j]} + \sum_{k=1}^{v} g_{i_k}^{[1]} f_k^{[v+j]} + \sum_{k=1}^{r} w_{j_k}^{[1]} h_{j_k}^{[v+j]}\right) T_1 & + \\
& \vdots & + \\
& \left(\sum_{k=1}^{m} e_k^{[v]} x_k^{[v+j]} + \sum_{k=1}^{v} g_{i_k}^{[v]} f_k^{[v+j]} + \sum_{k=1}^{r} w_{j_k}^{[v]} h_{j_k}^{[v+j]}\right) T_v & = \\
& \left(\sum_{k=1}^{m} T(e_k) x_k^{[v+j]} + \sum_{k=1}^{v} T(g_{i_k}) f_k^{[v+j]} + \sum_{k=1}^{r} T(w_{j_k}) h_{j_k}^{[v+j]}\right) & = \\
& \left(\sum_{k=1}^{m} T(e_k) x_k^{[v+j]} + \sum_{k=1}^{r} T(w_{j_k}) h_{j_k}^{[v+j]}\right) & = \\
& \left(\sum_{k=1}^{m} \widetilde{e}_k \widetilde{x}_k^{[j]} + \sum_{k=1}^{r} \widetilde{w}_{j_k} \widetilde{h}_{j_k}^{[j]}\right).
\end{aligned}$$

Here conditions (4.36) and notations (4.38) were used. ■

From (4.39) it follows that row erasures are temporary excluded. The decoder should correct errors of rank m and column erasures of rank r. The next step is to exclude column erasures.

4.4.2 Exclusion of column erasures

Continue modifications of syndrome equations. Let us modify (4.39) similar to (4.34):

$$
\begin{aligned}
\widetilde{s}_{\mathrm{mod}}^{\top} &= \begin{pmatrix} \widetilde{s}_{0,\mathrm{mod}} \\ \widetilde{s}_{1,\mathrm{mod}} \\ \vdots \\ \widetilde{s}_{d-2-v,\mathrm{mod}} \end{pmatrix} = \begin{pmatrix} \widetilde{s}_{0}^{[n]} \\ \widetilde{s}_{1}^{[n-1]} \\ \vdots \\ \widetilde{s}_{d-2-v}^{[n-d+2+v]} \end{pmatrix} \\
&= \sum_{k=1}^{m} \widetilde{x}_k \begin{pmatrix} \widetilde{e}_{k}^{[n]} \\ \widetilde{e}_{k}^{[n-1]} \\ \vdots \\ \widetilde{e}_{k}^{[n-d+2+v]} \end{pmatrix} + \sum_{k=1}^{r} \widetilde{h}_{j_k} \begin{pmatrix} \widetilde{w}_{j_k}^{[n]} \\ \widetilde{w}_{j_k}^{[n-1]} \\ \vdots \\ \widetilde{w}_{j_k}^{[n-d+2+v]} \end{pmatrix}.
\end{aligned}
\tag{4.40}
$$

Elements $\widetilde{h}_{j_k}$, $k = 1, 2, \ldots, r$, are known. Define the linearized polynomial

$$
L(z) = \sum_{i=0}^{r} L_i z^{[i]}, \tag{4.41}
$$

that has all $\mathbb{F}_q$-linear combinations of $\widetilde{h}_{j_k}$, $k = 1, 2, \ldots, r$, as roots. In particular,

$$
L(\widetilde{h}_{j_k}) = 0, \quad k = 1, 2, \ldots, r. \tag{4.42}
$$

Coefficients L_i are used to exclude unknowns $\widetilde{w}_{j_k}$, $k = 1, \ldots, r$, and modify the syndrome (4.39). Denote the final syndrome by $\widehat{\mathbf{s}} = (\widehat{s}_0 \ \widehat{s}_1 \ \ldots \ \widehat{s}_{d-3-v-r} \ \widehat{s}_{d-2-v})$. It has dimension $d - 1 - v - r$ and can be computed as follows:

$$
\begin{aligned}
\widehat{\mathbf{s}}^{\top} &= \begin{pmatrix} \widehat{s}_0 & \widehat{s}_1 & \ldots & \widehat{s}_{d-3-v-r} & \widehat{s}_{d-2-v-r} \end{pmatrix}^{\top} \\
&= \begin{pmatrix} \widetilde{s}_{0,\mathrm{mod}} & \widetilde{s}_{1,\mathrm{mod}}^{[1]} & \ldots & \widetilde{s}_{r,\mathrm{mod}}^{[r]} & \\ \widetilde{s}_{1,\mathrm{mod}} & \widetilde{s}_{2,\mathrm{mod}}^{[1]} & \ldots & \widetilde{s}_{r+1,\mathrm{mod}}^{[r]} & \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ \widetilde{s}_{d-3-v-r,\mathrm{mod}} & \widetilde{s}_{d-2-v-r,\mathrm{mod}}^{[1]} & \ldots & \widetilde{s}_{d-3-v,\mathrm{mod}}^{[r]} & \\ \widetilde{s}_{d-2-v-r,\mathrm{mod}} & \widetilde{s}_{d-1-v-r,\mathrm{mod}}^{[1]} & \ldots & \widetilde{s}_{d-2-v,\mathrm{mod}}^{[r]} & \end{pmatrix} \begin{pmatrix} L_0 \\ L_1 \\ \vdots \\ L_r \end{pmatrix}.
\end{aligned}
\tag{4.43}
$$

Lemma 4.4. *The final syndrome $\widehat{s}$ can be written as:*

$$\widehat{\mathbf{s}}^{\top} = \begin{pmatrix} \widehat{s}_0 \\ \widehat{s}_1 \\ \vdots \\ \widehat{s}_{d-3-v-r} \\ \widehat{s}_{d-2-v-r} \end{pmatrix} = \sum_{k=1}^{m} \widehat{e}_k \begin{pmatrix} \widehat{x}_k^{[n]} \\ \widehat{x}_k^{[n-1]} \\ \vdots \\ \widehat{x}_k^{[n-d+2+v+r]} \end{pmatrix}, \tag{4.44}$$

where

$$\begin{array}{rcll} \widehat{e}_k & = & L(\widetilde{x}_k); & k = 1, 2, \ldots, m; \\ \widehat{x}_k & = & \widetilde{e}_k; & k = 1, 2, \ldots, m. \end{array} \tag{4.45}$$

Proof. From (4.40) (4.43) we get

$$\begin{aligned} \widehat{s}_j = \; & \widetilde{s}_{j,\mathrm{mod}} L_0 + \widetilde{s}^{[1]}_{j+1,\mathrm{mod}} L_1 + \cdots + \widetilde{s}^{[r-1]}_{j+r-1,\mathrm{mod}} L_{r-1} + \widetilde{s}^{[r]}_{j+r,\mathrm{mod}} L_r && = \\ & \left(\sum_{k=1}^{m} \widetilde{x}_k \widetilde{e}_k^{[n-j]} + \sum_{k=1}^{r} \widetilde{h}_{j_k} \widetilde{w}_{j_k}^{[n-j]} \right) L_0 && + \\ & \left(\sum_{k=1}^{m} \widetilde{x}_k^{[1]} \widetilde{e}_k^{[n-j]} + \sum_{k=1}^{r} \widetilde{h}_{j_k}^{[1]} \widetilde{w}_{j_k}^{[n-j]} \right) L_1 && + \\ & \ldots && + \\ & \left(\sum_{k=1}^{m} \widetilde{x}_k^{[r]} \widetilde{e}_k^{[n-j]} + \sum_{k=1}^{r} \widetilde{h}_{j_k}^{[r]} \widetilde{w}_{j_k}^{[n-j]} \right) L_r && = \\ & \left(\sum_{k=1}^{m} L(\widetilde{x}_k) \widetilde{e}_k^{[n-j]} + \sum_{k=1}^{r} L(\widetilde{h}_{j_k}) \widetilde{w}_{j_k}^{[n-j]} \right) && = \\ & \sum_{k=1}^{m} L(\widetilde{x}_k) \widetilde{e}_k^{[n-j]} && = \\ & \sum_{k=1}^{m} \widehat{e}_k \widehat{x}_k^{[n-j]}. \end{aligned}$$

Here we use conditions (4.42) and notations (4.45). ∎

Equations (4.44) allow us to compute errors of rank m if $2m \le d - 1 - v - r$.

4.4.3 Short description of the algorithm correcting errors and erasures simultaneously

The basic steps of the algorithm are as follows.

1. Input: the received matrix Y and side information about row and column erasures:
$$\begin{array}{ll} g_{i_s}, & s = 1, 2, \ldots, v, \\ h_{j_u}, & u = 1, 2, \ldots, r. \end{array}$$
Compute the corresponding linearized polynomials $T(z)$ and $L(z)$.

2. Transform the received matrix Y to the vector $\mathbf{y}$ and compute the syndrome (4.31).

3. Compute the final syndrome (4.43) and find $\{\widehat{e}_k, \widehat{x}_k\}$.

4. Find $\{\widetilde{e}_k, \widetilde{x}_k\}$ from (4.45) and compute $\widetilde{w}_{j_k}$ from (4.39).

5. Find $\{e_k, x_k, w_{j_k}\}$ from (4.38) and compute $\{f_k\}$ from (4.32).

6. Correct the received vector by removing all errors found.

4.4.4 Correction of erasures only

The above algorithm can be simplified if only erasures occur during transmission and there are no errors. In this case, the syndrome is as follows:

$$s^\top = \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{d-2} \end{pmatrix} = \sum_{k=1}^{v} g_{i_k} \begin{pmatrix} f_k \\ f_k^{[1]} \\ \vdots \\ f_k^{[d-2]} \end{pmatrix} + \sum_{k=1}^{r} w_{j_k} \begin{pmatrix} h_{j_k} \\ h_{j_k}^{[1]} \\ \vdots \\ h_{j_k}^{[d-2]} \end{pmatrix}. \tag{4.46}$$

If there are erasures of columns only, then (4.46) is a system with $d-1$ linear equations with unknowns $\{w_{j_k},\ k = 1, 2, \ldots, r\}$, which can be solved using a standard method.

If there are erasures of rows only, then (4.34) is a system of $d-1$ linear equations with unknowns $\{f_k,\ k = 1, 2, \ldots, v\}$, which can be solved in a similar way.

In the general case with row and column erasures, the modified syndrome (4.39) is a system of $(d-1-v)$ linear equations with unknowns $\{\widetilde{w}_{j_k},\ k = 1, 2, \ldots, r\}$. Unknowns $\{f_k,\ k = 1, 2, \ldots, v\}$ can be found using another linear system of equations.

4.5 Examples

As an example let us consider a MRD $(5,1,5)$-code over $\mathbb{F}_{2^5}$. with the generator matrix

$$\mathbf{G} = (\alpha\, \alpha^{30}\, \alpha^{18}\, \alpha^{7}\, \alpha^{20}).$$

A check matrix is :

$$\mathbf{H}_4 = \mathbf{H}_{d-1} = \begin{pmatrix} \alpha^2 & \alpha^{29} & \alpha^5 & \alpha^{14} & \alpha^9 \\ \alpha^4 & \alpha^{27} & \alpha^{10} & \alpha^{28} & \alpha^{18} \\ \alpha^8 & \alpha^{23} & \alpha^{20} & \alpha^{25} & \alpha^5 \\ \alpha^{16} & \alpha^{15} & \alpha^9 & \alpha^{19} & \alpha^{10} \end{pmatrix}. \qquad (4.47)$$

These matrices are connected by the equation: $\mathbf{G}\mathbf{H}_4^\top = 0$.

If the information symbol $u = 1$ then the code vector is

$$\underline{\mathbf{g}}(\mathbf{u}) = (\alpha\, \alpha^{30}\, \alpha^{18}\, \alpha^{7}\, \alpha^{20}).$$

The corresponding code matrix $M(\mathbf{u})$ is

$$M(\mathbf{u}) = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Let us consider some variants of errors and erasures.

Variant 1: 1 **error and** 2 **erasures**
Let the noise matrix be

$$E = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Here we assume that the first row and the first column are erased, and the rest is an error. The received matrix is

$$Y = M(\mathbf{u}) + E = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Transform the received matrix Y to the vector $\underline{\mathbf{y}}$:

$$\underline{\mathbf{y}} = (\alpha^{21}\, \alpha^{13}\, \alpha\, \alpha^{22}\, \alpha^{18}).$$

Compute the syndrome

$$\underline{\mathbf{s}}^\top = \mathbf{H}\underline{\mathbf{y}}^\top = \begin{pmatrix} \alpha^{17} \\ \alpha^{22} \\ \alpha^{17} \\ \alpha^{15} \end{pmatrix}.$$

Extract the known variables $g_{i_1} = 1$, $h_{j_1} = h_0 = \alpha^2$. Compute the linearized polynomials

$$T(z) = z^2 + z, \qquad T_0 = 1, \quad T_1 = 1.$$

$$L(z) = z(z + \widetilde{h}_0) = z(z + h_0^2) = z^2 + \alpha^4 z, \quad L_0 = \alpha^4, \quad L_1 = 1.$$

Compute the syndromes

$$\widetilde{\mathbf{s}}^\top = \begin{pmatrix} \widetilde{s}_0 \\ \widetilde{s}_1 \\ \widetilde{s}_2 \end{pmatrix} = \begin{pmatrix} s_1 & s_0^2 \\ s_2 & s_1^2 \\ s_3 & s_2^2 \end{pmatrix} \begin{pmatrix} T_0 \\ T_1 \end{pmatrix} = \begin{pmatrix} \alpha^3 \\ \alpha^{23} \\ \alpha^{26} \end{pmatrix},$$

$$\widetilde{\mathbf{s}}_{\mathrm{mod}}^\top = \begin{pmatrix} \widetilde{s}_{0,\mathrm{mod}} \\ \widetilde{s}_{1,\mathrm{mod}} \\ \widetilde{s}_{2,\mathrm{mod}} \end{pmatrix} = \begin{pmatrix} \widetilde{s}_0 \\ \widetilde{s}_1^{16} \\ \widetilde{s}_2^{8} \end{pmatrix} = \begin{pmatrix} \alpha^3 \\ \alpha^{27} \\ \alpha^{22} \end{pmatrix}.$$

$$\widehat{\mathbf{s}}^\top = \begin{pmatrix} \widehat{s}_0 \\ \widehat{s}_1 \end{pmatrix} = \begin{pmatrix} \widetilde{s}_{0,\mathrm{mod}} & \widetilde{s}_{1,\mathrm{mod}}^2 \\ \widetilde{s}_{1,\mathrm{mod}} & \widetilde{s}_{2,\mathrm{mod}}^2 \end{pmatrix} \begin{pmatrix} L_0 \\ L_1 \end{pmatrix} = \begin{pmatrix} \alpha^{16} \\ \alpha^{14} \end{pmatrix}.$$

Find $\widehat{e}_1$,$\widehat{x}_1$:

$$\widehat{\underline{\mathbf{s}}}^\top = \begin{pmatrix} \alpha^{16} \\ \alpha^{14} \end{pmatrix} = \widehat{e}_1 \begin{pmatrix} \widehat{x}_1 \\ \widehat{x}_1^{16} \end{pmatrix},$$

$$\begin{aligned} \widehat{e}_1\widehat{x}_1 &= \alpha^{16}, \\ \widehat{e}_1\widehat{x}_1^{16} &= \alpha^{14}. \\ \widehat{e}_1 &= \alpha^{12}, \\ \widehat{x}_1 &= \alpha^4. \end{aligned}$$

To find errors we solve the following equations:

$$\widetilde{x}_1^2 + \alpha^4\widetilde{x}_1 = \widehat{e}_1 = \alpha^{12} \longrightarrow \widetilde{x}_1 = \alpha^{16}.$$

$$\widetilde{e}_1 = \widehat{x}_1 = \alpha^4, \quad \widetilde{x}_1 = x_1^2 = \alpha^{16} \;\longrightarrow x_1 = \alpha^8.$$

$$\widetilde{e}_1 = e_1^2 + e_1 = \alpha^4 \;\longrightarrow\; e_1 = \alpha^{12}.$$

$$\begin{aligned} (u_1\, u_2\, u_3\, u_4\, u_5)(\alpha^2\, \alpha^{29}\, \alpha^5\, \alpha^{14}\alpha^9)^\top &= x_1 \longrightarrow \\ (u_1\, u_2\, u_3\, u_4\, u_5) &= (1\,1\,0\,0\,0) \longrightarrow \\ \underline{e} &= (\alpha^{12}\, \alpha^{12}\, 0\,0\,0) \end{aligned}$$

To find column erasures we solve the following equations:

$$\widetilde{s}_0 = \alpha^3 = \widetilde{e}_1\widetilde{x}_1 + \widetilde{w}_1\widetilde{h}_0 = \alpha^4\alpha^{16} + \alpha^4\widetilde{w}_1 \longrightarrow \widetilde{w}_1 = \alpha^{29}.$$

$$w_1^2 + w_1 = \widetilde{w}_1 = \alpha^{29} \;\longrightarrow\; w_1 = \alpha^{22}.$$

$$\underline{e}_{\text{col}} = (\alpha^{22}\, 0\,0\,0\,0)$$

To find row erasures we solve the following equations:

$$s_0 = \alpha^7 = e_1x_1 + g_1f_1 + w_1h_0 = \alpha^{12}\alpha^8 + 1\cdot f_1 + \alpha 22\alpha^2 \;\longrightarrow f_1 = \alpha^{19}.$$

$$\begin{aligned} (\alpha^2\, \alpha^{29}\, \alpha^5\, \alpha^{14}\alpha^9)(r_1\, r_2\, r_3\, r_4\, r_5)^\top &= f_1 \longrightarrow \\ (r_1\, r_2\, r_3\, r_4\, r_5) &= (1\,0\,1\,1\,1) \longrightarrow \\ \underline{e}_{\text{row}} &= (1\,0\,1\,1\,1) \end{aligned}$$

The total error vector is

$$\underline{\mathbf{e}}_{\text{total}} = \underline{\mathbf{e}} + \underline{\mathbf{e}}_{\text{col}} + \underline{\mathbf{e}}_{\text{row}} = (\alpha^9, \alpha^{12}, 1, 1, 1)$$

The decoding result:

$$\underline{\mathbf{y}} + \mathbf{e}_{\text{total}} =$$

$$(\alpha^{21}, \alpha^{13}, \alpha, \alpha^{22}, \alpha^{8}) + (\alpha^{9}, \alpha^{12}, 1, 1, 1) = (\alpha, \alpha^{30}, \alpha^{18}, \alpha^{7}, \alpha^{20}) =$$

$$\underline{\mathbf{g}}(\mathbf{u}).$$

Variant 2: Column erasures
Let the noise matrix be

$$E = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

where 4 columns $2, 3, 4, 5$ are erased. The noise vector is: $\bar{\mathbf{e}} = (0, \alpha^3, \alpha^2, \alpha, 1)$. The received matrix is

$$Y = M + E = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Transform the received matrix Y to the vector $\underline{\mathbf{y}} = (\alpha\, \alpha^9\, \alpha^{11}\, \alpha^{28}\, \alpha^8)$.
First, compute the syndrome

$$\underline{\mathbf{s}}^\top = \mathbf{H}\underline{\mathbf{y}}^\top = \begin{pmatrix} \alpha^{17} \\ \alpha^{28} \\ \alpha^{4} \\ \alpha^{25} \end{pmatrix}.$$

Since we have the case of column erasures only, using (4.46) we get the system of equations for unknowns $w_k, k = \overline{1, 4}$:

$$\begin{array}{lcllll} s_0 & = & h_1 w_1 + & h_2 w_2 + & h_3 w_3 + & h_4 w_4; \\ s_1 & = & h_1^2 w_1 + & h_2^2 w_2 + & h_3^2 w_3 + & h_4^2 w_4; \\ s_2 & = & h_1^4 w_1 + & h_2^4 w_2 + & h_3^4 w_3 + & h_4^4 w_4; \\ s_3 & = & h_1^8 w_1 + & h_2^8 w_2 + & h_3^8 w_3 + & h_4^8 w_4, \end{array} \tag{4.48}$$

with $h_1 = \alpha^{29}, h_2 = \alpha^5, h_3 = \alpha^{14}, h_4 = \alpha^9, s_0 = \alpha^{17}, s_1 = \alpha^{28}, s_2 = \alpha^4, s_3 = \alpha^{25}$. Hence, we have the system

$$\begin{array}{rclllll} \alpha^{17} & = & \alpha^{29}w_1+ & \alpha^5 w_2+ & \alpha^{14}w_3+ & \alpha^9 w_4; \\ \alpha^{28} & = & \alpha^{27}w_1+ & \alpha^{10}w_2+ & \alpha^{28}w_3+ & \alpha^{18}w_4; \\ \alpha^{4} & = & \alpha^{23}w_1+ & \alpha^{20}w_2+ & \alpha^{25}w_3+ & \alpha^{5}w_4; \\ \alpha^{25} & = & \alpha^{15}w_1+ & \alpha^{9}w_2+ & \alpha^{19}w_3+ & \alpha^{10}w_4 \end{array} \tag{4.49}$$

with solution: $w_1 = \alpha^3, w_2 = \alpha^2, w_3 = \alpha, w_4 = 1$. Accordingly, the noise vector is $\overline{e} = (0, \alpha^3, \alpha^2, \alpha, 1.)$

To find the transmitted information vector $\mathbf{u}$ subtract from the received vector $\underline{\mathbf{y}} = (\alpha\,\alpha^9\,\alpha^{11}\,\alpha^{28}\,\alpha^8)$ the noise vector $\overline{\mathbf{e}} = (0, \alpha^3, \alpha^2, \alpha, 1)$ and get $\mathbf{u} = (\alpha, \alpha^{30}, \alpha^{18}, \alpha^7, \alpha^{20})$.

Variant 3: Column and row erasures. Consider the case of 2 row erasures and 2 column erasures. Let the noise matrix be the same as in Variant 2

$$E = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{4.50}$$

but here we assume that the 1-st and the 4-th rows as well as the 3-rd and 4-th columns are erased. The noise vector is again $\overline{e} = (0, \alpha^3, \alpha^2, \alpha, 1)$, the received matrix is again

$$Y = M + E = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix},$$

and the received vector is again $\underline{\mathbf{y}} = (\alpha\,\alpha^9\,\alpha^{11}\,\alpha^{28}\,\alpha^8)$.
The syndrome is again

$$\underline{\mathbf{s}}^\top = \mathbf{H}\underline{\mathbf{y}}^\top = \begin{pmatrix} \alpha^{17} \\ \alpha^{28} \\ \alpha^4 \\ \alpha^{25} \end{pmatrix}.$$

In this variant of mixed erasures we need the linearized polynomial

$$T(z)=\sum_{i=0}^{v} T_i z^{[i]} = T_0 z + T_1 z^2 + T_2 z^4 \tag{4.51}$$

that has all $\mathbb{F}_q$-linear combinations of g_{i_k}, $k=1,2$, as roots. In particular,

$$T(g_{i_k})=0, \quad k=1,2. \tag{4.52}$$

In this case, the elements $1,\ \alpha^3,\ 0,\ (1+\alpha^3)$ are all the roots of the polynomial $T(z)$, hence

$$T(z)=(z-0)(z-1)(z-\alpha^3)(z-1-\alpha^3)=\alpha z+\alpha^{18}z^2+z^4$$

with coefficients $T_0=\alpha,\ T_1=\alpha^{18},\ T_2=1$.

We use the coefficients T_i to exclude the unknowns f_k, $k=1,2$, and to obtain the modified syndrome $\tilde{s}=(\tilde{s}_0\tilde{s}_1)$. It has dimension $d-3=2$ and is computed as follows

$$\tilde{\mathbf{s}}^\top = \begin{pmatrix} \tilde{s}_0 \\ \tilde{s}_1 \end{pmatrix} = \begin{pmatrix} s_2 & s_1^{[1]} & s_0^{[2]} \\ s_3 & s_2^{[1]} & s_1^{[2]} \end{pmatrix} \begin{pmatrix} T_0 \\ T_1 \\ T_2 \end{pmatrix}, \tag{4.53}$$

where $s_0=\alpha^{17},\ s_0^4=\alpha^6,\ s_1=\alpha^{28},\ s_1^2=\alpha^{25},\ s_2=\alpha^4,\ s_2^2=\alpha^8,\ s_3=\alpha^{25},\ T_0=\alpha,\ T_1=\alpha^{18},\ T_2=1$. From (4.53) we obtain the modified syndrome $\tilde{s}_0=1,\ \tilde{s}_1=\alpha^{19}$.

Now we use (4.39) to remove items that correspond to errors and to keep items with unknowns $\widetilde{w}_{j_k}$

$$\begin{aligned} \tilde{s}_0 &= \widetilde{w}_3\widetilde{h}_3+\widetilde{w}_4\widetilde{h}_4; \\ \tilde{s}_1 &= \widetilde{w}_3\widetilde{h}_3^2+\widetilde{w}_4\widetilde{h}_4^2, \end{aligned} \tag{4.54}$$

where $\widetilde{h}_3=h_3^4=\alpha^{20},\ \widetilde{h}_4=h_4^4=\alpha^{25}$. The solution of the system is $\widetilde{w}_3=\alpha^4,\ \widetilde{w}_4=\alpha^{21}$.

Taking into account notations (4.38) and using $\widetilde{w}_3,\ \widetilde{w}_4$, we solve the following system of equations to find $w_{j_k},\ j_k=3,4$,

$$\begin{aligned} \alpha^4 &= w_3^4+\alpha^{18}w_3^2+\alpha w_3; \\ \alpha^{21} &= w_4^4+\alpha^{18}w_4^2+\alpha w_4. \end{aligned} \tag{4.55}$$

The solution is $w_3=\alpha^2,\ w_4=\alpha$.

Substitute obtained $w_3 = \alpha^2,\ w_4 = \alpha$ into (4.34), where we remove items that include errors, and find unknowns $f_k,\ k = 1, 2, :$

$$\mathbf{s}_{\mathrm{mod}}^{\top} = \begin{pmatrix} s_0^{[n]} \\ s_1^{[n-1]} \end{pmatrix} = \sum_{k=1}^{2} f_k \begin{pmatrix} g_{i_k}^{[n]} \\ g_{i_k}^{[n-1]} \end{pmatrix} + \sum_{k=1}^{2} h_{j_k} \begin{pmatrix} w_{j_k}^{[n]} \\ w_{j_k}^{[n-1]} \end{pmatrix}. \tag{4.56}$$

Using the values $n = 5,\ s_0 = \alpha^{17},\ s_1 = \alpha^{28},\ g_{1_1} = 1,\ g_{4_2} = \alpha^3,\ w_{3_1} = \alpha^2,\ w_{4_2} = \alpha$ gives the following system of equations for $f_{1_1},\ f_{4_2}$:

$$\begin{array}{rl} \alpha^{17} = & f_{1_1} + \alpha^3 f_{4_2} + \alpha^7 + \alpha^{15}; \\ \alpha^{14} = & f_{1_1} + \alpha^{17} f_{4_2} + \alpha^6 + \alpha^{30}. \end{array} \tag{4.57}$$

with the solution $f_{1_1} = \alpha^9,\ f_{4_2} = \alpha^{29}$.

Express $f_{1_1},\ f_{4_2}$ using elements of the first and the fourth rows of the error matrix $f_{i_k} = \sum_{p=1}^{5} h_{p-1} r_{k,p},\ k = 1, 2,\ i = 1,\ 4.$ Using the additive form of the field elements for powers greater than 4, yields

$$\begin{array}{rcl} \alpha^4 + \alpha^3 + \alpha & = & \alpha^4(r_{14} + r_{15}) + \alpha^3(r_{12} + r_{14} + r_{15}) \\ & + & \alpha^2(r_{11} + r_{13} + r_{14}) + \alpha r_{15} + (r_{12} + r_{13} + r_{14}); \\ \alpha^3 + 1 & = & \alpha^4(r_{41} + r_{45}) + \alpha^3(r_{42} + r_{44} + r_{45}) \\ & + & \alpha^2(r_{41} + r_{43} + r_{44}) + \alpha r_{45} + (r_{42} + r_{43} + r_{44}). \end{array} \tag{4.58}$$

Equating coefficients of the same powers of α in the first equation gives the system of linear equations for $r_{k,p},\ k = 1,\ p = \overline{1, 5}$,

$$\begin{array}{rcll} 1 & = & r_{14}+ & r_{15}; \\ 1 & = & r_{12}+ & r_{14} + r_{15}; \\ 0 & = & r_{11}+ & r_{13} + r_{14}; \\ 1 & = & r_{15}; & \\ 0 & = & r_{12}+ & r_{13} + r_{14} \end{array} \tag{4.59}$$

with the solution

$$r_{11} = r_{12} = r_{13} = r_{14} = 0;\ r_{15} = 1.$$

To find $r_{k,p},\ k = 4,\ p = \overline{1, 5}$, we use the second equation of (4.58) in the same way which yields the system

$$\begin{array}{rcll} 0 & = & r_{44}+ & r_{45}; \\ 1 & = & r_{22}+ & r_{44} + r_{45}; \\ 0 & = & r_{41}+ & r_{43} + r_{44}; \\ 0 & = & r_{45}; & \\ 1 & = & r_{42}+ & r_{43} + r_{44} \end{array} \tag{4.60}$$

with solution $r_{41} = r_{43} = r_{44} = r_{45} = 0;\ r_{42} = 1$.

Using the elements of the third and the fourth columns of the noise matrix $w_3 = \alpha^2,\ w_4 = \alpha$, which were obtained earlier, and obtained values $r_{k,p},\ k = 1,\ 4,\ p = \overline{1,5}$, we obtain the following noise matrix:

$$E = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Comparison with the given noise matrix (4.50) shows that both matrices coincide. Hence the decoding is correct.

4.6 Error correction in the Hamming metric

A vector MRD code is simultaneously a Maximum Distance Separable (MDS) code in the Hamming metric, which reaches the Singleton bound. Hence, it is natural to ask the question: What is the Hamming norm for the error vectors corrected by the decoding algorithm proposed above?

First of all, of course, all error vectors of Hamming weight at most $t = \frac{d-1}{2}$ will be corrected. In case of ordinary MDS codes, the Berlekamp-Massey algorithm or its modifications corrects these error vectors only. The decoding algorithm for MRD codes corrects many more (N_i) error vectors, where

$$N_i = \sum_{i=1}^{t} L_i(n) = \sum_{i=1}^{t} \begin{bmatrix} n \\ i \end{bmatrix} (q^N - 1)(q^N - q) \dots (q^N - q^{i-1}), \tag{4.61}$$

and $L_i(n)$ is the number of n-vectors over $\mathbb{F}_{q^N}$ with rank norm t.

Let us count the number of error vectors with Hamming norm s that are corrected by our algorithm. Denote by $A_n(s,i)$ the number of vectors of length n with rank norm i and Hamming norm s. For $s < i$, set $A_n(s,i) = 0$.

Lemma 4.5. *For $A_n(s,i)$ holds*

$$A_n(s,i) = C_n^s \sum_{k=0}^{s} (-1)^{k+s} C_s^k L_i(k). \tag{4.62}$$

Indeed, $A_n(s,i) = C_n^s A_s(s,i)$. In addition, for all $i \le s \le n$

$$\sum_{i=1}^{s} A_n(s,i) = \sum_{s=i}^{n} C_n^s A_s(s,i) = L_i(n). \tag{4.63}$$

By inverting the system (4.63) we obtain (4.62).

From Lemma 4.5 follows

Theorem 4.6. *The proposed above decoding algorithm for MRD codes corrects*

$$M_s = \sum_{i=1}^{s} A_n(s,i) = C_n^s \sum_{i=1}^{t} \sum_{k=i}^{s} (-1)^{k+s} C_s^k L_i(k),\ s = 1, 2, \ldots, n, \tag{4.64}$$

error vectors of Hamming norm s.

It can be shown that for $s \le t$ holds: $M_s = C_n^s (q^N - 1)^s$.

As an illustration consider codes over $\mathbb{F}_{2^N}$ with $n = N$ and $d = 3$. In this case $t = 1$ and according to (4.61) the total number of correctable error vectors is $N_1 = (2^N - 1)^2$. Out of this number, $M_1 = C_N^1 (2^N - 1)$ error vectors have Hamming norm 1 and $M_2 = C_N^2 (2^N - 1)$ vectors have Hamming norm 2, i.e., double errors. The fraction of correctable double errors is $\frac{1}{(2^N - 1)}$. The norm of other correctable errors is at least 3.

A slight modification of the decoding algorithm allows us also to interpret these error vectors as double errors. Assume that our decoding algorithm outputs the error vector $(E, E, \ldots, E, 0, \ldots, 0)$, with rank norm 1 and with Hamming norm $s \ge 3$. Let us solve the system

$$\begin{aligned} Xh_1 + Yh_2 &= E(h_1 + h_2 + \ldots + h_s), \\ Xh_1^{[1]} + Yh_2^{[1]} &= E(h_1^{[1]} + h_2^{[1]} + \ldots + h_s^{[1]}), \end{aligned} \tag{4.65}$$

where $h_1, h_2, \ldots, h_N$ are the elements of the first row of the check matrix. Then the vector $(X, Y, 0, \ldots, 0)$ has Hamming norm 2 and belongs to the same coset as the vector $(E, E, \ldots, E, 0, \ldots, 0)$. Thus, in the Hamming metric, the modified algorithm gets closer to the full decoding algorithm. The full algorithm corrects $2^{2N} - 1$ error vectors of Hamming norms 1 and 2. The modified algorithm corrects only $(2^N - 1)^2$ error vectors of norms 1 and 2, i.e., it does not correct $2^{N+1} - 2$ double errors in comparison with the full algorithm.

Similar modifications are possible for codes with a larger distance as well, however the complexity of the additional part of the algorithm grows fast with the Hamming norm of correctable errors.

5

Symmetric rank codes

5.1 Introduction

Rank metric codes can be described using either the *matrix* or the *vector* form. We recall it here again since we are going to introduce a new class of rank metric codes called symmetric rank codes.

Let $\mathbb{F}_q$ be a field consisting of q elements and $\mathbb{F}_{q^n}$ be its extension of order n. In this chapter we consider square code matrices only.

To obtain the *matrix* description consider a normed ring $M_n(\mathbb{F}_q)$ of $n \times n$ square matrices over the *base* field $\mathbb{F}_q$. The *norm* of a matrix G is its rank, $\mathrm{rank}(G)$, and the *rank distance* $d(G_1, G_2)$ between matrices G_1, G_2 is the rank of their difference, $d(G_1, G_2) = \mathrm{rank}(G_1 - G_2)$. Any subset $\mathcal{M} \subseteq M_n(\mathbb{F}_q)$ is called a *code. The code distance* $d(\mathcal{M}) = d$ is the minimum pairwise distance between code matrices, $d = \min\{\mathrm{rank}(G_1 - G_2) : G_1, G_2 \in \mathcal{M}; G_1 \neq G_2\}$. A code is called $\mathbb{F}_q$-*linear*, if any linear combination of code matrices with coefficients from $\mathbb{F}_q$ also belongs to the code. The code obtained by transposing matrices of $\mathcal{M}$ is called the *transposed code* $\mathcal{M}^T$. The codes $\mathcal{M}$ and $\mathcal{M}^T$ have the same number of code matrices and the same code distance. If $\mathcal{M}$ is $\mathbb{F}_q$-*linear* then $\mathcal{M}^T$ is $\mathbb{F}_q$-*linear* as well.

To get the *vector* description consider the normed space $\mathbb{F}_{q^n}^n$ of n-vectors over the *extension* field $\mathbb{F}_{q^n}$. *The norm or the rank* of a vector $\mathbf{g}$ is the maximum number $r(\mathbf{g})$ of its components that are linearly independent over the base field

$\mathbb{F}_q$. The *rank distance* $d(\mathbf{g}_1,\mathbf{g}_2)$ between vectors $\mathbf{g}_1,\mathbf{g}_2$ is the norm of their difference, $d(\mathbf{g}_1,\mathbf{g}_2)=r(\mathbf{g}_1-\mathbf{g}_2)$. *A code* $\mathcal{V}\subseteq\mathbb{F}_{q^n}^n$ is a subset of vectors $\mathbb{F}_{q^n}^n$. *The code distance* $d(\mathcal{V})=d$ is the minimum pairwise distance between code vectors, $d=\min\{r(\mathbf{g}_1-\mathbf{g}_2):\mathbf{g}_1,\mathbf{g}_2\in\mathcal{V};\mathbf{g}_1\neq\mathbf{g}_2\}$. The code $\mathcal{V}$ is $\mathbb{F}_{\mathrm{q}}$-*linear* if any linear combination of code vectors with coefficients from $\mathbb{F}_{\mathrm{q}}$ also belongs to the code. The code $\mathcal{V}$ is $\mathbb{F}_{q^n}$-*linear* if any linear combination of code vectors with coefficients from $\mathbb{F}_{q^n}$ also belongs to the code, i.e., if $\mathcal{V}$ is a linear subspace of the space $\mathbb{F}_{q^n}^n$. $\mathbb{F}_q$-linearity follows from $\mathbb{F}_{q^n}$-linearity, however, the inverse statement is not true. For $k=1,2,\dots,n$ there are known $\mathbb{F}_{q^n}$ linear (n,k,d)-codes with maximum possible rank distance (MRD) $d=n-k+1$. These codes are k-dimensional subspaces of the space $\mathbb{F}_{q^n}^n$.

Let $\Omega=\{\omega_1,\omega_2,\dots,\omega_n\}$ be a basis of the extension field $\mathbb{F}_{q^n}$ over the base field $\mathbb{F}_q$. Let $\theta^{-1}:\mathbb{F}_{q^n}\Rightarrow\mathbb{F}_q^n$ be the isomorphism from the field $\mathbb{F}_{q^n}$ to the space of column n-vectors over $\mathbb{F}_q$. Elements of the basis are transformed to the linear independent columns $\mathbf{b}_1,\mathbf{b}_2,\dots,\mathbf{b}_n\in\mathbb{F}_q^n$, where $\mathbf{b}_j=\theta^{-1}(\omega_j)$, $j=1,2,\dots,n$.

Let $\theta:\mathbb{F}_q^n\Rightarrow\mathbb{F}_{q^n}$ be the inverse transform $\theta(\mathbf{b})=\beta$. Applying it to each column of the matrix $M\in M_n(\mathbb{F}_q)$ we obtain one to one mapping $\Theta:M_n(\mathbb{F}_q)\Rightarrow\mathrm{K}_\mathrm{n}^\mathrm{n}$ of the space of $(n\times n)$-matrices over $\mathbb{F}_q$ to the space of n-vectors over $\mathbb{F}_{q^n}$. Obviously, the rank of matrix M after the transform $\Theta(M)=\mathbf{g}$ coincides with the rank of the vector $\mathbf{g}$, i.e., $\mathrm{rank}(M)=r(\mathbf{g})$.

The transform Θ is isometric. Given a matrix code $\mathcal{M}$ the transform allows us to get the vector code using $\mathcal{V}=\Theta(\mathcal{M})$. And vice versa, given a vector code $\mathcal{V}$, we get the matrix code $\mathcal{M}=\Theta^{-1}(\mathcal{V})$ with the same distance properties.

Vector form is more convenient to describe rank metric codes and fast decoding algorithms. Matrix form is useful in the systems with coded modulation, e.g. in the theory of space-time codes.

Using a known rank metric code one can design a new code with the same cardinality and code distance as follows. Given a code $\mathcal{V}$ in vector form, two transforms θ and $\widetilde{\theta}$, and also connected with them transforms Θ and $\widetilde{\Theta}$. We obtain a new code $\mathcal{V}^T$ using the following chain of transforms

$$\mathcal{V}\xrightarrow{\Theta^{-1}}\mathcal{M}\longrightarrow\mathcal{M}^T\xrightarrow{\widetilde{\Theta}}\mathcal{V}^{\mathcal{T}}. \tag{5.1}$$

The code $\mathcal{V}^T$ we call *the transposed code in vector form.* Note that transforms θ and $\widetilde{\theta}$ may be different.

The code $\mathcal{V}^T$ has the same volume and the same rank-weight distribution as the code $\mathcal{V}$. However, if the code $\mathcal{V}$ is $\mathbb{F}_{q^n}$-linear (e.g. an MRD (n,k,d=n-k+1)-code), then the code $\mathcal{V}^T$ is not necessarily $\mathbb{F}_{q^n}$-linear, despite it remaining

$\mathbb{F}_q$-linear. This is a drawback of the construction, since fast decoding methods for such codes are not known. One can decode the corrupted code vector $\mathbf{y} = \mathbf{w} + \mathbf{e},\ \mathbf{w} \in \mathcal{V}^T$, transforming it using (5.1) to the corrupted vector $\mathbf{z} = \mathbf{v} + \widetilde{\mathbf{e}},\ \mathbf{v} \in \mathcal{V}$, and use a standard method for decoding $\mathcal{V}$. However, in this case the question arises: Why should we use the code $\mathcal{V}^T$ at all? Another disadvantage of $\mathbb{F}_q$-linear codes is an increase in the size of a generator matrix in comparison with $\mathbb{F}_{q^m}$-linear codes.

Let us demonstrate this with the following example.

Example 1. Let $q = 2$. For the code $\mathcal{V}$ we take the following one dimensional $\mathbb{F}_{q^n}$-linear $(n, 1, n)$-code, $n = 3$.

$$\begin{aligned}&\mathcal{V} = \\ &\{(0,0,0),(1,\alpha,\alpha^2),(\alpha,\alpha^2,\alpha^3),(\alpha^2,\alpha^3,\alpha^4),\\ &(\alpha^3,\alpha^4,\alpha^5),(\alpha^4,\alpha^5,\alpha^6),(\alpha^5,\alpha^6,1),(\alpha^6,1,\alpha)\},\end{aligned}$$

where α is a root of the primitive polynomial $f(\lambda) = \lambda^3 + \lambda^2 + 1$. The generator matrix of the code consists of a single row $\mathbf{G} = (1, \alpha, \alpha^2)$, $\mathbf{u} = (u),\ u \in \mathbb{F}_{2^3}$, is an one dimensional information vector, the code vectors are $\mathbf{v} = \mathbf{uG} = (u, u\alpha, u\alpha^2)$.

Let θ^{-1} be defined by $0 \leftrightarrow (0,0,0)^T, 1 \leftrightarrow (1,0,0)^T, \alpha \leftrightarrow (0,1,0)^T,\ \alpha^2 \leftrightarrow (0,0,1)^T$. Then the code $\mathcal{M}$ is the following set of (3×3)-matrices:

$$M_0 = \begin{pmatrix}0&0&0\\0&0&0\\0&0&0\end{pmatrix}, M_1 = \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}, M_2 = \begin{pmatrix}0&0&1\\1&0&0\\0&1&1\end{pmatrix}, M_3 = \begin{pmatrix}0&1&1\\0&0&1\\1&1&1\end{pmatrix},$$

$$M_4 = \begin{pmatrix}1&1&1\\0&1&1\\1&1&0\end{pmatrix}, M_5 = \begin{pmatrix}1&1&0\\1&1&1\\1&0&1\end{pmatrix}, M_6 = \begin{pmatrix}1&0&1\\1&1&0\\0&1&0\end{pmatrix}, M_7 = \begin{pmatrix}0&1&0\\1&0&1\\1&0&0\end{pmatrix}.$$

The transposed code in vector form using θ is

$$\begin{aligned}&\mathcal{V}^T = \\ &\{(0,0,0),(1,\alpha,\alpha^2),(\alpha^2,1,\alpha^6),(\alpha^6,\alpha^2,\alpha^4),\\ &(\alpha^4,\alpha^6,\alpha^3),(\alpha^5,\alpha^4,\alpha^3),(\alpha^3,\alpha^5,\alpha),(\alpha,\alpha^3,1)\}.\end{aligned}$$

The code $\mathcal{V}^T$ is $\mathbb{F}_q$-linear, but *it is not* a linear space, i.e., it is not $\mathbb{F}_{q^n}$-linear. A generator matrix of the code is

$$\mathbf{G} = \begin{pmatrix}1&\alpha&\alpha^2\\ \alpha^2&1&\alpha^6\\ \alpha^6&\alpha^2&\alpha^4\end{pmatrix},$$

an information vector is $\mathbf{u} = (u_1, u_2, u_3)$, $u_1, u_2, u_3 \in \mathbb{F}_2$. Code vectors are $\mathbf{w} = \mathbf{uG} = (u_1 + u_2\alpha^2 + u_3\alpha^6, u_1\alpha + u_2 + u_3\alpha^2, u_1\alpha^2 + u_2\alpha^6 + u_3\alpha^4)$.

The finite field $\mathbb{F}_{q^n}$ can be described in terms of $(n \times n)$-matrices A over the field $\mathbb{F}_q$ such that powers A^i, $i = 1, 2, \ldots, q^n - 1$, correspond to all nonzero elements of $\mathbb{F}_{q^n}$. In this chapter, we will show that for fields $\mathbb{F}_{q^n}$ of characteristic 2 one can select a symmetric matrix A. We will show constructions of symmetric matrices representing a field. Together with all-zero matrix these matrices form a $\mathbb{F}_{q^n}$-linear code with maximum distance $d = n$ and with maximum possible volume q^n for this distance. These codes are called *symmetric rank codes*. In vector form, they are MRD $(n, 1, n)$-codes with maximum rank distance and can be decoded using known methods of error correction in rank metric. For the symmetric codes, we will suggest a method for erasure symmetrization that allows for decreasing decoding complexity substantially in comparison with standard approaches.

We will also show that a linear $(n, k, d = n - k + 1)$ MRD code $\mathcal{V}_k$ that includes the previously mentioned one-dimensional symmetric code as a subcode has the following property: corresponding transposed code is $\mathbb{F}_{q^n}$-linear. Such codes have increased capability to correct *symmetric* errors and erasures.

Given a linear $(n, k, d = n - k + 1)$ MRD code $\mathcal{V}$ in vector form, can we find transforms Θ and $\widetilde{\Theta}$ (if they exist) such that the transposed code $\mathcal{V}^T$ in vector form is also a linear $(n, k, d = n - k + 1)$ MRD code?

A positive answer will be given for a special case $(n, 1, d = n)$ MRD codes and for fields $\mathbb{F}_{q^n}$ of characteristic 2, i.e., $q = 2^r$. From(5.1) it is easy to see: if the set $\mathcal{M}$ consists of *symmetric* matrices, then $\mathcal{M} = \mathcal{M}^T$ and for $\Theta = \widetilde{\Theta}$ we obtain $\mathcal{V} = \mathcal{V}^T$. A linear $(n, 1, d = n)$ MRD code $\mathcal{V}$ can be defined by a single-row generator matrix

$$\mathbf{G} = (g_1, g_2, \ldots, g_n),$$

where elements $g_j \in \mathbb{F}_{q^n}$, $j = 1, 2, \ldots, n$, are linearly independent over $\mathbb{F}_q$. In this case, the code consists of the all zero vector $\mathbf{0}$ and vectors $\alpha^s\mathbf{G}$, $s = 0, 1, \ldots, q^n - 2$. We will show that there exist a single-row matrix $\mathbf{G}$ and a transform Θ such that $\Theta^{-1}(\alpha^s\mathbf{G}) = A^s$, where A is a symmetric matrix.

5.2 Matrix and vector representations of extension finite fields

Let $A \in M_n(\mathbb{F}_q)$.

Definition 2. *A matrix A represents the field $\mathbb{F}_{q^n}$ if the algebra of polynomials $\mathbb{F}_q[A]$ is isomorphic to $\mathbb{F}_{q^n}$.*

We say that the matrix A gives a *primitive* representation of the field if all matrices $A^s,\ s = 1, 2, \dots, q^n - 1$, are different. The following lemma gives a characterization of such matrices.

Lemma 5.1. *A matrix $A \in M_n(\mathbb{F}_q)$ gives a primitive representation of the field $\mathbb{F}_{q^n}$ if and only if its characteristic polynomial* $\det(\lambda I_n - A)$ *is a primitive polynomial $f(\lambda)$ over $\mathbb{F}_q$ of degree n,*

$$f(\lambda) = \lambda^n + f_{n-1}\lambda^{n-1} + f_{n-3}\lambda^{n-2} + \ldots + f_1\lambda^1 + f_0. \tag{5.2}$$

Recall the definition: A non-reducible over $\mathbb{F}_q$ polynomial $f(\lambda)$ of degree n is called primitive if $f(\lambda)$ divides the binomial $\lambda^{q^n-1} - 1$, but does not divide the binomials $\lambda^s - 1,\ 1 \le s \le q^n - 2$.

Proof. Let $\det(\lambda I_n - A) = f(\lambda)$, where $f(\lambda)$ is primitive. Then $f(A) = O_n$, where O_n is the $n \times n$ all zero matrix. Since the polynomial $f(\lambda)$ divides $\lambda^{q^n-1} - 1$, but does not divide the binomials $\lambda^s - 1,\ 1 \le s \le q^n - 2$, we have $A^{q^n-1} = I_n$, and all the matrices $A^s,\ s = 1, 2, \dots, q^n - 1$, are different. Moreover, all the matrices A^s can be written as linear combinations of matrices $I_n, A, A^2, \dots, A^{n-1}$ using $A^n = -f_{n-1}A^{n-1} - f_{n-2}A^{n-2} - \ldots - f_1A - f_0I_n$. Hence, the algebra of matrix polynomials $\mathbb{F}_{q^n}[A]$ is isomorphic to the field $\mathbb{F}_{q^n}$ obtained by joining a root α of the primitive polynomial $f(\lambda)$ to the field $\mathbb{F}_q$. Thus, the matrix A gives primitive representation of the field $\mathbb{F}_{q^n}$.

The inverse is also true. Let the matrix A give primitive representation of the field $\mathbb{F}_{q^n}$. Then the minimal polynomials of A and α are the same and they coincide with a primitive polynomial $f(\lambda)$. Since the characteristic polynomial is divisible by the minimal polynomial and has the same degree and the same leading coefficient, we get $\det(\lambda I_n - A) = f(\lambda)$. ■

Corollary 5.2. *All the matrices A that represent the field $\mathbb{F}_{q^n}$ are similar to the matrix*

$$C = \begin{pmatrix} 0 & 0 & \dots & 0 & -f_0 \\ 1 & 0 & \dots & 0 & -f_1 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & \dots & 0 & -f_{n-2} \\ 0 & 0 & \dots & 1 & -f_{n-1} \end{pmatrix},$$

i.e., $A = QCQ^{-1}$, where $Q \in M_n(\mathbb{F}_q)$ is a nonsingular matrix and $f_0, f_1, \dots, f_{n-1}$ are coefficients of a monic primitive polynomial

$$f(\lambda) = \lambda^n + f_{n-1}\lambda^{n-1} + f_{n-3}\lambda^{n-2} + \ldots + f_1\lambda^1 + f_0.$$

Proof. Characteristic polynomials of similar matrices coincide. We have $\det(\lambda I_n - C) = \lambda^n + f_{n-1}\lambda^{n-1} + f_{n-2}\lambda^{n-2} + \ldots + f_1\lambda^1 + f_0 = f(\lambda)$. Let A be an $n \times n$ matrix with a characteristic polynomial $\det(\lambda I_n - A) = f(\lambda)$. Since $f(\lambda)$ is primitive, the sets of invariant polynomials of the matrices $\lambda I_n - A$ and $\lambda I_n - C$ are the same: $f(\lambda), 1, \dots, 1$. Hence, according to the necessary and sufficient condition [Gan67], the matrix A is similar to the matrix C, i.e., $A = QCQ^{-1}$, where Q is a non-singular matrix over the base field $\mathbb{F}_q$. ■

Let $M[j]$ denote the $j-$th column of a matrix M. Let A be a matrix that gives primitive representation of the field $\mathbb{F}_{q^n}$. Define *induced* vector representation of the field $\mathbb{F}_{q^n}$ as follows

$$\begin{array}{llll} \theta^{-1}(0) & = O_n[1], & \theta(O_n[1]) & = 0, \\ \theta^{-1}(\alpha^s) & = A^s[1], & \theta(A^s[1]) & = \alpha^s,\ s = 0, 1, \dots, q^n - 2. \end{array} . \tag{5.3}$$

We say that this representation *is agreed* with the matrix A.

Lemma 5.3. *Let $c \in \mathbb{F}_{q^n}$ then*

$$\theta^{-1}(\alpha c) = A\theta^{-1}(c),$$

where α is a primitive element of $\mathbb{F}_{q^n}$.

Proof. Since $c = \alpha^s$ for some s, then $\theta^{-1}(\alpha c) = \theta^{-1}(\alpha^{1+s}) = A^{1+s}[1] = AA^s[1] = A\theta^{-1}(c)$. ■

Recall: given a vector $\mathbf{c} = (c_1, c_2, \dots, c_n) \in \mathbb{F}_{q^n}$, we define

$$\Theta^{-1}(\mathbf{c}) = (\theta^{-1}(c_1), \theta^{-1}(c_2), \dots, \theta^{-1}(c_n)). \tag{5.4}$$

Thus, $\Theta^{-1}(\mathbf{c}) = M$ is an $(n \times n)$-matrix over the field $\mathbb{F}_q$.

Clearly

$$\Theta^{-1}(\alpha\mathbf{c}) = A\Theta^{-1}(\mathbf{c}) = AM,$$

and in general case

$$\Theta^{-1}(\alpha^s\mathbf{c}) = A^s\Theta^{-1}(\mathbf{c}) = A^sM, \ s = 1, 2, \dots . \tag{5.5}$$

The inverse also holds:

$$\Theta(A^sM) = \alpha^s\Theta(M) = \alpha^s\mathbf{c}.$$

In addition, if $\mathbf{c} \in \mathbb{F}_{q^n}$ and R is an $(n \times m)$-matrix over the field $\mathbb{F}_q$, then

$$\Theta^{-1}(\mathbf{c}R) = \Theta^{-1}(\mathbf{c})R = MR.$$

5.3 Symmetric matrices representing a field

Let us show that the matrix A representing the field F_{q^n}, $q = 2^n$, of characteristic 2 can be selected to be symmetric[1]. The first such construction was suggested in [GP02] for fields of characteristic 2, and it uses $2n - 1$ free parameters. Here we describe a simpler construction with n free parameters only [GP04, GP06].

5.3.1 Auxiliary matrices and determinants

All operations are in a field $\mathbb{F}$ of characteristic 2.

Let $D_n(\lambda)$ be the tridiagonal $\lambda-$matrix of order n, with λ on the main

[1] Examples show that for $n = 2, 3$ one can find symmetric matrices representing the field of arbitrary characteristic p. For example, the matrix $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ represents the field $\mathbb{F}_{3^2}$. However, a general construction is not known. The fields of characteristic 0 cannot be represented by symmetric matrices.

diagonal and 1 in the neighboring positions

$$D_n(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 & 0 & 0 \\ 1 & \lambda & 1 & \dots & 0 & 0 & 0 \\ 0 & 1 & \lambda & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \lambda & 1 & 0 \\ 0 & 0 & 0 & \dots & 1 & \lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 & \lambda \end{pmatrix}. \tag{5.6}$$

The determinant of this matrix is denoted by $d_n(\lambda)$.

Let $H_n(\lambda)$ be the tridiagonal $\lambda-$matrix of order n, where the last element of the main diagonal is $\lambda + 1$:

$$H_n(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 & 0 & 0 \\ 1 & \lambda & 1 & \dots & 0 & 0 & 0 \\ 0 & 1 & \lambda & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \lambda & 1 & 0 \\ 0 & 0 & 0 & \dots & 1 & \lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 & \lambda+1 \end{pmatrix}. \tag{5.7}$$

Denote the determinant of this matrix by $h_n(\lambda)$. Let us define $d_{-1}(\lambda) = 0$, $d_0(\lambda) = 1$, $h_{-1}(\lambda) = 1$, $h_0(\lambda) = 1$. It is easy to see that $d_1(\lambda) = \lambda$, $h_1(\lambda) = \lambda + 1$.

The determinants $d_n(\lambda)$ and $h_n(\lambda)$ can be computed recurrently

$$\begin{aligned} d_n(\lambda) &= d_1(\lambda)d_{n-1}(\lambda) + d_{n-2}(\lambda),\ n \geq 2; \\ h_n(\lambda) &= d_1(\lambda)h_{n-1}(\lambda) + h_{n-2}(\lambda),\ n \geq 2. \end{aligned} \tag{5.8}$$

Further, using (5.8) repeatedly, we get for $s \geq 1$

$$\begin{aligned} d_n(\lambda) &= d_s(\lambda)d_{n-s}(\lambda) + d_{s-1}(\lambda)d_{n-s-1}(\lambda),\ n \geq 2; \\ h_n(\lambda) &= d_s(\lambda)h_{n-s}(\lambda) + d_{s-1}(\lambda)h_{n-s-1}(\lambda),\ n \geq 2. \end{aligned} \tag{5.9}$$

5.3.2 The main construction

In fields of characteristic 2, every element is a square of another. Select the elements $a_{n-1}, a_{n-2} = b_{n-2}^2, a_{n-3} = b_{n-3}^2, \dots, a_0 = b_0^2 \in \mathbb{F}$. Let $\mathbf{b} =$

$(b_{n-2}, b_{n-3}, \dots, b_0)$. Consider the following bordered symmetric matrix:

$$A = \begin{pmatrix} a_{n-1} & \mathbf{b} \\ \mathbf{b}^T & H_{n-1}(0) \end{pmatrix} = \begin{pmatrix} a_{n-1} & b_{n-2} & b_{n-3} & b_{n-4} & \dots & b_2 & b_1 & b_0 \\ b_{n-2} & 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ b_{n-3} & 1 & 0 & 1 & \dots & 0 & 0 & 0 \\ b_{n-4} & 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ b_2 & 0 & 0 & 0 & \dots & 0 & 1 & 0 \\ b_1 & 0 & 0 & 0 & \dots & 1 & 0 & 1 \\ b_0 & 0 & 0 & 0 & \dots & 0 & 1 & 1 \end{pmatrix}. \tag{5.10}$$

Let

$$g(\lambda) = \lambda^n + g_{n-1}\lambda^{n-1} + g_{n-3}\lambda^{n-2} + \dots + g_1\lambda^1 + g_0 \tag{5.11}$$

be *an arbitrary* monic polynomial of degree n over $\mathbb{F}$.

Theorem 5.4. *There exists a matrix (5.10) with a characteristic polynomial $g(\lambda)$.*

Proof. Let us compute the characteristic polynomial of A

$$\chi_n(\lambda) = \det(\lambda I_n + A) = \det \begin{pmatrix} \lambda + a_{n-1} & \mathbf{b} \\ \mathbf{b}^T & H_{n-1}(\lambda) \end{pmatrix}$$

$$= \det \begin{pmatrix} \lambda + a_{n-1} & b_{n-2} & b_{n-3} & b_{n-4} & \dots & b_2 & b_1 & b_0 \\ b_{n-2} & \lambda & 1 & 0 & \dots & 0 & 0 & 0 \\ b_{n-3} & 1 & \lambda & 1 & \dots & 0 & 0 & 0 \\ b_{n-4} & 0 & 1 & \lambda & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ b_2 & 0 & 0 & 0 & \dots & \lambda & 1 & 0 \\ b_1 & 0 & 0 & 0 & \dots & 1 & \lambda & 1 \\ b_0 & 0 & 0 & 0 & \dots & 0 & 1 & \lambda + 1 \end{pmatrix}. \tag{5.12}$$

By decomposing the determinant using elements of the first row, and then decomposing the determinants obtained using elements of the first column, after simplifications we obtain

$$\begin{aligned}\chi_n(\lambda) \quad &= (\lambda + a_{n-1})h_{n-1}(\lambda) + b_{n-2}^2 h_{n-2}(\lambda) + b_{n-3}^2 d_1(\lambda)h_{n-3}(\lambda) + \dots \\ &+ b_1^2 d_{n-3}(\lambda)h_1(\lambda) + b_0^2 d_{n-2}(\lambda) \\ &= (\lambda + a_{n-1})h_{n-1}(\lambda) + a_{n-2}h_{n-2}(\lambda) + a_{n-3}d_1(\lambda)h_{n-3}(\lambda) + \dots \\ &+ a_1 d_{n-3}(\lambda)h_1(\lambda) + a_0 d_{n-2}(\lambda),\end{aligned} \tag{5.13}$$

where polynomials $h_i(\lambda)$ and $d_i(\lambda)$ are defined by (5.8).

The relation (5.13) shows that the characteristic polynomial $\chi_n(\lambda)$ is a linear combination of polynomials

$$(\lambda h_{n-1}(\lambda), h_{n-1}(\lambda), h_{n-2}(\lambda), d_1(\lambda)h_{n-3}(\lambda), \dots, d_{n-3}(\lambda)h_1(\lambda), d_{n-2}(\lambda)) \tag{5.14}$$

with coefficients

$$(1, a_{n-1}, a_{n-2}, \dots, a_1, a_0). \tag{5.15}$$

Let us show that the polynomials (5.14) are linearly independent over $\mathbb{F}$. The polynomial $\lambda h_{n-1}(\lambda)$ has degree n, the polynomial $h_{n-1}(\lambda)$ has degree $n-1$, and the rest of the polynomials

$$(h_{n-2}(\lambda), d_1(\lambda)h_{n-3}(\lambda), \dots, d_{n-3}(\lambda)h_1(\lambda), d_{n-2}(\lambda)) \tag{5.16}$$

have degree $n-2$. It is sufficient to show the linear independency of polynomials (5.16). Let us add the polynomial $h_{n-2}(\lambda)$ in the system (5.16) to all the other polynomials $d_s(\lambda)h_{n-2-s}(\lambda)$, $s = 1, 2, \dots, n-2$. Using (5.9), we get $h_{n-2}(\lambda) + d_s(\lambda)h_{n-2-s}(\lambda) = d_{s-1}(\lambda)h_{n-3-s}(\lambda)$, where the degrees of polynomials $d_{s-1}(\lambda)h_{n-3-s}(\lambda)$ are $n-4$. As a result, the system of polynomials (5.16) is transformed to the system

$$(h_{n-2}(\lambda), h_{n-4}(\lambda), d_1(\lambda)h_{n-5}(\lambda), \dots, d_{n-5}(\lambda)h_1(\lambda), d_{n-4}(\lambda), d_{n-3}(\lambda)). \tag{5.17}$$

The first polynomial $h_{n-2}(\lambda)$ of the system has degree $n-2$, the last one, $d_{n-3}(\lambda)$, has degree $n-3$, the remaining polynomials

$$(h_{n-4}(\lambda), d_1(\lambda)h_{n-5}(\lambda), \dots, d_{n-5}(\lambda)h_1(\lambda), d_{n-4}(\lambda))$$

have degree $n-4$ and are similar to (5.16). By iterative continuation of this procedure, we reduce the system (5.16) to the system

$$\begin{aligned}&(h_{n-2}(\lambda), h_{n-4}(\lambda), h_{n-6}(\lambda), \ldots, h_2(\lambda), h_0(\lambda), d_1(\lambda), d_3(\lambda), \ldots, d_{n-3}(\lambda))\\ &\quad \text{for even } n, \text{ and}\\ &(h_{n-2}(\lambda), h_{n-4}(\lambda), h_{n-6}(\lambda), \ldots, h_1(\lambda), d_0(\lambda), d_2(\lambda), d_4(\lambda), \ldots, d_{n-3}(\lambda))\\ &\quad \text{for odd } n.\end{aligned} \tag{5.18}$$

All the polynomials in this system have different degrees and hence they are linearly independent over $\mathbb{F}$.

We proved that the system of polynomials (5.14) is linearly independent. Hence, there exists a nonsingular matrix M_n of order n with elements 0 and 1, such that

$$\begin{aligned}&(\lambda h_{n-1}(\lambda), h_{n-1}(\lambda), h_{n-2}(\lambda), d_1(\lambda)h_{n-3}(\lambda), \ldots, d_{n-3}(\lambda)h_1(\lambda), d_{n-2}(\lambda))^T\\ &= M_n(\lambda^n, \lambda^{n-1}, \lambda^{n-2}, \ldots, \lambda, 1)^T.\end{aligned} \tag{5.19}$$

The rows of the matrix M_n are formed by coefficients of the corresponding polynomials from the left part of (5.19).

Thus, for a given polynomial (5.11), elements of the symmetric matrix (5.10) with this characteristic polynomial can be obtained by

$$\begin{aligned}&(1, a_{n-1}, a_{n-2}, \ldots, a_1, a_0) =\\ &(1, g_{n-1}, g_{n-2}, \ldots, g_1, g_0)M_n^{-1}\end{aligned} \tag{5.20}$$

and taking the square root of a_s, $s = 1, 2, \ldots, n-1$, defined earlier. ■

In particular, if the polynomial (5.11) coincides with the primitive polynomial (5.2) then the matrix A represents the field $\mathbb{F}_{q^n}$.

Example 5. *Let $q = 4$, $\mathbb{F}_q = \mathbb{F}_4$, $n = 2$, $\mathbb{F}_{q^2} = \mathbb{F}_{16}$. Let t be a primitive element of the field $\mathbb{F}_q$, i.e, $t^2 + t + 1 = 0$. The polynomial $f(\lambda) = \lambda^2 + \lambda(t+1) + (t+1)$ is primitive over $\mathbb{F}_q$. The symmetric matrix*

$$A = \begin{pmatrix} t & t \\ t & 1 \end{pmatrix}$$

represents the field $\mathbb{F}_{q^2} = \mathbb{F}_{16}$ since it has the characteristic polynomial $f(\lambda)$.

Example 6. *Let $q = 2$, $\mathbb{F}_q = \mathbb{F}_2$, $n = 4$, $\mathbb{F}_{q^4} = \mathbb{F}_{16}$. The polynomial $f(\lambda) =$*

$\lambda^4+\lambda^3+1$ *over* $\mathbb{F}_q$ *is primitive. The symmetric matrix*

$$A=\begin{pmatrix}0&0&1&1\\0&0&1&0\\1&1&0&1\\1&0&1&1\end{pmatrix}$$

has the characteristic polynomial $f(\lambda)$ *and hence* A *represents the field* $\mathbb{F}_{16}$*.*

5.3.3 Other constructions

Let $n=ms$. Then the field $\mathbb{F}_{q^n}$ can be defined by an irreducible over $\mathbb{F}_{q^m}$ primitive polynomial or degree s. Let a symmetric matrix $A\in M_s(\mathbb{F}_{q^m})$ of order s represent the field $\mathbb{F}_{q^n}$. In turn, let a symmetric matrix $B\in M_m(\mathbb{F}_{q^s})$ of order m represent the field $\mathbb{F}_{q^m}$. Let us replace every element of the matrix A by corresponding symmetric matrix of order m. As a result we obtain a symmetric matrix D of order $ms=n$ with elements from $\mathbb{F}_q$. The characteristic polynomial of the matrix will be irreducible. If it is also irreducible then D represents $\mathbb{F}_{q^n}$. Otherwise, one can consider a linear combination of powers of the matrix D that has a primitive characteristic polynomial (frequently it is sufficient to consider the matrix $D+I_n$).

Example 7. *The matrix* $B=\begin{pmatrix}0&1\\1&1\end{pmatrix}$ *represents the field* $\mathbb{F}_4$*. We replace elements in the matrix* A *of Example 5 by corresponding powers of the matrix* B*:*

$$A=\begin{pmatrix}t&t\\t&1\end{pmatrix}\to D=\begin{pmatrix}0&1&0&1\\1&1&1&1\\0&1&1&0\\1&1&0&1\end{pmatrix}.$$

The characteristic polynomial of the matrix D *is* $\lambda^4+\lambda+1$*, hence* D *represents the field* $GF(16)$*, since the characteristic polynomial is primitive over* F_2*.*

5.4 Codes based on symmetric matrices

Let a symmetric matrix $A \in M_n(\mathbb{F}_q)$ primitively represent the field $\mathbb{F}_{q^n}$. Consider the matrix code $\mathcal{M}$ that consists of q^n matrices

$$\mathcal{M} = \left\{ O_n, I_n, A, A^2, \ldots, A^{q^n-2} \right\}. \tag{5.21}$$

Lemma 5.5. *The code $\mathcal{M}$ is an $\mathbb{F}_q-$linear MRD code with rank code distance $d = n$.*

Proof. Since A represents $\mathbb{F}_{q^n}$, an $\mathbb{F}_q-$linear combination of matrices from $\mathcal{M}$ belongs to $\mathcal{M}$. The difference of any two different matrices from $\mathcal{M}$ is a nonzero matrix from $\mathcal{M}$ and has rank n. The code volume is maximum possible for the code distance $d = n$, since the code parameters reach the Singleton bound. Volume $\mathcal{M}$ of the code is maximum possible for the distance $d = n$, since any code with cardinality more than q^n has a pair of matrices, such that their difference has all-zero row, hence the distance between them is less than n. ∎

Let us transform the matrix code $\mathcal{M}$ to the vector code $\mathcal{V}_1$ using a vector representation of the field (5.3) agreed with the matrix A.

Lemma 5.6. *The vector code $\mathcal{V}_1$ is $\mathbb{F}_{q^n}$-linear $(n, 1, n)$ MRD code.*

Proof. Take the vector $\Theta(I_n)$

$$\mathbf{g}_0 = (g_1, g_2, \ldots, g_n) = \Theta(I_n) \tag{5.22}$$

as the only row of the generator matrix. $\mathbb{F}_{q^n}$-linear $(n, 1, n)$ MRD code $\mathcal{V}_1$, generated by this matrix, consists of the vectors

$$\mathbf{0}, \mathbf{g}_0, \alpha\mathbf{g}_0, \alpha^2\mathbf{g}_0, \ldots, \alpha^{q^n-2}\mathbf{g}_0. \tag{5.23}$$

According to (5.5) we have: $\Theta^{-1}(\alpha\mathbf{g}_0) = A\Theta^{-1}(\mathbf{g}_0) = AI_n = A$ and similarly $\Theta^{-1}(\alpha^s\mathbf{g}_0) = A^s\Theta^{-1}(\mathbf{g}_0) = A^sI_n = A^s$, $s = 2, \ldots, q^n - 2$. This proves that the vector linear code (5.23) is the preimage of the matrix code (5.21). ∎

Obviously, the transposed code $\mathcal{V}_1^T$ coincides with $\mathcal{V}_1$ and hence is linear too.

5.5 Erasure correction

It is appropriate to explain rank erasures for the *matrix form* of a code. For general MRD codes joint error and erasure correction was considered in Chapter 4.

In applications, a code vector should be converted to a matrix form, and every element of the matrix is transmitted over a channel. The receiver makes a hard decision about every element. Only after this, is the matrix converted to a vector to be used by an algebraic decoder. The received matrix is $Y = M + E$, where M is a code matrix and E is an error matrix, which will also be called a rank error. If $\operatorname{rank}(E) \le (d-1)/2$, then the algebraic decoder corrects this error.

Sometimes, while making the hard decision the unreliability of every symbol can be estimated. Then the matrix of unreliabilities Z can be used for decoding together with the matrix Y. An element z_{ij} of the matrix Z shows the unreliability of the element y_{ij} of the matrix Y. We consider an idealized case where the matrix Z consists of zeroes and ones only. The value $z_{ij} = 0$ shows that the decision about y_{ij} is correct. The value $z_{ij} = 1$ means that the decision about y_{ij} can be wrong. In this case, we assume that the symbol was *erased*, despite, in fact, some decision about the symbol having been made. In this case, we call the matrix E *rank erasure.* The decoder obtains the matrix Y and the matrix Z of reliabilities, and hence it knows the error free positions. The matrix E has zeros at these positions, known to the decoder. We say that such a matrix E is *agreed* with the matrix of unreliabilities Z.

The *rank of erasure* is the rank of the matrix E. Consider *all* the matrices E agreed with the matrix Z. Let $r_{\max}(Z)$ denote the maximum possible rank of the matrix E. Obviously, a code with rank distance d corrects rank erasure E agreed with the matrix Z if $r_{\max}(Z) \le d-1$.

To estimate $r_{\max}(Z)$ it is convenient to use the concept of the term rank of a matrix from combinatorics.

The *term rank* of a matrix A, denoted by $\operatorname{termrank}(A)$, is the maximum number t of nonzero elements in the matrix such that no two of them belong to one line (row or column).

Lemma 5.7. *The term rank of a* $(0,1)$*-matrix* Z *is the minimum number* t *of lines (rows and columns) that contain all nonzero elements of the matrix* Z.

Using this lemma we obtain

Lemma 5.8. $r_{\max(Z)} = \mathrm{termrank}(Z)$.

Proof. We have $\mathrm{rank}(E) \le \mathrm{termrank}(E)$. For any matrix E, agreed with the matrix Z, it holds that $\mathrm{termrank}(E) \le \mathrm{termrank}(Z)$. Hence, on the one hand it follows that

$$r_{\max}(Z) \le \mathrm{termrank}(Z).$$

On the other hand, let $\mathrm{termrank}(Z) = t$. Then there are t positions with nonzero elements in Z such that no two of them belong to one line. Take a matrix E agreed with Z that has nonzero elements at these positions and zeros elsewhere. The rank of E is t, hence

$$r_{\max}(Z) \ge \mathrm{termrank}(Z)$$

and the statement of the lemma follows. ■

Consider erasure correction using the code $\mathcal{V}_1$, defined by (5.21) and (5.22).

Denote $[j] = q^j$ if $j \ge 0$ and $[j] = q^{n+j}$ if $j < 0$. The expression $g^{[j]} = g^{q^j}$ is called j-th Frobenius power of the element g. In particular, $g^{[n]} = g^{q^n} = g$. Frobenius power of a vector is computed componentwise.

For decoding we will use the following check matrix $\mathbf{H}_{n-1} = (h_j^{[i]})$, $i = 0, 1, \ldots, n-2$, $j = 1, 2, \ldots, n$, such that $\mathbf{g}_0 \mathbf{H}_{n-1}^T = \mathbf{0}$.

Let $\mathbf{y} = \alpha^s \mathbf{G} + \mathbf{e}$ be the received signal in vector form where $\mathbf{e} = (e_1, e_2, \ldots, e_n)$ denotes the vector form of the rank erasure E. Calculation of the syndrome gives the system of $n-1$ equations over the field $\mathbb{F}_{q^n}$:

$$\sum_{j=1}^{n} e_j h_j^{[i]} = s_i, \;\; i = 0, 1, \ldots, n-2.$$

Since the positions of possible errors in the matrix E are known, the system can be rewritten as a system with $n(n-1)$ linear equations over the base field, considering possible errors as unknowns. The number of unknowns depends on the configuration of the matrix E. If the rank of erasure is $n-1$ and errors are in $n-1$ rows or in $n-1$ columns, then the number of unknowns is maximal and equals $n(n-1)$. In this case the complexity to obtain a solution is maximal. If the rank of erasure is $n-1$ and errors are in $\lfloor n/2 \rfloor$ rows and in $\lfloor (n-1)/2 \rfloor$ columns, then the number of unknowns s is $s = n(n-1) - \lfloor n/2 \rfloor \lfloor (n-1)/2 \rfloor$, i.e., it is decreased by approximately a quarter. Thus, the syndrome decoding of erasures can be reduced to solving a system of $n(n-1)$ linear equations with $n(n-1)$ unknowns at most. The complexity decreases with decreasing the number of unknowns.

In the case of symmetric rank codes, the number of unknowns can be substantially decreased using a trick that we call *symmetrization* of rank erasures

Let $Y = M + E$ be a received signal in matrix form and E be a rank erasure. Additional information about errors can be obtained by computing the matrix $Q = Y + Y^T = M + M^T + E + E^T$. Since for symmetric codes $M = M^T$, $M \in \mathcal{M}$, we have for fields of *characteristic* 2: $M + M^T = O_n$, therefore we know

$$Q = Y + Y^T = E + E^T.$$

The matrix of unreliabilities Z shows the positions of zeroes in the matrix E. This allows us, during analysis of the matrix $E + E^T$, to obtain part of the errors directly and obtain additional information for another part.

Let us show the possible situations by the following example.

Example 5. Let $n = 4$, $d = 4$ and let the matrix of unreliabilities be

$$Z = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

This means that the matrix of errors is

$$E = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_5 & a_6 & a_7 & a_8 \\ 0 & 0 & 0 & a_9 \\ 0 & 0 & 0 & a_{10} \end{pmatrix},$$

and it has the rank $d - 1 = 3$ at most. In total, the matrix has *ten* binary unknowns a_i at known positions. Then we have

$$Q = E + E^T = \begin{pmatrix} 0 & a_2 + a_5 & a_3 & a_4 \\ a_5 + a_2 & 0 & a_7 & a_8 \\ a_3 & a_7 & 0 & a_9 \\ a_4 & a_8 & a_9 & 0 \end{pmatrix}.$$

From this matrix, we immediately obtain the error values a_3, a_4, a_7, a_8, a_9. We also know the sum $a_2 + a_5 = b$. However, the matrix Q has no information about "diagonal" errors a_1, a_6, a_{10}.

Let us modify the received matrix Y by adding the upper triangular known matrix

$$R = \begin{pmatrix} 0 & b & a_3 & a_4 \\ 0 & 0 & a_7 & a_8 \\ 0 & 0 & 0 & a_9 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

We obtain

$$Y_{\text{mod}} = Y + R = M + E + R = M + E_{\text{mod}},$$

where

$$E_{\text{mod}} = \begin{pmatrix} a_1 & a_5 & 0 & 0 \\ a_5 & a_6 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a_{10} \end{pmatrix}$$

is a *symmetric* error matrix, which has only *four* unknown error values at known positions. We call this procedure *symmetrization* of erasures.

The matrix Y_{mod} can be decoded using the syndrome correction of erasures. The preliminary symmetrization decreased the number of unknowns from 10 to 4.

Remark. In the class of codes under consideration, any line (row or column) of a code matrix is an information set. If for every known line we *precompute* the rest of the code matrix, then the decoding can be simplified when one of lines in the received matrix is error free. In Example 5, after symmetrization we have the error matrix that has zero lines (the third row or column), hence the syndrome decoding can be avoided.

In the general case, the symmetrization decreases the number of unknowns by at least half. For the case where erasure rank is $d - 1 = n - 1$ and all errors are in $n - 1$ rows, the symmetrization decreases the number of unknowns to $n(n-1)/2$ in comparison with $n(n-1)$ without symmetrization.

Let $n = 2s + 1$. If the erasure rank is $n - 1$ and the errors are in the first s rows and the last s columns then after the symmetrization the number of unknowns decreases from $\frac{(3n^2-2n-1)}{4}$ to $\frac{(n^2-1)}{4}$, i.e., making it approximately three times smaller.

5.6 Codes with subcodes of symmetric matrices

Consider the $\mathbb{F}_{q^n}$-linear rank $(n, k, d = n - k + 1)$ MRD code $\mathcal{V}_k$ with the generator matrix

$$\mathbf{G}_k = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_n^{[1]} \\ \cdot & \cdot & \cdots & \cdot \\ g_1^{[k-1]} & g_2^{[k-1]} & \cdots & g_n^{[k-1]} \end{pmatrix}. \tag{5.24}$$

As the first row of this matrix we take the vector $\mathbf{g}_0$ from (5.22).

A code $\mathcal{V}_k$ *is based on symmetric matrices* if it contains a one-dimensional subcode $\mathcal{V}_1$ of symmetric matrices.

Let the transposed code $\mathcal{V}_k^T$ be obtained using the transforms Θ and Θ^{-1} defined by (5.3) and (5.4). We will show that the code $\mathcal{V}_k^T$ is also $\mathbb{F}_{q^n}$-linear and it is based on symmetric matrices. Moreover, the joint use of codes $\mathcal{V}_k$ and $\mathcal{V}_k^T$ allows us to correct *symmetric* errors (erasures) beyond the bound $\lfloor (d-1)/2 \rfloor$ ($d-1$ respectively).

Auxiliary results. Denote by

$$\mathbf{g}_i = (g_1^{[i]}, g_2^{[i]}, \ldots, g_n^{[i]}),\ i = 0, 1, 2, \ldots, n-1,$$

the vectors obtained by Frobenius powers of the vector $\mathbf{g}_0 = (g_1, g_2, \ldots, g_n)$. These vectors are linearly independent over $\mathbb{F}_q$.

The components of every vector $\mathbf{g}_i$ form a basis of the field $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Hence, there exists a nonsingular matrix $D \in M_n(\mathbb{F}_q)$ such that $\mathbf{g}_1 = \mathbf{g}_0 D$. From here it follows that $\mathbf{g}_i = \mathbf{g}_0 D^i$. Besides, $D^i \neq I_n$ if $i \leq n-1$, but $D^n = I_n$, since $\mathbf{g}_n = \mathbf{g}_0 D^n = (g_1^{[n]}, g_2^{[n]}, \ldots, g_n^{[n]}) = (g_1, g_2, \ldots, g_n) = \mathbf{g}_0$. In matrix form, the vectors $\mathbf{g}_i$ are as follows

$$G_i = \Theta^{-1}(\mathbf{g}_i) = D^i. \tag{5.25}$$

Recall that A is a symmetric matrix representing the field.

Lemma 5.9. *The following relations hold*

$$\mathbf{g}_0 A = \alpha \mathbf{g}_0, \tag{5.26}$$

$$\mathbf{g}_1 A = \alpha^q \mathbf{g}_1, \tag{5.27}$$

$$DA = A^q D, \tag{5.28}$$

$$D^r A^s = A^{sq^r} D^r,\ r = 0, 1, \ldots, n-1,\ s = 0, 1, \ldots, q^n - 2. \tag{5.29}$$

Proof. To prove (5.26) we apply to its both parts the transform Θ^{-1}: $\Theta^{-1}(\mathbf{g}_0 A) = \Theta^{-1}(\mathbf{g}_0)A = I_n A = A$. On the other hand according to (5.5) we obtain $\Theta^{-1}(\alpha\mathbf{g}_0) = A\Theta^{-1}(\mathbf{g}_0) = AI_n = A$.

The relation (5.27) follows from (5.26) if we raise both parts of (5.26) to the first Frobenius power and take into account that $A \in M_n(\mathbb{F}_q)$. We obtain (5.28) if we apply the transform Θ to both parts of (5.27).

The relation (5.29) follows from (5.28) if we separate factors DA in the left part of (5.29) and use (5.28). ■

Lemma 5.10. *The matrices D and D^T are connected by the relation*

$$D^T = A^m D^{n-1}, \tag{5.30}$$

where m is an integer.

Proof. Transpose matrices in (5.28) and take into account that A is a symmetric matrix, then we obtain $D^T A^q = AD^T$. Left multiply both parts of (5.28) by the matrix D^T and obtain $D^T DA = D^T A^q D = AD^T D$. It follows from here that the matrix $D^T D$ commutes with the matrix A. Since all eigenvalues of the matrix A (in some field extension) are different, the matrix $D^T D$ can only be a polynomial in A and hence it is a power m of A [Gan67]. ■

Matrix form of the code $\mathcal{V}_k$. A generator matrix of the code $\mathcal{V}_k$ consists of the first k vectors $\mathbf{g}_j$, $j = 0, 1, \ldots, k-1$. Write components of an information vector $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1})$ as powers of α, i.e., $\mathbf{u} = (\varepsilon_0\alpha^{s_0}, \varepsilon_1\alpha^{s_1}, \ldots, \varepsilon_{k-1}\alpha^{s_{k-1}})$. Here the coefficients ε_j equal zero if $u_j = 0$ and equal 1 if $u_j \neq 0$. Then the code vector corresponding to the information vector $\mathbf{u}$ is

$$\mathbf{g}(\mathbf{u}) = \sum_{j=0}^{k-1} \varepsilon_j \alpha^{s_j} \mathbf{g}_j.$$

Let us convert this vector to the matrix $M(\mathbf{u})$ using (5.5) and (5.25):

$$M(\mathbf{u}) = \Theta^{-1}(\mathbf{g}(\mathbf{u})) = \sum_{j=0}^{k-1} \varepsilon_j A^{s_j} D^j. \tag{5.31}$$

The set of matrices $\mathcal{M} = \{M(\mathbf{u})\}$ from (5.31) for the all possible information vectors $\mathbf{u}$ define the code $\mathcal{V}_k$ in matrix form.

Matrix and vector forms of the transposed code. Let us obtain the transposed matrix code $\mathcal{M}^T = \left\{M(\mathbf{u})^T\right\}$:

$$M(\mathbf{u})^T = \sum_{j=0}^{k-1} \varepsilon_j (D^j)^T A^{s_j}.$$

Using (5.30) and (5.29) and changing the order of summation we obtain

$$M(\mathbf{u})^T = \sum_{i=n-k+1}^{n} \varepsilon_{n-i} A^{m_i} D^i,$$

where

$$m_i = s_{n-i} q^i + m(q^{i+1} + q^{i+2} + \cdots + q^n),$$
$$i = n-k+1, n-k+2, \ldots, n-1,\ m_n = s_0 q^n.$$

Let us obtain the transposed code in vector form using the transform Θ:

$$\widetilde{\mathbf{g}}(\mathbf{u}) = \Theta(M(\mathbf{u})^T) = \sum_{i=n-k+1}^{n} \Theta(\varepsilon_{n-i} A^{m_i} D^i) = \sum_{i=n-k+1}^{n} \varepsilon_{n-i} \alpha^{m_i} \mathbf{g}_i. \qquad (5.32)$$

The vector (5.32) can be considered as a code vector of the $\mathbb{F}_{q^n}$-linear [n,k,d=n-k+1] MRD code $\mathcal{V}_k^T$ with the generator matrix

$$\widetilde{\mathbf{G}}_k = \begin{pmatrix} g_1^{[n-k+1]} & g_2^{[n-k+1]} & \cdots & g_n^{[n-k+1]} \\ g_1^{[n-k+2]} & g_2^{[n-k+2]} & \cdots & g_n^{[n-k+2]} \\ . & . & \cdots & . \\ g_1^{[n]} & g_2^{[n]} & \cdots & g_n^{[n]} \end{pmatrix}$$

and with the information vector $\widetilde{\mathbf{u}} = (\varepsilon_{k-1}\alpha^{m_0}, \varepsilon_{k-2}\alpha^{m_1}, \ldots, \varepsilon_0 \alpha^{m_{k-1}})$. This code contains one dimensional subcode $\mathcal{V}_1$ defined by the last row of $\widetilde{\mathbf{G}}_k$ and consisting of symmetric matrices.

Thus, we have proved that the transposed code $\mathcal{V}_k^T$ is also $\mathbb{F}_{\mathrm{q}^{\mathrm{n}}}$-linear and it is based on symmetric matrices.

Joint decoding using both $\mathcal{V}_k$ and $\mathcal{V}_k^T$. Let a check matrix of the code

$\mathcal{V}_k$ be written as follows

$$\mathbf{H}_{n-k} = \begin{bmatrix} h_1 & h_2 & \cdots & h_n \\ h_1^{[1]} & h_2^{[1]} & \cdots & h_n^{[1]} \\ h_1^{[2]} & h_2^{[2]} & \cdots & h_n^{[2]} \\ \cdot & \cdot & \cdots & \cdot \\ h_1^{[d-2]} & h_2^{[d-2]} & \cdots & h_n^{[d-2]} \end{bmatrix}. \tag{5.33}$$

It can be shown that a check matrix of the code $\mathcal{V}_k^T$ can be written as follows

$$\widetilde{\mathbf{H}}_{n-k} = \begin{bmatrix} h_1^{[d]} & h_2^{[d]} & \cdots & h_n^{[d]} \\ h_1^{[d+1]} & h_2^{[d+1]} & \cdots & h_n^{[d+1]} \\ h_1^{[d+2]} & h_2^{[d+2]} & \cdots & h_n^{[d+2]} \\ \cdot & \cdot & \cdots & \cdot \\ h_1^{[2d-2]} & h_2^{[2d-2]} & \cdots & h_n^{[2d-2]} \end{bmatrix}. \tag{5.34}$$

First, consider *correction of rank errors.* Let $\mathbf{y} = \mathbf{g}(\mathbf{u}) + \mathbf{e}$ be a received signal in vector form, where $\mathbf{e} = (e_1, e_2, \dots, e_n)$ is the error in vector form. Let E be the same error in matrix form.

For the transposed code we have $\widetilde{\mathbf{y}} = \widetilde{\mathbf{g}}(\widetilde{\mathbf{u}}) + \widetilde{\mathbf{e}}$, where $\widetilde{\mathbf{e}} = (\widetilde{e}_1, \widetilde{e}_2, \dots, \widetilde{e}_n)$ is the error vector, the matrix form of which is $\widetilde{E} = E^T$. For decoding we compute two syndromes $\mathbf{r} = \mathbf{y}\mathbf{H}_{n-k}^T = \mathbf{e}\mathbf{H}_{n-k}^T$ and $\widetilde{\mathbf{r}} = \widetilde{\mathbf{y}}\,\widetilde{\mathbf{H}}_{n-k}^T = \widetilde{\mathbf{e}}\,\widetilde{\mathbf{H}}_{n-k}^T$. Using both syndromes does not give any advantage in comparison with standard decoding methods in general. One of these syndromes is sufficient for decoding. If the rank of an error is at most $t = (d-1)/2$ then it will be corrected using the syndrome $\mathbf{r}$.

However, to correct errors of a special class, it can be useful to use both syndromes. One class of such errors is the class of *symmetric errors*, i.e., errors having symmetric matrix: $E = \widetilde{E} = E^T$, or equivalently $\mathbf{e} = \widetilde{\mathbf{e}}$. In this case, one can use the joint syndrome

$$\mathbf{R} = (\mathbf{r}, \widetilde{\mathbf{r}}) = (\mathbf{e}\mathbf{H}_{n-k}^T, \widetilde{\mathbf{e}}\,\widetilde{\mathbf{H}}_{n-k}^T) = (\mathbf{e}\mathbf{H}_{n-k}^T, \mathbf{e}\,\widetilde{\mathbf{H}}_{n-k}^T).$$

The syndrome $\mathbf{R}$ can be considered as the syndrome of the code that has a check matrix consisting of *different* rows of *both* matrices (5.33) and (5.34). Depending on the code rate, there are two cases:

1. Let $2d - 2 < n$, i.e., $R = k/n > 1/2$. Then all rows of both matrices are different. The corresponding code can have a distance up to $D = 2d - 1$, hence, symmetric errors of rank up to $(D - 1)/2 = d - 1$ can be corrected using the syndrome $\mathbf{R}$.

2. Let $2d - 2 \geq n$, i.e., $R = k/n \leq 1/2$. Then the number of different rows in both matrices is $n - 1$. The corresponding code has the distance $D = n$, and symmetric errors of rank up to $(n - 1)/2$ can be corrected using the syndrome $\mathbf{R}$.

Similar results hold for *correction of symmetric rank erasures*. If $R = k/n > 1/2$ then for some codes, symmetric erasures of rank up to $D - 1 = 2d - 2$ can be corrected using the syndrome $\mathbf{R}$. If $R = k/n \leq 1/2$ then symmetric erasures of rank up to $n - 1$ can be corrected using the syndrome $\mathbf{R}$.

5.7 Conclusions

We have shown that finite fields of characteristic 2 can be defined by symmetric matrices, and we have presented a matrix code with maximum possible distance and volume.

6

Rank metric codes in network coding

6.1 Principles of network coding

Network coding is a relatively new research field. It is based on modification of information flow in a ordinary network. Formally, *a communication network* can be described as a *finite* directed graph, where vertices (nodes) can be connected by more than one edge. A vertex without input edges is called a *source node.*

Consider the following model. A communication network consists of vertices connected by communication channels (lines). Information is transmitted over each channel without distortions with a rate up to the channel capacity. Data from a source vertex should be transmitted to a set of fixed *destination nodes.* The natural question is: Given the restrictions above on the communication channels, can this problem be solved and how can it be done efficiently?

Existing computer networks transmit messages (packets) from a source to destinations using a number of intermediate nodes working on the principle "receive and forward". An intermediate node receives a packet from an input line, stores it in a buffer, and then sends copies of the packet via output lines that can deliver the packet to destinations possibly using other intermediate nodes. No other processing of packets at intermediate nodes is assumed. The optimal routing problem should be solved for this traditional approach. A simple model of a traditional network consists of one source, one destination, and a number of intermediate nodes.

The concept “network coding” was introduced in 2000 [ANLY00]. The authors consider packets as vectors over finite fields and assume that intermediate nodes can compute linear combinations of received packets. In the new model, an intermediate node is responsible for the following operations:

- receive packets;
- store them in a buffer;
- compute linear combinations of received packets;
- send the linear combinations to a next node.

Transmission of linear combinations of packets makes it possible to increase the network capacity: the maximum number of packets that can be transmitted to a destination per time unit. In the case of multiple destinations, the transmission time is the minimum time until *all* the destinations have received *all* the transmitted packets. The authors of [ANLY00] were the first to show by an example that network coding can increase the capacity of a network.

The possibility of increasing network capacity aroused considerable interest among researchers. In a number of publications, linear combinations of packets were considered with both random and deterministic coefficients. It was shown that the problems of network coding intersect with problems of error correcting codes and with general information theory. The first publications assumed that network coding should depend on the known topology of a network. This was not convenient for both theory and practice.

A new approach based on the subspace metric was suggested in 2007 by Kötter and Kschischang [KK08]. Soon after this, Silva, a PhD student of Kschischang,joined the research team. In their research, Silva, Kötter, and Kschischang [SKK08] considered linear combinations of packets with random coefficients. Such network coding was called *random network coding*. Later it was also called *non-coherent* coding. Network coding with known coefficients was called *non-coherent*. Silva, Kötter, and Kschischang show that problems of subspace coding can be reduced to problems of algebraic coding, such as designing codes in a given metric, obtaining bounds for optimal codes, constructing coding and decoding algorithms. They used Gabidulin rank metric codes for error correction in networks.

6.2 Spaces and subspaces

Before we describe subspace network codes let us recall main definitions connected with spaces and subspaces [Sag10].

6.2.1 Linear vector spaces

A *linear vector space* over the finite field $\mathbb{F}_q$ is a set of vectors V that satisfies the following conditions.

- The set V is an abelian additive group.
- For any $\gamma \in \mathbb{F}_q$ and $v \in V$ it holds that $\gamma v \in V$.
- Axioms of distributivity are satisfied: if $\gamma \in \mathbb{F}_q$ and $v, u \in V$, then $\gamma(u+v) = \gamma u + \gamma v$; if $\gamma, \lambda \in \mathbb{F}_q$ and $v \in V$, then $(\gamma + \lambda)v = \gamma v + \lambda v$.
- Associativity of multiplication: $(\gamma\lambda)v = \gamma(\lambda v)$.

Elements $\gamma, \lambda \in \mathbb{F}_q$ are called *scalars*.

The maximum number of linearly independent vectors of a space is called its *dimension*, and a set of such vectors is called a *basis* of the space.

A subset of a space is called a *subspace* if this subset satisfies the conditions of a space.

Denote by $W_{N,q}$ a fixed N-dimensional vector space over the finite field $\mathbb{F}_q$ and by $\mathcal{P}(W_{N,q})$ denote the set of all subspaces in $W_{N,q}$.

The dimension of an element $V \in \mathcal{P}(W_{N,q})$ is denoted by $\dim(V)$. There are subspaces of dimensions $0, 1, \dots, N$. The subspace O of dimension 0 consists of a single all zero N-vector. An m-dimensional subspace V consists of q^m vectors of length N over the field $\mathbb{F}_q$. It can be viewed as a row space of an $n \times N$ matrix $M(V)$ of rank m over $\mathbb{F}_q$, where $n \geq m$. The matrix $M(V)$ is called a *generator* matrix of m-dimensional subspace V and it is not unique. Let T be a nonsingular square matrix of order n over the field $\mathbb{F}_q$, then the row space of the matrix $TM(V)$ coincides with the subspace V. Hence, the matrix $TM(V)$ is a generator matrix of the subspace V as well. Obviously, the dimension of the subspace and the rank of a generator matrix are equal, i.e., $\dim(V) = \mathrm{Rk}(M(V))$, where $\mathrm{Rk}(A)$ denotes the rank of matrix A. If $n = m$, then the matrix $M(V)$ is called a *basic generator* matrix.

6.2.2 Subspace metric

Let us define two operations on the set $\mathcal{P}(W_{N,q})$.

The *sum* of two subspaces $U, V \in \mathcal{P}(W_{N,q})$ is defined as a unique subspace $C \in \mathcal{P}(W_{N,q})$ of *minimum* dimension containing both subspaces U and V. The sum is denoted by $C = U \uplus V$. If U and V are given by their generator matrices $M(U)$ and $M(V)$, then the subspace $C = U \uplus V$ coincides with the row space of the following block matrix

$$M(C) = \begin{bmatrix} M(U) \\ M(V) \end{bmatrix}.$$

The dimension $\dim(C)$ of the sum can be computed as rank of the block matrix

$$\dim(C) = \mathrm{Rk}(M(C)) = \mathrm{Rk}\left(\begin{bmatrix} M(U) \\ M(V) \end{bmatrix}\right).$$

The *product* also called the *intersection* of two subspaces $U, V \in \mathcal{P}(W_{N,q})$ is defined as a unique subspace $C \in \mathcal{P}(W_{N,q})$ of *maximum* dimension that is contained simultaneously in both subspaces U and V. The product is denoted by $C = U \cap V$.

Kötter and Kschischang [KK08] use the following metric on the set $\mathcal{P}(W_{N,q})$. The *subspace distance* between subspaces U and V is defined as

$$d(U, V) = \dim(U \uplus V) - \dim(U \cap V). \tag{6.1}$$

Since $\dim(U \uplus V) = \dim(U) + \dim(V) - \dim(U \cap V)$, the following equalities hold

$$\begin{aligned} d(U, V) &= \dim(U) + \dim(V) - 2\dim(U \cap V), \\ d(U, V) &= 2\dim(U \uplus V) - \dim(U) - \dim(V). \end{aligned} \tag{6.2}$$

If $M(U)$ and $M(V)$ are generator matrices of subspaces U and V, then

$$\begin{aligned} d(U, V) &= \mathrm{Rk}(M(U)) + \mathrm{Rk}(M(V)) - 2\dim(U \cap V), \\ d(U, V) &= 2\mathrm{Rk}\left(\begin{bmatrix} M(U) \\ M(V) \end{bmatrix}\right) - \mathrm{Rk}(M(U)) - \mathrm{Rk}(M(V)). \end{aligned} \tag{6.3}$$

The function of distance has values $\{0, 1, 2, \ldots, N\}$.

It should be noted that implicitly this metric can be obtained from the papers of Delsarte [Del76], [Del78], or from Ceccherini [Cec84], and also from the paper by Barg and Nogin [BN06], however, these papers do not mention communication networks.

Notice that the subspace distance is not invariant with respect to the sum of subspaces. For example, the distance between O and $W_{N,q}$ is $d(O, W_{N,q}) = N$. Let $Z \in \mathcal{P}(W_{N,q})$ be a subspace of a positive dimension. Add it to O and to $W_{N,q}$. We get $O \uplus Z = Z$, $W_{N,q} \uplus Z = W_{N,q}$. Hence, $d(O \uplus Z, W_{N,q} \uplus Z) = d(Z, W_{N,q}) = N - \dim(Z) < d(O, W_{N,q}) = N$. In the general case

$$d(U, V) \geq d(U \uplus Z, V \uplus Z).$$

6.2.3 Grassmannian

The set of all l-dimensional sub-spaces of N-dimensional vector space $\mathcal{P}(W_{N,q})$ over the field $\mathbb{F}_q$ is called the *Grassmannian* $G_l(N, q)$. The cardinality of a Grassmannian is given by *Gaussian binomial coefficients* $\left[{N \atop l} \right]_q$ defined for $l = 0, 1, \ldots, N$ as follows

$$\begin{bmatrix} N \\ l \end{bmatrix}_q = \begin{cases} 1, & \text{if } l = 0; \\ \frac{(q^N-1)(q^N-q)\cdots(q^N-q^{l-1})}{(q^l-1)(q^l-q)\cdots(q^l-q^{l-1})}, & \text{if } 1 \leq l \leq N. \end{cases} \tag{6.4}$$

The Gaussian binomial coefficients satisfy

$$\begin{aligned} \begin{bmatrix} N \\ l \end{bmatrix}_q &= \begin{bmatrix} N \\ N-l \end{bmatrix}_q, \ l = 0, \ldots, N; \\ \begin{bmatrix} N \\ l \end{bmatrix}_q &= q^l \begin{bmatrix} N-1 \\ l \end{bmatrix}_q + \begin{bmatrix} N-1 \\ l-1 \end{bmatrix}_q; \\ \begin{bmatrix} N \\ 0 \end{bmatrix}_q &< \begin{bmatrix} N \\ 1 \end{bmatrix}_q < \cdots < \begin{bmatrix} N \\ \lfloor \frac{N}{2} \rfloor \end{bmatrix}_q. \end{aligned} \tag{6.5}$$

The cardinality of the Grassmannian $G_l(N, q)$ is given by the l-th Gaussian coefficient

$$|G_l(N, q)| = \begin{bmatrix} N \\ l \end{bmatrix}_q. \tag{6.6}$$

The space $\mathcal{P}(W_{N,q})$ can be written as

$$\mathcal{P}(W_{N,q}) = \bigcup_{l=0}^{N} G_l(N,q).$$

The cardinality of $\mathcal{P}(W_{N,q})$ is

$$L = |\mathcal{P}(W_{N,q})| = \sum_{l=0}^{N} \begin{bmatrix} N \\ l \end{bmatrix}_q . \tag{6.7}$$

6.3 Subspace codes

Let us consider the set $\mathcal{P}(W_{N,q})$ as a code alphabet or as a signal space.

A nonempty subset of $\mathcal{C} \subseteq \mathcal{P}(W_{N,q})$ is called a *code*. Code cardinality $|\mathcal{C}|$ is the number of elements (codewords), which is the number of subspaces in this case. The minimum distance of the code $\mathcal{C}$ is $d(\mathcal{C}) = \min\limits_{U,V \in \mathcal{C}: U \neq V} d(U,V)$. The maximum dimension of code elements is $l(\mathcal{C}) = \max \dim(V)$, $(V \in \mathcal{C})$, where $\dim V$ is dimension of the subspace V. The code rate is defined as $R = \frac{\log_q(|\mathcal{C}|)}{Nl(\mathcal{C})}$.

The main problem of coding theory for this metric is to design codes with a given distance. In [SKK08], some code classes for subspace metric are proposed, including codes with distance 2 (not optimal), and also code constructions that are similar to Reed-Solomon codes in rank metric. The two last constructions are essentially the same. In all these codes, every codeword (subspace) has the same dimension.

6.3.1 Kötter-Kschischang model

Consider a network with one source and one destination. The source should transmit n row vectors (packets) $X(1), \dots, X(n)$ of length $n+m$ over the field $\mathbb{F}_q$, and forms an $n \times (n+m)$ matrix $\mathbf{X}$ having these packets as rows. In the Kötter-Kschischang model, a message is a row space of the matrix $\mathbf{X}$. Hence, the matrix $\mathbf{X}$ is a generator matrix of the message subspace.

Each intermediate node in the network computes a random $\mathbb{F}_q$-linear combination of input packets, where every packet is considered as an element of the finite field $\mathbb{F}_{q^{n+m}}$, and sends the linear combination via an outgoing line. The destination node collects n_r received packets $Y(1), \ldots, Y(n_r)$ of length $n+m$ over $\mathbb{F}_q$ and make an $n_r \times (n+m)$ matrix $\mathbf{Y}$ using the packets as rows. The number n_r of received packets can differ from the number of transmitted packets n, n_r can be equal to n, or can be more or less than n.

The task is to recover transmitted packets $X(1), \ldots, X(n)$, i.e., to recover the matrix $\mathbf{X}$, using the received matrix $\mathbf{Y}$.

The channel can be described by the following equation

$$\mathbf{Y} = \mathbf{AX} + \mathbf{E}_{out}, \tag{6.8}$$

where $\mathbf{A}$ – $n_r \times n$ is the matrix over $\mathbb{F}_q$ that corresponds to all the linear combinations of packets computed at intermediate nodes. The relation (6.8) is a basic channel model for random network coding. In the general case, the matrix $\mathbf{A}$ creates *internal* distortions of the transmitted matrix $\mathbf{X}$ and $\mathbf{E}_{out}$ is an *outer* $n_r \times (n+m)$ matrix over $\mathbb{F}_q$ of errors. The rows of $\mathbf{E}_{out}$ disturb the rows of the matrix $\mathbf{AX}$. For example, such disturbances can be created by so called Byzantine intruders inside the network that create erroneous packets $z_1, \ldots, z_p$ of length $n+m$. These packets can be seen as rows of $l \times (n+m)$ matrix $\mathbf{Z}$, $l = p$, over $\mathbb{F}_q$. Then, on the way to the destination, these packets $z_1, \ldots, z_p$ undergo their linear transformations, which are described by an $n_r \times p$ matrix $\mathbf{B}$. The outer error matrix of rank p can be written as $\mathbf{E}_{out} = \mathbf{BZ}$. In wireless networks, the matrix $\mathbf{E}_{out}$ appears because of a source of noise outside the network. If the rank of the matrix is p, it can be written again as $\mathbf{BZ}$ like in the Byzantine model.

6.3.2 Lifting construction of network codes

Let us consider the construction of network codes by Silva, Kötter, and Kschischang (SKK codes) proposed in 2008 [SKK08].

Let $\mathcal{M}$ be a matrix code consisting of $n \times m$ matrices $\mathbf{M}$. A *lifting code* $\mathcal{X}$ is the set of generator matrices $\mathbf{X}$

$$\mathcal{X} = \left\{\mathbf{X} : \mathbf{X} = \begin{bmatrix}\mathbf{I}_n & \mathbf{M}\end{bmatrix}, \mathbf{M} \in \mathcal{M}\right\},$$

where $\mathbf{I}_n$ is the identity matrix of order n.

The authors of [SKK08] use a rank code in matrix form as $\mathcal{M}$.

6.3.3 Matrix rank codes in network coding

Since a matrix rank metric code is a component of a subspace lifting code, let us recall the main definitions. The *rank norm* of a matrix X is defined as $N_{\mathrm{Rk}} = \mathrm{Rk}(X)$, the *rank distance* between matrix X and Y of the same size is the rank of their difference $d_{\mathrm{Rk}}(X, Y) = \mathrm{Rk}(X - Y)$.

Denote by $\mathbb{F}_q$ the finite field consisting of q elements and by $\mathbb{F}_{q^m}$ denote its extension of order m. If α is a primitive element of $\mathbb{F}_{q^m}$, then every nonzero element β from $\mathbb{F}_{q^m}$ is a power of α, i.e., $\beta = \alpha^s$. For integers $r \neq s$ there exists an integer k, such that $\alpha^r - \alpha^s = \alpha^k$. Let A be a nonsingular square matrix of order m over the base field $\mathbb{F}_q$, representing the field $\mathbb{F}_{q^m}$. This means that all matrices A^j, $j = 0, 1, \dots, q^m - 2$, are different and for integers $r \neq s$ there exists an integer k, such that $A^r - A^s = A^k$. A matrix A represents the field $\mathbb{F}_{q^m}$if and only if its characteristic polynomial has degree m and coincides with a monic primitive polynomial over the field $\mathbb{F}_q$.

For any matrix A representing the field $\mathbb{F}_{q^m}$ define the set $\mathcal{A}_1$ of $m \times m$ square matrices

$$\mathcal{A}_1 = \{O_m, I_m, A, A^2, \dots, A^{q^m-2}\}, \tag{6.9}$$

where O_m is the all-zero matrix and I_m is the identity matrix. This set will be used later to design some block matrices.

Simultaneously, the set $\mathcal{A}_1$ can be seen as a matrix code in *rank metric* with maximum possible code distance $d_{\mathrm{Rk}}(\mathcal{A}_1) = m$ and with cardinality $|\mathcal{A}_1| = q^m$.

Let $\mathcal{A}_1^{\mathrm{short}}$ be a punctured code obtained from $\mathcal{A}_1$ by puncturing $m - n$ rows and columns in every code matrix. The code $\mathcal{A}_1^{\mathrm{short}}$ is a punctured code of rectangular matrices of size $n \times m$ or $m \times n$, $n < m$, with a maximum distance $d_{\mathrm{Rk}} = n$ for a rank code of this size. The code cardinality is $\left|\mathcal{A}_1^{\mathrm{short}}\right| = q^m$.

In the general case, there exists a matrix D such that the set of matrices

$$\mathcal{A}_k = \left\{ \sum_{i=0}^{k-1} \varepsilon_i A^{s_i} D^i,\ \varepsilon_i \in \{0, 1\},\ 0 \le s_i \le q^m - 2 \right\} \tag{6.10}$$

is a code with rank distance $d_{\mathrm{Rk}}(\mathcal{A}_k) = m - k + 1$ and with cardinality $|\mathcal{A}_k| = q^{mk}$.

Let $\mathcal{A}_k^{\text{short}}$ be a shortened punctured code of rectangular matrices of size $n \times m$ or $m \times n$, $n < m$, obtained from $\mathcal{A}_k$ by puncturing $m - n$ rows and columns in every code matrix. The code $\mathcal{A}_k^{\text{short}}$ has cardinality $\left|\mathcal{A}_k^{\text{short}}\right| = q^{mk}$ and maximum rank code distance $d_{\text{Rk}} = n - k + 1$.

Assume that the source uses SKK code $\mathcal{X}$ and transmits the matrix

$$\mathbf{X} = \begin{bmatrix} \mathbf{I}_n & \mathbf{M} \end{bmatrix}.$$

Using the channel model (6.8), the destination node receives the matrix $\mathbf{Y}$

$$\mathbf{Y} = \mathbf{AX} + \mathbf{E}_{\text{out}}.$$

Let us write matrices $\mathbf{AX}$ and $\mathbf{E}_{\text{out}} = \mathbf{BZ}$ as

$$\begin{aligned} \mathbf{AX} &= \begin{bmatrix} \mathbf{A} & \mathbf{AM} \end{bmatrix}, \\ \mathbf{E}_{\text{out}} &= \begin{bmatrix} \mathbf{E}_1 & \mathbf{E}_2 \end{bmatrix}, \end{aligned}$$

where $\mathbf{E}_1$ and $\mathbf{E}_2$ are matrices of sizes $n_r \times n$ and $n_r \times m$ respectively. Then

$$\mathbf{Y} = \begin{bmatrix} \mathbf{A} + \mathbf{E}_1 & \mathbf{AM} + \mathbf{E}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{Y}_1 & \mathbf{Y}_2 \end{bmatrix}, \tag{6.11}$$

where

$$\mathbf{Y}_1 = \mathbf{A} + \mathbf{E}_1, \quad \mathbf{Y}_2 = \mathbf{AM} + \mathbf{E}_2, \tag{6.12}$$

We can assume that rank of matrices $\mathbf{B}$, $\mathbf{Z}$, and $\mathbf{BZ}$ is p.

Given the received matrix $\mathbf{Y}$ or equivalently $\mathbf{Y}_1$ and $\mathbf{Y}_2$, the task is to recover the matrix $\mathbf{M}$.

Since linearly dependent packets can be discarded by the receiver, later on we assume w.l.o.g. that the received matrix $\mathbf{Y}$ has full rank, i.e.,

$$Rk(\mathbf{Y}) = n_r. \tag{6.13}$$

Denote $Rk(\mathbf{Y}_1) = r \le \min\{n_r, n\}$ and recall that $Rk(\mathbf{E_{out}}) = p$.

6.3.4 Preliminary linear transformations

Using $\mathbf{A} = \mathbf{Y}_1 - \mathbf{E}_1$ rewrite (6.11) as

$$\mathbf{Y} = \begin{bmatrix} \mathbf{Y}_1 & \mathbf{Y}_1\mathbf{M} - \mathbf{E}_1\mathbf{M} + \mathbf{E}_2 \end{bmatrix}. \tag{6.14}$$

Let us apply Gaussian elimination to the matrix $\mathbf{Y}$ to obtain the reduced row echelon form of the matrix $\mathbf{Y}_1$. There exists a unique nonsingular $(n_r \times n_r)$ matrix $\mathbf{S}$ that transforms the matrix $\mathbf{Y}_1$ to the reduced row echelon form:

$$\mathbf{S}\mathbf{Y}_1 = \begin{bmatrix} \mathbf{G} \\ \mathbf{O} \end{bmatrix}, \tag{6.15}$$

where $\mathbf{G}$ is an $r \times n$ matrix with leading coefficients "1" in every row and $\mathbf{O}$ is $((n_r - r) \times n)$ all zero matrix. Left multiply both sides of (6.14) by the matrix $\mathbf{S}$:

$$\begin{aligned} \mathbf{SY} &= \begin{bmatrix} \mathbf{SY}_1 & \mathbf{SY}_1\mathbf{M} - \mathbf{SE}_1\mathbf{M} + \mathbf{SE}_2 \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{G} & \mathbf{GM} + \mathbf{S}_1(-\mathbf{E}_1\mathbf{M} + \mathbf{E}_2) \\ \mathbf{O} & \mathbf{S}_2(-\mathbf{E}_1\mathbf{M} + \mathbf{E}_2) \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{G} & \mathbf{R} \\ \mathbf{0} & \mathbf{C} \end{bmatrix} \end{aligned}, \tag{6.16}$$

where $\mathbf{S}_1$ and $\mathbf{S}_2$ are the upper and the lower blocks of the matrix $\mathbf{S}$ respectively:

$$\mathbf{S} = \begin{bmatrix} \mathbf{S}_1 \\ \mathbf{S}_2 \end{bmatrix}.$$

The matrix $\mathbf{S}_1$ consists of r first rows of the matrix $\mathbf{S}$. The matrix $\mathbf{S}_2$ consists of $(n_r - r)$ last rows of the matrix $\mathbf{S}$. After these transformations, the receiver knows the matrix $\mathbf{GM} + \mathbf{S}_1(-\mathbf{E}_1\mathbf{M} + \mathbf{E}_2)$ denoted by $\mathbf{R}$ and the matrix $\mathbf{S}_2(-\mathbf{E}_1\mathbf{M} + \mathbf{E}_2)$ denoted by $\mathbf{C}$. By (6.13) rank $\mathrm{Rk}(\mathbf{C}) = n_r - r$.

Lemma 6.1. *The following inequality holds*

$$n_r - r \le p. \tag{6.17}$$

Proof. We have

$$\begin{aligned} \mathrm{Rk}(\mathbf{C}) = n_r - r &= \mathrm{Rk}(\mathbf{S}_2(-\mathbf{E}_1\mathbf{M} + \mathbf{E}_2)) \\ &\le \min\{\mathrm{Rk}(\mathbf{S}_2), \mathrm{Rk}(-\mathbf{E}_1\mathbf{M} + \mathbf{E}_2)\}. \end{aligned}$$

From $\mathrm{Rk}(\mathbf{S}_2) = n_r - r$ it follows that

$$\mathrm{Rk}(\mathbf{S}_2) \le \mathrm{Rk}(-\mathbf{E}_1\mathbf{M} + \mathbf{E}_2) \le p.$$

■

Recall that we write

$$\mathbf{E}_{\text{out}} = \mathbf{B}\mathbf{Z}, \tag{6.18}$$

where $\mathbf{B}$ is an $n_r \times p$ matrix of rank p and a $\mathbf{Z}$ is $p \times (n+m)$ matrix of rank p. Such decomposition is not unique. Indeed, if $\mathbf{V}$ is an invertible square matrix of order p, then we have $\mathbf{E}_{\text{out}} = \widetilde{\mathbf{B}}\widetilde{\mathbf{Z}}$, where $\widetilde{\mathbf{B}} = \mathbf{B}\mathbf{V}$ and $\widetilde{\mathbf{Z}} = \mathbf{V}^{-1}\mathbf{Z}$.

Lemma 6.2. *There exist a decomposition (6.18) with a matrix $\mathbf{B} = \begin{bmatrix}\mathbf{B}_1 & \mathbf{B}_2\end{bmatrix}$, where $\mathbf{B}_1$ is the $n_r \times (n_r - r)$ submatrix of rank $n_r - r$, $\mathbf{B}_2$ is the $n_r \times (p - n_r + r)$ submatrix of rank $p - n_r + r$, such that the square matrix $\mathbf{T} = \mathbf{S}_2\mathbf{B}_1$ of order $n_r - r$ is invertible.*

Proof. Matrix $\mathbf{S}_2\mathbf{B}$ has size $(n_r - r) \times p$ and should have rank $n_r - r$. Otherwise the rank of matrix $\mathbf{C}$ would be less than $n_r - r$. Hence, there exist $n_r - r$ linearly independent columns $\mathbf{L} = \begin{bmatrix}\mathbf{b}_{j_1} & \mathbf{b}_{j_2} & \dots & \mathbf{b}_{j_{n_r - r}}\end{bmatrix}$ of the matrix $\mathbf{B}$ such that $\mathbf{S}_2\mathbf{L}$ is an invertible matrix. We can shift these columns to the first $n_r - r$ positions by selecting a proper matrix $\mathbf{V}$. Thus, $\mathbf{B}_1 = \mathbf{L}$ and $\mathbf{T} = \mathbf{S}_2\mathbf{B}_1$ is an invertible matrix. ■

We have also $\mathbf{E}_1 = \mathbf{B}\mathbf{Z}_1$, $\mathbf{E}_2 = \mathbf{B}\mathbf{Z}_2$, where $\mathbf{Z} = \begin{bmatrix}\mathbf{Z}_1 & \mathbf{Z}_2\end{bmatrix}$. Rewrite the matrix $(-\mathbf{E}_1\mathbf{M} + \mathbf{E}_2)$ as

$$\begin{aligned}
-\mathbf{E}_1\mathbf{M} + \mathbf{E}_2 &= \mathbf{B}(-\mathbf{Z}_1\mathbf{M} + \mathbf{Z}_2)\\
&= \begin{bmatrix}\mathbf{B}_1 & \mathbf{B}_2\end{bmatrix}\begin{bmatrix}\mathbf{W}_1\\ \mathbf{W}_2\end{bmatrix}\\
&= \mathbf{B}_1\mathbf{W}_1 + \mathbf{B}_2\mathbf{W}_2.\\
-\mathbf{Z}_1\mathbf{M} + \mathbf{Z}_2 &= \begin{bmatrix}\mathbf{W}_1\\ \mathbf{W}_2\end{bmatrix}.
\end{aligned}$$

Now (6.16) can be written as

$$\begin{aligned}
\mathbf{S}\mathbf{Y} &= \begin{bmatrix}\mathbf{G} & \mathbf{R}\\ \mathbf{0} & \mathbf{C}\end{bmatrix}\\
&= \begin{bmatrix}\mathbf{G} & \mathbf{G}\mathbf{M} + \mathbf{S}_1\mathbf{B}_1\mathbf{W}_1 + \mathbf{S}_1\mathbf{B}_2\mathbf{W}_2\\ \mathbf{O} & \mathbf{S}_2\mathbf{B}_1\mathbf{W}_1 + \mathbf{S}_2\mathbf{B}_2\mathbf{W}_2\end{bmatrix}\\
&= \begin{bmatrix}\mathbf{G} & \mathbf{G}\mathbf{M} + \mathbf{S}_1\mathbf{B}_1\mathbf{T}^{-1}\mathbf{T}\mathbf{W}_1 + \mathbf{S}_1\mathbf{B}_2\mathbf{W}_2\\ \mathbf{O} & \mathbf{T}\mathbf{W}_1 + \mathbf{S}_2\mathbf{B}_2\mathbf{W}_2\end{bmatrix}.
\end{aligned} \tag{6.19}$$

Since $\mathbf{T}\mathbf{W}_1 = \mathbf{C} - \mathbf{S}_2\mathbf{B}_2\mathbf{W}_2$, we get

$$\mathbf{R} = \mathbf{G}\mathbf{M} + \mathbf{S}_1(\mathbf{B}_1\mathbf{T}^{-1})\mathbf{C} - \mathbf{S}_1(\mathbf{B}_1\mathbf{T}^{-1}\mathbf{S}_2 - \mathbf{S}_1)\mathbf{B}_2\mathbf{W}_2. \tag{6.20}$$

The matrix $\mathbf{R}$ consists of r rows. If $r < n$ let us include all-zero rows to get n rows as follows. If the matrix G has a gap between two rows with leading "1"s, and the value of gap is a, then a allzero rows are inserted between these two rows. Let, for example, the leading element "1" be in the first column of the first row and in the 6-th column of the second row. The gap equals 4, and 4 all-zero rows are inserted between the first and the second rows. Denote this operation by "hat". Thus, e.g. matrix $\mathbf{R}$ after including all-zero rows is denoted by $\widehat{\mathbf{R}}$. We use the same notation for other matrices as well. We have

$$\widehat{\mathbf{R}} = \widehat{\mathbf{G}}\mathbf{M} + \widehat{\mathbf{S}}_1\mathbf{B}_1\mathbf{T}^{-1}\mathbf{C} - \widehat{\mathbf{S}}_1(\mathbf{B}_1\mathbf{T}^{-1}\mathbf{S}_2 - \mathbf{S}_1)\mathbf{B}_2\mathbf{W}_2. \tag{6.21}$$

Write $(n \times n)$ matrix $\widehat{\mathbf{G}}$ as

$$\widehat{\mathbf{G}} = \mathbf{I}_n + \mathbf{L},$$

where $\mathbf{L}$ has exactly $(n - r)$ nonzero columns. Denote $\mathbf{D} = \widehat{\mathbf{S}}_1\mathbf{B}_1\mathbf{T}^{-1}$ and $\mathbf{E}_{\text{rest}} = -\widehat{\mathbf{S}}_1(\mathbf{B}_1\mathbf{T}^{-1}\mathbf{S}_2 - \mathbf{S}_1)\mathbf{B}_2\mathbf{W}_2$. Rank of D is at most $\text{Rk}(\mathbf{B}_1) = (n_r - r)$. Rank of $\mathbf{E}_{\text{rest}}$ is at most $\text{Rk}(\mathbf{B}_2) = (p - n_r + r)$. We can write

$$\widehat{\mathbf{R}} = \mathbf{M} + \mathbf{L}\mathbf{M} + \mathbf{D}\mathbf{C} + \mathbf{E}_{\text{rest}}, \tag{6.22}$$

where

$$\text{Rk}(\mathbf{L}) \leq n - r, \tag{6.23}$$

$$\text{Rk}(\mathbf{C}) = n_r - r, \tag{6.24}$$

$$\text{Rk}(\mathbf{E}_{\text{rest}}) \leq p - n_r + r. \tag{6.25}$$

Thus, the decoding of SKK subspace codes is reduced to decoding rank codes with errors and generalized erasures.

6.4 Decoding of rank codes

6.4.1 When errors and generalized erasures will be corrected

Let us analyze (6.22). The item $\widehat{\mathbf{R}}$ can be considered as a received matrix of the rank code that consists of four items shown in the right part of the equation. The first item $\mathbf{M}$ is the transmitted matrix of the rank code. The second item $\mathbf{LM}$, where the matrix $\mathbf{L}$ is known, corresponds to a *generalized row erasure* of rank at most $n - r$. The third item $\mathbf{DC}$, where the matrix $\mathbf{C}$ is known, corresponds to a *generalized column erasure* of rank at most $n_r - r$ (since matrix D in product DC can have rank at most $n_r - r$). The fourth item $\mathbf{E}_{\text{rest}}$ corresponds to a random rank error of rank at most $p - n_r + r$.

The matrix $\mathbf{M}$ can be successfully recovered if the following condition is satisfied

$$(n - r) + (n_r - r) + 2(p - n_r + r) = 2p + n - n_r \leq d_r - 1. \tag{6.26}$$

Simultaneous correction of rank errors and some types of erasures of columns and rows was described in 1992 by Gabidulin, Paramonov and Tretjakov [GPT92], by Gabidulin and Pilipchuk [GP08] in 2008, and by Silva, Kschischang, and Kötter [SKK08] in 2008. In [GPT92] rank erasures of exactly v rows or l columns with known positions are described.

The results in [GP08] can be applied unchanged to correct generalized rank erasures of rows and columns. If the receiver knows the generalized erasures, then column erasures and then row erasures can be excluded. As a result, the length of the modified syndrome becomes $(d - 1 - v - l)$. If the modified syndrome is a nonzero vector then there are also rank random errors and they can be corrected using fast decoding algorithms if the rank t of the error satisfies $(2t \leq d - 1 - v - l)$. As it shown in [GP08], generalized erasures can be corrected after correction of random errors. In the example of Section 6.5 this decoding algorithm is shown in detail.

6.4.2 Possible variants of errors and erasures

Let us consider different scenarios arising during decoding. Parameters n, n_r, r as well as matrices $\mathbf{S}$, $\mathbf{S}_1$, $\mathbf{S}_2$, $\mathbf{L}$, $\mathbf{C}$ are known to the decoder after preliminary computations. Parameter p is not known but can be estimated during decoding.

To obtain conditions for parameters n, n_r, r, p, so that the receiver has different combinations of errors and erasures, let us analyze (6.22). There are three different events: random rank errors, generalized row erasures and generalized column erasures. These events can happen in different combinations: separately, or combinations of two events, or all three events together. In total, there are seven combinations of the events, which will be considered below.

Random error and generalized rank erasures of rows and columns

There are random errors if the rank of the matrix $\mathbf{E}_{\text{rest}}$ is greater than zero, i.e. $p - n_r + r > 0$, where p is the rank of the outer error $\mathbf{E}_{\text{out}}$, n_r is the number of rows in the received matrix $\mathbf{Y}_1$, r is the rank of its submatrix $\mathbf{Y}_1$. Row erasures occur if the rank of matrix $\mathbf{L}$ is greater than 0, i.e., when $n - r > 0$, where n is the number of rows in the transmitted matrix. Column erasures take place if the rank of the matrix $\mathbf{C}$ is greater than 0, i.e., when $n_r - r > 0$. Values of r, n, n_r are known to the decoder, parameter p can be lower bounded by $n_r - r \leq p$ using Lemma 6.1.

For this combination of events, any relations between n and n_r are possible: it can be that $n_r > n$, or $n_r < n$, or $n_r = n$. But in every case the rank p of the outer error $\mathbf{E}_{\text{out}}$ is greater than 0 and all the following conditions are satisfied simultaneously:

$$r < n, \quad r < n_r, \quad n_r - r < p. \tag{6.27}$$

Generalized erasures of rows and columns

We start the consideration of combinations of two events by analyzing the case of simultaneous erasures of rows and columns. Hence the first two conditions in (6.27) are satisfied and the third one is replaced by $p = n_r - r$. Indeed, it was shown that rank of the error matrix $\text{Rk}(\mathbf{E}_{\text{rest}}) = p - n_r + r$ For the rank equal to zero we get $p = n_r - r$. However, it should be $p = n_r - r > 0$ since when $p = n_r - r = 0$ there are no column erasures. Thus we get the relations

$$r < n, \quad r < n_r, \quad p = n_r - r > 0. \tag{6.28}$$

For this combinations of erasures any relations between n and n_r: $n_r > n$, or $n_r < n$, or $n_r = n$ are also possible. The rank p of outer-error-matrix $\mathbf{E}_{\text{out}}$ is equal to the rank of matrix $\mathbf{C}$, which describes column erasures, and is greater then zero.

Random rank errors and generalized row erasures

Random errors occur if $p > n_r - r$. Row erasures take place if $n - r > 0$. There are no column erasures if $n_r - r = 0$. Hence, we get the following relations

$$n_r < n, \quad n_r = r, \quad p > 0. \tag{6.29}$$

Thus, for this combination of errors and erasures, the number of rows of the transmitted matrix is larger than the number of rows of the received matrix, which is equal to rank of the submatrix $\mathbf{Y_1}$ of the matrix $\mathbf{Y}$. There is an outer matrix $\mathbf{E_{out}}$ with unknown rank $p > 0$.

Random rank errors and generalized column erasures

Random errors occur if $p > n_r - r$. Column erasures take place if $n_r - r > 0$. There are no row erasures if $n - r = 0$. Hence, we get the following relations

$$n = r < n_r, \quad n < n_r, \quad p > n_r - r > 0. \tag{6.30}$$

Thus, for this combination of errors and erasures, the number of rows of the transmitted matrix is less than the number of rows of the received matrix and is equal to the rank of the submatrix $\mathbf{Y}_1$. The number of rows in the received matrix is larger than the rank of $\mathbf{Y}_1$. The rank of the matrix $\mathbf{E}_{\text{out}}$ is larger than the difference between the number of rows in the received matrix and the rank of the matrix $\mathbf{Y}_1$.

Let us consider now single events.

Random rank errors

Random errors occur if $p > n_r - r$. There are no row erasures if $n - r = 0$. There are no column erasures if $n_r - r = 0$. It means that the relations between parameters are

$$r = n = n_r, \, p > 0. \tag{6.31}$$

The transmitted and the received matrices have the same number of rows that is equal to the rank of the matrix $\mathbf{Y}_1$. The rank of the outer error matrix $\mathbf{E}_{\text{out}}$ is strictly positive.

Generalized row erasures

In this case, there are no errors and no column erasures. There are no column erasures if $n_r - r = 0$. No errors if $p = n_r - r$, i.e., in this case rank of matrix of outer error $\mathbf{E}_{\text{out}}$ equals $p = 0$. Since there were row erasures, the relation $n - r > 0$ should be satisfied. Hence, we have the relations:

$$r < n, \, r = n_r, \, p = 0. \tag{6.32}$$

The transmitted matrix has more rows than the received matrix. The number of rows of the received matrix is equal to rank of the matrix $\mathbf{Y}_1$. The rank of the matrix of outer error $\mathbf{E}_{\text{out}}$ equals 0.

Generalized column erasures

In this case, there are no errors and no row erasures, but there are column erasures. There are no row erasures if $n - r = 0$. There are column erasures if $n_r - r > 0$. There are no errors if $p = n_r - r$. It means that the relations between parameters are:

$$r = n < n_r, \, p = n_r - r > 0. \tag{6.33}$$

The transmitted matrix has fewer rows than the received matrix.

The number of rows of the received matrix is more than the rank of matrix $\mathbf{Y}_1$. The rank p of the outer error matrix $\mathbf{E}_{\text{out}}$ is strictly positive.

The results of the above analysis are shown in the following table.

Table 6.1: Parameters for seven combinations of errors and erasures

1	Errors only	$n_r = n = r, \ p > 0$
2	Row erasures only	$r = n_r < n, \ p = 0$
3	Errors and row erasures	$r = n_r < n, \ p > 0$
4	Column erasures only	$r = n < n_r, \ p = n_r - r$
5	Errors and column erasures	$r = n < n_r, \ p > n_r - r$
6	Erasures of rows and columns	$n > r, n_r > r, \ p = n_r - r$
7	Errors and erasures of rows and columns	$n > r, n_r > r, \ p > n_r - r > 0$

6.5 An example

Let us give an example of simultaneous correction of errors and erasures of rows and columns.

6.5.1 Code, channel, received matrix

For $q = 2$ let us design a $(5, 1, d_r = 5)$ MRD code using nonreducible polynomial $f(\lambda) = \lambda^5 + \lambda^2 + 1$ with a primitive element α. We take the generator matrix

$\mathbf{G}_1 = (\alpha, \alpha^{30}, \alpha^{18}, \alpha^7, \alpha^{20})$ then a check matrix is

$$\mathbf{H}_4 = \begin{bmatrix} \alpha^2 & \alpha^{29} & \alpha^5 & \alpha^{14} & \alpha^9 \\ \alpha^4 & \alpha^{27} & \alpha^{10} & \alpha^{28} & \alpha^{18} \\ \alpha^8 & \alpha^{23} & \alpha^{20} & \alpha^{25} & \alpha^5 \\ \alpha^{16} & \alpha^{15} & \alpha^9 & \alpha^{19} & \alpha^{10} \end{bmatrix}. \tag{6.34}$$

Select code vector

$$\mathbf{v} = \begin{bmatrix} \alpha & \alpha^{30} & \alpha^{18} & \alpha^7 & \alpha^{20} \end{bmatrix}. \tag{6.35}$$

Using the table of powers of α we write the code vector in matrix form:

$$\mathbf{M} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \end{bmatrix}, \tag{6.36}$$

where $m_i,\ i = \overline{1,5}$ denote rows of the matrix. Using the lifting construction we obtain the matrix of subspace code to be transmitted:

$$\mathbf{X} = \begin{bmatrix} \mathbf{I}_5 & \mathbf{M} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \tag{6.37}$$

The channel from source to destination we describe by the matrices

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}, \mathbf{BZ}_1 = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}, \mathbf{BZ}_2 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

The received matrix is

$$\mathbf{Y} = \begin{bmatrix} \mathbf{Y}_1 & \mathbf{Y}_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

where

$$\mathbf{Y}_1 = \mathbf{A} + \mathbf{B}\mathbf{Z}_1 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}, \ \mathbf{Y}_2 = \mathbf{A}\mathbf{M} + \mathbf{B}\mathbf{Z}_2 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}. \tag{6.38}$$

The transmitted and the received matrices have the same number of rows: $n = n_r = 5$. In this example, all three types of errors occur.

6.5.2 Preliminary transformations

The matrix $\mathbf{S}$ of Gaussian eliminations that brings the matrix $\mathbf{Y}_1$ to the reduced echelon form and its blocks $\mathbf{S}_1, \ \mathbf{S}_2$ are

$$\mathbf{S} = \begin{bmatrix} \mathbf{S}_1 \\ \mathbf{S}_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix},$$

where

$$\mathbf{S}_1 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix}, \ \mathbf{S}_2 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

The reduced row echelon form is:

$$\mathbf{S}\mathbf{Y}_1 = \begin{bmatrix} \mathbf{G} \\ \mathbf{O} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

where

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \ \mathbf{O} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

hence, the parameter $r = \mathrm{Rk}(\mathbf{Y}_1) = \mathrm{Rk}(\mathbf{SY}_1) = \mathrm{Rk}(\mathbf{G}) = 4$. Next,

$$\mathbf{SY}_2 = \begin{bmatrix} \mathbf{R} \\ \mathbf{C} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}, \tag{6.39}$$

where

$$\mathbf{R} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \ \mathbf{C} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

For decoding we need to obtain the equation like (6.22). For this, we should add an all-zero row to the 4×5 matrix $\mathbf{G}$, to obtain a square matrix. Leading elements “1” in the matrix $\mathbf{G}$ are it positions $i_1 = 1,\ i_2 = 2,\ i_3 = 3,\ i_4 = 4$, hence, before rows $1 \dots 4$ we can not insert the all zero row. So, we insert $n - i_4 = 5 - 4 = 1$ all zero row after the last row and obtain:

$$\widehat{\mathbf{G}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Write $\widehat{\mathbf{G}} = \mathbf{I}_5 + \mathbf{L}$ and obtain

$$\mathbf{L} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{6.40}$$

Rank of the matrix $\mathbf{L}$ is 1.

Similarly, we obtain the matrix $\widehat{\mathbf{R}}$ by adding one all-zero row after the last row of the matrix $\mathbf{R}$:

$$\widehat{\mathbf{R}} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \tag{6.41}$$

For rank decoding we obtain the equation

$$\widehat{\mathbf{R}} = \mathbf{M} + \mathbf{LM} + \mathbf{DC} + \mathbf{E}_{\text{rest}} \tag{6.42}$$

wher $\widehat{\mathbf{R}}$, $\mathbf{L}$, $\mathbf{C}$ are defined by (6.42), (6.40), (6.39). Since the rank of the matrix $\mathbf{L}$ is 1, and rank of $\mathbf{C}$ is 1, it is necessary to correct single row and single column erasures.

6.5.3 Syndrome computation

Transform the matrix $\widehat{\mathbf{R}}$ to the vector $\mathbf{y}$:

$$\mathbf{y} = \begin{bmatrix}\alpha & \alpha^5 & \alpha^{12} & \alpha^{18} & \alpha^{29}\end{bmatrix}. \tag{6.43}$$

Compute the syndrome $\mathbf{s}$:

$$\mathbf{s} = \mathbf{y}\mathbf{H}_4^\top = \begin{bmatrix}s_0 & s_1 & s_2 & s_3\end{bmatrix} = \begin{bmatrix}\alpha^5 & \alpha^{28} & \alpha^3 & 0\end{bmatrix}. \tag{6.44}$$

Since the code distance is $d_r = n = 5$, the rank of row erasure is 1, and rank of column erasures is 1, we can correct an error of rank 1: $1 + 1 + 2 = d_r - 1$.

An error and its components we write in the vector form:

$$\mathbf{e} = (\mathbf{e}_{\text{rand}} + \mathbf{e}_{\text{row}} + \mathbf{e}_{\text{col}})$$

where $\mathbf{e}_{\text{rand}} = e_1\mathbf{u}_1$ is a random error of rank 1, e_1 is an element of the extension field $\mathbb{F}_{2^5}$, $\mathbf{u}_1 = [u_{11}\ u_{12}\ u_{13}\ u_{14}\ u_{15}]$ is a vector with 5 components from the base (binary in our case) field. The element e_1 and the vector $\mathbf{u}_1$ are unknown.

$\mathbf{e}_{\text{row}} = a\mathbf{r}_1$, where $a = \alpha^{30}$ is a known element of the field $\mathbb{F}_{2^5}$, defined by the matrix $\mathbf{L}$, $\mathbf{r}_1 = [r_{11}\ r_{12}\ r_{13}\ r_{14}\ r_{15}]$ is an unknown vector over the base field.

$\mathbf{e}_{\text{col}} = w_1\mathbf{C} = w_1[0\ 0\ 1\ 0\ 0]$, where w_1 is unknown element of the field $\mathbb{F}_{2^5}$.

Let us find the parts of the syndrome due to components of the error. The part of the syndrome due to the random error:

$$\mathbf{s}_{\text{rand}} = e_1\mathbf{u}_1\mathbf{H}_4^\top = e_1[x_1\ x_1^2\ x_1^4\ x_1^8], \tag{6.45}$$

where

$$x_1 = \alpha^2 u_{11} + \alpha^{29} u_{12} + \alpha^5 u_{13} + \alpha^{14} u_{14} + \alpha^9 u_{15}. \tag{6.46}$$

The part of the syndrome due to row erasures

$$\mathbf{s}_{\text{row}} = \alpha^{30}[r_{11}\ r_{12}\ r_{13}\ r_{14}\ r_{15}]\mathbf{H}_4^\top = \alpha^{30}[\theta_1\ \theta_1^2\ \theta_1^4\ \theta_1^8], \tag{6.47}$$

where

$$\theta_1 = \alpha^2 r_{11} + \alpha^{29} r_{12} + \alpha^5 r_{13} + \alpha^{14} r_{14} + \alpha^9 r_{15}. \tag{6.48}$$

Part of the syndrome due to column erasures

$$\mathbf{s}_{\text{col}} = w_1[0\ 0\ 1\ 0\ 0]\mathbf{H}_4^\top = w_1[\alpha^5\ \alpha^{10}\ \alpha^{20}\ \alpha^9] = w_1[\gamma_1\ \gamma_1^2\ \gamma_1^4\ \gamma_1^8], \tag{6.49}$$

where $\gamma_1 = \alpha^5$. By equating corresponding syndrome components we obtain the system of syndrome equations

$$\begin{array}{l} \alpha^5 = e_1 x_1 + \alpha^{30}\theta_1 + w_1\gamma_1; \\ \alpha^{28} = e_1 x_1^2 + \alpha^{30}\theta_1^2 + w_1\gamma_1^2; \\ \alpha^3 = e_1 x_1^4 + \alpha^{30}\theta_1^4 + w_1\gamma_1^4; \\ 0 = e_1 x_1^8 + \alpha^{30}\theta_1^8 + w_1\gamma_1^8. \end{array} \tag{6.50}$$

6.5.4 Exclusion of column erasures

Let us define a linearized polynomial $\Gamma(x) = \Gamma_0 x + \Gamma_1 x^2$ with roots γ_1 and 0. Consider the equation $\Gamma(\gamma_1) = \Gamma_0\gamma_1 + \Gamma_1\gamma_1^2 = 0$. Set $\Gamma_1 = 1$, and find $\Gamma_0 = \gamma_1 = \alpha^5$. Build the matrix

$$\mathbf{\Gamma} = \begin{bmatrix} \Gamma_0 & 0 & 0 \\ \Gamma_1 & \Gamma_0^2 & 0 \\ 0 & \Gamma_1^2 & \Gamma_0^4 \\ 0 & 0 & \Gamma_1^4 \end{bmatrix} = \begin{bmatrix} \alpha^5 & 0 & 0 \\ 1 & \alpha^{10} & 0 \\ 0 & 1 & \alpha^{20} \\ 0 & 0 & 1 \end{bmatrix}.$$

As the first modification we multiply the syndrome and its components by the matrix Γ

$$\widetilde{\mathbf{s}} = \mathbf{s}\mathbf{\Gamma} = [\alpha_{11}\ \alpha_{13}\ \alpha_{23}] = [\widetilde{s}_0\ \widetilde{s}_1\ \widetilde{s}_2], \tag{6.51}$$

$$\mathbf{s}_{\text{rand}}\mathbf{\Gamma} = e_1[\widetilde{x_1}\ \widetilde{x_1}^2\ \widetilde{x_1}^4], \tag{6.52}$$

where $\widetilde{x_1} = \Gamma(x_1)$.

$$\mathbf{s}_{\text{row}}\mathbf{\Gamma} = \alpha^{30}[\widetilde{\theta_1}\ \widetilde{\theta_1}^2\ \widetilde{\theta_1}^4], \tag{6.53}$$

where $\widetilde{\theta_1} = \Gamma(\theta_1)$.

$$\mathbf{s}_{\mathrm{col}}\mathbf{\Gamma} = [0\ 0\ 0]. \tag{6.54}$$

By equating components of the modified syndrome we obtain:

$$\begin{aligned} \widetilde{s}_0 &= \alpha^{11} = e_1\widetilde{x_1} + \alpha^{30}\widetilde{\theta_1}, \\ \widetilde{s}_1 &= \alpha^{13} = e_1\widetilde{x_1}^2 + \alpha^{30}\widetilde{\theta_1}^2, \\ \widetilde{s}_2 &= \alpha^{23} = e_1\widetilde{x_1}^4 + \alpha^{30}\widetilde{\theta_1}^4. \end{aligned} \tag{6.55}$$

6.5.5 Exclusion of row erasures

Let us make the second (intermediate) modification of the syndrome to avoid powers of θ_1 higher than 1. The first component of the modified syndrome we raise to the power $2^n = 2^5 = 32$, we raise the second component to the power $2^{n-1} = 2^4 = 16$, and the third component to power $2^{n-2} = 2^3 = 8$:

$$\widetilde{s}_{0\mathrm{mod}} = \widetilde{s}_0^{32} = \alpha^{11},\ \widetilde{s}_{1\mathrm{mod}} = \widetilde{s}_1^{16} = \alpha^{22},\ \widetilde{s}_2^{8} = \alpha^{29}.$$

For the third modification of the syndrome we use the linearized polynomial $\Lambda(x) = \Lambda_0 x + \Lambda_1 x^2$ with roots $a = \alpha^{30}$ and 0. Set $\Lambda_1 = 1$ in the equation $\Lambda_0\alpha^{30} + \Lambda_1\alpha^{29} = 0$ and obtain $\Lambda_0 = \alpha^{30}$. Similar to the previous modification, we build the matrix

$$\mathbf{\Lambda} = \begin{bmatrix} \Lambda_1^{16} & 0 \\ \Lambda_0^{16} & \Lambda_1^{3} \\ 0 & \Lambda_0^{8} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \alpha^{15} & 1 \\ 0 & \alpha^{23} \end{bmatrix}.$$

As the third modification we multiply the syndrome and its component due to the random error by the matrix $\mathbf{\Lambda}$:

$$\begin{aligned} &\widehat{\mathbf{s}} = \widetilde{\mathbf{s}}\mathbf{\Lambda} = [\alpha^8\ \alpha^8] = [\widehat{s}_0\ \widehat{s}_1] \\ &\widetilde{x_1}[e_1\ e_1^{16}\ e_1^{8}]\mathbf{\Lambda} = \widetilde{x_1}[\widetilde{e_1}^2\ \widetilde{e_1}] \end{aligned} \tag{6.56}$$

where $\widetilde{e_1} = (\Lambda(e_1))^8$. By equating the components of the modified syndrome we obtain the following system of two equations with two unknowns $\widetilde{x_1}$, $\widetilde{e_1}$

$$\begin{aligned} \widehat{s}_0 &= \alpha^8 = \widetilde{x_1}\widetilde{e_1}^2, \\ \widehat{s}_1 &= \alpha^8 = \widetilde{x_1}\widetilde{e_1} \end{aligned} \tag{6.57}$$

with solution $\widetilde{x_1} = \alpha^8$, $\widetilde{e_1} = 1$.

6.5.6 Correction of random error

Trying all field elements we solve the equation

$$\widetilde{x_1} = \alpha^8 = x_1^2 + \alpha^5 x_1.$$

There are two solutions: $x_1 = \alpha^{12}$ or $x_1 = \alpha^{27}$. Similarly we solve

$$\widetilde{e_1} = 1 = (\alpha^{30} e_1 + e_1^2)^8.$$

There are two solutions: $e_1 = \alpha^5$ or $e_1 = \alpha^{26}$.

Let us use the first solutions: $x_1 = \alpha^{12}$ and $e_1 = \alpha^5$. Given x_1, let us find the components of the vector $\mathbf{u}_1$ using

$$x_1 = \alpha^{12} = \alpha^2 u_{11} + \alpha^{29} u_{12} + \alpha^5 u_{13} + \alpha^{14} u_{14} + \alpha^9 u_{15} \qquad (6.58)$$

we obtain a solution $\mathbf{u}_1 = [0\ 1\ 0\ 1\ 1]$.

Write the random error in the vector form: $\mathbf{e}_{\text{rand}} = e_1 \mathbf{u}_1 = \alpha^5 [0\ 1\ 0\ 1\ 1]$.

Transform the random error to the matrix form:

$$\mathbf{E}_{\text{rand}} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

6.5.7 Erasure correction

Substitute the known values of $\widetilde{s_0} = \alpha^{11}$, $e_1 = \alpha^5$, $\widetilde{x_1} = \alpha^8$, $a = \alpha^{30}$ to the first equation of the system (6.55). Solving the equation

$$\alpha^{11} = \alpha^5 \alpha^8 + \alpha^{30} \widetilde{\theta}_1.$$

we obtain $\widetilde{\theta}_1$ and obtain solutions $\theta_1 = \alpha^7$ or $\theta_1 = \alpha^{10}$.

We use (6.48) for θ_1 and substitute the solution $\theta_1 = \alpha^7$. Solve the equation

$$\alpha^7 = \alpha^2 r_{11} + \alpha^{29} r_{12} + \alpha^5 r_{13} + \alpha^{14} r_{14} + \alpha^9 r_{15}$$

and obtain: $\mathbf{r}_1 = [0\ 1\ 0\ 1\ 0]$. The vector of row erasures is $\mathbf{e}_{\text{row}} = \alpha^{30}[0\ 1\ 0\ 1\ 0]$, i.e., in matrix form

$$\mathbf{E}_{\text{row}} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

To find w_1 we substitute to first equation of the main system (6.50):

$$s_0 = e_1 x_1 + \alpha^{30}\theta_1 + \alpha^5 w_1 = \alpha^5,$$

the known values $x_1 = \alpha^{12}$, $e_1 = \alpha^5$, $\theta_1 = \alpha^7$. We obtain $w_1 = \alpha^8$. The column erasures in vector form are $\mathbf{e}_{\text{col}} = \alpha^8[0\ 0\ 1\ 0\ 0]$, and in matrix form

$$\mathbf{E}_{\text{col}} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

The error vector is

$$\begin{aligned} \mathbf{e} &= \mathbf{e}_{\text{rand}} + \mathbf{e}_{\text{row}} + \mathbf{e}_{\text{col}} \\ &= [0\ \alpha^5\ 0\ \alpha^5\ \alpha^5] + [0\ \alpha^{30}\ 0\ \alpha^{30}\ 0] + [0\ 0\ \alpha^8\ 0\ 0] \\ &= [0\ \alpha^{26}\ \alpha^8\ \alpha^{26}\ \alpha^5]. \end{aligned} \tag{6.59}$$

Let us check the solution. Subtract from the received vector $\mathbf{y}$ (6.43) the error vector (6.59):

$$\begin{aligned} \mathbf{y} + \mathbf{e} &= [\alpha\ \alpha^5\ \alpha^{12}\ \alpha^{18}\ \alpha^{29}] + [0\ \alpha^{26}\ \alpha^8\ \alpha^{26}\ \alpha^5] \\ &= [(\alpha + 0)\ \ (\alpha^5 + \alpha^{26})\ \ (\alpha^{12} + \alpha^8)\ \ (\alpha^{18} + \alpha^{26})\ \ (\alpha^{29} + \alpha^5)] \\ &= [\alpha\ \alpha^{30}\ \alpha^{18}\ \alpha^7\ \alpha^{20}]. \end{aligned} \tag{6.60}$$

Comparing the solution with the transmitted code vector (6.35), we see that they coincide.

In matrix form the error is

$$\mathbf{E} = \mathbf{E}_{\text{rand}} + \mathbf{E}_{\text{row}} + \mathbf{E}_{\text{col}} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}. \tag{6.61}$$

The rank of the error matrix is 4.

The difference of the received matrix $\widehat{\mathbf{R}}$ and error matrix $\mathbf{E}$ (6.61) is

$$\widehat{\mathbf{R}}+\mathbf{E}=\begin{bmatrix}0&1&0&1&1\\1&0&1&1&0\\0&1&1&0&0\\0&0&1&0&1\\0&0&0&0&0\end{bmatrix}+\begin{bmatrix}0&1&1&1&1\\0&1&0&1&0\\0&1&1&1&1\\0&0&1&0&0\\0&1&0&1&0\end{bmatrix}=\begin{bmatrix}0&0&1&0&0\\1&1&1&0&0\\0&0&0&1&1\\0&0&0&0&1\\0&1&0&1&0\end{bmatrix}=\mathbf{M}. \tag{6.62}$$

The solution is correct since the code matrix $\mathbf{M}$ was transmitted.

6.6 Conclusions

We have considered the principles suggested by Kötter, Kschischang, Silva for designing subspace codes based on rank Gabidulin codes. The code matrices consist of the identity matrix and a matrix of the rank code. This construction is called the lifting of rank codes. The network channel forms linear combinations of rows of a code matrix and adds outer errors. The decoding algorithm consists of two steps: first obtain the distorted matrix of the rank code using Gaussian elimination and then use a standard algorithm for decoding rank codes.

7

Multicomponent prefix codes

In this chapter, we introduce a class of codes that is called multicomponent prefix codes. These codes generalize the codes of Silva-Kötter-Kschischang (SKK). A multicomponent code is a union of different component codes that are SKK codes with a fixed code distance, and the minimum subspace distances between the code components are not less than the code distance of the components.

7.1 Gabidulin–Bossert subspace codes

Subspace codes with maximum code distance were proposed by Gabidulin and Bossert in [GB08].

Lemma 7.1. *Let U and V be subspaces of N-dimensional vector space. The subspace distance between them is $d(U,V) = N$, if and only if*

1. *Subspaces U and V intersect trivially, i.e., the intersection is the subspace of dimension zero.*

2. *The dimension of the union is* $\dim(U) + \dim(V) = N$.

Proof. If both conditions are satisfied then from (6.2) it follows that $d(U,V) = \dim(U) + \dim(V) - 2\dim(U \cap V) = N$ since $\dim(U \cap V) = 0$.

Assume now that $d(U,V)=N$. Denote $Z=U\cap V$. We have

$$\begin{aligned}
&d(U,V)=\dim(U)+\dim(V)-2\dim(Z)=N,\\
&\dim(U\uplus V)=\dim(U)+\dim(V)-\dim(Z)\leq N,\\
&\dim(Z)\geq 0.
\end{aligned}\tag{7.1}$$

The system of equations (7.1) has a unique solution $\dim(Z)=0$. This means that the subspaces U and V intersect trivially and $\dim(U)+\dim(V)=N$. ■

Let $\mathcal{C}$ be a code with maximum subspace distance $d(\mathcal{C})=N$.

Theorem 7.2. *If N is odd, then the cardinality of any code $\mathcal{C}$ with subspace distance N is $|\mathcal{C}|=2$. Such a code consists of two subspaces $\mathcal{C}=\{U,V\}$, where U and V intersect trivially and*

$$\dim(U)+\dim(V)=N.\tag{7.2}$$

Proof. The code $\mathcal{C}$ has at most 2 subspaces. Otherwise, at least two subspaces would have dimensions of the same parity and an even distance $d\leq N$ between them. The second part of the theorem follows from Lemma 7.1. ■

The situation changes drastically if N is even, $N=2m$.

Lemma 7.3. *If the code $\mathcal{C}$ with the maximum (even) distance N consists of $|\mathcal{C}|\geq 3$ subspaces, then the subspaces pairwise intersect trivially and have equal dimension $N/2=m$.*

Proof. Let a code $\mathcal{C}$ consist, for example, of 3 subspaces U_1,U_2,U_3. By Lemma 7.1, any pair of subspaces intersect trivially. In addition to this $\dim(U_1)+\dim(U_2)=2m$, $\dim(U_1)+\dim(U_3)=2m$, $\dim(U_3)+\dim(U_2)=2m$. Hence, $\dim(U_1)=\dim(U_2)=\dim(U_3)=m$. ■

Lemma 7.4. *The cardinality of a code $\mathcal{C}$ with maximum even distance $N=2m$ satisfies the bound*

$$|\mathcal{C}|\leq q^m+1.\tag{7.3}$$

Proof. Every m-dimensional subspace has q^m-1 nonzero vectors from N-dimensional vector space. The number of nonzero vectors in $\mathcal{C}$ equals $|\mathcal{C}|(q^m-1)$, since the subspaces of the code $\mathcal{C}$ intersect trivially. The relation $|\mathcal{C}|(q^m-1)\leq q^N-1=q^{2m}-1$ holds, and we have, $|\mathcal{C}|\leq q^m+1$. ■

Theorem 7.5. *There exists a code $\mathcal{C}$ with maximum even distance $N = 2m$ and with maximum cardinality*

$$|\mathcal{C}| = q^m + 1. \tag{7.4}$$

Proof. Represent m-dimensional subspace by $m \times 2m$ basis matrices of full rank $[C\ D]$, where C and D are square matrices of order m. Let A be a matrix of order m that represents the field $\mathbb{F}_{q^m}$ (6.9). Define the set of m-dimensional subspaces in $\mathcal{C}$ by the following basis matrices:

$$[I_m\ O_m], [I_m\ I_m], [I_m\ A], \cdots, [I_m\ A^{q^m-2}], [O_m\ I_m]. \tag{7.5}$$

The number of matrices in this set is $q^m + 1$. Each matrix has full rank m. Hence, the corresponding subspaces have rank m each. Let us show that these subspaces pairwise intersect trivially. Denote by S the subspace generated by the matrix $M(S) = [I_m\ O_m]$, by $V_j, j = 0, \ldots, q^m - 2$ denote subspaces generated by the matrices $M(V_j) = [I_m\ A^j]$, and by R the subspace generated by the matrix $M(R) = [O_m\ I_m]$. Then we have

$$\dim(S \uplus V_j) = \mathrm{Rk}\left(\begin{bmatrix} I_m & O_m \\ I_m & A^j \end{bmatrix}\right) = 2m \quad \Rightarrow \quad \dim(S \cap V_j) = 0,$$

$$\dim(S \uplus R) = \mathrm{Rk}\left(\begin{bmatrix} I_m & O_m \\ O_m & I_m \end{bmatrix}\right) = 2m \quad \Rightarrow \quad \dim(S \cap R) = 0,$$

$$\dim(V_i \uplus V_j) = \mathrm{Rk}\left(\begin{bmatrix} I_m & A^i \\ I_m & A^j \end{bmatrix}\right) = 2m \quad \Rightarrow \quad \dim(V_i \cap V_j) = 0,$$

$$\dim(V_i \uplus R) = \mathrm{Rk}\left(\begin{bmatrix} I_m & A^i \\ O_m & I_m \end{bmatrix}\right) = 2m \quad \Rightarrow \quad \dim(V_i \cap R) = 0.$$

Hence, the code defined by (7.5) is an optimal code with distance $N = 2m$. ■

7.2 Multicomponent Gabidulin-Bossert subspace codes

New subspace codes based on rank codes were proposed by Gabidulin and Bossert [GB09] and were called multicomponent prefix codes. Let us consider constructions of these codes.

Write $N = m_1 + m_2 + \cdots + m_k$, where $m_1 \geq m_2 \geq \cdots \geq m_k$. We will design a code $\mathcal{X}$ as the union of component codes $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2 \cup \cdots \cup \mathcal{X}_k$. Pairwise intersection of the component codes should be empty. Let us define the component codes as follows:

$$\begin{aligned}
&\mathcal{X}_1 = \left\{X : X = \begin{bmatrix} I_{m_1} & x_1 \end{bmatrix} \mid x_1 \in \mathcal{M}_1\right\} \\
&\mathcal{X}_2 = \left\{X : X = \begin{bmatrix} O_{m_2}^{m_1} & I_{m_2} & x_2 \end{bmatrix} \mid x_2 \in \mathcal{M}_2\right\} \\
&\vdots \\
&\mathcal{X}_{k-1} = \left\{X : X = \begin{bmatrix} O_{m_{k-1}}^{m_1+\cdots+m_{k-2}} & I_{m_{k-1}} & x_{k-1} \end{bmatrix} \mid x_{k-1} \in \mathcal{M}_{k-1}\right\} \\
&\mathcal{X}_k = \left\{X : X = \begin{bmatrix} O_{m_k}^{N-m_k} & I_{m_k} \end{bmatrix}\right\}.
\end{aligned} \tag{7.6}$$

Here

- $\mathcal{M}_1$ is a rank code consisting of $m_1 \times (N - m_1)$ matrices over $\mathbb{F}_q$ with rank code distance $d_{r1} \leq \min\{m_1, N - m_1\}$;
- $\mathcal{M}_2$ is a rank code consisting of $m_2 \times (N - m_1 - m_2)$ matrices over $\mathbb{F}_q$ with rank code distance $d_{r2} \leq \min\{m_2, N - m_1 - m_2\}$;
- $\vdots$
- $\mathcal{M}_{k-1}$ is a rank code consisting of $m_{k-1} \times (N - m_1 - \cdots - m_{k-1})$ matrices over $\mathbb{F}_q$ with rank code distance $d_{r\ (k-1)} \leq \min\{m_{k-1}, N - m_1 - \cdots - m_{k-1}\}$.

Obviously, $\mathcal{X}_i \cap \mathcal{X}_j = \varnothing$, $i \neq j$.

The code has the following characteristics:

- cardinality

$$\mathcal{X} = |\mathcal{C}| = \sum_{i=1}^{k} |\mathcal{C}_i|,$$

- subspace distance

$$d(\mathcal{X}) = \min\{\min_{i\neq j}(m_i + m_j), \min_{1\leq i\leq k-1}\{2d_{ri}\}\}.$$

7.3 Decoding codes with maximum distance

First consider the subspace code of length N consisting of two subspaces: the first is generated by rows of the identity matrix $X_1 = I_N$, the second by rows of all zero matrix $X_2 = O_N$.

If the matrix X_1 has been transmitted, then the received matrix is

$$Y = AX_1 + BZ = A + BZ,$$

if X_2 was transmitted, then the received matrix is

$$Y = AX_2 + BZ = BZ.$$

The decoder computes rank $\mathrm{Rk}(Y)$ of the received matrix Y and the distance between the subspace $\langle Y\rangle$ and $\langle X_1\rangle$ and $\langle X_2\rangle$ respectively:

$$d_1 = d(\langle Y\rangle, \langle X_1\rangle) = 2\mathrm{Rk}\left(\begin{bmatrix} Y \\ I_N \end{bmatrix}\right) - \mathrm{Rk}(Y) - \mathrm{Rk}(I_N) = N - \mathrm{Rk}(Y)$$

and

$$\begin{aligned} d_2 = d(\langle Y\rangle, \langle X_2\rangle) &= 2\mathrm{Rk}\left(\begin{bmatrix} Y \\ O_N \end{bmatrix}\right) - \mathrm{Rk}(Y) - \mathrm{Rk}(O_N) \\ &= 2\mathrm{Rk}(Y) - \mathrm{Rk}(Y) = \mathrm{Rk}(Y). \end{aligned}$$

If $d_1 < d_2$, i.e., $\mathrm{Rk}(Y) > N/2$, then the decoder makes a decision $X_1 = I_N$, otherwise the decision is $X_2 = O_N$.

For $N = 2m$, the code $\mathcal{X}$ with maximum subspace distance $2m$ can be seen as the union of two subcodes $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$, where

$$\mathcal{X}_1 = \left\{X : X = \begin{bmatrix} I_m & x \end{bmatrix}, x \in \mathcal{C}\right\}$$

is the code of cardinality q^m having a single $m \times m$ code matrix x of the rank code, and

$$\mathcal{X}_2 = \left\{X : X = \begin{bmatrix} O_m & I_m \end{bmatrix}\right\}$$

is the code of cardinality 1.

Let the received matrix be

$$Y = AX + BZ = \begin{bmatrix} \widehat{A} & y \end{bmatrix}.$$

Decoding consists of two steps. In the first step, the decoder tries to determine whether the received subspace $\langle Y \rangle$ corresponds to the transmitted matrix $\mathcal{X}_1$ or $\mathcal{X}_2$. This is equivalent to finding whether the subspace $\langle \widehat{A} \rangle$ originates from $\langle I_m \rangle$ or from $\langle O_m \rangle$. It was shown above that the solution is based on the rank of the matrix $\mathrm{Rk}(\widehat{A})$:

- If $\mathrm{Rk}(\widehat{A}) < m/2$, then the subspace $\langle Y \rangle$ originates from $\mathcal{X}_2$. Then we go to the second step: consider the matrix $\begin{bmatrix} O_m & I_m \end{bmatrix}$ as the decoding result.
- If $\mathrm{Rk}(\widehat{A}) \geq m/2$, then the subspace $\langle Y \rangle$ originates from $\mathcal{X}_1$. Go to the second step: run SKK decoder, extract the matrix $x \in \mathcal{C}$ and get $X = \begin{bmatrix} I_m & x \end{bmatrix}$ as the decoding result.

7.4 Decoding multicomponent prefix codes

Let us generalize the approach we considered for decoding multicomponent codes. Let Y be a received matrix

$$Y = AX + BZ$$

and X belongs to one of the component codes (7.6). Write Y as

$$Y = \begin{bmatrix} \widehat{A}_1 & \widehat{A}_2 & \dots & \widehat{A}_{k-1} & y \end{bmatrix},$$

where $\widehat{A}_1$ is an $n_r \times m_1$ matrix, $\widehat{A}_2$ is an $n_r \times m_2$ matrix, …, $\widehat{A}_{k-1}$ is an $n_r \times m_{k-1}$ matrix.

- The decoder should solve the following problem: does the received subspace $\langle Y \rangle$ originate from the subcode $\mathcal{X}_1$or from $\mathcal{X}_2 \cup \dots \cup \mathcal{X}_k$? Instead, the decoder solves an equivalent problem: does the subspace $\langle \widehat{A}_1 \rangle$ originate from the subspace $\langle I_{m_1} \rangle$ or from $\langle O_{m_1} \rangle$? To find the solution, the decoder computes the rank of $\widehat{A}_1$: $r_1 = \mathrm{Rk}(\widehat{A}_1)$.

  1. If $r_1 \geq m_1/2$, then the decision is: $\langle Y \rangle$ originates from $\mathcal{X}_1$. Using the SKK decoder, find $x_1 \in \mathcal{M}_1$. The decoder outputs the matrix $X = \begin{bmatrix} I_{m_1} & x_1 \end{bmatrix}$ as the decoding result.

2. If $r_1 < m_1/2$, then the decision is: $\langle Y \rangle$ originates from the subcode $\mathcal{X}_2 \cup \cdots \cup \mathcal{X}_k$. The decoder goes to the next step.

- The decoder should solve the following problem: does the received subspace $\langle Y \rangle$ $\mathcal{X}_2$ or from the subcode $\mathcal{X}_3 \cup \cdots \cup \mathcal{X}_k$? Instead, the decoder solves an equivalent problem: does the subspace $\left\langle \begin{bmatrix} \widehat{A}_1 & \widehat{A}_2 \end{bmatrix} \right\rangle$ originate from the subspace $\left\langle \begin{bmatrix} O_{m_2}^{m_1} & I_{m_2} \end{bmatrix} \right\rangle$ or from $\left\langle \begin{bmatrix} O_{m_2}^{m_1} & O_{m_2} \end{bmatrix} \right\rangle$? To find the solution, the decoder computes the rank $r_2 = \mathrm{Rk}\left(\begin{bmatrix} \widehat{A}_1 & \widehat{A}_2 \end{bmatrix} \right)$.

  1. If $r_2 \geq m_2/2$, then the desicion is: $\langle Y \rangle$ originates from the subcode $\mathcal{X}_2$. Using the SKK decoder to find $x_2 \in \mathcal{M}_2$. The matrix $X = \begin{bmatrix} O_{m_2}^{m_1} & I_{m_2} & x_2 \end{bmatrix}$ is the decoding result.
  2. If $r_2 < m_2/2$, then the decision is: $\langle Y \rangle$ originates from the subcode $\mathcal{X}_3 \cup \cdots \cup \mathcal{X}_k$. The decoder goes to the next step.

- The algorithm is running until the final decision is found. The number of required steps is k at most.

7.5 Cardinality of MZP codes

The multicomponent codes with zero prefix (MZP) were presented in 2008 by Gabidulin and Bossert [GB08]. They were based on the lifted rank codes by Kötter, Kschischang, Silva [KK08], [SKK08]. Let $n = m + r\delta + s$ be code length, where m is the dimension, r is an integer, $r \geq 1$, $0 \leq s \leq \delta - 1$.

The first component is the SKK-code. It consists of a set of matrices

$$\mathcal{C}_{\text{skk}} = \left\{ \begin{pmatrix} I_m & M_1 \end{pmatrix} \mid M_1 \in \mathcal{M}_1 \right\}, \tag{7.7}$$

where I_m is the identity matrix of order m, while M_1 is a code matrix of size $m \times (n - m)$ of the rank matrix code $\mathcal{M}_1$ with rank distance $d_{\text{rank}} = \delta$ [Gab85]. The *subspace distance* of the code $\mathcal{C}_{\text{skk}}$ is more than twice the *rank distance* of the matrix code $\mathcal{M}_1$: $d_{\text{sub}}(\mathcal{C}_{\text{skk}}) = 2d_{rank}(\mathcal{M}_1) = 2\delta$.

The cardinality of a subspace code is a very important characteristic. There are many works which estimate this characteristic and compare it with upper bounds (see, for example, [GP17b], [GP17a]) .

The cardinality $|\mathcal{C}_{\mathrm{skk}}|$ of SKK-code is equal to the size of the rank code with rank distance $d_{\mathrm{rank}} = \delta$ and code length $(n-m)$:

$$|\mathcal{C}_{\mathrm{skk}}| = q^{(n-m)(m-\delta+1)}, \tag{7.8}$$

where $\delta \leq m, n \geq 2m$.

For $i = 2, \dots, r$, the (i)-th component consists of matrices of the form

$$\mathcal{C}_{mzp\,i} = \left\{ \begin{pmatrix} 0_m^\delta & \dots & 0_m^\delta & I_m & M_i \end{pmatrix} \mid M_i \in \mathcal{M}_i \right\},$$

where the first $i-1$ block matrices are the all-zero matrices 0_m^δ of size $m \times \delta$. I_m is the identity matrix, M_i is a code matrix of size $m \times (n-m-(i-1)\delta)$ of the rank matrix code $\mathcal{M}_i$ with rank distance δ. The cardinality of the ith component is as follows:

$$|\mathcal{C}_{mzp\,i}| = q^{(n-m-(i-1)\delta)(m-\delta+1)} = q^{n_i(m-\delta+1)}, \tag{7.9}$$

where $n_i = n - m - (i-1)\delta$ is the code length of the rank code. The last component is the concatenation of all-zero matrix of size $m \times (n-m)$, the identity matrix I_M, and a matrix A_m^s of size $m \times s$ which may have a rank less than or equal to $s \leq \delta - 1$. Hence the last component delivers only one code matrix. The total number of components is equal to $l+1$. The cardinality of the MZP code is the sum of the cardinalities of all components because the components do not intersect:

$$M_{mzp} = |\mathcal{C}_{mzp}| = \sum_{i=1}^{l} q^{((n-m)-(i-1)\delta)(m-\delta+1)} + 1. \tag{7.10}$$

7.6 Additional cardinality

In many articles the most attention is given to SSK codes as subspace codes obtained by lifting of rank codes. The cardinality of the lifting codes obtained can differ just by one code word, but this code word is not known. This case corresponds to our two components code and we use the last word. In matrix presentation it is the concatenation of zero matrix and the identity matrix.

Here, we show that multicomponent code can increase cardinality by considerably more than one code word. Let us construct the multicomponent code, where n is code length, m is dimension, $d = 2\delta$ is code distance. The cardinality of each component is the following:

$$M_{skk} = M_1 = q^{(m-\delta+1)(n-m)};$$

$$M_2 = q^{(m-\delta+1)(n-m-\delta)};$$

$$M_i = q^{(m-\delta+1)(n-m-(i-1)\delta)}.$$

Let the total number of components be (i+1), where $n - m - (i-1)\delta = m$, that is $i = 1 + \frac{n-2m}{\delta}$. The last component is a concatenation of the all-zero matrix of size $m \times (n-m)$, the identity matrix I_m, and a matrix A_m^s.

The total cardinality is

$$M_{\text{mzp}} = q^{k(n-m)} + \frac{q^{k(n-m-\delta)}q^{k\delta} - q^{km}}{q^{k\delta} - 1} + 1 = M_{skk} + \Delta,$$

where $k = m - \delta + 1$ and

$$\Delta = \frac{q^{k(n-m-\delta)}q^{k\delta} - q^{km}}{q^{k\delta} - 1} + 1.$$

Δ is the number of additional words except words of the first component.

Now, let us estimate the ratio that is the additional cardinality to the first component cardinality $\nu = \frac{\Delta}{M_{skk}}$.

$$\nu = \frac{1}{q^{k\delta} - 1} - \frac{q^{km} - q^{k\delta} + 1}{(q^{k\delta} - 1)q^{k(n-m)}}.$$

$$\nu \simeq \frac{1}{q^{k\delta} - 1}$$

under the condition

$$q^{k(n-m)\gg(q^{km}-q^{k\delta}+1q^{km}-q^{k\delta}+1)}.$$

If $m = \delta$, $k = 1$, then this condition is the following

$$q^{k(n-m)} \gg 1,$$

and it is evident that $M_{skk} = q^{k(n-m)}$. Let us give numerical examples. They are shown in Table 7.1.

Table 7.1: Additional cardinality

ν	0.312	0.328	0.321	0.333	0.143
M_{skk}	16	64	256	4194304	4096
Δ	5	21	85	1398101	585
n	6	8	10	24	15
m	2	2	2	2	3
δ	2	2	2	2	3

7.7 Efficiency of MZP codes with maximal code distance

From now on we consider MZP-codes with the following parameters: $n = mr + s$, $\delta = m$, $0 < s \leq (m-1)$. Recall that we call these codes MZP spreads. Let us calculate their cardinality for different parameters and compare their values with the existing bounds. Put $\delta = m$ in (7.10) and obtain the following equation:

$$M_{mzp} = |\mathcal{C}_{mzp}| = \sum_{i=1}^{r-1} q^{(mr+s-im)} + 1 = \frac{q^n - q^{m+s}}{q^m - 1} + 1. \tag{7.11}$$

If $s = 0$ and $n = rm$ are used the cardinality coincides with the *upper* bound $M_{\text{segre}} = \frac{q^n-1}{q^m-1}$ (see, [Seg64], [Beu75], [DF79], [WXSN03], [CW13], [Kur16], [HKK18], [Kur17], [SN17b], [SN17a]).

Now, if $n = rm + 1$ and $s = 1$ we have from (7.11)

$$M_{mzp} = |\mathcal{C}_{mzp}| = \frac{q^n - q^{m+1}}{q^m - 1} + 1.$$

This value coincides with the *upper* bound [Beu75] $M_{beut} = \frac{q^n-1}{q^m-1} - (q-1)$.

If $n = rm + 2$ and $s = 2$ we have from (7.11)

$$M_{mzp} = |\mathcal{C}_{mzp}| = \frac{q^n - q^{m+2}}{q^m - 1} + 1.$$

[DF79] gives the upper bound for spreads with parameter $s \geq 2$. Using the corresponding formula in [GP16] represent it as a sum of two terms: the first term is the cardinality of the MZP spread and the second is γ_1, where γ_1 is some quantity.

$$M_{dr-fr} \leq \frac{q^n - q^{m+s}}{q^m - 1} + 1 + \gamma_1, \tag{7.12}$$

where $\gamma_1 = (q^s - \lfloor \theta \rfloor) - 2$, parameter θ depends on m and s in the following way:

$$\lfloor \theta \rfloor = \begin{cases} q^{s-1} - 1, & \text{if } 2s < m + 2; \\ q^{s-1} - 2, & \text{if } 2s = m + 2; \\ q^{s-1} - 2^{2s-m-3} - 1, & \text{if } 2s > m + 2. \end{cases}$$

Let $q = 2$, $m = 3$ and $s = 2$. Then $\gamma_1 = 1$. In this case the cardinality of this MZP spread does not coincide with the upper bound with difference 1. To increase cardinality up to the upper bound in the paper [GP16] a subspace code from the paper [EZJS+10] was used. It was obtained there for parameters $r = 2$, $m = 3$, $s = 2$, $n = 8$ by exhaustive search. We used it as the last component MZP code for $n = mr + 8$, where $m = 3$.

Here, for $q = 2$, $r \geq 2$, $m = 4$ and $s = 2$ we use the upper bound from the paper [Kur16]:

$$M_{Kurz} = \frac{2^{4r+2} - 49}{15}. \tag{7.13}$$

Applying our formula for cardinality to the MZP spread (7.11) with the same parameters, one can see that the cardinality of the MZP spread coincides with this upper bound.

Now we will use the upper bounds from [HKK18]. In this paper there are two important theorems. Let us give our interpretation and our designations for these theorems.

Theorem 7.6. *If $0 < s < m$ and $m > q^s$, then the maximal cardinality of subspace code is the following: $M_{HKK1} = \frac{q^{mr+s} - q^{m+s} + q^m - 1}{q^m - 1}$.*

Let us compare M_{HKK1} (7.6) and M_{mzp} (7.11). One can see that both formulas for cardinality coincide. That means that the cardinality of the MZP spread achieves the upper bound if the conditions indicated in the theorem are satisfied: $0 < s < m$ and $m > q^s$.

If the conditions are not satisfied there is another theorem in the paper [HKK18].

Theorem 7.7. *If $0 < s \leq (m-1)$ and $m < q^s$, then the maximal cardinality of subspace code is the following: $M_{HKK2} = \frac{q^n - q^{m+s} + q^m - 1}{q^m - 1} + \gamma_2$, where $\gamma_2 > 1$, it is calculated by means of auxiliary parameters.*

We see that the MZP spread does not coincide with the upper bound at these conditions.

There are two values γ_2: $\gamma_{21} > 1$ and $\gamma_{22} > 1$. We have

$$\gamma_{21} = \lceil 2^m - \frac{1}{2}(1 + 2^{m+2}(2^m - 2^s))^{\frac{1}{2}} \rceil - 1$$

and

$$\gamma_{22} = \lceil 2^s - \frac{1}{2}(1 + 2^{s+2}(m - s))^{\frac{1}{2}} \rceil - 1.$$

For γ_2 one should select the minimum between γ_{21} and γ_{22}.

We would also like to estimate by Drake–Freeman [DF79]. For this purpose we will use the parameter $\gamma_1 = (q^s - \lfloor \theta \rfloor) - 2$. At the chosen parameters we calculate three values γ_1, γ_{21} and γ_{22}, take the smallest value and add to the cardinality value of the MZP spread. We consider the value obtained as an estimation M_{up} of the upper bound at these conditions. The efficiency of the MZP spread is denoted $\eta = \frac{M_{mzp}}{M_{up}}$.

Table 7.2: Efficiency of MZP spread

η	0.971	0.970	0.985	0.996	0.992	0.997	0.996
M_{mzp}	33	129	513	513	2049	2049	4097
M_{up}	34	133	521	515	2066	2055	4112
n	8	11	14	15	17	18	19
m	3	4	5	6	6	7	7
s	2	3	4	3	5	4	5
γ_{21}	1	4	8	2	18	6	15
γ_{22}	1	5	11	3	25	7	22
γ_1	1	4	10	3	17	7	19

One can see from Table 7.2 that the efficiency $\eta = \frac{M_{mzp}}{M_{up}}$ is about $\eta = 0.99$ for all the cases where $m < 2^s$.

7.8 Dual multicomponent codes

Let a subspace X of dimension m be given by a matrix L of size $m \times n$ with rank m. The orthogonal subspace $X^{\perp}$ of dimension $n-m$ will be given by the matrix $L^{\perp}$ of size $(n-m) \times n$ such that

$$(L^{\perp})(L^{\top}) = 0,$$

where $L^{\top}$ means the transposed matrix L.

Let us construct the dual multicomponent code (DMC). For $j = 1, \dots r$, the components of the MZP codes with dimension m and length $n = rm + s$ are given by matrices of rank m with the following form:

$$L_j = \begin{bmatrix} \mathbf{0}_m & \dots & \mathbf{0}_m & \mathbf{I}_m & \mathbf{M}_j \end{bmatrix}.$$

The matrices consist of the zero matrix prefix of size $m \times (j-1)m$, the unity submatrix $\mathbf{I}_m$ of order m and the submatrix $\mathbf{M}_j$ of size $m \times n - jm$.

The orthogonal matrix$L_j^{\perp}$ with rank $n-m$ is the following

$$L_j^{\perp} = \begin{bmatrix} \mathbf{I}_{(j-1)m} & \mathbf{0}_{(j-1)m}^{m} & \mathbf{0}_{(j-1)m}^{n-jm} \\ \mathbf{0}_{n-jm}^{(j-1)m} & -\mathbf{M}^{\top} & \mathbf{I}_{n-jm} \end{bmatrix},$$

where $\mathbf{0}_l^v$ is the zero matrix of size $l \times v$.

DMC code $L_j^{\perp}$ has dimension $n-m$ and subspace code distance $d_{\text{sub}} = 2m$. For the parameters $n = mr + s, m = 2, 3, s = 0, 1$ these codes have maximal cardinality.

7.9 Maximal cardinality MZP and DMC codes

First we consider MZP code. Let the parameters be $\delta = m$ and $n = (r+1)m + s$, $s = 0$. Then

$$M_{mzp} = \sum_{i=1}^{r-1} q^{(r-i+1)m(m-m+1)} + 1 = \frac{q^n - 1}{q^m - 1}.$$

This formula coincides with the *upper* bound $M_{\max}(0)$ [WXSN03].

Now $n = (r+1)m + 1$, $s = 1$, then

$$M_{mzp} = q\frac{q^{(r+1)m} - 1}{q^m - 1} - (q-1).$$

This formula coincides with the more precise *upper* bound

$$M_{\max}(1) = q\frac{q^{(r+1)m} - 1}{q^m - 1} - (q-1).$$

It means that for $m = 2$ the MZP codes have the maximal cardinality for any value of the parameters n, d. If $m = 3$ the MZP codes have maximal cardinality at $\delta = 3$ and $n = (r+1)m + s$, $s = 0, 1$. The corresponding dual codes have the same cardinality at the same parameters except dimension, which is $m' = n - m$.

Example 8. *Let us construct MZP codes with parameters* $n = (2 \times 3) + 1 = 7$, $d = 6$ *and the corresponding dual code with dimension* $n - 3 = 4$. *In this case the MZP code consists of two components.*

The first component is concatenation of two matrices I_3 of order 3 and the matrix M of size 3×4 of the rank code. The second component is also concatenation of two matrices. The first matrix is zero matrix 0_3^4 of size 3×4, the second matrix is the identity matrix I_3 of order 3. The cardinality of the first component is $M_1 = 2^4$, the cardinality of the second component is $M_2 = 1$. The total cardinality is $M_{max} = 17$. This value coincides with the upper bound.

The corresponding dual code also consists of two components. The first component is concatenation of two matrices, where the first matrix is the transposed 4×3 matrix $-M^T$ of the rank code and the initial MZP code has dimension 3. In this case the code word length is not equal to the double dimension $(2 \times m' = 8)$. Nevertheless, this dual code has maximal cardinality. This small example shows that construction of dual codes increases the general number of codes with maximum cardinality.

7.10 ZJSSS codes with maximal cardinality

Now let us use the following parameters: $(n = rm + 2) = 8$, $m = 3$. In this case our MZP code has cardinality $M = 33$, but the upper bound is one word greater, that is $M_{max} = 34$.

The paper [EZJS+10] constructs the code with the parameters indicated above. The method used is exhaustive search. This code has maximal cardinality 34. We designated this code ZJSSS using the first letters of author names. Here code subspaces of dimension $m = 3$ are given by binary generating matrices of size 3×8. For brevity each 8-bits row is written as a decimal binary number. The code matrices are the following.

$A_1=(169, 75, 5)$	$A_2 = (195, 43, 6)$	$A_3 = (108, 29, 3)$
$A_4=(130, 72, 20)$	$A_5=(144, 68, 33)$	$A_6 = (65, 61, 2)$
$A_7 = (66, 19, 4)$	$A_8=(140, 87, 1)$	$A_9=(35, 16, 9)$
$A_{10} = (147, 99, 7)$	$A_{11} = (155, 76, 38)$	$A_{12}=(69, 40, 24)$
$A_{13}=(132, 103, 12)$	$A_{14} = (152, 88, 56)$	$A_{15} = (153, 94, 39)$
$A_{16}=(196, 34, 11)$	$A_{17}=(167, 97, 15)$	$A_{18} = (159, 84, 32)$
$A_{19} = (154, 71, 55)$	$A_{20}=(145, 80, 50)$	$A_{21}=(131, 54, 13)$
$A_{22} = (134, 74, 53)$	$A_{23} = (166, 18, 8)$	$A_{24}=(164, 64, 31)$
$A_{25}=(138, 90, 60)$	$A_{26} = (135, 73, 27)$	$A_{27} = (146, 77, 37)$
$A_{28}=(171, 105, 17)$	$A_{29}=(158, 79, 52)$	$A_{30} = (128, 89, 47)$
$A_{31} = (129, 22, 10)$	$A_{32}=(143, 83, 46)$	$A_{33}=(205, 36, 21)$
$A_{34} = (137, 91, 44)$		

7.11 Dual ZJSSS code

We designate dual ZJSSS code as DZJSSS.

$A_1^{\perp}=(135, 66, 39, 16, 13)$	$A_2^{\perp} = (137, 73, 40, 16, 7)$
$A_3^{\perp} = (128, 43, 75, 12, 19)$	$A_4^{\perp}=(130, 72, 32, 20, 1)$
$A_5^{\perp}=(144, 68, 33, 8, 4)$	$A_6^{\perp} = (128, 69, 36, 20, 12)$
$A_7^{\perp} = (128, 32, 8, 67, 17)$	$A_8^{\perp}=(134, 66, 32, 18, 14)$
$A_9^{\perp}=(128, 64, 34, 11, 4)$	$A_{10}^{\perp} = (144, 85, 53, 8, 3)$
$A_{11}^{\perp} = (129, 71, 35, 17, 14)$	$A_{12}^{\perp}=(128, 65, 56, 5, 2)$
$A_{13}^{\perp}=(141, 65, 33, 16, 3)$	$A_{14} = (232, 24, 4, 2, 1)$
$A_{15}^{\perp} = (161, 98, 19, 11, 6)$	$A_{16}^{\perp}=(132, 68, 42, 16, 9)$
$A_{17}^{\perp}=(138, 67, 41, 16, 6)$	$A_{18}^{\perp} = (129, 69, 20, 9, 3)$
$A_{19}^{\perp} = (131, 98, 51, 11, 5)$	$A_{20}^{\perp}=(129, 83, 34, 8, 4)$
$A_{21}^{\perp}=(137, 64, 43, 27, 7)$	$A_{22}^{\perp} = (129, 71, 33, 17, 15)$
$A_{23}^{\perp} = (132, 64, 36, 22, 1)$	$A_{24}^{\perp}=(133, 37, 17, 9, 3)$
$A_{25}^{\perp}=(150, 84, 36, 14, 1)$	$A_{26}^{\perp} = (132, 67, 32, 22, 13)$
$A_{27}^{\perp} = (130, 72, 41, 18, 5)$	$A_{28}^{\perp}=(130, 74, 40, 25, 4)$
$A_{29}^{\perp}=(131, 65, 38, 21, 10)$	$A_{30}^{\perp} = (67, 34, 19, 9, 6)$
$A_{31}^{\perp} = (129, 64, 32, 20, 14)$	$A_{32}^{\perp}=(135, 70, 35, 22, 12)$
$A_{33}^{\perp}=(136, 72, 37, 25, 2)$	$A_{34}^{\perp} = (131, 66, 36, 18, 13)$

7.12 The family of MZP and combined codes

The algorithm of MZP code construction makes it possible to input ZJSSS code as two last components in order to increase cardinality of the MZP code.

Example 9. *Let $n = 11$. The MZP code consists of 3 components.*

The first component is SKK . Let us substitute the last two components of MZP code for the code ZJSSS, where we add zero prefix matrix $\mathbf{0}_3$ of order 3. The cardinality of this ZJSSS code is 34 which is maximal for chosen parameters $n = 8$ and $d = 2m = 6$. We have obtained a two component combined $[11, 6, 3]$ MZP-ZJSSS code with maximal cardinality 290.

Table 7.3: Cardinality of MZP and MZP-ZJSSS codes

r	n	M_{max}	M_{mzp}	$M_{\text{max}} - M_{\text{mzp}}$
2	8	34	33	1
3	11	290	289	1
4	14	2338	2337	1
5	17	18722	18721	1

Use the same method and set parameters $n = 3(r-1)+8 = 3(r+1)+2$, $m = 3$, $d = 6$. We will obtain a family of subspace codes with maximal cardinality. First of all, we construct an MZP-ZJSSS code with code word length $n = 3 \times r + 2$, where r is an integer. For example $r = 2, 3, 4, 5$, $n = 8, 11, 14, 17$. Let us calculate the cardinality of MZP and MZP-ZJSSS codes. We put this data in the Table 7.3.

Example 10. *Two component combined MZP-ZJSSS code). Using combined MZP-ZJSSS code with parameters $n = 11$, $m = 3$, $d = 6$, we construct a combined dual two component code and designate it by CD2C.*

The first component is given by the matrix:

$$\begin{bmatrix} M^T & I_8 \end{bmatrix}.$$

The second component is given by the matrix:

$$\begin{bmatrix} I_3 & 0_3^8 \\ 0_5^3 & Z^{\perp} \end{bmatrix},$$

where $Z^{\perp}$ is a DZJSSS code matrix with size 5×8. The matrix with size 8×11 is a concatenation of two submatrices, where the first submatrix M^T is a transposed rank code matrix of size 3×8, and the second submatrix is the identity matrix I_8 of order 8. The second component is the dual ZJSSS code in the form of the general matrix of size 8×11. The general matrix consists of four submatrices: the identity matrix I_3 of order 3 is located in the left upper corner, the zero matrix 0_3^8 with size 3×8 is located in the right upper corner, the zero matrix 0_5^3 of size 5×3 is located in the left down corner, the matrix of size 5×8 is located in the right down corner. This matrix is orthogonal to the ZJSSS code matrix of size 3×8.

Example 11. *Three component combined MZP-ZJSSS code.*

We construct a three component combined MZP-ZJSSS code with maximal cardinality with the following parameters: code word length $n = 14$, dimension $m' = n - m = 14 - 3 = 11$. The matrix of the first component is in the form $[I_3\ M_{11}\ M_{12}\ M_{13}\ M_{14}]$, where the rank code matrix M_1 is written as the concatenation of four matrices $M_1 = [M_{11}M_{12}M_{13}M_{14}]$, where the size of each of the first three matrices is 3×3, the size of the fourth matrix is 3×2. The corresponding first component of the dual code is in the form:

$$\begin{bmatrix} M_{11}^T & I_3 & 0^3 & 0^3 & 0^2 \\ M_{12}^T & 0^3 & I_3 & 0^3 & 0^2 \\ M_{13}^T & 0^3 & 0^3 & I_3 & 0^2 \\ M_{14}^T & 0^3 & 0^3 & 0^3 & I_2 \end{bmatrix}.$$

The second component of the MZP code is the following $\left[0_3^3\ I_3\ M_{21}\ M_{22}\ M_{23}\right]$, where the rank code matrix M_2 is in the form of concatenation of three matrices $M_2 = [M_{21}\ M_{22}\ M_{23}]$. The size of each of the first three matrices is 3×3, the size of the fourth matrix is 3×2. The corresponding second component of the dual code is

$$\begin{bmatrix} I_3 & 0^3 & 0^3 & 0^3 & 0^2 \\ 0^3 & M_{21}^T & I_3 & 0^3 & 0^2 \\ 0^3 & M_{22}^T & 0^3 & I_3 & 0^2 \\ 0^3 & M_{23}^T & 0^3 & 0^3 & I_2 \end{bmatrix}.$$

The third component of the combined three component code is presented as the concatenation of two zero matrices with size 3×3 and the matrix of the ZJSSS code with size 3×8:

$$\left[0_3^3\ 0_3^3\ Z\right],$$

where Z is a matrix of the ZJSSS code. The corresponding third component of the dual code is the following:

$$\begin{bmatrix} I_3 & 0_3^3 & 0_3^8 \\ 0_3^3 & I_3 & 0_3^8 \\ 0_5^3 & 0_5^3 & Z^T \end{bmatrix},$$

where Z^T is a transposed matrix with size 5×8 of the ZJSSS code.

7.13 MZP codes with dimension $m \geq 4$ and dual codes

In [Kur17] it is shown that the upper bound is equal to $M_{max} = 2^{m+2} + 1$ if the parameters are the following $n = 2m + 2$, $m \geq 4$, $d = 2m$. Our two component MZP code has this cardinality.

Let $m = 4$, $n = 10$, $d = 8$. The first component is SKK code with the matrix $[I_4\ M_{11}\ M_{12}]$ and the cardinality $M_1 = 2^{m+2} = 64$, the second component is the identity matrix with zero prefix which is a zero matrix with size 4×6. The cardinality of the second component is one code word.

The corresponding dual code also consists of two components. The first component is

$$\begin{bmatrix} M_{11}^T & I_4 & 0_4^2 \\ M_{12}^T & 0_2^4 & I_2 \end{bmatrix}.$$

The second component is

$$\begin{bmatrix} I_4 & 0_4^4 & 0_4^2 \\ 0_2^4 & 0_2^4 & I_2 \end{bmatrix}.$$

The new dimension is $m' = n - m = 10 - 4 = 6$. As one can see the double value of dimension $2m' = 12$ does not coincide with the code distance $d = 8$. Let $n = 3m + 2 = 14$, $m = 4$, $d = 8$. The initial three component code is

$$\begin{bmatrix} I_4 & M_{11} & M_{12} & M_{13} \\ 0_4^4 & I_4 & M_{21} & M_{22} \\ 0_4^4 & 0_4^4 & 0_4^2 & I_4 \end{bmatrix},$$

where each matrix row is the corresponding component, each of the matrices M_{11}, M_{12}, M_{21} has size 4×4, the size of each matrices M_{13} and M_2 is 4×2

The first component of the dual code is in the form

$$\begin{bmatrix} M_{11}^T & I_4 & 0_4^4 & 0_4^2 \\ M_{12}^T & 0_4^4 & I_4 & 0_4^2 \\ M_{13}^T & 0_2^4 & 0_2^4 & I_2 \end{bmatrix},$$

The second component of the dual code is in the form

$$\begin{bmatrix} I_4 & 0_4^4 & 0_4^4 & 0_4^2 \\ 0_4^4 & M_{21}^T & I_4 & 0_4^2 \\ 0_2^4 & M_{22}^T & 0_2^4 & I_2 \end{bmatrix}.$$

The third component of the dual code is in the form

$$\begin{bmatrix} I_4 & 0_4^4 & 0_4^4 & 0_4^2 \\ 0_4^4 & I_4 & 0_4^4 & 0_4^2 \\ 0_2^4 & 0_2^4 & 0_2^4 & I_2 \end{bmatrix}.$$

7.14 Conclusions

This chapter is devoted to multicomponent subspace codes. We have shown the place of these codes in random network coding. We have described the constructions and have estimated the cardinality of the codes. The efficiency of the MZP codes is defined as ratio of its cardinality to the upper bound at the same parameters. At maximum code distance, the efficiency is maximum, i.e., it is equal to 1 or near 1. It depends on the dimension. We have also demonstrated the iterative decoding algorithm.

8

Multicomponent codes based on combinatorial block designs

8.1 Introduction

A code cardinality, i.e., the number of codewords, is an important code parameter. Therefore, researches try to design multicomponent codes with large cardinality and distance d as a union of several codes having the same distance d. The cardinality of a multicomponent code is usually equal to the sum of the cardinalities of its components. Etzion and Silbershtein [ES09] show that projective spaces can be used to design multicomponent codes.

In this chapter, we will show multicomponent subspace codes, based on rank metric codes and combinatorial block designs [Hal67]. Examples of some multicomponent subspace codes will be given. Special rank metric codes with restrictions for these constructions will be considered. We also will pay attention to the decoding of multicomponent subspace codes in networks.

8.2 Reduced row echelon form of matrices

Recall that an SKK-code for network coding is a set of $k \times n$ matrices over the base field $\mathbb{F}_q$

$$\mathcal{C} = \left\{ \begin{bmatrix} I_k & M \end{bmatrix} \right\}, \tag{8.1}$$

where I_k is the identity matrix of order k, and matrix $M \in \mathcal{M}$ is a code matrix of the code $\mathcal{M}$ that consists of $k \times (n-k)$ matrices over the base field $\mathbb{F}_q$. Let $d_r(\mathcal{M})$ be *rank distance* of the code, then subspace code distance is $d(\mathcal{C}) = 2d_r(\mathcal{M})$.

Because of the identity matrix I_k, the code matrices can be seen as a particular case of matrices in reduced row echelon form. Let us consider a general case of such matrices.

Let X be a matrix of size $k \times n$ and rank k. Apply Gaussian elimination to X to obtain the matrix in *reduced row echelon form*, which satisfies:

- the leading element of a row is on the right of the leading element of the previous row;
- the leading entry in each nonzero row is a 1 (called a leading 1);
- each column containing a leading 1 has zeros in all its other entries.

Thus, a matrix in reduced row echelon form has k *ones* as leading elements and a number of neighboring *zeroes*. All the rest elements are called *free parameters*. Denote the set of free parameters by $\mathbf{a}$.

Assume that the leading element of the first row has position i_1, the leading element of the second row has position i_2, the leading element of the last k-th row has position i_k. Then $1 \le i_1 < i_2 < \cdots < i_k \le n$. The integers $i_1,\ i_2,\ \ldots,\ i_k$ and the free parameters $\mathbf{a}$ completely define the basis matrix in *reduced row echelon form.*

We call the vector $\mathbf{i} = [i_1\ i_2\ \ldots\ i_k]$ *indicator* of reduced row echelon form and denote it by (ID). The corresponding (subspace-) basis matrix is denoted by $X(\mathbf{i}, \mathbf{a})$. Let $n = 6, k = 3$, $ID = [i_1\ i_2\ i_3] = [1\ 3\ 4]$. Then the basis matrix $X(\mathbf{i}, \mathbf{a})$ for this indicator is

$$X(\mathbf{i}, \mathbf{a}) = \begin{bmatrix} 1 & a_{1,1} & 0 & 0 & a_{1,2} & a_{1,3} \\ 0 & 0 & 1 & 0 & a_{2,2} & a_{2,3} \\ 0 & 0 & 0 & 1 & a_{3,2} & a_{3,3} \end{bmatrix}.$$

This matrix has 7 free parameters $a_{i,j}$, which can be selected arbitrarily from the field $\mathbb{F}_q$. Hence, there are q^7 different 3-dimensional subspaces for this indicator.

In general case, the first row has $n - k + 1 - i_1$ free parameters, the j-th row has $n - k + j - i_j$ free parameters, $j = 1, \dots, k$. The total number of free parameters is

$$f = \sum_{i=1}^{k} f_i = nk - \frac{(k-1)k}{2} - i_1 - i_2 - \cdots - i_k. \tag{8.2}$$

From this example one can see that a code matrix of SKK code is a particular case of a matrix in reduced row echelon form with the identity matrix on the left part and a rank code matrix on the right. In other cases, columns of the identity matrix can occupy other positions, and the remaining positions can be occupied by columns of a rank code. Keep in mind that some elements of these remaining positions must be zero, the other elements, denoted by **a** in the example, are free.

8.3 Rank codes with restrictions

Consider a vector MRD $[n, k, d]$-code with generator matrix G. Let the information vector be $\mathbf{u} = (u_1, \dots, u_k)$, then the code vector is $g(\mathbf{u}) = \mathbf{u}G$, and gives code matrix

$$M(\mathbf{u}G) = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{N1} & a_{N2} & \dots & a_{Nn} \end{bmatrix}.$$

A code matrix is called *a matrix with restrictions* if $a_{ij} = 0$ for fixed positions. Rank code with such matrices is called *rank code with restrictions.*

Problem: Given a rank distance, design the rank code with restrictions.

Let us solve the problem as follows: find the restrictions on the information vectors $\mathbf{u}$, design a vector code with these restrictions and transform it to the matrix form.

8.4 Singleton bound

First we give the Singleton bound for standard rank codes, then we derive a bound for the rank metric codes with restrictions.

Let a rank metric code in matrix form consist of $|M|$ matrices of size $N \times n$, $n \leq N$, with rank distance d.

Let us obtain an upper bound for $|M|$. Every code matrix we write as $[A_i, B_i]$, $i = \overline{1, |M|}$, where matrices A_i have size $N \times (d-1)$, and matrices B_i have size $N \times (n-d+1)$). All matrices B_i are different, otherwise, if say $B_1{=}B_2$ then the code matrix $[A_1 - A_2, 0]$ has rank at most $d-1$. For the code without restrictions, every matrix B_i has $N \times (n-d+1)$ elements. Hence, the number of code words is upper bounded by $q^{N \times (n-d+1)}$, the number of different matrices B_i. Thus, the Singleton upper bound for a rank metric code is $\log_q |M| \leq N \times (n-d+1)$. The rank codes we considered before reach this bound.

Let us obtain an upper bound for the cardinality of a rank metric code with distance d and with restrictions, i.e., there are fixed positions in the code matrices that are always zero. Let us select $d-1$ columns with maximum number of free elements, move these columns to the left part of the matrix and call the submatrix A. The remaining columns we order in a way that the number of free elements decreases from left to right and denote this submatrix by B.

Denote the number of free elements in columns of A by $N_1, N_2, \ldots, N_{d-1}$, and for the matrix B by $N_d, N_{d+1}, \ldots, N_n$. We will use the same derivation as in the case without restrictions. The number of different matrices B is $q^{N_d+N_{d+1}+\ldots+N_n}$. Hence, the Singleton type bound for a code with restrictions depends on the restrictions and has the form $|M| \leq q^{N_d+N_{d+1}+\ldots+N_n}$.

Let us show by an example how to compute the bound and design a code that reaches this bound. Code parameters: $q = 2,\ n = 3,\ k = 2,\ d = 2$. The primitive polynomial to generate the field is $\alpha^3 + \alpha^2 + 1 = 0$. The generator matrix of the rank [3,2,2] code is

$$G = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{bmatrix}. \tag{8.3}$$

A code matrix with restrictions is

$$M_{\text{restrict}}(\widehat{\mathbf{u}}G) = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & a_{32} & a_{33} \end{bmatrix}. \tag{8.4}$$

To obtain the bound we transpose the matrix. The matrix A has the first column (of the transposed matrix) that has $N_1 = 3$ free elements. The matrix B has other two columns with $N_d + N_n = 2 + 2 = 4$ free elements. Hence, $|M| \le 2^4 = 16$.

Let us show that the [3,2,2] code with restricted information symbols reaches the Singleton bound. We take $1, \alpha, \alpha^2$ as the basis of the field $\mathbb{F}_{2^3}$. Transform a code matrix into the vector form $b = (b_1, b_2, b_3)$,

$$b = ((a_{11}\cdot 1 + a_{21}\cdot\alpha + a_{31}\cdot\alpha^2), (a_{12}\cdot 1 + a_{22}\cdot\alpha + a_{32}\cdot\alpha^2), (a_{13}\cdot 1 + a_{23}\cdot\alpha + a_{33}\cdot\alpha^2)).$$

Here $a_{21} = a_{31} = 0$, hence, $b_1 = a_{11}$.

For the information vector (u_1, u_2) we get the code vector (b_1, b_2, b_3)

$$(u_1, u_2)\begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{bmatrix} = ((u_1 + u_2), (u_1\alpha + u_2\alpha^2), (u_1\alpha^2 + u_2\alpha^4)),$$

where $b_1 = a_{11} = (u_1 + u_2)$, $u_2 = u_1 + a_{11}$. Let the information symbol u_1 be equal to one of $2^3 = 8$ field elements of $\mathbb{F}_{2^3}$. Since a_{11} can be 0 or 1 only, the information symbol $u_2 = u_1 + a_{11}$ takes only 2 values for fixed u_1. Thus with the restrictions on information symbols we have $2 \times 2^3 = 16$ codewords, and the restricted code reaches the Singleton type bound.

Now consider the case $d = 3$. We will use [3,1,3] rank code with generator matrix

$$G = \begin{bmatrix} 1 & \alpha & \alpha^2 \end{bmatrix}. \tag{8.5}$$

The matrix A has $d - 1 = 2$ columns, where all elements are free. The matrix B has one column, which contains *one* free element a_{11} and two zero elements, and we obtain the bound $|M| \le 2^1 = 2$.

The information vector of length 1 is (u_1). The corresponding code vector is $b = (u_1)G = (u_1, u_1\alpha, u_1\alpha^2) = (b_1, b_2, b_3)$. From the restriction (8.4) we have restriction for the information symbol $u_1 = a_{11} \in \mathbb{F}_2$. Hence, there are two code words in the restricted code, and the Singleton type bound is reached.

8.5 Combinatorial block designs

To construct multicomponent subspace codes we will use basis matrices of the subspaces in reduced row echelon form and rank metric codes with restrictions. The multicomponent code is a union of subcodes that are called *components* of the code. To guarantee a fixed subspace distance between code components, we will use combinatorial block designs [Hal67].

In combinatorial analysis, one of the problems is: place in a special way some elements in given sets. The i-th element should appear r_i times in the sets such that the j-th set contains k_j elements, and also pairs, triples and other combinations of elements should appear a fixed number of times. Such placement is called an *incidence structure* or *tactical configuration*. A particular type of such placements is *balanced incomplete block designs*. By definition, balanced incomplete block design is a placement of v different elements in b blocks, such that every block contains exactly K different elements, every element appears in r different blocks, and every pair of different elements a_i, a_j appears in exactly λ blocks. In combinatorics, balanced incomplete block designs can be called simply block designs or designs. We will mostly use the name *combinatorial block designs*.

Given the finite set $\mathcal{N} = \{1, 2, \ldots, n\}$ and integers $K, r, \lambda \geq 1$, we will build a design, called 2 B-block, as a set of subsets consisting of K elements from $\mathcal{N}$. The following conditions should be satisfied: the number r of blocks that contain $i \in \mathcal{N}$ does not depend on i, and the number λ of blocks that contain different pairs $i, j \in \mathcal{N}$ also does not depend on i, j. Here:

1. n is the number of elements in $\mathcal{N}$;
2. b is the number of blocks;
3. r is the number of blocks containing a given element from $\mathcal{N}$;
4. K is the number of elements in every block;
5. λ is the number of blocks that contain a given pair of different elements.

Such designs are defined by parameters (n, K, λ), or equivalently by (n, b, r, K, λ). It is shown in [Hal67] that these parameters are connected as follows: $bK = vr$ and $r(K-1) = \lambda(v-1)$.

Construction of a code with 7 components

Let $k = 3$, $n = 7$, $d_r = 2$. We construct subspace code will consist of 7 components and will have subspace code distance $2d_r = 4$. We use $b = 7$ blocks of block design as the following indicators of reduced echelon forms of code matrices

$$\begin{aligned} &B_1^\top = \begin{bmatrix}1\\2\\3\end{bmatrix},\ B_2^\top = \begin{bmatrix}1\\4\\5\end{bmatrix},\ B_3^\top = \begin{bmatrix}1\\6\\7\end{bmatrix},\ B_4^\top = \begin{bmatrix}2\\4\\6\end{bmatrix},\\ &B_5^\top = \begin{bmatrix}2\\5\\7\end{bmatrix},\ B_6^\top = \begin{bmatrix}3\\4\\7\end{bmatrix},\ B_7^\top = \begin{bmatrix}3\\5\\6\end{bmatrix}. \end{aligned} \tag{8.6}$$

(Every two blocks have in common exactly $\lambda = 1$ components.)

The corresponding structures of code matrices of 7 components are:

$$B_1^\top = \begin{bmatrix}1\\2\\3\end{bmatrix} \to \begin{pmatrix} 1 & 0 & 0 & a_1 & a_2 & a_3 & a_4 \\ 0 & 1 & 0 & a_5 & a_6 & a_7 & a_8 \\ 0 & 0 & 1 & a_9 & a_{10} & a_{11} & a_{12} \end{pmatrix}$$

$$B_2^\top = \begin{bmatrix}1\\4\\5\end{bmatrix} \to \begin{pmatrix} 1 & a_1 & a_2 & 0 & 0 & a_3 & a_4 \\ 0 & 0 & 0 & 1 & 0 & a_5 & a_6 \\ 0 & 0 & 0 & 0 & 1 & a_7 & a_8 \end{pmatrix}$$

$$B_3^\top = \begin{bmatrix}1\\6\\7\end{bmatrix} \to \begin{pmatrix} 1 & a_1 & a_2 & a_3 & a_4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$B_4^\top = \begin{bmatrix}2\\4\\6\end{bmatrix} \to \begin{pmatrix} 0 & 1 & a_1 & 0 & a_2 & 0 & a_3 \\ 0 & 0 & 0 & 1 & a_4 & 0 & a_5 \\ 0 & 0 & 0 & 0 & 0 & 1 & a_6 \end{pmatrix}$$

$$B_5^\top = \begin{bmatrix}2\\5\\7\end{bmatrix} \to \begin{pmatrix} 0 & 1 & a_1 & a_2 & 0 & a_3 & 0 \\ 0 & 0 & 0 & 0 & 1 & a_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$B_6^\top = \begin{bmatrix}3\\4\\7\end{bmatrix} \to \begin{pmatrix} 0 & 0 & 1 & 0 & a_1 & a_2 & 0 \\ 0 & 0 & 0 & 1 & a_3 & a_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$B_7^\top = \begin{bmatrix}3\\5\\6\end{bmatrix} \to \begin{pmatrix} 0 & 0 & 1 & a_1 & 0 & 0 & a_2 \\ 0 & 0 & 0 & 0 & 1 & 0 & a_3 \\ 0 & 0 & 0 & 0 & 0 & 1 & a_4 \end{pmatrix},$$

where a_i denotes free parameters.

Here we used a balanced incomplete block design with parameters $n = v = b = 7$, $r = K = 3$, $\lambda = 1$. The blocks B_i of the design above serve as the indicators for the 7 base matrices for the 7 components. Next, we will fill columns of matrices with free elements by columns of restricted rank code. This allows us to construct the required subspace code with subspace distance 4 as a union of the 7 component codes of cardinalities $256, 16, 1, 16, 2, 4, 2$ respectively.

The rank code distance of every component code will be at least $d_r = 2$, since we use restricted rank metric mother code with $d_r = 2$. Hence, the subspace code distance of every component code will be at least $2d_r = 4$. The minimum subspace distance between components of the code will be 4. As a result, the multicomponent code has subspace distance 4 and 297 code words, which is 16% more than the cardinality of the first component.

Below we will show code matrices of the first two components of the code.

8.5.1 Matrices of the first and the second components

Matrices of the first component code. In the example above, the first component of the multicomponent code coincides with the SKK code. Let us construct a code matrix of the subspace code for a given information vector.

The parameters of the rank code are $q = 2$, $d_r = 2$, $k = n-d_r+1 = 3-2+1 = 2$.

To design the extension field select the primitive polynomial $f(\lambda) = \lambda^4+\lambda+1$. The generator matrix of the rank code is

$$G = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{bmatrix}. \tag{8.7}$$

For information vector (u_1, u_2) compute the code vector

$$g = (u_1, u_2)G = ((u_1 + u_2), (u_1\alpha + u_2\alpha^2), (u_1\alpha^2 + u_2\alpha^4)) = (g_1, g_2, g_3).$$

Let the information symbols be $u_1 = \alpha, u_2 = \alpha^2$. Then the code vector is $g = (\alpha^5, \alpha^{10}, \alpha^2)$ and the code matrix is

$$M_1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix},$$

with the transposed matrix

$$M_1^T = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Using lifting we obtain the basis of the code subspace as rows of the matrix $X_1 = [I_3 \ \ M_1^T]$

$$X_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

The first component has $2^8 = 256$ code matrices.

Matrices of the second component code. The code parameters and the generator matrix are the same for all components: $q = 2$, $d_r = 2$, $k = n - d_r + 1 = 3 - 2 + 1 = 2$.

The indicator for the second component is

$$B_2\text{=}[1 \ 4 \ 5] \tag{8.8}$$

and the code matrices of the second component have the following structure

$$X_2 = \left[\begin{array}{ccccccc} 1 & a_{11} & a_{12} & 0 & 0 & a_{13} & a_{14} \\ 0 & 0 & 0 & 1 & 0 & a_{23} & a_{24} \\ 0 & 0 & 0 & 0 & 1 & a_{33} & a_{34} \end{array} \right], \tag{8.9}$$

hence, the structure of a code matrix of the restricted rank code is

$$M_1 = \begin{bmatrix} a_{11} & 0 & 0 \\ a_{12} & 0 & 0 \\ a_{13} & a_{23} & a_{33} \\ a_{14} & a_{24} & a_{34} \end{bmatrix}. \tag{8.10}$$

Here we have 8 free elements $a_{11}, a_{12}, a_{13}, a_{14}, a_{23}, a_{24}, a_{33}, a_{34}$. Four positions are filled by zeros $a_{21} = 0, a_{22} = 0, a_{31} = 0, a_{32} = 0$. These are restrictions. Let us design all the code matrices and all the allowed information vectors.

We use $1, \alpha, \alpha^2, \alpha^3$ as a basis of the extension field. Transform the second and the third columns of the matrix into elements g_2 and g_3 of the extension field. Using, G, we obtain for information symbols u_1, u_2 the following system of equations

$0 \cdot 1 + 0 \cdot \alpha + a_{23}\alpha^2 + a_{24}\alpha^3 = u_1\alpha + u_2\alpha^2;$
$0 \cdot 1 + 0 \cdot \alpha + a_{33}\alpha^2 + a_{34}\alpha^3 = u_1\alpha^2 + u_2\alpha^4,$
from which we get
$u_1 = a_{33}\alpha^{11} + a_{34}\alpha^{12} + a_{23}\alpha^{13} + a_{24}\alpha^{14}$
$u_2 = a_{33}\alpha^{10} + a_{34}\alpha^{11} + a_{23}\alpha^{11} + a_{24}\alpha^{12}.$

We see that four binary elements of the matrix define the information vector and, hence, the code word. Thus, there are 16 allowed information vectors out of 256 defined by 4 bits $a_{23}, a_{24}, a_{33}, a_{34}$, which can be considered as 4 information bits. Three out of the 16 allowed information vectors and corresponding 16 code matrices are listed below.

1. Let $a_{23} = a_{24} = a_{33} = a_{34} = 0$. The information vector is all-zero

$$M_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

2. Let $a_{23} = a_{24} = a_{33} = 0, a_{34} = 1$. Then $u_1 = \alpha^{12}$, $u_2 = \alpha^{11}$ and $g_1 = u_1 + u_2 = 1$, $g_2 = u_1\alpha + u_2\alpha^2 = 0$, $g_3 = u_1\alpha^2 + u_2\alpha^4 = \alpha^3$. The code vector is $g = (1\ 0\ \alpha^3)$ and the code matrix of the rank code is

$$M_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

3. Let $a_{23} = 1, a_{24} = 1, a_{33} = 1, a_{34} = 1$. Then $u_1 = \alpha^{13} + \alpha^{14} + \alpha^{11} + \alpha^{12} = \alpha^8$, $u_2 = \alpha^{11} + \alpha^{12} + \alpha^{10} + \alpha^{11} = \alpha^3$ and $g_1 = u_1 + u_2 = \alpha^{13}$, $g_2 = u_1\alpha + u_2\alpha^2 = \alpha^6$, $g_3 = u_1\alpha^2 + u_2\alpha^4 = \alpha^6$. The code vector is $g = (\alpha^{13}\ \alpha^6\ \alpha^6)$ and the code matrix

$$M_{16} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

8.6 Decoding a restricted rank code

Let us consider the decoding of the restricted rank code used in the second component. Since the restricted code is a subcode of the mother rank code, we can decode the received word by decoding the mother code using any known decoding algorithm.

Assume the code matrix M_{16} has been transmitted over a noisy channel that adds the following noise matrix of rank 1

$$M_n = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

The received corrupted matrix is

$$Y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

To start decoding we transform the received matrix to the vector form $y = (1\,0\,0)$. Using the generator matrix (8.3), let us compute a check matrix

$$H = \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix}.$$

Since the generator matrix is orthogonal to a check matrix we write $GH^T = 0$ as

$$\begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \tag{8.11}$$

and obtain the system of equations for elements of the matrix H

$$h_1 + \alpha h_2 + \alpha^2 h_3 = 0, \quad h_1 + \alpha^2 h_2 + \alpha^4 h_3 = 0. \tag{8.12}$$

Setting $h_1 = 1$ we find $h_2 = \alpha^2$ and $h_3 = \alpha^{12}$.

The syndrome of the received vector is $S = yH^T$, i.e.,

$$S = (1\ 0\ 0) \begin{pmatrix} 1 \\ \alpha^2 \\ \alpha^{12} \end{pmatrix} = 1. \tag{8.13}$$

Since the syndrome is nonzero we can detect an error during the transmission. The restricted code has code distance $d_r = 2$ like the mother code, and can detect errors but cannot correct them.

8.7 Decoding subspace code

Let us use the following matrix of restricted rank code

$$M_{16} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

to build the code matrix X_{16} of the second component, having the indicator $B = [1\ 4\ 5]$:

$$X_{16} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}. \tag{8.14}$$

Assume that the rows of the matrix X_{16} were transmitted as packets via a network with linear random network coding and the matrix received is

$$Y = AX_{16}. \tag{8.15}$$

Let the matrix A in our example be the singular matrix

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \tag{8.16}$$

then the received matrix is

$$Y = AX_{16} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{8.17}$$

Transform the matrix Y to the reduced row echelon form

$$\widetilde{Y} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{8.18}$$

The positions of leading elements in the first two rows of the matrix $\widetilde{Y}$ allow us to find two columns of the identity matrix: the first and the forth. The fifth column can be found using indicators. As a result, we have the positions of indicators $1, 4, 5$. Fixing the positions $1, 4, 5$ of the component indicators, allows us to find the channel matrix A from $\widetilde{Y}$. Let us write $A = I + L$, where

$$L = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{8.19}$$

The unindexed columns of the matrix $\widetilde{Y}$ form the matrix $A\widetilde{M}_{16}$

$$A\widetilde{M}_{16} = M_{16} + LM_{16} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{8.20}$$

Write the transposed matrices

$$M_{16}^T + M_{16}^T L^T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \tag{8.21}$$

and

$$L^T = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}. \tag{8.22}$$

Transform the matrix M_{16}^T into a vector, denoted by $(m_1\ m_2\ m_3)$. Multiply the vector by the matrix L^T: $(m_1\ m_2\ m_3)L^T = (m_3\ 0\ m_3)$. Write the syndrome using the unknown m_3 as

$$S_1 = m_3(1\ 0\ 1)\begin{pmatrix} 1 \\ \alpha^2 \\ \alpha^{12} \end{pmatrix} = m_3(1+\alpha^{12}) = m_3\alpha^{11}. \tag{8.23}$$

Transform the matrix $\widetilde{M_{16}^T}$ into the vector $y = (1\ \alpha^6\ 0)$ and compute the syndrome

$$(1\ \alpha^6\ 0)\begin{pmatrix} 1 \\ \alpha^2 \\ \alpha^{12} \end{pmatrix} = 1+\alpha^8 = \alpha^2. \tag{8.24}$$

By equating the expressions for the syndrome we obtain $m_3\alpha^{11} = \alpha^2$, i.e., $m_3 = \alpha^6$. Error in vector form is $e = (m_3\ 0\ m_3) = (\alpha^6\ 0\ \alpha^6)$. The transmitted vector is $y+e = (1+\alpha^6\ \alpha^6\ \alpha^6) = (\alpha^{13}\ \alpha^6\ \alpha^6)$ and corresponding decoded matrix is

$$M_{16} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}. \tag{8.25}$$

The decoding was correct.

Construction of a code with 13 components

Let us use a block design with parameters $n = v = b = 13$, $r = K = 4$, $\lambda = 1$ from Table 1 in [Hal67] to construct a multicomponent subspace code with subspace distance $2d_r = 6$, where code binary matrices have size $n \times r$. The rows of the following table, which are blocks of the code design, will be used as indicators for 13 components. Here every row and every column has 4 different positions.

Table of indicators (rows) of 13 components

1	2	3	4									
1				5	6	7						
1							8	9	10			
1										11	12	13
	2			5			8			11		
	2				6			9			12	
	2					7			10			13
		3		5				9				13
		3			6				10	11		
		3				7	8				12	
			4	5					10		12	
			4		6		8					13
			4			7		9		11		

As an example let us show structures of code matrices of the second and the thirteens components of the subspace code.
A code matrix of the second component has the following structure

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

A code matrix of the 13-th component has the following structure

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

Symbols a denote free elements. These free positions can be filled by elements of a code word of the restricted $[13, 11, 3]$ rank metric code over the extension field $\mathbb{F}_{2^4}$.

The number of code words in this subspace code with 13 components and subspace distance 6 is $2^{18}+2^{12}+2^6+2^0+2^6+2^4+2^2+2^3+2^4+2^5+2^3+2^4+2^5 = 266501$. Using this multicomponent construction we increase the cardinality of the first component, which is the SKK code of cardinality $2^{18} = 262144$, by less than 2%. However, the multicomponent code has 4357 additional code words.

8.8 Conclusions

We have developed the principles for building multicomponent subspace codes using combinatorial block designs and rank codes. The required parameters have been selected in such a way that the minimum subspace distances between the code components are not less than the code distance of the components. We have also elaborated the rank codes with restriction, which are required for the multicomponent codes.

9

Problems

9.1 Subgroups

Problem 1.

1. Find all subgroups of the additive group of the ring $\mathbb{Z}_{30}$. Specify which subgroups are cyclic and give generator elements for them.

2. Find the maximal multiplicative group of the ring $\mathbb{Z}_{30}$ and give all subgroups of the group.

Solution

1. An operation of addition in additive group of the ring $\mathbb{Z}_{30}$ is the addition modulo 30. The group is cyclic and consists of elements $\{0, 1, 2, \ldots, 28, 29\}$ with the generator element 1. The order of the group is 30. Orders of subgroups should divide 30, i.e., the orders are 1, 2, 3, 5, 6, 10, 15, 30. The subgroup of order 1 consists of one element 0. The subgroup of order 2 (which is cyclic with the generator element 15) consists of elements $\{0, 15\}$. The subgroup of order 3 (which is cyclic with the generator element 10) consists of elements $\{0, 10, 20\}$. The subgroup of order 5 (which is cyclic with the generator element 6) consists of elements $\{0, 6, 12, 18, 24\}$. The subgroup of order 6 (which is cyclic with the generator element 5) consists

of elements $\{0, 5, 10, 15, 20, 25\}$. The subgroup of order 10 (which is cyclic with the generator element 3) consists of elements $\{0, 3, 6, 9, 12, 15, 20, 25\}$. The subgroup of order 15 (which is cyclic with the generator element 2) consists of elements $\{0, 2, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28\}$.

2. An operation of multiplication in the ring $\mathbb{Z}_{30}$ is the multiplication modulo 30. The maximal multiplicative group consists of all elements that are co-prime with the module 30. These are $\{1, 7, 11, 13, 17, 19, 23, 29\}$. The order of the group is 8. The group is not cyclic. Orders of subgroups should divide 8, i.e., the orders are $\{1, 2, 4, 8\}$. The subgroup of order 1 consists of one element 1. There are 3 different subgroups of order 2. These are: the cyclic subgroup $\{1, 11\}$ with the generator element 11; the cyclic subgroup $\{1, 19\}$ with the generator element 19; the cyclic subgroup $\{1, 29\}$ with the generator element 29. The are 3 different subgroups of order 4. These are: the cyclic subgroup $\{1, 7, 19, 13\}$ with the generator element 7; the cyclic subgroup $\{1, 17, 19, 23\}$ with the generator element 17; the subgroup $\{1, 11, 19, 29\}$ (which is the product of two different subgroups of order 2 with the generator elements 11 and 19).

Problem 2.

1. Find all subgroups of the additive group of the ring $\mathbb{Z}_{19}$ and specify the generator elements for the subgroups.
2. Show that the maximal multiplicative group of the ring $\mathbb{Z}_{19}$ is cyclic and find all the generator elements. Give all subgroups of the group.

Solution

1. An operation of addition in the additive group of the ring $\mathbb{Z}_{19}$ is the addition modulo 19. The group is cyclic and consists of the elements $\{0, 1, 2, \ldots, 17, 18\}$. A generator element is any nonzero element of the group. Since the order 19 of the group is prime, there are two subgroups: the group itself and $\{0\}$.
2. The operation of multiplication in the ring $\mathbb{Z}_{19}$ is the multiplication modulo 19. The maximal multiplicative group consists of all elements that are co-prime with the module 19. These are all nonzero elements $\{1, 2, 3, \ldots, 17, 18\}$. The order of the group is 18. The order of the subgroup $\{18, 9, 6, 3, 2, 1\}$ divides 18. The maximal group of order 18 is cyclic.

A generator element is, e.g., 2. Indeed, all 18 powers $2, 2^2, 2^3, \ldots, 2^{17}, 2^{18}$ are different modulo 18. Other generator elements are $3, 10, 13, 14, 15$. The subgroup of order 9 is cyclic with the generator element 4. The subgroup of order 6 is cyclic with the generator element 8. The subgroup of order 3 is cyclic with the generator element 7. The subgroup of order 2 is cyclic and consists of elements $\{18, 1\}$. The subgroup of order 1 has only one element 1.

Problem 3.

Find the greatest common divisor of the polynomials $r_1(x)$ and $r_2(x)$ in the ring GF(2)[x].
$r_1(x) = x^7 + x^5 + x^4 + x^3 + x$,
$r_2(x) = x^{14} + x^{12} + x^8 + x^6 + x^5 + x^4 + 1$.

Solution
$r(x) = x^2 + x + 1$.

Problem 4.

Find the greatest common divisor of the polynomials $r_1(x)$ and $r_2(x)$ in the ring GF(2)[x], where
$r_1(x) = x^{10} + x^9 + x^7 + x^6 + x^5 + x^2 + 1$,
$r_2(x) = x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^9 + x^6 + x^4 + x^2 + x + 1$.

Solution
$r(x) = x^3 + x^2 + 1$.

9.2 Rank codes

Problem 1.

Consider linearized polynomials $r_1 = \alpha x + \alpha^4 x^2$, $r_2 = \alpha^3 x + \alpha^8 x^2$ over the field $GF(2^4)$, generated by the irreducible polynomial $x^4 + x^3 + 1$. Find linearized polynomials $r_1 + r_2, r_1 * r_2, r_2 * r_1$.

Problem 2.

The check matrix of the rank code of length $n = 3$ with code distance $d = 3$ over $GF(2^3)$ is

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{bmatrix},$$

where α is a root of the polynomial $\varphi(x) = x^3 + x^2 + 1$. Find a generator matrix of the code.

Let a code word *matrix* V has been transmitted. Decode the received matrix

$$Y = V + E = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

assuming that the error matrix E has rank 1.

Solution

1. Build the table of the field generted by $x^3 + x^2 + 1$:

0	$1 = \alpha^0$	α	α^2	α^3	α^4	α^5	α^6
0	1	α	α^2	$1+\alpha^2$	$1+\alpha+\alpha^2$	$1+\alpha$	$\alpha+\alpha^2$

.

2. Find a generator matrix $G = \begin{bmatrix} g_1 & g_2 & g_3 \end{bmatrix}$ using the equation

$$GH^\top = 0.$$

Let $g_1 = 1$, then $g_2 = \alpha^3, g_3 = \alpha^4$, and

$$G = \begin{bmatrix} 1 & \alpha^3 & \alpha^4 \end{bmatrix}.$$

3. Transform the matrix Y into the vector form:

$$Y = V + E = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix} \Rightarrow \mathbf{y} = \mathbf{v} + \mathbf{e} = \begin{bmatrix} \alpha^6 & 1 & \alpha^3 \end{bmatrix}.$$

4. The error vector of rank 1 can be written as

$$\mathbf{e} = e_1 \begin{bmatrix} u_1 & u_2 & u_3 \end{bmatrix} = e_1 U,$$

where $e_1 \in GF(2^3)$, $u_i \in GF(2)$.

5. Compute the syndrome vector $\mathbf{y}H^\top = (\mathbf{v}+\mathbf{e})H^\top = \mathbf{e}H^\top$:

$$\begin{aligned} \mathbf{y}H^\top &= \begin{bmatrix} s_0 & s_1 \end{bmatrix} = \begin{bmatrix} \alpha^3 & \alpha^6 \end{bmatrix} \\ &= e_1 \begin{bmatrix} 1 \cdot u_1 + \alpha u_2 + \alpha^2 u_3 & 1^2 \cdot u_1 + \alpha^2 u_2 + \alpha^4 u_3 \end{bmatrix} \\ &= e_1 [x_1 \; x_1^2]. \end{aligned}$$

6. Get the system of equations

$$\begin{aligned} \alpha^3 &= e_1 x_1, \\ \alpha^6 &= e_1 x_1^2. \end{aligned}$$

Here $x_1 = \frac{s_1}{s_0} = \alpha^3$, $e_1 = \frac{s_0}{x_1} = 1$.

7. Find

$$x_1 = \alpha^3 = 1 \cdot 1 + \alpha \cdot 0 + \alpha^2 \cdot 1 = 1 \cdot u_1 + \alpha \cdot u_2 + \alpha^2 \cdot u_3.$$

The error vector is

$$\mathbf{e} = e_1 \begin{bmatrix} u_1 & u_2 & u_3 \end{bmatrix} = 1 \cdot \begin{bmatrix} 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \end{bmatrix}.$$

The output of decoding is the code vector

$$\mathbf{v} = \mathbf{y} + \mathbf{e} = \begin{bmatrix} \alpha^6 + 1 & 1 + 0 & \alpha^4 + \alpha^3 + 1 \end{bmatrix} = \begin{bmatrix} \alpha^4 & 1 & \alpha \end{bmatrix}.$$

Problem 3.

The check matrix of the rank code of length $n = 3$ with code distance $d = 3$ over $GF(2^3)$ is

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{bmatrix},$$

where α is a root of the polynomial $\varphi(x) = x^3 + x^2 + 1$. Find a generator matrix of the code.

A code vector $\mathbf{v}$ has been transmitted. Decode $\mathbf{y} = \mathbf{v} + \mathbf{e} = \begin{bmatrix} \alpha^5 & 0 & \alpha^6 \end{bmatrix}$ assuming that rank af the error vector $\mathbf{e}$ is 1.

Solution

1. Build the table of the field generated by $x^3 + x^2 + 1$:

0	$1 = \alpha^0$	α	α^2	α^3	α^4	α^5	α^6
0	1	α	α^2	$1+\alpha^2$	$1+\alpha+\alpha^2$	$1+\alpha$	$\alpha+\alpha^2$

.

2. Find a generator matrix $G = \begin{bmatrix} g_1 & g_2 & g_3 \end{bmatrix}$ using the equation

$$GH^\top = 0.$$

Let $g_1 = 1$, then $g_2 = \alpha^3, g_3 = \alpha^4$, and

$$G = \begin{bmatrix} 1 & \alpha^3 & \alpha^4 \end{bmatrix}.$$

3. Write the error vector of rank 1 as

$$\mathbf{e} = e_1 \begin{bmatrix} u_1 & u_2 & u_3 \end{bmatrix} = e_1 U,$$

where $e_1 \in GF(2^3)$, $u_i \in GF(2)$.

4. Compute the syndrome $\mathbf{y}H^\top = (\mathbf{v} + \mathbf{e})H^\top == \mathbf{e}H^\top$:

$$\begin{aligned} \mathbf{y}H^\top &= \begin{bmatrix} s_0 & s_1 \end{bmatrix} = \begin{bmatrix} 1 & \alpha^6 \end{bmatrix} \\ &= e_1 \begin{bmatrix} 1 \cdot u_1 + \alpha u_2 + \alpha^2 u_3 & 1^2 \cdot u_1 + \alpha^2 u_2 + \alpha^4 u_3 \end{bmatrix} \\ &= e_1 [x_1 \; x_1^2]. \end{aligned}$$

5. We obtain the system of equations

$$\begin{aligned} 1 &= e_1 x_1, \\ \alpha^6 &= e_1 x_1^2. \end{aligned}$$

Here $x_1 = \frac{s_1}{s_0} = \alpha^6$, $e_1 = \frac{s_0}{x_1} = \alpha$.

6. Find

$$x_1 = \alpha^6 = 1 \cdot 0 + \alpha \cdot 1 + \alpha^2 \cdot 1 = 1 \cdot u_1 + \alpha u_2 + \alpha^2 u_3.$$

The error vector is

$$\mathbf{e} = e_1 \begin{bmatrix} u_1 & u_2 & u_3 \end{bmatrix} = \alpha \begin{bmatrix} 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & \alpha & 0\alpha \end{bmatrix}.$$

The output of the decoder is the code vector

$$\mathbf{v} = \mathbf{y} + \mathbf{e} = \begin{bmatrix} \alpha^5 + 0 & 0 + \alpha & \alpha^6 + \alpha \end{bmatrix} = \begin{bmatrix} \alpha^5 & \alpha & \alpha^2 \end{bmatrix}.$$

Problem 4.

The check matrix of the rank code of length $n = 3$ with code distance $d = 3$ over $GF(2^3)$ is

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{bmatrix},$$

where α is a root of the polynomial $\varphi(x) = x^3 + x^2 + 1$. Find a generator matrix of the code.

A code vector $\mathbf{v}$ has been transmitted.

Decode $\mathbf{y} = \mathbf{v} + \mathbf{e} = \begin{bmatrix} \alpha^3 & 1 & 0 \end{bmatrix}$ assuming that the rank of error vector $\mathbf{e}$ is 1.

Solution

1. Build the table of the field generated by $x^3 + x^2 + 1$:

0	$1 = \alpha^0$	α	α^2	α^3	α^4	α^5	α^6
0	1	α	α^2	$1 + \alpha^2$	$1 + \alpha + \alpha^2$	$1 + \alpha$	$\alpha + \alpha^2$

2. Find a generator matrix $G = \begin{bmatrix} g_1 & g_2 & g_3 \end{bmatrix}$ using the equation

$$GH^\top = 0.$$

Let $g_1 = 1$, then $g_2 = \alpha^3, g_3 = \alpha^4$, and

$$G = \begin{bmatrix} 1 & \alpha^3 & \alpha^4 \end{bmatrix}.$$

3. The error vector of rank 1 write as

$$\mathbf{e} = e_1 \begin{bmatrix} u_1 & u_2 & u_3 \end{bmatrix} = e_1 U,$$

where $e_1 \in GF(2^3)$, $u_i \in GF(2)$.

4. Compute the syndrome $\mathbf{y}H^\top = (\mathbf{v} + \mathbf{e})H^\top = \mathbf{e}H^\top$:

$$\begin{aligned} \mathbf{y}H^\top &= \begin{bmatrix} s_0 & s_1 \end{bmatrix} = \begin{bmatrix} 1 & \alpha^6 \end{bmatrix} \\ &= e_1 \begin{bmatrix} 1 \cdot u_1 + \alpha u_2 + \alpha^2 u_3 & 1^2 \cdot u_1 + \alpha^2 u_2 + \alpha^4 u_3 \end{bmatrix} \\ &= e_1 [x_1 \; x_1^2]. \end{aligned}$$

5. Obtain the system of equations

$$\begin{aligned} 1 &= e_1 x_1, \\ \alpha^6 &= e_1 x_1^2. \end{aligned}$$

Here $x_1 = \frac{s_1}{s_0} = \alpha^6$, $e_1 = \frac{s_0}{x_1} = \alpha$.

6. Find

$$x_1 = \alpha^6 = 1 \cdot 0 + \alpha \cdot 1 + \alpha^2 \cdot 1 = 1 \cdot u_1 + \alpha u_2 + \alpha^2 u_3.$$

The error vector is

$$\mathbf{e} = e_1 \begin{bmatrix} u_1 & u_2 & u_3 \end{bmatrix} = \alpha \begin{bmatrix} 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & \alpha & 0\alpha \end{bmatrix}.$$

The output of the decoder is the code vector

$$\mathbf{v} = \mathbf{y} + \mathbf{e} = \begin{bmatrix} \alpha^5 + 0 & 0 + \alpha & \alpha^6 + \alpha \end{bmatrix} = \begin{bmatrix} \alpha^5 & \alpha & \alpha^2 \end{bmatrix}.$$

9.3 q-cyclic codes

Problem 1.

Let $q = 2,\ m = 3$. Consider the ring of linearized polynomials over the field $\mathbb{F}_{q^m} = \mathbb{F}_8$. Let α be a primitive element of the field that satisfies $\alpha^3 + \alpha + 1 = 0$. Let us write the binomial $x^{q^3} - x$ as $x^{q^3} - x = H_1 \otimes G_1$, where $H_1(x) = x^q + \alpha x,\ G_1(x) = x^{q^2} + \alpha^4 x^q + \alpha^6 x$. Factorize the binomial $x^{[12]} - x$ as follows

$$\begin{aligned} x^{[12]} - x &= (x^{q^3} - x) \otimes (x^{q^3} - x) \otimes (x^{q^3} - x) \otimes (x^{q^3} - x) \\ &= H_1 \otimes G_1 \otimes H_1 \otimes G_1 \otimes H_1 \otimes G_1 \otimes H_1 \otimes G_1 \\ &= H_1 \otimes G_1 \otimes H_1 \otimes G_1 \otimes H_1 \otimes H_1 \otimes G_1 \otimes G_1 \\ &= H \otimes G, \end{aligned}$$

where

$$\begin{aligned} &H = H_1 \otimes G_1 \otimes H_1 \otimes G_1 \otimes H_1 \otimes H_1, \\ &G = G_1 \otimes G_1 = x^{q^4} + \alpha x^{q^3} + x^{q^2} + \alpha^5 x^q + \alpha^5 x. \end{aligned}$$

Build a q-cyclic code of length 12, then a 3-shortened q-cyclic code. Using this code build a 6-shortened q-cyclic code that is also a pseudo-cyclic code.

Solution

Let us build a q-cyclic code of length $4m = 12$ using the polynomial $G(x)$. A generator matrix of the code is as follows

$$\mathbf{G}=\begin{pmatrix}\alpha^5&\alpha^5&1&\alpha&1&0&0&0&0&0&0&0\\0&\alpha^3&\alpha^3&1&\alpha^2&1&0&0&0&0&0&0\\0&0&\alpha^6&\alpha^6&1&\alpha^4&1&0&0&0&0&0\\0&0&0&\alpha^5&\alpha^5&1&\alpha&1&0&0&0&0\\0&0&0&0&\alpha^3&\alpha^3&1&\alpha^2&1&0&0&0\\0&0&0&0&0&\alpha^6&\alpha^6&1&\alpha^4&1&0&0\\0&0&0&0&0&0&\alpha^5&\alpha^5&1&\alpha&1&0\\0&0&0&0&0&0&0&\alpha^3&\alpha^3&1&\alpha^2&1\end{pmatrix}.$$

By deleting the last three rows and the last three columns in the matrix $\mathbf{G}$ we obtain a generator matrix $\mathbf{G}_1$ of 3-shortened q-cyclic code of length $3m=9$:

$$\mathbf{G}_1=\begin{pmatrix}\alpha^5&\alpha^5&1&\alpha&1&0&0&0&0\\0&\alpha^3&\alpha^3&1&\alpha^2&1&0&0&0\\0&0&\alpha^6&\alpha^6&1&\alpha^4&1&0&0\\0&0&0&\alpha^5&\alpha^5&1&\alpha&1&0\\0&0&0&0&\alpha^3&\alpha^3&1&\alpha^2&1\end{pmatrix}.$$

This code is also a pseudo-q-cyclic code of length $3m=9$, generated by the same polynomial $G(x)$ in the factor-ring $\mathbb{L}_m(f_1(x))[x]=\mathbb{R}_m[x]/f_1(x)$, where

$$\begin{aligned}f_1(x)&=(x^{q^3}-x)\otimes(x^{q^3}-x)\otimes(x^{q^3}-x)\\&=x^{[9]}+x^{[6]}+x^{q^3}+x.\end{aligned}$$

By deleting the last three rows and the last three columns in the matrix $\mathbf{G}_1$ we obtain a generator matrix $\mathbf{G}_2$ of a 6-shortened q-cyclic code of length 6:

$$\mathbf{G}_2=\begin{pmatrix}\alpha^5&\alpha^5&1&\alpha&1&0\\0&\alpha^3&\alpha^3&1&\alpha^2&1\end{pmatrix}.$$

This code is also a pseudo-q-cyclic code of length $2m=6$, generated by the same polynomial $G(x)$ in the factor-ring $\mathbb{L}_m(f_2(x))[x]=\mathbb{R}_m[x]/f_2(x)$, where

$$\begin{aligned}f_2(x)&=(x^{q^3}-x)\otimes(x^{q^3}-x)\\&=x^{[6]}+x.\end{aligned}$$

This code is a q-cyclic code of length 6. In this problem, we analyzed sm-shortened q-cyclic codes for $q=2,\ m=3,\ s=4,\ s=1,2$. However, if the shortening is not a multiple of m, then we can not obtain shortened cyclic or pseudo-q-cyclic codes. *Remark.* Consider, e.g., an 8-shortened q-cyclic code of length 5 and dimension 1. It has a generator matrix

$$\mathbf{G}_3 = \begin{pmatrix} \alpha^5 & \alpha^5 & 1 & \alpha & 1 \end{pmatrix}.$$

This code of length 5 is neither a q-cyclic nor a pseudo-q-cyclic code.

9.4 Fast decoding algorithms

Problem 1.

The check matrix of a rank code is

$$\mathbf{H}_4 = \begin{bmatrix} \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^{16} & \alpha^{32} & \alpha^{64} \\ \alpha^2 & \alpha^4 & \alpha^8 & \alpha^{16} & \alpha^{32} & \alpha^{64} & \alpha \\ \alpha^4 & \alpha^8 & \alpha^{16} & \alpha^{32} & \alpha^{64} & \alpha & \alpha^2 \\ \alpha^8 & \alpha^{16} & \alpha^{32} & \alpha^{64} & \alpha & \alpha^2 & \alpha^4 \end{bmatrix},$$

where α is a root of an irreducible polynomial of degree 7.

Let the received matrix be

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

Find the error matrix and the transmitted matrix assuming that the rank of the error matrix is at most 2.

9.5 Symmetric rank codes

Problem 1.

Find symmetric matrices that generate the fields $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$.

9.6 Rank codes in network coding

Problem 1.

A subspace code $\mathcal{X}$ is defined by the set of base matrices

$$\mathcal{X} = \left\{ \mathbf{X} : \mathbf{X} = \begin{bmatrix} \mathbf{I}_n & \mathbf{M} \end{bmatrix} \right\},$$

where $\mathbf{I}_n$ is the identity matrix of order n, and $\mathbf{M}$ is an $n \times m$ matrix of a matrix code $\mathcal{M}$ with a rank distance d. Find the subspace distance of the code $\mathcal{X}$.

9.7 Codes based on combinatorial block designs

Problem 1.

Let the parameters of the block design be $v = 9$, $n = b = 12$, $r = 4, K = 3$, $\lambda = 1$. The i-th row of Table 9.1 gives indicators of the i-th component of the code. Design these 12 components and find their cardinalities.

Table 9.1: Table of indicators of 12 components

1	2	3						
			4	5	6			
						7	8	9
1			4			7		
	2			5			8	
		3			6			9
1				5				9
	2				6	7		
		3	4				8	
1					6		8	
	2		4					9
		3		5		7		

Problem 2.

Let the parameters of the block design be $n = v = b = 13, r = K = 4, \lambda = 1$. The i-th row of Table 9.2 gives indicators of the i-th component of the code.

Table 9.2: Table of indicators of 13 components

1	2	3	4									
1				5	6	7						
1							8	9	10			
1										11	12	13
	2			5			8			11		
	2				6			9			12	
	2					7			10			13
		3		5				9				13
		3			6				10	11		
		3				7	8				12	
			4	5					10		12	
			4		6		8					13
			4			7		9		11		

Design these 13 components and find their cardinalities.

Epilogue

This monograph presents the main results related to rank metric codes, obtained so far by the author of the book and by other authors. It is shown that rank codes can be successfully applied in multichannel communication systems, in network coding and for information protection against unauthorized use. The work of the following authors deserves special attention: Kötter (Germany), Kschischang (Canada), and Silva (Brazil). Their joint works [KK08], [SKK08] in 2007-2008 created new subspace codes for random network coding. They use the so-called lifting principle, where an identity matrix is concatenated with a matrix of a rank code as if the former matrix had lifted the letter up. Because of this principle, these codes are sometimes called lifted codes. The merit of creating these new codes, which are characterized by high cardinality, belongs entirely to these three authors. Following these authors, the works of Bossert and Gabidulin [GB08], [GB09] increased the power of these codes and brought them to the upper limit. Over a series of papers, these authors introduced and elaborated the concept of subspace multicomponent codes. Here, these results are presented.

The theory of rank codes is developing successfully. New designs are being created. The constructions of Kshevetskiy-Gabidulin [KG05] are among them. New rank codes have been published by Irish scientist Sheekey [She16]. Research in this area is being carried out in Germany, Turkey, Switzerland and other countries. It is generally agreed that the new codes can be used in cryptosystems to increase security.

The development of rank coding theory is also reflected in a series of papers by Sidorenko with coauthors [SJB11], [LSS14], where the new codes are called interleaved rank metric codes. They improve the correcting ability of Gabidulin codes.

Bibliography

[ALR18] D. Augot, P. Loidreau, and G. Robert, "Generalized Gabidulin codes over fields of any characteristic," *Des. Codes Cryptogr.*, vol. 86, no. 8, pp. 1807–1848, 2018.

[ANLY00] R. Ahlswede, Ning Cai, S. . R. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.

[Bar17] H. Bartz, "Decoding of subspace and rank-metric codes," Ph.D. dissertation, Technical University of Munich, Munich, Germany, 2017.

[Beu75] A. Beutelspacher, "Partial spreads in finite projective spaces and partial designs," *Math. Z.*, vol. 145, pp. 211–229, 1975.

[BN06] A. Barg and D. Nogin, "Spectral approach to linear programming bounds on codes," *Probl Inf Transm*, vol. 42, pp. 77–89, 2006.

[BU09] D. Boucher and F. Ulmer, "Coding with skew polynomial rings," *Journal of Symbolic Computation*, vol. 44, no. 12, pp. 1644–1656, 2009.

[Cec84] P. Ceccherini, " A q-analogous of the characterization of hypercubes as graphs," *J. of Geometry*, vol. 22, pp. 57–74, 1984.

[Coo97] B. Cooperstein, "External flats to varieties in pg(mn,n(gf(q))),"*Linear Algebra and its Applications*, vol. 267, pp. 175 – 186, 1997.

[CW13] J. Cruz and W. Willems, "On network codes and partial spreads," in *Seventh International Workshop on Optimal Codes and Related Topics*, Albena, Bulgaria, 2013, pp. 77–78.

[Del76] P. Delsarte, "Association schemes and t-designs in regular semilattices," *Journal of Combinatorial Theory, Series A*, vol. 20, no. 2, pp. 230 – 243, 1976.

[Del78] ——, "Bilinear Forms over a Finite Field, with Applications to Coding Theory," *Journal of Combinatorial Theory, Series A*, vol. 25, no. 3, pp. 226–241, 1978.

[DF79] D. Drake and J. Freeman, "Partial t-spreads and group constructible s, r, μ-nets," *J. Geom.*, vol. 13, no. 2, pp. 210–216, 1979.

[ES09] T. Etzion and N. Silberstein, "Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 2909–2919, 2009.

[EZJS$^+$10] S. El-Zanati, H. Jordon, G. F. Seelinger, P. Sissokho, and L. E. Spence, "The maximum size of a partial 3-spread in a finite vector space over GF(2)," *Designs, Codes and Cryptography*, vol. 54, pp. 101–107, 2010.

[GA86] E. Gabidulin and V. Afanasyev, *Coding in radio-electronics (in Russian).* Moscow, Russia: Radio and Svyaz, 1986.

[Gab85] E. M. Gabidulin, "Theory of Codes with Maximum Rank Distance," *Probl. of Inform. Transm.*, vol. 21, no. 1, pp. 1–12, Jul 1985.

[Gab92] ——, "A fast matrix decoding algorithm for rank-error-correcting codes," in *Algebraic Coding*, G. Cohen, A. Lobstein, G. Zémor, and S. Litsyn, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992, pp. 126–133.

[Gan67] F. Gantmacher, *The Theory of Matrices (in Russian).* Nauka, Moscow, 1967.

[GB08] E. Gabidulin and M. Bossert, "Codes for network coding," in *Proc. ISIT*, Toronto, Canada, 2008, pp. 867–870.

[GB09] ——, "A family of algebraic codes for network coding," in *Proc. ISIT*, Seoul, Korea, 2009.

[GL08] E. Gabidulin and P. Loidreau, "Properties of subspace subcodes of Gabidulin codes," *Adv. Math. Commun.*, vol. 2, pp. 147–157, 2008.

[GOHA03] E. M. Gabidulin, A. V. Ourivski, B. Honary, and B. Ammar, “Reducible rank codes and their applications to cryptography,” *IEEE Transactions on Information Theory*, vol. 49, no. 12, pp. 3289–3293, 2003.

[GP02] E. Gabidulin and N. Pilipchuk, “Representation of a finite field by symmetric matrices and applications,” in *Proc. Eighth Int. Workshop on Algebraic and Combinatorial Coding Theory*, Tsarskoe Selo, Russia, 2002, pp. 120–123.

[GP04] ——, “Symmetric Rank Codes,” *Problems of Information Transmission*, vol. 40, pp. 103–117, 2004.

[GP06] E. M. Gabidulin and N. I. Pilipchuk, “Symmetric matrices and codes correcting rank errors beyond the $(d-1)/2$ bound,” *Discrete Applied Mathematics*, vol. 154, no. 2, pp. 305 – 312, 2006.

[GP08] ——, “Error and erasure correcting algorithms for rank codes,” *Designs, Codes and Cryptography*, vol. 49, no. 1, pp. 105–122, Dec 2008.

[GP16] E. Gabidulin and N. Pilipchuk, “Multicomponent codes with maximal code distance,” *Probl. Inform. Transm.*, vol. 52, pp. 84–91, 2016.

[GP17a] ——, “Cardinality of multicomponent zero prefix spreads,” in *Proceeding of Workshop on Coding and Cryptography*, Moscow, Russia, 2017.

[GP17b] ——, “Cardinality of subspace multicomponent codes,” in *Proc. of Fourth International Conference on Engineering and Telecommunications (En&T)*, Moscow, Russia, 2017, pp. 11–14.

[GPT92] E. Gabidulin, A. Paramonov, and O. Tretjakov, “Rank errors and rank erasures correcting,” in *Proc.4th Int. Colloquium on Coding Theory*, Dilijan, Yerevan, Armenia, 1992, pp. 11–19.

[GR92] E. M. Gabidulin and R. M. Roth, “Comments on "Maximum-rank arrays codes and their application to crisscross error correction" [with reply],” *IEEE Transactions on Information Theory*, vol. 38, no. 3, p. 1183, 1992.

[GR18] E. Gorla and A. Ravagnani, *Codes Endowed with the Rank Metric*. Cham: Springer International Publishing, 2018, pp. 3–23.

[GX12] V. Guruswami and C. Xing, “List Decoding Reed–Solomon, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound,” *Electr. Colloq. Comp. Complexity*, vol. 19, no. 146, 2012.

[GY08] M. Gadouleau and Z. Yan, “Packing and covering properties of rank metric codes,” *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 3873–3883, 2008.

[Hal67] M. Hall, *Combinatorial Theory*, ser. Blaisdell book in pure and applied mathematics. Wiley, 1967.

[HKK18] T. Honold, M. Kiermaier, and S. Kurz, “Partial spreads and vector space partitions,” *Signals and Communication Technology*, pp. 131–170, 2018.

[HTR18] A.-L. Horlemann-Trautmann and J. Rosenthal, “Constructions of constant dimension codes,” in *Network coding and subspace designs*, ser. Signals and Communication Technology, M. Greferath, M. O. Pavčević, N. Silberstein, and M. Á. Vázquez-Castro, Eds. Cham: Springer, Januar 2018, pp. 25–42.

[Hua51] L.-K. Hua, “A theorem on matrices over a sfield and its applications,” *Acta Mathematica Sinica*, vol. 1, no. 2, pp. 109–163, 1951.

[KG05] A. Kshevetskiy and E. Gabidulin, “The new construction of rank codes,” in *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.*, 2005, pp. 2105–2108.

[KK08] R. Koetter and F. Kschischang, “Coding for Errors and Erasures in Random Network Coding,” *Inform. Theory, IEEE Trans. on*, vol. 54, no. 8, pp. 3579–3591, Aug. 2008.

[Kur16] S. Kurz, “Improved upper bounds for partial spreads,” *Designs, Codes and Cryptography*, vol. 85, no. 1, pp. 97–106, Oct 2016.

[Kur17] ——, “Packing vector spaces into vector spaces,” *The Australian Journal of Combinatorics*, vol. 68, no. 1, pp. 122–130, March 2017.

[LGB03] P. Lusina, E. Gabidulin, and M. Bossert, “Maximum rank distance codes as space-time codes,” *IEEE Transactions on Information Theory*, vol. 49, no. 10, pp. 2757–2760, 2003.

[Li15] W. Li, “Decoding evaluation codes and their interleaving,” Ph.D. dissertation, University of Ulm, Ulm, Germany, 2015.

[LN83] R. Lidl and H. Niederreiter, *Finite Fields*, ser. Encyclopedia of mathematics and its applications. Addison-Wesley, Advanced Book Program/World Science Division, 1983.

[LO06] P. Loidreau and R. Overbeck, “Decoding rank errors beyond the error correcting capability,” in *Proc. Int. Workshop on Algebraic and Combinatorial Coding Theory*, 2006, pp. 186–190.

[LSS14] W. Li, V. Sidorenko, and D. Silva, “On transform-domain error and erasure correction by Gabidulin codes,” *Designs, Codes and Cryptography*, vol. 73, pp. 571–586, 2014.

[LTZ18] G. Lunardon, R. Trombetti, and Y. Zhou, “Generalized twisted Gabidulin codes,” *Journal of Combinatorial Theory, Series A*, vol. 159, pp. 79–106, Oct 2018.

[Mar17] U. Martínez-Peñas, “On the roots and minimum rank distance of skew cyclic codes,” *Designs, Codes and Cryptography*, vol. 83, no. 3, pp. 639–660, 2017.

[Moo96] E. Moore, “A two-fold generalization of Fermat’s theorem,” *Bull. Amer. Math. Soc.*, vol. 2, no. 7, pp. 189–199, 04 1896.

[MV19] H. Mahdavifar and A. Vardy, “Algebraic list-decoding in projective space: Decoding with multiplicities and rank-metric codes,” *IEEE Transactions on Information Theory*, vol. 65, no. 2, pp. 1085–1100, 2019.

[Ner20] A. Neri, “Systematic encoders for generalized Gabidulin codes and the q-analogue of Cauchy matrices,” *Linear Algebra and its Applications*, vol. 593, pp. 116–149, 2020.

[OÖ16] K. Otal and F. Özbudak, “Explicit constructions of some non-Gabidulin linear maximum rank distance codes,” *Advances in Mathematics of Communications*, vol. 10, 2016.

[OÖ17] ——, “Additive rank metric codes,” *IEEE Transactions on Information Theory*, vol. 63, no. 1, pp. 164–168, 2017.

[PRLS17] S. Puchinger, J. Rosenkilde né Nielsen, W. Li, and V. Sidorenko, “Row Reduction Applied to Decoding of Rank-Metric and Subspace Codes,” *Designs, Codes and Cryptography*, vol. 82, no. 1-2, pp. 389–409, 2017.

[PRS17] S. Puchinger, J. Rosenkilde né Nielsen, and J. Sheekey, “Further generalisations of twisted Gabidulin codes,” in *Proceedings of International Workshop on Coding and Cryptography*, 2017.

[Puc18] S. Puchinger, “Construction and decoding of evaluation codes in Hamming and rank metric,” Ph.D. dissertation, University of Ulm, Ulm, Germany, 2018.

[Rot91] R. M. Roth, “Maximum-Rank Array Codes and their Application to Crisscross Error Correction,” *IEEE Transactions on Information Theory*, vol. 37, no. 2, pp. 328–336, 1991.

[Sag10] Y. L. Sagalovich, *Introduction to algebraic codes (in Russian).* IITP RAS, Moscow, Russia, 2010.

[Seg64] B. Segre, “Teoria di Galois fibrazioni proettive e geometric non desarguesiane,” *Ann. Mat. pura appl.*, vol. 64, pp. 1–76, 1964.

[She16] J. Sheekey, “A new family of linear maximum rank distance codes,” *Advances in Mathematics of Communications*, vol. 10, pp. 475–488, 2016.

[SJB11] V. Sidorenko, L. Jiang, and M. Bossert, “Skew-Feedback Shift-Register Synthesis and Decoding Interleaved Gabidulin Codes,” *Inform. Theory, IEEE Trans. on*, vol. 57, no. 2, pp. 621–632, Feb. 2011.

[SKK08] D. Silva, F. Kschischang, and R. Koetter, “A Rank-Metric Approach to Error Control in Random Network Coding,” *Inform. Theory, IEEE Trans. on*, vol. 54, no. 9, pp. 3951–3967, Sep. 2008.

[SN17a] P. Sissokho and E. Nastase, “The maximum size of a partial spread II: Upper bounds,” *Discrete Math.*, vol. 340, pp. 1481–1487, 2017.

[SN17b] ——, “The maximum size of a partial spread in a finite projective space,” *J.Combin.Theory Ser.A.*, vol. 152, pp. 122–130, 2017.

[WXSN03] H. Wang, C. Xing, and R. Safavi-Naini, “Linear authentication codes: bounds and constructions,” *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 866–872, 2003.

[WZ13] A. Wachter-Zeh, “Decoding of block and convolutional codes in rank metric,” Ph.D. dissertation, University of Ulm, Ulm, Germany, 2013.