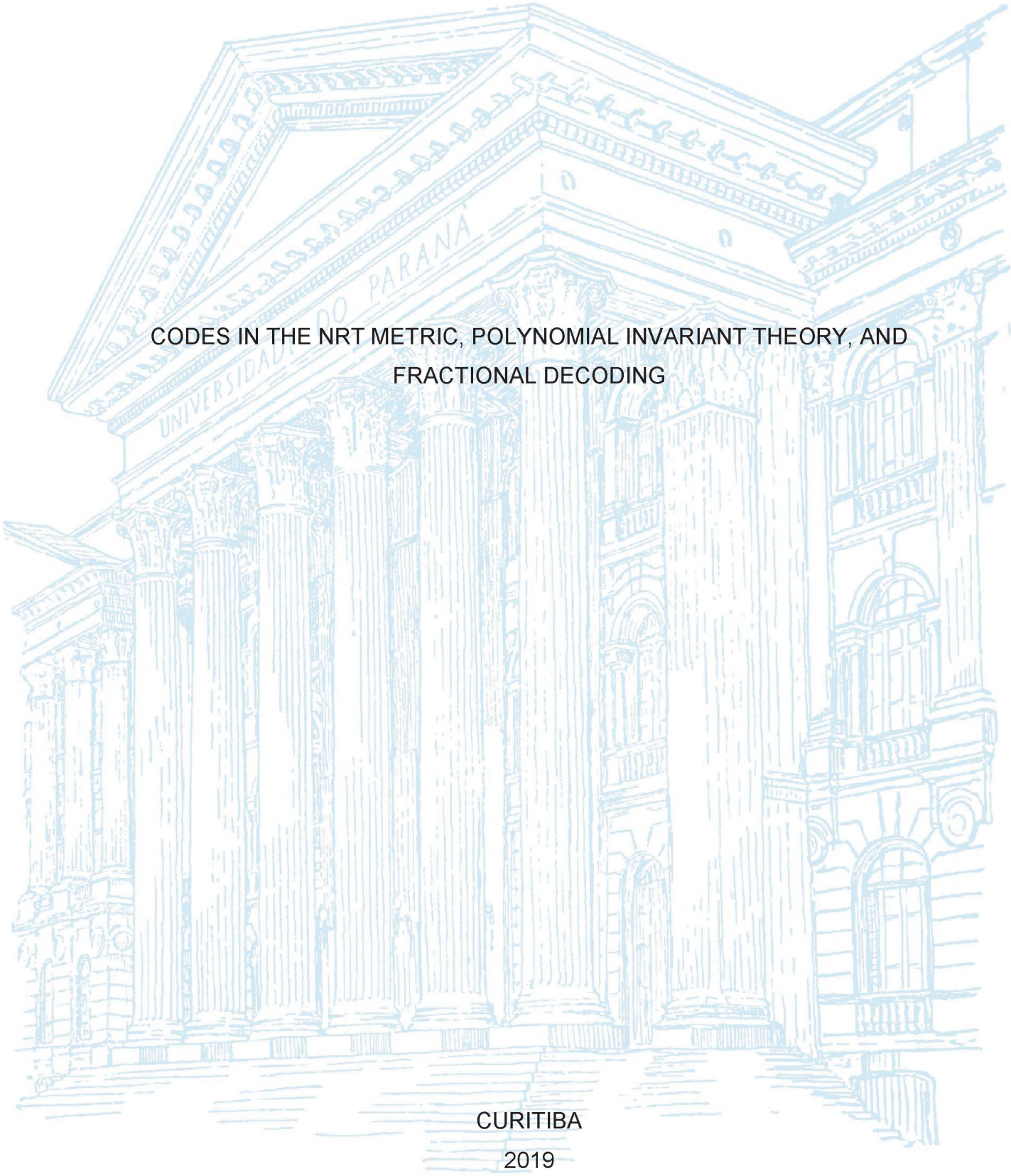
UNIVERSIDADE FEDERAL DO PARANÁ

WELINGTON SANTOS



CODES IN THE NRT METRIC, POLYNOMIAL INVARIANT THEORY, AND FRACTIONAL DECODING

CURITIBA

2019

WELINGTON SANTOS

CODES IN THE NRT METRIC, POLYNOMIAL INVARIANT THEORY, AND FRACTIONAL DECODING

Tese apresentada ao Programa de Pós-Graduação em Matemática, Setor de Ciências exatas, Universidade Federal do Paraná, como requisito parcial à obtenção do título de Doutor em Matemática.

Orientador: Prof. Dr. Marcelo Muniz Silva Alves (UFPR-Brasil)

Coorientador: Prof. Dr. Alexander Barg (University of Maryland-EUA)

CURITIBA

2019

Catalogação na Fonte: Sistema de Bibliotecas, UFPR
Biblioteca de Ciência e Tecnologia

S237c Santos, Welington
Codes in the NRT metric, polynomial invariant theory, and fractional decoding [recurso eletrônico] / Welington Santos. – Curitiba, 2019.

Tese - Universidade Federal do Paraná, Setor de Ciências Exatas, Programa de Pós- Graduação em Matemática, 2019.

Orientador: Marcelo Muniz Silva Alves. Coorientador: Alexander Barg.

1. Códigos de controle de erros (Teoria da informação). 2. Teoria da informação em matemática. 3. Teoria dos erros. I. Universidade Federal do Paraná. II. Alves, Marcelo Muniz Silva. III. Barg, Alexander. IV. Título.

CDD: 511.43

Bibliotecária: Vanusa Maciel CRB- 9/1928

MINISTÉRIO DA EDUCAÇÃO
SETOR DE CIENCIAS EXATAS
UNIVERSIDADE FEDERAL DO PARANÁ
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO MATEMÁTICA - 40001016041P1

ATA Nº031

ATA DE SESSÃO PÚBLICA DE DEFESA DE DOUTORADO PARA A OBTENÇÃO DO GRAU DE DOUTOR EM MATEMÁTICA

No dia dezesseis de agosto de dois mil e dezenove às 14:00 horas, na sala Anfiteatro A, Centro Politécnico da UFPR - Bloco PC - Rua Cel. Francisco H. dos Santos, 100 - Jardim das Américas, foram instaladas as atividades pertinentes ao rito de defesa de tese do doutorando **WELINGTON SANTOS**, intitulada: **Codes in the NRT-metric, Polynomial Invariant Theory and Fractional Decoding**, sob orientação do Prof. Dr. MARCELO MUNIZ SILVA ALVES. A Banca Examinadora, designada pelo Colegiado do Programa de Pós-Graduação da Universidade Federal do Paraná em MATEMÁTICA, foi constituída pelos seguintes Membros: MARCELO MUNIZ SILVA ALVES (UNIVERSIDADE FEDERAL DO PARANÁ), MATHEUS BATAGINI BRITO (UNIVERSIDADE FEDERAL DO PARANÁ), GIULIANO GADIOLI LA GUARDIA (UNIVERSIDADE ESTADUAL DE PONTA GROSSA), MARCELO FIRER (UNIVERSIDADE ESTADUAL DE CAMPINAS), EMERSON LUIZ DO MONTE CARMELO (UNIVERSIDADE ESTADUAL DE MARINGÁ). A presidência iniciou os ritos definidos pelo Colegiado do Programa e, após exarados os pareceres dos membros do comitê examinador e da respectiva contra argumentação, ocorreu a leitura do parecer final da banca examinadora, que decidiu pela APROVAÇÃO. Este resultado deverá ser homologado pelo Colegiado do programa, mediante o atendimento de todas as indicações e correções solicitadas pela banca dentro dos prazos regimentais definidos pelo programa. A outorga de tíutlo de doutorado está condicionada ao atendimento de todos os requisitos e prazos determinados no regimento do Programa de Pós-Graduação. Nada mais havendo a tratar a presidência deu por encerrada à sessão, da qual eu, MARCELO MUNIZ SILVA ALVES, lavrei a presenta ata, que vai assinada por mim e pelos demais membros da Comissão Examinadora.

CURITIBA, 16 de Agosto de 2019.

MARCELO MUNIZ SILVA ALVES
Presidente da Banca Examinadora

MATHEUS BATAGINI BRITO
Avaliador Interno (UNIVERSIDADE FEDERAL DO PARANÁ)

GIULIANO GADIOLI LA GUARDIA
Avaliador Externo (UNIVERSIDADE ESTADUAL DE PONTA GROSSA)

MARCELO FIRER
Avaliador Externo (UNIVERSIDADE ESTADUAL DE CAMPINAS)

EMERSON LUIZ DO MONTE CARMELO
Avaliador Externo (UNIVERSIDADE ESTADUAL DE MARINGÁ)

MINISTÉRIO DA EDUCAÇÃO
SETOR DE CIENCIAS EXATAS
UNIVERSIDADE FEDERAL DO PARANÁ
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO MATEMÁTICA - 40001016041P1

TERMO DE APROVAÇÃO

Os membros da Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação em MATEMÁTICA da Universidade Federal do Paraná foram convocados para realizar a arguição da tese de Doutorado de **WELINGTON SANTOS** intitulada: **Codes in the NRT-metric, Polynomial Invariant Theory and Fractional Decoding**, sob orientação do Prof. Dr. MARCELO MUNIZ SILVA ALVES, que após após terem inquirido o aluno e realizado a avaliação do trabalho, são de parecer pela sua APROVAÇÃO no rito de defesa.

A outorga do título de doutor está sujeita à homologação pelo colegiado, ao atendimento de todas as indicações e correções solicitadas pela banca e ao pleno atendimento das demandas regimentais do Programa de Pós-Graduação.

CURITIBA, 16 de Agosto de 2019.

MARCELO MUNIZ SILVA ALVES
Presidente da Banca Examinadora

MATHEUS BATAGINI BRITO
Avaliador Interno (UNIVERSIDADE FEDERAL DO PARANÁ)

GIULIANO GADIOLI LA GUARDIA
Avaliador Externo (UNIVERSIDADE ESTADUAL DE PONTA GROSSA)

MARCELO FIRER
Avaliador Externo (UNIVERSIDADE ESTADUAL DE CAMPINAS)

EMERSON LUIZ DO MONTE CARMELO
Avaliador Externo (UNIVERSIDADE ESTADUAL DE MARINGÁ)

" Thus we may have knowledge of the past but cannot control it; we may control the future but have no knowledge of it."

Claude Shannon

Acknowledgements

This dissertation represents an important part of my work as a PhD student at the Graduate in Mathematics Program (PPGM) at Federal University of Paraná. Several people contributed to its constitution and I would like to express my immeasurable appreciation and deepest gratitude for the help and support from the following persons.

First and foremost, I am grateful to my doctoral adviser Marcelo Muniz Silva Alves for his constant support, for providing a great working environment, and of course, for his advice, guidance, valuable comments, suggestions and care, he take shelter when conducting these surveys.

I greatly appreciate my co-advisor Alexander Barg, who provided me with the opportunity of spend six wonderful and fruitful months at the Institute for Systems Research at the University of Maryland, and especially for changing my way of thinking coding theory.

I am especially beholden to my dissertation committee for their encouragement, insightful comments, and hard questions which was a valuable contribution to this work.

I would like to thank all my current and former colleagues at the PPGM. In particular, I want to give thanks to my friends Cristian Schmidt, Wagner Augusto Almeida de Moraes, Tiago Luiz Ferrazza, and Wesley dos Santos Villela Batista for their frienship.

I would like to thank the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior-CAPES, for the financial support.

Last but not least, I wish to mention my dear girlfriend Bianca for her unconditional love, support and -whenever necessary- also patience, and my parents and my brother for their support, understanding and love.

Preface

This dissertation presents recent results of my research activities at the Graduate in Mathematics Program (PPGM) at Federal University of Paraná and at the Institute for Systens Research at University of Maryland. My work has been supported by Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). Parts of the results are in the following articles in conference proceedings and scientic journals:

1. W. Santos; Marcelo Muniz Alves, *Polynomial Invariant Theory and the Shape Enumerator of Self-Dual Codes in the NRT Metric*, (ArXiv:1904.04333), 2019.

2. W. Santos, *On Fractional Decoding of Reed-Solomon Codes*, Proc. 2019 IEEE Int. Sympos. Information Theory, July 8-12, 2019, Paris, France, pp. 1552-1556.

RESUMO

Esta tese aborda dois aspectos distintos da Teoria de Códigos: o estudo de códigos lineares sobre métricas diferentes da métrica de Hamming e o estudo da decodificação de códigos de Reed-Solomon. Na primeira parte desta tese, desenvolve-se a teoria de códigos lineares na métrica de Niederreiter-Rosenbloom-Tsfasman (ρ-métrica); tais códigos são chamados de códigos NRT. Desenvolve-se a teoria de polinômios invariantes com o objetivo de estudar o enumerador de shape de códigos NRT auto-duais. Por fim, apresenta-se novas construções de códigos NRT auto-duais. Em um segundo momento, estuda-se a família de códigos Reed-Solomon (RS) e códigos Reed-Solomon intercalados (IRS), assim como um método para decodificação colaborativa. Apresenta-se o conceito de decodificação fracionada e seus principais resultados, em especial um limitante superior para o α-raio de decodificação. Um novo método de decodificação fracionada para uma classe de códigos de Reed-Solomon é apresentado. Este método é capaz de realizar (com alta probabilidade) decodificação fracionada além do α-raio de decodificação. Por fim, uma conexão entre decodificação fracionada e códigos na ρ-métrica é apresentada.

Palavras-chave: Enumerador de shape. Códigos auto-duais. ρ-métrica. Códigos de Reed-Solomon. Decodificação fracionada.

ABSTRACT

This dissertation aims to study two distinct aspects of coding theory: a study of linear codes endowed with non-Hamming metrics and a study of decoding of Reed-Solomon codes. In the first part, the theory of linear codes in the Niederreiter-Rosenbloom-Tsfasman metric (ρ-metric) is developed. Such codes are called the NRT codes. In order to study the shape enumerator of self-dual NRT codes, we extended the classic results of invariant theory to the case of the NRT metric. Finally, new constructions of self-dual NRT codes are presented. In the second part, we study Reed-Solomon (RS) codes and interleaved Reed-Solomon (IRS) codes and their collaborative decoding. We present the concept of fractional decoding and main results related to it, including an upper bound on the α-decoding radius. We present a new method of fractional decoding of RS codes. This method can with high probability correct errors beyond the α-decoding radius of the codes. Finally, we present a connection between fractional decoding and codes endowed with the ρ-metric.

Keywords: Shape enumerator. Self-dual codes. ρ-metric. Reed-Solomon codes. Fractional decoding.

Contents

Introduction

In classical coding theory, an $[n, k]$ linear code C is a subspace of dimension k of the metric space $\mathbb{F}_q^n$, endowed with the metric d_H, called Hamming metric, and defined for $u, v \in C$ as the following $d_H(u, v) := |\{i \in \{1, 2, \ldots, n\} : u_i \neq v_i\}|$. An important concept in this setting is the dual code $C^\perp$ of a linear code $C \subseteq \mathbb{F}_q^n$ with respect to usual (Euclidean) inner product on $\mathbb{F}_q^n$.

One of the most important theorems in coding theory is the MacWilliams theorem (1962), which are known as the "MacWilliams Identities", which relates the weight enumerator of a linear code and its dual code. A remarkable theorem, due to Gleason [23] shows that the weight enumerator of a binary doubly-even self-dual code is a polynomial in other two polynomials, namely, the weight enumerators of the Hamming code of length 8 and of the Golay code of length 24. Sloane *et al.* presented some generalizations of Gleason's Theorem to other families of codes [39, 68, 40, 47]. A technique that can be used to derive those generalizations is polynomial invariant theory, specifically, the well-known Molien's series of a finite group of matrices [46].

Polynomial invariant theory deals with the question of explicit description of polynomial functions that are invariant under the transformations from a given linear group. For example, consider the action of the matrix group $G = \{I, -I\} \leqslant GL(2, \mathbb{C})$ on the linear space $\mathbb{F}_q^2$ by left multiplication, that is, for $v = (x, y) \in \mathbb{F}_q^2$ and $A \in G$, the action of A in $\mathbb{F}_q^2$ is given by sending $v \in \mathbb{F}_q^2$ to $Av^T \in \mathbb{F}_q^2$. This action induces naturally an action on $\mathbb{F}_q[x, y]$ if we consider $v = (x, y)$ as a "vector of variables" and define $A \cdot f(v) = f(Av^T)$ for $A \in G$. Then clearly the polynomial $p(x, y) = x^2 + 2xy$ is an invariant of this action. It is possible to show that the set of all the polynomials that are invariant under the action of a group G forms a ring that is called the invariant ring of G. In the 19th century it was found that the set of all homogeneous invariants under group a G can be described fully by finite set of generators for several suggestive special cases of G. We will study the invariant rings of some finite groups

which come from coding theory.

Coding theory has also been developed with respect to alternative metrics. One of the most investigated of those metrics is the NRT metric, which was introduced to study array codes that are subspaces of the linear space of all $n \times s$ matrices $M_{n,s}(\mathbb{F}_q)$ with entries from a finite field. The NRT metric space was introduced by Rosenbloom and Tsfasman in [75] by considering a generalization of RS codes in the space of all $n \times s$ matrices $M_{n,s}(\mathbb{F}_q)$; in this same paper the authors pointed out that this metric models transmission over a set of parallel channels subject to fading. Since then several coding-theoretic questions with respect to this metric have been investigated, such as the MacWilliams identities [15] and MDS codes [15, 16, 66]. Independently, Niederreiter [49] studied a maximization problem in finite vector spaces which turned out to be equivalent to coding theory problems in the NRT space, as was shown by Brualdi, Graves, and Lawrence [7]. In view of many applications to different branches of combinatorial mathematics, the NRT metric has gained significance comparable to the Hamming metric.

Dougherty and Skriganov showed in [15] that the weight enumerators of mutually NRT dual codes generally do not determine each other by any sort of MacWilliams identity, since there are examples of nonequivalent codes which have the same weight enumerators but whose duals have distinct weight enumerators. However, in the same paper they considered orbits of linear groups preserving the NRT weight and showed that the weight enumerator associated with such orbits (called the H-enumerator) satisfies a MacWilliams type identity for mutually NRT dual codes.

Recently, Barg et al. [52, 1, 2, 3] introduced the definition of shapes of codewords and a shape enumerator for NRT codes. The shape enumerator coincides with the H-enumerator. Park and Barg in [2] gave a new proof of the MacWilliams identity of [15] based on the multivariate Tutte polynomial of an NRT code that naturally arises by considering shapes of the codewords.

The first part of this dissertation aims to study self-dual codes in the NRT metric. In particular, we consider binary self-dual codes in $M_{n,s}(\mathbb{F}_2)$, and utilize polynomial invariant theory and the MacWilliams identity of [15, 2] to describe the shape enumerator of these codes. In particular, for binary self-dual NRT codes in $M_{n,2}(\mathbb{F}_2)$ we completely describe the ring of invariants that contains their shape enumerator; the same is done for binary doubly-even self-dual NRT codes, and for binary doubly-doubly-even self-dual NRT codes in $M_{n,2}(\mathbb{F}_2)$. We find the number of invariant polinomials that we must find to describe the shape enumerator of a self-

dual NRT code of $M_{n,2}(\mathbb{F}_2)$. We define the concept of ordered flip of a matrix $A \in M_{k,ns}(\mathbb{F}_q)$, and present some constructions of self-dual NRT codes in $M_{n,s}(\mathbb{F}_q)$ extending previous results for Self-dual NRT codes in $M_{1,s}(\mathbb{F}_q)$ from [42]. Finally, we present an application of the ordered flip to the classification of self-dual NRT codes of dimension two.

Another topic of study in coding theory is the problem of decoding, which is the process of recover the original transmitted message even when a few symbols of the received codeword are in error. There are many common methods of mapping messages to codewords. These are often used to recover messages sent over a noisy channel. An important result on decoding problem is that any linear code can correct at most $t = \lfloor \frac{d-1}{2} \rfloor$ errors, where d denotes the minimum distance of the code. The number $\tau = \lfloor \frac{d-1}{2} \rfloor$ is called the decoding radius of the code. It is well-Known that for any $[n, k]$ linear code C, its decoding radius, τ, is upper bounded by $\lfloor \frac{n-k}{2} \rfloor$, where the equality is true for linear codes whose parameters satisfy $d = n - k + 1$. Those codes are called Maximum Distance Separable (MDS) codes.

The most famous family of MDS codes is the family of Reed-Solomon codes [57], which are applied, for example, in CD-ROMs, wireless communications, space communications, DSL, DVD, and digital TV. Reed-Solomon codes are also known to have some good decoding methods [53, 21].

Schmidt *et at.* [62] used an encoding method known as Interleaved Reed-Solomon codes to and a decoding approach called collaborative decoding of Interleaved Reed-Solomon codes [60] to perform (with high probability) decoding of Reed-Solomon codes beyond its decoding radius.

Lately, error-correcting codes are being studied in the context of Distributed Storage Systems [9], [10], and [13] such as those run by Google and Facebook. In a distributed system, we usually face a limitation on the disk input/output operations as well as on the amount of information transmitted for the purpose of decoding. In this case, we no longer have access to all the coordinates of the codewords and vectors in general. Considering the decoding of linear and array codes from errors when we are only allowed to download a part of the codeword. More specifically, supposing that k data symbols are encoded using an $[n, k]$ code and during storage, some of the codeword coordinates might be corrupted by errors. Tamo, Ye, and Barg [73] studied the problem of recover the original data by reading the corrupted codeword with a limit on the transmitting bandwidth, namely, the decoder can only download an α proportion of the corrupted codeword. This problem is called fractional decoding problem. The main propose

of [73] is to answering the natural question of how many errors we can guarantee to correct in this setup. This paper shows that for any k-dimensional code in $\mathbb{F}_q^n$ the number of correctable errors under this constraint is upper bounded by $\left\lfloor \frac{n-\frac{k}{\alpha}}{2} \right\rfloor$ and also presents two families of codes which achieve this bound.

The second part of this dissertation aims to study Reed-Solomon codes and Interleaved Reed-Solomon codes. In particular, we are interested in the investigation of the collaborative decoding approach of Interleaved Reed-Solomon codes [60], which can be used to perform decoding of Reed-Solomon codes beyond the decoding radius [77]. We present the definition and properties of fractional decoding and α-decoding radius [73] of linear codes and present a new probabilistic approach to perform fractional decoding of a class of Reed-Solomon codes $RS(q^s, n, k)$ beyond the α-decoding radius. We also point out some connections between fractional decoding and NRT codes.

Outline of the dissertation

Let us give a more detailed description of the content of this Ph.D dissertation.

In Chapter 1, we review some basic definitions of polynomial invariant theory [46],[45] and [69], some useful theorems and propositions about the existence of a polynomial invariant basis for finite groups are given and we present the well-known Molien Theorem.

In Chapter 2, we present some of the main definitions and properties of linear codes in $\mathbb{F}_q^n$. On the basis of [15], we recall the concept of matrix code and the definition of the Niederreiter-Rosenbloom-Tsfasman Metric (NRT metric). Finally, a study of the geometry of the NRT metric is performed, and the shape enumerator [52] of NRT codes as well as a Macwilliams identity for the shape enumerator is described.

In Chapter 3, using polynomial invariant theory and the MacWilliams identity for the shape enumerator, we present new results that characterize the shape enumerator of self-dual NRT codes in $M_{n,2}(\mathbb{F}_2)$. A study on the shape enumerator of self-dual NRT codes in $M_{n,s}(\mathbb{F}_2)$ is also done.

In Chapter 4, we introduce new constructions of self-dual codes in the NRT metric, starting with constructions that are derived from codes in the Hamming metric. We define the ordered flip of an array. This new concept enable us to present new constructions of self-dual codes in the NRT metric. Finally, using the definition of ordered flip and results of Alves [65], we provide a classification of self-dual NRT codes of dimension two.

In Chapter 5, the well-known family of Reed-Solomon codes and the syndrome decod-

ing approach are reviewed. Afterwards the definition of interleaved Reed Solomon codes, and a probabilistic collaborative decoding approach given by Schmidt [60] are briefly described.

Finally, in Chapter 6, we present the definition of fractional decoding and the α-decoding radius. We give a new probabilistic fractional decoding approach for a class of Reed Solomon codes that can correct errors beyond the α-decoding radius. We propose connections between NRT codes and fractional decoding, and give an α-decoding radius for the case of linear NRT codes in $M_{1,s}(\mathbb{F}_q)$.

Chapter 1

Elementary Polynomial Invariant Theory

In this chapter, we recall the polynomial invariant theory of finite groups [46, 45, 69, 72, 29, 56, 12]. The basic goal is to describe all polynomials which are unchanged when we change variables according to the action of a given finite group of matrices.

1.1 Basic definitions

In this section, we will give some basic definitions for invariants of finite matrix groups and we will compute some examples to illustrate what questions the general theory should address.

Definition 1.1. *A finite matrix group G of $M_{n,n}(\mathbb{C})$ is a subgroup of the group $GL(n,\mathbb{C})$ of invertible $n \times n$ matrices with entries in $\mathbb{C}$, i.e., G is a nonempty set of complex invertible matrices with the following properties:*

a) If A and B are in G so is the product AB.

b) The identity matrix I_n is in G.

c) The inverse matrix A^{-1} of a matrix A in G is also in G.

The number of elements of G is called the order of G and is denoted by $|G|$.

Given a finite matrix group $G < GL(n,\mathbb{C})$ and $A_1, \ldots, A_m$ in G, we say that $A_1, \ldots, A_m$ *generate* the group G if every matrix A in G can be written in the form $A = B_1 B_2 \ldots B_t$ where $B_i \in \{A_1, \ldots, A_m\}$ for every i. In this case, we write $G = \langle A_1, \ldots, A_m \rangle$.

The group $GL(n, \mathbb{C})$ of invertible $n \times n$ matrices acts on the ring $\mathbb{C}[z_1, \ldots, z_n]$ by

$$A \cdot f(z_1, \ldots, z_n) = f\left(\sum_{j=1}^{n} a_{1,j} z_j, \ldots, \sum_{j=1}^{n} a_{n,j} z_j\right). \tag{1.1}$$

We may describe the action in a more concise manner. Consider the "vector of variables" $Z = (z_1, \ldots, z_n)^t$. The previous equation may be rewritten as

$$A \cdot f(Z) = f(AZ).$$

A remarkable fact is that sometimes this process gives back the same polynomial that we started with. For example, if we let $f(z_1, z_2) = z_1^2 + z_2^2$ and $A = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$, then one can check that

$$A \cdot f(z_1, z_2) = f(z_1, z_2).$$

In this case, we say that f is invariant under A. Moreover, note that $f(z_1, z_2)$ is invariant under every matrix $B \in G = \langle A \rangle$. This leads to the following fundamental definition.

Definition 1.2. *Let G be a group of $n \times n$ of $M_{n,s}(\mathbb{C})$, and $f(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]$. The polynomial $f(z_1, \ldots, z_n)$ is called an invariant of G (or G-invariant), if for all $A \in G$*

$$A \cdot f(z_1, \ldots, z_n) = f(z_1, \ldots, z_n).$$

Clearly if f, g are invariants of G so are $f + g$ and fg. Then the set of invariants form a ring, which is denoted by $\mathcal{J}(G)$.

Given a polynomial $f \in \mathbb{C}[z_1, \ldots, z_n]$ and a finite matrix group G, note that the action (1.1) does not change the degree of f, so any invariant is a sum of homogeneous invariants and to characterize the ring $\mathcal{J}(G)$ it is suffices to characterize the invariants that are homogeneous polynomials.

One can check that the action of $GL(n, \mathbb{C})$ on the ring $\mathbb{C}[z_1, \ldots, z_n]$ has the following property.

Lemma 1.3. *Let G be a finite matrix group of $GL(n, \mathbb{C})$ and $f \in \mathbb{C}[z_1, \ldots, z_n]$. For any $A, B \in G$, we have*

$$(AB) \cdot f(z_1, \ldots, z_n) = A \cdot (B \cdot f(z_1, \ldots, z_n)).$$

The following lemma is useful in determining whether a given polynomial is invariant under a finite matrix group.

Lemma 1.4. *Let G be the finite matrix group generated by $A_1, \ldots, A_m$, that is, $G = \langle A_1, \ldots, A_m \rangle$. A polynomial $f(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]$ is an invariant of G if and only if*

$$f(z_1, \ldots, z_n) = A_1 \cdot f(z_1, \ldots, z_n) = \ldots = A_m \cdot f(z_1, \ldots, z_n).$$

Proof. We first show that if f is invariant under the matrices $B_1, \ldots, B_t$, then it is also invariant under their product $B_1 \ldots B_t$. This is clearly true for $t = 1$. If we assume it is true for $t - 1$, then

$$\begin{aligned} (B_1 B_2 \ldots B_t) \cdot f(x_1, \ldots, x_n) &= B_1 \cdot ((B_2 \ldots B_t) \cdot f(z_1, \ldots, z_n)) \\ &= B_1 \cdot f(z_1, \ldots, z_n) \\ &= f(z_1, \ldots, z_n). \end{aligned}$$

Now suppose that f is invariant under $A_1, \ldots, A_m$. Since elements $A \in G$ can be written as $A = B_1 \ldots B_t$, where every B_i is one of $A_1, \ldots, A_m$, it follows immediately that $f \in \mathcal{J}(G)$. The converse is trivial and the lemma is proved. □

The example below describes how we can use the previous Lemma.

Example 1.5. *Consider the finite Klein four-group of $GL(2, \mathbb{C})$.*

$$V_4 = \left\{ \begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{bmatrix} \right\}.$$

It is possible to check that the two matrices

$$A_1 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \text{ and } A_2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

generate V_4. Then Lemma 1.4 implies that a polynomial $f(z_1, z_2) \in \mathbb{C}[z_1, z_2]$ is V_4-invariant if and only if

$$A_1.f(z_1, z_2) = f(z_1, z_2)$$

and

$$A_2.f(z_1, z_2) = f(z_1, z_2).$$

Writing $f(z_1, z_2) = \sum a_{ij} z_1^i z_2^j$, we can understand the first of these conditions as follows:

$$\begin{aligned} f(z_1, z_2) = f(-z_1, z_2) &\iff \sum a_{ij} z_1^i z_2^j = \sum a_{ij} (-z_1)^i z_2^j \\ &\iff \sum a_{ij} z_1^i z_2^j = \sum (-1)^i a_{ij} z_1^i z_2^j \end{aligned}$$

$$\iff \quad a_{ij} = (-1)^i a_{ij} \text{ for all i,j}$$
$$\iff \quad a_{ij} = 0 \text{ for i odd.}$$

It follows that only even powers of z_1 appear in homogeneous components of $f(x_1, x_2)$. Similarly, the condition $f(z_1, z_2) = f(z_1, -z_2)$ implies that only even powers of z_2 appear in homogeneous components of $f(z_1, z_2)$. Thus, we can write

$$f(z_1, z_2) = g(z_1^2, z_2^2)$$

for an unique polynomial $g(z_1, z_2) \in \mathbb{C}[z_1, z_2]$. Conversely, every polynomial f of this form is clearly invariant under V_4. This proves that

$$\mathcal{J}(V_4) = \mathbb{C}[z_1^2, z_2^2].$$

Hence, every invariant of V_4 can be uniquely written as a polynomial in the two homogeneous invariants z_1^2 and z_2^2.

1.2 Existence of a basic set of invariants for finite groups

Given a finite matrix group G of $GL(n, \mathbb{C})$, a classical question about the invariant ring $\mathcal{J}(G)$ of G that is: can we find finitely many homogeneous invariants $f_1, \ldots, f_m$ such that every invariant is a polynomial in $f_1, \ldots, f_m$?

Definition 1.6. *Given polynomials $f_1, \ldots, f_m \in \mathbb{C}[z_1, \ldots, z_n]$, we denote by $\mathbb{C}[f_1, \ldots, f_m]$ the subset of $\mathbb{C}[z_1, \ldots, z_n]$ consisting of all polynomial expressions in $f_1, \ldots, f_m$ with coefficients in $\mathbb{C}$.*

In words, each element f in $\mathbb{C}[f_1, \ldots, f_m]$ is a polynomial that can be written in the form

$$f = h(f_1, \ldots, f_m)$$

where h is a polynomial in m variables with coefficients in $\mathbb{C}$.

It is possible to check that $\mathbb{C}[f_1, \ldots, f_m]$ is closed under multiplication and addition. Moreover, $\mathbb{C}[f_1, \ldots, f_m]$ is a subring of $\mathbb{C}[z_1, \ldots, z_n]$ which contains $\mathbb{C}$. We say that $\mathbb{C}[f_1, \ldots, f_m]$ is generated by $f_1, \ldots, f_m$ over $\mathbb{C}$.

Definition 1.7. *The polynomials $f_1, \ldots, f_m$ in $\mathbb{C}[z_1, \ldots, z_n]$ are algebraically dependent if there is a nonzero polynomial $P(z_1, z_2, \ldots, z_m)$ in $\mathbb{C}[z_1, \ldots, z_m]$ such that $P(f_1, \ldots, f_m)$ is identically zero. Otherwise, the polynomials $f_1, \ldots, f_m$ are said to be algebraically independent.*

Theorem 1.8. *([30].) Any $n+1$ polynomials in n variables are algebraically dependent.*

Given polynomials $f_1, \ldots, f_m$ in $\mathbb{C}[z_1, \ldots, z_n]$, we would like to know whether they are algebraically dependent or independent. The Jacobian criterion, discussed next gives a useful tool to text algebraic independence.

Definition 1.9. *Given polynomials $f_1, \ldots, f_m \in \mathbb{C}[z_1, \ldots, z_n]$ their Jacobian matrix is defined as*

$$J(f_1, \ldots, f_m) := \begin{bmatrix} \frac{\partial f_1}{\partial z_1} & \frac{\partial f_1}{\partial z_2} & \cdots & \frac{\partial f_1}{\partial z_n} \\ \frac{\partial f_2}{\partial z_1} & \frac{\partial f_2}{\partial z_2} & \cdots & \frac{\partial f_2}{\partial z_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial z_1} & \frac{\partial f_m}{\partial z_2} & \cdots & \frac{\partial f_m}{\partial z_n} \end{bmatrix}.$$

Theorem 1.10. *(Jacobian criterion [35, 18]). The polynomials $f_1, \ldots, f_m$ in $\mathbb{C}[z_1, \ldots, z_n]$ are algebraically independent if and only if the Jacobian matrix has full rank over the rational field $\mathbb{C}(z_1, \ldots, z_n)$. In particular, in the case $m = n$, the polynomials $f_1, \ldots, f_m$ are algebraically independent if only if $\det(J(f_1, \ldots, f_m)) \neq 0$.*

Thus, given a finite matrix group $G < GL(n, \mathbb{C})$, the most convenient description (at this moment) of $\mathcal{J}(G)$ is a set of homogeneous G-invariants $\{f_1, \ldots, f_m\}$ which are algebraically independent and are such that every polynomial in $\mathcal{J}(G)$ is a polynomial in $f_1, \ldots, f_m$. In this case, $\{f_1, \ldots, f_m\}$ is said to be a *polynomial basis* (or a *integrity basis*) for the invariants of G. If $m > n$ there are polynomial equations, which are called *syzygies*, relating $f_1, \ldots, f_m$.

The following theorem, whose proof will be omitted but can be found in [55], states that a polynomial basis for the ring of invariants of a finite matrix group always exists.

Theorem 1.11. *(E. Noether's Theorem [51],[76]). Let G of $GL(n, \mathbb{C})$ be a finite matrix group of order g. The invariant ring $\mathcal{J}(G)$ of G, has a polynomial basis consisting of not more than $\binom{g+n}{n}$ invariant polynomials, where each polynomial has degree not exceeding g.*

Theorem 1.11 says that a polynomial basis for $\mathcal{J}(G)$ can always be found. Finding invariant polynomials is fairly easy using the following operator that is introduced during the proof of Theorem 1.11.

Definition 1.12. *Given a finite matrix group G of $GL(n, \mathbb{C})$, the **Reynolds operator** of G is the map $\Gamma_G : \mathbb{C}[z_1, \ldots, z_n] \longrightarrow \mathbb{C}[z_1, \ldots, z_n]$ defined by the formula*

$$\Gamma_G(f)(z_1, \ldots, z_n) = \frac{1}{|G|} \sum_{A \in G} A \cdot f(z_1, \ldots, z_n)$$

for each $f(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]$.

Proposition 1.13. *Let* Γ_G *be the Reynolds operator of the finite matrix group* $G < GL(n, \mathbb{C})$.

i) $\Gamma_G : \mathbb{C}[z_1, \ldots, z_n] \to \mathbb{C}[z_1, \ldots, z_n]$ *is* $\mathbb{C}$*-linear.*

ii) If $f \in \mathbb{C}[z_1, \ldots, z_n]$, *then* $\Gamma_G(f) \in \mathcal{J}(G)$.

iii) If $f \in \mathcal{J}(G)$, *then* $\Gamma_G(f) = f$.

Proof. We will only prove the second item. For any A' in G,

$$\begin{aligned} A' \cdot \Gamma_G(f)(z_1, \ldots, z_n) &= \frac{1}{|G|} \sum_{A \in G} A' \cdot (A \cdot f(z_1, \ldots, z_n)) \\ &= \frac{1}{|G|} \sum_{A \in G} (A'A) \cdot f(z_1, \ldots, z_n) \\ &= \frac{1}{|G|} \sum_{B \in G} B \cdot f(z_1, \ldots, z_n) \\ &= \Gamma_G(f)(z_1, \ldots, z_n). \end{aligned}$$

□

Corollary 1.14. *Let* G *be a finite matrix group of* $GL(n, \mathbb{C})$ *and* Γ_G *the Reynolds operator of* G. *The invariant ring of* G *is given by*

$$\mathcal{J}(G) = \Gamma_G(\mathbb{C}[z_1, \ldots, z_n]).$$

Proof. It follows directly from Items ii) and iii) of the previous proposition. □

Definition 1.15. *Let* $G < GL(n, \mathbb{C})$ *be a finite matrix group. A* ***good polynomial basis*** *for the invariant ring* $\mathcal{J}(G)$ *consists of homogeneous invariants* $f_1, \ldots, f_m$ $(m \geq n)$, *where* $f_1, \ldots f_n$ *are algebraically independent, and*

$$\mathcal{J}(G) = \mathbb{C}[f_1, \ldots, f_n] \quad if \quad m = n, \tag{1.2}$$

or, if $m > n$,

$$\mathcal{J}(G) = \mathbb{C}[f_1, \ldots, f_n] \oplus f_{n+1}\mathbb{C}[f_1, \ldots, f_n] \oplus \ldots \oplus f_m\mathbb{C}[f_1, \ldots, f_n]. \tag{1.3}$$

Roughly speaking, $\mathcal{J}(G)$ has a good polynomial basis then any invariant of G can be written as a polynomial in $f_1, \ldots, f_n$ (if $m = n$), or as such a polynomial plus f_{n+1} times another such

polynomial plus f_{n+2} times another such polynomial and so on (if $m > n$). The polynomials $f_1, \ldots, f_n$ are called *primary invariants* and $f_{n+1}, \ldots, f_m$ are *secondary invariants*.

A good polynomial basis can always be found, according to the following theorem given by Hochster and Eagon whose proof can be found in [29], [69] or [8].

Theorem 1.16. *(Hochster and Eagon [29].) A good polynomials basis for the invariant ring $\mathcal{J}(G)$ of any finite matrix group $G < GL(n, \mathbb{C})$ always exists.*

1.3 The Molien's theorem

Given a finite matrix group G of $GL(n, \mathbb{C})$, a fundamental problem is to know, or at least to estimate, how many algebraically independent invariants are required to form a polynomial basis of $\mathcal{J}(G)$. Fortunately, there are some efficient methods for finding a generating set of invariants. The main tool is the Molien theorem, which enables one to predict in advance the number of linearly independent homogeneous invariants of a given degree.

The following theorem is a weak version of the Molien theorem and its proof can be found in [55, 59].

Theorem 1.17. *(Molien [59]). Given a finite matrix group G of $GL(n, \mathbb{C})$, the number of linearly independent invariants of G of the first degree is*

$$\frac{1}{|G|} \sum_{A \in G} \operatorname{trace}(A).$$

The next theorem is the beautiful and well-known theorem of T. Molien [46], published in 1897. The proof can be found in [46, 45, 69, 72].

Theorem 1.18. *(Molien [46].) Given a finite matrix group G of $GL(n, \mathbb{C})$, the number of linearly independent invariants of G of degree t is the coefficient of λ^t in the expansion of*

$$\Phi_G(\lambda) = \frac{1}{|G|} \sum_{A \in G} \frac{1}{\det(I - \lambda A)}.$$

$\Phi_G(\lambda)$ is called the Molien series of G.

Lemma 1.19. *The Molien series of any finite matrix group $G < GL(n, \mathbb{C})$ can be written as*

$$\Phi_G(\lambda) = \frac{1}{|G|} \sum_{A \in G} \frac{\det(A)}{\det(A - \lambda I)}.$$

Proof. By definition the Molien series of G, is given by

$$\begin{aligned}
\Phi_G(\lambda) &= \frac{1}{|G|}\sum_{A\in G}\frac{1}{\det(I-\lambda A)} \\
&= \frac{1}{|G|}\sum_{A\in G}\frac{\det(AA^{-1})}{\det(AA^{-1}-\lambda A)} \\
&= \frac{1}{|G|}\sum_{A\in G}\frac{\det(A)\det(A^{-1})}{\det(A)\det(A^{-1}-\lambda I)} \\
&= \frac{1}{|G|}\sum_{A\in G}\frac{\det(A^{-1})}{\det(A^{-1}-\lambda I)} \\
&= \frac{1}{|G|}\sum_{A\in G}\frac{\det(A)}{\det(A-\lambda I)}.
\end{aligned}$$

□

A good polynomial basis and Molien series of the invariant ring of a finite matrix group G match in the following sense: given a good polynomial basis $\{f_1,\ldots,f_m\}$ of $\mathcal{J}(G)$ such that $d_1=\deg f_1,\ldots,d_m=\deg f_m$, we have that

$$\Phi_G(\lambda)=\frac{1}{\prod_{i=1}^{n}(1-\lambda^{d_i})},\ \text{if}\quad m=n, \tag{1.4}$$

or

$$\Phi_G(\lambda)=\frac{1+\sum_{j=n+1}^{m}\lambda^{d_j}}{\prod_{i=1}^{n}(1-\lambda^{d_i})},\ \text{if}\quad m>n. \tag{1.5}$$

In the next example we show how the Molien series and polynomial basis are related to each other.

Example 1.20. *Let G be the finite matrix group of $GL(2,\mathbb{C})$ defined by*

$$G=\left\{\begin{bmatrix}1&0\\0&1\end{bmatrix},\begin{bmatrix}-1&0\\0&-1\end{bmatrix}\right\}.$$

Writing $f(z_1,z_2)=\sum a_{ij}z_1^iz_2^j$, the condition

$$\begin{bmatrix}-1&0\\0&-1\end{bmatrix}\cdot f(z_1,z_2)=f(z_1,z_2)$$

can be understood as

$$f(z_1,z_2)=f(-z_1,-z_2)\iff \sum a_{ij}z_1^iz_2^j=\sum a_{ij}(-z_1)^i(-z_2)^j$$

$$\begin{aligned} &\iff \sum a_{ij} z_1^i z_2^j = \sum (-1)^{i+j} a_{ij} z_1^i z_2^j \\ &\iff a_{ij} = (-1)^{i+j} a_{ij} \textit{ for all i,j} \\ &\iff a_{ij} = 0 \textit{ for i+j odd.} \end{aligned}$$

If $a_{ij} \neq 0$, then i and j are both even or odd. Writing $i = 2q_i + r_i$ and $j = 2q_j + r_j$ we have that the terms where a_{ij} is nonzero can be written as $a_{ij} z_1^i z_2^j = a_{ij} (z_1^2)^{q_i} (z_2^2)^{q_j} z_1^{r_i} z_2^{r_2}$ and as i and j have the same parity, $a_{ij} z_1^i z_2^j = a_{ij} (z_1^2)^{q_i} (z_2^2)^{q_j}$ or $a_{ij} z_1^i z_2^j = a_{ij} (z_1^2)^{q_i} (z_2^2)^{q_j} z_1 z_2$, so any invariant polynomial $f \in \mathcal{J}(G)$ is such that $f \in \mathbb{C}[z_1^2, z_2^2] \oplus z_1 z_2 \mathbb{C}[z_1^2, z_2^2]$ that is $\mathcal{J}(G)$ is a subset of $\mathbb{C}[z_1^2, z_2^2] \oplus z_1 z_2 \mathbb{C}[z_1^2, z_2^2]$. On other hand, the polynomials $f_1(z_1, z_2) = z_1^2$, $f_2(z_1, z_2) = z_2^2$ are algebraically independent since $\det(J(f_1, f_2)) = 4 z_1 z_2$ and we can apply Theorem 1.10. The polynomial $f_3(z_1, z_2) = z_1 z_2$ is a secondary invariant of G. So $\{f_1, f_2, f_3\}$ is a good polynomial basis with $\deg f_1 = \deg f_2 = \deg f_3 = 2$. Moreover, $f_3^2 \in \mathbb{C}[z_1^2, z_2^2]$. Finally, the invariant ring of G is

$$\mathcal{J}(G) = \mathbb{C}[z_1^2, z_2^2] \oplus z_1 z_2 \mathbb{C}[z_1^2, z_2^2].$$

In other words, If $f(z_1, z_2) \in \mathcal{J}(G)$, then

$$f(z_1, z_2) = h_1(z_1^2, z_2^2) + z_1 z_2 h_2(z_1^2, z_2^2).$$

The Molien series of G is

$$\Phi_G(\lambda) = \frac{1}{2} \left(\frac{1}{(1+\lambda)^2} + \frac{1}{(1-\lambda)^2} \right) = \frac{1+\lambda^2}{(1-\lambda^2)^2}.$$

When we have a good polynomial basis for the invariant ring $\mathcal{J}(G)$ of a finite matrix group G, the Molien series of G can be put into the standard form of (1.4), (1.5) (with denominator consisting of a product of m factors $(1-\lambda^{d_i})$ and numerator consisting of a sum of powers of λ with positive coefficientes) whose degrees of the polynomials of the basis match with the powers of λ occurring in the standard form of the Molien series.

On the other hand, the converse is not true. It is not always true that when the Molien series has been put into the form (1.4), (1.5), then a good polynomial basis for $J(G)$ whose degrees match the powers of λ in $\Phi(\lambda)$ can be found. This was shown by the following example due to Stanley [71, Ex 3.8].

Example 1.21. *Let $G < GL(3, \mathbb{C})$ be the finite matrix group of order 8 defined by*

$$G = \left\langle \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & i \end{bmatrix} \right\rangle.$$

The Molien series of G can be written as

$$\Phi_G(\lambda) = \frac{1}{(1-\lambda^2)^3} = \frac{1+\lambda^2}{(1-\lambda^2)^2(1-\lambda^4)}.$$

A good polynomial basis exists corresponding to $\Phi_G(\lambda) = \frac{1+\lambda^2}{(1-\lambda^2)^2(1-\lambda^4)}$. Namely,

$$J(G) = \mathbb{C}[x^2, y^2, z^4] \oplus xy\mathbb{C}[x^2, y^2, z^4].$$

On the other hand, there is no good polynomial basis corresponding to $\Phi_G(\lambda) = \frac{1}{(1-\lambda^2)^3}$.

Chapter 2

Linear Codes and The Niederreiter-Rosenbloom-Tsfasman Metric

In this chapter, we review some of the basic definitions on code theory [28]. We also introduce some definitions and results on linear codes endowed with the Niederreiter-Rosenbloom-Tsfasman metric. Those definitions and results can be found in [7], [14], [75], and [66]. In special, we focus on the shape enumerator of a linear code endowed with the Niederreiter-Rosenbloom-Tsfasman metric, and in a MacWilliams type identity for the shape enumerator which was proved by Barg, and Park [2].

2.1 Linear codes in $\mathbb{F}_q^n$

Definition 2.1. *Let $\mathbb{F}_q^n$ denote the vector space of all n-tuples over the finite field $\mathbb{F}_q$. A $[n,k]$ linear code C of length n and dimension k is a linear subspace of $\mathbb{F}_q^n$ of dimension k .*

In the case where $q = 2$ we say that a subspace C of $\mathbb{F}_2^n$ of dimension k is an $[n,k]$ binary linear code. A vector $v \in C$ is called a *codeword* of C. An $[n,k]$ linear code C can be defined by its *generator matrix* using a basis of the k-dimensional subspace C.

Definition 2.2. *Let C be an $[n,k]$ linear code over $\mathbb{F}_q$. A generator matrix G of C is a $k \times n$ matrix whose rows are a basis of C over $\mathbb{F}_q$.*

Notice that there is more than one generator matrix for a given $[n,k]$ linear code C, since we

can choose any basis of the k-dimensional subspace C over $\mathbb{F}_q$ in an arbitrary order.

An important invariant of a code is the minimum distance between its codewords. The *Hamming weight* $\omega_H(v)$ of a vector v in $\mathbb{F}_q^n$ is the number of nonzero coordinates in v.The *Hamming distance* $d_H(v,u)$ between two vectors $v,u \in \mathbb{F}_q^n$ is defined to be the number of coordinates in which v and u differ, that is, $\omega_H(v-u)$.

The *minimum distance* of a linear code C is the smallest distance between two distinct codewords. It is well known that the minimum distance of a linear code C in $\mathbb{F}_q^n$ is the minimum weight of the nonzero codewords of C. Thus a result of this fact the minimum distance is also called the *minimum weight* of the code. If the minimum weight d of an $[n,k]$ code is known, then we refer to the code as an $[n,k,d]$ linear code.

Let w_r , also denoted $w_r(C)$, be the number of codewords of weight r in C. The list w_r for $0 \leqslant r \leqslant n$ is called the *weight distribution* or *weight spectrum* of C.

2.1.1 Dual codes

Recall that the standard inner product of vectors $v=(v_0,\ldots,v_{n-1}), u=(u_0,\ldots,u_{n-1})$ in $\mathbb{F}_q^n$ is defined by $\langle v,u\rangle_E = \sum_{i=0}^{n-1} v_i u_i$.

Definition 2.3. *Euclidean dual code of an $[n,k]$ linear code C in $\mathbb{F}_q^n$ is defined to be the $[n,k^\perp]$ linear code $C^\perp$ in $\mathbb{F}_q^n$ given by*

$$C^\perp := \{u \in \mathbb{F}_q^n \ : \ \langle v,u\rangle_E = 0 \ \forall \ v \in C\}.$$

A code C in $\mathbb{F}_q^n$ is *self-orthogonal* provided $C \subseteq C^\perp$, and *self-dual* provided $C = C^\perp$. The length n of a self-dual code is even and the dimension k is $\frac{n}{2}$.

The dual code of an $[n,k]$ linear code over $\mathbb{F}_q$ has dimension $k^\perp = n-k$ and length n. Therefore, the dual code $C^\perp$ is an $[n,n-k]$ linear code, *i.e.*, an $(n-k)$-dimensional subspace of $\mathbb{F}_q^n$, which can be used to define the *parity-check matrix* of C.

Definition 2.4. *(parity-check matrix). An $(n-k)\times n$ matrix H over $\mathbb{F}_q$ is called a parity-check matrix of an $[n,k]$ linear code C over $\mathbb{F}_q$ if and only if it is a generator matrix of the $[n,n-k]$ dual code $C^\perp$ over $\mathbb{F}_q$.*

Note that for any $c \in C$, the multiplication with the parity-check matrix gives $cH^T = 0$ and $GH^T = 0$. A parity-check matrix is therefore a matrix whose right kernel is the code C.

Definition 2.5. *For a vector v in $\mathbb{F}_q^n$ and a parity-check matrix H of an $[n,k]$ linear code C, the vector $s = vH^T \in \mathbb{F}_q^{n-k}$ is called the syndrome of v.*

By definition, given a vector v in $\mathbb{F}_q^n$, note that the syndrome s of v is such that $s = 0$ if and only if $v \in C$.

2.1.2 Weight enumerator

Let C be an $[n,k,d]$ linear code in $\mathbb{F}_q^n$ with weight distribution w_r for $0 \leqslant r \leqslant n$, then the *weight enumerator* of C is defined to be

$$W_C(z_0, z_1) = \sum_{r=0}^{n} w_r z_0^{n-r} z_1^r \tag{2.1}$$

where z_0 and z_1 are indeterminates. The polynomial $W_C(z_0, z_1)$ in (2.1) can also be written as

$$W_C(z_0, z_1) = \sum_{v \in C} z_0^{n-\omega_H(v)} z_1^{\omega_H(v)}. \tag{2.2}$$

Example 2.6. *We will compute the weight enumerator of some linear codes.*

(a) Let $C_1 = \{(0,0),(1,1)\}$ in $\mathbb{F}_2^2$, then the weight enumerator of C_1 is $W_{C_1}(z_0, z_1) = z_0^2 + z_1^2$.

(b) More generally, let $C_2 = \{(0,0,\ldots,0),(1,1,\ldots,1)\}$ be the $[n,1]$ repetition code in $\mathbb{F}_2^n$, then $W_{C_2}(z_0, z_1) = z_0^n + z_1^n$.

(c) The $[7,4]$ Hamming code $\mathcal{H}_3$ in $\mathbb{F}_2^7$ is given by

$$\mathcal{H}_3 := \left\{ \begin{array}{cccc} (0,0,0,0,0,0,0) & (1,1,1,0,1,0,0) & (1,0,0,1,1,1,0) & (0,1,0,0,1,1,1) \\ (0,1,1,1,0,1,0) & (0,0,1,1,1,0,1) & (1,0,1,0,0,1,1) & (1,1,0,1,0,0,1) \\ (1,1,1,1,1,1,1) & (0,0,0,1,0,1,1) & (1,0,0,0,1,0,1) & (1,1,0,0,0,1,0) \\ (0,1,1,0,0,0,1) & (1,0,1,1,0,0,0) & (0,1,0,1,1,0,0) & (0,0,1,0,1,1,0) \end{array} \right\},$$

and $W_{C_3}(z_0, z_1) = z_0^7 + 7z_0^4 z_1^3 + 7z_0^3 z_1^4 + z_1^7$.

Example 2.7. *Let $\hat{\mathcal{H}_3} \subseteq \mathbb{F}_2^8$ be the $[8,4]$ linear code obtained from $\mathcal{H}_3$ by adding at the end of each codeword a new digit that checks the parity of the codeword. The code $\hat{\mathcal{H}_3}$ is called the $[8,4]$ extended Hamming code, and its codewords are*

$$\hat{\mathcal{H}_3} := \left\{ \begin{array}{cccc} (0,0,0,0,0,0,0,0) & (1,1,1,0,1,0,0,0) & (1,0,0,1,1,1,0,0) & (0,1,0,0,1,1,1,0) \\ (0,1,1,1,0,1,0,0) & (0,0,1,1,1,0,1,0) & (1,0,1,0,0,1,1,0) & (1,1,0,1,0,0,1,0) \\ (1,1,1,1,1,1,1,1) & (0,0,0,1,0,1,1,1) & (1,0,0,0,1,0,1,1) & (1,1,0,0,0,1,0,1) \\ (0,1,1,0,0,0,1,1) & (1,0,1,1,0,0,0,1) & (0,1,0,1,1,0,0,1) & (0,0,1,0,1,1,0,1) \end{array} \right\}.$$

It is possible to check that $\hat{\mathcal{H}}_3$ is self-dual code and its weight enumerator is given by

$$W_{\hat{\mathcal{H}}_3}(z_0, z_1) = z_0^8 + 14 z_0^4 z_1^4 + z_1^8.$$

One of the most important theorems in coding theory is a theorem due to MacWilliams (1962), which is known as "the MacWilliams identity" and states that the weight enumerator of the dual code $C^{\perp}$ is uniquely determined by the weight enumerator of C.

Theorem 2.8. *(MacWilliams [38]). If C is an $[n, k, d]$ linear code over $\mathbb{F}_q$ with dual code $C^{\perp}$, then*

$$W_{C^{\perp}}(z_0, z_1) = \frac{1}{q^k} W_C(z_0 + (q-1)z_1, z_0 - z_1). \tag{2.3}$$

In the binary case (when $q = 2$), Theorem 2.8 can be write as

$$W_{C^{\perp}}(z_0, z_1) = \frac{1}{2^k} W_C(z_0 + z_1, z_0 - z_1), \tag{2.4}$$

or, equivalently,

$$\sum_{v \in C^{\perp}} z_0^{n-\omega_H(v)} z_1^{\omega_H(v)} = \frac{1}{2^k} \sum_{v \in C} (z_0 + z_1)^{n-\omega_H(v)} (z_0 - z_1)^{\omega_H(v)}. \tag{2.5}$$

2.2 Linear codes in $M_{n,s}(\mathbb{F}_q)$

Definition 2.9. *Let $M_{n,s}(\mathbb{F}_q)$ be the linear space of all matrices with n rows and s columns with entries in a finite field $\mathbb{F}_q$ of q elements.A $[ns, k]$ linear code C is a linear subspace C of dimension k of $M_{n,s}(\mathbb{F}_q)$.*

Similarly to the case of codes in $\mathbb{F}_q^n$, we can define an *Hamming weight* on $M_{n,s}(\mathbb{F}_q)$, denoted by ω_H, as the number of non-zero entries of $\mathbf{v}$, where $\mathbf{v} \in M_{n,s}(\mathbb{F}_q)$. In this case the *Hamming distance* between $\mathbf{v}$ and $\mathbf{u}$ with $\mathbf{v}, \mathbf{u} \in M_{n,s}(\mathbb{F}_q)$ is given by $\omega_H(\mathbf{v} - \mathbf{u})$.

Codes in $M_{n,s}(\mathbb{F}_q)$ are also studied in some other nonHamming metrics, for example, the Rank metric, which was introduced by Loo-Keng Hua [37], and Ernst M. Gabidulin [22]. In this work, we will study another nonHamming metric that was introduced by Rosenbloom and Tsfasman [75], which is described more precisely in the next sections.

2.3 Codes and Niederreiter-Rosenbloom-Tsfasman metric

Let $M_{n,s}(\mathbb{F}_q)$ be the $\mathbb{F}_q$-vector space of $n \times s$ matrices with entries in $\mathbb{F}_q$. Given an $n \times s$ matrix $\mathbf{v}$,

$$\mathbf{v} = \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1s} \\ v_{21} & v_{22} & \cdots & v_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \cdots & v_{ns} \end{bmatrix},$$

its i-th row will be denoted by v_i, and we will write $\mathbf{v} = [v_1; v_2; \cdots; v_n]$. According to this notation, the Niederreiter-Rosenbloom-Tsfasman weight or, for short, the NRT weigth of $\mathbf{v}$ is defined by the following formula:

$$\rho(\mathbf{v}) := \sum_{i=1}^{n} \rho(v_i)$$

where $\rho(v_i) := \max\{0 \leq j \leq s\,;\, v_{ij} \neq 0\}$.

The canonical metric, $d_\rho(\mathbf{u}, \mathbf{v}) = \rho(\mathbf{u} - \mathbf{v})$, associated to the NRT weight is called the NRT metric. The space $(M_{n,s}(\mathbb{F}_q), \rho)$ is called NRT space.

The Hamming metric, and the Niederreiter-Rosenbloom-Tsfasman metric on $M_{n,s}(\mathbb{F}_q)$ are related by the following inequalities

$$\omega_H(\mathbf{v}) \leqslant \rho(\mathbf{v}) \leqslant s\omega_H(\mathbf{v}).$$

This metric space was introduced with an information-theoretic motivation, and since then several coding-theoretic questions with respect to this metric have been investigated, such as MDS codes [15, 16, 66] and MacWilliams Duality [15]. Independently, Niederreiter worked with a maximization problem in finite vector spaces which turned out to be equivalent to classical coding theory problems in NRT spaces [50, 49] and by this reason we call the ρ-metric the Niederreiter-Rosenbloom-Tsfasman Metric. It is worth noting that in the context of the theory of uniform distributions, the metric ρ was also introduced in papers [41] by Martin and Stinson and [66, **?**] by Skriganov.

Definition 2.10. *An $[ns, k]$ linear NRT code C is a linear subspace C of dimension k of $(M_{n,s}(\mathbb{F}_q), \rho)$.*

For a given NRT linear code C in $M_{n,s}(\mathbb{F}_q)$, the following set of non-negative integers

$$\omega_r(C) := |\{\mathbf{v} \in C \,:\, \rho(\mathbf{v}) = r\}|,$$

$0 \leqslant r \leqslant ns$ is called the NRT weight spectrum of the NRT code C. Define the *ρ-weight enumerator*, or the NRT weight of a linear code C in $M_{n,s}(\mathbb{F}_q)$ by

$$W_C(z) = \sum_{r=0}^{ns} w_r(C) z^r = \sum_{\mathbf{v} \in C} z^{\rho(\mathbf{v})}.$$

Now let $\mathbf{v} = [v_1; v_2; \cdots ; v_n]$ and $\mathbf{u} = [u_1; u_2; \cdots ; u_n]$ be two elements of $M_{n,s}(\mathbb{F}_q)$. We define the inner product $\langle , \rangle_N$ on the space $M_{n,s}(\mathbb{F}_q)$ endowed with the NRT metric by

$$\langle \mathbf{v}, \mathbf{u} \rangle_N = \langle \mathbf{u}, \mathbf{v} \rangle_N := \sum_{i=1}^{n} \langle v_i, u_i \rangle_N$$

with

$$\langle v_i, u_i \rangle_N = \langle u_i, v_i \rangle_N := v_{i1}u_{is} + v_{i2}u_{i(s-1)} + \ldots + v_{i(s-1)}u_{i2} + v_{is}u_{i1} = \sum_{j=1}^{s} v_{ij}u_{i(s-j+1)}.$$

This inner product is a non-degenerate bi-linear map on $M_{n,s}(\mathbb{F}_q) \times M_{n,s}(\mathbb{F}_q)$.

Definition 2.11. *The dual code of an k-dimensional linear NRT code C in $M_{n,s}(\mathbb{F}_q)$ is defined to be the $k^\perp$-dimensional linear NRT code $C^\perp$ in $M_{n,s}(\mathbb{F}_q)$ given by*

$$C^\perp := \{\mathbf{u} \in M_{n,s}(\mathbb{F}_q) : \langle \mathbf{u}, \mathbf{v} \rangle_N = 0 \; \forall \; \mathbf{v} \in C\}.$$

A NRT code C is said to be a *self-orthogonal NRT code* if $C \subseteq C^\perp$ and *self-dual NRT code* if $C = C^\perp$. Moreover, the dimensions of the codes C and $C^\perp$ are related by the following equation: if $k = \dim(C)$ and $k^\perp = \dim(C^\perp)$ then

$$k + k^\perp = ns. \tag{2.6}$$

MacWilliams-type theorems for the ρ-weight enumerators of mutually dual codes can be found in two cases. In the case of $s = 1$ and arbitrary n, the ρ-weight enumerator satisfies the following classical MacWilliams theorem for Hamming weight enumerators [15].

$$W_{C^\perp}(z) = \frac{1}{|C|}(1 + (q-1)z)^n W_C\left(\frac{1-z}{1+(q-1)z}\right).$$

In the case of $n = 1$ and arbitrary s, we have the following identity [67].

$$(qz-1)W_{C^\perp}(z) + 1 - z = |C^\perp| z^{s+1}\left(q(1-z)W_C\left(\frac{1}{qz}\right) + qz - 1\right).$$

It is easy to see that direct extensions does not exist for the ρ-weight enumerator in the case n and s arbitrary as we can see in the following example due to [15].

Example 2.12. *Consider two linear NRT codes C_1 and C_2 in $M_{2,2}(\mathbb{F}_2)$,*

$$C_1 = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \right\}, C_2 = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right\}$$

both have ρ-weight enumerator

$$W_{C_1}(z) = W_{C_2}(z) = 1 + z^2.$$

The dual codes $C_1^{\perp}$ and $C_2^{\perp}$ in $M_{2,2}(\mathbb{F}_2)$ are described below

$$C_1^{\perp} = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \right\},$$

and

$$C_2^{\perp} = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\}.$$

The ρ-weight enumerator for $C_1^{\perp}$ and $C_2^{\perp}$ turns out to be different:

$$W_{C_1^{\perp}}(z) = 1 + 4z^4 + 2z + z^2 \tag{2.7}$$

$$W_{C_2^{\perp}}(z) = 1 + 2z^4 + z^3 + 3z^2 + z. \tag{2.8}$$

Therefore, the ρ-weight enumerators (2.7) and (2.8) cannot be related by a MacWilliams type relation.

2.4 The NRT metric geometry

Two linear NRT codes C and C' in $M_{n,s}(\mathbb{F}_q)$ are *equivalent* if there is a linear isometry ϕ of $M_{n,s}(\mathbb{F}_q)$ such that $\phi(C) = C'$. The group $GL\left(M_{n,s}(\mathbb{F}_q)\right)$ of linear isometries of an NRT space $M_{n,s}(\mathbb{F}_q)$ was described in [34] (also independently in [15]) and it is isomorphic to the semidirect product of $(T_s)^n$ and S_n, where:

i) T_s is the group of all upper triangular matrices of $M_{s,s}(\mathbb{F}_q)$ with non-zero diagonal elements;

ii) $(T_s)^n$ denotes the direct product of n copies of T_s;

iii) S_n is the symmetric group of order n.

An element of S_n acts on $\mathbf{v} = [v_1; v_2; \cdots ; v_n]$ by permuting rows, and an element $(M_1, M_2, \ldots, M_n)$ of T_s^n sends $\mathbf{v} = [v_1; v_2; \cdots ; v_n]$ to $[v_1 M_1^T; v_2 M_2^T; \cdots ; v_n M_n^T]$.

It is clear that if $\mathbf{v} = [v_1; v_2; \cdots ; v_n]$ and $\mathbf{u} = [u_1; u_2; \cdots ; u_n]$ are two elements of $M_{n,s}(\mathbb{F}_q)$ that lie in the same $GL\,(M_{n,s}(\mathbb{F}_q))$-orbit then $\mathbf{u}$ and $\mathbf{v}$ have the same NRT weight. The converse will not hold in general, since $GL(M_{n,s}(\mathbb{F}_q))$ is not transitive on spheres. In order to parametrize the $GL(M_{n,s}(\mathbb{F}_q))$-orbits, which were already studied in [15], Barg and Purkayastha [3] define a new parameter of a matrix $\mathbf{v} = [v_1; v_2; \cdots ; v_n] \in M_{n,s}(\mathbb{F}_q)$ which is called the shape of $\mathbf{v}$.

Definition 2.13. *Let* $\mathbf{v} \in M_{n,s}(\mathbb{F}_q)$ *be a matrix written as* $\mathbf{v} = [v_1; v_2; \cdots ; v_n]$, *where* $v_i = (v_{i1}, \ldots, v_{is})$ *for* $i = 1, \ldots, n$. *The shape of* $\mathbf{v}$ *with respect to the NRT weight is the* s*-vector* $e = (e_1, \ldots, e_s)$, *where*

$$e_j = |\{i \text{ such that } 1 \leqslant i \leqslant n \text{ and } \rho(v_i) = j\}|.$$

Also define $e_0 := n - |e|$, *where* $|e| := \sum_{j=1}^{s} e_j$.

Since the action of $GL(M_{n,s}(\mathbb{F}_q))$ on matrices of a fixed shape is transitive, then the shape is an invariant for this action. The NRT weight can be also defined in terms of shapes: if $e = (e_1, \ldots, e_s)$ is the shape of the matrix $\mathbf{v} = [v_1; v_2; \cdots ; v_n]$ in $M_{n,s}(\mathbb{F}_q)$, then

$$\rho(\mathbf{v}) := \sum_{j=1}^{s} j e_j.$$

2.5 The shape enumerator and a MacWilliams identity

The NRT weight is a special case of *poset weight*, as introduced by Brualdi, Graves, and Lawrence in [7]. There is a notion of dual code for every poset code but only in rare cases does the weight enumerator of the code determine the enumerator of its dual; precisely, this is the case if and only if the poset is hierarchical [31], and an NRT weight is associated

to a hierarchical poset only when $n = 1$ (whcih corresponds to a chain) or $s = 1$ (which corresponds to the Hamming weight). Nevertheless, analogues of those identities do hold when one considers other kinds of enumerator polynomials. Dougherty and Skriganov [15], defined a generalized weight enumerator for a linear NRT code, the H-enumerator, which counts the number of codewords in each $GL(M_{n,s}(\mathbb{F}_q))$-orbit. In the same paper it was shown that the H-enumerator of mutually dual codes satisfies a MacWilliams-type identity, which we will state next according to the version presented in [2], using the concept of shape vector.

A shape vector e induces a partition of n into a sum of $s+1$ parts. We will denote by $\Delta_{s,n} := \{e \in \mathbb{N}^s : \ e_0 + e_1 + e_2 + \ldots + e_s = n\}$ such partition (recall that $e_0 = n - |e|$). In the language of shapes, the description of $GL(M_{n,s}(\mathbb{F}_q))$-orbits is as follows

Proposition 2.14. *([15], Proposition 2.2 (ii)) Let* $\mathbf{u} \in M_{n,s}(\mathbb{F}_q)$ *be a nonzero matrix. The* $GL(M_{n,s}(\mathbb{F}_q))$*-orbits of* $\mathbf{u}$ *is the set of all matrices* $\mathbf{v} \in M_{n,s}(\mathbb{F}_q)$ *which have the same shape of* $\mathbf{u}$.

Definition 2.15. *Let* C *be a linear NRT code in* $M_{n,s}(\mathbb{F}_q)$. *The shape enumerator of* C *is the polynomial of* $\mathbb{C}[z_0, z_1, \ldots, z_s]$ *defined by*

$$H_C(z_0, z_1, \ldots, z_s) = \sum_{e \in \Delta_{s,n}} \mathcal{A}_e z_0^{e_0} z_1^{e_1} \ldots z_s^{e_s}, \tag{2.9}$$

where $\mathcal{A}_e = |\{\mathbf{v} \in C \ : \ \text{shape}(\mathbf{v}) = e\}|$.

The shape enumerator of a NRT code C is a homogeneous polynomial $H_C(Z)$ with $s+1$ variables, which coincides with the H-enumerator introduced in [15]. In order to state the MacWilliams identity shown in [15]. We need to remember the action (1.1) of $GL(s+1, \mathbb{C})$ on $\mathbb{C}[z_0, z_1, \ldots, z_s]$, given by

$$A \cdot f(z_0, z_1, \ldots, z_s) = f\left(\sum_{j=0}^{s} a_{0,j} z_j, \ldots, \sum_{j=0}^{s} a_{s,j} z_j\right). \tag{2.10}$$

This action can be describe in a more concise manner. Considering the "vector of variables" $Z = (z_0, z_1, \ldots, z_s)^t$ and rewritten the previous equation as

$$A \cdot f(Z) = f(AZ).$$

Using this notation, the next result presents the MacWilliams identity for the shape enumerator.

Theorem 2.16. *[2] The shape enumerator of mutually dual linear NRT codes C and $C^{\perp}$ in $M_{n,s}(\mathbb{F}_q)$ are closely related by*

$$H_{C^{\perp}}(Z) = \frac{1}{|C|} H_C(\Theta_s Z),$$

where $\Theta_s = (\theta_{lk}) \in M_{s+1,s+1}(\mathbb{F}_q)$, $0 \leqslant l, k \leqslant s$, has the following entries

$$\theta_{lk} = \begin{cases} 1 & \text{if} \quad k = 0 \\ q^{l-1}(q-1) & \text{if} \quad 0 < k \leqslant s-l \\ -q^{l-1} & \text{if} \quad l+k = s+1 \\ 0 & \text{if} \quad l+k > s+1 \end{cases}.$$

For example, we have for $s = 1, 2$ and 3.

$$\Theta_1 = \begin{bmatrix} 1 & q-1 \\ 1 & -1 \end{bmatrix}, \Theta_2 = \begin{bmatrix} 1 & q-1 & q(q-1) \\ 1 & q-1 & -q \\ 1 & -1 & 0 \end{bmatrix},$$

$$\Theta_3 = \begin{bmatrix} 1 & q-1 & q(q-1) & q^2(q-1) \\ 1 & q-1 & q(q-1) & -q^2 \\ 1 & q-1 & -q & 0 \\ 1 & -1 & 0 & 0 \end{bmatrix}.$$

In [15] it is shown that Θ_s satisfies the equality

$$\{\Theta_s\}^2 = q^s I_{s+1}. \tag{2.11}$$

Note that Θ_s is a sub-matrix of Θ_{s+1}, explicitly, if we denote $\Theta_{s+1} = (\theta_{s+1})_{l,k}$ and $\Theta_s = (\theta_s)_{l,k}$, so $(\theta_{s+1})_{l,k} = (\theta_s)_{l-1,k}$ for $l > 0$ and $s+1 > k$. Note also that the first and second rows of Θ_s differ only by their last element.

Example 2.17. *Let C_1 be the NRT code in $M_{2,2}(\mathbb{F}_2)$ given by*

$$C_1 := \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \right\}.$$

The NRT dual code $C_1^{\perp}$ in $M_{2,2}(\mathbb{F}_2)$ is easily calculated:

$$C_1^{\perp} := \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \right\}.$$

The ρ-weight enumerators of the codes C_1 and $C_1^{\perp}$ are given respectively by $W_{C_1}(z) = 1 + z^2$ and $W_{C_1^{\perp}}(z) = 1 + 2z + z^2 + 4z^4$. Let us calculate the shape enumerator of C_1 and $C_1^{\perp}$. First of all, note that

$$\begin{aligned} \Delta_{2,2} &= \{e \in \mathbb{N}^2 \ : \ e_1 + e_2 \leqslant 2\} \\ &= \{(0,0),(0,1),(1,0),(1,1),(2,0),(0,2)\}, \end{aligned}$$

and the shape vectors of the elements of C_1 and $C_1^{\perp}$ are given, respectively, by

$$(0,0),(2,0)$$

and

$$(0,0),(0,2),(0,2),(0,2),(0,2),(1,0),(1,0),(2,0).$$

Hence, by definition,

$$H_{C_1}(z_0,z_1,z_2) = \sum_{e \in \Delta_{2,2}} \mathcal{A}_e z_0^{e_0} z_1^{e_1} z_2^{e_2}$$

with $\mathcal{A}_e = |\{\mathbf{v} \in C_1 \ : \ \mathrm{shape}(\mathbf{v}) = e\}|$. In our case, $\mathcal{A}_{(0,0)} = \mathcal{A}_{(2,0)} = 1$ and $\mathcal{A}_e = 0$ for $e \notin \{(0,0),(2,0)\}$. Moreover, considering the shape vector $(0,0)$, we have $e_0 = 2$, and for the shape vector $(2,0)$ we have $e_0 = 0$. So the shape enumerator de C_1 is

$$H_{C_1}(z_0,z_1,z_2) = z_0^2 + z_1^2.$$

Analogously, the shape enumerator $H_{C_1^{\perp}}$ of $C_1^{\perp}$ is given by

$$\begin{aligned} H_{C_1^{\perp}}(z_0,z_1,z_2) &= z_0^2 + z_1^2 + 4z_2^2 + 2z_0z_1 \\ &= \frac{1}{2}(2z_0^2 + 2z_1^2 + 8z_2^2 + 4z_0z_1) \\ &= \frac{1}{|C_1|} H_{C_1}(\Theta_2(z_0,z_1,z_2)), \end{aligned}$$

where

$$\Theta_2 = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 1 & -2 \\ 1 & -1 & 0 \end{bmatrix}.$$

Chapter 3

Polynomial Invariant Theory and Shape Enumerator

In this chapter, using the MacWilliams Theorem 2.16 and polynomial invariant theory, we investigate the shape enumerator (H-enumerator) of a binary self-dual NRT codes in $M_{n,s}(\mathbb{F}_2)$. We will follow the steps of Sloane's work on self-dual codes and invariant theory [68, 40], which will be described in the first section of this chapter.

3.1 Codes and polynomial invariant theory

To compute the weight enumerator of a code with wide parameters can be a complicated task. Thus, a topic of investigation in coding theory is to describe the weight enumerator of some code families. In 1970, Gleason [23] showed an interesting result on the weight enumerator of self-dual codes in $\mathbb{F}_2^n$, more precisely:

Theorem 3.1. *(Gleason [23]) Let C be a binary self-dual code in $\mathbb{F}_2^n$ and $W_C \in \mathbb{C}[z_0, z_1]$ be its weight enumerator. Then $W_C \in \mathbb{C}[z_0^2 + z_1^2, z_0^8 + 14 z_0^4 z_1^4 + z_1^8]$.*

Roughly speaking, Gleason showed that the weight enumerator of any binary self-dual code is a polynomial in the weight enumerators of the repetition code $C_1 = \{(0,0),(1,1)\}$ and the $[8,4]$ extended Hamming code $\hat{\mathcal{H}}_3$ of Example 2.7.
Gleason also proved similar theorems for binary codes with weights divisible by 4 and for self-dual codes of $\mathbb{F}_3^n$.

Theorem 3.2. *(Gleason [23]) The weight enumerator of a self-dual code C in $\mathbb{F}_2^n$ with weight*

divisible by 4*, is a polynomial in* $W_{\hat{\mathcal{H}}_3}$ *and* W_{C_4}*, where*

$$W_{\hat{\mathcal{H}}_3}(z_0, z_1) = z_0^8 + 14z_0^4z_1^4 + z_1^8$$

is the weight enumerator of the $[8, 4]$ *extended Hamming code of Example* 2.7*, and*

$$W_{C_4}(z_0, z_1) = z_0^{24} + 759z_0^{16}z_1^8 + 2576z_0^{12}z_1^{12} + 759z_0^8z_1^{16} + z_1^{24}$$

is the weight enumerator of the $[24, 12]$ *extendend Golay code [28, 11].*

MacWilliams *et al.* [68, 40] showed that the classical polynomial invariant theory allows Gleason's theorem and generalizations, as for example the following theorem.

Theorem 3.3. *(Sloane [39, 40]) The weight enumerator of any* $[n, k]$ *self-dual code* C *in* $\mathbb{F}_2^n$ *is a polynomial in* $g, h \in \mathbb{C}[z_0, z_1]$*, where* $g(z_0, z_1) = z_0^2 + (q-1)z_1^2$ *and* $h(z_0, z_1) = z_1(z_0 - z_1)$*.*

Next, we give an application to show how powerful those theorems are.

Application: 3.4. *There exist an* $[32, 16, 10]$ *self-dual code* C *in* $\mathbb{F}_2^{32}$*?*
Suppose there is a $[32, 16, 10]$ *self-dual code in* $\mathbb{F}_2^n$*, say* C*. On one hand, its weight enumerator is*

$$W_C(z_0, z_1) = z_0^{32} + 0z_0^{31}z_1 + 0z_0^{30}z_1^2 + \ldots + A_{10}z_0^{22}z_1^{10} + \ldots \tag{3.1}$$

since the minimum weight of C *is* 10*. On the other hand, Gleason's Theorem 3.1 states that* $W_C(z_0, z_1)$ *is a polynomial in* $W_{C_1}(z_0, z_1) = z_0^2 + z_1^2$ *and* $W_{\hat{\mathcal{H}}_3}(z_0, z_1) = z_0^8 + 14z_0^4z_1^4 + z_1^8$*, that is,*

$$W_C(z_0, z_1) = a_1W_{C_1}^{16} + a_2W_{C_1}^{16}W_{\hat{\mathcal{H}}_3} + a_3W_{C_1}^8W_{\hat{\mathcal{H}}_3}^2 + a_4W_{C_1}^4W_{\hat{\mathcal{H}}_3}^3 + a_5W_{\hat{\mathcal{H}}_3}^4. \tag{3.2}$$

Comparing equations (3.4) and (3.1),

$$W_C(z_0, z_1) = z_0^{32} + 4960z_0^{22}z_1^{10} - 3437z_0^{20}z_1^{12} + \ldots$$

contradicting the definition of weight enumerator. So, there is no such code.

In the next sections we will use invariant theory to study the shape enumerator of self-dual codes with respect to the Niederreiter-Rosenbloom-Tsfasman metric.

3.2 Invariant ring for self-dual NRT codes in $M_{n,2}(\mathbb{F}_2)$

Let C be an $[ns, k]$ binary NRT code in $M_{n,2}(\mathbb{F}_2)$. Theorem 2.16 can be written as

Theorem 3.5. *The shape enumerator of mutually dual NRT linear codes C and $C^\perp$ in $M_{n,2}(\mathbb{F}_2)$ are related by*

$$H_{C^\perp}(Z) = \frac{1}{2^k} H_C(\Theta_2 Z),$$

where $\Theta_2 = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 1 & -2 \\ 1 & -1 & 0 \end{bmatrix}$.

If we assume that C is a linear self-dual NRT code of dimension k, that is, $C = C^\perp$ (consequently $k = k^\perp$), then we conclude that $k = n$, and Theorem 3.5 means that $H_C(Z)$, the shape enumerator of C is such that $H_C(Z) = \frac{1}{2^n} H_C(\Theta_2 Z)$. Since, by definition, $H_C(Z)$ is a homogeneous polynomial of degree n, the last expression for $H_C(Z)$ may be rewritten as

$$H_C(Z) = H_C\left(\frac{\Theta_2}{2} Z\right),$$

which means that the polynomial H_C is invariant by $T = \frac{\Theta_2}{2}$. Moreover, as $T^2 = \left(\frac{\Theta_2}{2}\right)^2 = I_3$, the shape enumerator H_C is an element of $\mathcal{J}(G_1)$, where G_1 is the finite group of order 2 generated by T, $G_1 = \langle T \rangle = \{I, T\}$. We will try construct a good polynomial basis for $\mathcal{J}(G_1)$.

From Molien's Theorem 1.18, the number of linearly independent invariants of degree t over the group G_1 is equal to the coefficient of λ^t in

$$\Phi_{G_1}(\lambda) = \frac{1}{2} \sum_{A \in G_1} \frac{\det(A)}{\det(A - \lambda I_3)}.$$

Let's calculate $\Phi_{G_1}(\lambda)$. First note that

$$T := \frac{\Theta_2}{2} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & 1 \\ \frac{1}{2} & \frac{1}{2} & -1 \\ \frac{1}{2} & -\frac{1}{2} & 0 \end{bmatrix}. \tag{3.3}$$

It is easy to check that $\det(T) = -1$, $\det(T - \lambda I_3) = (\lambda - 1)(1 - \lambda^2)$ and therefore

$$\begin{aligned} \Phi_{G_1}(\lambda) &= \frac{1}{2} \sum_{A \in G_1} \frac{\det(A)}{\det(A - \lambda I_3)} \\ &= \frac{1}{2} \left(\frac{1}{(1-\lambda)^3} + \frac{1}{(1-\lambda)(1-\lambda^2)} \right) \end{aligned}$$

$$\begin{aligned} &= \frac{1}{2}\left(\frac{1-\lambda^2+(1-\lambda)^2}{(1-\lambda)^3(1-\lambda^2)}\right) \\ &= \frac{1}{2}\left(\frac{1-\lambda^2+1-2\lambda+\lambda^2}{(1-\lambda)^3(1-\lambda^2)}\right) \\ &= \frac{1}{2}\left(\frac{2-2\lambda}{(1-\lambda)^3(1-\lambda^2)}\right) \\ &= \frac{1}{(1-\lambda)^2(1-\lambda^2)}. \end{aligned}$$

So in order to find a good polynomial basis for G_1, we should looking for one invariant of degree two and two invariants of degree one.

Since the shape enumerator of a NRT code C in $M_{n,2}(\mathbb{F}_2)$ has degree n, we start looking for shape enumerators of linear self-dual NRT codes in $M_{1,2}(\mathbb{F}_2)$. There exist just five linear codes in $M_{1,2}(\mathbb{F}_2)$, namely: The trivial codes $C_0 := \{(0,0)\}$, $C_4 := M_{1,2}(\mathbb{F}_2)$ and the non-trivial codes:

$$C_{1,1} := \{(0,0),(0,1)\};$$

$$C_{1,2} := \{(0,0),(1,0)\};$$

$$C_{1,3} := \{(0,0),(1,1)\}.$$

It is clear that all except the trivial codes are self-dual codes, and their shape enumerators are

$$H_{C_{1,1}}(z_0,z_1,z_2) = z_0+z_2;$$

$$H_{C_{1,2}}(z_0,z_1,z_2) = z_0+z_1;$$

$$H_{C_{1,3}}(z_0,z_1,z_2) = z_0+z_2.$$

Note that $H_{C_{1,2}}(z_0,z_1,z_2) = H_{C_{1,3}}(z_0,z_1,z_2)$ and this was already expected, since there exists a linear isometry between $C_{1,2}$ and $C_{1,3}$. We choose $\phi_1(z_0,z_1,z_2) = z_0+z_2$ and $\phi_2(z_0,z_1,z_2) = z_0+z_1$; it is obvious that ϕ_1,ϕ_2 are algebraically independent and invariant under G_1.

Now to find an invariant polynomial of degree two, we will consider a linear self-dual NRT code in $M_{2,2}(\mathbb{F}_2)$ and compute its shape enumerator. Let

$$C_{2,1} := \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \right\}.$$

The code $C_{2,1}$ is a self-dual NRT code and $H_{C_{2,1}}(z_0,z_1,z_2) = z_0^2+z_1^2+2z_2^2$. Define $\phi_3(z_0,z_1,z_2) = z_0^2+z_1^2+2z_2^2$, so $\phi_3(z_0,z_1,z_2)$ is invariant under G_1. We claim that the set

$\{\phi_1, \phi_2, \phi_3\}$ is algebraically independent. In fact, the set $\{\phi_1, \phi_2\}$ is algebraically independent, so we need just prove that ϕ_3 is algebraically independent of ϕ_1 and ϕ_2. We can check that

$$\begin{aligned}
\bigtriangledown\phi_1(z_0, z_1, z_2) &= (1, 0, 1); \\
\bigtriangledown\phi_2(z_0, z_1, z_2) &= (1, 1, 0); \\
\bigtriangledown\phi_3(z_0, z_1, z_2) &= (2z_0, 2z_1, 4z_2).
\end{aligned}$$

Therefore,

$$\begin{aligned}
\det(J(\phi_1, \phi_2, \phi_3)) &= \det \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 2z_0 & 2z_1 & 4z_2 \end{bmatrix} \\
&= 4z_1 + 4z_2 - 2z_0 \\
&\neq 0,
\end{aligned}$$

proving that $\{\phi_1, \phi_2, \phi_3\}$ is algebraically independent by Theorem 1.10. In short, we just proved the following theorem.

Theorem 3.6. *Let C be a self-dual NRT code in $M_{n,2}(\mathbb{F}_2)$. Then, the shape enumerator of C is an invariant polynomial under the action of $G_1 = \langle T \rangle$, where T is the matrix given in (3.3). Moreover, the invariant ring of the group G_1 is $\mathbb{C}[\phi_1, \phi_2, \phi_3]$, where*

$$\begin{aligned}
\phi_1(z_0, z_1, z_2) &= z_0 + z_2; \\
\phi_2(z_0, z_1, z_2) &= z_0 + z_1; \\
\phi_3(z_0, z_1, z_2) &= z_0^2 + z_1^2 + 2z_2^2.
\end{aligned}$$

In words, Theorem 3.6 means that the shape enumerator of any binary linear self-dual NRT code C in $M_{n,2}(\mathbb{F}_2)$ is a polynomial in ϕ_1, ϕ_2, and ϕ_3.

3.2.1 Invariant ring for Doubly-even self-dual NRT codes in $M_{n,2}(\mathbb{F}_2)$

Let us now consider that C is a doubly-even linear self-dual NRT code in $M_{n,2}(\mathbb{F}_2)$, i.e., a self-dual NRT code C whose every codeword of C has even weight. From the definition of shape enumerator of C, it follows that $H_C(z_0, z_1, z_2) \in \mathbb{C}[z_0, z_1, z_2]$ is such that z_1 always has even degree. So in this case

$$H_C(z_0, z_1, z_2) = H_C(z_0, -z_1, z_2).$$

Thats is, H_C is invariant by

$$A := \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Since C is a self-dual NRT code, we already known that H_C is also invariant by the action of the matrix T given in (3.3). Finally, the shape enumerator H_C of C is invariant by the group $G_2 = \langle T, A \rangle$. It is easy to check that

$$G_2 = \{I, A, T, AT, TA, TAT\}, \tag{3.4}$$

where

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, T = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & 1 \\ \frac{1}{2} & \frac{1}{2} & -1 \\ \frac{1}{2} & -\frac{1}{2} & 0 \end{bmatrix}, AT = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & 1 \\ -\frac{1}{2} & -\frac{1}{2} & 1 \\ \frac{1}{2} & -\frac{1}{2} & 0 \end{bmatrix},$$

$$TA = \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} & 1 \\ \frac{1}{2} & -\frac{1}{2} & -1 \\ \frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix}, TAT = \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} & 1 \\ -\frac{1}{2} & \frac{1}{2} & 1 \\ \frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix}, I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Simple computations show that:

i) $\det(I) = 1$ iii) $\det(T) = -1$ v) $\det(TA) = 1$

ii) $\det(A) = -1$ iv) $\det(AT) = 1$ vi) $\det(TAT) = -1$.

and

i) $\det(I - \lambda I_3) = (1-\lambda)^3$ iv) $\det(AT - \lambda I_3) = (1-\lambda^3)$

ii) $\det(A - \lambda I_3) = (1-\lambda^2)(\lambda - 1)$ v) $\det(TA - \lambda I_3) = (1-\lambda^3)$

iii) $\det(T - \lambda I_3) = (\lambda - 1)(1-\lambda^2)$ vi) $\det(TAT - \lambda I_3) = (1-\lambda^2)(\lambda - 1)$.

Hence the Molien's series of G_2 is given by

$$\begin{aligned} \Phi_{G_2}(\lambda) &= \frac{1}{6} \sum_{A \in G_2} \frac{\det(A)}{\det(A - \lambda I_3)} \\ &= \frac{1}{6} \left(\frac{2}{1-\lambda^3} + \frac{1}{(1-\lambda)^3} + \frac{3}{(1-\lambda^2)(1-\lambda)} \right) \\ &= \frac{1}{6} \left(\frac{2(1-\lambda)^3(1-\lambda^2) + (1-\lambda^3)(1-\lambda^2) + 3(1-\lambda)^2(1-\lambda^3)}{(1-\lambda^3)(1-\lambda)^3(1-\lambda^2)} \right) \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{6}\left(\frac{(1-\lambda)(-\lambda^4-\lambda^3+\lambda+1)+3(1-\lambda)^2(1-\lambda^3)+2(1-\lambda)^3(1-\lambda^2)}{(1-\lambda^3)(1-\lambda)^3(1-\lambda^2)}\right)\\
&= \frac{1}{6}\left(\frac{-\lambda^4-\lambda^3+\lambda+)+3(1-\lambda)^2(1-\lambda^3)+2(1-\lambda)^3(1-\lambda^2)}{(1-\lambda^3)(1-\lambda)^2(1-\lambda^2)}\right)\\
&= \frac{1}{6}\left(\frac{-\lambda^4-\lambda^3+\lambda+1+\lambda^4+\lambda^3-7\lambda+5}{(1-\lambda)^2(1-\lambda^2)(1-\lambda^3)}\right)\\
&= \frac{1}{6}\left(\frac{6-6\lambda}{(1-\lambda)^2(1-\lambda^2)(1-\lambda^3)}\right)\\
&= \frac{1}{(1-\lambda)(1-\lambda^2)(1-\lambda^3)}.
\end{aligned}
$$

It suggests that we should search for one invariant of degree one, one invariant of degree two and one invariant of degree three in order to determine a polynomial basis of invariants. The code $C_{1,1} = \{(0,0),(0,1)\}$ is such that $C_{1,1}$ is a self-dual NRT code and all its codewords has even weight. Moreover, $H_{C_{1,1}}(z_0,z_1,z_2) = z_0 + z_2$ is a G_2-invariant. Now consider $C_{2,1}$ in $M_{2,2}(\mathbb{F}_2)$ given by

$$
C_{2,1} := \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \right\}.
$$

The code $C_{2,1}$ is a self-dual NRT code and all its codewords have even weight. Furthermore, the shape enumerator of $C_{2,1}$ is the polynomial $H_{C_{2,1}}(z_0,z_1,z_2) = z_0^2 + z_1^2 + 2z_2^2$, which is of course, an invariant polynomial of the group G_2. Putting p_1 and p_2 as $p_1(z_0,z_1,z_2) = z_0 + z_2$ and $p_2(z_0,z_1,z_2) = z_0^2 + z_1^2 + 2z_2^2$, we have an algebraically independent set $\{p_1,p_2\}$. So, we just need do find another polynomial $p_3(z_0,z_1,z_2)$ such that p_3 is algebraically independent of p_1 and p_2.

Define $C_{3,3}$ in $M_{3,2}(\mathbb{F}_2)$ by

$$
C_{3,3} := \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix} \right\}
$$

The code $C_{3,3}$ is a self-dual NRT code, and all its codewords have even weight. Moreover, the shape enumerator $H_{C_{3,3}}(z_0,z_1,z_2) = z_0^3 + 4z_2^3 + 3z_1^2z_0$ of $C_{3,3}$ is invariant under G_2. Defining

$p_3(z_0, z_1, z_2) = H_{C_{3,3}}(z_0, z_1, z_2)$, we claim that the set $\{p_1, p_2, p_3\}$ is algebraically independent. Since

$$\begin{aligned}
\bigtriangledown p_1(z_0, z_1, z_2) &= (1, 0, 1) \\
\bigtriangledown p_2(z_0, z_1, z_2) &= (2z_0, 2z_1, 4z_2) \\
\bigtriangledown p_3(z_0, z_1, z_2) &= (3z_0^2 + 3z_1^2, 6z_1z_0, 12z_2^2).
\end{aligned}$$

We obtain

$$\begin{aligned}
\det(J(p_1, p_2, p_3)) &= \det \begin{bmatrix} 1 & 0 & 1 \\ 2z_0 & 2z_1 & 4z_2 \\ 3z_0^2 + 3z_1^2 & 6z_0z_1 & 12z_2^2 \end{bmatrix} \\
&= 24z_2^2z_1 + 6z_0^2z_1 - 6z_1^3 - 24z_0z_1z_2 \neq 0.
\end{aligned}$$

By Jacobian criteria. Summing up, we have just proved the following:

Theorem 3.7. *Let C be a self-dual NRT code in $M_{n,2}(\mathbb{F}_2)$ such that all its codewords has even weight. Then, the shape enumerator of C is an invariant polynomial for the group G_2 given in (3.4). Moreover, the invariant ring of G_2 is $\mathbb{C}[p_1, p_2, p_3]$, where the polynomials p_1, p_2, and p_3 are given by*

$$\begin{aligned}
p_1(z_0, z_1, z_2) &= z_0 + z_2; \\
p_2(z_0, z_1, z_2) &= z_0^2 + z_1^2 + 2z_2^2; \\
p_3(z_0, z_1, z_2) &= z_0^3 + 4z_2^3 + 3z_1^2z_0.
\end{aligned}$$

In other words, if C is a self-dual NRT code in $M_{n,2}(\mathbb{F}_2)$ whose codewords have even weight then its shape enumerator is a polynomial in p_1, p_2 and p_3.

3.2.2 Invariant ring for Doubly-doubly-even self-dual NRT codes in $M_{n,2}(\mathbb{F}_2)$

Let C be a self-dual NRT code in $M_{n,2}(\mathbb{F}_2)$ whose every codeword has an even number of rows with weight one and an even number of rows with weight two. In this case, by definition of shape enumerator, $H_C(z_0, z_1, z_2)$ is such that z_1 and z_2 are always of degree even, therefore, $H_C(z_0, z_1, z_2) = H_C(z_0, -z_1, -z_2)$ holds. This implies that $H_C(z_0, z_1, z_2)$, the shape enumerator of C, is invariant under the action of the matrix

$$B := \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

Since C is a self-dual NRT code it also follows that H_C is invariant by the matrix T defined in (3.3), and therefore the polynomial H_C is invariant under the action of the group

$$G_3 := \langle T, B \rangle. \tag{3.5}$$

We can check that $|G_3| = 12$. More precisely, G_3 is the following group:

$$\left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & 1 \\ \frac{1}{2} & \frac{1}{2} & -1 \\ \frac{1}{2} & -\frac{1}{2} & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} & -1 \\ \frac{1}{2} & -\frac{1}{2} & 1 \\ \frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix} \right.$$

$$\begin{bmatrix} \frac{1}{2} & \frac{1}{2} & 1 \\ -\frac{1}{2} & -\frac{1}{2} & 1 \\ -\frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix}, \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} & 1 \\ \frac{1}{2} & -\frac{1}{2} & 1 \\ \frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} & -1 \\ -\frac{1}{2} & \frac{1}{2} & -1 \\ -\frac{1}{2} & -\frac{1}{2} & 0 \end{bmatrix}, \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} & 1 \\ -\frac{1}{2} & \frac{1}{2} & -1 \\ -\frac{1}{2} & -\frac{1}{2} & 0 \end{bmatrix}$$

$$\left. \begin{bmatrix} -\frac{1}{2} & -\frac{1}{2} & -1 \\ \frac{1}{2} & \frac{1}{2} & -1 \\ \frac{1}{2} & -\frac{1}{2} & 0 \end{bmatrix} \begin{bmatrix} -\frac{1}{2} & -\frac{1}{2} & -1 \\ -\frac{1}{2} & -\frac{1}{2} & 1 \\ -\frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \right\}$$

Note that

$$\frac{1}{|G_3|} \sum_{A_i \in G_3} \text{trace}(A_i) = 0.$$

Therefore, there is no invariant of degree one. Let's calculate the Molien's series of G_3. Initially, note that

i) $\det(I) = 1$

ii) $\det(A) = -1$

iii) $\det(T) = -1$

iv) $\det(A_3) = -1$

v) $\det(A_4) = -1$

vi) $\det(A_5) = 1$

vii) $\det(A_6) = -1$

viii) $\det(A_7) = 1$

ix) $\det(A_8) = 1$

x) $\det(A_9) = -1$

xi) $\det(A_{10}) = 1$

xii) $\det(A_{11}) = -1.$

And is also easy to check that

i) $\det(I - \lambda I) = (1 - \lambda)^3$

ii) $\det(A - \lambda I) = (1 - \lambda)(1 - \lambda)^2$

iii) $\det(T - \lambda I) = (1 - \lambda^2)$

iv) $\det(A_3 - \lambda I) = (1 + \lambda^3)$

v) $\det(A_4 - \lambda I) = 1 + \lambda^3$

vi) $\det(A_5 - \lambda I) = (1 - \lambda)(1 + \lambda)^2$

vii) $\det(A_6 - \lambda I) = (1 - \lambda)(1 - \lambda^2)$

viii) $\det(A_7 - \lambda I) = 1 - \lambda^3$

ix) $\det(A_8 - \lambda I) = 1 - \lambda^3$

x) $\det(A_9 - \lambda I) = (1 - \lambda)(1 - \lambda^2)$

xi) $\det(A_{10} - \lambda I) = (1 - \lambda)(1 + \lambda)^2$

xii) $\det(A_{11} - \lambda I) = (1 + \lambda)^3$.

The Molien's series of G_3 becomes

$$\begin{aligned}
\Phi_{G_3}(\lambda) &= \frac{1}{12}\left(\frac{1}{(1-\lambda)^3} + \frac{1}{(1+\lambda)^3} + \frac{3}{(1-\lambda)(1+\lambda)^2} + \frac{3}{(1-\lambda)(1-\lambda^2)} + \frac{2}{1+\lambda^3} + \frac{2}{1-\lambda^3}\right) \\
&= \frac{1}{12}\left(\frac{12 + 12\lambda^4}{(1-\lambda^2)^2(1-\lambda^6)}\right) \\
&= \frac{1+\lambda^4}{(1-\lambda^2)^2(1-\lambda^6)} \\
&= \frac{1}{(1-\lambda^2)^2(1-\lambda^6)} + \frac{\lambda^4}{(1-\lambda^2)^2(1-\lambda^6)},
\end{aligned}$$

which suggests that in order to obtain a good polynomial basis for $\mathcal{J}(G_3)$ we should search for three primary invariants ϕ_1, ϕ_2, and ϕ_3 of degree $2, 2, 6$ respectively, and one secondary invariant ϕ_4 of degree 4.

Unfortunately, there exists only one linear code C in $M_{2,2}(\mathbb{F}_2)$ such that the required properties are satisfied, namely $C_{2,2}$ of the previous section, so we can choose the polynomial ϕ_1 as $\phi_1(z_0, z_1, z_2) = H_{C_{2,2}}(z_0, z_1, z_2) = z_0^2 + z_1^2 + 2z_2^2$. By averaging z_0^2 under the group G_3, using the Reynolds operator, we obtain the invariant $\phi_2(z_0, z_1, z_2) = 5z_0^2 - 2z_0z_1 + z_1^2 + 8z_2^2 + 8z_2z_1$.

Now we will work to find an invariant of degree six. Averaging z_1z_2 over the group G_3, using again the Reynolds operator, we obtain a homogeneous invariant $\phi_3^\star$ of degree two, namely $\phi_3^\star(z_0, z_1, z_2) = 2z_0^2 - 2z_1^2 + 8z_1z_2$. The set $\{\phi_1, \phi_2, \phi_3^\star\}$ is algebraically independent. Indeed, we need to show that the Jacobian matrix of $\phi_1, \phi_2, \phi_3^\star$ has determinant nonzero. It is easy to check that

$$\begin{aligned}
\bigtriangledown\phi_1(z_0, z_1, z_2) &= (2z_0, 2z_1, 4z_2) \\
\bigtriangledown\phi_2(z_0, z_1, z_2) &= (10z_0 - 2z_1, 2z_1 - 2z_0 + 8z_2, 16z_2 + 8z_1) \\
\bigtriangledown\phi_3^\star(z_0, z_1, z_2) &= (4z_0, -4z_1 + 8z_2, 8z_1).
\end{aligned}$$

Therefore,

$$\begin{aligned}\det(J(\phi_1,\phi_2,\phi_3^\star)) &= \det\begin{bmatrix} 2z_0 & 2z_1 & 4z_2 \\ 10z_0-2z_1 & 2z_1-2z_0+8z_2 & 18z_2+8z_1 \\ 4z_0 & -4z_1+8z_2 & 8z_1 \end{bmatrix} \\ &= 16(-2z_0^2z_1+2z_0^2z_2+4z_0z_1z_2-4z_0z_2^2+2z_1^3+2z_1^2z_2-4z_1z_2^2) \\ &\neq 0\end{aligned}$$

proving that $\{\phi_1,\phi_2,\phi_3^\star\}$ is algebraically independent. Let $\phi_3 \in \mathbb{C}[z_0,z_1,z_2]$ be the polynomial given by $\phi_3 = (\phi_3^\star)^3$, so $\deg\phi_3 = 6$ and $\{\phi_1,\phi_2,\phi_3\}$ is algebraically independent. Of course, if this set is algebraically dependent then there exists constants not all null, such that

$$\sum_{i,j,k} c_{i,j,k}\phi_1^i\phi_2^j\phi_3^k = 0.$$

In this way there are constants not all zero $c_{i,j,k}$ such that

$$\sum_{i,j,k} c_{i,j,k}\phi_1^i\phi_2^j(\phi_3^\star)^{3k} = 0.$$

That is impossible once that $\{\phi_1,\phi_2,\phi_3^\star\}$ is an algebraically independent set.

The polynomial ϕ_4 can be obtained through some algorithms found in the literature [12, 24, 74, 25]. This process will be omitted because needs more theory about invariant polynomials. We use Magma Computer Algebra program [6] to find the secondary invariant $\phi_4(z_0,z_1,z_2) = z_0^4+6z_0^2z_1z_2-z_1^4+2z_1^3z_2+8z_1z_2^3$.

Theorem 3.8. *Let C be a self-dual NRT code in $M_{n,2}(\mathbb{F}_2)$ such that all its codewords has an even number of rows with weight one, and an even number of rows with weight two. Then, the shape enumerator of C is an invariant polynomial for the group G_3 given in (3.5). Moreover, the invariant ring of G_3 is $\mathbb{C}[\phi_1,\phi_2,\phi_3]\oplus\phi_4\mathbb{C}[\phi_1,\phi_2,\phi_3]$, where the polynomials ϕ_1,ϕ_2 and ϕ_3 are:*

$$\begin{aligned}\phi_1(z_0,z_1,z_2) &= z_0^2+z_1^2+2z_2^2; \\ \phi_2(z_0,z_1,z_2) &= 5z_0^2-2z_0z_1+z_1^2+8z_2^2+8z_2z_1; \\ \phi_3(z_0,z_1,z_2) &= \left(2z_0^2-2z_1^2+8z_1z_2\right)^2;\end{aligned}$$

and

$$\phi_4(z_0,z_1,z_2) = z_0^4+6z_0^2z_1z_2-z_1^4+2z_1^3z_2+8z_1z_2^3.$$

In other words, if C is a self-dual NRT code in $M_{n,2}(\mathbb{F}_2)$ whose every codeword has an even number of rows with weight one and an even number of rows with weight two its shape enumerator is a polynomial in ϕ_1,ϕ_2 and ϕ_3 plus ϕ_4 times another such polynomial.

3.3 The general case for self-dual NRT codes in $M_{n,s}(\mathbb{F}_2)$

For the purpose of studying the shape enumerator of a self dual NRT code C in $M_{n,s}(\mathbb{F}_2)$, we will first look closely at the matrix Θ_s. We know that $\Theta_s \in M_{s+1,s+1}(\mathbb{F}_2)$, where $\Theta_s = (\theta_{l,k})_{l,k=0,\cdots,s}$ is given by the following rules

$$\theta_{l,k} := \begin{cases} 1 & \text{if} \quad k = 0 \\ 2^{l-1} & \text{if} \quad 0 < k \leqslant s - l \\ -2^{l-1} & \text{if} \quad l + k = s + 1 \\ 0 & \text{if} \quad l + k > s + 1 \end{cases},$$

that is,

$$\Theta_s := \begin{bmatrix} 1 & 1 & 2 & 4 & \cdots & 2^{s-4} & 2^{s-3} & 2^{s-2} & 2^{s-1} \\ 1 & 1 & 2 & 4 & \cdots & 2^{s-4} & 2^{s-3} & 2^{s-2} & -2^{s-1} \\ 1 & 1 & 2 & 4 & \cdots & 2^{s-4} & 2^{s-3} & -2^{s-2} & 0 \\ 1 & 1 & 2 & 4 & \cdots & 2^{s-4} & -2^{s-3} & 0 & 0 \\ 1 & 1 & 2 & 4 & \cdots & -2^{s-4} & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & 2 & -4 & \cdots & 0 & 0 & 0 & 0 \\ 1 & 1 & -2 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \end{bmatrix}.$$

We will show that Θ_s have the following properties:

Theorem 3.9. *The matrix Θ_s given by $\Theta_s = (\theta_{l,k})_{l,k=0,\ldots,s}$ where*

$$\theta_{l,k} := \begin{cases} 1 & \textit{if} \quad k = 0, \\ 2^{k-1} & \textit{if} \quad 0 < k \leqslant s - l, \\ -2^{k-1} & \textit{if} \quad l + k = s + 1, \\ 0 & \textit{if} \quad l + k > s + 1, \end{cases}$$

satisfies the following properties:

a) $\Theta_s^2 = 2^s I_{s+1}$

b) $\operatorname{trace}(\Theta_s) = \begin{cases} 2^{\frac{s}{2}} & \textit{if} \quad s \quad \textit{is} \quad \textit{even} \\ 0 & \textit{if} \quad s \quad \textit{is} \quad \textit{odd} \end{cases}$

c) $\det(\Theta_s) := \begin{cases} (-1)^{\frac{s+1}{2}} 2^{\frac{s(s+1)}{2}} & \textit{if} \quad s \quad \textit{is} \quad \textit{odd} \\ (-1)^{\frac{s}{2}} 2^{\frac{s(s+1)}{2}} & \textit{if} \quad s \quad \textit{is} \quad \textit{even} \end{cases}$

Proof. Item a) is immediate and also is also observed in [15]. So we will prove items b) and c).

b) By definition of Θ_s, we have that $\mathrm{trace}(\Theta_s) = \sum_{i=0}^{s} \theta_{ii}$, where

$$\theta_{ii} := \begin{cases} 1 & \text{if} \quad i = 0 \\ 2^{i-1} & \text{if} \quad 0 < i \leqslant s - i \\ -2^{i-1} & \text{if} \quad 2i = s + 1 \\ 0 & \text{if} \quad 2i > s + 1 \end{cases}.$$

If s is even then the trace of Θ_s becomes

$$\begin{aligned} \mathrm{trace}(\Theta_s) &= \sum_{i=0}^{s} \theta_{ii} \\ &= 1 + \sum_{i=1}^{s} \theta_{ii} \\ &= 1 + \sum_{i=1}^{\frac{s}{2}} \theta_{ii} + \sum_{i=\frac{s}{2}+1}^{s} \theta_{ii} \\ &= 1 + \sum_{i=1}^{\frac{s}{2}} 2^{i-1} + \sum_{i=\frac{s}{2}+1}^{s} 0 \\ &= 1 + 2^{\frac{s}{2}} - 1 \\ &= 2^{\frac{s}{2}}. \end{aligned}$$

On the other hand, if s is odd the trace of Θ_s will be

$$\begin{aligned} \mathrm{trace}(\Theta_s) &= \sum_{i=0}^{s} \theta_{ii} \\ &= 1 + \sum_{i=1}^{\frac{s-1}{2}} \theta_{ii} + \theta_{\frac{s+1}{2},\frac{s+1}{2}} + \sum_{i=\frac{s+1}{2}+1}^{s} \theta_{ii} \\ &= 1 + \sum_{i=1}^{\frac{s-1}{2}} 2^{i-1} + (-2^{\frac{s+1}{2}} - 1) + \sum_{i=\frac{s+1}{2}+1}^{s} 0 \\ &= 1 + (2^{\frac{s-1}{2}} - 1) - 2^{\frac{s-1}{2}} + 0 \\ &= 0. \end{aligned}$$

And we have just proved that

$$\mathrm{trace}(\Theta_s) = \begin{cases} 2^{\frac{s}{2}} & \text{if} \quad s \quad \text{is} \quad \text{even}, \\ 0 & \text{if} \quad s \quad \text{is} \quad \text{odd}. \end{cases}$$

c) Setting $\Theta_0 = 1$ and applying Laplace expansion along the last column of Θ_s, we find for every $s \geq 1$.

$$\det(\Theta_s) = 2^{s-1}(-1)^s \det(\Theta_{s-1}) - 2^{s-1}(-1)^{s+1} \det(\Theta_{s-1}) = 2^s(-1)^s \det(\Theta_{s-1}). \quad (3.6)$$

If $s \geqslant 2$ is even, we will show that by induction on s

$$\det(\Theta_s) = (-1)^{\frac{s}{2}} 2^{\frac{s(s+1)}{2}}. \quad (3.7)$$

Indeed,

$$\begin{aligned} \det(\Theta_2) &= 2^2(-1)^2 \det(\Theta_1) \\ &= 4 \det(\Theta_1) \\ &= -8 \\ &= (-1)^{\frac{2}{2}} 2^{\frac{2(2+1)}{2}}. \end{aligned}$$

proving the result for $s = 2$. Suppose that the result is true for $s = 2t$, that is,

$$\det(\Theta_{2t}) = (-1)^{\frac{2t}{2}} 2^{\frac{2t(2t+1)}{2}}.$$

We will prove that the same is true for $s = 2t + 2$. More precisely,

$$\det(\Theta_{2t+2}) = (-1)^{\frac{2t+2}{2}} 2^{\frac{(2t+2)(2t+3)}{2}}.$$

Indeed,

$$\begin{aligned} \det(\Theta_{2t+2}) &= 2^{2t+2}(-1)^{2t+2} \det(\Theta_{2t+1}) \\ &= 2^{2t+2} \det(\Theta_{2t+1}), (*) \end{aligned}$$

and

$$\begin{aligned} \det(\Theta_{2t+1}) &= 2^{2t+1}(-1)^{2t+1} \det(\Theta_{2t}) \\ &= -2^{2t+1} \det(\Theta_{2t}), (**) \end{aligned}$$

Replacing $(**)$ in $(*)$,

$$\begin{aligned} \det(\Theta_{2t+2}) &= (-2^{2t+1} \det(\Theta_{2t})) \\ &= 2^{2t+2}(-2)^{2t+1}(-1)^{\frac{2t}{2}} 2^{\frac{2t(2t+1)}{2}} \\ &= (-1)^{\frac{2t+2}{2}} 2^{4t+3} 2^{\frac{2t(2t+1)}{2}} \end{aligned}$$

$$\begin{aligned} &= (-1)^{\frac{2t+2}{2}} 2^{\frac{4t^2+10t+6}{2}} \\ &= (-1)^{\frac{2t+2}{2}} 2^{\frac{(2t+2)(2t+3)}{2}}. \end{aligned}$$

This concludes the proof for s even.

Suppose that $s \geqslant 1$ is odd. We will show by induction on s that

$$\det(\Theta_s) = (-1)^{\frac{s-1}{2}} 2^{\frac{s(s+1)}{2}}.$$

For $s = 1$ the result is clearly true. Let us assume that the result is true for $s = 2t + 1$, that is,

$$\det(\Theta_{2t+1}) = (-1)^{\frac{2t+2}{2}} 2^{\frac{(2t+1)(2k+2)}{2}}.$$

We will show that for $s = 2t + 3$

$$\det(\Theta_{2t+3}) = (-1)^{\frac{2t+4}{2}} 2^{\frac{(2t+3)(2t+4)}{2}}.$$

Indeed, Again by Laplace's Theorem,

$$\begin{aligned} \det(\Theta_{2t+3}) &= 2^{2t+3}(-1)^{2t+3} \det(\Theta_{2t+2}) \\ &= -2^{2t+3} \det(\Theta_{2t+2}) \quad (\triangle). \end{aligned}$$

since $2t + 2$ is even we can use Equation (3.7),

$$\det(\Theta_{2t+2}) = (-1)^{\frac{2t+2}{2}} 2^{\frac{(2t+2)(2t+3)}{2}} \quad (\blacktriangle)$$

replacing $(\blacktriangle)$ in $(\triangle)$

$$\begin{aligned} \det(\Theta_{2t+3}) &= -2^{2k+3} \det(\Theta_{2t+2}) \\ &= -2^{2t+3}(-1)^{\frac{2t+2}{2}} 2^{\frac{(2t+2)(2t+3)}{2}} \\ &= (-1)^{\frac{2t+4}{2}} 2^{\frac{2(2t+3)+(2t+2)(2t+3)}{2}} \\ &= (-1)^{\frac{2t+4}{2}} 2^{\frac{(2t+3)(2t+4)}{2}}. \end{aligned}$$

for any odd number s, concluding the proof of c).

□

Theorem 3.10. *Let m_{Θ_s} and P_{Θ_s} be the minimal and the characteristic polynomials respectively of the matrix Θ_s in Theorem 3.9. Then,*

$$m_{\Theta_s}(\lambda) = (\lambda - 2^{\frac{s}{2}})(\lambda + 2^{\frac{s}{2}}),$$

and

$$p_{\Theta_s}(\lambda) = \begin{cases} (\lambda - 2^{\frac{s}{2}})^{\frac{s+2}{2}}(\lambda + 2^{\frac{s}{2}})^{\frac{s}{2}} & \textit{if } s \textit{ is even} \\ (\lambda - 2^{\frac{s}{2}})^{\frac{s+1}{2}}(\lambda + 2^{\frac{s}{2}})^{\frac{s+1}{2}} & \textit{if } s \textit{ is odd} \end{cases}.$$

Proof. Item a) of Theorem 3.9 states that

$$0 = \Theta_s^2 - 2^s I_{s+1} = (\Theta_s - 2^{\frac{s}{2}} I_{s+1})(\Theta_s + 2^{\frac{s}{2}} I_{s+1})$$

and it follows that $m_{\Theta_s}(\lambda) = (\lambda - 2^{\frac{s}{2}})(\lambda + 2^{\frac{s}{2}})$ is the minimal polynomial of Θ_s, since m_{Θ_s} is a monic polynomial of degree two such that $m_{\Theta_s}(\Theta_s) = 0$ and obviously no polynomial of degree one vanishes on Θ_s. Therefore, the characteristic polynomial of Θ_s decomposes as a product

$$p_{\Theta_s}(\lambda) = (\lambda - 2^{\frac{s}{2}})^{r_1}(\lambda + 2^{\frac{s}{2}})^{r_2}, \tag{3.8}$$

where r_1 and r_2 are the multiplicities of the eigenvalues $\beta_1 = 2^{\frac{s}{2}}$ and $\beta_2 = -2^{\frac{s}{2}}$. In particular, $r_1 + r_2 = s + 1$. From (3.8) it follows that

$$\mathrm{trace}(\Theta_s) = r_1(2^{\frac{s}{2}}) + r_2(-2^{\frac{s}{2}}), \tag{3.9}$$

and therefore for every $s \geq 1$ we have the system of equations

$$\begin{cases} r_1 + r_2 &= s + 1 \\ r_1 - r_2 &= \dfrac{\mathrm{trace}(\Theta_s)}{2^{\frac{s}{2}}} \end{cases}.$$

If s is an odd number, then $\mathrm{trace}(\Theta_s) = 0$ by Item b) of Theorem 3.9. In this case, the above system has $r_1 = r_2 = \frac{s+1}{2}$ as unique solution. Therefore, in the case of an odd s, the characteristic polynomial of Θ_s is

$$p_{\Theta_s}(\lambda) = (\lambda - 2^{\frac{s}{2}})^{\frac{s+1}{2}}(\lambda + 2^{\frac{s}{2}})^{\frac{s+1}{2}}.$$

If s is even, then $\mathrm{trace}(\Theta_s) = 2^{\frac{s}{2}}$, and the corresponding system of equations has solution $r_1 = \frac{s+2}{2}, r_2 = \frac{s}{2}$. In this case the characteristic polynomial of Θ_s is

$$p_{\Theta_s}(\lambda) = (\lambda - 2^{\frac{s}{2}})^{\frac{s+2}{2}}(\lambda + 2^{\frac{s}{2}})^{\frac{s}{2}}.$$

We have just proved that $p_{\Theta_s}(\lambda) = \begin{cases} (\lambda - 2^{\frac{s}{2}})^{\frac{s+2}{2}}(\lambda + 2^{\frac{s}{2}})^{\frac{s}{2}} & \text{if } s \text{ is even} \\ (\lambda - 2^{\frac{s}{2}})^{\frac{s+1}{2}}(\lambda + 2^{\frac{s}{2}})^{\frac{s+1}{2}} & \text{if } s \text{ is odd} \end{cases}$ □

3.3.1 Shape enumerator for self-dual NRT codes in $M_{n,s}(\mathbb{F}_2)$ with odd s

The main purpose of this subsection is to utilize the properties of the shape enumerator of a self-dual NRT code in $M_{n,s}(\mathbb{F}_2)$ and the properties of the matrix Θ_s to obtain information about an invariant ring that contains the shape enumerators of self-dual NRT codes.

Recall that Theorem 2.16 states that the shape enumerator H_C of a self-dual NRT code C in $M_{n,s}(\mathbb{F}_2)$, satisfies the equation

$$H_C(z_0, \ldots, z_s) = \frac{1}{|C|} H_C(\Theta_s(z_0, \ldots, z_s)), \tag{3.10}$$

which can be rewriten as

$$\begin{aligned} H_C(z_0, \ldots, z_s) &= \frac{1}{2^{\frac{ns}{2}}} H_C(\Theta_s(z_0, \ldots, z_s)) \\ &= H_C\left(\frac{\Theta_s}{2^{\frac{s}{2}}}(z_0, \ldots, z_s)\right). \end{aligned}$$

In polynomial invariant theory language, this is equivalent to saying that H_C is invariant by

$$T = \frac{\Theta_s}{2^{\frac{s}{2}}}. \tag{3.11}$$

So H_C will be invariant under the cyclic group G generated by T. Note also that from Item a) of Theorem 3.9

$$T^2 = \left(\frac{\Theta_s}{2^{\frac{s}{2}}}\right)^2 = \frac{\Theta_s^2}{2^s} = I_{s+1},$$

and the group G is given by $G = \langle T \rangle = \{I_{s+1}, T\}$. Since G is finite, it is well-known that $\mathcal{J}(G)$ has a good polynomial basis of invariants [29].

Let us calculate the Molien's series of G which tells us what kind of invariants we should looking for. Since s is odd

i) $\mathrm{trace}(T) = 0$;

ii) $\det(T) = (-1)^{\frac{s+1}{2}}$;

iii) $p_T(\lambda) = (-1)^{\frac{s+1}{2}}(1-\lambda)^{\frac{s+1}{2}}(1+\lambda)^{\frac{s+1}{2}}$.

Thus,

$$\begin{aligned} \Phi(\lambda) &= \frac{1}{2}\sum_{A \in G} \frac{\det(A)}{\det(A - \lambda I_{s+1})} \\ &= \frac{1}{2}\left[\frac{(-1)^{\frac{s+1}{2}}}{(-1)^{\frac{s+1}{2}}(1-\lambda)^{\frac{s+1}{2}}(1+\lambda)^{\frac{s+1}{2}}} + \frac{1}{(1-\lambda)^{s+1}}\right] \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{2}\frac{(1-\lambda)^{\frac{s+1}{2}}+(1+\lambda)^{\frac{s+1}{2}}}{(1+\lambda)^{\frac{s+1}{2}}(1-\lambda)^{s+1}} \\
&= \frac{1}{2}\frac{\sum_{k=0}^{\frac{s+1}{2}}\binom{\frac{s+1}{2}}{k}\lambda^k+\sum_{k=0}^{\frac{s+1}{2}}\binom{\frac{s+1}{2}}{k}(-\lambda)^k}{(1-\lambda)^{\frac{s+1}{2}}(1-\lambda^2)^{\frac{s+1}{2}}}.
\end{aligned}
$$

Consider the subcase of $\frac{s+1}{2}$ even, that is, $\frac{s+1}{2} = 2t$ for some $t \geq 0$. The Molien's series of G can be rewritten as

$$
\begin{aligned}
\Phi(\lambda) &= \frac{1}{2}\frac{\sum_{k=0}^{2t}\binom{2t}{k}\lambda^k+\sum_{k=0}^{2t}\binom{2t}{k}(-\lambda)^k}{(1-\lambda)^{2t}(1-\lambda^2)^{2t}} \\
&= \frac{1}{2}\frac{2\sum_{l=0}^{t}\binom{2t}{2l}\lambda^{2l}}{(1-\lambda)^{2t}(1-\lambda^2)^{2t}}.
\end{aligned}
$$

Hence, in this case

$$
\Phi(\lambda) = \frac{\sum_{l=0}^{t}\binom{2t}{2l}\lambda^{2l}}{(1-\lambda)^{2t}(1-\lambda^2)^{2t}}. \tag{3.12}
$$

Note that the term $(1-\lambda)^{2t}$ in the denominator indicates that to form a good basis we should looking for $\frac{s+1}{2}$ invariants of degree one, but by Theorem 1.17, and Item b) of Theorem 3.9 there are no invariant polynomials under G of degree one. So we are not using all the information about the shape enumerator of C.

Since the dimension of C is $k = \frac{ns}{2}$ and s is an odd number we must have n even, which implies that H_C will be invariant by $-I$, so H_C is invariant under the action of the group

$$
G_1 := \{-I, I, -T, T\}.
$$

It is easy to see that the Molien's series of G_1 can be written as

$$
\Phi_{G_1}(\lambda) = \frac{1}{2}\left(\Phi_G(\lambda) + \Phi_G(-\lambda)\right),
$$

and so

$$
\begin{aligned}
\Phi_{G_1}(\lambda) &= \frac{1}{2}\frac{\sum_{l=0}^{t}\binom{2t}{2l}\lambda^{2l}}{(1-\lambda)^{2t}(1-\lambda^2)^{2t}} + \frac{\sum_{l=0}^{t}\binom{2t}{2l}\lambda^{2l}}{(1+\lambda)^{2t}(1-\lambda^2)^{2t}} \\
&= \frac{1}{2}\frac{\sum_{l=0}^{t}\binom{2t}{2l}\lambda^{2l}\left[(1+\lambda)^{2t}+(1-\lambda)^{2t}\right]}{(1-\lambda)^{2t}(1+\lambda)^{2t}(1-\lambda^2)^{2t}}
\end{aligned}
$$

$$= \frac{1}{2}\frac{\sum_{l=0}^{t}\binom{2t}{2l}\lambda^{2l}\left[2\sum_{l=0}^{t}\binom{2t}{2l}\lambda^{2l}\right]}{(1-\lambda^2)^{4t}}$$
$$= \frac{\left[\sum_{l=0}^{t}\binom{2t}{2l}\lambda^{2l}\right]^2}{(1-\lambda^2)^{4t}}.$$

Now, if we consider the sub-case where $\frac{s+1}{2}$ is odd, $\frac{s+1}{2} = 2t+1$, for some $t \geq 0$, then proceeding in the same way as in the even case one obtains the following expression for the Molien's series:

$$\Phi_{G_1}(\lambda) = \frac{\left[\sum_{l=0}^{t}\binom{2t+1}{2l}\lambda^{2l}\right]^2}{(1-\lambda^2)^{4t+2}}.$$

In short, we have proved the following result:

Theorem 3.11. *Let C be a self-dual NRT code in $M_{n,s}(\mathbb{F}_2)$, and suppose that s is an odd number. The shape enumerator H_C of C is invariant under the group $G_1 := \{I, -I, T, -T\}$, where T is given by (3.11), and the Molien's series of G_1 is*

$$\Phi_{G_1}(\lambda) = \begin{cases} \frac{\left[\sum_{l=0}^{t}\binom{2t}{2l}\lambda^{2l}\right]^2}{(1-\lambda^2)^{4t}} & \text{if } \frac{s+1}{2} = 2t, t = 0, 1, \ldots \\ \frac{\left[\sum_{l=0}^{t}\binom{2t+1}{2l}\lambda^{2l}\right]^2}{(1-\lambda^2)^{4t+2}} & \text{if } \frac{s+1}{2} = 2t+1, t = 0, 1, \ldots \end{cases}.$$

Thus, Theorem 3.11 gives us an expectation of how many algebraically independent invariants we must find to form a base of invariants for $\mathcal{J}(G_1)$.

Note that in the case $s = 1$ we have $\frac{s+1}{2} = 1 = 2(0)+1$ and so the Molien's series of G_1 is given by

$$\Phi_{G_1}(\lambda) = \frac{\left[\sum_{l=0}^{0}\binom{1}{2l}\lambda^{2l}\right]}{(1-\lambda^2)^2} = \frac{1}{(1-\lambda^2)^2},$$

which agrees with Theorem 3.3, This fact was expected since the Hamming metric coincides with the NRT-metric in the case where $s = 1$ and the shape enumerator is the Hamming weight enumerator.

3.3.2 Shape enumerator for self-dual NRT codes in $M_{n,s}(\mathbb{F}_2)$ with even s

Following the same steps as in the previous subsection we can prove an analogous result for the case of even s.

Theorem 3.12. *Let C be a self-dual NRT code in $M_{n,s}(\mathbb{F}_2)$ such that s is an even number. The shape enumerator H_C of C is invariant under the group $G := \{I, T\}$, where T is given by (3.11), and the Molien's series of G_1 is*

$$\Phi_G(\lambda) = \begin{cases} \dfrac{\sum_{l=0}^{t} \binom{2t}{2l} \lambda^{2l}}{(1-\lambda^2)^{2t}(1-\lambda)^{2t+1}} & \text{if } \frac{s}{2} = 2t, t = 1, \ldots \\ \dfrac{\sum_{l=0}^{t} \binom{2t+1}{2l} \lambda^{2l}}{(1-\lambda^2)^{2t+1}(1-\lambda)^{2t+2}} & \text{if } \frac{s}{2} = 2t+1, t = 0, 1, \ldots \end{cases}.$$

Theorem 3.12 gives us an expectation of how many algebraically independent invariants we must find to form a base of invariants for $\mathcal{J}(G)$.

Note that for $s = 2$ we have $\frac{s}{2} = 1 = 2(0) + 1$, and so the Molien's series of G is given by

$$\Phi_G(\lambda) = \frac{\sum_{l=0}^{0} \binom{1}{2l} \lambda^{2l}}{(1-\lambda^2)(1-\lambda)^2} = \frac{1}{(1-\lambda^2)(1-\lambda)^2},$$

Which matches with Theorem 3.6 of section 3.2.

Example 3.13. *For $s = 4$, we have $\frac{s}{2} = 2 = 2(1)$ and by Theorem 3.12 the Molien's series of the invariant ring of G is*

$$\Phi_G(\lambda) = \frac{1+\lambda^2}{(1-\lambda)^3(1-\lambda^2)^2}$$

Using Magma Computer Algebra program [6], we find the following basis:

Primary invariants of degree one:

$\phi_1(z_0, z_1, z_2, z_3, z_4) = 5z_0 + z_1 + 2z_2 + 4z_3 + 8z_4$;

$\phi_2(z_0, z_1, z_2, z_3, z_4) = 3z_1 + z_2 + 2z_3 - 6z_4$;

$\phi_3(z_0, z_1, z_2, z_3, z_4) = z_2 - z_3$.

Primary invariants of degree two:

$\phi_4(z_0, z_1, z_2, z_3, z_4) = z_0(z_1 + 2z_2 + 4z_3 - 9z_4) + z_1(2z_2 + 4z_3 - 9z_4) + z_2(8z_3 - 18z_4) - 36z_3z_4 + 2z_2^2 + 9z_1^2 + 8z_3^2 + 32z_4^2$;

$\phi_5(z_0, z_1, z_2, z_3, z_4) = z_0(2z_1 + 4z_2 + 8z_3 + 16z_4) + z_1(4z_2 + 8z_3 + 16z_4) + z_2(16z_3 + 34z_4) + 64z_3z_4 + 17z_0^2 + 4z_2^2 + z_1^2 + 16z_3^2 + 64z_4^2$.

Secondary invariants of degree two:

$\phi_6(z_0, z_1, z_2, z_3, z_4) = z_0^2 - 2z_0z_1 + z_1^2 + 16z_4^2$.

So the shape enumerator H_C of any self-dual NRT code C in $M_{n,4}(\mathbb{F}_2)$ is such that

$$H_C \in \mathbb{C}[\phi_1, \phi_2, \phi_3, \phi_4, \phi_5] \oplus \phi_6\mathbb{C}[\phi_1, \phi_2, \phi_3, \phi_4, \phi_5].$$

Example 3.14. *For $s = 6$, we have $\frac{s}{2} = 3 = 2(1) + 1$ and by Theorem 3.12 the Molien's series of the invariant ring of G is*

$$\Phi_G(\lambda) = \frac{1 + 3\lambda^2}{(1 - \lambda)^4(1 - \lambda^2)^3}$$

Using Magma Computer Algebra program [6], we find the following basis:

Primary invariants of degree one:

$\phi_1(z_0, z_1, z_2, z_3, z_4, z_5, z_6) = 9z_0 + z_1 + 2z_2 + 4z_3 + 8z_4 + 16z_5 + 36z_6$;

$\phi_2(z_0, z_1, z_2, z_3, z_4, z_5, z_6) = 5z_1 + z_2 + 2z_3 + 4z_4 + 8z_5 - 20z_6$;

$\phi_3(z_0, z_1, z_2, z_3, z_4, z_5, z_6) = 3z_2 + z_3 + 2z_4 - 6z_5$;

$\phi_4(z_0, z_1, z_2, z_3, z_4, z_5, z_6) = z_3 - z_4$.

Primary invariants of degree two:

$\phi_5(z_0, z_1, z_2, z_3, z_4, z_5, z_6) = 2^{10}z_5z_6 + 65z_0^2 + z_1^2 + 4z_2^2 + 16z_3^2 + 64z_4^2 + 256z_5^2 + 1024z_6^2 + \sum_{i=1}^{6} 2^i z_0z_i + \sum_{i=2}^{6} 2^i z_1z_i + \sum_{i=3}^{6} 2^{i+1} z_2z_i + \sum_{i=4}^{6} 2^{i+1} z_3z_i + \sum_{i=5}^{6} 2^{i+3} z_4z_i$;

$\phi_6(z_0, z_1, z_2, z_3, z_4, z_5, z_6) = -33z_0z_6 - 33z_1z_6 + 33z_1^2 + 2z_2^2 - 66z_2z_6 + 8z_3^2 - 132z_3z_6 + 32z_4^2 + 128z_4z_5 - 264z_4z_6 + z_5^2 - 528z_5z_6 + 512z_6^2 + \sum_{i=1}^{5} 2^{i-1} z_0z_i + \sum_{i=2}^{5} 2^{i-1} z_1z_i + \sum_{i=3}^{5} 2^i z_2z_i + \sum_{i=4}^{5} 2^{i+1} z_3z_i$;

$\phi_7(z_0, z_1, z_2, z_3, z_4, z_5, z_6) = (z_5 - z_6)(z_0 + z_1 + 2z_2 + 4z_3 + 8z_4 - 16z_6) + z_1^2 - z_2^2$.

Secondary invariants of degree two:

$\phi_8(z_0, z_1, z_2, z_3, z_4, z_5, z_6) = z_0^2 + z_1^2 + 4z_2^2 + 64z_5^2 + z_0(2z_1 - 4z_2) - 4z_1z_2$;

$\phi_9(z_0, z_1, z_2, z_3, z_4, z_5, z_6) = z_0^2 + z_1^2 - 2z_2(z_0 + z_1)$;

$\phi_{10}(z_0, z_1, z_2, z_3, z_4, z_5, z_6) = z_0^2 + z_1^2 + z_6^2 - 2z_0z_2$.

So the shape enumerator H_C of any self-dual code C in $M_{n,6}(\mathbb{F}_2)$ is such that

$$\begin{aligned} H_C \in\ & \mathbb{C}[\phi_1, \phi_2, \phi_3, \phi_4, \phi_5, \phi_6, \phi_7] \oplus \phi_8\mathbb{C}[\phi_1, \phi_2, \phi_3, \phi_4, \phi_5, \phi_6, \phi_7] \\ & \oplus \phi_9\mathbb{C}[\phi_1, \phi_2, \phi_3, \phi_4, \phi_5, \phi_6, \phi_7] \oplus \phi_{10}\mathbb{C}[\phi_1, \phi_2, \phi_3, \phi_4, \phi_5, \phi_6, \phi_7]. \end{aligned}$$

3.4 Open problems

a) In [39], using the results for Hamming codes, Sloane derived new bounds for the minimum distance of self-dual codes in the Hamming metric. Can we do the same for self-dual NRT codes?

b) Can we find a polynomial basis that matches the Molien's series for any s?

c) Using the results obtained can we answer questions about the existence of self-dual NRT codes with certain given parameters?

Chapter 4

Constructions of Self-Dual Codes in the NRT Metric

In this chapter, we define the concept of ordered flip of a matrix A in $M_{k,ns}(\mathbb{F}_q)$ and present some constructions of self-dual codes in $M_{n,s}(\mathbb{F}_q)$, extending previous results for $M_{1,s}(\mathbb{F}_q)$ in [42]. Finally, we present an application of the ordered flip to the classification of self-dual NRT codes of dimension two.

4.1 Self-dual codes in NRT spaces from self-dual codes in Hamming spaces

Definition 4.1. *Given a vector* $v = (v_1, \ldots, v_{s-1}, v_s)$ *in* $\mathbb{F}_q^s$*, the flip of* v*, denoted by* $\mathrm{flip}(v)$*, is the vector* $\mathrm{flip}(v) = (v_s, v_{s-1}, \ldots, v_1) \in \mathbb{F}_q^s$.

Remarks 4.2. *Let* $\mathrm{flip} : \mathbb{F}_q^s \longrightarrow \mathbb{F}_q^s$ *be the function taking* $v \in \mathbb{F}_q^s$ *to its flip. The following properties hold:*

a) For any $s \in \mathbb{N}$, $\mathrm{flip} : \mathbb{F}_q^s \longrightarrow \mathbb{F}_q^s$ *is a linear operator;*

b) If $s = 1$*, then* $\mathrm{flip} \equiv I$*, where* I *denotes the identity operator.*

c) Let $\langle , \rangle_E$ *be the Euclidean inner product on* $\mathbb{F}_q^s$*. For any* $u, v \in \mathbb{F}_q^s$, $\langle \mathrm{flip}(u), \mathrm{flip}(v) \rangle_E = \langle u, v \rangle_E$.

In next theorem, we present a construction of a self-orthogonal NRT code in $M_{1,2s}(\mathbb{F}_q)$ derived from a code C in the Hamming space $\mathbb{F}_q^s$ with the standard inner product $\langle , \rangle_E$.

Theorem 4.3. *Let C be an $[s,k]$ linear code in the Hamming space $\mathbb{F}_q^s$, and let $C^\perp$ be its dual code with respect to the standard inner product. The code C_o in $M_{1,2s}(\mathbb{F}_q)$ given by*

$$C_o := \{(v, \mathrm{flip}(u)) \ : \ v \in C, \text{ and } u \in C^\perp\}$$

is an $[2s, k+k^\perp]$ self-orthogonal NRT code with $k^\perp = \dim(C^\perp)$.

Proof. Indeed, let $(v_1, \mathrm{flip}(u_1)), (v_2, \mathrm{flip}(u_2)) \in C_o$ where $v_1, v_2 \in C$ and $u_1, u_2 \in C^\perp$. Then

$$\begin{aligned} \langle (v_1, \mathrm{flip}(u_1)), (v_2, \mathrm{flip}(u_2)) \rangle_N &= \langle v_1, u_2 \rangle_E + \langle \mathrm{flip}(u_1), \mathrm{flip}(v_2) \rangle_E \\ &= \langle v_1, u_2 \rangle_E + \langle u_1, v_2 \rangle_E \\ &= 0, \end{aligned}$$

which means that $C_o \subseteq (C_o)^\perp$. It is easy to check that $\dim C_o = k + k^\perp$. □

Example 4.4. *Choose the $[2,1]$ linear code $C := \{(0,0),(1,0)\}$ in the Hamming space $\mathbb{F}_2^2$. Its dual code is given by $C^\perp = \{(0,0),(0,1)\}$. The NRT code C_o in $M_{1,4}(\mathbb{F}_2)$ of Theorem 4.3 is the following $[4,2]$ self-orthogonal NRT code*

$$C_o := \{(0,0,0,0),(0,0,1,0),(1,0,0,0),(1,0,1,0)\}.$$

It is worth to mentioning that if we consider C_o as an $[4,2]$ linear code over the Hamming space, $\mathbb{F}_2^4$, C_o is not a self-orthogonal code since $(1,0,0,0) \in C_o$ but $(1,0,0,0) \notin C_o$. Note also that C_o is not a self-dual NRT code since $(0,1,0,1) \notin C_o$ but $(0,1,0,1) \in C_o^\perp$.

Theorem 4.5. *Let C be an $[s,k]$ self-orthogonal code in the Hamming space $\mathbb{F}_q^s$. The code*

$$C_{ort} := \{(v, \mathrm{flip}(v)) \in M_{1,2s}(\mathbb{F}_q) \ : \ v \in C\}$$

is an $[2s,k]$ self-orthogonal NRT code.

Proof. Let $\mathbf{v} = (v, \mathrm{flip}(v)), \mathbf{u} = (u, \mathrm{flip}(u)) \in C_{ort}$ with $v, u \in C$. Then

$$\langle \mathbf{v}, \mathbf{u} \rangle_N = \langle (v, \mathrm{flip}(v)), (u, \mathrm{flip}(u)) \rangle_N = 2\langle v, u \rangle_H = 0$$

since $v, u \in C$, and C is a self-orthogonal code over the Hamming space. Clearly, $\dim C_{ort} = k$, so C_{ort} is an $[2s,k]$ self-orthogonal NRT code. □

Example 4.6. *Let $C = \{(0,0,0),(1,1,0)\}$ be the $[3,1]$ self-orthogonal code given by in the Hamming space $\mathbb{F}_2^3$. The code C_{ort} of Theorem 4.5 is the following $[6,1]$ self-orthogonal NRT code in $M_{1,6}(\mathbb{F}_2)$*

$$C_{ort} = \{(0,0,0,0,0,0),(1,1,0,0,1,1)\}.$$

Theorem 4.7. *Let C be an $[s,k]$ self-dual code in the Hamming space $\mathbb{F}_q^s$. The code*

$$C_N := \{(v, \mathrm{flip}(v')) \ : \ v, v' \in C\}$$

is an $[2s, 2k]$ self-dual NRT code in $M_{1,2s}(\mathbb{F}_q)$.

Proof. Let $\mathbf{v} = (v_1, \mathrm{flip}(v_1')), \mathbf{u} = (u_1, \mathrm{flip}(u_1')) \in C_N$ with $v_1, v_1', u_1, u_1' \in C$. Then,

$$\langle \mathbf{v}, \mathbf{u} \rangle_N = \langle (v_1, \mathrm{flip}(v_1')), (u_1, \mathrm{flip}(u_1')) \rangle_N = \langle v_1, u_1 \rangle_E + \langle v_1', u_1' \rangle_E = 0,$$

since C is a self-dual code in the Hamming space $\mathbb{F}_q^s$. So C_N is a self-orthogonal NRT code. Note that C_N will be a self-dual NRT code if $\dim(C_N) = 2k$. Choose a basis $\beta := \{v_1, \ldots v_k\}$ of C. Since $\mathrm{flip} : \mathbb{F}_q^s \longrightarrow \mathbb{F}_q^s$ is a linear isomorphism, the set $flip(\beta) := \{\mathrm{flip}(v_1), \ldots, \mathrm{flip}(v_k)\}$ is a basis of $flip(C)$. Define

$$\beta_N := \{(v_1, 0), \ldots, (v_k, 0), (0, \mathrm{flip}(v_1)), \ldots, (0, \mathrm{flip}(v_k))\}$$

where 0 denotes the vector $(0, \ldots, 0) \in \mathbb{F}_q^s$. The set β_N is a basis for C_N which has $2k$ elements, and it follows that C_N is an $[2s, 2k]$ self-dual NRT code. □

Example 4.8. *Let $C := \{(0,0), (1,1)\}$ be the $[2,1]$ self-dual code in the Hamming space $\mathbb{F}_2^2$. The code C_N given by Theorem 4.7 is the following $[4,2]$ self-dual NRT code in $M_{1,4}(\mathbb{F}_2)$*

$$C_N = \{(0,0,0,0), (0,0,1,1), (1,1,0,0), (1,1,1,1)\}.$$

Example 4.9. *Consider the $[8,4]$ Extended Hamming code $\hat{\mathcal{H}_3}$. It is well known that $\hat{\mathcal{H}_3}$ is a self-dual code in the Hamming space $\mathbb{F}_2^8$, and thus the construction of Theorem 4.7 applied to $\hat{\mathcal{H}_3}$ gives us an code C_N, which is an $[16,8]$ self-dual NRT code in $M_{1,16}(\mathbb{F}_2)$.*

4.2 Constructions of self-dual NRT codes via generator matrices

In this section, we will present some constructions of self-dual NRT codes starting from other self-dual NRT codes. These constructions are inspired by the those introduced by Marka *et al.* in [42], where some constructions of self-dual NRT codes for $n = 1$ are given. In order to describe NRT codes by generator matrices, we will order lexicographically the entries of an element $\mathbf{v} \in M_{n,s}(\mathbb{F}_q)$, identifying the matrix $\mathbf{v} = [v_1; v_2; \cdots ; v_n] \in M_{n,s}(\mathbb{F}_q)$ with a row vector $(v_1 \mid v_2 \mid \ldots \mid v_n) \in M_{1,ns}(\mathbb{F}_q)$.

Definition 4.10. *A generator matrix for an* $[ns, k]$ *linear code* C *in the* NRT *space* $M_{n,s}(\mathbb{F}_q)$ *is a matrix* $G \in M_{k,ns}(\mathbb{F}_q)$ *whose rows form a basis of* C*. A generator matrix* $G \in M_{k,ns}(\mathbb{F}_q)$ *of an* $[ns, k]$ *linear NRT code* C *in* $M_{n,s}(\mathbb{F}_q)$ *can be written as*

$$G = \left[\; G_1 \; \middle| \; G_2 \; \middle| \cdots \middle| \; G_{n-1} \; \middle| \; G_n \; \right],$$

where each G_i *is an* $k \times s$ *matrix for* $i = 1, \ldots, n$*.*

The main point in the constructions given in [42] is the definition of a flip of a matrix $A \in M_{n,s}(\mathbb{F}_q)$, which is described below.

Definition 4.11. *Let* $A = (a_{i,j}) \in M_{n,s}(\mathbb{F}_q)$*. Then, the flip of* A*, denoted by* $\mathrm{Flip}(A)$*, is defined by*

$$\mathrm{Flip}(A) = (a_{iu}),$$

where $u = s - j + 1$ *for* $1 \leqslant i \leqslant n$ *and* $1 \leqslant j \leqslant s$*. We denote the transpose of* $\mathrm{Flip}(A)$ *as* A^o*.*

Example 4.12. *Let* $A \in M_{n,s}(\mathbb{F}_q)$ *given by*

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,s-1} & a_{1,s} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,s-1} & a_{2,s} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1,1} & a_{n-1,2} & \cdots & a_{n-1,s-1} & a_{n-1,s} \\ a_{n,1} & a_{n,2} & \cdots & a_{n,s-1} & a_{n,s} \end{bmatrix}.$$

Then, $\mathrm{Flip}(A)$ *and* A^o *are given respectively by*

$$Flip(A) = \begin{bmatrix} a_{1,s} & a_{1,s-1} & \cdots & a_{1,2} & a_{1,1} \\ a_{2,s} & a_{2,s-1} & \cdots & a_{2,2} & a_{2,1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1,s} & a_{n-1,s-1} & \cdots & a_{n-1,2} & a_{n-1,1} \\ a_{n,s} & a_{n,s-1} & \cdots & a_{n,2} & a_{n,1} \end{bmatrix}$$

$$A^o = \begin{bmatrix} a_{1,s} & a_{2,s} & \cdots & a_{n-1,s} & a_{n,s} \\ a_{1,s-1} & a_{2,s-1} & \cdots & a_{n-1,s-1} & a_{n,s-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{1,2} & a_{2,2} & \cdots & a_{n-1,2} & a_{n,2} \\ a_{1,1} & a_{2,1} & \cdots & a_{n-1,1} & a_{n,1} \end{bmatrix}.$$

Note that by the definition of the NRT metric, in the case $n = 1$, a code C in $M_{1,s}(\mathbb{F}_q)$ is an $[s, k]$ self-orthogonal NRT code if and only if $GG^o = 0$, where G is a generator matrix of the code C.

In order to define self-dual NRT codes by generator matrices, we introduce a new concept; the ordered flip of a matrix $A \in M_{k,ns}(\mathbb{F}_q)$.

Definition 4.13. *Let* $A = \left[\begin{array}{c|c|c|c|c} A_1 & A_2 & \cdots & A_{n-1} & A_n \end{array}\right]$ *be an* $k \times ns$ *matrix. The ordered flip of* A *is the matrix* $\mathrm{OFlip}(A) := \left[\begin{array}{c|c|c|c|c} \mathrm{Flip}(A_1) & \mathrm{Flip}(A_2) & \cdots & \mathrm{Flip}(A_{n-1}) & \mathrm{Flip}(A_n) \end{array}\right]$. *We denote the transpose of* $\mathrm{OFlip}(A)$ *by* A^{od}. *Note that*

$$A^{od} = [\mathrm{OFlip}(A)]^T = \begin{bmatrix} A_1^o \\ A_2^o \\ \vdots \\ A_{n-1}^o \\ A_n^o \end{bmatrix}.$$

Example 4.14. *Let* C *be the* $[8, 4]$ *linear NRT code in* $M_{2,4}(\mathbb{F}_2)$, *whose generator matrix is given by*

$$G = \left[\begin{array}{c|c} G_1 & G_2 \end{array}\right] = \left[\begin{array}{cccc|cccc} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}\right].$$

Then

$$OFlip(G) = \left[\begin{array}{cccc|cccc} 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right],$$

and

$$G^{\circ} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

The definition of ordered flip and NRT metric implies the following remark.

Remark 4.15. *Let C be an $[ns, k]$ linear NRT code in $M_{n,s}(\mathbb{F}_q)$, and let G is a generator matrix of C. The equivalence hold: C is a self orthogonal NRT code if and only if $GG^{od} = 0$.*

Theorem 4.16. *Let C_i be an $[ns, k_i]$ self-orthogonal NRT code in $M_{n,s}(\mathbb{F}_q)$, $i = 1, 2$. Let also $G^{(i)} = [G_1^{(i)}|\ldots|G_n^{(i)}]$ be a generator matrix of C_i. The matrix $G \in M_{k_1+k_2,2ns}(\mathbb{F}_q)$ defined by*

$$G = \left[\begin{array}{c|c|c|c|c} G_1^{(1)} & 0 & \cdots & G_n^{(1)} & 0 \\ 0 & G_1^{(2)} & \cdots & 0 & G_n^{(2)} \end{array}\right]$$

is a generator matrix of an $[2ns, k_1 + k_2]$ self-orthogonal NRT code C^N.

Proof. We need to prove that $GG^{od} = 0$. Indeed, by definition of ordered flip we have

$$OFlip(G) = \left[\begin{array}{c|c|c|c|c} Flip(G_1^{(1)}) & 0 & \cdots & Flip(G_n^{(1)}) & 0 \\ 0 & Flip(G_1^{(2)}) & \cdots & 0 & Flip(G_n^{(2)}) \end{array}\right],$$

and

$$G^{od} = \left[\begin{array}{cc} (G_1^{(1)})^o & 0 \\ 0 & (G_1^{(2)})^o \\ (G_2^{(1)})^o & 0 \\ \vdots & \vdots \\ (G_n^{(1)})^o & 0 \\ 0 & (G_n^{(2)})^o \end{array}\right],$$

therefore,

$$\begin{aligned} GG^{od} &= G_1^{(1)}(G_1^{(1)})^o + \ldots + G_n^{(1)}(G_n^{(1)})^o + [G_1^{(2)}(G_1^{(2)})^o + \ldots + G_n^{(2)}(G_n^{(2)})^o] \\ &= G_1 G_1^{od} + G_2 G_2^{od} = 0, \end{aligned}$$

since C_1 and C_2 are self-dual NRT codes. It follows from Remark 4.15 that C^N is a self-orthogonal NRT code. It is easy to see that the rows of G form a basis of C^N, so we concluded that $\dim C^N = k_1 + k_2$, and C^N is an $[2ns, k_1 + k_2]$ self-orthogonal NRT code. □

Corollary 4.17. *Let C_i be an $\left[ns, \frac{ns}{2}\right]$ self-dual NRT code, $i = 1, 2$. Let also $G^{(i)} = [G_1^{(i)}|\ldots|G_n^{(i)}]$ be a generator matrix of C_i. The matrix $G \in M_{ns,2ns}(\mathbb{F}_q)$ defined by*

$$G = \left[\begin{array}{c|c|c|c|c} G_1^{(1)} & 0 & \cdots & G_n^{(1)} & 0 \\ 0 & G_1^{(2)} & \cdots & 0 & G_n^{(2)} \end{array}\right]$$

is a generator matrix of an $[2ns, ns]$ self-dual NRT code C^N.

Example 4.18. *In Example* 4.8*, given the self-dual code* $C = \{(0,0),(1,1)\}$ *in the Hamming space* $\mathbb{F}_2^2$*, we obtain the self-dual NRT code* C_N *in* $M_{1,4}(\mathbb{F}_2)$ *which a generator matrix given by*

$$G^{(1)} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Applying the construction of Theorem 4.16, we obtain the $[8,4]$ *self-dual NRT code* C^{N_1} *in* $M_{2,4}(\mathbb{F}_2)$ *defined by the generator matrix*

$$G := \left[\begin{array}{cccc|cccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right].$$

Example 4.19. *Applying the construction to the* $[8,4]$ *self-dual NRT code* C^{N_1} *in* $M_{2,4}(\mathbb{F}_2)$ *of Example* 4.18*, we obtain the* $[16,8]$ *self-dual NRT code* C^{N_2} *given by the generator matrix*

$$G := \left[\begin{array}{cccc|cccc|cccc|cccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right].$$

Theorem 4.20. *Let* C_i *be an* $[n_i s_i, k_i]$ *self-orthogonal NRT code in* $M_{n_i s_i}(\mathbb{F}_q)$*,* $1 \leqslant i \leqslant t$*, such that* $k = k_1 + \ldots + k_t \leqslant \bar{n}\bar{s}$*, where* $\bar{n} := \max\{n_i\}$ *and* $\bar{s} := \max\{s_i\}$*. Let also* $G^{(i)} = [G_1^{(i)} | \ldots | G_{n_i}^{(i)}]$ *be a generator matrix of* C_i*. The matrix* $G \in M_{k,\bar{s}(n_1+\ldots+n_t)}(\mathbb{F}_q)$ *defined by*

$$G = \left[\begin{array}{c|c|c|c|c|c|c|c|c|c|c|c} \widetilde{G}_1^{(1)} & \widetilde{G}_2^{(1)} & \ldots & \widetilde{G}_{n_1}^{(1)} & 0 & 0 & \ldots & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & \widetilde{G}_1^{(2)} & \widetilde{G}_2^{(2)} & \ldots & \widetilde{G}_{n_2}^{(2)} & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & \ldots & \widetilde{G}_1^{(t)} & \widetilde{G}_2^{(t)} & \ldots & \widetilde{G}_{n_t}^{(t)} \end{array}\right]$$

is a generator matrix of an $[\bar{s}(n_1+\ldots+n_t), k]$ *self-orthogonal NRT code* $C_\star$*, where the matrices* $\widetilde{G}_{j_i}^{(i)} \in M_{k_i \bar{s}}(\mathbb{F}_q)$*,* $1 \leqslant i \leqslant t$ *and* $1 \leqslant j_i \leqslant n_i$ *are given by* $\widetilde{G}_{j_i}^{(i)} = [G_{j_i}^{(i)}]$ *if* $s_i = \bar{s}$ *or* $\widetilde{G}_{j_i}^{(i)} = [G_{j_i}^{(i)} \mid 0]$ *if* $s_i < \bar{s}$*, where* $0 \in M_{k_i \bar{s} - s_i}(\mathbb{F}_q)$ *is the null matrix.*

Corollary 4.21. *Let C_i be an $[ns, k_i]$ self-orthogonal NRT code for $1 \leqslant i \leqslant t$ such that $k = k_1 + \ldots + k_t \leqslant ns$ and $G^{(i)} = [G_1^{(i)}|\ldots|G_n^{(i)}]$ be a generator matrix of C_i. Then the matrix $G \in M_{k,tns}(\mathbb{F}_q)$ defined by*

$$G = \left[\begin{array}{c|c|c|c|c|c|c|c|c|c|c|c|c} G_1^{(1)} & G_2^{(1)} & \ldots & G_n^{(1)} & 0 & 0 & \ldots & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & G_1^{(2)} & G_2^{(2)} & \ldots & G_n^{(2)} & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & \ldots & G_1^{(t)} & G_2^{(t)} & \ldots & G_n^{(t)} \end{array}\right]$$

is a generator matrix of a $[tns, k]$ self-orthogonal NRT code $C_\star$.

In particular, we can apply the preceding corollary to construct a self-dual NRT code $C_\star$ equivalent to the code C^N from the construction in Theorem 4.16, more precisely

Corollary 4.22. *Let C_1 and C_2 be two $\left[ns, \frac{ns}{2}\right]$ self-dual NRT codes in $M_{n,s}(\mathbb{F}_q)$. Let also $G^{(1)} = [G_1^{(1)}|\ldots|G_n^{(1)}]$ be a generator matrix of C_1, and $G^{(2)} = [G_1^{(2)}|\ldots|G_n^{(2)}]$ be a generator matrix of C_2. The matrix $G \in M_{ns,2ns}(\mathbb{F}_q)$ defined by*

$$G = \left[\begin{array}{c|c|c|c|c|c} G_1^{(1)} & \ldots & G_n^{(1)} & 0 & \ldots & 0 \\ 0 & \ldots & 0 & G_1^{(2)} & \ldots & G_n^{(2)} \end{array}\right]$$

is a generator matrix for an $[2ns, ns]$ self-dual NRT code $C_\star$.

Example 4.23. *Let C^{N_1} be the $[8, 4]$ Self-dual NRT code of Example 4.18. Then, by the construction of Theorem 4.22, the following matrix*

$$G := \left[\begin{array}{cccc|cccc|cccc|cccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right],$$

is a generator matrix for an $[16, 8]$ self-dual NRT code $C_\star$, which is, equivalent to the code C^{N_2} of Example 4.19.

4.3 An application of the ordered flip concept

In [65], Alves gave an analogue for NRT codes of the well-known standard form of generator matrices for codes in Hamming space. In this section, we remember this analogue generator matrix, and we will use this to classify self- dual NRT codes dimension two.

Definition 4.24. *A matrix $A \in M_{n,k}(\mathbb{F}_q)$ is said $T_s(\mathbb{F}_q)$-reduced if, modulo permutations of rows,*

$$A = \left[\begin{array}{c|c|c|c} c_1 & c_2 & \ldots & c_s \end{array} \right]$$

where each column c_j is either the zero vector or a vector of the form

$$c_j = (c_{(1,j)}, \ldots, c_{(\omega_{j-1},j)}, 1, 0, \ldots, 0),$$

with $\omega_j < \omega_{j'}$ whenever $j < j'$, and c_j and $c_{j'}$ are nonzero.

Example 4.25. *The following matrix is $T_6(\mathbb{F}_2)$-reduced.*

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

In fact, permuting the second and the third rows we get the matrix

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

whose columns satisfy the definition of $T_6(\mathbb{F}_2)$-reduced.

Definition 4.26. *Let C be an $[ns, k]$ NRT code in $M_{n,s}(\mathbb{F}_q)$. A generator matrix G for C is said to be in the NRT-triangular form if*

$$G = \left[\begin{array}{c|c|c|c} G_1 & G_2 & \ldots & G_n \end{array} \right]$$

where each G_i is a $k \times s$ matrix, and:

1. *G is in block echelon form, i.e., if the last t rows of G_i are zero, then the last t rows of $G_1, \ldots G_{i-1}$ are also zero;*

2. *The rows no zeros of G_1 are distinct canonical vectors, arranged in order of increasing NRT weight;*

3. *For each $i = 2, \ldots, n$, the following proprieties hold:*

   (i) G_i is $T_s(\mathbb{F}_q)$-reduced or,

   (ii) $G_i = \begin{bmatrix} A^i & B^i \\ J^i & 0 \end{bmatrix}$, where A^i and B^i are $T_m(\mathbb{F}_q)$-reduced, J^i is a matrix whose non-zero rows are distinct canonical vectors (also arranged in order of increasing NRT weight) and whose the last column is nonzero, and all entries of A^i above each nonzero entry of J^i are zero.

Theorem 4.27. *([65].) Let C be an $[ns, k]$ linear NRT code in $M_{n,s}(\mathbb{F}_q)$. Then C is equivalent to another linear NRT code C' in $M_{n.s}(\mathbb{F}_q)$, which has a generator matrix*

$$G = \left[\; G_1 \; \middle| \; G_2 \; \middle| \; \ldots \; \middle| \; G_n \; \right]$$

in the NRT-triangular form.

Theorem 4.27 gives us a simple NRT-triangular form for NRT codes of dimension two.

Corollary 4.28. *([65].) Let C be an $[ns, 2]$ linear NRT code in $M_{n,s}(\mathbb{F}_q)$. Then, C has a generator matrix of the form*

$$G = [G_1|G_2|\ldots|G_n],$$

where each G_i is an $2 \times s$ matrix of one of the following types: Null matrix, $\begin{bmatrix} e_i \\ 0 \end{bmatrix}$, $\begin{bmatrix} 0 \\ e_i \end{bmatrix}$, $\begin{bmatrix} e_i \\ e_j \end{bmatrix}$, $\begin{bmatrix} e_i + \lambda e_j \\ e_j \end{bmatrix}$, where $e_i \in \mathbb{F}_q^s$ denotes the i-th canonical vector, $1 \leqslant i \leqslant j$, and $\lambda \neq 0$.

Proof. See [65]. □

Theorem 4.29. *Let C be an $[ns, k]$ self-dual NRT code of dimension two. Then one of the followings holds.*

i) If $n = 1$, $s = 4$, any $[4, 2]$ self-dual NRT code C in $M_{1,4}(\mathbb{F}_q)$ has as a generator matrix one of the matrices

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$\left[\begin{array}{cccc} 1 & 0 & \lambda & 0 \\ 0 & 0 & 1 & 0 \end{array}\right], \left[\begin{array}{cccc} 1 & \lambda & 0 & 0 \\ 0 & 1 & 0 & 0 \end{array}\right], \left[\begin{array}{cccc} 0 & 1 & 0 & \lambda \\ 0 & 0 & 0 & 1 \end{array}\right], \left[\begin{array}{cccc} 0 & 0 & 1 & \lambda \\ 0 & 0 & 0 & 1 \end{array}\right].$$

ii) If $n = 2$, $s = 2$, any $[4, 2]$ self-dual NRT code C in $M_{2,2}(\mathbb{F}_q)$ has as a generator matrix one of the matrices

$$\left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right], \left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right], \left[\begin{array}{cc|cc} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right], \left[\begin{array}{cc|cc} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right],$$
$$\left[\begin{array}{cc|cc} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right], \left[\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{array}\right], \left[\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right], \left[\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{array}\right],$$
$$\left[\begin{array}{cc|cc} 0 & 1 & 1+\lambda & 0 \\ 0 & 0 & 1 & 0 \end{array}\right], \left[\begin{array}{cc|cc} 0 & 1 & 0 & 1+\lambda \\ 0 & 0 & 0 & 1 \end{array}\right], \left[\begin{array}{cc|cc} 1 & 0 & 1+\lambda & 0 \\ 0 & 0 & 1 & 0 \end{array}\right], \left[\begin{array}{cc|cc} 1 & 0 & 0 & 1+\lambda \\ 0 & 0 & 0 & 1 \end{array}\right].$$

iii) If $n = 4$, $s = 1$, in this case the NRT metric space and the Hamming metric are equivalent. The classification of self-dual codes in this case is given by Pless in [54].

Proof. The definition of ordered flip and Corollary 4.28 can be used to find all possible generator matrices of a self-dual NRT code of dimension two. In fact, if C is an $[ns, k]$ self-dual NRT code in $M_{n,s}(\mathbb{F}_q)$ of dimension two, then $2 = dim(C) = \frac{ns}{2}$ and so $ns = 4$, which implies that one of the following cases holds.

i) $n = 1$ and $s = 4$;

ii) $n = 2$ and $s = 2$;

iii) $n = 4$ and $s = 1$.

The result follows by the definition of ordered flip of a matrix and Remark 4.15. □

4.4 Open problems

a) Can we get new constructs of self-dual NRT codes from the definition of ordered flip of a matrix?

b) What happens if we apply the constructs already obtained to good codes in the Hamming metric? (Will we obtain good NRT codes?)

c) Using the same strategy of the previous section can we classify self-dual NRT codes with dimension greater than two?

Chapter 5

Reed-Solomon Codes and Interleaved Reed-Solomon Codes

In this chapter, we will discuss some of the properties of an well-known family of codes, the Reed-Solomon codes [57]. We also review the concept of Interleaved Reed-Solomon codes and a collaborative decoder of interleaved Reed-Solomon codes [60]. The main objective of this chapter is to point out that will be used to perform fractional decoding beyond the α-decoding radius [73].

5.1 Reed-Solomon codes

In 1960, Irving S. Reed and Gustave Solomon published the remarkable paper *Polynomial Codes over Certain Finite Fields* [57]. In this paper, they introduced a new error-correcting code based on sampling points on a polynomial, as described in the following:

Definition 5.1. *Let $\mathcal{L} = \{\gamma_1, \ldots, \gamma_n\}$ be a set of distinct nonzero elements of a finite field $\mathbb{F}_q$, and let $\mathbb{F}_q[x]_k$ denotes the set of all univariate polynomials of degree less than k. For a given polynomial $f(x) \in \mathbb{F}_q[x]_k$, we write*

$$f(\mathcal{L}) = (f(\gamma_1), \ldots, f(\gamma_n)) .$$

Let $n < q$, a Reed-Solomon code $RS(q, n, k)$ over a field $\mathbb{F}_q$ is given by

$$RS(q, n, k) = \{c = f(\mathcal{L}) : \ f(x) \in \mathbb{F}_q[x]_k\}. \tag{5.1}$$

The set $\mathcal{L}$ is called the evaluation set of $RS(q, n, k)$.

Reed-Solomon codes are known to be maximum-distance separable (MDS), i.e., their minimum Hamming distance is $d = n - k + 1$. For fixed n, and $\mathcal{L} = \{\gamma_1, \ldots, \gamma_n\}$, the various $RS(q, n)$ codes enjoy the nice embedding property $RS(q, n, k-1) \subseteq RS(q, n, k)$.

Let us recall a natural interpretation of the $RS(q, n, k)$ code can be made by means of its encoding map. To encode a message $m = (m_0, \ldots, m_{k-1}) \in \mathbb{F}_q^k$, we interpret the message as the polynomial

$$p(x) = m_0 + m_1 x + \ldots + m_{k-1} x^{k-1} \in \mathbb{F}_q^n[x],$$

and then the evaluation of the polynomial p at the points $\gamma_1, \gamma_2, \ldots, \gamma_n$ generates the codeword $(p(\gamma_1), p(\gamma_2), \ldots, p(\gamma_n))$ corresponding to m.

Let $C = RS(q, n, k)$ be a Reed-Solomon code, and $c \in C$ with $c = f(\mathcal{L})$ for some $f \in \mathbb{F}_q[x]_k$. Assume that c was transmitted over a noisy channel, and that $y = c + e$ was the received word with error $e = (e_1, \ldots, e_n)$.

To locate the erroneous positions in y, we can use a technique introduced by Peterson [53] and define a polynomial, called *error-locator-polynomial* by

$$\Lambda(x) = \prod_{i \in \mathcal{J}} (x - \gamma_i), \tag{5.2}$$

where $\mathcal{J} = \{i \,:\, e_i \neq 0\}$ with $|\mathcal{J}| = t$, the set of error locations of y.

Let $r(x) \in \mathbb{F}_q[x]$ be the unique interpolation polynomial of degree $\deg r(x) < n$ such that $r(\gamma_i) = y_i$ for all $i = 1, \ldots, n$. The polynomial $r(x)$ can be calculated by using the Lagrange interpolation formula

$$r(x) = \sum_{i=1}^{n} y_i L_i(x) \text{ with } L_i(x) = \prod_{m \neq i} \frac{x - \gamma_m}{\gamma_i - \gamma_m}.$$

Let H be a parity-check matrix of C and denote the syndrome vector of length $n - k$ by

$$s = yH^T = eH^T = (S_1, \ldots, S_{n-k}),$$

Let $S(x)$ be the corresponding *syndrome polynomial* $S(x) = \sum_{i=1}^{n-k} S_i x^{i-1}$. By definition we have that $S(x) = r(x) - f(x)$, and

$$\Lambda(\gamma_j)(r(\gamma_j) - f(\gamma_j)) = \Lambda(\gamma_j)(e_j) \tag{5.3}$$

$$= \begin{cases} 0.e_j, & \text{if } j \in \mathcal{J} \\ \Lambda(\gamma_j).0, & \text{if } j \notin \mathcal{J} \end{cases} \tag{5.4}$$

Thus, $(x-\gamma_j)|\Lambda(x)S(X)$ and so $G(x) = \prod_{j=1}^{n}(x-\gamma_j)$ divides $\Lambda(x)S(X)$. We can write the following Key-Equation

$$\Lambda(x)S(x) \equiv 0 \mod G(x), \tag{5.5}$$

which give us a polynomial relation between the error-locator-polynomial and the syndrome polynomial. Note that $\Lambda(x)$ is not known at the receiver, but $r(x)$ and $G(x)$ are.

Equation (5.5) gives rise to a linear system of n equations. From these equations, $n-k-t$ equations depends only on the $n-k$ coefficients from $S(x)$, which are the syndromes $S_1, S_2, \ldots, S_{n-k}$, and the unknown coefficients of the error-locator polynomial $\Lambda(x)$. Hence, we extract a linear system of $n-k-t$ equations and t unknown variables $\lambda_1, \lambda_2, \ldots, \lambda_t$. This system of equations can be represented by the matrix equation

$$\begin{bmatrix} S_1 & S_2 & \cdots & S_t \\ S_2 & S_3 & \cdots & S_{t+1} \\ \vdots & \vdots & \ddots & \vdots \\ S_{n-k-t} & S_{n-k-t+1} & \cdots & S_{n-k-1} \end{bmatrix} \begin{bmatrix} \Lambda_t \\ \Lambda_{t-1} \\ \vdots \\ \Lambda_1 \end{bmatrix} = \begin{bmatrix} -S_{t+1} \\ -S_{t+2} \\ \vdots \\ -S_{n-k} \end{bmatrix}. \tag{5.6}$$

If (5.6) has a unique solution, it can be used to calculate the coefficients of a unique error locator polynomial $\Lambda(x)$, and hence the erroneous positions of y are known, the most difficult part of decoding is accomplished. If the error locations are known, the error values can be uniquely determined. Error evaluation can be performed using standard techniques like *Recursive Extension* [4] or the *Forney algarithm* [21].

A unique solution of (5.6) can only exist if the number of unknowns is not larger than the number of equations, i.e., as long as $t \leqslant n-k-t$ and we are never able to correct more than $\left\lfloor \frac{n-k}{2} \right\rfloor$ errors, that is,

$$t \leqslant \left\lfloor \frac{n-k}{2} \right\rfloor = \tau.$$

The number τ is called the *maximum correcting radius* of the $RS(q,n,k)$ code.

5.2 Interleaved Reed-Solomon codes

Interleaved codes are not a family of codes, but rather an encoding mode.

Definition 5.2. *Let $C_0, \ldots, C_{n-1}$ code in $\mathbb{F}_q^n$, an interleaved code of order m induced by $C_0, \ldots, C_{m-1}$ is the following matrix form.*

$$IC = \left\{ \mathbf{c} = \begin{bmatrix} c_{0,1} & c_{0,2} & \cdots & c_{0,n-1} & c_{0,n} \\ c_{1,1} & c_{1,2} & \cdots & c_{1,n-1} & c_{1,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_{m-1,1} & c_{m-1,2} & \cdots & c_{m-1,n-1} & c_{m-1,n} \end{bmatrix} : (c_{i,1}, \ldots, c_{i,n}) \in C_i, 1 \leqslant i \leqslant n-1 \right\}. \tag{5.7}$$

Sometimes we write the codewords $\mathbf{c}$ of an interleaved code IC as

$$\mathbf{c} = \begin{bmatrix} c^{(0)} \\ c^{(1)} \\ \vdots \\ c^{(m-1)} \end{bmatrix},$$

where $c^{(i)} \in C_i$. In special, when the underlying codes are Reed-Solomon codes, which are arranged in a matrix form, the resulting interleaved code is said to be an Interleaved Reed-Solomon code. Formally,

Definition 5.3. *Let $k_0, k_1, \ldots, k_{m-1}$ be positive integers, where $k_j < n$ for any $1 \leqslant j \leqslant n-1$. An interleaved RS code $IRS(q, n, \mathcal{K}, m)$ of order m is given by*

$$IRS(q, n, \mathcal{K}, m) = \left\{ \mathbf{c} = \begin{bmatrix} f_0(\mathcal{L}) \\ f_1(\mathcal{L}) \\ \vdots \\ f_{m-1}(\mathcal{L}) \end{bmatrix} : f_j(x) \in \mathbb{F}_q[x]_{k_j} \right\}, \tag{5.8}$$

The codewords $f_j(\mathcal{L}) \in RS(q, n, k_i)$ are called elementary codewords of the $IRS(q, n, \mathcal{K}, m)$-code.

If the dimensions k_j in Definition 5.3 are equal for all $j = 0, \ldots, m-1$, the IRS code is called *Homogeneous interleaved RS Code*. Otherwise, the IRS code is called *Heterogeneous interleaved RS Code*.

The common way to decode an interleaved code is to decode each of the row codewords $(c_{i,1}, \ldots, c_{i,n}) \in C_i$ separately. Using this decoding process, the maximum error correcting radius of the $IRS(q, n, \mathcal{K}, m)$ code is $\left\lfloor \frac{n-\bar{k}}{2} \right\rfloor$, where $\bar{k} = \max\{k_0, k_1, \ldots, k_{m-1}\}$.

5.2.1 Collaborative decoding of interleaved Reed-Solomon codes

Schmidt *et al.* [60], introduced the concept of collaborative decoding for interleaved RS codes. This decoder is based on the fact that the errors occur in the same positions of each elementary codeword of the interleaved RS code. In the following we present the main idea and results from [60].

Let $\mathbf{c} \in IRS(q, n, \mathcal{K}, m)$ and its received word $\mathbf{y} = \mathbf{c} + \mathbf{e}$, where $\mathbf{e} = (e_1, \ldots, e_n)$ denotes the error vector with t erroneous columns, that is, $w(\mathbf{e}) := |\{i : e_i \neq 0\}| = t$. The m elementary codewords of an IRS code are affected by m elementary error words $e^{(0)}, e^{(1)}, \ldots, e^{(m-1)}$ of weight $w_H(e^{(j)}) = t_j \leqslant t$. Let $\mathcal{E}^{(j)}$ denote the set of error positions for the j-th elementary received word. Since we are considering column errors, the union of the m sets of error positions $\mathcal{E} = \mathcal{E}^{(0)} \cup \mathcal{E}^{(1)} \cup \ldots \cup \mathcal{E}^{(m-1)}$ is a subset of $\{1, \ldots, n\}$ with cardinality $|\mathcal{E}| = t$.

Assume that the codewords of an IRS code are transmitted over a q^m-ary channel. The first step of collaborative decoding is to calculate the m syndrome polynomials $S^{(0)}(x), \ldots, S^{(m-1)}(x)$ of degree smaller than $n - k_j$ and obtain the Key-Equations

$$\Lambda(x)S^{(j)} \equiv 0 \mod G(x),\ j = 0, \ldots, m-1.$$

Shift-Register Synthesis Algorithm 4 of [61] applied to the syndromes $S^{(0)}, \ldots, S^{(m-1)}$ yields a polynomial $\Lambda(x)$ and a shift register length t.

So, as in the classical case, these syndromes are used to form a linear system of equations $S\Lambda = V$,

$$\begin{bmatrix} S^{(0)} \\ S^{(1)} \\ \vdots \\ S^{(m-1)} \end{bmatrix} \begin{bmatrix} \Lambda_1 \\ \Lambda_2 \\ \vdots \\ \Lambda_t \end{bmatrix} = \begin{bmatrix} V^{(0)} \\ V^{(1)} \\ \vdots \\ V^{(m-1)} \end{bmatrix}, \tag{5.9}$$

where each sub-matrix $S^{(j)}$ is a $(n - k_j - t) \times t$ matrix and each $V^{(j)}$ is a column vector of length $n - k_j - t$:

$$S^{(j)} = \begin{bmatrix} S_1^{(j)} & S_2^{(j)} & \cdots & S_t^{(j)} \\ S_2^{(j)} & S_3^{(j)} & \cdots & S_{t+1}^{(j)} \\ \vdots & \vdots & \ddots & \vdots \\ S_{n-k_j-t}^{(j)} & S_{n-k_j-t+1}^{(j)} & \cdots & S_{n-k_j-1}^{(j)} \end{bmatrix}, V^{(j)} = \begin{bmatrix} -S_{t+1}^{(j)} \\ -S_{t+2}^{(j)} \\ \vdots \\ -S_{n-k_j}^{(j)} \end{bmatrix}. \tag{5.10}$$

The system of equations (5.9) has $\sum_{j=0}^{m-1}(n-k_j-t)$ equations and t unknowns. In order to guarantee unambiguous decoding, the number of linearly independent equations has to be greater than or equal to the number of unknowns. Under the assumption that all equations in (5.9) are linearly independent, we obtain the following restriction on t:

$$\sum_{j=0}^{m-1}(n-k_j-t) \geqslant t \tag{5.11}$$

which can be rewritten as

$$t \leqslant \frac{m}{m+1}\left(n-\frac{1}{m}\sum_{i=0}^{m-1}k_j\right). \tag{5.12}$$

The number

$$\tau_{IRS} := \frac{m}{m+1}\left(n-\frac{1}{m}\sum_{i=0}^{m-1}k_j\right)$$

is called the burst-error-correcting capability of the interleaved RS code.

Note that for $m = 1$, that is, considering just one Reed-Solomon code $RS(q, n, k_0)$, τ_{IRS} is reduced to

$$\tau_{IRS} = \frac{1}{2}(n-k_0) = \tau.$$

By the definition of the error locator polynomial, $\Lambda(x)$ is only a valid error locator polynomial if it has exactly t distinct roots. Hence, a Λ-polynomial obtained from [61] is accepted only if it conforms to be the following definition

Definition 5.4. *A polynomial $\Lambda(x)$ over $\mathbb{F}_q$ is called t-valid if it is polynomial of degree t and possesses exactly t distinct roots in $\mathbb{F}_q$.*

The collaborative decoding algorithm given by Schmidt *et al.* in [60] is the following

Algorithm 1: Collaborative IRS Decoder

Input: Received word $\mathbf{y} = \begin{bmatrix} y^{(0)} \\ y^{(1)} \\ \vdots \\ y^{(m-1)} \end{bmatrix}$ Calculate syndromes $S^{(0)}, \ldots, S^{(m-1)}$.

Compute t and $\Lambda(x)$ by Algorithm 4 in [61].

if $t < \tau_{IRS}$ ***and*** $\Lambda(x)$ *is t-valid* **then**

  for each j from 0 to $m-1$ **do**

  evaluate errors, and calculate $e^{(j)}$

  calculate $\hat{c}^{(j)} = y^{(j)} + e^{(j)}$

else

  decoding failure

output: $\mathbf{c} \in IRS(q, n, \mathcal{K}, m)$ or decoding failure

Collaborative decoding of IRS codes provides a method of decoding errors beyond half the minimum distance. However, there is a certain probability that some of the equations (5.9) are linearly dependent. In this case, there is no unique solution of the system of equations and we declare a *decoding failure*.

In order to analyze the probability $P_f(t)$ for the decoding failure, we assume that for each column of the interleaved RS code, each error pattern occurs equiprobable. More precisely, we assume that the burst errors

$$e_j = \begin{bmatrix} e_j^{(0)} \\ \vdots \\ e_j^{(m-1)} \end{bmatrix}$$

are random vectors, uniformly distributed over $\mathbb{F}_q^m \setminus \{0\}$.

To obtain an upper bound on the failure probability of Algorithm 1, we have first to show that whenever Algorithm 1 yields a decoding failure, then there exist multiple solutions for (5.9).

Lemma 5.5. *[60] Consider a codeword* $\mathbf{c}$ *in an* $IRS(q, n, \mathcal{K}, m)$*. Assume that this word is corrupted by an error matrix* $\mathbf{e}$ *with* t *nonzero columns, and that Algorithm 1 yields a decoding failure. The linear system of equations (5.9) with* t *unknowns has multiple solutions.*

Lemma 5.6. *[60] Let* $C_0, \ldots, C_{m-1}$ *be* m *q-ary linear codes of length* n'*, and let the dimension*

of the code C_j be $n' - s^{(j)}$. Further, let

$$\mathbf{w} = \begin{bmatrix} c^{(0)} \\ \vdots \\ c^{(m-1)} \end{bmatrix} = (c_1, \ldots, c_{n'})$$

be a $m \times n'$ matrix such that $c_j \neq 0$ for all $j = 1, \ldots, n'$, i.e., that $\mathbf{w}$ does not have an all-zero column. Furthermore, assume that all columns of $\mathbf{w}$ are uniformly distributed over all non-zero vectors of length m. Let $P_{n'}$ be the probability that

$$c^{(j)} \in C_j, \ \forall j = 0, \ldots, m-1. \tag{5.13}$$

Thus $P_{n'}$ is overbounded by

$$P_{n'} \leqslant \frac{q^{mn'}}{(q^m - 1)^{n'}} q^{-\sum_{j=0}^{m-1} s^{(j)}}. \tag{5.14}$$

Proof. Let $\mathcal{A}$ be the set of all $m \times n'$ matrices whose rows fulfill (5.13). Futher, let $\mathcal{B}_{n'}$ be the set of all $m \times n'$ matrices with elements from $\mathbb{F}_q$, and let the subset $\mathcal{B}^v_{n'} \subseteq \mathcal{B}_{n'}$ be formed by all matrices without any-nonzero column. Then, the probability $P_{n'}$ that the matrix $\mathbf{w}$ without any all-zero column fulfills (5.13) can be calculated by

$$P_{n'} = \frac{|\mathcal{A} \cap \mathcal{B}^v_{n'}|}{|\mathcal{B}^v_{n'}|} \leqslant \frac{|\mathcal{A}|}{|\mathcal{B}^v_{n'}|}.$$

The cardinality $|\mathcal{A}|$ is obtained by

$$|\mathcal{A}| = \prod_{j=0}^{m-1} |C^{(j)}| = q^{mn' - \sum_{j=0}^{m-1} s^{(j)}},$$

and the cardinality $|\mathcal{B}^v_{n'}|$ is calculated by

$$|\mathcal{B}^v_{n'}| = (q^m - 1)^{n'}.$$

Consequently, $P_{n'}$ is overbounded by

$$P_{n'} \leqslant \frac{q^{mn'}}{(q^m - 1)^{n'}} q^{-\sum_{j=0}^{m-1} s^{(j)}}.$$

□

Definition 5.7. *An independent random vector of $\mathbb{F}_q^n$ is a random vector $v = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$ where the value of each coordinate v_i does not depend on the other coordinates v_j of v.*

Theorem 5.8. ***(Failure Probability)****[60] Consider an interleaved RS code, which is decoded by Algorithm 1. Furthermore assume that* $\mathbf{y}$ *is corrupted by* t *column errors, where each column vector is an independent random vector uniformly distributed over* $\mathbb{F}_q^m \setminus \{0\}$*. Then, the probability for a decoding failure is overbounded by*

$$P_f(t) \leqslant \bar{P}_f(t) = \left(\frac{q^m - \frac{1}{q}}{q^m - 1}\right)^t \frac{q^{-(m+1)(\tau_{IRS}-t)}}{q-1}, \tag{5.15}$$

where $\tau_{IRS} = \frac{m}{m+1}\left(n - \frac{1}{m}\sum_{j=0}^{m-1} k_j\right)$.

Proof. According to Lemma 5.5, the failure probability of Algorithm 1 can be overbounded by considering the cases in which the system of equation (5.9) with t unknowns has multiple solutions. We have such a case whenever $\mathrm{rank}(S) < t$, i.e., whenever there exists a column vector $u \neq 0$, such that $Su = 0$. Equivalently, we can say that (5.9) cannot have a unique solution if

$$\exists u \neq 0 \text{ such that } S^{(j)}u = 0 \text{ for all } j = 0, \ldots, m-1. \tag{5.16}$$

Since the syndrome matrices $S^{(0)}, \ldots, S^{(m-1)}$ depends on the error matrix $\mathbf{e}$, we are able to express the failure probability$P_f(t)$ in a general way by

$$P_f(t) = \frac{\text{number of matrices } \mathbf{e}_t \text{ satisfying (5.16)}}{\text{total number of matrices } \mathbf{e}_t},$$

where $\mathbf{e}_t$ denotes an error matrix with exactly t non-zero columns. Now, we consider matrices with non-zero columns at fixed indices $j_1, \ldots, j_t$. More precisely, for a fixed set $\{j_1, \ldots, j_t\}$ of t indices, we consider the ensemble $\mathcal{M}_t(j_1, \ldots, j_t)$ of matrices, in which every column with index $j \in \{j_1, \ldots, j_t\}$ is an independent random vector uniformly distributed over $\mathbb{F}_q^m \setminus \{0\}$, and all other column are zero vectors. Then, the probability that (5.16) is satisfied for matrices $\mathbf{e}_t$ from the ensemble $\mathcal{M}_t(j_1, \ldots, j_t)$ is calculed by

$$P_f(j_1, \ldots, j_t) = \frac{|\mathbf{e} \in \mathcal{M}_t(j_1, \ldots, j_t) \text{ such that } \mathbf{e} \text{ satisfies (5.16)}|}{|\mathcal{M}_t(j_1, \ldots, j_t)|}.$$

We will now derive an upper bound on $P_f(j_1, \ldots, j_t)$, which does not depend on the indices $j_1, \ldots, j_t$, but only on the number of erroneous columns t. Hence, this bound will directly provide us with the upper bound on $P_f(t)$, in which we are actually interested in.

For calculating $P_t(j_1, \ldots, j_t)$, let the number of rows in $S^{(j)}$ be denoted by $s^{(j)}$, i.e., $s^{(j)} = n - k_j - t$. It is known (cf. e.g. [4]) that a syndrome matrix $S^{(j)}$ can be decomposed into

$$S^{(j)} = H^{(j)}F^{(j)}DV,$$

where V is a $t \times t$ Vandermonde matrix, D and $F^{(j)}$ are $t \times t$ diagonal matrices, and the matrix $H^{(j)}$ is a $s^{(j)} \times t$ matrix consisting of $s^{(j)}$ rows of a transposed Vandermonde matrix. Hence, $H^{(j)}$ represents a parity-check matrix of a (shortened) Reed-Solomon code of length t and dimension $t - s^{(j)}$, which we denote by $\mathcal{K}^{(j)}$. The product $v = DVu$ defines a one-to-one mapping $u \mapsto v$. Consequently, the statement

$$\exists v \neq 0 \text{ such that } H^{(j)}F^{(j)}v = 0 \text{ for all } j = 0, \ldots, m-1 \tag{5.17}$$

is equivalent to (5.16). With $w^{(j)} = (F^{(j)}v)^T$, and the fact that $H^{(j)}$ is a parity-check matrix of the code $\mathcal{K}^{(j)}$, we can state another equivalent condition for a decoding failure:

$$\exists v \neq 0 \text{ such that } w^{(j)} \in \mathcal{K}^{(j)} \text{ for all } j = 0, \ldots, m-1.$$

Assume that we have a vector v with Hamming weight $\omega_H(v) = n'$. Then, the vector $w^{(j)}$ have at most n' non-zero components, for each $j = 0, \ldots, m-1$. Now consider the matrix

$$\mathbf{w} = \begin{bmatrix} w^{(0)} \\ \vdots \\ w^{(m-1)} \end{bmatrix}.$$

Since we know that all the vectors $e_{j_i} = (e_{j_i}^{(0)}, \ldots, e_{j_i}^{(m-1)})^T$, $i = 1, \ldots, t$, are non-zero, and that all non-zero patterns are distributed uniformly, we also know that $\mathbf{w}$ contains exactly n' non-zero columns uniformly distributed over all non-zero vectors in $\mathbb{F}_q^m$. Assume that the non-zero columns in $\mathbf{w}$ are located at the indices $i_1, i_2, \ldots, i_{n'}$, let $\mathbf{w}_{n'}$ be a $m \times n'$ matrix consisting of the non-zero columns of $\mathbf{w}$, and let $H_{n'}^{(j)}$ be obtained from $H^{(j)}$ by removing all columns whose indices are not in the set $\{i_1, i_2, \ldots, i_{n'}\}$. Furthermore, denote by $\mathcal{K}_{n'}^{(j)}$ the code defined by the $n' \times s^{(j)}$ parity-check matrix $H_{n'}^{(j)}$. Thus, the statements $H^{(j)}W^T = 0$ and $H^{(j)}W_{n'}^T = 0$ are equivalent. Consequently, we can apply Lemma 5.6 on $\mathcal{K}_{n'}^{(j)}$, and $W_{n'}$ to overbound the probability $P_{n'}$ that a fixed vector v of weight n' satisfies

$$H^{(j)}F^{(j)}v = 0 \text{ for all } j = 0, \ldots, m-1. \tag{5.18}$$

We observe that the probability $P(v)$ for a vector v to fulfill (5.18) is independent of the positions of the non-zero symbols in v, but only depends on the weight $\omega_H(v) = n'$, i.e.,

$$P(v \text{ such that } \omega_H(v) = n') = P_{n'}.$$

Hence, the probability $P_f(j_1, \ldots, j_t)$ that (5.16) or equivalently (5.17) is satisfied can be over-bounded using a union bounding technique, by summing up over all non-zero vectors v:

$$P_f(j_1, \ldots, j_t) \leqslant \sum_{v \in \mathbb{F}_q^m \setminus \{0\}} P(v) = \sum_{n'=1}^{t} \sum_{\{v : \omega_H(v) = n'\}} P_{n'}. \tag{5.19}$$

Since the right side of (5.19) is independent of the indices $j_1, \ldots, j_t$ but only depends on t, we see that (5.19) is also an upper bound on the failure probability $P_f(t)$.

To improve (5.19), we should take care about the following fact: if a vector v fulfills (5.18), a vector $v' = \alpha v$ also fulfills (5.18) for all $\alpha \in \mathbb{F}_q \setminus \{0\}$. Therefore, we call v and αv *equivalent vectors*. Since there are $q - 1$ different non-zero elements in $\mathbb{F}_q$, there exists $q - 1$ equivalent vectors for each non-zero vector over $\mathbb{F}_q$. Thus, the number $N_{n'}$ of non-equivalent vectors of lenght t with a certain weight n' is calculated by

$$N_{n'} = \binom{t}{n'} \frac{(q-1)^{n'}}{q-1} = \binom{t}{n'} (q-1)^{n'-1}. \tag{5.20}$$

Hence, to obtain a better upper bound on $P_f(t)$, we can multiply the probabilities $P_{n'}$ bounded by (5.14) by the number of non-equivalent words of weight n' calculated by (5.20), and sum up over all weight $1 \leqslant n' \leqslant t$. In this way we obtain

$$\begin{aligned} P_f(t) &\leqslant \sum_{n'}^{t} P_{n'} N_{n'} \\ &\leqslant \frac{q^{-\sum_{j=0}^{m-1} s^{(j)}}}{q-1} \sum_{n'=0}^{t} \binom{t}{n'} \left(\frac{(q-1)q^m}{q^m - 1} \right)^{n'} \\ &= \left(\frac{q^m - \frac{1}{q}}{q^m - 1} \right)^t \frac{q^{-(m+1)(\tau_{IRS} - t)}}{q-1}. \end{aligned}$$

□

Chapter 6

Fractional Decoding and Collaborative Decoding

In a distributed system, we usually face a limitation on the disk input/output operations as well as on the amount of information transmitted for the purpose of decoding (decoding bandwidth). We known that under no limitations on the decoding bandwidth, given a linear code C it is possible to recover the information from any $\lfloor \frac{d-1}{2} \rfloor$ errors, where d denotes the minimum distance of the code.

Efficient recovery of data from a part of the codeword has been studied recently in the context of applications to distributed storage. One special case of this problem is *erasure correction* by array codes and in particular by MDS array codes. The most well-studied case of the erasure correction problem is recovery of one erasure from part of the codeword. This problem was introduced by Dimakis *et al.* [13].

Assuming that the system permits the decoder to utilize only an $\alpha \leqslant 1$ proportion of the whole codeword, Tamo *et al.* [73] extended the problem of erasure correction from partial information to the problem of *error correction.*

Clearly we should take $\alpha > \frac{k}{n}$ because the codewords encodes k data symbols, and even without errors to recover the data the decoder needs at least as many input symbols. If $\alpha = 1$, we return to the standard decoding problem.

The problem of study error correction for α in the range $\frac{k}{n} \leqslant \alpha < 1$ is called fractional decoding problem [73].

6.1 Fractional decoding

An $[sn, k]$ array code C is formed by a subset of $s \times n$ matrices $\mathbf{c} = (c_1, \ldots, c_n)$ in $(\mathbb{F}_q^s)^n$, where $\mathbb{F}_q$ is a finite field. Each column c_i of the matrix is a codeword coordinate, and the parameter s that determines the dimension of the column vector c_i is called *sub-packetization*. We may also consider C as a code over the alphabet $\mathbb{F}_q^s$, and then one error amounts to an incorrect column c_i.

Correcting up to t errors means correcting any combination of errors $\mathbf{e} = (e_1, \ldots, e_n)$ in $(\mathbb{F}_q^s)^n$ of Hamming weight $\omega(\mathbf{e}) := |\{i : e_i \neq 0\}| \leqslant t$, where the received codeword is the matrix $\mathbf{y} = \mathbf{c} + \mathbf{e}$. Note that the Hamming weight of a matrix counts the number of nonzero columns, not the number of nonzero entries.

Definition 6.1. *(Fractional decoding and α-decoding radius). Consider an $[sn, k]$ array code $C = \{\mathbf{c} = (c_1, \ldots, c_n)\}$ over the field $\mathbb{F}_q$, where $c_i \in \mathbb{F}_q^s$ is a column vector for $i = 1, \ldots, n$.*

i) We say that C can correct up to t errors by downloading an α-proportion of the codeword if there exist $n + 1$ functions

$$f_i : \mathbb{F}_q^s \longrightarrow \mathbb{F}_q^{\alpha_i s}, i = 1, \ldots, n \quad \text{and} \quad g : \mathbb{F}_q^{(\sum_{i=1}^n \alpha_i)s} \longrightarrow \mathbb{F}_q^{ns} \tag{6.1}$$

such that $\sum_{i=1}^{n} \alpha_i \leqslant n\alpha$ and for any codeword $(c_1, \ldots, c_n) \in C$ and any error vector $\mathbf{e} = (e_1, \ldots, e_n)$ of Hamming weight $\omega(\mathbf{e}) \leqslant t$, we have

$$g(f_1(c_1 + e_1), f_2(c_2 + e_2), \ldots, f_n(c_n + e_n)) = (c_1, c_2, \ldots, c_n). \tag{6.2}$$

ii) For $\alpha \geqslant \frac{k}{n}$, define the α-decoding radius $r_\alpha(C) = \tau_\alpha$ as the maximum number of t errors that the code C can correct by downloading an α-proportion of the codeword.

iii) For $\alpha \geqslant \frac{k}{n}$, we define the α-decoding radius of $[sn, k]$ codes as

$$r_\alpha(sn, k) = \max_{C \in \mathcal{C}_{sn,k}} r_\alpha(C) \tag{6.3}$$

where $\mathcal{C}_{sn,k}$ is the set of all $[sn, k]$ codes.

It is well known that for any code C we have $r_1(C) = \tau \leqslant \lfloor \frac{n-k}{2} \rfloor$, and the equality holds for MDS codes, since in the case $\alpha = 1$ we are deal with the standard decoding problem. So, in this case $r_1(sn, k) = \lfloor \frac{n-k}{2} \rfloor$.

Using the fact that given an MDS code C if we pick αn coordinates to form a punctured code $\widetilde{C}$, then this punctured code is an MDS code of length αn and dimension k, Tamo *et al.* [73] obtain the following lower bound on $r_\alpha(sn, k)$.

Lemma 6.2. *[73] For any $k \leqslant n$ and $\frac{k}{n} \leqslant \alpha \leqslant 1$,*

$$r_\alpha(sn, k) \geqslant \left\lfloor \frac{\alpha n - k}{2} \right\rfloor .$$

The main result of [73] is the following upper bound on $r_\alpha(C)$.

Theorem 6.3. *[73] Let C be an $[sn, k]$ array code over a field $\mathbb{F}_q$ and $\frac{k}{n} \leqslant \alpha \leqslant 1$. Then*

$$r_\alpha(C) \leqslant \left\lfloor \frac{n - \frac{k}{\alpha}}{2} \right\rfloor \tag{6.4}$$

An $[sn, k]$ array code C with $r_\alpha(C) = \left\lfloor \frac{n-\frac{k}{\alpha}}{2} \right\rfloor$ for α such that $\frac{k}{n} \leqslant \alpha < 1$ is said to have the *optimal α-decoding radius*.

Lemma 6.2 and Theorem 6.3 give us the following inequalities.

$$\left\lfloor \frac{\alpha n - k}{2} \right\rfloor \leqslant r_\alpha(sn, k) \leqslant \left\lfloor \frac{n - \frac{k}{\alpha}}{2} \right\rfloor . \tag{6.5}$$

More precisely, it was also shown in [73] that $RS(q^s, n, k)$ codes with evaluation set $\mathcal{L} \subseteq \mathbb{F}_q$ attain the optimal α-decoding radius.

Theorem 6.4. *[73] Given $k \leqslant n$ and $\frac{k}{n} \leqslant \alpha \leqslant 1$. Then*

$$r_\alpha(sn, k) = \left\lfloor \frac{n - \frac{k}{\alpha}}{2} \right\rfloor . \tag{6.6}$$

Note that to link the $RS(q^s, n, k)$ code with the Definition 6.1, each codeword coordinate is viewed as a vector of dimension s over $\mathbb{F}_q$. Thus $RS(q^s, n, k)$ can be viewed as an $[sn, k]$ array code over the base field $\mathbb{F}_q$.

Another family of codes which also have optimal α-decoding radius among all the codes of same length and dimension are the Folded Reed-Solomon (FRS) codes introduced by Guraswami and Rutra [26].

Definition 6.5. ***(Folded Reed-Solomon code).*** *Let $\mathbb{F}_q$ be a finite field of cardinality $q > sn$. Let γ be a primitive element of $\mathbb{F}_q$. An FRS code $FRS(sn, k)$ is an MDS array code with codewords in $\mathbb{F}_q^{sn}$ given by*

$$\left\{ \mathbf{c} = (c_1, \ldots, c_n) : c_i = (h(\gamma^{(i-1)s}), h(\gamma^{(i-1)s+1}), \ldots, h(\gamma^{(i-1)s+s-1})) \in \mathbb{F}_q^s \right\},$$

where $h \in \mathbb{F}_q[x]$, with $\deg h \leqslant ks - 1$ and $k < n$.

Example 6.6. *Let $\mathbb{F}_q$ be a finite field with $q > 16$ and γ be a primitive element of $\mathbb{F}_q$. The $FRS(sn,k) \subseteq \mathbb{F}_q^{sn}$ with $s = n = 4$ and $k = 2$ is the $FRS(4.4,2) \subseteq \mathbb{F}_q^{4.4}$ MDS array code given by*

$$\left\{\mathbf{c} = (c_1, \ldots, c_4) : c_i = (h(\gamma^{4(i-1)}), h(\gamma^{4(i-1)+1}), h(\gamma^{4(i-1)+2}), h(\gamma^{4(i-1)+3})) \in \mathbb{F}_q^4\right\},$$

where $h \in \mathbb{F}_q[x]$ with $\deg h(x) \leqslant 7$. Each codeword $\mathbf{c} \in FRS(4.4,2)$ can be written as

$$\mathbf{c} = \begin{bmatrix} h(\gamma^0) & h(\gamma^4) & h(\gamma^8) & h(\gamma^{12}) \\ h(\gamma^1) & h(\gamma^5) & h(\gamma^9) & h(\gamma^{13}) \\ h(\gamma^2) & h(\gamma^6) & h(\gamma^{10}) & h(\gamma^{14}) \\ h(\gamma^3) & h(\gamma^7) & h(\gamma^{11}) & h(\gamma^{15}) \end{bmatrix},$$

where $\deg h(x) \leqslant 7$.

Theorem 6.7. *[73] We have*

$$r_\alpha(FRS(sn,k)) = \left\lfloor \frac{n - \frac{k}{\alpha}}{2} \right\rfloor.$$

Proof. We need to define $n+1$ functions f_i, $i = 1, 2, \ldots, n$ and g that satisfy (6.2). Choose $f : \mathbb{F}_q^s \longrightarrow \mathbb{F}_q^{\alpha s}$ as follows: For any $(d_1, \ldots, d_s) \in \mathbb{F}_q^s$,

$$f(d_1, \ldots, d_s) = (d_1, d_2, \ldots, d_{\alpha s}). \tag{6.7}$$

Let $f_i = f$ for $1 \leqslant i \leqslant n$. Define a new code

$$C^\alpha = \{\mathbf{c} = (c_1^\alpha, \ldots, c_n^\alpha) = (f(c_1), \ldots, f(c_n)) : (c_1, \ldots, c_n) \in FRS(sn,k)\}. \tag{6.8}$$

It is easy to see that C^α defined above has the following equivalent description:

$$C^\alpha = \left\{(c_1^\alpha, \ldots, c_n^\alpha) : c_i^\alpha = (h(\gamma^{(i-1)s}), \ldots, h(\gamma^{(i-1)s+\alpha s-1})) \in \mathbb{F}_q^s, 1 \leqslant i \leqslant n, \right\} \tag{6.9}$$

where $h \in \mathbb{F}_q[x]$, with $\deg h \leqslant ks - 1$.

Since any $\frac{k}{\alpha}$ coordinates of C^α contain $\left(\frac{k}{\alpha}\right)(s\alpha)$ evaluations of the encoding polynomial h of degree less than sk, we can recover h and thus the whole codeword from any $\frac{k}{\alpha}$ of C^α. We thus conclude that C^α is an $\left[\alpha sn, \frac{k}{\alpha}\right]$ MDS array code, and so it can correct up to $\left\lfloor \frac{n-\frac{k}{\alpha}}{2} \right\rfloor$ errors.

If e_i is the error in the it-h coordinate of the codeword, we can write $f(c_i+e_i) = f(c_i)+ f(e_i)$ for $i = 1, 2, \ldots, n$. Suppose that $(c_1, \ldots, c_n) \in FRS(sn,k)$ and $|\{i : e_i \neq 0\}| \leqslant \left\lfloor \frac{n-\frac{k}{\alpha}}{2} \right\rfloor$,

then $(f(c_1),\ldots,f(c_n)) \in C^\alpha$ and $|\{i : f(e_i) \neq 0\}| \leqslant \left\lfloor \frac{n-\frac{k}{\alpha}}{2} \right\rfloor$. As a result, we can recover the codeword $(f(c_1),\ldots,f(c_n)) \in C^\alpha$ and thus recover the encoding polynomial h and finally the codeword $(c_1,\ldots,c_n) \in FRS(sn,k)$ from $(f(c_1+e_1),\ldots,f(c_n+e_n))$. This shows that

$$r_\alpha(FRS(sn,k)) \geqslant \left\lfloor \frac{n-\frac{k}{\alpha}}{2} \right\rfloor,$$

and proof is concluded. □

Example 6.8. *Let $\mathbb{F}_q$ be a finite field with $q > 24$, γ be a primitive element of $\mathbb{F}_q$, and C be the $FRS(4.6,2)$-code given by*

$$C = \left\{ \mathbf{c} = (c_1,\ldots,c_6) : c_i = (h(\gamma^{4(i-1)}), h(\gamma^{4(i-1)+1}), h(\gamma^{4(i-1)+2}), h(\gamma^{4(i-1)+3})) \in \mathbb{F}_q^4 \right\},$$

where $h \in \mathbb{F}_q[x]$ with $\deg h(x) \leqslant 7$. Each codeword $\mathbf{c} \in C$ can be written as

$$\mathbf{c} = \begin{bmatrix} h(\gamma^0) & h(\gamma^4) & h(\gamma^8) & h(\gamma^{12}) & h(\gamma^{16}) & h(\gamma^{20}) \\ h(\gamma^1) & h(\gamma^5) & h(\gamma^9) & h(\gamma^{13}) & h(\gamma^{17}) & h(\gamma^{21}) \\ h(\gamma^2) & h(\gamma^6) & h(\gamma^{10}) & h(\gamma^{14}) & h(\gamma^{18}) & h(\gamma^{22}) \\ h(\gamma^3) & h(\gamma^7) & h(\gamma^{11}) & h(\gamma^{15}) & h(\gamma^{19}) & h(\gamma^{23}) \end{bmatrix}.$$

Considering $\alpha = \frac{1}{2}$ the code C^α of Theorem 6.7 is given by

$$C^\alpha = \left\{ \mathbf{c}^\alpha = (c_1^\alpha,\ldots,c_n^\alpha) : c_i^\alpha = (h(\gamma^{4(i-1)}),\ldots,h(\gamma^{4(i-1)+3})) \in \mathbb{F}_q^4, 1 \leqslant i \leqslant 6 \right\},$$

and each codeword $\mathbf{c}^\alpha$ can be written as

$$\mathbf{c}^\alpha = \begin{bmatrix} h(\gamma^0) & h(\gamma^4) & h(\gamma^8) & h(\gamma^{12}) & h(\gamma^{16}) & h(\gamma^{20}) \\ h(\gamma^1) & h(\gamma^5) & h(\gamma^9) & h(\gamma^{13}) & h(\gamma^{17}) & h(\gamma^{21}) \end{bmatrix}.$$

Downloading those symbols of the codeword $\mathbf{c}$, we can correct at most $\left\lfloor \frac{6-\frac{2}{1/2}}{2} \right\rfloor = 1$ error.

6.2 Fractional decoding and collaborative decoding

In this section we propose a new probabilistic decoding method that can perform fractional decoding beyond the α-decoding radius.

6.2.1 Using collaborative decoding to increase the decoding radius

Schmidt *et al.* [62, 63] suggested to extend a low-rate $RS(n,k)$ code to an IRS code to perform syndrome decoding of the $RS(n,k)$ code beyond half the minimum distance, of course, with some failure probability. The scheme by Schmidt extends a usual low-rate RS code to an IRS code. This IRS code is denoted by $VIRS(q,n,k,m)$, where n and k are the original parameters of the $RS(q,n,k)$ code. The parameter m denotes the order of virtual interleaving. The Virtual IRS code can be defined as follows

Definition 6.9. *Let $RS(q,n,k)$ be an Reed-Solomon code. The virtually extended IRS code $VIRS(n,k,m)$ of extension order m is given by*

$$VIRS(n,k,m) = \left\{ \mathbf{c} = \begin{bmatrix} c^{(0)} \\ \vdots \\ c^{(m-1)} \end{bmatrix} = \begin{bmatrix} f^0(\mathcal{L}) \\ \vdots \\ f^{m-1}(\mathcal{L}) \end{bmatrix} \right\}, \tag{6.10}$$

where $f^i(x) = (f(x))^{i+1} \in \mathbb{F}_q[x]$ and $\deg f^i(x) < (i+1)(k-1)+1$. Clearly, the parameter m must satisfy $m(k-1)+1 \leqslant n$.

Note that the evaluation of $(f(x))^{i+1}$ corresponds to taking the $i+1$-th power of each element of the codeword $c = (c_1, \ldots, c_n) \in RS(q,n,k)$, i. e., $(c_1^{i+1}, \ldots, c_n^{i+1})$.

Using the approach of Algorithm 1, it is possible to correct $t < \tau_{VIRS}$ errors, where

$$\tau_{VIRS} = \frac{m}{m+1}\left(n - \left(\frac{m+1}{2}(k-1)+1\right)\right). \tag{6.11}$$

Note that this approach is also probabilistic and even though we consider $\mathbf{y} = \mathbf{c}+\mathbf{e}$ as a received word of a heterogeneous IRS code, we cannot apply the upper bound on the failure probability (5.15). The reason for this is the fact that in (5.15) it was assumed that the erroneous columns in the received matrices are distributed uniformly over all non-zero vectors. This is not true for the virtual extended code, since all symbols in a erroneous column j are just powers of the error symbols e_j. However, a bound on the failure probability $P_{f,VIRS}(t)$ for $m = 2$ is given in [62].

$$P_{f,VIRS}(t) \leqslant \left(\frac{q}{q-1} + \frac{1}{q}\right)^t \frac{q^{-3(\tau_{VIRS}-t)}}{q-1}.$$

Another approach used to increase the decoding radius of Reed-Solomon codes is found in [77], where Zeh *et al.*, defined the mixed virtual extension of a *homogeneous interleaved RS code* to an *heterogeneous interleaved RS code* with objective of perform decoding beyond its joined error-correcting capability [5].

6.2.2 Virtual projection of a Reed-Solomon code

In this subsection, we introduce the concept of virtual projection of a Reed-Solomon code $RS(q^s, n, k)$ in $\mathbb{F}_{q^s}^n$ with evaluation set $\mathcal{L} = \{\gamma_1, \ldots, \gamma_n\}$ in $\mathbb{F}_q$ to a heterogeneous RS code $IRS(q, n, \mathcal{K}, m)$. Our purpose is to use the virtual projection to perform fractional decoding beyond the α-decoding radius.

Definition 6.10. *Let $A_0, A_1, \ldots, A_{m-1}$ be m pairwise disjoint sets of the field $\mathbb{F}_q$. For each $j = 0, 1, \ldots, m-1$, define the annihilator polynomials of the set A_j to be*

$$p_j(x) = \prod_{\omega \in A_j} (x - \omega) \in \mathbb{F}_q[x]. \tag{6.12}$$

Note that, $\deg p_j(x) = |A_j|$ for $j = 0, \ldots, m-1$.

Definition 6.11. *Let $B = \mathbb{F}_q$, and let $F = \mathbb{F}_{q^s}$ be a finite field extension of B of degree s. The field trace is defined as follows: for any $\beta \in F$,*

$$tr_{F/B}(\beta) = \beta + \beta^q + \beta^{q^2} + \ldots + \beta^{q^{s-1}}.$$

Lemma 6.12. *Given an finite extension $\mathbb{F}_q^s$ of $\mathbb{F}_q$, the field trace is $\mathbb{F}_q$-linear.*

Theorem 6.13. *[4] Let $\{\zeta_0, \zeta_1, \ldots, \zeta_{s-1}\}$ be a basis of F over B, and let $\{\nu_0, \nu_1, \ldots, \nu_{s-1}\}$ be the dual basis (i.e., $tr_{F/B}(\zeta_i \nu_j) = \delta_{i,j}$ for all i, j). Then*

$$\beta = \sum_{i=0}^{s-1} tr_{F/B}(\zeta_i \beta) \nu_i.$$

In other words, any element β in F can be calculated from its s projections $\left\{tr_{F/B}(\zeta_i \beta)\right\}_{i=0}^{s-1}$ on B.

We remark that given a basis $\{\zeta_0, \zeta_1, \ldots, \zeta_{s-1}\}$ of F over B, its trace dual basis always exists [4].

Let $\mathcal{L} \subseteq \mathbb{F}_q$, in [73] to show that an $RS(q^s, n, k)$ with evaluation points in $\mathcal{L}$ has the optimal α-decoding radius, Tamo defined a decoding scheme based on downloading an amount of symbols of each codeword coordinates. The next definition is a modification of the downloading symbols in [73].

Definition 6.14. *Given a polynomial $h(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \ldots + a_0 \in \mathbb{F}_{q^s}[x]$ and m pairwise disjoint subsets $A_0, \ldots, A_{m-1}$ of $\mathbb{F}_q$, define $h_i(x) \in \mathbb{F}_q[x]$ by*

$$h_i(x) = tr(\zeta_i a_{k-1})x^{k-1} + tr(\zeta_i a_{k-2})x^{k-2} + \ldots + tr(\zeta_i a_0). \tag{6.13}$$

For each $j = 0, \ldots, m-1$ *consider the polynomial*

$$T_j(h)(x) = h_{s-m+j}(x)(p_j(x))^{(s-m)(j+1)} + \sum_{u=0}^{s-m-1} h_u(x)(p_j(x))^{u(j+1)} \tag{6.14}$$

Lemma 6.15. *Let* $C = RS(q^s, n, k)$ *be a Reed-Solomon code with evaluation set* $\mathcal{L}$ *in* $\mathbb{F}_q$*, and let* $h(\mathcal{L}) \in C$ *be a codeword of* C*. Then, each* $T_j(h)(\mathcal{L})$ *is a codeword of the RS code*

$$\mathcal{C}_j = RS\left(q, n, k + |A_j|(s-m)(j+1)\right). \tag{6.15}$$

Proof. First note that

$$\deg T_j(h)(x) \leqslant \max\left\{\deg h_{s-m+j}(x)(p_j(x))^{(s-m)(j+1)}, \deg \sum_{u=0}^{s-m-1} h_u(x)(p_j(x))^{u(j+1)}\right\}$$

and we can check that

$$\begin{aligned}\deg h_{s-m+j}(x)(p_j(x))^{(s-m)(j+1)} &= \deg h_{s-m+j}(x) + |A_j|(s-m)(j+1) \\ &< k + |A_j|(s-m)(j+1),\end{aligned}$$

and

$$\deg \sum_{u=0}^{s-m-1} h_u(x)(p_j(x))^{u(j+1)} < k + |A_j|(s-m)(j+1).$$

So, $\deg T_j(h)(x) < k + |A_j|(s-m)(j+1)$ for all $j = 0, 1, \ldots m-1$. Now we must check that $T_j(h)(\mathcal{L}) \in \mathbb{F}_q^n$. By definition, $T_j(h)(\mathcal{L}) = (T_j(h)(\gamma_1), \ldots, T_j(h)(\gamma_n))$, so we just need to prove that $T_j(h)(\gamma_i) \in \mathbb{F}_q$ for all $i = 1, \ldots, n$. For all $j = 0, \ldots, m-1$, we have

$$T_j(h)(\gamma_i) = h_{s-m+j}(\gamma_i)(p_j(\gamma_i))^{(s-m)(j+1)} + \sum_{u=0}^{s-m-1} h_u(\gamma_i)(p_j(\gamma_i))^{u(j+1)}$$

as $h_u(x), p_j(x) \in \mathbb{F}_q[x]$ and $\gamma_i \in \mathbb{F}_q$, it is clear that $T_j(h)(\gamma_i) \in \mathbb{F}_q$ for all $i = 1, \ldots, n$ and $j = 0, \ldots, m-1$. □

Definition 6.16. *Let* $C = RS(q^s, n, k)$ *be a Reed-Solomon code with evaluation set* $\mathcal{L}$ *in* $\mathbb{F}_q$ *given by* $\mathcal{L} = \{\gamma_1, \ldots, \gamma_n\}$ *and let* $A_0, \ldots, A_{m-1}$ *any pairwise disjoint subsets of* $\mathbb{F}_q$ *such that* $\sum_{j=0}^{m-1} |A_j| \geqslant k$*. The Virtual Projection* $\mathcal{C}_{P_{m/s}}(q, n, \mathcal{K})$ *is given by*

$$\mathcal{C}_{P_{m/s}} = \left\{ \begin{bmatrix} c^{(0)} \\ c^{(1)} \\ \vdots \\ c^{(m-1)} \end{bmatrix} = \begin{bmatrix} T_0(h)(\mathcal{L}) \\ T_1(h)(\mathcal{L}) \\ \vdots \\ T_{m-1}(h)(\mathcal{L}) \end{bmatrix} \right\}, \tag{6.16}$$

where $T_j(h)(x)$ is defined in (1.8), $\mathcal{K} = \{k_0, \ldots, k_{m-1}\}$ and the dimensions k_j are given by $k_j = k + |A_j|(s-m)(j+1)$ for all $j = 0, \ldots, m-1$.

Assume that a codeword $c(\mathcal{L}) = (c(\gamma_1), \ldots, c(\gamma_n)) \in RS(q^s, n, k)$ is transmitted over a noisy channel, which adds t errors in such a way that the word $y(\mathcal{L}) = c(\mathcal{L}) + e(\mathcal{L})$ where $y(x), e(x) \in \mathbb{F}_{q^s}[x]_n$ is observed at the channel output. Using the observed word $y(\mathcal{L})$, we calculate the m polynomials $T_j(y)(x)$, $j = 0, \ldots, m-1$, and create the matrix

$$\mathbf{y} = \begin{bmatrix} T_0(y)(\gamma_1) & \ldots & T_0(y)(\gamma_n) \\ T_1(y)(\gamma_1) & \ldots & T_1(y)(\gamma_n) \\ \vdots & \ddots & \vdots \\ T_{m-1}(y)(\gamma_1) & \ldots & T_{m-1}(y)(\gamma_n) \end{bmatrix} \tag{6.17}$$

Theorem 6.17. *Let $c(\mathcal{L})$ be a codeword of a Reed-Solomon code $C = RS(q^s, n, k)$ with evaluation set $\mathcal{L}$ in $\mathbb{F}_q$. Assume that $c(\mathcal{L})$ was transmitted over a noisy channel and that the word $y(\mathcal{L}) = c(\mathcal{L}) + e(\mathcal{L})$ is received. If $e = (e_1, \ldots, e_n)$ has t nonzero coefficients $e_{i_1}, \ldots, e_{i_t}$ then the matrix $\mathbf{y}$ is a corrupted codeword of the $\mathcal{C}_{P_{m/s}}(q, n, \mathcal{K})$ code with at most t erroneous columns at the positions $i_1, \ldots, i_t$.*

Proof. If $e = 0$, then $y = c \in RS(q^s, n, k)$, and Lemma 6.15 states that $\mathbf{y}$ is a codeword of the virtual projection $\mathcal{C}_{P_{m/s}}(q, n, \mathcal{K})$. Note that

$$T_j(y)(\gamma_i) = T_j(c+e)(\gamma_i) = T_j(c)(\gamma_i) + T_j(e)(\gamma_i).$$

It follows by the fact that the trace field $tr_{\mathbb{F}_{q^s}/\mathbb{F}_q}$ is $\mathbb{F}_q$-linear and $\gamma_i \in \mathcal{L} \subseteq \mathbb{F}_q$ that if $e_i = 0$, that is, if $i \notin \{i_1, \ldots, i_t\}$, then $T_j(e)(\gamma_i) = 0$ for all $j = 0, \ldots, m-1$. Otherwise if $i \in \{i_1, \ldots, i_t\}$, then $T_j(e)(\gamma_i)$ must be non-zero, so $\mathbf{y}$ has at most t erroneous columns. □

Unlike the virtual extension to an IRS code [63], where it is possible to ensure that given a word $y = c + e$ the virtual extension of y is a word with exactly t erroneous columns, in the virtual projection we can not assure it.

Given a codeword $c \in RS(q, n, k)$ and its virtual extension $\mathbf{c} \in VIRS$. In addition, in the virtual extension approach, when we recover the word $\mathbf{c} \in VIRS$, we immediately recover the codeword $c \in RS(q, n, k)$ (the first row of the codeword C). Given a codeword $c \in RS(q^s, n, k)$ and its virtual projection $\mathbf{c} \in \mathcal{C}_{P_{m/s}}$. In virtual projection, it is not so immediate that we can recover the codeword $c \in RS(q^s, n, k)$ just by recovering the codeword $\mathbf{c} \in \mathcal{C}_{P_{m/s}}$, but the following ensures it.

Lemma 6.18. *Let* $\{T_j(h)(x)\}_{j=0}^{m-1}$ *be polynomials as in (6.14). Suppose that* $A_0, \ldots, A_{m-1}$ *subsets of* $\mathbb{F}_q$ *are such that* $\sum_{j=0}^{m-1} |A_j| \geqslant \deg h(x)$*, then we can recover the polynomials* $\{h_j(x)\}$ *and consequently, we can recover* $h(x)$*.*

Proof. $T_j(h)(\omega) = h_0(\omega)$ for all $\omega \in A_j$; of course, we can rewrite (6.14) as

$$\begin{aligned} T_j(h)(x) &= h_{s-m+j}(x)(p_j(x))^{(s-m)(j+1)} \\ &\quad + \sum_{u=0}^{s-m-1} h_u(x)(p_j(x))^{u(j+1)} \\ &= h_{s-m+j}(x)(p_j(x))^{(s-m)(j+1)} \\ &\quad + h_0(x)(p_j(x))^{0(j+1)} + \sum_{u=1}^{s-m-1} h_u(x)(p_j(x))^{u(j+1)}. \end{aligned}$$

So, $T_j(h)(\omega) = h_0(\omega)$ for all $\omega \in A_j$. Then, we know the evaluations of $h_0(\omega)$ at all the points $\cup_{j=0}^{m-1} A_j$ and by assumption, $\sum_{j=0}^{m-1} |A_j| \geqslant \deg h(x) \geqslant \deg h_0(x)$, so we can recover $h_0(x)$. Now from $h_0(x)$ and $\{T_j(h)(x)\}_{j=0}^{m-1}$, we can calculate the polynomials

$$\begin{aligned} T_j^{(1)}(h)(x) &= \frac{T_j(h)(x) - h_0(x)}{p_j(x)^{j+1}} \\ &= h_{s-m+j}(x)(p_j(x))^{(s-m-1)(j+1)} \\ &\quad + h_1(x) + \sum_{u=2}^{s-m-1} h_u(x)(p_j(x))^{(u-1)(j+1)}. \end{aligned}$$

So, $T_j^{(1)}(h)(\omega) = h_1(\omega)$ for all $\omega \in A_j$, and again, we know the evaluation of $h_1(x)$ in $\cup_{j=0}^{m-1} A_j$. So, we can recover $h_1(x)$. From $h_0(x), h_1(x)$ and $\{T_j(h)(x)\}_{j=0}^{m-1}$ we can calculate the polynomials

$$T_j^{(2)} = \frac{T_j^{(1)}(h)(x) - h_1(x)}{p_j(x)^{j+1}}.$$

Since $T_1^{(2)}(h)(\omega) = h_2(\omega)$ for all $\omega \in A_j$, by the previous argument we can recover $h_2(x)$. Generally, the polynomials $\{h_{l-m+j}(x)\}_{j=0}^{m-1}$ can be recovered from

$$h_{s-m+j}(x) = \frac{T_j(h)(x) - \sum_{u=0}^{s-m-1} h_u(x)(p_j(x))^{u(j+1)}}{(p_j(x))^{(s-m)(j+1)}}.$$

□

Given an $RS(q^s, n, k)$-code with evaluation set $\mathcal{L}$ in $\mathbb{F}_q$ and its virtual projection $\mathcal{C}_{P_{m/s}}$ by Lemma 6.18, we conclude that it is possible to recover a codeword $c \in RS(q^s, n, k)$ using the code $\mathcal{C}_{P_{m/s}}$ whenever the received word $y = c + e$ has no more than t errors with $t < \tau_{P_{m/s}}$,

where $\tau_{P_{m/s}}$ denotes the decoding radius of $\mathcal{C}_{P_{m/s}}$. Hence, we have the following algorithm.

Algorithm 2: Virtual Projection IRS Decoder

Input: Received word $y(\mathcal{L}) = c(\mathcal{L}) + e(\mathcal{L})$, $\alpha = m/s$

For: $j = 0$ to $m-1$ **do**

Create the matrix $\mathbf{y}$ from $T_j(y)(\mathcal{L})$ and calculate the syndromes $S^{(0)}, \ldots, S^{(m-1)}$.

Compute t and $\Lambda(x)$ by Algorithm 1 in [60] .

if $t < \tau_{P_\alpha}$ *and* $\Lambda(x)$ *is* t*-valid* **then**

  for each j from 0 to $m-1$ **do**

  evaluate errors, and calculate $T_j(e)(\mathcal{L})$

  calculate $T_j(\hat{c})(\mathcal{L}) = T_j(y)(\mathcal{L}) - T_j(e)(\mathcal{L})$

  Use Lemma 6.18 to compute $c(\mathcal{L})$

else

  decoding failure

output: $c(\mathcal{L}) \in RS(q^s, n, k)$ or decoding failure

Theorem 6.19. *Let $C = RS(q^s, n, k)$ be a Reed-Solomon code then its virtual projection code $\mathcal{C}_{P_{m/s}}(q, n, \mathcal{K})$ given by Definition 6.16. The maximum decoding radius $\tau_{P_{m/s}}$ is*

$$\tau_{P_{m/s}} = \frac{m}{m+1}\left(n - k - \frac{(s-m)}{m}\sum_{j=0}^{m-1}|A_j|(j+1)\right). \tag{6.18}$$

Proof. The decoding radius of the code $\mathcal{C}_{P_{m/s}}(q, n, \mathcal{K})$ is the error-correcting radius of the heterogeneous $IRS(q, n, \mathcal{K}, m)$ code with $\mathcal{K} = \{k_0, \ldots, k_{m-1}\}$ and dimensions k_j given by $k_j = k + |A_j|(s-m)(j+1)$ for all $j = 0, \ldots, m-1$. The correcting radius is given by (5.12)

$$\begin{aligned}\tau_{P_{m/s}} &= \frac{m}{m+1}\left(n - \frac{1}{m}\sum_{j=0}^{m-1}k_i\right)\\ &= \frac{m}{m+1}\left(n - k - \frac{s-m}{m}\sum_{j=0}^{m-1}|A_j|(j+1)\right).\end{aligned}$$

□

Corollary 6.20. *Let $C = RS(q^s, n, k)$ be a Reed-Solomon code and $\mathcal{C}_{P_{m/s}}(q, n, \mathcal{K})$ its virtual projection as in (6.16), then the following parameters hold:*

i) If $m = s$, then $\tau_{P_{m/s}} = \frac{s}{s+1}(n-k)$;

ii) If $m = s = 1$,then $\tau_{P_{m/s}} = \frac{n-k}{2} = \tau$;

iii) If $|A_j| = b$ *for all* $j = 0, \ldots, m-1$, *then*

$$\tau_{P_{m/s}} = \frac{m}{m+1}\left(n - k - b\frac{(s-m)}{m}\binom{m+1}{2}\right).$$

Proof. Straight forward calculation from (6.18). □

It is worth to mentioning a few special cases: if $m = s$, then $\tau_{P_{m/s}}$ is the decoding radius of a *homogeneous* interleaved RS code [60, 63]. For $m = s = 1$ the result $\tau_{P_{m/s}}$ is the decoding radius of the $RS(q, n, k)$ Reed-Solomon code over $\mathbb{F}_q$.

6.2.3 Fractional decoding beyond the α-decoding radius

Let $C = RS(q^s, n, k)$ be a Reed-Solomon code with evaluation set $\mathcal{L} = \{\gamma_1, \ldots, \gamma_n\}$ in $\mathbb{F}_q$. Let $\alpha = m/s$, where m and s are positive integers and K is a multiple of m. We will show that it is possible to perform fractional decoding beyond the α-decoding radius.

Let $c = (c_1, \ldots, c_n) = (h(\gamma_1), \ldots, h(\gamma_n)) \in RS(q^s, n, k)$, where $h(x) \in \mathbb{F}_{q^s}[x]_k$. Let also $A_0, \ldots, A_{m-1}$ be m pairwise disjoint subsets of $\mathbb{F}_q$, each of size k/m. The m symbols we download from the i-th coordinate are

$$d_i^j = tr_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\zeta_{s-m+j}c_i)(p_j(\gamma_i))^{(s-m)(j+1)} + \sum_{u=0}^{s-m-1} tr_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\zeta_u c_i)(p_j(\gamma_i))^{u(j+1)}. \quad (6.19)$$

Substituting c_i by $h(\gamma_i)$ for all $i = 1, \ldots, n$, we see that $(d_1^j, \ldots, d_n^j) = (T_j(h)(\gamma_1), \ldots, T_j(h)(\gamma_n))$ is the j-th row of the virtual projection code $\mathcal{C}_{P_\alpha}$ of C. Now by the fact that $|A_j| = k/m$ for all j, Corollary 6.20 yields

$$\tau_{P_\alpha} = \frac{1}{m+1}\left(mn + k\binom{m}{2} - \frac{k}{\alpha}\binom{m+1}{2}\right). \quad (6.20)$$

As $\sum_{j=0}^{m-1} |A_j| = k$, Algorithm 1 is able to recover the codeword c in $RS(q^s, n, k)$ with failure probability given by Theorem 6.22 if c has no more than $t \leqslant \tau_{P_\alpha}$ errors.

Note that if $m = 1$,then $\alpha = 1/s$ and

$$\begin{aligned}\tau_{P_\alpha} &= \frac{1}{2}\left(n + k\binom{1}{2} - sk\binom{2}{2}\right)\\ &= \frac{1}{2}\left(n - \frac{k}{\alpha}\right) = \tau_\alpha.\end{aligned}$$

For $m \geqslant 2$, we would like to improve the fractional decoding radius of $RS(q^s, n, k)$, it means that we are interested in the case $\tau_{P_\alpha} \geqslant \tau_\alpha$, that is,

$$\tau_{P_\alpha} = \frac{1}{m+1}\left(mn + k\binom{m}{2} - \frac{k}{\alpha}\binom{m+1}{2}\right) \geqslant \frac{n - k/\alpha}{2}. \quad (6.21)$$

and it is possible to check that (6.21) is true if and only if

$$R = \frac{k}{n} \leqslant \frac{\alpha}{m(1-\alpha)+1} = \frac{m}{m(s-m)+s}. \tag{6.22}$$

This can be summarized in the following theorem.

Theorem 6.21. *Let $RS(q^s, n, k)$ be a Reed-Solomon Code with evaluation set $\mathcal{L} = \{\gamma_1, \ldots, \gamma_n\}$ in $\mathbb{F}_q$ and $\alpha = m/s$. If $m \geqslant 2$ and the rate of C is restricted as in (6.22), then the maximum α-decoding radius of C using Algorithm 1 is*

$$\tau_{P_\alpha} = \frac{1}{m+1}\left(mn + k\binom{m}{2} - \frac{k}{\alpha}\binom{m+1}{2}\right). \tag{6.23}$$

Moreover, in this case, $\tau_{P_\alpha} \geqslant \tau_\alpha$.

6.2.4 Failure probability of the virtual projection IRS decoder algorithm

The failure probability can be calculated in the same way as done in [60] and [77]. We observe that the values of $T_{j_1}(e)(\gamma_i)$ and $T_{j_2}(e)(\gamma_i)$ do not depend of each other for all $j_1, j_2 \in \{0, \ldots, m-1\}$, and then we can assume that if $\mathbf{y}$ in (6.17) is corrupted by t errors, that is, $\mathbf{y} = \mathbf{c} + \mathbf{e}$ where $\mathbf{e}$ has t non-zero columns, then each non-zero column is an independent random vector uniformly distributed over $\mathbb{F}_q^m \setminus \{0\}$. Hence, we can apply Lemma 5.6 and Theorem 5.8 to upper bound the failure probability of Algorithm 2.

Theorem 6.22. *Let $C = RS(q^s, n, k)$ be a Reed-Solomon Code with evaluation set $\mathcal{L} = \{\gamma_1, \ldots, \gamma_n\}$ in $\mathbb{F}_q$, and $\alpha = m/s$. If $m \geqslant 2$ and the rate of C is restricted as in (6.22). The probability for a decoding failure using the Algorithm 2 is upper bounded by*

$$P_{f_\alpha}(t) \leqslant \left(\frac{q^m - \frac{1}{q}}{q^m - 1}\right)^t \frac{q^{-(m+1)(\tau_{P_\alpha} - t)}}{q-1}.$$

Example 6.23. *Let $\mathcal{C} = RS(31^5, 31, 4)$ be a Reed-Solomon code with evaluation set $\mathcal{L} \subseteq \mathbb{F}_{31}$ in this case the decoding radius of C is $\tau = 13$ and $R \simeq 0.1290$. By definition, $\alpha = \frac{m}{5}$ and $\frac{4}{31} \leqslant \frac{m}{5} < 1$, thus $m \in \{1, 2, 3, 4\}$. Let $\alpha_i = \frac{i}{5}$ for $i = 2, 3, 4$. For each α_i we have*

a) $\tau_{\alpha_1} = \tau_{P_{\alpha_1}} = 5$.

b) $\tau_{\alpha_2} = 10 < 12 = \tau_{P_{\alpha_2}}$.

c) $\tau_{\alpha_3} = 12 < 16 = \tau_{P_{\alpha_3}}$.

d) $\tau_{\alpha_4} = 13 < 19 = \tau_{P_{\alpha_4}}$.

The failure probability of c) is given in Table I.

Table 6.1: FAILURE PROBABILITY $P_{f_{\alpha_3}}(t)$ FOR THE REED-SOLOMON CODE $RS(31^5, 31, 4)$.

t	12	13	14	15
$P_{f_{\alpha_3}}(t)$	4.58×10^{-26}	4.23×10^{-20}	3.91×10^{-14}	3.61×10^{-8}

Example 6.24. *Let $\mathcal{C} = RS((2^5)^5, 31, 6)$ be a Reed-Solomon code with evaluation set $\mathcal{L} \subseteq \mathbb{F}_{2^5}$ in this case the decoding radius of $\mathcal{C}$ is $\tau = \lfloor \frac{n-k}{2} \rfloor = 12$ and $R = \frac{k}{n} \simeq 0.1935$. By definition $\alpha = \frac{m}{5}$ and $\frac{6}{31} \leqslant \frac{m}{5} < 1$, thus $m \in \{1, 2, 3, 4\}$. If we denoted $\alpha_i = \frac{i}{5}$ for $i = 2, 3, 4$ then for each α_i we have*

a) $\tau_{\alpha_2} = 8 > \tau_{P_{\alpha_2}} = 7$.

This is due to the fact that $R \simeq 0.1935$ and $\frac{\alpha_2}{2(1-\alpha_2)+1} \simeq 0.1818$ that is (6.22) is not true in this case.

b) $\tau_{\alpha_3} = 10 < 12 = \tau_{P_{\alpha_3}}$.

c) $\tau_{\alpha_4} = 11 < 16 = \tau_{P_{\alpha_4}}$.

Note that $\tau_{P_{\alpha_4}}$ is even greater than the decoding radius of C. So, without accessing the entire codeword it is possible to recover more than $\lfloor \frac{n-k}{2} \rfloor$ errors with failure probability given in the Table II.

Table 6.2: FAILURE PROBABILITY $P_{f_{\alpha_4}}(t)$ FOR THE REED-SOLOMON CODE $RS((2^5)^5, 31, 6)$.

t	11	12	13	14	15
$P_{f_{\alpha_4}}(t)$	7.58×10^{-40}	2.54×10^{-32}	8.53×10^{-25}	2.86×10^{-17}	9.61×10^{-10}

6.3 Fractional decoding and NRT metric codes

As mentioned in Chapter 2, the NRT metric is a special case of the poset metrics. In addition, we have observed that many concepts related to the codes provided with the Hamming

metric can be extended and studied for codes equipped with the NRT metric, and poset metrics in general.

In this section, we will describle the problem of fractional decoding of linear codes provided with the Niederreiter-Rosenbloom-Tsfasman metric. We start introducing the basic concepts about poset codes [19].

6.3.1 Poset codes

A partial order relation over a set X is a binary relation $\preceq$ satisfying the following conditions:

1. (Reflexivity) $i \preceq i$ for all $i \in X$;
2. (Anti-symmetry) Given $i, j \in X$, if $i \preceq j$ and $j \preceq i$, then $i = j$;
3. (Transitivity) $i \preceq j$ and $j \preceq k$, then $i \preceq k$.

The pair $P = (X, \preceq)$, consisting of a non-empty set $X$and a partial order $\preceq$ over X, is called a *partially ordered set*, or, for short, a *poset*. We say that $i, j \in X$ are comparable in P if either $i \preceq j$ or $j \preceq i$ otherwise i and j are said to be incomparable in P.

Given a poset $P = (X, \preceq)$ and a subset $Y \subseteq X$, the restriction of $\preceq$ to Y is called the restricted order. To emphasize this inclusion relation we may write $P_X = (X, \preceq)$ and $P_Y = (Y, \preceq)$. In this situation we say that Y is a *subposet* of X.

Definition 6.25. *A subposet I of X is called an ideal of P if it satisfies the closeness property: If $i \in I$ and $j \preceq i$, then $j \in I$.*

Let $P = (X, \preceq)$ be a poset and A a subset of X, the smallest ideal containing A is called the *ideal generated* by A and denoted by $\langle A \rangle_P$.

In this section we are concerned with finite posets, that is, poset over finite sets. It follows that, up to isomorphism, we assume that $X = [n] = \{1, \ldots, n\}$ for some positive integer n.

Example 6.26. *An anti-chain is a poset $P_A = ([n], \preceq_A)$ where any two distinct elements of $[n]$ are incomparable, that is,*

$$P_A = ([n], \{1 \preceq_A 1, 2 \preceq_A 2, \ldots, n \preceq_A n\}).$$

Example 6.27. *A chain is a poset* $P_C = ([n], \preceq_C)$ *given by*

$$P_C = ([n], \{1 \preceq_C 2 \preceq_C 3 \preceq_C \ldots \preceq_C n\}).$$

Example 6.28. *Consider a partition*

$$[n] = \bigcup_{i=1,\ldots,l} H_i,$$

with $h_i = |H_i|$. *Define* $H = (H_1, \ldots, H_l)$ *and* $h = (h_1, \ldots, h_l)$ *to be hierarchy spectrum and hierarchy array, respectively. We remark that* $n = h_1 + h_2 + \ldots + h_l$. *A hierarchical poset (also known as weak order) with hierarchy spectrum* H *is the poset* $P_H = ([n], \preceq_H)$, *where*

$$a \preceq_H b \text{ iff } a \in H_i, b \in H_j \text{ and } i < j.$$

If we consider a natural labelling of the poset, we must have $H_1 = \{1, 2, \ldots, h_1\}$ *and*

$$H_j = \{(h_1 + \ldots + h_{j-1}) + 1, (h_1 + \cdots + h_{j-1}) + 2, \ldots, (h_1 + \cdots + h_{j-1}) + h_j\}$$

for every $1 < j \leqslant l$.

We remark that, in case $l = 1$, *we have only one level and the poset is an anti-chain. On the other hand, in case* $l = n$, *we have that each* $h_i = 1$ *and so, we have a hierarchical poset with hierarchy array* $h = (1, 1, \ldots, 1)$, *that is, a total order.*

Example 6.29. *Consider a partition*

$$[n] = \bigcup_{i=1,\ldots,l} R_i$$

and define $s_i = |R_i| > 0$. *We call* $R = (R_1, \ldots, R_l)$ *and* $S = (s_1, \ldots, s_l)$ *the chain spectrum and chain array, respectively. We remark that* $n = s_1 + s_2 + \ldots + s_l$. *We write*

$$R_1 = \{x_{1,1}, x_{1,2}, \ldots, x_{1,s_1}\}, \ldots, R_l = \{x_{l,1}, x_{l,2}, \ldots, x_{l,s_l}\}$$

and define the poset $P_R = ([n], \preceq_R)$ *with relation* $\preceq_R$ *given by*

$$x_{i,j} \preceq_R x_{i',j'} \text{ iff } i = i' \text{ and } j \leq j'.$$

We remark that, in case $l = 1$ *we have only one chain, so a multi-chain poset with chain array* $S = (n)$ *is a chain. On the other hand, in case* $l = n$, *we have that each* $s_i = 1$ *and so, a multi chain poset with chain array* $S = (1, 1, \ldots, 1)$, *that is, an anti-chain.*

Example 6.30. *In Example 6.29, consider a partition*

$$[m] = \bigcup_{i=1,\ldots,n} R_i,$$

where $s = s_i = |R_i|$, $R = (R_1, \ldots, R_n)$ *and* $S = (s, \ldots, s)$, *so in this case* $m = ns$. *We say that* P_{NRT} *is a Niederreiter-Rosenbloom-Tsafsman poset, or NRT poset. In this case, we denote it by* $P_{NRT}(n, s) = ([ns], \preceq_{NRT})$.

Given a finite poset $P = ([n], \preceq)$ and a finite field $\mathbb{F}_q$, the set $[n]$ and the coordinates of any $x \in \mathbb{F}_q^n$ are related by the function $f : [n] \to \mathbb{F}_q^n$ given by $f(i) = x_i$. So, it is possible to define a P-weight on $\mathbb{F}_q^n$.

Definition 6.31. *Given a finite poset* $P = ([n], \preceq)$ *and* $x \in \mathbb{F}_q^n$, *the* P*-weight of* x *is given by*

$$\omega_P(x) = |\langle supp(x) \rangle_P|$$

where $supp(x) := \{i : x_i \neq 0\}$.

Example 6.32. *Let* $x = (1, 0, 1, 0) \in \mathbb{F}_2^4$, *and the posets*

$$\begin{aligned} P_A = ([4], \preceq_A) &= ([4], \{1 \preceq_A 1, 2 \preceq_A 2, 3 \preceq_A 3, 4 \preceq_A 4\}) \\ P_N = ([4], \preceq_N) &= ([4], \{1 \preceq_N 1, 2 \preceq_N 2, 3 \preceq_N 3, 4 \preceq_N 4, 1 \preceq_N 3, 2 \preceq_N 3, 2 \preceq_N 4\}). \end{aligned}$$

Then $\omega_H(1, 0, 1, 0) = |\langle 1, 3 \rangle_H| = |\{1, 3\}| = 2$ *and* $\omega_H(1, 0, 1, 0) = |\langle 1, 3 \rangle_N| = |\{1, 2, 3\}| = 3$.

Example 6.33. *Consider the anti-chain poset* $P_A = ([n], \preceq_A)$ *of Example 6.26 and* $x \in \mathbb{F}_q^n$, *then*

$$\begin{aligned} \omega_{P_A}(x) &= |\langle supp(x) \rangle_A| \\ &= |\{i : x_i \neq 0\}|, \end{aligned}$$

which coincides with the Hamming weight of x.

Example 6.34. *Let*$P_C = ([n], \preceq_C)$ *be the chain poset of Example 6.27 and* $x \in \mathbb{F}_q^n$, *then*

$$\begin{aligned} \omega_{P_C}(x) &= |\langle supp(x) \rangle_C| \\ &= \max\{j : x_j \neq 0\} \end{aligned}$$

Example 6.35. *Let us consider the NRT poset consisting of n disjoint chains, each having length equal to s, as in Example 6.30. We write $m = ns$ and express*

$$x = (x_{1,1}, \ldots, x_{1,s}; x_{2,1}, \ldots, x_{2,s}; \ldots; x_{n,1}, \ldots, x_{n,s}) \in \mathbb{F}_q^m \tag{6.24}$$

where $x_{i,1}, \ldots, x_{i,s}$ are the coordinates corresponding to the i-th chain. We just recall that $x_{i,j} \preceq_{NRT} x_{i',j'}$ if and only if $i = i'$ and $j \leqslant j'$. We define $\rho(x_{i,j}) := \max\{j : x_{i,j} \neq 0\}$, and $\omega_{P_{NRT}}(x) = \sum_{i=1}^{n} \rho(x_{i,j})$. In other words, the P_{NRT} weight equivalent to the NRT weight of Chapter 2. To be more precise with the language of Chapter 2, we use the well-known fact that $\mathbb{F}_q^{ns} \cong M_{n,s}(\mathbb{F}_q)$, and then a vector x in $\mathbb{F}^m$ can be write as

$$\mathbf{x} = \begin{bmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,s} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,s} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n,1} & x_{n,2} & \cdots & x_{n,s} \end{bmatrix}.$$

Definition 6.36. *Let $P = ([n], \preceq)$ be a poset and $x, y \in \mathbb{F}_q^n$. The P-distance between x and y is given by $d_p(x, y) = \omega_P(x - y)$.*

Indeed, the P-distance is a metric on $\mathbb{F}_q^n$, which is called P-metric.

Definition 6.37. *Let $P = ([n], \preceq)$ be a poset and d_P the related P-metric. A poset code is a linear subspace C of the metric space $\left(\mathbb{F}_q^n, d_p\right)$.*

6.3.2 Packing radius of NRT codes

It is well-known that if C is a $[n, k]$ linear code and d is the minimum Hamming distance of C, then the packing radius of C is

$$\tau = \left\lfloor \frac{n-k}{2} \right\rfloor. \tag{6.25}$$

When considering the family of poset metrics, Eq. (6.25) does not hold always, but we have the following inequality.

$$\left\lfloor \frac{d_P - 1}{2} \right\rfloor \leqslant \tau_{d_P} \leqslant d_P - 1. \tag{6.26}$$

where d_P denotes the minimum P-distance of C.

It is known [20] that the upper bound is attained when the poset is a n-chain, while the lower bound holds for the Hamming metric. In the general case, the packing radius is not a

function of the minimum distance and finding the packing radius of a poset code is (in general) a NP-hard problem [17].

Let us consider a code C in $(\mathbb{F}_q^s)^n$ as a n-chain poset code, that is, C is a subspace of the metric space $(\mathbb{F}_q^s, d_{P_C})$, where P_C is the poset of Example 6.27. In this case each codeword

$$\mathbf{c} = \begin{bmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,n} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{s,1} & c_{s,2} & \cdots & c_{s,n} \end{bmatrix} \in C$$

can be see as a vector $c = (c_1, \ldots, c_n) \in (\mathbb{F}_q^s)^n$ and

$$\omega_{P_C}(\mathbf{c}) = \omega_{P_C}(c) = \max\{i : c_i \neq 0\}.$$

In particular, one error amounts to an incorrect collumn $c_i = (c_{i1}, \ldots, c_{is})$. Accordingly to correcting up to t errors means correcting any combination of errors $e = (e_1, \ldots, e_n) \in (\mathbb{F}_q^s)^n$ of P_C-weight, $\omega_{P_C}(e) = \max\{i : e_i \neq 0\} \leqslant t$, where the received word is $y = c + e = (c_1 + e_1, \ldots, c_n + e_n) \in (\mathbb{F}_q^s)^n$.

It is known [20] that in this specific case the upper bound in (6.26) is attained and then we know the packing radius of C in this case, named

$$\tau_{d_{P_C}} = d_{P_C} - 1 \tag{6.27}$$

We can apply Singleton bound, $d_{P_C} \leqslant n - k + 1$, on the minimum distance d_{P_C} of C to obtain the following inequality

$$r_1(C) = \tau_{d_{P_C}} = d_{P_C} - 1 \leqslant n - k.$$

So, by definition we also obtain that

$$r_1(\mathcal{C}) = n - k$$

with equality if C is an MDS code. Finally,

$$r_1(sn, k) = n - k.$$

We would like to obtain an upper bound on the α-decoding radius of an $[sn, k]$ linear code endowed with the d_{P_C} metric. Firstly, let us remember the definition of the projection of an $[sn, k]$ NRT code $C \in (\mathbb{F}^s)^n$ onto $(\mathbb{F}^{s'})^{n'}$.

Definition 6.38. *Let C be an $[sn,k]$ NRT code in $(\mathbb{F}_q^s)^n$. The projection π of C on $(\mathbb{F}_q^{s'})^{n'}$ with $s' \leqslant s$ and $n' \leqslant n$ is given by*

$$\pi\left(\begin{bmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,n} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{s,1} & c_{s,2} & \cdots & c_{s,n} \end{bmatrix}\right) = \begin{bmatrix} c_{1,n-n'+1} & c_{1,n-n'+2} & \cdots & c_{1,n} \\ c_{2,n-n'+1} & c_{2,n-n'+2} & \cdots & c_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{s',n-n'+1} & c_{s',n-n'+2} & \cdots & c_{s',n} \end{bmatrix}.$$

The projection of C onto $(\mathbb{F}_q^{s'})^{n'}$ is $[s'n', k']$ NRT code, which is called profection code of C and is denoteded by $\pi(C)$. The projection code has following propriety.

Lemma 6.39. *([66]) Let C be an MDS code in $(\mathbb{F}^l)^n$ with q^k elements. Suppose that $s' \leqslant s$, $n' \leqslant n$, and $s'n' \geqslant k$. Then the projection of C onto $(\mathbb{F}^{s'})^{n'}$ is an MDS code.*

As we are considering codes endowed with the d_{P_C} metric, we consider the projection code $\pi(C)$ of C on $(\mathbb{F}_q^s)^{n'}$. We have the following lower bound on $r_\alpha\,(sn,k)$.

Lemma 6.40. *For any $k \leqslant n$ and $k/n \leqslant \alpha \leqslant 1$.*

$$r_\alpha(sn,k) \geqslant \alpha n - k \tag{6.28}$$

Proof. To see this, let C be an maximum distance separable $[sn,k]$ NRT code in $(\mathbb{F}_q^s)^n$ and $C' = \pi(C)$ its projection onto $(\mathbb{F}_q^s)^{\alpha n}$. By assumption, $\alpha n \geqslant k$ and C is an MDS code then, Lemma 6.39 implies that C' is an $[\alpha sn, k]$ MDS-code. So (6.28) follows by definition. □

Let us prove the following upper bound on $r_\alpha(sn,k)$.

Theorem 6.41.

$$r_\alpha(sn,k) \leqslant n - \frac{k}{\alpha}.$$

Proof. By definition, we need to show that if an $[sn,k]$ NRT code C in $(\mathbb{F}_q^s)^n$ can correct up to t errors by downloading αsn symbols of $\mathbb{F}_q$, then $t \leqslant n - k/\alpha$. By assumption for any error vector $e = (e_1, \ldots, e_n)$ in $(\mathbb{F}^s)^n$ of weight $\omega_{P_C}(e) = \max\{i : e_i \neq 0\} \leqslant t$, there exist $n+1$ functions $f_i : \mathbb{F}_q^s \longrightarrow \mathbb{F}_q^{\alpha_i s}$, $i = 1, \ldots, n$ and $g : \mathbb{F}_q^{(\sum_{i=1}^n \alpha_i)s} \longrightarrow (\mathbb{F}_q^s)^n$ that satisfy Definition 6.1.

We claim that $\sum_{i\in\mathcal{I}} \alpha_i \geqslant k$ for any set $\mathcal{I} \subseteq \{1, \ldots, n\}$ with cardinality $|\mathcal{I}| = n - t$. Assume toward a contradiction that there exists a set $\mathcal{I}_0 \subseteq \{1, \ldots, n\}$, $|\mathcal{I}_0| = n - t$ such that $\sum_{i\in\mathcal{I}_0} \alpha_i < k$. Let us assume that $\mathcal{I}_0 = \{i_1, \ldots, i_{n-t}\}$ and let $\mathcal{J} = \{1, \ldots, n\} \setminus \mathcal{I}_0$. Since the dimension of C is k, there are a total of $|\mathbb{F}_q|^{sk}$ codewords. At the same time, the vector

$(f_{i_r}(c_{i_r}), r = 1, \ldots, n-t)$ takes at most $\prod_{i_r \in \mathcal{I}_0} |\mathbb{F}_q|^{\alpha_{i_r} s} = |\mathbb{F}_q|^{(\sum_{i_r \in \mathcal{I}_0} \alpha_{i_r}) s}$ different values, so there exist two distinct codewords $\hat{c}$ and $\tilde{c}$ for which these vectors coincide:

$$\big(f_{i_1}(\widetilde{c_{i_1}}), \ldots, f_{i_{n-t}}(\widetilde{c_{i_{n-t}}})\big) = \big(f_{i_1}(\widehat{c_{i_1}}), \ldots, f_{i_{n-t}}(\widehat{c_{i_{n-t}}})\big) \tag{6.29}$$

Define the error vectors $\hat{e}$ and $\tilde{e}$ by setting

$$\tilde{e} = (\widetilde{c_{i_1}}, \ldots, \widetilde{c_{i_t}}, 0, \ldots, 0) \text{ and } \hat{e} = (\widehat{c_{i_1}}, \ldots, \widehat{c_{i_t}}, 0, \ldots, 0), \text{where } i_r \in \mathcal{J}, r = 1, \ldots, t. \tag{6.30}$$

Clearly, the weight of both $\hat{e}$ and $\tilde{e}$ is at most t. By Definition 6.1, we have

$$g(f_1(\hat{c_1}+\hat{e_1}), \ldots, f_n(\hat{c_n}+\hat{e_n})) = (\hat{c_1}, \ldots, \hat{c_n}) \text{ and } g(f_1(\tilde{c_1}+\tilde{e_1}), \ldots, f_n(\tilde{c_n}+\tilde{e_n})) = (\tilde{c_1}, \ldots, \tilde{c_n}) \tag{6.31}$$

According to (6.29) and (6.30), $f_{i_r}(\widehat{c_{i_r}}) = f_{i_r}(\widetilde{c_{i_r}})$ if $i_r \in \mathcal{I}_0$, so f_{i_r}, $\widehat{c_{i_r}}$ and $\widetilde{c_{i_r}}$ are such that $f_{i_r}(\widehat{c_{i_r}} + \widehat{e_{i_r}}) = f_{i_r}(\widehat{c_{i_r}} + \widetilde{c_{i_r}}) = f_{i_r}(\widetilde{c_{i_r}} + \widetilde{e_{i_r}})$. As a result, $\hat{c} = \tilde{c}$, in contradiction to our assumption. We conclude that $\sum_{i \in \mathcal{I}} \alpha_i \geqslant k$ for any set $\mathcal{I} \subseteq \{1, \ldots, n\}$ of size $|\mathcal{I}| = n - t$.

Let $\mathcal{I}$ be an $(n-t)$-subset of $\{1, \ldots, n\}$ such that the quantity $\sum_{i \in \mathcal{I}} \alpha_i$ is the smallest among all $(n-t)$-subsets. By the above argument the averange proportion of information transmitted from a coordinate in the set $\mathcal{I}$ is at least $k/(n-t)$. On the other hand, by definition, the averange proportion transmitted from all the coordinates is at most α, which is at least $k/(n-t)$ because of the property the set $\mathcal{I}$ satisfies. Hence we get $k/(n-t) \leqslant \alpha$, and this concludes the proof. □

6.4 Open problems

a) Can we perform fractional decoding beyond the α decoding radius to other kinds of codes, e.g. interleaved Goppa codes, Reed-Muller codes, etc. ?

b) Can we find a family of NRT codes C in $M_{1,n}(\mathbb{F}_q)$ whose α-decoding radius is $n - \frac{k}{n}$?

c) What can we say on the fractional decoding of poset codes in general?

Bibliography

[1] A. Barg and M. Firer, *Translation association schemes, poset metric, and the shape enumerator of codes*, IEEE International Symposium on Information Theory Proceedings, pp. 101-105, 2012.

[2] A. Barg and W. Park, *On linear ordered codes*, Moscow Mathematical Journal, vol. 15, pp. 679-702, 2015.

[3] A. Barg and P. Purkayastha, *Bounds on ordered codes and orthogonal arrays*, Moscow Mathematical Journal, vol. 9, pp. 211-243, 2009.

[4] R. E. Blahut, *Theory and practice of error control codes*, Addison-Wesley Publishing Company, Massachusetts, 1983.

[5] D. Bleichenbacher, A. Kiayias, and M. Yung, *Decoding of Interleaved Reed Solomon Codes over a Noisy Data*, Springer Lecture Notes in Computer Science, Vol. 2719, pp. 97-108, 2003.

[6] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, Journal of Symbolic Computation, vol. 24, pp. 235-265, 1997.

[7] R. A. Brualdi, J. S. Graves, and K. M. Lawrence, *Codes with a poset metric*, Discrete Mathematics, vol.147, pp. 57-72, 1995.

[8] W. Bruns and J. Herzog, *Cohen-Macaulay rings*, Cambridge University Press, Cambridge, 1993.

[9] V. Cadambe and A. Mazumdar, *Alphabet-size dependent bounds for exact repair in distributed storage*. In Proc. 2015 IEEE Information Theory workshop-Fall (ITW 2015), Oct. 11-15,2015, Jeju, South Korea, pp. 1-3, 2015.

[10] V. R. Cadambe, S. A.Jafar, H. Maleki, K. Ramchandran, and S. Changho, *Asymptotic interference alignment for optimal repair of MDS codes in distributed storage*, IEEE Transactions on Information Theory, vol. 59, pp. 2974-2987, 2013.

[11] R. Chapman, *Constructions of the Golay codes: A Survey*, 1997.

[12] H. Derksen and G. Kemper, *Computational invariant theory*, Invariant Theory and Algebraic Transformation Groups, I, Springer-Verlag, 2002.

[13] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, *Network coding for distributed storage systems*, IEEE Transactions on Information Theory, vol. 56, pp. 4539-4551, 2010.

[14] S. T. Dougherty and M. M. Skriganov, *Maximum distance separable codes in the ρ metric over arbitrary alphabets*. Journal of Algebraic Combinatorics, vol. 16, 71-81, 2002.

[15] S. T. Dougherty and M. M. Skriganov, *MacWilliams duality and the Rosenbloom-Tsfasman metric*, Moscow Mathematical Journal, vol. 2, pp. 81-97, 2002.

[16] S. Dougherty and K. Shiromoto, *Maximum Distance Codes in $Mat_{N,S}(Z(K))$ with a Non-Hamming Metric and Uniform Distributions*, Designs Codes Cryptography, vol. 33, pp. 45-61, 2004.

[17] R. G. L. D'Oliveira and M. Firer, *The packing radius of a code and partitioning problems: The case for poset metrics on finite vector spaces*, Discrete Mathematics, vol. 338, pp. 2143-2167, 2015.

[18] R. Ehrenborg and G. C. Rota, *Apolarity and canonical forms for homogeneous polynomials*, European Journal of Combinatorics, vol.12, pp. 157-181, 1993.

[19] M. Firer, M.M.S. Alves, J.A. Pinheiro, and L. Panek, *Poset Codes: Partial Orders, Metrics, and Coding Theory*, Springer, 2018.

[20] M. Firer, L. Panek, and M.M.S. Alves, *Classification of Niederreiter-Rosenbloom-Tsfasman block codes*, IEEE Transactions on Information Theory, vol. 56, pp. 5207-5216, 2010.

[21] G. D. Forney, *On decoding BCH codes*, IEEE Transactions on Information Theory, vol. 11, pp. 549-557, 1965.

[22] E. M. Gabidulin, A.V. Paramonov, and O.V. Tretjakov, *Rank errors and rank erasures correction*. Proceedings of the 4th International Colloquium on Coding Theory, Dilijan, Armenia, pp. 11-19, Yerevan, 1992.

[23] A. M. Gleason, *Weight polynomials of self-dual codes and the MacWilliams identities*, in: Actes, Proceedings of the Congrés International de Mathématiques, Vol. 3, pp. 211-215, 1970.

[24] D. R. Grayson and M.E. Stillman, *Macaulay2, a software system for research in algebraic geometry*, available at www.math.uiuc.edu/Macaulay2/.

[25] K. Gregor, *Calculating invariant rings of finite groups over arbitrary fields*, Journal of Symbolic Computation, pp. 351-366, 1996.

[26] V. Guruswami and A. Rudra, *Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy*, IEEE Transactions on Information Theory, vol. 54, pp. 135-150, 2008.

[27] A. Hefez and M. Villela, *Códigos corretores de erros*. Série de computação e Matemática. Instituto de Matemática Pura e Aplicada, 2008.

[28] W. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.

[29] M. Hochster and J. A. Eagon, *Cohen-Macaulay rings, invariant theory, and generic perfection of determinantal loci*, American Journal of Mathematics, vol. 93, pp. 1020-1058, 1971.

[30] N. Jacobson, *Lectures in abstract algebra*, Van Nostrand Princeton, vol. 3, NJ, 1964.

[31] H. K. Kim and D. Y. Oh, *A classification of posets admitting the MacWilliams identity*, IEEE Transactions on Information Theory, vol. 51, pp. 1424-1431, 2005.

[32] H. K. Kim and J. Y. Hyun, *Maximum distance separable poset codes*, Designs, Codes and Cryptography, vol.48, pp. 247-261, 2008.

[33] S. Lane and G. Birkhoff, *Algebra*, Chelsea Publishing Company, New York, 1999.

[34] K. Lee, *The automorphism group of a linear space with the Rosenbloom-Tsfasman metric*, European Journal of Combinatories, vol. 24, pp. 607-6017, 2003.

[35] S. Lefschetz, *Algebraic geometry*, Princeton University Press, Princeton, N. J., 1953, 2nd edn., 1964.

[36] R. Lidl and H. Niederreiter, *Finite fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1997.

[37] Hua, Loo-Keng, *A theorem on matrices over a sfield and its applications*, Chinese Mathematical Society, vol. 1, pp. 109-163, 1951.

[38] F. J. MacWilliams, *A theorem on the distribution of weights in a systematic code*, Bell System Technical Journal, vol. 42, pp. 79-84, 1963.

[39] F. J. MacWilliams, C. L. Mallows, and N. J. A Sloane *Generalizations of Gleason's theorem on weight enumerators of self-dual codes*, IEEE Transactions on Information Theory, vol.18, pp. 794-805, 1972.

[40] C. L. Mallows and N. J. A Sloane, *Generalizaations of Gleason's theorem on weight enumerators of self-dual codes*, PGIT vol. 19, pp. 794-805, 1972.

[41] W. J. Martin and D. R. Stinson, *Association schemes for ordered orthogonal arrays and (T,M,S)-nets*, Canadian Journal of Mathematics, vol. 51, pp. 326-346, 1999.

[42] V. Marka, R. S. Selvaraj, and I. Gnanasudha *Self-dual codes in the Rosenbloom-Tsfasman metric*, Mathematical Communications, vol. 22, pp. 75-87, 2017.

[43] O. Mehmet and S. Irfan, *On the structure and decoding of linear Codes with respect to the Rosenbloom-Tsfasman metric*, Selcuk Journal of Applied Mathematics, vol. 5, pp. 25-31, 2004.

[44] O. Mehmet and S. Irfan, *Linear codes over* $\mathbb{F}_q[u]/(u^s)$ *with respect to the Rosenbloom-Tsfasman metric*, Designs, Codes and Criptography, vol. 38, pp. 17-29, 2006.

[45] G. A. Miller, H. F. Blichfeldt, and L. E. Dickson, *Theory and applications of finite groups*, Dover, NY, 1961.

[46] T. Molien, *Ueber die invarianten der linear Substitutionsgruppe*. Sitzungsber König. Akad. Wiss., pp. 1152-1156, 1897.

[47] G. Nebe, E. M. Rains, and N. J. A. Sloane, *The invariants of the Clifford groups*, Designs, Codes and Cryptography, vol. 24, pp. 99-121, 2001.

[48] G. Nebe, E. Rains, and N.J.A. Sloane, *Self-Dual Codes and Invariant Theory*, Springer, 2006.

[49] H. Niederreiter, *A combinatorial problem for vectors spaces over finite fields*, Discrete Mathematics, vol. 96, pp. 221-228, 1991.

[50] H. Niederreiter, *Point sets and sequences with small discrepancy*, Monatshefte für Mathematik, vol. 104 (1987), pp. 273-337, 1987.

[51] E. Noether, *Der Endlichkeilsatz der invarianten endlicher Gruppen*, Mathematische Annalen, vol. 77, pp. 89-92, 1916.

[52] W. Park and A. Barg, *Linear ordered codes, shape enumarators and parallel channels*, Forty-Eighth Annual Allerton Conference, pp. 361-368, 2010.

[53] W. W. Peterson, *Encoding and error-correction procedures for the Bose-Chaudhuri codes*, IEEE Transactions on Information Theory, vol. 6, pp. 459-470, 1960.

[54] V. Pless, *A Classification of self-orthogonal codes over* $GF(2)$, Discrete Mathematics, vol. 3, pp. 209-246, 1972.

[55] E. M. Rains and N. J. A. Sloane, *Self-dual codes*. In: Handbook of Coding Theory, North Holland, 1998.

[56] S. J. Rallis, *New and old results in invariant theory with applications to arithmetic groups in symmetric spaces*. W. M. Boothby and G. L. Weiss, Eds., Pure appl. Math, pp 443-458, Dekker, NY, 1972.

[57] I.S. Reed and G. Solomon, *Polynomial codes over certain finite fields*, Society for Industrial and Applied Mathematics, Vol. 8, 1960.

[58] J. J. Rotman, *Advanced modern algebra*, Prentice-Hall, 2002.

[59] J. P. Serre, *Linear representations of finite groups*, Springer-Verlag, NY, 1997.

[60] G. Schmidt, V. R. Sidorenko, and M. Bossert, *Collaborative decoding of Interleaved Reed-Solomon codes and concatenated code designs*, IEEE Transactions on Information Theory, vol. 55, no. 7, pp. 2991-3012, 2009.

[61] G. Schmidt and V. R. Sidorenko, *Linear shift-register synthesis for multiple sequences of varying length*, Preprint, avaliable online at ArXiv, arXiv:cs.IT/0605044, 2006.

[62] G. Schmidt, V. R. Sidorenko, and M. Bossert, *Syndrome decoding of Reed-Solomon codes beyond half the minimum distance based on shift-register synthesis*, IEEE Transactions on Information Theory, vol. 56, no. 10, pp. 5245-5252, 2010.

[63] G. Schmidt, V. Sidorenko, and M. Bossert, *Enhancing the correcting radius of Interleaved Reed-Solomon decoding using syndrome extension techniques*, IEEE International Symposium on Information Theory (ISIT), pp. 1341-1345, 2007.

[64] C. E. Shannon, *A mathematical theory of communication*, Bell System Technical Journal, vol. 27, pp. 379-423, 1948.

[65] M. M. Silva Alves, *A standard form for generator matrices with respect to the Niederreiter-Rosenbloom-Tsfasman metric*, Proc. 2011 IEEE Information Theory Workshop, Oct. 16-20, 2011, Paraty, Brazil, pp.486-489.

[66] M. M. Skriganov, *Coding theory and uniform distributions*, St. Petersburg Mathematical Journal, vol. 13, pp. 310-337, 2002.

[67] M. M. Skriganov, *Coding theory and uniform distributions*, Algebra i Analiz, vol. 13, pp. 191-239, 2001.

[68] N. J. A Sloane, *On the classification and enumeration of self-dual codes*, Journal of Combinatorial theory, Series A, vol. 18, pp. 313-335, 1975.

[69] L. Smith, *Polynomial invariants of finite groups*, Peters, Wellesley, MA, 1995.

[70] R. Stanley, *Enumerative combinatorics*, Cambridge University Press, Cambridge, 2002.

[71] R. P. Stanley, *Hilbert function of graded algebras*, Advances in Mathematics, vol. 28, pp. 57-83, 1978.

[72] B. Sturmfels, *Algorithms in invariant Theory*, Springer-Verlag, NY, 1993.

[73] I. Tamo, M. Ye, and A. Barg, *Fractional decoding: Error correction from partial information*, arXiv preprint arXiv:1701.06969, 2017.

[74] H. Thomas, *Computing the invariant ring of a finite group*, Journal of Software for Algebra and Geometry, pp. 15-19, 2013.

[75] M. Y. Tsfasman and M. A. Rosenbloom, *Codes for the m-metric*. Problemy Peredachi Informatsii, vol. 33, pp. 55-63, 1997.

[76] H. Weyl, *The classical groups*. Princeton University Press, Princeton, NJ, 1946.

[77] A. W. Zeh, A. Zeh, and M. Bossert, *Decoding Interleaved Reed-Solomon codes beyond their Joint error-correcting capability*, Designs, Codes and Cryptography, vol. 71, pp. 261-281, 2014.