Decoding and constructions of codes in rank and Hamming metric

Wrya Karim Kadir

Thesis for the degree of Philosophiae Doctor (PhD)
University of Bergen, Norway
2022

UNIVERSITY OF BERGEN

Decoding and constructions of codes in rank and Hamming metric

Wrya Karim Kadir

Thesis for the degree of Philosophiae Doctor (PhD)
at the University of Bergen

Date of defense: 27.05.2022

Year: 2022

Title: Decoding and constructions of codes in rank and Hamming metric

Name: Wrya Karim Kadir

Print: Skipnes Kommunikasjon / University of Bergen

“My Lord! Increase me in knowledge.”

Taha (20) - 114

Acknowledgements

As I start writing the Acknowledgment, I am trying to name all the people who helped, encouraged, and supported me during my Ph.D. studies and it seems to me that they are countless. In fact, I am not even sure where to start from. So as a tradition I start thanking my friend and supervisor Dr. Chunlei Li who in the first place gave me the opportunity to perform my Ph.D. under his supervision and in the second place hold my hand and walked me through this challenging journey. He always had a smile on his face even after listening to my stupid ideas and we always had meetings with very friendly atmosphere. Thank you Chunlei for your support and you were the best Ph.D. supervisor that someone could hope for.

I am also very thankful to my co-supervisor Ferdinando Zullo with whom I enjoyed valuable discussions and fruitful collaborations. He was the one who always been available for me to discuss my brainstorm ideas no matter when and where he was. His favorite emoji and status "Sempre Avanti!" always gave me courage and hope. I also like to thank my other co-authors Alessio, Yibo and Yongbo. My talented master student Ola Andreas Storstein, thanks for being part of my Ph.D. journey.

Doing Ph.D. without a friendly working environment is almost impossible. I was lucky to be part of the Selmer center and I really enjoyed our lunch discussions that were able to go from politics to Italian Pizza and from religion to nowhere. I appreciate the support that I received from all my friends in Selmer center: Irene, Navid, Isaac, Andrea, Alessandro, Igor, Dan, Qian, Matthew, Marco, Nikolay, Diana, Ermes, Sachin, Stein and George.

I would like to say a special thank you to Professor Lilya Budaghyan for her brilliant leadership of Selmer center. Professor Tor Helleseth is the one who I will appreciate his encouragement for ever. He attended my first Ph.D. seminar and his positive comments made me believe that I am able to accomplish a Ph.D.

Aside from research, I had the chance of having a lot of very good friends at Informatics Department. I would like to thank the members of the group “iii” with whom I had afternoon tea and discussed about the non-Ph.D. life. Namely, I would like to thank Ahmad and Navid , who were my private mentors, and also Farhad, Fourough, Nooshin, Ramin, Reza and Erfan.

I am also very thankful to the support received from my friends for life, Hilal, Chwas, Hardi, Hawsar and Mohammed.

Last but not least, I would like to say thank you to my family. My dad, my late mom and my siblings who supported, encouraged and motivated me through my entire life. Also I will never forget the support of my parents in law at the beginning of my Ph.D. and later. My best friend and my kind wife Tarza and my beautiful daughter Mina, this dissertation is dedicated to you. I would not be able to survive this without your full support and what I owe to you is immeasurable.

Wrya K. Kadir

Bergen, 2022

Abstract

As coding theory plays an important role in data transmission, decoding algorithms for new families of error correction codes are of great interest. This dissertation is dedicated to the decoding algorithms for new families of maximum rank distance (MRD) codes including additive generalized twisted Gabidulin (AGTG) codes and Trombetti-Zhou (TZ) codes, decoding algorithm for Gabidulin codes beyond half the minimum distance and also encoding and decoding algorithms for some new optimal rank metric codes with restrictions.

We propose an interpolation-based decoding algorithm to decode AGTG codes where the decoding problem is reduced to the problem of solving a projective polynomial equation of the form $q(x) = x^{q^u+1} + bx + a = 0$ for $a, b \in \mathbb{F}_{q^m}$. We investigate the zeros of $q(x)$ when $gcd(u, m) = 1$ and proposed a deterministic algorithm to solve a linearized polynomial equation which has a close connection to the zeros of $q(x)$.

An efficient polynomial-time decoding algorithm is proposed for TZ codes. The interpolation-based decoding approach transforms the decoding problem of TZ codes to the problem of solving a quadratic polynomial equation. Two new communication models are defined and using our models we manage to decode Gabidulin codes beyond half the minimum distance by one unit. Our models also allow us to improve the complexity for decoding GTG and AGTG codes.

Besides working on MRD codes, we also work on restricted optimal rank metric codes including symmetric, alternating and Hermitian rank metric codes. Both encoding and decoding algorithms for these optimal families are proposed. In all the decoding algorithms presented in this thesis, the properties of Dickson matrix and the BM algorithm play crucial roles.

We also touch two problems in Hamming metric. For the first problem, some cryptographic properties of Welch permutation polynomial are investigated and we use these properties to determine the weight distribution of a binary linear codes with few weights. For the second one, we introduce two new subfamilies for maximum weight spectrum codes with respect to their weight distribution and then we investigate their properties.

List of Articles

1. Wrya K. Kadir, and Chunlei Li. *"On decoding additive generalized twisted Gabidulin codes."* Cryptography and Communications (2020): 987-1009.

2. Wrya K. Kadir, Chunlei Li, and Ferdinando Zullo, *"On interpolation-based decoding of a class of maximum rank distance codes."* 2021 IEEE International Symposium on Information Theory (ISIT), (2021): 31-36.

3. Wrya K. Kadir *"New Communication Models and Decoding of Maximum Rank Distance Codes. "* 2021 XVII International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY), (2021): 125-130.

4. Wrya K. Kadir, Chunlei Li, and Ferdinando Zullo. *"Encoding and decoding of several optimal rank metric codes."* Cryptography and Communications (2022): 1-20.

5. Yibo Wang , Wrya K. Kadir, Chunlei Li, and Yongbo Xia. *"On cryptographic properties of the Welch permutation and a related conjecture."* International Conference on Sequences and Their Applications (SETA) Russia, Saint-Petersburg, 2020.

6. Alessio Meneghetti, and Wrya K. Kadir. *"Characterisation of the parameters of maximum weight spectrum codes according to their spread."* International Conference on Sequences and Their Applications (SETA) Russia, Saint-Petersburg, 2020.

Contents

Chapter 1

Preliminaries

This chapter is a brief introduction about the tools needed in this thesis. First, we will give brief results in the theory of finite fields and then we will bring the concept of block codes in both Hamming and rank metrics. We also recall new families of rank metric codes, their properties and known decoding algorithms.

1.1 Notation

Let p be a prime integer. We denote a *prime field* of order p by $\mathbb{F}_p = \{0,1,\ldots,p-1\}$. Let q be a power of p ($q = p^r$), then the *finite field* of order q is denoted by $\mathbb{F}_q$ which contains q elements. Here, p is called the *characteristic* of the finite field $\mathbb{F}_q$. All the non-zero elements $\{a_1,\ldots,a_{q-1}\}$ of finite field $\mathbb{F}_q$ can be generated by a *primitive element* $a \in \mathbb{F}_q$. An element $a \in \mathbb{F}_q$ has order t, if t is the smallest positive integer such that $a^t = 1$ and α is a primitive element in $\mathbb{F}_q$ if it has order $q-1$, i.e., $\alpha^{q-1} = 1$. The number of primitive elements in $\mathbb{F}_q$ coincides with the number of integers co-prime to $q-1$. An extension field of $\mathbb{F}_q$ of degree m is denoted by $\mathbb{F}_{q^m}$, which can be constructed by an irreducible polynomial $q(x)$ of degree m over $\mathbb{F}_q$. Irreducible polynomials of degree m exist for any m [30]. We call $\mathbb{F}_q$ a *sub-field* of $\mathbb{F}_{q^m}$. It is well-known that an extension field $\mathbb{F}_{q^m}$ can be seen as an $\mathbb{F}_q$-vector space of dimension m. So every element $a \in \mathbb{F}_{q^m}$ can be represented as a linear combination of linearly independent elements $\alpha_i \in \mathbb{F}_{q^m}$ where $i = 0,\ldots,m-1$. Linearly independent elements $\alpha_0,\ldots,\alpha_{m-1}$ form a basis for the extension field $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. We use the following notations and properties for finite fields in this thesis:

i. we denote $q^i = [i]$ and $q^{2i} = [\![i]\!]$ where $i \in \mathbb{Z}$,

ii. for $a \in \mathbb{F}_{q^m}$ and $i \in \mathbb{Z}$, $a^{[m]} = a$ and $a^{[i]} = a^{[i \mod m]}$,

iii. for $a \in \mathbb{F}_q$ and $i \in \mathbb{Z}$, $a^{[i]} = a$,

iv. $(a+b)^{p^i} = a^{p^i} + b^{p^i}$, where $a,b \in \mathbb{F}_{q^m}$, p is the characteristic of $\mathbb{F}_{q^m}$ and $i \in \mathbb{Z}$,

1.1.1 Trace, Norm and Bases

Definition 1 (Conjugates). *Let $\mathbb{F}_{q^m}$ be an extension field of $\mathbb{F}_q$ of degree m. The conjugates of $a \in \mathbb{F}_{q^m}$ are the set $a, a^q, \ldots, a^{q^{m-1}}$.*

Definition 2 (Trace). *Let $\mathbb{F}_{q^m}$ be an extension field of $\mathbb{F}_q$. The trace of $a \in \mathbb{F}_{q^m}$ is the linear map*

$$\mathrm{Tr}_{q^m/q}(a) = a + a^q + a^{q^2} + \cdots + a^{q^{m-1}},$$

in other words, the trace of a field element is the sum of its conjugates.

Definition 3 (Norm). *The norm of $a \in \mathbb{F}_{q^m}$ is the product of its conjugates*

$$\mathrm{Norm}_{q^m/q}(a) = a \cdot a^q \cdot a^{q^2} \cdots a^{q^{m-1}}.$$

The trace and norm are defined with respect to the sub-field on which the extension field is built.

Definition 4 (Basis). *An extension field $\mathbb{F}_{q^m}$ of degree m can be seen as an m-dimensional vector space over $\mathbb{F}_q$ and there are linearly independent basis elements $\{\alpha_0, \ldots, \alpha_{m-1}\}$ such that each element $a \in \mathbb{F}_{q^m}$ can be written as*

$$a = \sum_{i=0}^{m-1} a_i \alpha_i,$$

where $a_i \in \mathbb{F}_q$.

If the order of a basis is important, we call it an *ordered basis*. We use different ordered bases for different purposes throughout this thesis.

Definition 5 (Polynomial Basis). *Let α be a primitive element of $\mathbb{F}_{q^m}$, then the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ forms a basis for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and it is called a polynomial basis.*

Definition 6 (Normal Basis). *Consider some $\alpha \in \mathbb{F}_{q^m}$. If the set of conjugates of α, i.e., $N = \{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}\}$, forms a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ then α is called a normal element and N is called a normal basis.*

Definition 7 (Dual Bases). *Consider two bases $A = \{\alpha_i\}_{i=0}^{m-1}$ and $B = \{\beta_i\}_{i=0}^{m-1}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then A is called the dual of B if $\mathrm{Tr}_{q^m/q}(\alpha_i \cdot \beta_i) = \delta_{ij}$, where $\delta_{ij} = \begin{cases} 1 & \text{for } i = j, \\ 0 & \text{for } i \neq j \end{cases}$ and it is known as the Kronecker delta function. A basis is called self-dual if it is the dual of itself.*

Definition 8 (Vector and Matrix Representation). *Let $\alpha = (\alpha_0, \ldots, \alpha_{m-1})$ be an ordered basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Any vector $v = (v_0, \ldots, v_{n-1}) \in \mathbb{F}_{q^m}^n$ can be represented with respect to a basis α over sub-field $\mathbb{F}_q$ using the bijective map $B: \mathbb{F}_{q^m}^n \to \mathbb{F}_q^{m \times n}$ which is defined as*

$$v = (v_0, \ldots, v_{n-1}) \longmapsto V = B(v) = \begin{pmatrix} V_{11} & V_{12} & \cdots & V_{1n} \\ V_{21} & V_{22} & \cdots & V_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ V_{m1} & V_{m2} & \cdots & V_{mn} \end{pmatrix}_{m \times n}, \tag{1.1}$$

where $v_j = \sum_{i=0}^{m-1} V_{ij}\alpha_i$ *for* $j = 0, \ldots, n-1$.

Definition 9 (Moore Matrix)**.** *The matrix* $\mathcal{M}$ *of the form*

$$\mathcal{M} = \left(\alpha_i^{q^j}\right)_{m\times m} = \begin{pmatrix} \alpha_0 & \alpha_0^q & \cdots & \alpha_0^{q^{m-1}} \\ \alpha_1 & \alpha_1^q & \cdots & \alpha_1^{q^{m-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{m-1} & \alpha_{m-1}^q & \ldots & \alpha_{m-1}^{q^{m-1}} \end{pmatrix}, \tag{1.2}$$

is called the Moore matrix associated to the set $\alpha = \{\alpha_0, \ldots, \alpha_{m-1}\}$ *where* $\alpha_i \in \mathbb{F}_{q^m}$.

The Moore matrix associated to the set α is non-singular if $\alpha_0, \ldots, \alpha_{m-1}$ are $\mathbb{F}_q$-linearly independent [30]. So the Moore matrix associated to an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$ is always non-singular.

Example 1. *Let* $\mathbb{F}_{2^2} = \mathbb{F}_4$ *be the finite field of* 4 *elements. Let* θ *be a primitive element of* $\mathbb{F}_4$ *namely* $\mathbb{F}_4 = \{0, \theta, \theta^2, \theta^3 = 1\}$. *So the polynomial basis of* $\mathbb{F}_4$ *over* $\mathbb{F}_2$ *is* $\{\theta, \theta^3 = 1\}$. *We can write the field elements in vector form with respect to the basis elements as* $v_0 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $v_\theta = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $v_{\theta^2} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $v_{\theta^3} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ *and see the field* $\mathbb{F}_4$ *as a* 2*-dimensional vector space over* $\mathbb{F}_2$. *Moreover, it is easy to verify that* $\{\theta, \theta^2\}$ *forms a self-dual normal basis for* $\mathbb{F}_4$ *over* $\mathbb{F}_2$.

1.1.2 Metric Spaces

Let S be a non-empty set. A metric on S, or a distance function d, associates each pair of the elements in S to a real number and for $x, y, z \in S$ satisfies the following:

i. $d(x,y) \geq 0$ and $d(x,y) = 0 \iff x = y$,

ii. $d(x,y) = d(y,x)$,

iii. $d(x,y) \leq d(x,z) + d(z,y)$.

The ordered pair (S,d) is called a metric space. In this thesis we consider codes in two different metrics *Hamming metric* and *Rank metric*.

Definition 10 (Hamming Metric)**.** *Let* $x = (x_1, \ldots, x_n)$ *and* $y = (y_1, \ldots, y_n)$ *be two strings in a set* S^n. *The Hamming distance* d_H *between* x *and* y *is defined as*

$$d_H(x,y) = |\{i \in [1,n] \mid x_i \neq y_i\}|.$$

The Hamming weight $w_H(x)$ *of a string* $x \in S^n$ *is the number of its non-zero components.*

Definition 11 (Rank Metric)**.** *Let* $x \in \mathbb{F}_{q^m}^n$. *The rank (weight) of* x *is the number of linearly independent components of* x *over* $\mathbb{F}_q$ *which is equivalent to the rank of its corresponding matrix* X *in Definition 8. The rank distance between* $x, y \in \mathbb{F}_{q^m}^n$ *is defined as the rank of their differences, i.e.,* $d_R(x,y) = \mathrm{Rank}(x-y)$.

1.2 Linearized Polynomials

Ore in [42] introduced the notion of q-polynomials as a special class of skew polynomials [43]. When the value of q is known or the context is clear, we use *linearized polynomials* instead of q-polynomials. They have been used to define rank metric codes that will be introduced later.

Definition 12. *[42] The polynomial*

$$L(x) = \sum_{i=0}^{n-1} l_i x^{[i]},$$

where $l_i \in \mathbb{F}_{q^m}$ and $n \leq m$, is called a linearized polynomial over $\mathbb{F}_{q^m}$. The set of all linearized polynomials of the form $L(x)$ is denoted by $\mathcal{L}_n(\mathbb{F}_{q^m})$. The q-degree of a linearized polynomial is defined as $\deg_q(f) = \max\{0 \leq i < n \mid l_i \neq 0\}$.

The set of linearized polynomials $\mathcal{L}_n(\mathbb{F}_{q^m})$ forms a non-commutative ring while the operations are addition and symbolic multiplication. Addition operation $+$ coincides with addition of ordinary polynomials but symbolic multiplication $*$ differs from the multiplication of ordinary polynomials. For $f(x) = \sum_{i=0}^{r} f_i x^{[i]}$ and $h(x) = \sum_{i=0}^{s} h_i x^{[i]}$ in $\mathcal{L}_n(\mathbb{F}_{q^m})$, the symbolic multiplication is defined as

$$\begin{aligned} l(x) &= \sum_{i=0}^{r+s} l_i x^{[i]} = f(x) * h(x) = f(h(x)) \\ &= \sum_{i=0}^{r} f_i (h(x))^{[i]} = \sum_{i=0}^{r+s} \Big(\sum_{j+k=i} f_i h_k^{[i]} \Big) x^{[j+k]}, \end{aligned}$$

where $l(x)$ is still a linearized polynomial and the powers are taken on modulo q^m. A linearized polynomial $f(x) \in \mathcal{L}_n(\mathbb{F}_{q^m})$ satisfies the linearity: $f(a_1 x + a_2 y) = a_1 f(x) + a_2 f(y)$ where $a_1, a_2 \in \mathbb{F}_q$ and $x, y \in \mathbb{F}_{q^m}$. This shows the origin of naming *linearized polynomials* and it means any $\mathbb{F}_q$-linear combination of roots of a linearized polynomial $f(x)$ is also a root of $f(x)$. Moreover, an $f(x) \in \mathcal{L}_n(\mathbb{F}_{q^m})$ forms an $\mathbb{F}_q$-linear map f from $\mathbb{F}_{q^m}$ to itself. The kernel of this map is the root space of $f(x)$.

Theorem 1. *[30, Theorem 3.31] A polynomial $f(x)$ over $\mathbb{F}_{q^m}$ is a linearized polynomial if and only if, its root space forms a linear space over $\mathbb{F}_q$ and each root has the same multiplicity which is a power of q.*

The roots of $f(x)$ do not need to be elements of $\mathbb{F}_{q^m}$, they can be elements of a larger extension field.

Theorem 2. *[1] Let $l(x) \in \mathcal{L}_n(\mathbb{F}_{q^m}) \setminus \{0\}$. Then* $\dim(\ker(l)) \leq \deg_q(l)$, *where* $\ker(l)$ *is the kernel of $l(x)$ as an $\mathbb{F}_q$-linear map.*

Based on rank nullity Theorem and Theorem 2, the rank of a non-zero linearized polynomial $l(x) \in \mathcal{L}_n(\mathbb{F}_{q^m})$ is $\text{Rank}(l) \geq m - \deg_q(l)$.

Theorem 3. *[30] Let W be a linear subspace of $\mathbb{F}_{q^m}$ considered as a v-dimensional vector space over $\mathbb{F}_q$. Let $a_0,\ldots,a_{v-1}$ be an $\mathbb{F}_q$-basis of W. Then the minimal subspace polynomial*

$$M_{a_0,\ldots,a_{v-1}}(x)=\prod_{w\in W}\left(x-\sum_{i=0}^{v-1}a_iw_i\right), \tag{1.3}$$

is a linearized polynomial in $\mathcal{L}_n(\mathbb{F}_{q^m})$ with q-degree v. The unique minimal subspace polynomial has all the possible $\mathbb{F}_q$-linear combinations of $a_0,\ldots,a_{v-1}$ as its roots.

Theorem 4. *[31] Let $\alpha_0,\ldots,\alpha_{n-1}$ be an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$ and let $l(x)=\sum_{i=0}^{n-1}l_ix^{[i]}\in\mathcal{L}_n(\mathbb{F}_{q^n})$. Then there exists a unique vector $(\beta_0,\ldots,\beta_{n-1})\in\mathbb{F}_{q^n}^n$ such that*

$$l(x)=\mathrm{Tr}(\beta_0x)\alpha_0+\cdots+\mathrm{Tr}(\beta_{n-1}x)\alpha_{n-1}=\sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1}\alpha_j\beta_j^{q^i}\right)x^{[i]}. \tag{1.4}$$

Moreover, the rank of $l(x)$ is k if and only if the rank of $(\beta_0,\ldots,\beta_{n-1})$ is k, where $0\le k\le n$.

Proof. Let $f(x)\in\mathcal{L}_n(\mathbb{F}_{q^n})$ such that $f(x)\in\mathbb{F}_q$ for every $x\in\mathbb{F}_{q^n}$. Then there exists an element β such that $f(x)=\mathrm{Tr}(\beta x)$. This is because the set $\{\mathrm{Tr}(\beta x),\beta\in\mathbb{F}_{q^n}\}$ contains all q^n distinct linear maps from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ such that $\mathrm{Tr}(\beta x)\in\mathbb{F}_q$ for all $x\in\mathbb{F}_{q^n}$. Now the linearized polynomial $l(x)$ can be written as an $\mathbb{F}_q$-linear combination of $\alpha_0,\ldots,\alpha_{n-1}$ in the form

$$l(x)=f_0(x)\alpha_0+\cdots+f_{n-1}(x)\alpha_{n-1}=\mathrm{Tr}(\beta_0x)\alpha_0+\cdots+\mathrm{Tr}(\beta_{n-1}x)\alpha_{n-1},$$

where $f_i(x)\in\mathcal{L}_n(\mathbb{F}_{q^n})$ are linearized polynomials such that $f_i(x)\in\mathbb{F}_q$ for every $x\in\mathbb{F}_{q^n}$. One can expand the trace function and get

$$l(x)=\sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1}\alpha_j\beta_j^{q^i}\right)x^{[i]}. \tag{1.5}$$

To prove the second part let $B=\mathrm{span}(\beta_0,\ldots,\beta_{n-1})$ be the $\mathbb{F}_q$-subspace generated by $\beta_0,\ldots,\beta_{n-1}$ and let $B^\perp=\{x\in\mathbb{F}_{q^n}:\mathrm{Tr}(x\beta)=0,\text{ for every }\beta\in B\}$. Then

$$\mathrm{Ker}(l)=\{x\in\mathbb{F}_{q^n}:\mathrm{Tr}(\beta_ix)=0,\text{ for all }0\le i\le n-1\}=B^\perp.$$

Due to the fact that $<x,y>=\mathrm{Tr}(xy)$ is a non-degenerate bilinear form $\mathbb{F}_{q^n}\times\mathbb{F}_{q^n}\to\mathbb{F}_q$. It follows that the dimension of $B^\perp$ over $\mathbb{F}_q$ is equal to $n-\dim(B)$ over $\mathbb{F}_q$. So

$$\dim(\mathrm{Ker}(l))=\dim(B^\perp)=n-\dim(B)=n-\dim\{\beta_0,\ldots,\beta_{n-1}\}.$$

Thus the rank of the linearized polynomial $l(x)\in\mathcal{L}_n(\mathbb{F}_{q^n})$ is k if and only if $\mathrm{Rank}\{\beta_0,\ldots,\beta_{n-1}\}=k$. □

Theorem 5. *Let $l(x)=\sum_{i=0}^{n-1}l_ix^{[i]}$ be a linearized polynomial of rank k. Then there exist two sets*

$\{\alpha_1,\dots,\alpha_k\}$ and $\{\beta_1,\dots,\beta_k\}$ in $\mathbb{F}_{q^n}$ such that they are $\mathbb{F}_q$-linearly independent and

$$l(x) = \mathrm{Tr}(\beta_1 x)\alpha_1 + \cdots + \mathrm{Tr}(\beta_k x)\alpha_k = \sum_{i=0}^{n-1}\left(\sum_{j=1}^{k}\alpha_j\beta_j^{[i]}\right)x^{[i]}.$$

Proof. Let $\alpha_i\mathbb{F}_q$ be the $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$ generated by α_i. Then any linear map from $\mathbb{F}_{q^n} \to \alpha_i\mathbb{F}_q$ can be represented by $\alpha_i\,\mathrm{Tr}(\beta_i x)$ for some $\beta_i \in \mathbb{F}_{q^n}$. We assume $\{\alpha_1,\dots,\alpha_k\}$ to be the basis for the image space $l(x)$. So we can write $l(x)$ as

$$l(x) = \mathrm{Tr}(\beta_1 x)\alpha_1 + \cdots + \mathrm{Tr}(\beta_k x)\alpha_k = \sum_{i=0}^{n-1}\left(\sum_{j=1}^{k}\alpha_j\beta_j^{[i]}\right)x^{[i]},$$

where the final equality is obtained by expanding the trace function. Now we must show that $\beta_1,\dots,\beta_k$ are $\mathbb{F}_q$-linearly independent. Without loss of generality let assume $\beta_k = b_1\beta_1 + \cdots + b_{k-1}\beta_{k-1}$ where $b_i \in \mathbb{F}_q$. Then we have

$$\begin{aligned} l(x) =& \alpha_1\,\mathrm{Tr}(\beta_1 x) + \cdots + \alpha_{k-1}\,\mathrm{Tr}(\beta_{k-1}x) + \alpha_k\,\mathrm{Tr}((b_1\beta_1 + \cdots + b_{k-1}\beta_{k-1})x) \\ =& \alpha_1\,\mathrm{Tr}(\beta_1 x) + \cdots + \alpha_{k-1}\,\mathrm{Tr}(\beta_{k-1}x) + \alpha_k\,\mathrm{Tr}(b_1\beta_1 x) + \cdots + \alpha_k\,\mathrm{Tr}(b_{k-1}\beta_{k-1}x) \\ =& (\alpha_1 + b_1\alpha_k)\,\mathrm{Tr}(\beta_1 x) + \cdots + (\alpha_{k-1} + b_{k-1}\alpha_k)\,\mathrm{Tr}(\beta_{k-1}x), \end{aligned}$$

which means $l(x)$ can be generated by $k-1$ linearly independent points and this is a contradiction. □

Later in this thesis we will propose several decoding algorithms for rank metric codes. We will see that *Dickson matrix* associated with linearized polynomials and its properties play crucial roles in the decoding process. Moreover, they will be used to find zeros of linearized polynomials over their defined field.

Definition 13 (Dickson Matrix)**.** *[10] Let $l(x) = \sum_{i=0}^{n-1} l_i x^{[i]}$ be a linearized polynomial. The matrix*

$$D = \left(l_{i-j(\mathrm{mod}n)}^{q^j}\right)_{n\times n} = \begin{pmatrix} l_0 & l_{n-1}^{q} & \cdots & l_1^{q^{n-1}} \\ l_1 & l_0^{q} & \cdots & l_2^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n-1} & l_{n-2}^{q} & \cdots & l_0^{q^{n-1}} \end{pmatrix}, \tag{1.6}$$

is called the Dickson matrix associated with $l(x)$.

Proposition 1. *Let $l(x) = \sum_{i=0}^{n-1} l_i x^{[i]} \in \mathcal{L}_n(\mathbb{F}_{q^m})$ and D be its associated Dickson matrix. We have the following two properties:*

i. The Dickson matrix D has rank k, if the linearized polynomial $l(x)$ has rank k [10, 40].

ii. If D has rank k, then any $k\times k$ submatrix of D formed by k consecutive rows and columns is non-singular [53].

Proof. Let $l(x)$ be a linearized polynomial with rank k. Using Theorem 5, we can write the coefficients l_i as

$$l_i = \sum_{j=1}^{k} \alpha_j \beta_j^{[i]},$$

where $\alpha_1, \ldots, \alpha_k$ and $\beta_1, \ldots, \beta_k$ are two $\mathbb{F}_q$-linearly independent sets in $\mathbb{F}_{q^n}$. So we can write $D = M * W$ where

$$M = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_k \\ \alpha_1^{[1]} & \alpha_2^{[1]} & \cdots & \alpha_k^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{[n-1]} & \alpha_2^{[n-1]} & \ldots & \alpha_k^{[n-1]} \end{pmatrix}, W = \begin{pmatrix} \beta_1 & \beta_1^{[1]} & \cdots & \beta_1^{[n-1]} \\ \beta_2 & \beta_2^{[1]} & \cdots & \beta_2^{[n-1]} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_k & \beta_k^{[1]} & \ldots & \beta_k^{[n-1]} \end{pmatrix}, \tag{1.7}$$

since α_j's and also β_j's are linearly independent, any k successive rows of M and any k successive columns in W give non-singular matrices. The rest of the proof follows from these facts and Theorems 4 and 5. □

Let $\tilde{l} = (l_0, l_1, \ldots, l_{n-1})$ be the coefficient vector of a linearized polynomial $l(x) = \sum_{i=0}^{n-1} l_i x^{q^i}$ over $\mathbb{F}_{q^m}$. Evaluation of $l(x)$ on a point $a \in \mathbb{F}_{q^m}$ can be done as $l(a) = l_0 a + l_1 a^q + \cdots + l_{n-1} a^{q^{n-1}}$. We can similarly evaluate $l(x)$ on multiple points in $\beta = \{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$ over $\mathbb{F}_{q^m}$ and get their values as a vector of the form $l(\beta) = (l(\beta_0), l(\beta_1) \ldots, l(\beta_{n-1}))$. Equivalently, evaluation of $l(x)$ on points in β can be represented as

$$l(\beta) = (l(\beta_0), l(\beta_1) \ldots, l(\beta_{n-1})) = \tilde{l} \cdot \mathcal{M}^T, \tag{1.8}$$

where $\mathcal{M}$ is the Moore matrix associated to the points in β.

Definition 14. *[43] Let $\mathbb{F}_{q^m}$ be a field extension of $\mathbb{F}_q$ and let $\sigma \in Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$ be a generator of its Galois group. A skew polynomial ring $\mathbb{F}_{q^m}[x;\sigma]$ is the set of all polynomials of the form $f(x) = \sum_{i=0}^{s} f_i x^i$, where $s \in \mathbb{N}$, equipped with the usual addition and with multiplication determined by $ax = xa^\sigma$ for any scalar $a \in \mathbb{F}_{q^m}$.*

The skew polynomial ring $\mathbb{F}_{q^m}[x;\cdot^q]$, with the Frobenius automorphism $\cdot^\rho$ is isomorphic to the non-commutative ring $\mathcal{L}(\mathbb{F}_{q^m})$, i.e., $\mathbb{F}_{q^m}[x;\cdot^q] \cong \mathcal{L}(\mathbb{F}_{q^m})$. So skew polynomials are natural generalizations of linearized polynomials.

1.3 Block Codes

A (block) code $C = (n, M, d)$ over a finite field $\mathbb{K}$ with length (block length) n, size $M = |C| \geq 2$ and minimum distance d, with respect to the metric $d(\cdot,\cdot)$, is a subset $C \subseteq \mathbb{K}^n$ such that $d = \min\{d(x,y) | x, y \in C \setminus \{0\} \text{ and } x \neq y\}$. An element of C is called a *codeword*.

A code C is *linear* if it forms a vector space over $\mathbb{K}$. The dimension k of a linear code C is the dimension of C as a vector space over $\mathbb{K}$ and a linear code is denoted as $C = [n, k, d]$. A

linear code $C = [n,k,d]$ takes a message of length k over $\mathbb{K}$, add some *redundancy* symbols to the message and outputs a longer block (codeword) of length n. This is called the *encoding* process. Since there is a one-to-one correspondence between the message space and the set of codewords, the size of the linear code $[n,k,d]$ is $M = |\mathbb{K}|^k$.

Since a linear code forms a subspace in $\mathbb{K}^n$, one can generate a linear code using its *generator matrix*.

Definition 15 (Generator Matrix)**.** *A $k \times n$ matrix G is a generator matrix of a linear code $C = [n,k,d]$ over $\mathbb{K}$ if $Row(G) = C$, where $Row(G)$ is the row space of G. In other words, the rows of a generator matrix G of C form a basis for a k-dimensional vector space C over $\mathbb{K}$.*

Generator matrices are used to encode information words (messages) in $\mathbb{K}^k$ by transforming them into codewords of length n. This is done as $m \cdot G_{k\times n} = c$, where $m \in \mathbb{K}^k$ and $c \in C = [n,k,d] \subseteq \mathbb{K}^n$. Linear code $C = [n,k,d]$ has multiple generator matrices.

Definition 16 (Dual Code)**.** *Let C be any code of length n (not necessarily linear) over $\mathbb{K}$. The dual of C is defined as*

$$C^{\perp} = \{x \in \mathbb{K}^n |\, x \cdot c = 0, \textit{ for all } c \in C\},$$

where $x \cdot c$ is the usual inner product. For a linear code $C = [n,k,d]$ over $\mathbb{K}$ with a generator matrix G we can also define its dual as $C^{\perp} = \{x \in \mathbb{K}^n |\, G \cdot x^T = \mathbf{0}\}$, where $\mathbf{0}$ is the zero vector of length k. So the vectors in $C^{\perp}$ are the transpose of the vectors in the null space of G and hence $C^{\perp} = [n, n-k]$.

Definition 17 (Parity Check Matrix)**.** *Let $C^{\perp}$ be the dual of a linear code $C = [n,k,d]$ with a generator matrix G over $\mathbb{K}$. An $(n-k) \times n$ generator matrix H of $C^{\perp}$ where $G \cdot H^T = 0$ is called the parity check matrix of C. So $c \cdot H^T = \mathbf{0}$ for all $c \in C$. A parity check matrix of a linear code C can be found if its generator matrix is given.*

Definition 18 (Syndrome)**.** *Let C be a linear code over $\mathbb{K}$ with parity check matrix H. The syndrome of a word $x \in \mathbb{K}^n$ is $s = x \cdot H^T \in \mathbb{K}^{n-k}$. A word $y \in \mathbb{K}^n$ is a codeword if and only if its syndrome is $\mathbf{0}$.*

Definition 19 (Weight Distribution and Weight Enumerator)**.** *The weight distribution of a code C with length n is $A(C) = \{A_0, A_1, \ldots, A_n\}$ where A_i denotes the number of codewords in C with weight i. The weight enumerator of C is defined as $1 + A_1 x + A_2 x^2 + \cdots + A_n x^n$. The code C is called a t-weight codes if the number of non-zero A_i's for $1 \leq i \leq n$ is equal to t.*

Investigation of linear codes with few non-zero weights has been one of the main trends in coding theory [11, 12, 13, 24, 28, 29]. In Chapter 7, we will discuss a related problem.

Definition 20 (Code Rate)**.** *Let C be a linear code with length n and size M over a finite field $\mathbb{K}$ with size q. The rate of C is defined as $R_C = \log_q M/n$.*

A linear code C is called a *low rate* code if $R_C < \frac{1}{2}$ and it is called *high rate* otherwise.

In Chapters 3-6, we consider the following simple problem:

Problem 1. *Suppose Alice wants to communicate with Bob. She first encodes her message m and submits the codeword c into a channel. The channel could be a phone line, the air in a room, a fibre-optic cable, a compact disc, and so on. But every time she sends a codeword, there is a chance that some of its symbols will be corrupted. The errors (noises) can come from human error, imperfections in the equipment, scratches on the disc, and so on. So the word r that Bob receives may not be the word that Alice sent. How Alice and Bob can communicate reliably?*

Our setup is shown in Figure 1.1. Bob can decode r by checking all the possible $|C|$ codewords in code C and find the closest codeword (codewords) c' to c. This brute force approach is not practical for long codes. One of the main concerns in coding theory is to find codes with efficient decoding algorithms. In the following, we discuss two different decoding principles for linear codes. Let $r = c + e$ be the received word, c be the sent codeword, e be the error added by a channel and $t = \lfloor \frac{d-1}{2} \rfloor$ be the decoding radius.

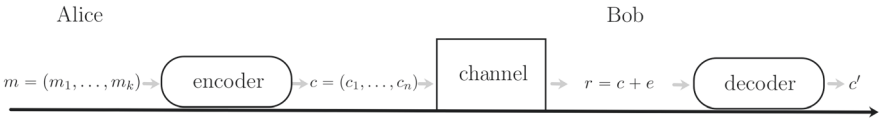

Figure 1.1: Communication Model

Definition 21 (Unique Decoding)**.** *A unique decoder approach returns a codeword of minimal distance to the received word among those codewords c with* $d(c,r) \leq t$.

Definition 22 (List Decoding)**.** *A list decoding approach returns a list of codewords which contains all the codewords* c' *such that* $d(r,c') \leq t$.

If the decoding radius is less than $\lfloor \frac{d-1}{2} \rfloor$ then there is at most one codeword c with $d(r,c) \leq t$. So in this case the above decoding approaches coincides and both return the same unique solution. In this thesis we only consider unique decoding algorithms.

1.4 Codes in Hamming Metric

The Hamming metric was defined in Definition 10 and in the current section we only consider linear codes with respect to the Hamming metric. The minimum distance of a linear code in the Hamming metric is the minimum weight between its nonzero codewords and it can be upper bounded as follows.

Theorem 6. *[73] Let* $C = [n,k,d]$ *be a linear code over* $\mathbb{F}_q$ *with minimum Hamming distance d. Then*

$$d \leq n - k + 1,$$

which is equivalent to $|C| \leq q^{n-d+1}$.

If a linear code C attains this bound, it is called a *maximum separable distance (MDS)* code. Linear MDS codes have largest possible minimum distance d for fixed integers n and k which means they have the best error detection and correction capabilities which will be discussed later. One of the most well-known families of MDS codes is the *Reed-Solomon codes* which was introduced by Reed and Solomon in 1960 [54]. Since that time they have been applied in secret sharing schemes [39], CD-ROMs [25], wireless communications [65], space communications [80] and QR codes [41]. These codes are evaluation codes and they are defined as follows.

Definition 23 (Reed-Solomon Codes)**.** *[54] Let $n < q$ and $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ be distinct points in $\mathbb{F}_q$. Then a Reed-Solomon (RS) code $C = [n,k,d] \in \mathbb{F}_q^n$ is defined as*

$$C = \{c = (f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{n-1}))|\ f(x) \in \mathbb{F}_q[x] \text{ and } \deg f < k\},$$

where $\mathbb{F}_q[x]$ is the set of all ordinary polynomials with coefficients in $\mathbb{F}_q$.

1.5 Codes in Rank Metric

Block codes with respect to rank metric were introduced by Delsarte [8], Gabidulin [17] and Roth [59], independently.

Definition 24 (Rank Metric Codes)**.** *A subset $\mathcal{C} \in \mathbb{F}_{q^m}^n$ is called a rank metric code where the distance between the elements in $\mathcal{C}$ is defined with respect to the rank metric.*

Definition 25. *A rank metric code $\mathcal{C}$, defined over $\mathbb{F}_{q^m}$ is called*

i. an additive rank metric code if for all $a,b \in \mathcal{C}$ we have $a+b \in \mathcal{C}$,

ii. an $\mathbb{F}_{q_0}$-linear if for all $a,b \in \mathcal{C}$ and $\alpha,\beta \in \mathbb{F}_{q_0}$ we have $\alpha a + \beta b \in \mathcal{C}$, where $\mathbb{F}_{q_0}$ is a subfield of $\mathbb{F}_{q^m}$.

iii. a linear ($\mathbb{F}_{q^m}$-linear) if for all $a,b \in \mathcal{C}$ and $\alpha,\beta \in \mathbb{F}_{q^m}$ we have $\alpha a + \beta b \in \mathcal{C}$.

The codes in ii. and iii. form vector spaces over $\mathbb{F}_{q_0}$ and $\mathbb{F}_{q^m}$, respectively.

Similar to the Hamming metric we have a Singleton-like bound for rank metric codes as follows:

Theorem 7 (Singleton-like Bound)**.** *[8, Theorem 5.4] Let $\mathcal{C}$ be a rank metric code with length n, dimension k and minimum distance d over $\mathbb{F}_{q^m}$. Then*

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

If a rank metric code $\mathcal{C}$ attains the above bound, it is called a *maximum rank distance (MRD)* code. We consider $k < n \leq m$ for the rest of this chapter unless stated otherwise. Gabidulin codes are the most well-known family of MRD codes and they have applications in cryptography [19], space-time coding [37], distributed storage [4, 59], random network coding [71] and digital watermarking [27].

Definition 26 (Gabidulin Codes)**.** *Let $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ be $\mathbb{F}_q$-linearly independent points in $\mathbb{F}_{q^m}$. A Gabidulin code $\mathcal{G}_{n,k}$ with length n and dimension k is defined by evaluation of*

$$\left\{ \sum_{i=0}^{k-1} l_i x^{q^i} \,|\, l_i \in \mathbb{F}_{q^m} \right\},$$

on linearly independent points $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ and it is equivalent to

$$\mathcal{G}_{n,k} = \{(l(\alpha_0), l(\alpha_1), \ldots, l(\alpha_{n-1}))|\, l(x) \in \mathcal{L}_n(\mathbb{F}_{q^m}) \text{ and } \deg_q(f) < k\}.$$

Gabidulin code $\mathcal{G}_{n,k}$ is an $\mathbb{F}_{q^m}$-linear MRD code. Its minimum rank distance and size for $n \leq m$ are $d = n-k+1$ and $M = q^{mk}$, respectively.

Codes that are $\mathbb{F}_{q^m}$-linear such as Gabidulin codes form subspaces in $\mathbb{F}_{q^m}^n$, hence we can represent each of them by a $k \times n$ *generator matrix*.

Definition 27 (Generator Matrix of Gabidulin Codes)**.** *Let $\mathcal{C}$ be an $\mathbb{F}_{q^m}$-linear code with length n and dimension k. Suppose $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{F}_{q^m}$ are linearly independent evaluation points. Then the matrix*

$$G = \left(\alpha_j^{q^i}\right)_{k\times n} = \begin{pmatrix} \alpha_0 & \alpha_1 & \ldots & \alpha_{n-1} \\ \alpha_0^q & \alpha_1^q & \ldots & \alpha_{n-1}^q \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{q^{k-1}} & \alpha_1^{q^{k-1}} & \ldots & \alpha_{n-1}^{q^{k-1}} \end{pmatrix}, \tag{1.9}$$

is a generator matrix of $\mathcal{G}_{n,k}$.

The matrix G is formed by the first k columns of the Moore matrix associated with linearly independent evaluation points $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ and its rows form a basis for $\mathcal{G}_{n,k}$. The set of all the coefficient vectors of linearized polynomials with q-degree less than k forms the message space $\mathbb{F}_{q^m}^k$. So the encoding of a message $\tilde{l} = (l_0, l_1, \ldots, l_{k-1}) \in \mathbb{F}_{q^m}^k$ (coefficient vector of $l(x) = \sum_{i=0}^{k-1} l_i x^{q^i}$) is conducted as

$$\tilde{l} = (l_0, l_1, \ldots, l_{k-1}) \mapsto c = (l(\alpha_0), l(\alpha_1), \ldots, l(\alpha_{n-1})) = \tilde{l} \cdot G,$$

where G is a generator matrix and $c \in \mathcal{G}_{n,k}$. Given a generator matrix G of $\mathcal{G}_{n,k}$, one can find an $(n-k) \times n$ parity check matrix H for $\mathcal{G}_{n,k}$ of the form

$$H = \left(h_j^{q^i}\right)_{(n-k)\times n} = \begin{pmatrix} h_0 & h_1 & \ldots & h_{n-1} \\ h_0^q & h_1^q & \ldots & h_{n-1}^q \\ \vdots & \vdots & \ddots & \vdots \\ h_0^{q^{n-k+1}} & h_1^{q^{n-k+1}} & \ldots & h_{n-1}^{q^{n-k+1}} \end{pmatrix}, \tag{1.10}$$

where $h_0, h_1, \ldots, h_{n-1} \in \mathbb{F}_{q^m}$ are $\mathbb{F}_q$-linearly independent and $G \cdot H^T = \mathbf{0}$. Parity check matrix of Gabidulin codes plays an important role in syndrome-based decoding approach which will be explained in Subsection 1.6.1. If a rank metric code is not $\mathbb{F}_{q^m}$-linear, we can not define a $k \times n$ generator matrix and consequently its $(n-k) \times n$ parity check matrix. For example

a generator matrix for an $\mathbb{F}_q$-linear code C over $\mathbb{F}_{q^m}$ is an $k \cdot m \times n$ matrix with entries in $\mathbb{F}_q$. Forms of the generator and parity check matrices of non $\mathbb{F}_{q^m}$-linear rank metric codes have not been studied in the literature.

Using the function $B : \mathbb{F}_{q^m}^n \to \mathbb{F}_q^{m\times n}$ defined in (1.1), one can represent the vector codeword $c \in \mathbb{F}_{q^m}^n$ of a rank metric code in matrix form $c' \in \mathbb{F}_q^{m\times n}$ as follows

$$c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_{q^m}^n \mapsto c' = B(c) = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{pmatrix}.$$

The vector and matrix representations of codewords in rank metric are equivalent but we mostly use their vector form in this thesis.

1.5.1 New MRD Codes

Gabidulin codes have been proven to be unsuitable for some applications in particular for cryptography due to their algebraic structure [46, 47]. Therefore finding new constructions is required. Gabidulin codes were generalized for the first time in [26] as follows:

Theorem 8. *Let $gcd(m,s) = 1$. The generalized Gabidulin (GG) code $\mathcal{GG}_{n,k}$ with length n and dimension k over $\mathbb{F}_{q^m}$ is defined by*

$$\mathcal{GG}_{n,k} = \left\{ (f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{n-1}))\,|\, f(x) = \sum_{i=0}^{k-1} f_i x^{q^{si}} \text{ and } f_i \in \mathbb{F}_{q^m} \right\}, \tag{1.11}$$

where $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ are linearly independent points in $\mathbb{F}_{q^m}$. This code is an $\mathbb{F}_{q^m}$-linear MRD code.

The choice of evaluation points $\alpha_0, \ldots, \alpha_{n-1}$ does not affect the rank property so it is common to omit the evaluation points in the definition of MRD codes and define for example the generalized Gabidulin code $\mathcal{GG}_{n,k}$ as the set of linearized polynomials $\mathcal{GG}_{n,k} = \{f(x) = \sum_{i=0}^{k-1} f_i x^{q^{si}} \,|\, f_i \in \mathbb{F}_{q^m}\}$. For the rest of this chapter we consider $n = m$.

John Sheekey in [63] established a new way to generalize Gabidulin codes to $\mathbb{F}_q$-linear MRD codes. He twisted the evaluation polynomial of Gabidulin codes and proposed *twisted Gabidulin (TG) codes*. After adding a twisted term, his evaluation polynomial $f(x)$ has q-degree at most k which leads to $\text{Rank}(f) \geq n-k$ and $d \geq n-k$ and this contradicts with being MRD. This issue is handled by recalling the following Lemma which characterizes a necessary condition for $f(x)$ to have rank $n-k$. This Lemma appeared for the first time in [23, Theorem 10].

Lemma 1. *[23, Theorem 10] Suppose a linearized polynomial $f(x) = \sum_{i=0}^{k} f_i x^{q^i} \in \mathcal{L}_n(\mathbb{F}_{q^n})$ with $f_k \neq 0$ has q^k roots in $\mathbb{F}_{q^n}$. Then $\text{Norm}_{q^n/q}(f_k) = (-1)^{nk}\text{Norm}_{q^n/q}(f_0)$, where* Norm *is the norm function in Definition 3.*

According to Lemma 1, if the condition is not met i.e. $\text{Norm}_{q^n/q}(f_k) \neq (-1)^{nk}\text{Norm}_{q^n/q}(f_0)$, a linearized polynomial $f(x)$ with q-degree k has rank at least $n-k+1$. The idea of Sheekey was generalized further in [36] as follows.

Definition 28. *[36, 63] Let $n,k,s,h \in \mathbb{Z}^+$ with $gcd(n,s) = 1$ and $k < n$. Let $\eta \in \mathbb{F}_{q^n}$ such that $\text{Norm}_{q^n/q}(\eta) \neq (-1)^{nk}$. Then the set*

$$\mathcal{GTG}_{n,k}(\eta,h) = \left\{ \sum_{i=0}^{k-1} f_i x^{q^{si}} + \eta f_0^{q^h} x^{q^{sk}} \mid f_i \in \mathbb{F}_{q^n} \right\}, \tag{1.12}$$

is an $\mathbb{F}_q$-linear MRD code of size q^{nk}. If $s = 1$ then the code gives a twisted Gabidulin code in [63].

In [50], the TG codes were further generalized by Puchinger, Rosenkilde and Sheekey as follows.

Definition 29. *[50] Let $n,k,t \in \mathbb{Z}^+$ such that $k < n$ and $t < n-k$. Let $\eta \in \mathbb{F}_{q^n} \setminus \{0\}$. Then the set*

$$\mathcal{TG}_{n,k}(t,\eta) = \left\{ \sum_{i=0}^{k-1} f_i x^{q^i} + \eta f_0 x^{q^{k-1+t}} \mid f_i \in \mathbb{F}_{q^n} \right\}, \tag{1.13}$$

is an MRD code of size q^{nk}. When $t = 1$ it gives the original TG codes in [63].

The first family of additive MRD codes were introduced by Otal and Özbudak in [44] which contains all the aforementioned MRD families, except the one in Definition 29, as sub-families. They considered the case when q is not prime and $q = q_0^u$ where $u \in \mathbb{Z}^+$ and $\mathbb{F}_{q_0}$ is a subfield of $\mathbb{F}_q$. The new family are $\mathbb{F}_{q_0}$-linear and they are known as *additive generalized twisted Gabidulin (AGTG) codes*.

Definition 30. *[44] Let $n,k,s,u,h \in \mathbb{Z}^+$ where $gcd(n,s) = 1$ and $q = q_0^u$. Let $\eta \in \mathbb{F}_{q^n}$ where $\text{Norm}_{q^{ns}/q_0^s}(\eta) \neq (-1)^{nku}$. The set*

$$\mathcal{AGTG}_{n,k}(\eta,h,u) = \left\{ \sum_{i=0}^{k-1} f_i x^{q^{si}} + \eta f_0^{q_0^h} x^{q^{sk}} \mid f_i \in \mathbb{F}_{q^n} \right\}, \tag{1.14}$$

is an $\mathbb{F}_{q_0}$-linear MRD code with size q^{nk}.

Trombetti and Zhou in [74] gave a new family of MRD codes and they showed that their construction is not equivalent to the other known MRD codes. We refer to the family as *Trombetti Zhou (TZ) codes*.

Definition 31. *[74] Let $n,k,s \in \mathbb{Z}^+$ satisfying $(s,2n) = 1$ and let $\gamma \in \mathbb{F}_{q^{2n}}$ satisfy that $Norm_{q^{2n}/q}(\gamma)$ is a non-square element in $\mathbb{F}_q$. Then the set*

$$\mathcal{D}_{k,s}(\gamma) = \left\{ ax + \sum_{i=1}^{k-1} f_i x^{q^{si}} + \gamma b x^{q^{sk}} \mid f_i \in \mathbb{F}_{q^{2n}}, a,b \in \mathbb{F}_{q^n} \right\}, \tag{1.15}$$

is an $\mathbb{F}_{q^n}$-linear MRD code of size q^{2nk} and minimum rank distance $2n-k+1$.

Note that the code is defined over $\mathbb{F}_{q^{2n}}$ but it is linear over the subfield $\mathbb{F}_{q^n}$. So we are not able to define the code with a $k \times 2n$ generator matrix. The first and the last coefficients of the polynomials in (1.15) are chosen independently from the base field $\mathbb{F}_{q^n}$. If q is even, all the elements of $\mathbb{F}_q$ are square elements, so TZ codes exist only when the field characteristic is odd.

Sheekey in [64] construct a new family of MRD codes which can be seen a generalized version of TG codes and it contains MRD codes that are not equivalent to any previously known constructions. He used a quotient ring of a skew polynomials (Definition 14) instead of ring of linearized polynomials.

Definition 32. *[64] Let $\mathbb{F}_{q^m}[x;\sigma]$ be a skew polynomial ring and $g(t)$ be an irreducible polynomial in $\mathbb{F}_q[t]$. Let $\gamma \in \mathbb{F}_{q^m}$ such that $\mathrm{Norm}(\gamma) \neq (-1)^{mkr}$. Then the image of the set of polynomials*

$$\{f \in \mathbb{F}_{q^m}[x;\sigma] : f_{rk} = \gamma f_0 \text{ and } deg(f) \leq rk\},$$

in the quotient ring

$$\frac{\mathbb{F}_{q^m}[x;\sigma]}{g(x^n)} \simeq M_{m\times m}(\mathbb{F}_{q^r}),$$

is an MRD code of size q^{mkr}. Here, $M_{m\times m}(\mathbb{F}_{q^r})$ is the set of all $m \times m$ matrices over $\mathbb{F}_{q^r}$.

Nonlinear MRD codes were proposed in [14, 45]. The codes in [14] exist only for some specific parameters while the codes in [45] exist for all parameters. Moreover, the codes in [45], which are known as *partition codes*, are not included in AGTG codes and also they do not cover all the GTG codes. So partition codes are the first nonlinear (non-additive) MRD families exist for all parameters.

There are also new MRD codes with length n and minimum distance $n-1$ and $n-2$ [5, 6, 7] which we do not consider in this thesis.

1.5.2 New Rank Metric Codes With Restrictions

After the work of Kshevetskiy and Gabidulin [26] in 2005, most of the new rank metric codes that meet the best known upper bounds for minimum distance (optimal codes) have been constructed based on Sheekey's idea in Lemma 1. There are some exceptions that are known as *restricted codes*. The first family of codes with restricted matrix form appeared in [9] where the authors considered alternating bilinear forms. In 2010, Schmidt in [60] studied the rank metric codes with symmetric matrix form and later in 2015 he investigated the association schemes, bounds, properties and construction of rank metric codes with alternating matrix form [61]. Later in 2018 he developed the theory of rank metric codes with Hermitian matrix form [62]. In Chapter 6, we propose polynomial-time encoding and decoding algorithms for symmetric, alternating and Hermitian rank metric codes and they are not linear over the main extension field. The studied codes meet the best known upper bounds for their minimum distances and this is the reason for naming them as *optimal codes*. In this section we give the definitions and upper bounds for optimal codes.

A matrix $A \in \mathbb{F}_q^{n\times n}$ is called *symmetric* if $A = A^T$ and it is an *alternating* matrix if $A = -A^T$. We denote the set of symmetric and alternating matrices of order n over $\mathbb{F}_q$ by $\mathrm{S}_n(q)$ and $\mathrm{A}_n(q)$,

respectively. Let the function $\lambda : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ defined as $x \mapsto x^q$ be the conjugate function. We denote by A^* the conjugate transpose of $A \in \mathbb{F}_{q^2}^{n\times n}$, which is obtained by applying the conjugate map to all entries A^T. A matrix $A \in \mathbb{F}_{q^2}^{n\times n}$ is called *Hermitian* if $A = A^*$. The set of all Hermitian matrices over $\mathbb{F}_{q^2}$ is denoted by $H_n(q^2)$. The sets $S_n(q)$, $A_n(q)$ and $H_n(q^2)$ form $\mathbb{F}_q$-vector spaces with

$$\dim_{\mathbb{F}_q}(\mathrm{S}_n(q)) = \frac{n(n+1)}{2},\ \dim_{\mathbb{F}_q}(\mathrm{A}_n(q)) = \frac{n(n-1)}{2},\ \dim_{\mathbb{F}_q}(\mathrm{H}_n(q^2)) = n^2.$$

In order to apply our decoding algorithm we need to describe the codes in terms of linearized polynomials, We recall the following known facts from [60] and [35].

Proposition 2. *[35] Let $l \in \mathbb{Z}$.*

i. For each u-dimensional $\mathbb{F}_q$-vector space V, any bilinear form $B : V \times \mathbb{F}_{q^n} \to \mathbb{F}_q$ can be written as

$$B(x,y) = \mathrm{Tr}_{q^n/q}(\sum_{i=0}^{u-1} c_i y x^{q^{i-l}}),$$

for some uniquely determined $c_0, \ldots, c_{u-1} \in \mathbb{F}_{q^n}$.

ii. For each u-dimensional $\mathbb{F}_{q^2}$-vector space V, any Hermitian form $H : V \times \mathbb{F}_{q^{2n}} \to \mathbb{F}_{q^2}$ can be written as

$$H(x,y) = \mathrm{Tr}_{q^{2n}/q^2}(\sum_{j=0}^{u-1} b_j y^q x^{q^{2(j-l)}}),$$

for some uniquely determined $b_0, \ldots, b_{u-1} \in \mathbb{F}_{q^n}$.

Considering symmetric bilinear form $S(x,y)$, alternating bilinear form $A(x,y)$ and Hermitian form $H(x,y)$ as $\mathbb{F}_q$-vector spaces, we can write them as

$$\begin{cases} S(x,y) = \mathrm{Tr}_{q^n/q}(f(x)\cdot y), \\ A(x,y) = \mathrm{Tr}_{q^n/q}(f(x)\cdot y), \\ H(x,y) = \mathrm{Tr}_{q^{2n}/q^2}(y^q \cdot l(x)), \end{cases}$$

where $f(x) \in \mathcal{L}_n(\mathbb{F}_{q^n})$ and $l(x) \in \mathcal{L}_n(\mathbb{F}_{q^{2n}})$. Hence by choosing suitable basis of $\mathbb{F}_{q^n}$ ($\mathbb{F}_{q^{2n}}$) over $\mathbb{F}_q$ ($\mathbb{F}_{q^2}$) we can identify $S_n(q)$ as

$$\mathcal{S}_n(q) = \left\{ \sum_{i=0}^{n-1} a_i x^{q^i} : a_{n-i} = a_i^{q^{n-i}} \text{ for } i \in \{0,\ldots,n-1\} \right\} \subseteq \mathcal{L}_n(\mathbb{F}_{q^n}),$$

the set $\mathrm{A}_n(q)$ can be identified as

$$\mathcal{A}_n(q) = \left\{ \sum_{i=0}^{n-1} b_i x^{q^i} : b_{n-i} = -b_i^{q^{n-i}} \text{ for } i \in \{0,\ldots,n-1\} \right\} \subseteq \mathcal{L}_n(\mathbb{F}_{q^n}),$$

and similarly, the set $H_n(q^2)$ can be distinguished by

$$\mathcal{H}_n(q^2) = \left\{ \sum_{i=0}^{n-1} c_i x^{q^{2i}} : c_{n-i+1} = c_i^{q^{2n-2i+1}} \text{ for } i \in \{0,\dots,n-1\} \right\} \subseteq \mathcal{L}_n(\mathbb{F}_{q^{2n}}),$$

if n is odd then $c_{\frac{n+1}{2}} \in \mathbb{F}_{q^n}$. If we equip the set of matrices $S_n(q)$, $A_n(q)$ and $H_n(q^2)$ with rank metric, they are called *symmetric*, *alternating* and *hermitian* rank metric codes, respectively. We have the following bounds for these families which we use them as alternatives for Singleton-like bound to define the optimal codes.

Theorem 9. *[61, Theorem 3.3] Let $\mathcal{C}$ be an additive symmetric rank metric code in $\mathbb{F}_q^{n\times n}$ and d be an even integer. Then*

$$|\mathcal{C}| \leq \begin{cases} q^{n(n-d+2)/2} & \text{if } n-d \text{ is even}, \\ q^{(n+1)(n-d+2)/2} & \text{if } n-d \text{ is odd}. \end{cases}$$

Theorem 10. *[9, Theorem 4] Let $m = \lfloor \frac{n}{2} \rfloor$ and $\mathcal{C}$ be an alternating rank metric code in $\mathbb{F}_q^{n\times n}$ where $d = 2e$. Then*

$$|\mathcal{C}| \leq q^{\frac{n(n-1)}{2m}(m-e+1)}.$$

Theorem 11. *[62, Theorem 1] An additive Hermitian rank metric code $\mathcal{C}$ in $\mathbb{F}_{q^2}^{n\times n}$ satisfies*

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

Moreover, when d is odd, this upper bound holds also for non-additive Hermitian codes.

If the size of symmetric, alternating and Hermitian rank metric codes attain their associated bound they are called *optimal symmetric*, *optimal alternating* and *optimal Hermitian* rank metric codes, respectively. Schmidt in [61] and Delsarte in [9] presented the following constructions for optimal $\mathbb{F}_q$-linear symmetric and alternating rank metric codes.

Theorem 12. *[61, Theorem 4.4] Let n and d be two positive integers such that $1 \leq d \leq n$ and $n-d$ is even. The symmetric forms $S : \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \to \mathbb{F}_q$ are given by $S(x,y) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(yL(x))$ with*

$$L(x) = b_0 x + \sum_{j=1}^{\frac{n-d}{2}} \left(b_j x^{q^j} + (b_j x)^{q^{n-j}} \right), \tag{1.16}$$

as $b_0,\dots,b_{\frac{n-d}{2}}$ range over $\mathbb{F}_{q^n}$, form an $\mathbb{F}_q$-linear optimal rank metric code in $\mathrm{S}_n(q)$.

Theorem 13. *[9, Theorem 7] Let n and e be two positive integers such that n is odd and $1 \leq 2e \leq n-1$, and let $d = 2e$. The alternating form $A : \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \to \mathbb{F}_q$ is given by $A(x,y) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(yL(x))$ with*

$$L(x) = \sum_{j=e}^{\frac{n-1}{2}} \left(b_j x^{q^j} - (b_j x)^{q^{n-j}} \right), \tag{1.17}$$

as $b_e,\dots,b_{\frac{n-1}{2}}$ range over $\mathbb{F}_{q^n}$, form an $\mathbb{F}_q$-linear optimal rank metric code in $\mathrm{A}_n(q)$.

The following two theorems are stated by Schmidt in [62] provide constructions for optimal $\mathbb{F}_q$-linear Hermitian rank metric codes for all possible value of n and d, except if n and d are both even and $3 < d < n$.

Theorem 14. *[62, Theorem 4] Let n and d be two integers of opposite parities satisfying $1 \leq d \leq n$. The Hermitian forms $H : \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}} \to \mathbb{F}_{q^2}$ given by $H(x,y) = \mathrm{Tr}_{q^{2n}/q^2}\left(y^q L(x)\right)$ with*

$$L(x) = \sum_{j=1}^{\frac{n-d+1}{2}} \left((b_j x)^{q^{(2n-2j+2)}} + b_j^q x^{q^{(2j)}} \right), \tag{1.18}$$

as $b_1, \ldots, b_{\frac{n-d+1}{2}}$ range over $\mathbb{F}_{q^{2n}}$, form an $\mathbb{F}_q$-linear optimal rank metric code in $\mathrm{H}_n(q^2)$.

Theorem 15. *[62, Theorem 5] Let n and d be odd integers satisfying $1 \leq d \leq n$. The Hermitian forms $H : \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}} \to \mathbb{F}_{q^2}$ given by $H(x,y) = \mathrm{Tr}_{q^{2n}/q^2}\left(y^q L(x)\right)$ with*

$$L(x) = (b_0 x)^{q^{(n+1)}} + \sum_{j=1}^{\frac{n-d}{2}} \left((b_j x)^{q^{(n+2j+1)}} + b_j^q x^{q^{(n-2j+1)}} \right), \tag{1.19}$$

as b_0 ranges over $\mathbb{F}_{q^n}$ and $b_1, \ldots, b_{\frac{n-d}{2}}$ range over $\mathbb{F}_{q^{2n}}$, form an $\mathbb{F}_q$-linear optimal rank metric code in $\mathrm{H}_n(q^2)$.

1.6 Decoding Algorithms for Rank Metric Codes

The Gabidulin codes are known as q-analogue of Reed-Solomon codes. The decoding algorithms of Gabidulin codes are equivalent to the decoding algorithms for RS codes in Hamming metric. Known decoding algorithms for Gabidulin codes can be generally classified in two different approaches: syndrome-based decoding as in [16, 17, 58, 59] and interpolation-based decoding as in [34, 53]. Gabidulin in [17] solves the key equation in the decoding process by employing the linearized version of *extended Euclidean (LEE) algorithm*, while in [58], the key equation is solved by a linearized version of *Berlekamp-Massey (BM) algorithm*. The error values in both decoding algorithms in [17] and [58] are computed by an algorithm called *Gabidulin algorithm*. Loidreau in [34] proposed the first interpolation-based decoding approach for Gabidulin codes and considered the analogue of *Welch-Berlekamp (WB) algorithm*, which was originally used to decode Reed-Solomon codes [79]. The algorithm directly provides the code's interpolation polynomial and computing the error vector is not required in the decoding process. This section is dedicated to the known decoding algorithms for Gabidulin codes presented in [17, 34, 58] that undertake the following problem.

Problem 2 ($D(r, \mathcal{G}_{n,k}(\alpha), t)$)**.** *Suppose the linearly independent evaluation points $\alpha = (\alpha_0, \ldots, \alpha_{n-1}) \in \mathbb{F}_{q^m}^n$, the received vector $r = c + e$ and $t = \lfloor \frac{n-k}{2} \rfloor$ are given. Find, if it exists, $c \in \mathcal{G}_{n,k}$ and e such that* $\mathrm{Rank}(e) \leq t$.

1.6.1 Syndrome-Based Decoding

First we explain the syndrome-based decoding algorithms proposed in [17, 58]. Lets $r = c + e \in \mathbb{F}_{q^m}^n$ be a received word, where $c \in \mathcal{G}_{n,k}$ is the sent codeword and e is the error vector of rank t added by a noisy channel. The syndrome of r is defined as

$$s = (s_0, \ldots, s_{n-k-1}) = r \cdot H^T = (c+e) \cdot H^T = e \cdot H^T \in \mathbb{F}_{q^m}^{n-k}, \tag{1.20}$$

where $H_{(n-k)\times n}$ is the parity check matrix for $\mathcal{G}_{n,k}$ in (1.10). Hence the component s_i can be written in terms of the error vector components as

$$s_i = \sum_{j=0}^{n-1} e_j h_j^{[i]}. \tag{1.21}$$

Let $S(x) = \sum_{i=0}^{n-k-1} s_i x^{[i]}$ be the syndrome associated polynomial. In this approach the syndrome s is given and finding the error vector e is required. Since the rank of the error vector $e \in \mathbb{F}_{q^m}^n$ is t, it can be written as

$$e = a \cdot B = (a_0, \ldots, a_{t-1}) \cdot B_{t\times n}, \tag{1.22}$$

where both a and B have rank t. In other words, a is the basis for the column space of e and B fixes the row space. Vector a and matrix B are not unique but any pair of them works for decoding. Let $\Lambda(x) = \sum_{i=0}^{t} \Lambda_i x^{[i]}$ be the *error span polynomial* which is the minimal subspace polynomial of vector a with q-degree t and $\Lambda_t = 1$. The *key equation* for the decoding algorithm is defined as

$$\Delta(x) = \Lambda(x) \circ S(x) = \Lambda(S(x)) \mod x^{[n-k]}, \tag{1.23}$$

where $\Delta(x) = \sum_{j=0}^{t-1} \Delta_j x^{[i]}$ and $\Delta_j = \sum_{u=0}^{j} \Lambda_u s_{i-u}^{[u]}$ for $j = 0, \ldots, t-1$. We know $deg_q(\Delta) < t$ (the proof can be found in [75]), so the key equation is zero for $t \le i \le n-k-1$ and this gives a linear system of equations

$$\Delta_i = \sum_{j=0}^{i} \lambda_j s_{i-j}^{[j]} = \sum_{j=0}^{t} \Lambda_j s_{i-j}^{[j]} = 0 \ \text{ for } t \le i \le n-k-1. \tag{1.24}$$

Equivalently, it can be represented as the following homogeneous linear system of equations

$$\begin{pmatrix} \Delta_t \\ \Delta_{t+1} \\ \vdots \\ \Delta_{n-k-1} \end{pmatrix} = \tilde{S} \cdot \tilde{\Lambda} = \begin{pmatrix} s_t^{[0]} & s_{t-1}^{[1]} & \cdots & s_0^{[t]} \\ s_{t+1}^{[0]} & s_t^{[1]} & \cdots & s_1^{[t]} \\ \vdots & \vdots & \ddots & \vdots \\ s_{n-k-1}^{[0]} & s_{n-k-2}^{[1]} & \cdots & s_{n-k-1-t}^{[t]} \end{pmatrix} \cdot \begin{pmatrix} \Lambda_0 \\ \Lambda_1 \\ \vdots \\ \Lambda_{t-1} \end{pmatrix} = 0. \tag{1.25}$$

Remember we already know that $\Lambda_t = 1$. It was proven in [75, Lemma 3.9] that matrix $\tilde{S}$ has rank t if $t \le \lfloor (n-k)/2 \rfloor$. So the solution space of (1.25) has dimension one. This can be solved by applying Gaussian elimination and requires $\mathcal{O}(t^3)$ operations over $\mathbb{F}_{q^m}$. Moreover, it can be seen that the matrix $\tilde{S}$ in (1.25) is a submatrix of the Dickson matrix associated to $S(x)$. This observation helped Gabidulin in [17] to apply LEE algorithm and Richter and Plass in [58] to apply BM algorithm and solve (1.25) with $\mathcal{O}(t^2)$ operations over $\mathbb{F}_{q^m}$. Here we will explain the linearized version of BM algorithm to solve (1.25). We can take out the first column of the matrix $\tilde{S}$ and re-arrange (1.25) as

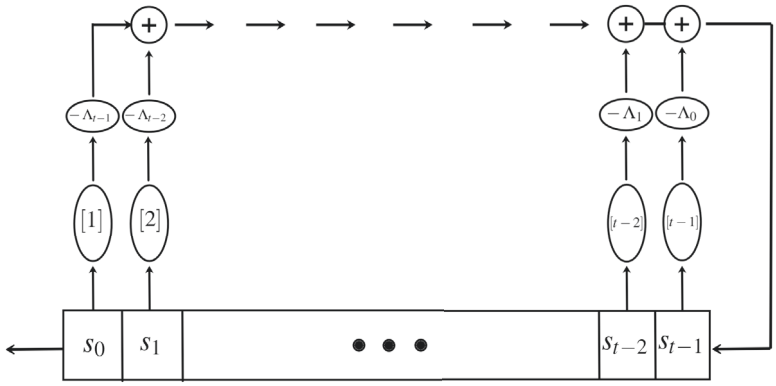

Figure 1.2: linear feedback shift register

$$\begin{pmatrix} s_{t-1}^{[1]} & s_{t-2}^{[2]} & \cdots & s_0^{[t]} \\ s_t^{[1]} & s_{t-1}^{[2]} & \cdots & s_1^{[t]} \\ \vdots & \vdots & \ddots & \vdots \\ s_{2t-2}^{[1]} & s_{2t-3}^{[2]} & \cdots & s_{t-1}^{[t]} \end{pmatrix}_{t\times t} \cdot \begin{pmatrix} \Lambda_0 \\ \Lambda_1 \\ \vdots \\ \Lambda_{t-1} \end{pmatrix} = \begin{pmatrix} -s_t \\ -s_{t+1} \\ \vdots \\ -s_{2t-1} \end{pmatrix}. \tag{1.26}$$

Since the $t \times t$ matrix in (1.26) is formed by t consecutive rows and t consecutive columns of the Dickson matrix associated with $S(x)$, so it has rank t and the above system of equations has a unique solution. It has been shown in [58, 66] that (1.26) can be seen as a *feedback shift register* with $\Lambda_0, \ldots, \Lambda_{t-1}$ to be the connection vector. Considering the $2t$ known syndrome coefficients $s = (s_0, \ldots, s_{2t-1})$ as the output of a shift register, BM algorithm is able to find the t coefficients $\tilde{\Lambda}^T = (\Lambda_0, \ldots, \Lambda_{t-1})$ which is the *shortest feedback shift register* and it is able to generate s. This step is the most dominant step in the decoding process and according to [21], BM algorithm is more efficient for high rate codes and it needs $2t(2t-1)$ operations over $\mathbb{F}_{q^m}$. The shift register is shown in Figure 1.2.

After finding the coefficients of $\Lambda(x)$, we can find the t linearly independent solutions $a_0, \ldots, a_{t-1}$ of $\Lambda(x)$, where $t \leq \lfloor (n-k)/2 \rfloor$. Now it is time to recover the error vector. Employing the $t \times n$ full rank matrix B in (1.22) one can write

$$Y = B \cdot H^T = \begin{pmatrix} y_0 & y_0^{[1]} & \cdots & y_0^{[n-k-1]} \\ y_1 & y_1^{[1]} & \cdots & y_1^{[n-k-1]} \\ \vdots & \vdots & \ddots & \vdots \\ y_{t-1} & y_{t-1}^{[1]} & \cdots & y_{t-1}^{[n-k-1]} \end{pmatrix}. \tag{1.27}$$

Since the rank of B is t, it is easy to verify that $y_0,\ldots,y_{t-1}$ are linearly independent and we can express (1.20) in terms of Y as

$$(s_0,\ldots,s_{n-k-1}) = (a_0,\ldots,a_{t-1})\cdot Y, \tag{1.28}$$

which is equivalent to

$$s_i = \sum_{j=0}^{t-1} a_j y_j^{[i]}, \text{ for } i = 0,\ldots,n-k-1,$$

and raising both sides to the power $[-i]$ gives

$$s_i^{[-i]} = \sum_{j=0}^{t-1} a_j^{[-i]} y_j, \text{ for } i = 0,\ldots,n-k-1. \tag{1.29}$$

Hence we have a system of linear equations with $n-k = 2t$ equations and the same number of variables which can be solved directly. Then we can compute matrix B from (1.27) and consequently the error vector e from (1.22). Finally, we can recover the sent codeword $c = r-e \in \mathcal{G}_{n,k}$. Silva and Kschischang in [72] also showed that using *self-dual normal bases* of $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ can reduce the complexity of low-rate Gabidulin codes.

In [72], the authors used normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and introduced the notion of *multiplication table* of normal basis. This allowed them to reduce the complexity of syndrome computation and also optimized the process of finding a basis for the root space of $\Lambda(x)$. They also showed that using $\mathbb{F}_q$-*self-dual* normal bases of $\mathbb{F}_{q^m}$ can reduce the complexity of decoding low-rate Gabidulin codes.

Puchinger and Wachter-Zeh in [52] presented an algorithm for fast (symbolic) multiplication of linearized polynomials which consequently reduced the complexity of symbolic division. They also derived two divide and conquer approaches for multi-point polynomial evaluation and minimal subspace computation. Moreover, they derived an efficient interpolation algorithm for linearized polynomials. These observations enabled them to propose a fast decoding algorithm for Gabidulin codes and improve the decoding approaches presented in [75]. There is also a different approach proposed in [76] which can be seen as a Gao-like algorithm [22] and uses an equivalent of the Euclidean Algorithm.

There are also several decoding algorithm for *interleaved Gabidulin codes* [33, 48, 49, 55, 67, 69, 70, 78]. Interleaved Gabidulin cods were defined in [33] as follows. Let C be a Gabidulin code with length n, dimension k and minimum distance d over $\mathbb{F}_{q^m}$ and let u be a positive integer. Then the corresponding u-interleaved Gabidulin code is defined as

$$\mathcal{IG}_{n,k} = \left\{ \begin{pmatrix} c^{(1)} \\ \vdots \\ c^{(u)} \end{pmatrix} \mid c^{(i)} \in \mathcal{G}_{n,k} \right\},$$

where u is called the interleaved order. The decoding algorithm proposed for u-interleaved Gabidulin codes are able to decode errors with rank up to $\frac{u(n-k)}{u+1}$. This high rank error decoding

ability can be utilized in rank-based cryptography [15, 20, 56, 77], network coding [57, 68] and space-time coding [3, 18, 38, 51]. The interleaved codes are not in the scope of this thesis so we do not discuss them further.

The main properties of Gabidulin codes that make the syndrome-based decoding approach applicable are the $\mathbb{F}_{q^m}$-linearity property and the Vandermonde form of the parity check matrices. We can define parity check matrix for codes that are not $\mathbb{F}_{q^m}$-linear but how to keep the Vandermonde structure is a challenge and it is not known how to apply syndrome-based decoding approach on MRD families which are not $\mathbb{F}_{q^m}$-linear.

1.6.2 Interpolation-Based Decoding

The first interpolation-based decoding algorithm for Gabidulin codes was given in [34] by Pierre Loidreau. He adapted the Welch-Berlekamp (WB) decoding algorithm, originally proposed for Reed-Solomon codes in [79], for Gabidulin codes. The algorithm was improved later in [2]. Here we recall the decoding algorithm explained in [34].

The author linked the *problem of decoding Gabidulin codes* $D(r, \mathcal{G}_{n,k}(\alpha), t)$ (Problem 2) to the *reconstruction problem of linearized polynomial* $R(r, \alpha, k, t)$.

Problem 3 ($R(r, \alpha, k, t)$)**.** *[32] Suppose two vectors* $r = (r_0, \ldots, r_{n-1}), \alpha = (\alpha_0, \ldots, \alpha_{n-1}) \in \mathbb{F}_{q^m}^n$ *and two positive integers* k, t *are given. Find the set* (g, f) *where* f *is a linearized polynomial with q-degree less than* k *and* g *is a non-zero linearized polynomial with q-degree up to* t*, such that*

$$g(r_i) = g(f(\alpha_i)), \text{ for } i = 0, \ldots, n-1. \tag{1.30}$$

This gives a quadratic system of n *equations and* $k+t+1$ *variables.*

The following theorem gives the relation between the decoding problem and the reconstruction problem.

Theorem 16. *[34] From any solution of reconstruction* $R(r, \alpha, k, t)$*, where* α_i *are linearly independent over* $\mathbb{F}_q$*, one gets a solution to decoding problem* $D(r, \mathcal{G}_{n,k}(\alpha), t)$ *in polynomial time.*

So Loidreau designed an algorithm to solve the reconstruction problem instead of solving the decoding problem. It is not clear how to solve the system given in (1.30), so he considered the following equivalent system: Find the set (g, S), where g, S are linearized polynomial such that

$$\begin{cases} g(r_i) = S(\alpha_i), & \text{for } i = 0, \ldots, n-1 \\ \deg_q(g) \leq t, & \\ \deg_q(S) \leq k+t-1. & \end{cases} \tag{1.31}$$

The current system is a linear system of n equations and $k+2t+1$ unknowns. The following theorem gives the necessary condition to direct the solution of (1.31) to the solution of the system in (1.30).

Theorem 17. *[34] Suppose a non-zero solution exists for* (1.30)*. If* $t \leq \lfloor (n-k)/2 \rfloor$*, then the solution space for the system in* (1.31) *has dimension one and any non-zero solution to* (1.31) *gives a solution to* (1.30)*.*

So based on Theorem 17, the decoding process consists of two steps:

1. Find a set (g, S) as a solution for (1.31);
2. Compute the *symbolic division* S/g, which gives the linearized polynomial $f(x)$ in (1.30). Then the error vector components e_i's can be found as

$$e_i = r_i - f(\alpha_i).$$

The second step conducts a symbolic division operation and as described in [42] it can be computed in polynomial-time. The first step can be done as follows.

The goal of the first step is to find two linearized polynomials g and S which satisfy the system of equations $g(r_i) - S(\alpha_i) = 0$ where $i = 0, \ldots, n-1$. The system is an under-determined system of linear equations of n equations and $n+1$ unknowns. This is equivalent to interpolating two pairs of linearized polynomials (g_0, S_0) and (g_1, S_1). After an initialization step, the polynomials are interpolated via a loop with indices ranging from k to $n-1$. If one manages to bound the q-degree of the polynomials as $\deg_q(g_j) \leq t$ and $\deg_q(S_j) \leq k+t-1$ for $j = 0$ or 1, it is done. The complexity of this step is in the order of $\mathcal{O}(n^2)$ over $\mathbb{F}_{q^m}$.

Bibliography

[1] Daniel Augot, Pierre Loidreau, and Gwezheneg Robert. Rank metric and Gabidulin codes in characteristic zero. In *2013 IEEE International Symposium on Information Theory*, pages 509–513, 2013.

[2] Daniel Augot, Pierre Loidreau, and Gwezheneg Robert. Generalized Gabidulin codes over fields of any characteristic. *Designs, Codes and Cryptography*, 86(8):1807–1848, 2018.

[3] Martin Bossert, Ernst M Gabidulin, and Paul Lusina. Space-time codes based on gaussian integers. In *Proceedings IEEE International Symposium on Information Theory,*, page 273. IEEE, 2002.

[4] Gokhan Calis and O Ozan Koyluoglu. A general construction for pmds codes. *IEEE Communications Letters*, 21(3):452–455, 2016.

[5] B. Csajbók, G. Marino, O. Polverino, and C. Zanella. A new family of MRD-codes. *Linear Algebra and its Applications*, 548:203 – 220, 2018.

[6] Bence Csajbók, Giuseppe Marino, Olga Polverino, and Yue Zhou. MRD codes with maximum idealisers. *DISCRETE MATHEMATICS*, 343(9), 2020.

[7] Bence Csajbók, Giuseppe Marino, and Ferdinando Zullo. New maximum scattered linear sets of the projective line. *Finite Fields and Their Applications*, 54:133 – 150, 2018.

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

[9] Philippe Delsarte and Jean-Marie Goethals. Alternating bilinear forms over GF(q). *Journal of Combinatorial Theory, Series A*, 19(1):26–50, 1975.

[10] L.E. Dickson. *Linear Groups, with an Exposition of the Galois Field Theory - Scholar's Choice Edition*. Creative Media Partners, LLC, 2015.

[11] Cunsheng Ding, Chunlei Li, Nian Li, and Zhengchun Zhou. Three-weight cyclic codes and their weight distributions. *Discrete Mathematics*, 339(2):415–427, 2016.

[12] Cunsheng Ding and Harald Niederreiter. Cyclotomic linear codes of order 3. *IEEE transactions on information theory*, 53(6):2274–2277, 2007.

[13] Kelan Ding and Cunsheng Ding. Binary linear codes with three weights. *IEEE Communications Letters*, 18(11):1879–1882, 2014.

[14] Nicola Durante and Alessandro Siciliano. Non-linear maximum rank distance codes in the cyclic model for the field reduction of finite geometries. *arXiv preprint arXiv:1704.02110*, 2017.

[15] Cédric Faure and Pierre Loidreau. A new public-key cryptosystem based on the problem of reconstructing p–polynomials. In *International Workshop on Coding and Cryptography*, pages 304–315. Springer, 2005.

[16] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In Donald W. Davies, editor, *Advances in Cryptology – EUROCRYPT'91*, pages 482–489. Springer, 1991.

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

[18] Ernst M Gabidulin, Martin Bossert, and Paul Lusina. Space-time codes based on rank codes. In *2000 IEEE International Symposium on Information Theory (Cat. No. 00CH37060)*, page 284. IEEE, 2000.

[19] Ernst M Gabidulin, AV Paramonov, and OV Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In *Advances in Cryptology – EUROCRYPT'91*, pages 482–489. Springer, 1991.

[20] Philippe Gaborit, Ayoub Otmani, and Hervé Talé Kalachi. Polynomial-time key recovery attack on the faure–loidreau scheme based on Gabidulin codes. *Designs, Codes and Cryptography*, 86(7):1391–1403, 2018.

[21] M. Gadouleau and Zhiyuan Yan. Complexity of decoding Gabidulin codes. In *2008 42nd Annual Conference on Information Sciences and Systems*, pages 1081–1085, March 2008.

[22] Shuhong Gao. A new algorithm for decoding reed-solomon codes. In *Communications, information and network security*, pages 55–68. Springer, 2003.

[23] Rod Gow and Rachel Quinlan. Galois theory and linear algebra. *Linear Algebra and its Applications*, 430(7):1778 – 1789, 2009. Special Issue in Honor of Thomas J. Laffey.

[24] Ziling Heng and Qin Yue. A class of binary linear codes with at most three weights. *IEEE Communications Letters*, 19(9):1488–1491, 2015.

[25] H Hoeve, J Timmermans, and LJ Vries. 3.4 error correction and concealment in the compact disc system. *Origins and Successors of the Compact Disc*, page 82, 1982.

[26] Alexander Kshevetskiy and Ernst Gabidulin. The new construction of rank codes. In *International Symposium on Information Theory, (ISIT)*, pages 2105–2108. IEEE, 2005.

[27] Pascal Lefèvre, Philippe Carré, and Philippe Gaborit. Application of rank metric codes in digital image watermarking. *Signal Processing: Image Communication*, 74:119–128, 2019.

[28] ChunLei Li, XiangYong Zeng, and Lei Hu. A class of binary cyclic codes with five weights. *Science China Mathematics*, 53(12):3279–3286, 2010.

[29] Kangquan Li, Chunlei Lia, Tor Helleseth, and Longjiang Qu. Binary linear codes with few weights from two-to-one functions. *IEEE Transactions on Information Theory*, 2021.

[30] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2 edition, 1997.

[31] San Ling and Longjiang Qu. A note on linearized polynomials and the dimension of their kernels. *Finite Fields and Their Applications*, 18(1):56–62, 2012.

[32] Pierre Loidreau. Sur la reconstruction des polynômes linéaires: un nouvel algorithme de décodage des codes de Gabidulin. *Comptes Rendus Mathematique*, 339(10):745–750, 2004.

[33] Pierre Loidreau. Decoding rank errors beyond the error-correcting capability. In *ACCT 2010, Tenth international workshop on Algebraic and Combinatorial Coding Theory*, 2006.

[34] Pierre Loidreau. A Welch–Berlekamp like algorithm for decoding Gabidulin codes. In Øyvind Ytrehus, editor, *International Workshop on Coding and Cryptography (WCC)*, pages 36–45, Berlin, Heidelberg, 2006. Springer.

[35] Giovanni Longobardi, Guglielmo Lunardon, Rocco Trombetti, and Yue Zhou. Automorphism groups and new constructions of maximum additive rank metric codes with restrictions. *Discrete Mathematics*, 343(7):111871, 2020.

[36] Guglielmo Lunardon, Rocco Trombetti, and Yue Zhou. Generalized twisted Gabidulin codes. *Journal of Combinatorial Theory, Series A*, 159:79–106, 2018.

[37] P. Lusina, E. Gabidulin, and M. Bossert. Maximum rank distance codes as space-time codes. *IEEE Transactions on Information Theory*, 49(10):2757–2760, 2003.

[38] Paul Lusina, Ernst Gabidulin, and Martin Bossert. Maximum rank distance codes as space-time codes. *IEEE Transactions on Information Theory*, 49(10):2757–2760, 2003.

[39] Robert J. McEliece and Dilip V. Sarwate. On sharing secrets and reed-solomon codes. *Communications of the ACM*, 24(9):583–584, 1981.

[40] Giampaolo Menichetti. Roots of affine polynomials. In A. Barlotti, M. Biliotti, A. Cossu, G. Korchmaros, and G. Tallini, editors, *Combinatorics '84*, volume 123 of *North-Holland Mathematics Studies*, pages 303–310. North-Holland, 1986.

[41] T Onoda and K Miwa. Hierarchized two-dimensional code, creation method thereof, and read method thereof. *available at Japan Patent Office*, 213336, 2005.

[42] Oystein Ore. On a special class of polynomials. *Transactions of the American Mathematical Society*, 35(3):559–559, 1933.

[43] Oystein Ore. Theory of non-commutative polynomials. *Annals of mathematics*, pages 480–508, 1933.

[44] Kamil Otal and Ferruh Özbudak. Additive rank metric codes. *IEEE Transactions on Information Theory*, 63(1):164–168, 2017.

[45] Kamil Otal and Ferruh Özbudak. Some new non-additive maximum rank distance codes. *Finite Fields and Their Applications*, 50:293 – 303, 2018.

[46] Raphael Overbeck. Extending gibson's attacks on the gpt cryptosystem. In *International Workshop on Coding and Cryptography*, pages 178–188. Springer, 2005.

[47] Raphael Overbeck. Structural attacks for public key cryptosystems based on Gabidulin codes. *Journal of cryptology*, 21(2):280–301, 2008.

[48] Sven Puchinger, Sven Müelich, David Mödinger, Johan Rosenkilde né Nielsen, and Martin Bossert. Decoding interleaved Gabidulin codes using alekhnovich's algorithm. *Electronic Notes in Discrete Mathematics*, 57:175–180, 2017.

[49] Sven Puchinger, Johan Rosenkilde né Nielsen, Wenhui Li, and Vladimir Sidorenko. Row reduction applied to decoding of rank-metric and subspace codes. *Designs, Codes and Cryptography*, 82(1-2):389–409, 2017.

[50] Sven Puchinger, Johan Rosenkilde, and John Sheekey. Further generalisations of twisted Gabidulin codes. In *Proceedings of the 10th International Workshop on Coding and Cryptography*, 2017.

[51] Sven Puchinger, Sebastian Stern, Martin Bossert, and Robert FH Fischer. Space-time codes based on rank-metric codes and their decoding. In *2016 International Symposium on Wireless Communication Systems (ISWCS)*, pages 125–130. IEEE, 2016.

[52] Sven Puchinger and Antonia Wachter-Zeh. Fast operations on linearized polynomials and their applications in coding theory. *Journal of Symbolic Computation*, 89:194 – 215, 2018.

[53] Tovohery Hajatiana Randrianarisoa. A decoding algorithm for rank metric codes. *arXiv.org.*, abs/1712.07060, 2017.

[54] Irving S Reed and Gustave Solomon. Polynomial codes over certain finite fields. *Journal of the society for industrial and applied mathematics*, 8(2):300–304, 1960.

[55] Julian Renner, Sven Puchinger, and Antonia Wachter-Zeh. Decoding high-order interleaved rank-metric codes. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 19–24. IEEE, 2021.

[56] Julian Renner, Sven Puchinger, and Antonia Wachter-Zeh. Liga: a cryptosystem based on the hardness of rank-metric list and interleaved decoding. *Designs, Codes and Cryptography*, 89(6):1279–1319, 2021.

[57] Julian Renner, Sven Puchinger, and Antonia Wachter-Zeh. Liga: a cryptosystem based on the hardness of rank-metric list and interleaved decoding. *Designs, Codes and Cryptography*, 89(6):1279–1319, 2021.

[58] G. Richter and S. Plass. Fast decoding of rank-codes with rank errors and column erasures. In *International Symposium on Information Theory (ISIT)*, pages 398–398, June 2004.

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

[60] Kai-Uwe Schmidt. Symmetric bilinear forms over finite fields of even characteristic. *Journal of Combinatorial Theory, Series A*, 117(8):1011–1026, 2010.

[61] Kai-Uwe Schmidt. Symmetric bilinear forms over finite fields with applications to coding theory. *Journal of Algebraic Combinatorics*, 42(2):635–670, 2015.

[62] Kai-Uwe Schmidt. Hermitian rank distance codes. *Designs, Codes and Cryptography*, 86(7):1469–1481, 2018.

[63] John Sheekey. A new family of linear maximum rank distance codes. *Advances in Mathematics of Communications*, 10:475, 2016.

[64] John Sheekey. New semifields and new MRD codes from skew polynomial rings. *Journal of the London Mathematical Society*, 101(1):432–456, 2020.

[65] Priyanka Shrivastava and Uday Pratap Singh. Error detection and correction using reed solomon codes. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(8), 2013.

[66] V. Sidorenko, G. Richter, and M. Bossert. Linearized shift-register synthesis. *IEEE Transactions on Information Theory*, 57(9):6025–6032, Sep. 2011.

[67] Vladimir Sidorenko and Martin Bossert. Decoding interleaved Gabidulin codes and multisequence linearized shift-register synthesis. In *2010 IEEE International Symposium on Information Theory*, pages 1148–1152. IEEE, 2010.

[68] Vladimir Sidorenko and Martin Bossert. Decoding interleaved Gabidulin codes and multisequence linearized shift-register synthesis. In *2010 IEEE International Symposium on Information Theory*, pages 1148–1152. IEEE, 2010.

[69] Vladimir Sidorenko and Martin Bossert. Fast skew-feedback shift-register synthesis. *Designs, Codes and Cryptography*, 70(1):55–67, 2014.

[70] Vladimir Sidorenko, Lan Jiang, and Martin Bossert. Skew-feedback shift-register synthesis and decoding interleaved Gabidulin codes. *IEEE transactions on information theory*, 57(2):621–632, 2011.

[71] D. Silva, F. R. Kschischang, and R. Koetter. A rank-metric approach to error control in random network coding. *IEEE Transactions on Information Theory*, 54(9):3951–3967, Sept 2008.

[72] Danilo Silva and Frank R Kschischang. Fast encoding and decoding of Gabidulin codes. In *International Symposium on Information Theory (ISIT)*, pages 2858–2862. IEEE, 2009.

[73] R. Singleton. Maximum distanceq-nary codes. *IEEE Transactions on Information Theory*, 10(2):116–118, 1964.

[74] R. Trombetti and Y. Zhou. A new family of MRD codes in $\mathbb{F}_q^{2n\times 2n}$ with right and middle nuclei $\mathbb{F}_{q^n}$. *IEEE Transactions on Information Theory*, 65(2):1054–1062, 2019.

[75] Antonia Wachter-Zeh. Decoding of block and convolutional codes in rank metric, 2013.

[76] Antonia Wachter-Zeh, Valentin Afanassiev, and Vladimir Sidorenko. Fast decoding of Gabidulin codes. *Designs, Codes and Cryptography*, 66(1-3):57–73, 2013.

[77] Antonia Wachter-Zeh, Sven Puchinger, and Julian Renner. Repairing the faure-loidreau public-key cryptosystem. In *2018 IEEE International Symposium on Information Theory (ISIT)*, pages 2426–2430. IEEE, 2018.

[78] Antonia Wachter-Zeh and Alexander Zeh. List and unique error-erasure decoding of interleaved Gabidulin codes with interpolation techniques. *Designs, codes and cryptography*, 73(2):547–570, 2014.

[79] Lloyd R Welch and Elwyn R Berlekamp. Error correction for algebraic block codes, December 30 1986. US Patent 4,633,470.

[80] William Wu, David Haccoun, Robert Peile, and Yasuo Hirata. Coding for satellite communication. *IEEE Journal on selected areas in communications*, 5(4):724–748, 1987.

Chapter 2

Introduction

In this chapter we give a high overview of the results presented in this document.

2.1 Interpolation-based Decoding Algorithms for New Rank Metric Codes

Randrianarisoa in [36] proposed a new interpolation-based decoding approach to decode Gabidulin codes and GTG codes. His algorithm later adapted to decode AGTG codes [22], TZ codes [23], optimal symmetric, alternating and Hermitian rank metric codes [24]. This algorithm uses Berlekamp-Massey algorithm described in 1.6.1 but in a different way. Here we give a brief explanation of the decoding algorithm for MRD codes of length n and dimension k that can be represented by a set of all linearized polynomials $f(x) = \sum_{i=0}^{k} f_i x^{[i]} \in \mathcal{L}_n(\mathbb{F}_{q^m})$ of q-degree at most k satisfying certain properties (TG, GTG, AGTG, TZ). For simplicity we consider $n = m$ in all the decoding algorithms described in Chapters 3-6. Let the code be defined on field extension $\mathbb{F}_{q^m}$. First we use the message vector $a = (a_0, \ldots, a_{k-1}) \in \mathbb{F}_{q^m}^k$ as the $k+1$-coefficient vector of $f(x)$ where the coefficients f_0 and f_k are derived from a_0. We evaluate the polynomial $f(x)$ on linearly independent points $\alpha_0, \ldots, \alpha_{m-1} \in \mathbb{F}_{q^m}$ and get the codeword c. The error vector e of rank $t \leq \frac{m-k}{2}$ is also derived by a linearized polynomial $g(x) = \sum_{i=0}^{m-1} g_i x^{[i]} \in \mathcal{L}_m(\mathbb{F}_{q^m})$ on the same linearly independent points $\alpha_0, \ldots, \alpha_{m-1}$. Let r be the received word and so as in (1.8) one can write $r = c + e = (\tilde{f} + \tilde{g}) \cdot M^T$ where M is the Moore matrix corresponding to the linearly independent evaluation points $\alpha_0, \ldots, \alpha_{m-1}$ and $\tilde{f} = (f_0, \ldots, f_k, 0, \ldots, 0)$ and $\tilde{g} = (g_0, \ldots, g_{m-1})$ are coefficient vectors of polynomials $f(x)$ and $g(x)$. Since M is non-singular we can calculate

$$\beta = r \cdot (M^T)^{-1} = f + g.$$

Due to the form $f(x)$ (it has degree k at most) we already know $m-k-1$ coefficients of $g(x)$ and in order to find the k unknown coefficients $g_0, \ldots, g_k$ we use the properties of the Dickson matrix $G(x)$ (Proposition 1) associated with $g(x)$. We know the error interpolation polynomial

$g(x)$ has rank t, any $t \times t$ submatrix of $G(x)$ formed by t consecutive rows and columns is nonsingular. If we write the first row of the Dickson matrix as a linear combination of the next t rows, we will get a linear system of equation of the form

$$g_i = \gamma_1 g_{i-1}^{[1]} + \gamma_2 g_{i-2}^{[2]} + \cdots + \gamma_t g_{i-t}^{[t]}, \quad 0 \leq i < m, \tag{2.1}$$

where the subscripts in g_i's are taken modulo m. We already know $g_{k+1}, \ldots, g_{m-1}$ and these known coefficients leads us to the following linear recursive equation

$$g_i = \gamma_1 g_{i-1}^{[1]} + \gamma_2 g_{i-2}^{[2]} + \cdots + \gamma_t g_{i-t}^{[t]}, \; k+t \leq i < m, \tag{2.2}$$

where $\gamma_0 \ldots, \gamma_t$ are unknowns. We divided the process in to two cases. In the first case when the rank of the error vector is $t < \frac{m-k}{2}$, the linear system in (2.2) has $\geq t$ equations with t variables and the BM algorithm described in 1.6.1 can solve the problem. In the second case when the rank of the error vector is $t = \frac{m-k}{2}$, the system in (2.2) will be an under-determined system with $t-1$ equations and t variables. Again the system can be solved using the BM algorithm described in [40] and one can get a one dimensional solution space with a free variable $\omega \in \mathbb{F}_{q^m}$.

2.1.1 Decoding of AGTG Codes

In the decoding algorithms for GTG in [36] and also for AGTG codes in Chapter 3, the relations between f_0 and f_k in the polynomial $f(x)$ and (2.1) will give the following projective polynomial with variable ω

$$P(\omega) = u_0 \omega^{q^v+1} + u_1 \omega^{q^v} + u_2 \omega + u_3 = 0. \tag{2.3}$$

In other words, When the rank of the error vector e meets the unique decoding radius, the decoding problems in [36] and Chapter 3 are reduced to the problem of solving a projective polynomial equation over $\mathbb{F}_{q^m}$. The solutions of $P(\omega) = 0$ when $u_0 = 0$ will be discussed in Chapter 3. When $u_0 \neq 0$, we can transform $P(x) = 0$ into a polynomial equation

$$q(x) = x^{q^u+1} + bx + a = 0, \text{ for } a, b \in \mathbb{F}_{q^m}. \tag{2.4}$$

The polynomial $q(x)$ has arisen in several different contexts [1, 5, 6, 7, 17, 18, 28, 42]. Bluher in [4] showed that $q(x)$ can have either $0, 1, 2$ or $q^d + 1$ zeros in $\mathbb{F}_{q^m}$ where $d = gcd(u, m)$. In Chapter 3, we first generalize the idea in [16] for any prime power q and write the roots of $q(x)$ in terms of three known roots of $q(x)$ in $\mathbb{F}_{q^m}$. Then we divide the discussion into two cases when q is even and when q is odd and $d = 1$. For the former case, we employe the result in [20] and explicitly give the root of $q(x)$ when it has a unique solution. For the latter case, we recall the criteria given in [30] for $q(x)$ to have $0, 1, 2$ and $q^d + 1$ solutions in $\mathbb{F}_{q^m}$. In [30], the authors noticed that $q(x)$ associates with the linearized polynomial

$$L(x) = xq(x^{q^u-1}) = x^{q^{2u}} + bx^{q^u} + ax, \; a, b \in \mathbb{F}_{q^m}, \tag{2.5}$$

and they used companion matrices to find the zeros of $L(x)$. In Chapter 3, we converted the task of finding zeros of $L(x)$ to the task of finding the determinant of Dickson matrix associated with $L(x)$. This was done by adapting the idea of Csajbók in [11, Corollary 3.4] which provided a

characterization for the rank of Dickson matrix. We provide a deterministic algorithm to solve linearized polynomial equations over $\mathbb{F}_{q^m}$ when $gcd(m,u)=1$. A probabilistic algorithm to solve $L(x)=0$ was proposed in [41]. Roots of linearized polynomials were also investigated in [12, 35].

Very recently, Kim, Choe and Mesnager in [26, 27] provided a complete solution for $q(x)=0$ over $\mathbb{F}_{q^m}$ without any restriction on q and $gcd(m,u)$. Their result will also make the decoding algorithms in [36] and [22] (Chapter 3) complete. Here we recall their result where, without loss of generality, they considered $b=1$ in $q(x)$, i.e.,

$$q(x)=x^{q^u+1}+x+a,\ \ a\in\mathbb{F}_{q^m}. \tag{2.6}$$

Let $d=gcd(m,u)$ and $k=m/d$. In [27], they defined the sequence of polynomials $\{A_r(x)\}$ in $\mathbb{F}_q[x]$ and polynomials $F(x)$ and $G(x)$ as follows:

$$\begin{aligned} A_1(x)&=1,\ A_2(x)=-1\\ A_{r+2}(x)&=-A_{r+1}(x)^{q^u}-x^{q^u}A_r(x)^{q^{2u}},\ \text{for } r\geq 1\\ F(x)&=A_k(x)\\ G(x)&=-A_{k+1}(x)-xA_{k-1}^{q^u}(x). \end{aligned}$$

They showed that if $p=2$ then $G(x)\in\mathbb{F}_{q^u}$ for any $x\in\mathbb{F}_{q^k}$ and if $F(a)\neq 0$ then $q(x)$ has at most two solutions in $\mathbb{F}_{q^m}$. One can find the zeros of $q(x)$ from the following two theorems when $F(a)\neq 0$.

Theorem 18. *[27, Theorem 9] Let p be an odd integer and $E=G(a)^2-4aF(a)^{q^u+1}$ then*

1. *$q(x)$ has no solution if and only if E is not a non-zero quadratic residue in $\mathbb{F}_{q^d}$.*
2. *$q(x)$ has a single solution of the form $x=-\frac{G(a)}{2F(a)}$ if and only if $F(a)\neq 0$ and $E=0$.*
3. *$q(x)$ has two solutions of the forms $x_{1,2}=\frac{\pm E^{1/2}-G(a)}{2F(a)}$ if and only if E is a non-zero quadratic residue in $\mathbb{F}_{q^d}$.*

Theorem 19. *[27, Theorem 11] Let p be an even integer, $H=\mathrm{Tr}_{q^d/q}(\frac{\mathrm{Norm}_{q^m/q^d}(a)}{G^2(a)})$ and $E=\frac{aF(a)^{q^u+1}}{G^2(a)}$, then $q(x)$*

1. *has no solution if and only if $G(a)\neq 0$ and $H\neq 0$.*
2. *has a single solution of the form $x=(aF(a)^{q^u-1})^{1/2}$ if and only if $F(a)\neq 0$ and $G(a)=0$.*
3. *has two solutions of the forms $x_1=\frac{G(a)}{F(a)}\cdot\mathrm{Tr}_{q^m/q}(\frac{E}{\lambda+1})$ and $x_2=x_1+\frac{G(a)}{F(a)}$, where $\lambda\in\{z\in\mathbb{F}_{q^{2m}}|z^{q^m+1}=1\}\setminus\{1\}$, if and only if $G(a)\neq 0$ and $H=0$.*

As we already mentioned, for $q(x)$ to have q^d+1 solutions in $\mathbb{F}_{q^m}$, we must first assume $F(a)=0$. The following theorem covers the remaining case (q^d+1 solutions) for an arbitrary prime integer p.

Theorem 20. *[26, Theorem 18] Let* $A_k(a) = 0$, $N = k(q^d - 1)$, $s = \frac{(q^{uk}-1)\cdot(q^d-1)}{(q^m-1)\cdot(q^u-1)}$, $G_1(X) = \sum_{i=0}^{k-2} A_{k-1-i}(a)^{q^{u(i+1)}} \cdot X^{q^{ui}}$ *and* $G_2(X) = \sum_{i=0}^{q^d-2} B_k(a)^{q^d-2-i} \cdot X^{q^{uki}}$. *It holds* $G_1(G_2(\mathbb{F}^*_{q^N})^s \cdot \mathbb{F}^*_{q^u} \cdot \mathbb{F}^*_{q^m})^{q^u-1} \neq 0$. *Choose an arbitrary* $y_0 \in G_1(G_2(\mathbb{F}^*_{q^N})^s \cdot \mathbb{F}^*_{q^u} \cdot \mathbb{F}^*_{q^m})^{q^u-1} \setminus \{0\}$, *then* y_0^2/a *would be a* (q^u-1)*-th power in* $\mathbb{F}_{q^m}$. *For* $\beta \in \mathbb{F}_{q^m}$ *such that* $\beta^{q^u-1} = y_0^2/a$, *the equation*

$$\omega^{q^u} - \omega + \frac{1}{\beta y_0} = 0, \tag{2.7}$$

had exactly q^d *solutions in* $\mathbb{F}_{q^m}$. *Let* ω_0 *be a solution of* (2.7) *in* $\mathbb{F}_{q^m}$. *Then the* q^d *solutions of* $q(x)$ *in* $\mathbb{F}_{q^m}$ *are* y_0 *and* $(\omega_0 + a\alpha)^{q^u-1} \cdot y_0$ *where* α *runs over* $\mathbb{F}_{q^d}$.

The equation (2.7) was previously solved in [32] and now we can identify all the solutions of the projective polynomial equation $q(x)$ if one of the solutions (previously denoted by y_0) is known. Under such condition, we can say the decoding algorithms proposed for TG, GTG and $AGTG$ codes work for any parameter over finite fields of an arbitrary characteristic.

2.1.2 Decoding of TZ Codes

In Chapter 4, we show that TZ codes can be decoded much faster than GTG and AGTG codes. In our proposed decoding algorithm we derive some relations between the coefficients f_0 and f_k in the evaluation polynomial. Using the obtained relations with equation (2.1) we can write the following quadratic equation in terms of ω

$$\omega^2 + a\omega + b = 0, \tag{2.8}$$

instead of the projective polynomial equation (2.3) which is obtained for AGTG codes in Chapter 3. Comparing the final equations in (2.3) and (2.8), one can see a significant difference between the complexities of solving these two equations and this will consequently affect the complexities of decoding AGTG codes and TZ codes. We also describe that (2.8) can be solved in polynomial time.

2.1.3 Decoding of MRD codes beyond half the minimum distance

In Chapter 5, an improvement of decoding GTG and AGTG codes is proposed. Moreover, we managed to decode rank errors beyond half the minimum distance by one unit. We suggested two new communication models which use constrained error interpolation polynomials instead of an arbitrary polynomial $g(x) \in \mathcal{L}_m(\mathbb{F}_{q^m})$ of rank t. This work was inspired by a paper of Pilipchuk and Gabidulin [34] which decoded symmetric error vectors and a paper by Jerkovits *et al.*[21] that targeted space-symmetric error vectors. Let $t \leq \frac{d-1}{2}$ and suppose α_{θ_1} and α_{θ_2} be two specific elements in $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$ where and $0 \leq \theta_1 < \theta_2 < m$. Using a polynomial

of the form

$$e_{\theta_1,\theta_2}(x) = \sum_{i=0}^{m-1} z_i x^{[i]},\ z_i \in \mathbb{F}_{q^m},$$
$$z_0^{[m/2]} - z_0 = \alpha_{\theta_1},$$
$$z_{k-1}^{[m/2]} - z_{k-1} = \alpha_{\theta_2},$$

as the error interpolation polynomial enables us to decode rank errors, with $\mathrm{Rank}(e) \leq t+1$, added to Gabidulin codeword in polynomial-time. Moreover, decoding problems of GTG and AGTG codes are reduced to the problem of solving a quadratic polynomial equation instead of a projective polynomial equation. We also showed that using a more restricted error interpolation polynomial, we will be able to decode any rank errors up to $t \leq k$ added to GTG or AGTG codewords.

2.1.4 Encoding and decoding of optimal rank metric codes with restrictions

Neither encoding nor decoding algorithms are given for the the optimal symmetric, alternating and Herimitian rank metric codes in the literature. In Chapter 6, we first prove that the interpolation encoding is the right encoding approach for these new optimal rank metric codes and then we provide interpolation-based polynomial-time encodings for each of them. We introduce the notion of Hermitian dual bases and use them as the set of linearly independent evaluation points in the encoding process for optimal hermitian rank metric codes. The bounds in Theorems 9,10 and 11 are used as alternatives for Singleton bound. We also adapt the interpolation-based decoding approach, described in the beginning of Section 2.1, for optimal symmetric, alternating and Hermitian rank metric codes.

2.2 Construction of binary linear codes from Boolean functions

Vectorial Boolean functions are functions from $\mathbb{F}_{2^m}$ to itself. They are of central interest in cryptography since they can be used to represent virtually all components of a block cipher; in particular, its nonlinear components can be expressed as vectorial Boolean functions. They have important applications in coding theory and they have been used to construct binary linear codes [8, 9, 25, 33, 37]. Ding in [15] proposed the following generic constructions of binary linear codes from Boolean functions and he also suggested several open problems based on his construction.

Let $D = \{d_1, \ldots, d_n\} \subseteq \mathbb{F}_{2^m}$ be the defining set. He defined a binary linear code of length n associated to D by

$$C_D = \{(\mathrm{Tr}_{2^m/2}(ad_1), \ldots, \mathrm{Tr}_{2^m/2}(ad_n)) \mid a \in \mathbb{F}_{2^m}\}.$$

The dimension of the code C_D is at most m. Choosing the defining set properly will give most of the known codes. Ding in [15] studied the images of some certain Boolean functions on $\mathbb{F}_{2^m}$ and derived the properties of some binary linear codes with few weights. Here we recall some necessary terms in order to understand the contribution of Chapter 6.

Let F be a Boolean function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. The support of F is defined as

$$D_F = \{x \in \mathbb{F}_{2^m} : F(x) = 1\} \subseteq \mathbb{F}_{2^m}.$$

The Hamming weight of $c_x = (\mathrm{Tr}(xd_1), \ldots, \mathrm{Tr}(xd_n))$ is $n - N_x(0)$ where for each $x \in \mathbb{F}_{2^m}$ we have $N_x(0) = |\{1 \leq i \leq n : \mathrm{Tr}(xd_i) = 0\}|$.

The derivative of F in direction of any $a \in \mathbb{F}_{2^m}$ is the function $D_aF : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ and it is defined as $D_a F(x) = F(x+a) + F(x)$. For any $a, b \in \mathbb{F}_{2^m}$ we define $N_F(a,b) = |\{x \in \mathbb{F}_{2^m} | F(x+a) + F(x) = b\}|$; i.e., $N_F(a,b)$ is the number of solutions x of the equation $D_aF(x) = b$ for some given a and b. Then the *differential uniformity* of F is defined as $\Delta_F = \max\{N_F(a,b) | a, b \in \mathbb{F}_{2^m}$ and $a \neq 0\}$.

A function F is called *deferentially δ-uniform* if $\Delta_F \leq \delta$. If $\delta = 2$ then F is almost perfect nonlinear (APN). This is optimal for finite fields of even characteristic since if x solves $F(x+a) + F(x) = b$, then so does $(x+a)$, and it means $N_F(a,b)$ is always even. Let $\omega_i = |\{(a,b) \in \mathbb{F}^*_{2^m} \times \mathbb{F}_{2^m} | N_F(a,b) = i\}|$ and δ be the differential uniformity of $F(x)$, then the *differential spectrum* of $F(x)$ is defined as the multi-set $\Omega_F = \{\omega_0, \ldots, \omega_\delta\}$.

A number of useful characterizations of APN functions can be given in terms of the so-called Walsh transform. The *Walsh transform* of $F(x)$ at (a,b) is defined as

$$W_F(a,b) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}(aF(x)+bx)},$$

and the *Walsh Spectrum* of $F(x)$ is defined as the multi-set $\Lambda_F = \{W_F(a,b) : a, b \in \mathbb{F}_{2^m}, a \neq 0\}$. A powerful attack against block ciphers is linear cryptanalysis, introduced by Matsui in [29]. The property of a function which measures the resistance to this kind of attack is called *non-linearity* which can be defined in terms of Walsh transform as

$$NL(F) = 2^{n-1} - \frac{1}{2} \max\{|W_F(a,b)| : a, b \in \mathbb{F}_{2^m}, a \neq 0\}.$$

For cryptographic applications, a vectorial Boolean function is required to have high non-linearity and low differential uniformity. The following theorem in [14] establishes a connection between Boolean functions F such that $2n_F + W_F(a,b) \neq 0$,for all $a, b \in \mathbb{F}^*_{2^m}$, and binary linear codes.

Theorem 21. *[14] Let F be a function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ and let D_F be the support of F. If $2n_F + W_F(a,b) \neq 0$ for all $a, b \in \mathbb{F}^*_{2^m}$, then C_{D_F} is a binary linear code with length n_F and dimension m. The weight distribution of C_{D_F} is given by the multiset*

$$\left\{ \frac{2n_F + W_F(a,b)}{4} : a, b \in \mathbb{F}^*_{2^m} \right\} \cup \{0\}.$$

Based on the connection in Theorem 21, determining the Walsh spectrum of F satisfying $2n_F + W_F(a,b) \neq 0$ for all $a,b \in \mathbb{F}_{2^m}^*$ is equivalent to the that of the weight distribution of of the binary linear code C_{D_F}. When the Boolean function F is chosen properly, it will give a binary linear code C_{D_F} with few weights.

We studied the differential spectrum and Walsh spectrum of $g(x) = x^{2^{n+1}+1} + x^3 + x$ over $\mathbb{F}_{2^{2n+1}}$ for an integer $n \geq 2$ in Chapter 7. The polynomial $g(x)$ is known as *Welch permutation polynomial*. Employing the Walsh transform of $g(x)$ and determining its Walsh spectrum enables us to derive the weight distribution of the code C_{D_g} constructed in [15, Conjecture 33] and partially solve the conjecture.

2.3 Linear codes with maximum non-zero distinct weights

Let $S(C)$ be the set of non-zero weights of a block code C. The parameter $S(C)$ has been considered for different purposes in the literature. For instance, Delsarte in [13] employed $S(C)$ and derived some properties of linear block codes. Binary linear codes with distinct non-zero weights was studied in [19] and later Shi *et al.*in [39], independently studied the problem of determining the maximum possible number of distinct weights in a block code (not necessarily linear) over a finite field with arbitrary characteristic. We denote the maximum number of distinct nonzero weights for an $[n,k,d]_q$ linear code by $N_{q,k}$. Shi *et al.*in [39] proposed the following upper bounds for $[n,k,d]_q$ linear codes.

Theorem 22. *[39] For all nonegative integers k,m and all prime powers q we have*

- $N_{q,k} \leq N_{q,k+1}$;
- $N_{q,k} \leq N_{q^m,k}$,

and for all prime powers q and integers $k \geq 1$ we have

$$N_{q,k} \leq \frac{q^k - 1}{q-1}. \tag{2.9}$$

They also conjectured the existence of linear codes that attain the bound in (2.9). Later in [3] and [31] two constructions for codes that attain this bound were given. Alderson and Neri in [3] named the linear codes with $N_{q,k} = \frac{q^k-1}{q-1}$ as *maximum weight spectrum (MWS)* codes. Codes with shorter length for a given dimension were later proposed in [2, 10].

Beside the upper bounds for $N_{q,k}$, we also saw the following lower bounds in [39].

Theorem 23. *[39] For all prime powers q we have*

- $k \leq N_{q,k}$ *for all integers* $k \geq 1$,
- $N_{q,k+1} \geq 2N_{q,k} + 1$ *for all integers* $k \geq 1$,
- $N_{q,k} \geq 2^{k-1}q + 2^{k-2} + 1$ *for all integers* $k \geq 2$.

An analogue of the function $N_{q,k}$ was defined in [39] for nonlinear codes of size M over an alphabet of size q and we denote it as $\tilde{N}_{q,M}$. We can find that $\tilde{N}_{q,M} = \binom{M}{2}$ in [39]. In [38]

the maximum number of nonzero weights for cyclic codes is discussed. In Chapter 8, we introduce two new subfamilies for MWS codes according to their weight distribution. The call the new sub-families as *compact* and *strictly compact* MWS codes. We also define the concept of spread for MWS codes and investigate their properties accordingly.

Definition 33. *Let C be an $[n,k,d]$ MWS code over $\mathbb{F}_q$ and let $N_{q,k} = \frac{q^k-1}{q-1}$. Then C is called a compact MWS code if $S(C) = \{d, d+1, \ldots, d+N_{q,k}-1\}$. Furthermore, a compact MWS C' is called strictly compact if $n \in S(C')$, i.e., $S(C') = \{d, d+1, \ldots, n\}$.*

Using the new defined parameter *spread* for MWS codes, we can examine how the weights of the MWS code is distributed across the set $\{1, \ldots, n\}$.

Definition 34. *Let C be an $[n,k,d]$ MWS code over $\mathbb{F}_q$. The spread of C with $S(C) = \{n - s_0, n - s_1, \ldots, n - s_{N_{q,k}-1}\}$ is defined as*

$$\Delta(C) = (s_0 - 0) + (s_1 - 1) + \cdots + (s_{N_{q,k}-1} - N_{q,k} + 1) \sum_{i=0}^{N_{q,k}-1} (s_i - 1).$$

From Definition 33, one can verify that a strictly compact MWS code C has $\Delta(C) = 0$ and it is optimal. In Chapter 8, we investigate the properties and parameters of compact and strictly compact MWS codes.

Bibliography

[1] Shreeram S. Abhyankar. Projective polynomials. *Proceedings of the American Mathematical Society*, 125(6):1643–1650, 1997.

[2] Tim Alderson. A note on full weight spectrum codes. *Transactions on Combinatorics*, 8(3):15–22, 2019.

[3] Tim L Alderson and Alessandro Neri. Maximum weight spectrum codes. *arXiv preprint arXiv:1803.04020*, 2018.

[4] Antonia W Bluher. On $x^{q+1}+ax+b$. *Finite Fields and Their Applications*, 10(3):285 – 305, 2004.

[5] C. Bracken and T. Helleseth. Triple-error-correcting BCH-like codes. In *2009 IEEE International Symposium on Information Theory*, pages 1723–1725, 2009.

[6] Carl Bracken, Chik How Tan, and Yin Tan. On a class of quadratic polynomials with no zeros and its application to apn functions. *Finite Fields and Their Applications*, 25:26–36, 2014.

[7] L. Budaghyan and C. Carlet. Classes of quadratic apn trinomials and hexanomials and related structures. *IEEE Transactions on Information Theory*, 54(5):2354–2357, 2008.

[8] Claude Carlet. A simple description of kerdock codes. In *International Colloquium on Coding Theory and Applications*, pages 202–208. Springer, 1988.

[9] Claude Carlet. The automorphism groups of the kerdock codes. *Journal of Information and Optimization Sciences*, 12(3):387–400, 1991.

[10] Gérard D. Cohen and Ludo Tolhuizen. Maximum weight spectrum codes with reduced length. *CoRR*, abs/1806.05427, 2018.

[11] Bence Csajbók. Scalar q-subresultants and Dickson matrices. *Journal of Algebra*, 547:116–128, 2020.

[12] Bence Csajbók, Giuseppe Marino, Olga Polverino, and Ferdinando Zullo. A characterization of linearized polynomials with maximum kernel. *Finite Fields and Their Applications*, 56:109 – 130, 2019.

[13] Philippe Delsarte. Four fundamental parameters of a code and their combinatorial significance. *Information and Control*, 23(5):407–438, 1973.

[14] Cunsheng Ding. Linear codes from some 2-designs. *IEEE Transactions on information theory*, 61(6):3265–3275, 2015.

[15] Cunsheng Ding. A construction of binary linear codes from boolean functions. *Discrete mathematics*, 339(9):2288–2303, 2016.

[16] H. Dobbertin, P. Felke, T. Helleseth, and P. Rosendahl. Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums. *IEEE Transactions on Information Theory*, 52(2):613–627, Feb 2006.

[17] Faruk Göloğlu, Robert Granger, Gary McGuire, and Jens Zumbrägel. On the function field sieve and the impact of higher splitting probabilities. In *Annual Cryptology Conference*, pages 109–128. Springer, 2013.

[18] Faruk Göloğlu, Robert Granger, Gary McGuire, and Jens Zumbrägel. Solving a 6120 -bit dlp on a desktop computer. In *International Conference on Selected Areas in Cryptography*, pages 136–152. Springer, 2013.

[19] Abdelfattah Haily, Driss Harzalla, et al. On the automorphism group of distinct weight codes. *Intelligent Information Management*, 7(02):80, 2015.

[20] Tor Helleseth and Alexander Kholosha. $x^{2^l+1}+x+a$ and related affine polynomials over GF(2^k). *Cryptography and Communications*, 2(1):85–109, 2010.

[21] Thomas Jerkovits, Vladimir Sidorenko, and Antonia Wachter-Zeh. Decoding of space-symmetric rank errors, 2021.

[22] Wrya K. Kadir and Chunlei Li. On decoding additive generalized twisted Gabidulin codes. *Cryptography and Communications*, 12:987 – 1009, 2020.

[23] Wrya K. Kadir, Chunlei Li, and Ferdinando Zullo. On interpolation-based decoding of a class of maximum rank distance codes. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 31–36, 2021.

[24] Wrya K Kadir, Chunlei Li, and Ferdinando Zullo. Encoding and decoding of several optimal rank metric codes. *Cryptography and Communications*, pages 1–20, 2022.

[25] Anthony M Kerdock. A class of low-rate nonlinear binary codes. *Information and control*, 20(2):182–187, 1972.

[26] Kwang Ho Kim, Jong Hyok Choe, and Sihem Mesnager. Complete solution over GFp^n of the equation $x^{p^k+1}+x+a=0$. *arXiv.org.*, abs/2101.01003, 2021.

[27] Kwang Ho Kim, Junyop Choe, and Sihem Mesnager. Solving xq+ 1+ x+ a= 0 over finite fields. *Finite Fields and Their Applications*, 70:101797, 2021.

[28] Maike Massierer. Some experiments investigating a possible l (1/4) algorithm for the discrete logarithm problem in algebraic curves. 2014.

[29] Mitsuru Matsui. Linear cryptanalysis method for des cipher. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 386–397. Springer, 1993.

[30] Gary McGuire and John Sheekey. A characterization of the number of roots of linearized and projective polynomials in the field of coefficients. *Finite Fields and Their Applications*, 57:68 – 91, 2019.

[31] Alessio Meneghetti. On linear codes and distinct weights. *arXiv preprint arXiv:1804.04373*, 2018.

[32] Sihem Mesnager, Kwang Ho Kim, Jong Hyok Choe, and Dok Nam Lee. Solving some affine equations over finite fields. *Finite Fields and Their Applications*, 68:101746, 2020.

[33] David E Muller. Application of boolean algebra to switching circuit design and to error detection. *Transactions of the IRE professional group on electronic computers*, (3):6–12, 1954.

[34] Nina I Pilipchuk and Ernst M Gabidulin. On codes correcting symmetric rank errors. In *International Workshop on Coding and Cryptography*, pages 14–21. Springer, 2005.

[35] Olga Polverino and Ferdinando Zullo. On the number of roots of some linearized polynomials. *arXiv e-prints*, page arXiv:1909.00802, September 2019.

[36] Tovohery Hajatiana Randrianarisoa. A decoding algorithm for rank metric codes. *arXiv.org.*, abs/1712.07060, 2017.

[37] Irving S Reed. A class of multiple-error-correcting codes and the decoding scheme. Technical report, Massachusetts Inst of Tech Lexington Lincoln Lab, 1953.

[38] Minjia Shi, Xiaoxiao Li, Alessandro Neri, and Patrick Solé. The largest number of weights in cyclic codes. *CoRR*, abs/1807.08418, 2018.

[39] Minjia Shi, Hongwei Zhu, Patrick Solé, and Gérard D Cohen. How many weights can a linear code have? *Designs, Codes and Cryptography*, 87(1):87–95, 2019.

[40] V. Sidorenko, G. Richter, and M. Bossert. Linearized shift-register synthesis. *IEEE Transactions on Information Theory*, 57(9):6025–6032, Sep. 2011.

[41] Vitaly Skachek and Ron M. Roth. Probabilistic algorithm for finding roots of linearized polynomials. *Designs, Codes and Cryptography*, 46(1):17–23, 2008.

[42] Chunming Tang. Infinite families of 3-designs from apn functions. *Journal of Combinatorial Designs*, 28(2):97–117, 2020.

Chapter 3

On decoding additive generalized twisted Gabidulin codes

In this chapter, we consider an interpolation-based decoding algorithm for a large family of maximum rank distance codes, known as the additive generalized twisted Gabidulin codes, over the finite field $\mathbb{F}_{q^n}$ for any prime power q, which extends the work of [24] on decoding these codes over finite fields in characteristic two. This chapter is based on my work with Chunlei Li [19].

3.1 Introduction

Error correction codes with the rank metric have found applications in space-time coding [28], random network coding [45] and cryptography [12]. Many important properties of rank metric codes including the Singleton like bound were independently studied by Delsarte [9] , Gabidulin [13] and Roth [39]. Codes that achieve this bound were called *maximum rank distance* (MRD) codes. The most famous sub-family of MRD codes are *Gabidulin codes* which is the rank metric analog of Reed-Solomon codes. They have been extensively studied in the literature [9, 12, 13, 26, 37, 39].

Finding new families of MRD codes has been an interesting research topic since the invention of Gabidulin codes. In [40], [21], the Frobenious automorphism in the Gabidulin codes were generalized to arbitrary automorphism and *generalized Gabidulin (GG)* codes were proposed. In the past few years, a considerable amount of work has been done on MRD codes. In [41], Sheekey twisted the evaluation polynomial of a Gabidulin code and proposed a large family of MRD codes termed *twisted Gabidulin (TG)* codes. Using the same idea for generalizing Gabidulin codes, arbitrary automorphism was employed to construct *generalized twisted Gabidulin (GTG)* codes. This family of MRD codes were first described in [41, Remark 9] and later comprehensively studied in [27]. Otal and Özbudak [31] later introduced a large family of MRD codes, known as *additive generalized twisted Gabidulin (AGTG)* codes, which contains all the aforementioned linear MRD codes as sub-families and new additive MRD codes. There are also some new families of MRD codes which are not equivalent to AGTG codes nor its subfamilies [5, 8, 43, 48]. Recent constructions of linear and nonlinear MRD codes were

lately summarized in [32, 42].

MRD codes with efficient decoding algorithm are of great interest in practice. In his pioneering work [13], Gabidulin gave a decoding algorithm based on extended Euclidean algorithm. Subsequently, Richter and Plass in [37], and Loidreau [26] proposed modified version of Berlekamp-Massey and Welch-Berlekamp algorithms to decode Gabidulin codes. Some of the aforementioned algorithms were further optimized in [46], [49]. Nevertheless, the known decoding algorithms for Gabidulin codes cannot be directly applied to those new MRD codes with twisted evaluation polynomials, especially when the MRD codes are only linear over the ground field $\mathbb{F}_q$ or its subfield. By modifying the decoding algorithm in [20] for subspace codes, Randrianarisoa and Rosenthal in [38] proposed a decoding method for the twisted Gabidulin codes, which works only for a limited option of parameters. Randrianarisoa later proposed an interpolation approach to decoding twisted Gabidulin codes in [36] , where he gave a brief discussion on the case when the rank of the error vector reaches the unique error-correcting radius of the twisted Gabidulin codes.

In this chapter, we apply the interpolation approach by Randrianarisoa [36] in decoding additive generalized twisted Gabidulin (AGTG) codes, which contain (generalized) twisted Gabidulin codes and (generalized) Gabidulin codes as special cases. For AGTG codes with minimum rank distance d, if an error vector has rank strictly less than $\frac{d-1}{2}$, the decoding process can be directly converted to the decoding of generalized Gabidulin codes, for which existing decoding algorithms in [26, 37, 49] can be applied. On the other hand, when the error vector has rank exactly $\frac{d-1}{2}$ (with d being odd), a new problem arises and one needs an efficient way to solve a quadratic polynomial. Solving a given quadratic polynomial over finite fields in general is a challenging problem. The quadratic polynomial derived from the decoding of the AGTG codes has a close connection to a projective polynomials $P(x)$. Different from the short discussion in [36], we study the projective polynomial $P(x)$ in greater depth. We start with the discussion on the number of roots of $P(x)$ according to its coefficients and the characteristic of the finite field $\mathbb{F}_{q^n}$, propose methods to find roots of $P(x)$ for each case, and finally adopt the result in the decoding algorithm for AGTG codes.

The remainder of this chapter is structured as follows. Section 2 introduces some preliminaries, where we particularly recall some properties of linearized polynomial and recently constructed twisted MRD codes. Section 3 summarizes the interpolation decoding approach for the additive generalized twisted Gabidulin codes and identifies the crucial quadratic polynomial when the rank of error reaches $\frac{d-1}{2}$ (with d being odd). Section 4 is dedicated to the study of the quadratic polynomial and to finding roots of the corresponding projective polynomial $P(x)$. Section 5 integrates the interpolation decoding procedure and the result of Section 4 into an explicit algorithm and discusses the complexity of the proposed algorithm. Section 3.6 concludes the work of this chapter.

3.2 Preliminaries

Let q be a power of a prime p. Throughout this chapter we denote by $\mathbb{F}_{q^r}$ the finite field with q^r elements for an arbitrary positive integer r.

3.2.1 Linearized polynomial

A polynomial of the form $L(x) = \sum_{i=0}^{k-1} l_i x^{q^i}$ over $\mathbb{F}_{q^n}$ is known as a q-polynomial [30]. Define a set

$$\mathcal{L}_k(\mathbb{F}_{q^n}) = \left\{ L(x) = \sum_{i=0}^{k-1} l_i x^{q^i} \,|\, L(x) \in \mathbb{F}_{q^n}[x]/(x^{q^n} - x) \right\}. \tag{3.1}$$

It is easy to verify that $\left(\mathcal{L}_k(\mathbb{F}_{q^n}), +, \circ\right)$ forms a non-commutative $\mathbb{F}_q$-algebra, where $+$ denotes the conventional polynomial addition and $\circ$ denotes the symbolic product given by $a(x) \circ b(x) = a(b(x))$. Note that symbolic product is associative and distributive, but non-commutative in general. For a nonzero $L(x) = \sum_{i=0}^{k-1} l_i x^{q^i}$ over $\mathbb{F}_{q^n}$, its q-degree is given by $\deg_q(L(x)) = \max\{0 \le i < k \,|\, l_i \neq 0\}$.

When q is fixed or the context is clear, it is also customary to speak of a *linearized polynomial* as it satisfies the linearity property: $L(c_1 x + c_2 y) = c_1 L(x) + c_2 L(y)$ for any $c_1, c_2 \in \mathbb{F}_q$ and any x, y in an arbitrary extension $\mathbb{F}_{q^n}$. Hence a linearized polynomial $L(x) \in \mathcal{L}_n(\mathbb{F}_{q^n})$ indicates an $\mathbb{F}_q$-linear transformation L from $\mathbb{F}_{q^n}$ to itself.

Known MRD codes in the literature are mostly given in the terms of linearized polynomials. Some relevant definitions and auxiliary results are recalled below.

Definition 35. *For a nonzero linearized polynomial $L(x) = \sum_{i=0}^{k-1} l_i x^{q^i}$ over $\mathbb{F}_{q^n}$, its rank is given by*

$$\mathrm{Rank}(L) := \dim_{\mathbb{F}_q}(\mathrm{Img}(L)) = n - \dim_{\mathbb{F}_q}(\mathrm{Ker}(L)),$$

where $\mathrm{Img}(L) = \left\{L(x) | x \in \mathbb{F}_{q^n}\right\}$ *and* $\mathrm{Ker}(L) = \{x \in \mathbb{F}_{q^n} | L(x) = 0\}$.

For a linearized polynomial $L(x) = \sum_{i=0}^{k} l_i x^{q^i}$ with q-degree k, i.e., $l_k \neq 0$, it is clear that $\mathrm{Ker}(L)$ has at most q^k elements. From the definition, the linearized polynomial $L(x)$ has

$$\mathrm{Rank}(L) = n - \dim_{\mathbb{F}_q}(\mathrm{Ker}(L)) \ge n - k.$$

Sheekey in [41] characterizes a necessary condition for $L(x)$ to have rank $n-k$ as below.

Lemma 2. *[41] Suppose a linearized polynomial $L(x) = l_0 x + l_1 x^q + \cdots + l_k x^{q^k}$, $l_k \neq 0$, in $\mathcal{L}_n(\mathbb{F}_{q^n})$ has q^k roots in $\mathbb{F}_{q^n}$. Then*

$$\mathrm{Norm}_{q^n/q}(l_k) = (-1)^{nk} \mathrm{Norm}_{q^n/q}(l_0), \tag{3.2}$$

where $\mathrm{Norm}_{q^n/q}(x) = x^{1+q+\cdots+q^{n-1}}$ *is the norm function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$.*

Furthermore, the necessary and sufficient condition for $L(x)$ with q-degree k to have q^k roots in $\mathbb{F}_{q^n}$ was independently characterized recently in [29, Theorem 7] and [7, Theorem 1.2], where all coefficients of $L(x)$ are involved.

Below we recall two interesting matrices, of which properties and connection are critical for the decoding algorithm in this chapter.

Definition 36. *[25, 50] Given a vector $a = (a_0, \ldots, a_{n-1})$ over $\mathbb{F}_{q^n}$, the Dickson matrix associated with a is given by*

$$D_a = \left(a^{q^j}_{i-j(\mathrm{mod}n)}\right)_{n\times n} = \begin{pmatrix} a_0 & a^q_{n-1} & \ldots & a^{q^{n-1}}_1 \\ a_1 & a^q_0 & \ldots & a^{q^{n-1}}_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a^q_{n-2} & \ldots & a^{q^{n-1}}_0 \end{pmatrix}, \tag{3.3}$$

and the Moore matrix associated with a is given by

$$M_a = \left(a_i^{q^j}\right)_{n\times n} = \begin{pmatrix} a_0 & a^q_0 & \ldots & a^{q^{n-1}}_0 \\ a_1 & a^q_1 & \ldots & a^{q^{n-1}}_1 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a^q_{n-1} & \ldots & a^{q^{n-1}}_{n-1} \end{pmatrix}. \tag{3.4}$$

The Dickson matrix and Moore matrix have the following properties:

Lemma 3. *For two vectors $a = (a_0, \ldots, a_{n-1})$ and $b = (b_0, \ldots, b_{n-1})$ over $\mathbb{F}_{q^n}$,*

i) $D_a^T = D_{a'}$ *with* $a' = (a_0, a^q_{n-1}, \ldots, a^{q^{n-1}}_1)$;

ii) $D_a \cdot D_b = D_u$, *where* $u = (u_0, \ldots, u_{n-1})$ *with* $u_i = \sum_{j=0}^{n-1} a^{q^j}_{i-j(\mathrm{mod}\, n)} b_j$;

iii) $M_a^T \cdot M_b = D_v$, *where* $v = (v_0, \ldots, v_{n-1})$ *with* $v_i = \sum_{j=0}^{n-1} a_j^{q^i} b_j$;

iv) $M_a \cdot D_b = M_w$, *where* $w = (w_0, \ldots, w_{n-1})$ *with* $w_i = \sum_{j=0}^{n-1} a_i^{q^j} b_j$.

The proof follows from direct calculations and is thus omitted here.

Let $\mathcal{D}_n(\mathbb{F}_{q^n})$ be the set of all $n \times n$ Dickson matrices over $\mathbb{F}_{q^n}$. It is shown in [50] that $\mathcal{D}_n(\mathbb{F}_{q^n})$ forms an $\mathbb{F}_q$-algebra and there is an isomorphism φ between $\mathcal{L}_n(\mathbb{F}_{q^n})$ and $\mathcal{D}_n(F_{q^n})$ given by

$$\varphi\left(\sum_{i=0}^{n-1} l_i x^{q^i}\right) = D_{(l_0,\ldots,l_{n-1})} = \left(l^{q^j}_{i-j(\mathrm{mod}n)}\right)_{n\times n}. \tag{3.5}$$

A Dickson matrix D will be said to be associated with a linearized polynomial $L(x)$ if $\varphi(L(x)) = D$.

Proposition 3. *[50]. Let L be the linear transformation induced by a linearized polynomial $L(x) \in \mathcal{L}_n(\mathbb{F}_{q^n})$ and D the Dickson matrix associated with $L(x)$. Then*

$$\mathrm{Rank}(L) = \mathrm{Rank}(D) \text{ and } \det(L) = \det(D).$$

It is well known [25] that given a linearized polynomial $L(x) = \sum_{i=0}^{n-1} l_i x^{q^i}$ over $\mathbb{F}_{q^n}$, it is a permutation of $\mathbb{F}_{q^n}$, i.e., $\mathrm{Rank}(L) = n$, if and only if its associated Dickson matrix is non-singular; or equivalently its associated Moore matrix is non-singular. It follows from the fact

that the determinant of a Moore matrix vanishes if and only if the entries of its first column are linearly dependent. In fact, more interesting connections between a linearized polynomial $L(x)$ in $\mathcal{L}_n(\mathbb{F}_{q^n})$ and its associated Dickson matrix can be established.

Proposition 4. *[36, Theorem 3] Assume a linearized polynomial $L(x) = \sum_{i=0}^{n-1} l_i x^{q^i}$ over $\mathbb{F}_{q^n}$ has rank k. Then its associated Dickson matrix D in* (3.5) *has rank k over $\mathbb{F}_{q^n}$. Moreover, any $k \times k$ submatrix formed by k consecutive rows and k consecutive columns in D is invertible.*

Remark 1. *Let $\sigma = q^s$ with $\gcd(s,n) = 1$. The σ-polynomial*

$$L_\sigma(x) = l_0 x + l_1 x^\sigma + \cdots + l_{n-1} x^{\sigma^{n-1}}, \quad l_i \in \mathbb{F}_{q^n},$$

which reduces to a q-polynomial over $\mathbb{F}_{q^n}$ for $s = 1$, is a generalization of q-polynomial. The aforementioned properties of q-polynomials can be similarly obtained as for σ-polynomials. For instance, the σ-polynomial $L_\sigma(x) = \sum_{i=0}^{k} l_i x^{\sigma^i}$ with $l_k \neq 0$ also has $\mathrm{Rank}(L) = n - \dim_{\mathbb{F}_q}(\mathrm{Ker}(L)) \geq n - k$ [15]. When q is replaced by σ in the definition of the Dickson and Moore matrices, they are called the σ-version Dickson matrix and the σ-version Moore matrix, respectively. The σ-version Dickson and Moore matrices have the same properties as characterized in Lemma 3 and Proposition 4.

3.2.2 Maximum rank distance (MRD) codes

Let n and m be two positive integers. The *rank* of a vector $a = (a_1, a_2, \ldots, a_n)$ over $\mathbb{F}_{q^m}$ is defined as the dimension of $\mathrm{span}_{\mathbb{F}_q}\langle a_1, a_2, \ldots, a_n\rangle$ which is the vector space spanned by a_i's over $\mathbb{F}_q$. The *rank distance* between two vectors $a, b \in \mathbb{F}_{q^m}$ is defined as $d_R(a,b) = \mathrm{Rank}(a - b)$.

Definition 37. *A rank metric (n, M, d)-code over $\mathbb{F}_{q^m}$ is a subset of $\mathbb{F}_{q^m}^n$ with size M and minimum rank distance d. Furthermore, it is called a maximum rank distance (MRD) code if it attains the Singleton-like bound $M \leq q^{\min\{m(n-d+1), n(m-d+1)\}}$.*

The Gabidulin codes are the most well-known MRD codes [13]. This family of MRD codes were further generalized in [21, 40], where the Frobenius automorphism of $\mathbb{F}_{q^n}$ was replaced by a generic automorphism $x \mapsto x^\sigma$ with $\sigma = q^s$ and $\gcd(s,n) = 1$. The generalized Gabidulin (GG) code $\mathcal{GG}_{n,k}$ over $\mathbb{F}_{q^m}$ with length n and dimension k is defined by

$$\mathcal{GG}_{n,k} = \left\{ (f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{n-1})) \,|\, f(x) = \sum_{i=0}^{k-1} f_i x^{\sigma^i} \text{ and } f_i \in \mathbb{F}_{q^m} \right\}, \tag{3.6}$$

where $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ in $\mathbb{F}_{q^m}$ are linearly independent over $\mathbb{F}_q$. When $\sigma = q$, i.e., $s = 1$, the code $\mathcal{GG}_{n,k}$ reduces to the original Gabidulin code [13]. The choice of independent points $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ does not affect the rank property. Hence it is customary to express generalized Gabidulin codes without the evaluation points as $\mathcal{GG}_{n,k} = \left\{ f(x) = \sum_{i=0}^{k-1} f_i x^{\sigma^i} \,|\, f_i \in \mathbb{F}_{q^m} \right\}$. We will also omit the evaluation points $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ in the following introduction of recent twisted MRD codes [27, 31, 41]. For consistency with the parameters of MRD codes in [27, 31, 41], throughout what follows we always assume $n = m$.

Recent constructions of MRD codes largely depend on the number of roots of certain linearized polynomials. From Lemma 2 it is readily seen that a linearized polynomial $L(x)$ of q-degree k has rank at least $n-k+1$ if the condition (3.2) is not met. In [41] Sheekey adopted Lemma 2 to construct *twisted Gabidulin (TG) codes* and described the *generalized twisted Gabidulin* (GTG) codes, which was intensively studied by Lunardon et al. [27].

Proposition 5. *[27, 41] Let n,k,s be positive integers such that $k<n$ and $\gcd(s,n)=1$. Let η be a nonzero element in $\mathbb{F}_{q^n}$ satisfying $\mathrm{Norm}_{q^{sn}/q^s}(\eta)\neq(-1)^{nk}$. Then the set*

$$\mathcal{H}_{k,s}(\eta,h)=\left\{\sum_{i=0}^{k-1} f_i x^{q^{si}}+\eta f_0^{q^h} x^{q^{sk}} \mid f_i\in\mathbb{F}_{q^n}\right\} \tag{3.7}$$

is an MRD code with minimum rank distance $d=n-k+1$.

The idea of manipulating some terms of linearized polynomials to construct new MRD codes was further extended in [31, 32, 34]. Below we recall from [31] the additive generalized twisted Gabidulin (AGTG) codes , for which we will propose an interpolation-based decoding algorithm in the next section.

Proposition 6. *[31] Let $n,k,s,h\in\mathbb{Z}^+$ satisfying $\gcd(s,n)=1$ and $k<n$. Let $q=q_0^u$ and $\eta\in\mathbb{F}_{q^n}$ such that $\mathrm{Norm}_{q^{sn}/q_0^s}(\eta)\neq(-1)^{nku}$. Then the set*

$$\mathcal{H}_{k,s,q_0}(\eta,h)=\left\{\sum_{i=0}^{k-1} f_i x^{q^{si}}+\eta f_0^{q_0^h} x^{q^{sk}} \mid f_i\in\mathbb{F}_{q^n}\right\} \tag{3.8}$$

is an $\mathbb{F}_{q_0}$-linear (but not necessarily $\mathbb{F}_q$-linear) MRD code of size q^{nk} and minimum rank distance $n-k+1$.

The above AGTG codes reduce to GTG codes when $q_0=q$ and to GG codes when $\eta=0$ or $q_0=2$. Very recently, Sheekey in [43] showed the existence of a new family of MRD codes which is not equivalent to AGTG codes and Trombetti-Zhou codes in [48]. Recent MRD codes that are constructed based on Lemma 2 were formulated in a united manner in[42] and [23].

3.3 Encoding and decoding for AGTG codes

Throughout this section we will denote $[i]:=\sigma^i=q^{si}$ for $i=0,\ldots,n-1$, where $(s,n)=1$, for simplicity.

Below we briefly describe the encoding process of the AGTG codes, which provides the notational conventions and a reference for the interpolation decoding process.

3.3.1 Encoding AGTG codes

For an AGTG code with evaluation points $\alpha_0,\alpha_1,\ldots,\alpha_{n-1}$ that are linearly independent over $\mathbb{F}_q$, the encoding of a message $f=(f_0,\ldots,f_{k-1})$ is the evaluation of the following linearized

polynomial at points $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$:

$$f(x) = \sum_{i=0}^{k-1} f_i x^{[i]} + \eta f_0^{q_0^h} x^{[k]}.$$

Let $\tilde{f} = (f_0, \ldots, f_{k-1}, \eta f_0^{q_0^h}, 0, \ldots, 0)$ be a vector of length n over $\mathbb{F}_{q^n}$ and M be the σ-version Moore matrix generated by α_i's, where $1 \le i, j \le n-1$, i.e.,

$$M = \left(\alpha_i^{[j]}\right)_{n\times n} = \begin{pmatrix} \alpha_0 & \alpha_0^{[1]} & \ldots & \alpha_0^{[n-1]} \\ \alpha_1 & \alpha_1^{[1]} & \ldots & \alpha_1^{[n-1]} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n-1} & \alpha_1^{[1]} & \ldots & \alpha_{n-1}^{[n-1]} \end{pmatrix}. \tag{3.9}$$

Then the encoding of AGTG codes can be expressed as

$$(f_0, \ldots, f_{k-1}) \mapsto c = (f(\alpha_0), \ldots, f(\alpha_{n-1})) = \tilde{f} M^T. \tag{3.10}$$

Here it is worth noting that in encoding process, one actually only needs to calculate the multiplication of the $(k+1)$-tuple $(f_0, \ldots, f_{k-1}, \eta f_0^{q_0^h})$ and the first $k+1$ row of M. Here we express it as in (3.10) for being consistent with the decoding procedure.

3.3.2 Decoding AGTG codes with an error-interpolation polynomial $g(x)$

For a received word $r = c + e$ with an error e added to the codeword c during transmission, when the error e has rank $t \le \lfloor \frac{n-k}{2} \rfloor$, the unique decoding task is to recover the unique codeword c such that $d_R(c, r) \le \lfloor \frac{n-k}{2} \rfloor$.

When the rank t of the error is strictly smaller than $\frac{n-k}{2}$, the decoding of AGTG codes $\mathcal{H}_{k,s,q_0}(\eta, h)$ can be converted to the decoding of GG codes $\mathcal{GG}_{n,k+1}$. More concretely, one can use the existing decoding algorithms, e.g., [26, 37, 49], for (generalized) Gabidulin codes to establish a system of $n-(k+1)-t$ independent affine equations and t unknowns, which is uniquely solvable since $2t \le n-(k+1)$. However, when the rank t achieves the unique error-correcting radius, i.e., $(n-k)$ is even and $t = \frac{n-k}{2}$, one needs more equation(s) on the unknowns and new techniques are required. In the interpolation decoding for the TG codes by Randrianarisoa [36], the problem was converted to certain quadratic equations. However, how to efficiently solve the corresponding quadratic equations was little considered in [36].

Below we shall extend Randrianarisoa's idea to the larger family of AGTG codes and investigate the quadratic equations in greater depth. For self-completeness, we briefly describe the process of interpolation decoding and how it is transformed to solving certain quadratic equation for the case that $2t = n-k$.

Suppose $g(x) = \sum_{i=0}^{n-1} g_i x^{[i]}$ is an error interpolation polynomial such that

$$g(\alpha_i) = e_i = r_i - c_i, \quad i = 0, \ldots, n-1. \tag{3.11}$$

It is clear that the error vector e is uniquely determined by the polynomial $g(x)$. Denote a vector $g = (g_0, \ldots, g_{n-1})$. From (3.10) and (3.11) it follows that

$$r = c + e = (\tilde{f} + g)M^T.$$

This is equivalent to

$$r \cdot (M^T)^{-1} = (f_0 + g_0, \ldots, f_{k-1} + g_{k-1}, \eta f_0^{q_0^h} + g_k, g_{k+1}, \ldots, g_{n-1}). \tag{3.12}$$

Letting $\gamma = (\gamma_0, \ldots, \gamma_{n-1}) = r \cdot (M^T)^{-1}$, we obtain

$$(g_{k+1}, \ldots, g_{n-1}) = (\gamma_{k+1}, \ldots, \gamma_{n-1}) \text{ and } -\eta g_0^{q_0^h} + g_k = \gamma_k - \eta \gamma_0^{q_0^h} \tag{3.13}$$

since $\eta f_0^{q_0^h} + g_k = \gamma_k$, and $f_0 + g_0 = \gamma_0$.

Therefore, the task of correcting error e is equivalent to reconstructing $g(x)$ from the available information characterized in (3.13). This reconstruction process heavily depends on the property of the associated σ-version Dickson matrix of $g(x)$ and will be discussed in Subsection 3.3.3.

3.3.3 Reconstructing the interpolation polynomial $g(x)$

Similarly to the definition in (3.3), the σ-version Dickson matrix associated with $g(x)$ can be given by

$$G = \left(g^{[j]}_{i-j \pmod n}\right)_{n\times n} = \begin{pmatrix} G_0 & G_1 & \ldots & G_{n-1} \end{pmatrix} \tag{3.14}$$

where the indices i, j run through $\{0, 1, \ldots, n-1\}$ and G_j is the j-th column of G.

According to Proposition 4, the matrix G has rank t and any $t \times t$ matrix formed by t successive rows and columns in G is nonsingular. Then G_0 can be expressed as a linear combination of $G_1, \ldots, G_t$, namely, $G_0 = \lambda_1 G_1 + \lambda_2 G_2 + \cdots + \lambda_t G_t$, where $\lambda_1, \ldots, \lambda_t$ are elements in $\mathbb{F}_{q^n}$. This yields the following recursive equations

$$g_i = \lambda_1 g^{[1]}_{i-1} + \lambda_2 g^{[2]}_{i-2} + \cdots + \lambda_t g^{[t]}_{i-t}, \quad 0 \le i < n, \tag{3.15}$$

where the subscripts in g_i's are taken modulo n. Recall that the elements $g_{k+1}, \ldots, g_{n-1}$ are known from (3.13). Hence we obtain the following linear equations with known coefficients and variables $\lambda_1, \ldots, \lambda_t$:

$$g_i = \lambda_1 g^{[1]}_{i-1} + \lambda_2 g^{[2]}_{i-2} + \cdots + \lambda_t g^{[t]}_{i-t}, \quad k + t + 1 \le i < n. \tag{3.16}$$

The above recurrence gives a generalized version of q-linearized shift register as described in [44], where $(\lambda_1, \ldots, \lambda_t)$ is the connection vector of the shift register. It is the *key equation* for the decoding algorithm in this chapter, by which we shall reconstruct $g(x)$ in two major steps:

Step 1. derive the coefficients $\lambda_1, \ldots, \lambda_t$ from (3.13) and (3.16);

Algorithm 1: A modified BM algorithm solving (3.16)

Input: elements $g_{k+1}, \cdots, g_{n-1}$

Output: A shortest FSR with coefficients $\lambda_1, \cdots, \lambda_t$ satisfying (3.16)

Set $L = 0$, $\Lambda^{(0)}(x) = x$, $B^{(0)}(x) = x$, $\Delta'_0 = 1$;
for *each r from* 0 *to* $n-k-2$ **do**
  Calculate $\Delta_r = -g_{k+1+r} + \sum_{i=1}^{L} \Lambda_i^{(r)} g_{k+1+r-i}^{q^{si}}$;
  if $\Delta_r = 0$ **then**
    $\Lambda^{(r+1)}(x) = \Lambda^{(r)}(x)$;
    $B^{(r+1)}(x) = x^{q^s} \circ B^{(r)}(x)$;
  else
    $\Lambda^{(r+1)}(x) = \Lambda^{(r)}(x) - \Delta_r x^{q^s} \circ B^{(r)}(x)$;
    if $2L > r$ **then**
      $B^{(r+1)}(x) = x^{q^s} \circ B^{(r)}(x)$;
    else
      $B^{(r+1)}(x) = \Delta_r^{-1} \Lambda^{(r)}(x)$;
      $L = r + 1 - L$;
    end
  end
  $r = r + 1$;
end
Set $t = L$;
Return t, the connection vector $\lambda_1, \cdots, \lambda_t$ in $\Lambda^{(n-k-1)}(x)$ and $B^{(n-k-1)}(x)$

Step 2. use $\lambda_1, \ldots, \lambda_t$ to compute $g_{k-1}, \ldots, g_0$ recursively from (3.15).

Note that Step 1 is the critical and challenging step in the decoding process, and Step 2 is simply a recursive that can be done fast. The following discussion shows how the procedure of Step 1 works.

As discussed in the beginning of this section, for an error vector with $\mathrm{Rank}(e) = t \leq \lfloor \frac{n-k}{2} \rfloor$, i.e., $2t + k \leq n$, we can divide the discussion into two cases.

Case 1: $2t + k < n$. In this case, (3.16) contains $n - k - t - 1 \geq t$ affine equations in variables $\lambda_1, \ldots, \lambda_t$, which has rank t. Hence the variables $\lambda_1, \ldots, \lambda_t$ can be uniquely determined. Here we assume the code has high code rate, for which the Berlekamp-Massey (BM) algorithm is more efficient [14]. Another reason for choosing the BM algorithm is that it outputs the intermediate polynomial $B^{(n-k-1)}(x)$ which will be used in Case 2. Although the recurrence equation (3.16) is a generalized version of the ones in [37, 44], the modified BM algorithm [37, 44] can be applied here to recover the coefficients $\lambda_1, \ldots, \lambda_t$. For self-completeness we recall the modified BM algorithm in Algorithm 1. The coefficients of $\Lambda^{(n-k-1)}(x)$ are the desired λ_i's.

Case 2: $2t + k = n$. In this case (3.16) gives $n - k - t - 1 = t - 1$ independent affine equations in variables $\lambda_1, \ldots, \lambda_t$. For such an under-determined system of linear equations, we will have a set of solutions $(\lambda_1, \ldots, \lambda_t)$ that has dimension 1 over $\mathbb{F}_{q^n}$. Namely, the solutions will be of

the form

$$\lambda + \omega\lambda' = (\lambda_1 + \omega\lambda'_1, \ldots, \lambda_t + \omega\lambda'_t),$$

where λ, λ' are fixed elements in $\mathbb{F}_{q^n}^t$ and ω runs through $\mathbb{F}_{q^n}$. As shown in [44, Th. 10], the solution can be derived from the modified BM algorithm with a free variable ω. Next we will show how the element ω is determined by other information in (3.13).

Observe that in (3.15), by taking $i = 0$ and $i = k+t$ and substituting the solution $\lambda + \omega\lambda'$, one gets the following two equations

$$\begin{aligned} g_0 &= (\lambda_1 + \omega\lambda'_1, \ldots, \lambda_t + \omega\lambda'_t) \cdot (g_{n-1}^{[1]}, \ldots, g_{n-t}^{[t]})^T \\ g_{k+t} &= (\lambda_1 + \omega\lambda'_1, \ldots, \lambda_t + \omega\lambda'_t) \cdot (g_{k+t-1}^{[1]}, \ldots, g_k^{[t]})^T \end{aligned}$$

Re-arranging the equations gives

$$\begin{aligned} g_0 &= c_0 + c_1\omega \\ g_{k+t} &= c_2 + c_3\omega + (\lambda_t + \lambda'_t\omega) g_k^{[t]}, \end{aligned} \tag{3.17}$$

where c_0, c_1, c_2, c_3 are derived from λ, λ' and the known g_i's. Furthermore, from (3.13) we have $-\eta g_0^{q_0^h} + g_k = \gamma_k - \eta\gamma_0^{q_0^h}$. Denoting $c_4 = \gamma_k - \eta\gamma_0^{q_0^h}$ and substituting $g_k = c_4 - \eta g_0^{q_0^h}$ into (3.17) gives

$$(\lambda_t + \lambda'_t\omega)(c_4 - \eta(c_0 + c_1\omega)^{q_0^h})^{[t]} - g_{k+t} + (c_2 + c_3\omega) = 0.$$

This equation can be re-arranged as

$$u_0\omega^{q_0^{v}+1} + u_1\omega^{q_0^{v}} + u_2\omega + u_3 = 0. \tag{3.18}$$

where $q = q_0^u$, $v = h + ust$, $u_0, \ldots, u_3$ are derived from $c_0, \ldots, c_5$ and η.

Since the error e with rank $t = \frac{n-k}{2} = \frac{d-1}{2}$ can be uniquely decoded, the polynomial

$$\mathcal{P}(x) = u_0 x^{q_0^{v}+1} + u_1 x^{q_0^{v}} + u_2 x + u_3$$

should have roots w in $\mathbb{F}_{q^n}$ that lead to solutions $\lambda + \omega\lambda'$ in (3.16) and (g_0, g_k) in (3.17).

With the coefficients $\lambda_1, \ldots, \lambda_t$ in Step 1 and the initial state $g_{n-1}, \ldots, g_{n-t}$, one can recursively compute $g_0, \ldots, g_{k-1}$ according to (3.15) in Step 2. Note that not all solutions of $\mathcal{P}(x)$ lead to correct coefficients of the error interpolation polynomial. In fact, by the expression of Dickson matrix of $g(x)$, correct $g(x)$ should have the sequence $(g_{n-1}, \ldots, g_{n-t}, \ldots)$ generated from (3.15) has period n. In other words, if the output sequence has period n, we know that the corresponding polynomial $g(x) = \sum_{i=0}^{n-1} g_i x^{[i]}$ is the desired error interpolation polynomial. From the above discussion, the remaining task of decoding is to efficiently find roots of $\mathcal{P}(x)$ in $\mathbb{F}_{q^n}$, which will be discussed in the next section.

3.4 Finding roots of the polynomial $\mathcal{P}(x)$

This subsection is dedicated to finding solutions to the following equation in $\mathbb{F}_{q^n} = \mathbb{F}_{q_0^{nu}}$:

$$\mathcal{P}(x) = u_0 x^{q_0^v+1} + u_1 x^{q_0^v} + u_2 x + u_3 = 0. \tag{3.19}$$

When $q = q_0^u = q_0$, the polynomial $\mathcal{P}$ can be reduced to $P(x)$ in [36, Page 10]. In [36], the author converted solving $P(x) = 0$ to the factorization of the linearized polynomial $x^{q^{2l}} + ax^{q^l} + bx$. Nevertheless, factoring $x^{q^{2l}} + ax^{q^l} + bx$ is not necessarily easy and there's no efficient algorithm, as far as we know, for factoring this linearized polynomial. Therefore, it's important to further investigate how to efficiently solve $\mathcal{P}(x)$.

Assume $d = (v, un)$. We start with the simplest case that $u_0 = 0$. In this case, (3.19) is reduced to an affine equation $u_1 x^{q_0^v} + u_2 x + u_3 = 0$. Furthermore,

i) if $(u_1, u_2) = (0,0)$, then $\mathcal{P}(x)$ has no zero if $u_3 \neq 0$ and every element in $\mathbb{F}_{q^n}$ as a zero otherwise;

ii) if $u_1 = 0,\ u_2 \neq 0$, then $\mathcal{P}(x)$ has a unique zero $x = -u_3/u_2$;

iii) if $u_1 \neq 0,\ u_2 = 0$, then $\mathcal{P}(x)$ has a unique zero $x = (-u_3/u_1)^{q_0^{nu-v}}$.

iv) if $u_1 u_2 \neq 0,\ u_3 = 0$, then $\mathcal{P}(x) = 0$ has q_0^d zeros in $\mathbb{F}_{q^n}$, if $-u_2/u_1$ is a $(q_0^d - 1)$ power of an element in $\mathbb{F}_{q^n}$; otherwise, $\mathcal{P}(x) = 0$ has a single zero $x = 0$.

When $u_0 \neq 0$, we transform the equation $\mathcal{P}(x) = 0$ into

$$P(x) = \frac{1}{u_0}\mathcal{P}(x - u_1 u_0^{-1}) = x^{q_0^v+1} + ax + b = 0, \tag{3.20}$$

where

$$a = \frac{u_2}{u_0} + (-\frac{u_1}{u_0})^{q_0^v} \text{ and } b = \frac{u_3}{u_0} - \frac{u_1 u_2}{u_0^2} + \frac{u_1}{u_0}(-\frac{u_1}{u_0})^{q_0^v} + (-\frac{u_1}{u_0})^{q_0^v+1}.$$

The polynomial $P(x)$ can be seen as a reduced version of the original polynomial $\mathcal{P}(x)$. It is clear that if $a = 0$, then $P(x) = 0$ has either no solution or

$$m = \gcd(q_0^v + 1, q_0^{nu} - 1) = \begin{cases} q_0^d + 1, & \text{if } \frac{nu}{\gcd(un,v)} \text{ is even,} \\ 2, & \text{if } \frac{nu}{\gcd(un,v)} \text{ and } q_0 \text{ are odd,} \\ 1, & \text{if } \frac{nu}{\gcd(un,v)} \text{ is odd, and } q_0 \text{ is even} \end{cases}$$

solutions, depending on whether $-b$ is an m-th power; and that if $b = 0$, $P(x) = 0$ has either zero as its unique solution or q_0^d solutions.

When $ab \neq 0$, the polynomial $P(x) = x^{q_0^v+1} + ax + b$ over $\mathbb{F}_{q_0^{un}}$ has a variety of applications in the construction of different sets with Singer parameters [10], construction error correcting codes [3], APN functions [4] and computing cross-correlation between m-sequences [11, 16].

The polynomial $P(x)$ is a type of project polynomials [1], which in general has the form

$$a_0 + a_1 x + a_2 x^{(2)} + \cdots + a_l x^{(l)} \in \mathbb{F}_{q^n}[x],$$

where $x^{(i)} = x^{\frac{q^i-1}{q-1}}$. Bluher in [2] showed that the projective polynomial

$$P(x) = x^{q^r+1} + ax + b, \qquad a,b \in \mathbb{F}_{q^n}^*, \tag{3.21}$$

where q is any prime power and r,n are arbitrary two positive integers, has exactly $0,1,2,q^{r_0}+1$ possible number of zeros in $\mathbb{F}_{q^n}$ with $r_0 = \gcd(r,n)$. Before the discussion on finding roots of $P(x)$, it is important to know the possible number of roots and the corresponding conditions on the coefficients of $P(x)$. In the following we will discuss different ways to find and express the zeros of $P(x)$.

First, we present a relations among roots of $P(x)$, which is inspired by [11, Lemma 22] and generalized it for any prime power q.

Proposition 7. *For positive integers r,n and a prime power q, the projective polynomial*

$$P(x) = x^{q^r+1} + ax + b, \quad a,b \in \mathbb{F}_{q^n}^*$$

has $0,1,2$ or $q^{r_0}+1$ roots $x \in \mathbb{F}_{q^n}$, where $r_0 = gcd(r,n)$. Moreover, if P has three different roots x_0,x_1 and $x_2 \in \mathbb{F}_{q^n}$, then all the roots can be characterized as

$$x_{A_0,A_1,A_2} = -x_0x_1x_2\frac{\frac{A_0}{x_0}+\frac{A_1}{x_1}+\frac{A_2}{x_2}}{A_0x_0+A_1x_1+A_2x_2} \tag{3.22}$$

where $(A_0,A_1,A_2) \neq (0,0,0)$ and $A_0+A_1+A_2 = 0$.

Proof. Suppose $P(x_0) = 0$ for an element x_0 in $\mathbb{F}_{q^n}$. For a nonzero $\lambda \in \mathbb{F}_{q^n}^*$, one has

$$\begin{aligned} P(\lambda + x_0) =& (\lambda + x_0)^{q^r+1} + a(\lambda + x_0) + b \\ =& (\lambda^{q^r+1} + x_0\lambda^{q^r} + \lambda x_0^{q^r} + x_0^{q^r+1}) + \lambda a + ax_0 + b \\ =& (\lambda^{q^r+1} + x_0\lambda^{q^r} + (x_0^{q^r} + a)\lambda) + P(x_0) \\ =& \lambda^{q^r+1}(1 + x_0/\lambda + (x_0^{q^r} + a)/\lambda^{q^r}). \end{aligned}$$

Thus $P(\lambda + x_0) = 0$ if and only if $\frac{1}{\lambda}$ is a solution of the affine equation $L_0'(z) = L_0(z) + 1 = 0$, where

$$L_0(z) = (x_0^{q^r} + a)z^{q^r} + x_0 z.$$

Depending on x_0, $L_0(z)$ may have a single solution if $x_0^{q^r} + a = 0$ or q^{r_0} solutions if $x_0(x_0^{q^r} + a)^{-1}$ is a $(q^{r_0}-1)$-th power in $\mathbb{F}_{q^n}$. Hence the affine equation $L_0'(z) = 0$ has either 0, 1 or q^{r_0} nonzero solutions in $\mathbb{F}_{q^n}$. For each nonzero solution z of $L_0'(z) = 0$, we get a root $x_0 + \frac{1}{z}$ of the projective polynomial $P(x)$.

On the other hand, when $P(x)$ has three distinct roots x_0,x_1 and x_2, we obtain two different roots $\frac{1}{x_1-x_0}$ and $\frac{1}{x_2-x_0}$ of the affine equation $L_0'(z) = 0$ and their difference $\frac{1}{x_1-x_0} - \frac{1}{x_2-x_0}$ is a root of the linearized polynomial $L_0(z) = 0$, i.e.,

$$\begin{aligned} L_0'\left(\frac{1}{x_1-x_0}\right) &= L_0\left(\frac{1}{x_1-x_0}\right)+1=0,\\ L_0'\left(\frac{1}{x_2-x_0}\right) &= L_0\left(\frac{1}{x_2-x_0}\right)+1=0,\\ L_0'\left(\frac{1}{x_1-x_0}\right)-L_0'\left(\frac{1}{x_2-x_0}\right) &= L_0\left(\frac{1}{x_1+x_0}-\frac{1}{x_2+x_0}\right)=0. \end{aligned}$$

So $y=\frac{1}{x_1-x_0}-\frac{1}{x_2-x_0}$ is a root of $L_0(z)$. Hence, $z=\frac{1}{x_1-x_0}+Ay$ runs through all roots of $L_0'(z)$. Consequently, assuming $(A_0,A_1,A_2)=(1,A,-(A+1))$,

$$\begin{aligned} x^{(A)} &= x_0+\frac{1}{z}=x_0+\frac{1}{\frac{1}{x_1-x_0}+Ay}\\ &= x_0+\frac{1}{\frac{1}{x_1-x_0}+\frac{A}{x_1-x_0}-\frac{A}{x_2-x_0}}\\ &= x_0+\frac{(x_1-x_0)(x_2-x_0)}{(x_2-x_0)+A(x_2-x_0)-A(x_1-x_0)}\\ &= -x_0x_1x_2.\frac{\frac{1}{x_0}+\frac{A}{x_1}-\frac{(A+1)}{x_2}}{x_0+Ax_1-(A+1)x_2}\\ &= -x_0x_1x_2.\frac{\frac{A_0}{x_0}+\frac{A_1}{x_1}+\frac{A_2}{x_2}}{A_0x_0+A_1x_1A_2x_2}=x_{(A_0,A_1,A_2)} \end{aligned}$$

runs through all roots of $P(x)$ different from x_0, while A runs through $\mathbb{F}_{q^{r_0}}$.

□

The above result gives a method to express all the roots of the projective polynomials $P(x)=x^{q^r+1}+ax+b, a,b\in\mathbb{F}_{q^m}^*$ in terms of the three known roots in $\mathbb{F}_{q^m}$. Moreover, from its proof, a method to describe the roots of the projective polynomial $P(x)$ in terms of the roots of the affine polynomial $L_0'(z)$. Nevertheless, the condition that characterizes the exact number of solutions to the affine equation $L_0'(z)=(x_0^{q^r}+a)z^{q^r}+x_0z+1$ is not clear.

In order to investigate the number of roots of $P(x)=x^{q^r+1}+ax+b$ in $\mathbb{F}_{q^n}$ according to its coefficients, we need to divide the discussion into two cases: q is even; or q is odd and $\gcd(r,n)=1$.

3.4.1 Solving the equation $P(x)=0$ over finite fields of characteristic 2

When the finite field $\mathbb{F}_{q^n}$ has characteristic 2, the polynomial $P(x)$ can be further converted to $F_c(x)=x^{q^r+1}+x+c=0$, which was intensively studied in [17, 18, 22]. Helleseth and Kholosha in [17, 18] explicitly gave the root of $F_c(x)=0$ in terms of the coefficient c when it has a single zero in $\mathbb{F}_{q^n}$ and when it has two zeros in $\mathbb{F}_{q^n}$ if $\gcd(r,n)$ is odd. Very recently, Kim and Mesnager in [22] further studied the equation for the case $q=2$ and $\gcd(r,n)=1$

and explicitly calculated all possible zeros of $F_c(x)$ in $\mathbb{F}_{q^n}$. Since for general AGTG codes, the parameter q_0 is always greater than 2. Below we shall recall the result by Helleseth and Kholosha [18] and apply it to find the roots of the projective polynomial $P(x)$ in some cases.

Note that in the AGTG codes are defined over $\mathbb{F}_{q^n}$ with q a prime power. In this context, we assume q is a power of 2. To avoid potential confusion of notations, below we recall the result from [18] and treat the underlying finite field as $\mathbb{F}_{2^m}$, where m is a positive integer. Let l be a positive integer with $d = \gcd(l,m)$ and denote $m_1 = l/d$. Define two sequences of polynomials in recurrence as follows: $C_1(x) = C_2(x) = Z_1(x) = 1$, and

$$C_{i+2}(x) = C_{i+1}(x) + x^{2^{il}} C_i(x), \quad Z_i(x) = C_{i+1}(x) + xC_{i-1}^{2^l}(x) \tag{3.23}$$

for $i = 1, 2, \cdots, m_1 - 1$.

Proposition 8. *[18, Prop. 3-5] Gvien a polynomial*

$$F_c(x) = x^{2^l+1} + x + c, \quad c \in \mathbb{F}_{2^m}^*, \tag{3.24}$$

i) it has exactly one zero in $\mathbb{F}_{2^m}$ if and only if $Z_{m_1}(c) = 0$ and $C_{m_1}(c) \neq 0$; and this zero is given by $x = (cC_{m_1}^{2^l-1}(c))^{2^{m-1}}$;

ii) it has exactly two zeros $\mathbb{F}_{2^m}$ if and only if $Z_{m_1}(c) \neq 0$ and $\mathrm{Tr}_1^d(\mathrm{N}_d^m(c)/Z_{m_1}^2(c)) = 0$, where the trace function $\mathrm{Tr}_1^d(z) = \sum_{i=0}^{d-1} z^{2^i}$ and $\mathrm{N}_d^m(z)$ is the norm function defined by $\mathrm{N}_d^m(z) = \prod_{i=0}^{m_1-1} x^{2^{di}}$. Moreover, if d is odd, then these two zeros are $(W+\mu)Z_{m_1}(c)/C_{m_1}(c)$ for $\mu \in \{0,1\}$, where

$$W = \frac{C_{m+1}(c)}{Z_{m+1}(c)} + \sum_{i=0}^{\frac{d-1}{2}} \left(\frac{\mathrm{N}_d^m(c)}{Z_{m_1}^2(c)} \right)^{2^{2i}};$$

iii) it has exactly $2^d + 1$ zeros in $\mathbb{F}_{2^m}$ if and only if $C_{m_1}(c) = 0$.

As an illustration, we apply Proposition 8 i) to a general polynomial $G(x)$ in the following proposition, which will be used to explicitly give the zero of $P(x)$ in $\mathbb{F}_{2^m}$ with $m = nuw$. The second cases can be applied in the similar manner.

Proposition 9. *The polynomial*

$$G(x) = x^{2^l+1} + a_1 x^{2^l} + a_2 x + a_3$$

over $\mathbb{F}_{2^m}$ has exactly one zero in $\mathbb{F}_{2^m}$ if and only if one of the following conditions holds:

i) $a_2 = a_1^{2^l}$ and $a_3 = a_1^{2^l+1}$; or

ii) $a_2 = a_1^{2^l}$, $a_3 \neq a_1^{2^l+1}$ and m_1 is odd; or

iii) $a_2 \neq a_1^{2^l}$, $Z_{m_1}(c) = 0$ and $C_{m_1}(c) \neq 0$ with $c = (a_1 a_2 + a_3)/(a_1 + a_2^{2^{n-l}})^{2^l+1}$.

Moreover, for Cases (i) and (ii), the zero of $G(x)$ is given by $x = a_1 + (a_1 a_2 + a_3)^{\frac{1}{2^l+1}}$; for Case (iii), the unique zero is given by $x = (a_1 + a_2^{2^{n-l}})(cC_{m_1}^{2^l-1}(c))^{2^{n-1}} + a_1$.

Proof. It is relatively easy to verify Case i) and Case ii). In fact, when $a_2 = a_1^{2^l}$, one obtains the equation

$$G(x) = (x+a_1)^{2^l+1} + (a_1a_2 + a_3) = 0.$$

The statement of Case i) immediately follows; and for Case ii), it is easily seen that the equation has a single solution only if $\gcd(2^l+1, 2^n-1) = 1$, equivalently, $m_1 = n/\gcd(l,n)$ is odd.

For Case iii), the equation $G(x) = 0$ can be reduced to a polynomial of the form $F_c(y) = y^{2^l+1} + y + c = 0$ by the following substitution

$$\begin{aligned} F_c(y) =& s^{-(2^l+1)} G(sy+a_1) \\ =& s^{-(2^l+1)} \Big((sy+a_1)^{2^l+1} + a_1(sy+a_1)^{2^l} + a_2(sy+a_1) + a_3 \Big) \\ =& s^{-(2^l+1)} \Big(s^{2^l+1} y^{2^l+1} + s(a_1^{2^l} + a_2)y + a_1a_2 + a_3 \Big) \\ =& y^{2^l+1} + y + c, \end{aligned}$$

where

$$s = (a_1^{2^l} + a_2)^{2^{m-l}} = (a_1 + a_2^{2^{m-l}}) \text{ and } c = \frac{a_1a_2 + a_3}{s^{2^l+1}} = \frac{a_1a_2 + a_3}{(a_1 + a_2^{2^{m-l}})^{(2^l+1)}}.$$

It is clear that y is a zero of $F_c(y) = y^{2^l+1} + y + c$ if and only if $x = sy + a_1$ is a zero of $G(x)$. The desired statement follows from Proposition 8. □

Corollary 1. *Let $q_0 = 2^w$ for a positive integer w, $l = wv$, $m = wun$ and $m_1 = m/\gcd(l,m)$. Let $C_i(x), Z_i(x)$ be defined as in* (3.23) *respectively. Then the polynomial $x^{q_0^v+1} + a_1x^{q_0^v} + a_2x + a_3$ over $\mathbb{F}_{q^n}$ has exactly one solution in $\mathbb{F}_{q^n}$ given by*

i) $x = a_1$ *if* $a_2 = a_1^{q_0^v}$ *and* $a_3 = a_1a_2$*;*

ii) $x = a_1 + (a_1a_2 + a_3)^{\frac{1}{q_0^v+1}}$ *if* $a_2 = a_1^{q_0^v}$, $a_3 \neq a_1a_2$ *and m_1 is odd;*

iii) $x = (a_1 + a_2^{q_0^{n-v}})(cC_{m_1}^{q_0^v-1}(c))^{2^{m-1}} + a_1$ *if* $a_2 \neq a_1^{q_0^v}$, $Z_{m_1}(c) = 0$ *and* $C_{m_1}(c) \neq 0$ *with* $c = (a_1a_2 + a_3)/(a_1 + a_2^{q_0^{n-v}})^{q_0^v+1}$.

3.4.2 Solving the equation $P(x) = 0$ over $\mathbb{F}_{q^n}$ when $\gcd(r,n) = 1$

For the projective polynomial $P(x) = x^{q^r+1} + ax + b$ with $\gcd(r,n) = 1$, McGuire and Sheekey recently in [29] gave a complete criteria on the coefficients a, b for $P(x) = 0$ to have $0, 1, 2$ and $q+1$ solutions in $\mathbb{F}_{q^n}$ by the analysis of the companion matrix of $P(x)$.

Let $\sigma = q^r$ and define a sequence of 2×2 matrices as follows:

$$C_0 = I_2,\ C = C_1 = \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}, \text{ and } C_k = C_{k-1}C^{\sigma^{k-1}} = CC_{k-1}^{\sigma}, \tag{3.25}$$

where C_1 is termed the companion matrix of $P(x)$, and $C_k^{\sigma^i}$ is the matrix obtained from C_k by applying to each of its entries the automorphism $x \mapsto x^{\sigma^i}$. Furthermore, define a matrix

$$A_P = C_n = CC^{\sigma} \cdots C^{\sigma^{n-1}}. \tag{3.26}$$

Since $\det(C_1) = b$ and $N(b) = b^{1+\sigma+\cdots+\sigma^{n-1}}$, one can easily verify $\det(A_P) = N(b)$. Denote

$$X = \begin{pmatrix} b/a & 0 \\ 0 & 1 \end{pmatrix}, Z_n = \begin{pmatrix} a^{(n-1)} & 0 \\ 0 & a^{(n)} \end{pmatrix} \text{ and } \quad Y_m = \begin{pmatrix} -G_{n-2}^{\sigma} & -G_{n-1}^{\sigma} \\ G_{n-1} & G_n \end{pmatrix}, \tag{3.27}$$

where $a^{(i)} = a^{\frac{\sigma^i - 1}{\sigma - 1}}$ and G_n can be computed using the recursive relation

$$G_n^{\sigma^2} - G_n = G_{n-1}^{\sigma} - G_{n-1}^{\sigma^2}. \tag{3.28}$$

Then it follows that

$$A_P = C_n = XY_nZ_n. \tag{3.29}$$

Hence one can express A_P associated with $P(x)$ in terms of G_n as follows:

$$A_P = N(a) \begin{pmatrix} -u^{q^{-1}}.G_{n-2}^{\sigma} & -\frac{b}{a}.G_{n-1}^{\sigma} \\ \frac{1}{a^{\sigma^{-1}}}.G_{n-1} & G_n \end{pmatrix}$$

where $N(a)$ denotes the field norm of $a \in \mathbb{F}_{q^n}$ from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ and $u = b^q/a^{q+1}$. Note that if $G_{n-1} = 0$ then A_P will be a diagonal matrix.

Theorem 24. *[29] The number of roots of the projective polynomial $P(x)$ in $\mathbb{F}_{q^n}$ is given by*

$$\sum_{\lambda \in \mathbb{F}_q} \frac{q^{n_\lambda} - 1}{q - 1}$$

where n_λ is the dimension of the eigenspace of A_P corresponding to the eigenvalue λ. The number of roots of $L(x)$ in $\mathbb{F}_{q^n}$ is given by q^{n_1}. In other words, the dimension of the kernel of $L(x)$ is $2 - Rank(A_L - I_2)$.

Theorem 25. *[29] The polynomial $P(x)$ has $\dfrac{q^d - 1}{q - 1}$ roots in $\mathbb{F}_{q^n}$ if and only if*

$$A_P = \lambda I_2$$

where d is the dimension of the eigenspace of the matrix A_P.

The characteristic polynomial $S_P(x) \in \mathbb{F}_q[x]$ of a 2×2 matrix A_P is of the form

$$S_P(x) = x^2 - \mathrm{Tr}(A_P)x + \det(A_P), \tag{3.30}$$

where $\mathrm{Tr}(A_P)$ is the trace of the matrix A_P and it is defined as the sum of its diagonal elements and $\det(A_L)$ is the determinant of the matrix A_P. The polynomial $S_P(x)$ can have $0, 1$ or 2 roots in $\mathbb{F}_q$. For odd prime power q, the discriminant Δ_S of the quadratic polynomial $S_P(x)$ is of the

form

$$\Delta_S = \mathrm{Tr}(A_P)^2 - 4\det(A_P). \tag{3.31}$$

Case 1) if Δ_S is a non-square in $\mathbb{F}_q$, $S_P(x)$ has no solutions in $\mathbb{F}_q$, then $P(x)$ has no solution in $\mathbb{F}_{q^n}$.

Case 2) If $\Delta_S = 0$, $S_P(x)$ has a unique solution λ in $\mathbb{F}_q$, then $P(x)$ has 1 or $q+1$ solutions in $\mathbb{F}_{q^n}$.

i) If the dimension of the eigenspace corresponding to λ is two, then $P(x)$ has $q+1$ solutions in $\mathbb{F}_{q^n}$. Due to Theorem 25, this will happen if and only if $A_P = \lambda I_2$ i.e. $G_{n-1} = 0$ and $G_n \in \mathbb{F}_q$.

ii) If the dimension of the eigenspace corresponding to λ is one, then $P(x)$ has one solution in $\mathbb{F}_{q^n}$. Due to Theorem 25, this will happen if and only if A_P is not a multiple of I_2 i.e. $G_{n-1} \neq 0$.

Case 3) If Δ_S is a non-zero square in $\mathbb{F}_q$, $S_P(x)$ has two distinct roots (eigenvalues) in $\mathbb{F}_q$. If dimension of the eigenspaces corresponding to each eigenvalue is one, due to Theorem 24, $P(x)$ has two solutions in $\mathbb{F}_{q^n}$.

Note that the projective polynomial $P(x) = x^{q^r+1} + ax + b$ associates with the following linearized polynomial

$$L(x) = xP(x^{q^r-1}) = x^{q^{2r}} + ax^{q^r} + bx, \quad a, b \in \mathbb{F}_{q^n}.$$

It is readily seen that if we can efficiently solve the linearized polynomial $L(x)$, the roots of $P(x)$ can be obtained accordingly. In [29] the authors also applied companion matrices to study the number of roots of the above linearized polynomial. Further works on the roots of linearized polynomials can be found in [7, 33, 47].

Below we provide another way of studying the roots of the linearized polynomials $L(x)$ via the Dickson matrix directly.

Theorem 26. *Let $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and $L(x) = \sum_{i=0}^{n-1} l_i x^{q^i}$ a linearized polynomial in $\mathcal{L}_n(\mathbb{F}_{q^n})$ with rank r. Let D be the associate Dickson matrix of $L(x)$. Suppose $D_0, D_1, \ldots, D_{n-1}$ are the n rows of D and $D_r = z_0 D_0 + z_1 D_1 + \cdots + z_{r-1} D_{r-1}$, where $z_0, \ldots, z_{r-1}$ in $\mathbb{F}_{q^n}$. Then the elements*

$$\beta_i = \sum_{j=0}^{r-1} \alpha_i^{q^{n-j}} z_j^{q^{n-j}} - \alpha_i^{q^{n-r}}, \quad i = 0, 1, \ldots, n-1,$$

are roots of $L(x)$. Moreover, the kernel of $L(x)$ in $\mathbb{F}_{q^n}$ is given by

$$\ker(L) = \mathrm{span}_{\mathbb{F}_q}\langle \beta_0, \beta_1, \ldots, \beta_{n-1} \rangle.$$

Proof. From Proposition 4 it is clear that the r-th row D_r can be expressed by a linear combination of $D_0, D_1, \ldots, D_{r-1}$ as $D_r = \sum_{t=0}^{r-1} z_t D_t$. That is to say, the vector $z = (z_0, \ldots, z_{n-1}) =$

$(z_0,\ldots,z_{r-1},-1,0,\ldots,0)$ satisfies $z\cdot D=(0,\ldots,0)$. Define

$$D_z^T = D_{(z_0,z_{n-1}^q,\ldots,z_1^{q^{n-1}})} = \begin{pmatrix} z_0 & \ldots & z_{r-1} & -1 & 0 & \ldots & 0 \\ 0 & z_0^q & \ldots & z_{r-1}^q & -1 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ldots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & z_0^{q^{n-r-1}} & \ldots & z_{r-1}^{q^{n-r-1}} & -1 \\ & & & \ddots & \ddots & \ddots & \\ & & & & \ddots & \ddots & \\ z_1^{q^{n-1}} & \ldots & z_r^{q^{n-1}} & 0 & \ldots & 0 & z_0^{q^{n-1}} \end{pmatrix}.$$

It follows from the pattern of the Dickson matrix D that $D_z^T\cdot D=0_{n\times n}$, where $0_{n\times n}$ is the $n\times n$ all zero matrix.

According to the definition of D_z, it is clear that it has rank at least $n-r$. On the other hand, since the Dickson matrix D has rank r and all rows of D_z are solution of $(y_0,\ldots,y_{n-1})D=(0,\ldots,0)$, the rank of D_z is at most $n-r$. This means that D_z has rank exactly $n-r$.

Let M_α be the Moore matrix associated with the basis $\alpha_0,\ldots,\alpha_{n-1}$. It follows from Lemma 3 i) and iv) that

$$M_\alpha D_z^T = M_\alpha D_{z'} = M_\beta = \begin{pmatrix} \beta_0 & \beta_0^q & \ldots & \beta_0^{q^{n-1}} \\ \beta_1 & \beta_1^q & \ldots & \beta_1^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{n-1} & \beta_{n-1}^q & \ldots & \beta_{n-1}^{q^{n-1}} \end{pmatrix},$$

where $z'=(z_0,z_{n-1}^q,\ldots,z_1^{q^{n-1}})=(z_0,0,\ldots,0,-1,z_{r-1}^{q^{n-(r-1)}},\ldots,z_1^{q^{n-1}})$ and

$$\beta_i=\sum_{j=0}^{n-1}\alpha_i^{q^j}z_{n-j}^{q^j}=\sum_{j=0}^{n-1}\alpha_i^{q^{n-j}}z_j^{q^{n-j}}=\sum_{j=0}^{r-1}\alpha_i^{q^{n-j}}z_j^{q^{n-j}}-\alpha_i^{q^{n-r}}$$

for $i=0,1,\ldots,n-1$. Recall that $D_z^T\cdot D=0_{n\times n}$. It immediately follows that

$$0_{n\times n}=M_\beta\cdot D=\begin{pmatrix} \beta_0 & \beta_0^q & \ldots & \beta_0^{q^{n-1}} \\ \beta_1 & \beta_1^q & \ldots & \beta_1^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{n-1} & \beta_{n-1}^q & \ldots & \beta_{n-1}^{q^{n-1}} \end{pmatrix}\begin{pmatrix} l_0 & l_{n-1}^q & \ldots & l_1^{q^{n-1}} \\ l_1 & l_0^q & \ldots & l_2^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n-1} & l_{n-2}^q & \ldots & l_0^{q^{n-1}} \end{pmatrix}.$$

Hence $L(\beta_i)=0$ for $i=0,1,\ldots,n-1$. Moreover, since the Moore matrix M_α is nonsingular, the rank of M_β is the same as that of the rank of D_z, which implies that the rank of $\beta_0,\ldots,\beta_{n-1}$ over $\mathbb{F}_q$ is equal to $n-r$. Thus the linear combination of $\beta_0,\ldots,\beta_{n-1}$ over $\mathbb{F}_q$ yields all the solution of $L(x)$ in $\mathbb{F}_{q^n}$. The desired conclusion follows. ■ □

From Theorem 26, we see that finding solutions of a linearized polynomial can be converted to the task of computing the rank of its associated Dickson matrix $D=(D_0,\ldots,D_{n-1})^T$ and of finding a solution of $D_r=x_0D_0+\cdots+x_{r-1}D_{r-1}$. In general, calculating the rank of a Dickson matrix D is nontrivial. Recently Csajbók in [6] proposed an interesting characterization of the

rank of D.

Theorem 27. *[6] Let D be the associated Dickson matrix of a linearized polynomial $L(x) = \sum_{i=0}^{n-1} l_i x^{q^i}$ over $\mathbb{F}_{q^n}$. Denote by D_t the submatrix of D by removing the first t rows and the last t columns. Then $L(x)$ has rank r if and only if*

$$|D_0| = \cdots = |D_{n-r-1}| = 0 \quad \textit{and} \quad |D_{n-r}| \neq 0.$$

By Theorem 27, in order to determine the rank of the Dickson matrix associated with $L(x)$, we need to calculate the determinant of D_0, D_1 and D_2. The calculation for the case D_2 is trivial. We only need to consider D_0 and D_1. To this end, we need the following result.

Theorem 28. *The determinant of the Dickson matrix*

$$D_0 = \begin{bmatrix} b & 0 & 0 & \dots & 0 & 1 & a^{q^{r(n-1)}} \\ a & b^{q^r} & 0 & \dots & 0 & 0 & 1 \\ 1 & a^{q^r} & b^{q^{2r}} & & & 0 & 0 \\ 0 & 1 & a^{q^{2r}} & & & \vdots & \vdots \\ \vdots & & & \ddots & \ddots & & \\ & & & \ddots & a^{q^{r(n-3)}} & b^{q^{r(n-2)}} & 0 \\ 0 & \dots & & & 1 & a^{q^{r(n-2)}} & b^{q^{r(n-1)}} \end{bmatrix} \tag{3.32}$$

associated with the linearized polynomial $L(x) = x^{q^{2r}} + ax^{q^r} + bx$ can be calculated using the recursive relation

$$|D_0| = (-1)^{n+1} \cdot a^{q^{r(n-1)}} |M_{n-1}| + 2b^{q^{r(n-1)}} |M_{n-2}| + N(a) + 1, \tag{3.33}$$

where $N(a)$ denotes the field norm of $a \in \mathbb{F}_{q^n}$ from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$, M_n is a tridiagonal matrix of order n and $M_{n-1} = D_1$.

Note that D_2 is a lower triangular matrix and its determinant can be directly computed $|D_2| = 1$. In order to prove Theorem 28 we need the following observation.

Lemma 4. *The determinant of the tridiagonal matrix*

$$M_n = \begin{bmatrix} a & b^q & 0 & \dots & & & 0 \\ c & a^q & b^{q^2} & & & & \vdots \\ 0 & c^q & a^{q^2} & & & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & & \vdots \\ \vdots & & & & & b^{q^{n-2}} & 0 \\ \vdots & & & & c^{q^{n-3}} & a^{q^{n-2}} & b^{q^{n-1}} \\ 0 & \dots & & & 0 & c^{q^{n-2}} & a^{q^{n-1}} \end{bmatrix} \tag{3.34}$$

is given by the recurrence relation

$$|M_n| = a^{q^{n-1}} |M_{n-1}| - b^{q^{n-1}} \cdot c^{q^{n-2}} |M_{n-2}| \tag{3.35}$$

where $|M_0| = 1$ *and* $|M_{-1}| = 0$.

Proof. Using Laplace expansion on the last column for $n \geq 2$ gives

$$
\begin{aligned}
|M_n| =& (-1)^{2n} \cdot a^{q^{n-1}} \begin{vmatrix} a & b^q & 0 & \cdots & & & 0 \\ c & a^q & b^{q^2} & & & & \vdots \\ 0 & c^q & a^{q^2} & & & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & & \vdots \\ & & & & & b^{q^{n-3}} & 0 \\ & & & & c^{q^{n-4}} & a^{q^{n-3}} & b^{q^{n-2}} \\ 0 & \cdots & & & 0 & c^{q^{n-3}} & a^{q^{n-2}} \end{vmatrix} \\
&+ (-1)^{2n-1} \cdot b^{q^{n-1}} \begin{vmatrix} a & b^q & 0 & \cdots & & 0 \\ c & a^q & b^{q^2} & & & \vdots \\ 0 & c^q & a^{q^2} & & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ & & & & a^{q^{n-3}} & b^{q^{n-2}} \\ 0 & \cdots & & & 0 & c^{q^{n-2}} \end{vmatrix} \\
&= a^{q^{n-1}} |M_{n-1}| - b^{q^{n-1}} \cdot c^{q^{n-2}} |M_{n-2}|.
\end{aligned}
$$

□

Proof of Theorem 28. The proof follows immediately by applying Laplace expansion and Lemma 4. Note that the determinant of an upper (lower) triangular matrix is the product of the elements in its main diagonal.

Theorem 28 characterizes the conditions for the associated Dickson matrix of $L(x) = x^{q^{2r}} + ax^{q^r} + bx$ to have rank $n, n-1$ and $n-2$. According to Theorem 26, one can obtain the roots of $L(x)$ by finding the coefficients in the linear combination of the first $n-1$ rows of D when D has rank $n-2$ and coefficients in the linear combination of all rows of D when D has rank $n-1$. Here the modified BM algorithm [44] will be employed, which requires $\mathcal{O}(n^2)$ operations in $\mathbb{F}_{q^n}$ for these two cases. With the coefficients, the roots of $L(x)$ are given by Theorem 26.

Instead of using Theorem 26 to compute the roots of the linearized polynomial $L(x)$, one may use the probabilistic method given in [47]. The problem of finding the root space of the linearized polynomial $L(x)$ is reduced to find the image space of another linearized polynomial $K(x)$ derived from

$$x^{q^n} - x = W(x) \circ K(x),$$

where $W(x) = \gcd(L(x), x^{q^n} - x)$. The idea is to randomly choose $y_i \in \mathbb{F}_{q^n}$ and calculate $K(y_i)$ until the base elements for the image space of $K(x)$ are obtained. Since $L(x)$ has σ-degree 2, we need to find two basis elements $K(y_1), K(y_s)$ for the image space of $K(x)$. According to [47], the algorithm has complexity in the order of $\mathcal{O}(n)$ operations in $\mathbb{F}_{q^n}$. In general the expected number of $y_j \in \mathbb{F}_{q^n}$ that need to be evaluated in order to find n linearly independent basis elements $K(y_0), \ldots, K(y_{n-1})$ is given by $\frac{1}{1-q^{j-n}}$ [47].

3.5 The decoding algorithm of AGTG codes

With the discussion in Subsections 3.3.2-3.4, we summarize the interpolation polynomial decoding algorithm of AGTG codes in Algorithm 2, and analyze its complexity accordingly.

Recall that reconstruction the error interpolation polynomial $g(x)$ is to solve (3.15) based on the available information in (3.13). For the case that $t = \frac{n-k}{2}$ with even $n-k$, according to Algorithm 1, $\Lambda^{(n-k-1)}(x)$ is the linearized polynomial obtained after $n-k$ iteration and its coefficients are the desired vector $(\lambda_1, \ldots, \lambda_t)$. L is the linear complexity of $\Lambda^{(n-k-1)}(x)$ and $B^{(n-k-1)}(x)$ is the auxiliary linearized polynomial which is used to store the value of $\Lambda^{(i)}(x)$ with the largest degree L_i such that $L_i < L$. Hence one can obtain from Algorithm 1 two t-dimensional vectors λ and λ' over $\mathbb{F}_{q^n}$. Then the solution of (3.13) is given as

$$\lambda + \omega\lambda' = (\lambda_1 + \omega\lambda'_1, \ldots, \lambda_t + \omega\lambda'_t),$$

from which the coefficients $g_0, \ldots, g_k$ can be calculated recursively. The relation of g_0 and g_k in (3.13) leads to a quadratic equation

$$\mathcal{P}(x) = u_0 x^{q_0^v+1} + u_1 x^{q_0^v} + u_2 x + u_3 = 0.$$

If $u_0 = 0$ calculate its zeros by cases i)-iv) after (3.19) or use Theorem 28, Berlekamp Massey Algorithm 1, Theorem 26 and Corollary 1 otherwise. The above process therefore can be integrated into the explicit Algorithm 2.

Remark 2. *In the proposed Algorithm 2, we reconstruct the error interpolation polynomial $g(x)$ by two major steps: calculate the coefficients $\lambda_1, \ldots, \lambda_t$ by the modified BM algorithm, and deal with the case $t = \lfloor (n-k)/2 \rfloor$ by investigating the zero of the established polynomial $\mathcal{P}(x)$. Subsection 3.4 investigates the solutions to $\mathcal{P}(x) = 0$ In the process, the calculation of the characterized conditions in Theorem 25 dominates the overall complexity. In Line* 1 *of Algorithm 2, the calculation of the interpolation polynomial $\gamma(x)$ at points (α_i, r_i) for $1 \le i \le n$. It has complexity in the order of $\mathcal{O}(n^3)$ operations over $\mathbb{F}_{q^n}$, which can be further optimized by the method in [35]. For the remaining steps in Algorithm 2, the modified BM algorithm dominates the overall complexity. Since the modified BM algorithm has operations in the order of $\mathcal{O}(n^2)$ over $\mathbb{F}_{q^n}$, the overall complexity of Algorithm 2 is in the order of $\mathcal{O}(n^2)$ over $\mathbb{F}_{q^n}$ when normal bases are used in the interpolation step.*

Algorithm 2: Interpolation decoding of AGTG codes

Input: A received word r with $t \leq \lfloor \frac{n-k}{2} \rfloor$ errors and linearly independent evaluation points $\alpha_1, \ldots, \alpha_n$

Output: The correct codeword $c \in \mathbb{F}_{q^n}^n$ or "Decoding Failure"

Calculate $\gamma(x) = \sum_{i=0}^{n-1} \gamma_i x^{[i]}$ such that $\gamma(\alpha_i) = r_i$ for $i = 1, \ldots, n$;
Apply modified BM algorithm to $(g_{k+1}, \ldots, g_{n-1}) = (\gamma_{k+1}, \ldots, \gamma_{n-1})$ and output L, $\Lambda^{(n-k-1)}(x)$, $B^{(n-k-1)}(x)$;
if $L = (n-k)/2$ **then**
    Denote $\Delta = -\omega + \sum_{i=1}^{L} \Lambda_i^{(n-k-1)} g_{n-1-i}^{q^{si}}$ with $\omega \in \mathbb{F}_{q^n}$;
    Express the coefficients of the polynomial

$$\Lambda^{(n-k)}(x) = \frac{1}{\Delta}\Lambda^{(n-k-1)}(x) + x^{q^s} \circ B^{(n-k-1)}(x),$$

    Derive the connection vector $(\lambda_1, \ldots, \lambda_t)$ from sonic $\Lambda^{(n-k)}(x)$;
    Derive the polynomial $\mathcal{P}(x) = u_0 x^{q_0^v+1} + u_1 x^{q_0^v} + u_2 x + u_3$ in (3.19);
    if $u_0 = 0$ **then**
        Calculate the zero to $\mathcal{P}(x)$ by Cases i)-iv) after (3.19);
    else
        Calculate the zero to $\mathcal{P}(x)$ by Theorem 28, the modified BM algorithm and Theorem 26;
    end
    Set $(\lambda_1, \ldots, \lambda_t) = \lambda + \omega\lambda'$ with ω as the zero of $\mathcal{P}(x)$;
    Calculate g_0, g_k from (3.19);
end
for *each* i *in* $\{1, \ldots, k\}$ **do**
    Calculate $g_i = \lambda_1 g_{i-1}^{[1]} + \cdots + \lambda_t g_{i-t}^{[t]}$, where the subscripts of g_j's are taken modulo n;
end
if *The sequence* $g_0, \ldots, g_{n-1}$ *derived from* $\lambda_1, \ldots, \lambda_t$ *has period* n **then**
    Return the codeword $c = (c_1, \ldots, c_n)$ with $c_i = r_i + g(\alpha_i)$
else
    Return "Decoding Failure"
end

3.6 Conclusion

This chapter further investigates the interpolation-based decoding algorithm for additive generalized twisted Gabidulin codes over finite fields with any characteristic. The main contribution of this chapter includes the discussion of efficiently finding the roots of the involved project polynomials and their corresponding linearized polynomials.

Bibliography

[1] Shreeram Abhyankar. Projective polynomials. *Proceedings of the American Mathematical Society*, 125(6):1643–1650, 1997.

[2] Antonia W Bluher. On $x^{q+1} + ax + b$. *Finite Fields and Their Applications*, 10(3):285 – 305, 2004.

[3] C. Bracken and T. Helleseth. Triple-error-correcting BCH-like codes. In *2009 IEEE International Symposium on Information Theory*, pages 1723–1725, 2009.

[4] L. Budaghyan and C. Carlet. Classes of quadratic apn trinomials and hexanomials and related structures. *IEEE Transactions on Information Theory*, 54(5):2354–2357, 2008.

[5] Bence Csajbók, Giuseppe Marino, Olga Polverino, and Yue Zhou. Maximum rank-distance codes with maximum left and right idealisers. *arXiv e-prints*, page arXiv:1807.08774, 2018.

[6] Bence Csajbók. Scalar q-subresultants and dickson matrices. *arXiv.org.*, abs/1909.06409, 2019.

[7] Bence Csajbók, Giuseppe Marino, Olga Polverino, and Ferdinando Zullo. A characterization of linearized polynomials with maximum kernel. *Finite Fields and Their Applications*, 56:109 – 130, 2019.

[8] Bence Csajbók, Giuseppe Marino, and Ferdinando Zullo. New maximum scattered linear sets of the projective line. *Finite Fields and Their Applications*, 54:133 – 150, 2018.

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

[10] J.F Dillon and Hans Dobbertin. New cyclic difference sets with singer parameters. *Finite Fields and Their Applications*, 10(3):342 – 389, 2004.

[11] H. Dobbertin, P. Felke, T. Helleseth, and P. Rosendahl. Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums. *IEEE Transactions on Information Theory*, 52(2):613–627, Feb 2006.

[12] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In Donald W. Davies, editor, *Advances in Cryptology – EUROCRYPT'91*, pages 482–489. Springer, 1991.

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

[14] M. Gadouleau and Zhiyuan Yan. Complexity of decoding Gabidulin codes. In *The 42nd Annual Conference on Information Sciences and Systems*, pages 1081–1085, March 2008.

[15] Rod Gow and Rachel Quinlan. Galois theory and linear algebra. *Linear Algebra and its Applications*, 430(7):1778 – 1789, 2009. Special Issue in Honor of Thomas J. Laffey.

[16] T. Helleseth, A. Kholosha, and G. J. Ness. Characterization of m-sequences of lengths $2^{2k}-1$ and 2^k-1 with three-valued cross correlation. *IEEE Transactions on Information Theory*, 53(6):2236–2245, 2007.

[17] Tor Helleseth and Alexander Kholosha. On the equation $x^{2^l+1}+x+a=0$ over $GF(2^k)$. *Finite Fields and Their Applications*, 14(1):159 – 176, 2008.

[18] Tor Helleseth and Alexander Kholosha. $x^{2^l}+1+x+a$ and related affine polynomials over $GF(2^k)$. *Cryptography and Communications*, 2(1):85–109, 2010.

[19] Wrya K. Kadir and Chunlei Li. On decoding additive generalized twisted Gabidulin codes. *Cryptography and Communications*, 12:987 – 1009, 2020.

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

[21] Alexander Kshevetskiy and Ernst Gabidulin. The new construction of rank codes. In *International Symposium on Information Theory, (ISIT)*, pages 2105–2108. IEEE, 2005.

[22] Sihem Mesnager Kwang Ho Kim. Solving $x^{2^k+1}+x+a=0$ over $GF(2^n)$. *arXiv.org.*, abs/1903.07481, 2019.

[23] Chunlei Li. Interpolation-based decoding of nonlinear maximum rank distance codes. In *International Symposium on Information Theory (ISIT)*, 2019.

[24] Chunlei Li and Wrya Kadir. On decoding additive generalized twisted Gabidulin codes. *presented at the International Workshop on Coding and Cryptography (WCC)*, 2019.

[25] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2 edition, 1997.

[26] Pierre Loidreau. A Welch–Berlekamp like algorithm for decoding Gabidulin codes. In Øyvind Ytrehus, editor, *International Workshop on Coding and Cryptography (WCC)*, pages 36–45, Berlin, Heidelberg, 2006. Springer.

[27] Guglielmo Lunardon, Rocco Trombetti, and Yue Zhou. Generalized twisted Gabidulin codes. *Journal of Combinatorial Theory, Series A*, 159:79–106, 2018.

[28] P. Lusina, E. Gabidulin, and M. Bossert. Maximum rank distance codes as space-time codes. *IEEE Transactions on Information Theory*, 49(10):2757–2760, 2003.

[29] Gary McGuire and John Sheekey. A characterization of the number of roots of linearized and projective polynomials in the field of coefficients. *Finite Fields and Their Applications*, 57:68 – 91, 2019.

[30] Oystein Ore. On a special class of polynomials. *Transactions of the American Mathematical Society*, 35(3):559–559, 1933.

[31] Kamil Otal and Ferruh Özbudak. Additive rank metric codes. *IEEE Transactions on Information Theory*, 63(1):164–168, 2017.

[32] Kamil Otal and Ferruh Özbudak. Constructions of cyclic subspace codes and maximum rank distance codes. In *Network Coding and Subspace Designs*, pages 43–66. Springer, 2018.

[33] Olga Polverino and Ferdinando Zullo. On the number of roots of some linearized polynomials. *arXiv e-prints*, page arXiv:1909.00802, September 2019.

[34] Sven Puchinger, Johan Rosenkilde, and John Sheekey. Further generalisations of twisted Gabidulin codes. In *Proceedings of the 10th International Workshop on Coding and Cryptography*, 2017.

[35] Sven Puchinger and Antonia Wachter-Zeh. Fast operations on linearized polynomials and their applications in coding theory. *Journal of Symbolic Computation*, 89:194–215, 2018.

[36] Tovohery Hajatiana Randrianarisoa. A decoding algorithm for rank metric codes. *arXiv.org.*, abs/1712.07060, 2017.

[37] G. Richter and S. Plass. Fast decoding of rank-codes with rank errors and column erasures. In *International Symposium on Information Theory (ISIT)*, pages 398–398, June 2004.

[38] Joachim Rosenthal and Tovohery Hajatiana Randrianarisoa. A decoding algorithm for twisted Gabidulin codes. In *International Symposium on Information Theory (ISIT)*, pages 2771–2774. IEEE, 2017.

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

[40] Ron M Roth. Tensor codes for the rank metric. *IEEE Transactions on Information Theory*, 42(6):2146–2157, 1996.

[41] John Sheekey. A new family of linear maximum rank distance codes. *Advances in Mathematics of Communications*, 10:475, 2016.

[42] John Sheekey. Mrd codes: Constructions and connections. *arXiv.org.*, abs/1904.05813, 2019.

[43] John Sheekey. New semifields and new mrd codes from skew polynomial rings. *Journal of the London Mathematical Society*, 101(1):432–456, 2020.

[44] V. Sidorenko, G. Richter, and M. Bossert. Linearized shift-register synthesis. *IEEE Transactions on Information Theory*, 57(9):6025–6032, Sep. 2011.

[45] D. Silva, F. R. Kschischang, and R. Koetter. A rank-metric approach to error control in random network coding. *IEEE Transactions on Information Theory*, 54(9):3951–3967, Sept 2008.

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

[47] Vitaly Skachek and Ron M. Roth. Probabilistic algorithm for finding roots of linearized polynomials. *Designs, Codes and Cryptography*, 46(1):17–23, 2008.

[48] R. Trombetti and Y. Zhou. A new family of mrd codes in $\mathbb{F}_q^{2n\times 2n}$ with right and middle nuclei $\mathbb{F}_{q^n}$. *IEEE Transactions on Information Theory*, 65(2):1054–1062, 2019.

[49] Antonia Wachter-Zeh, Valentin Afanassiev, and Vladimir Sidorenko. Fast decoding of Gabidulin codes. *Designs, Codes and Cryptography*, 66(1-3):57–73, 2013.

[50] Baofeng Wu and Zhuojun Liu. Linearized polynomials over finite fields revisited. *Finite Fields and Their Applications*, 22:79–100, 2013.

Chapter 4

On interpolation-based decoding of a class of maximum rank distance codes

In this chapter we present an interpolation-based decoding algorithm to decode a family of maximum rank distance codes proposed recently by Trombetti and Zhou. We employ the properties of the Dickson matrix associated with a linearized polynomial with a given rank and the modified Berlekamp-Massey algorithm in decoding. When the rank of the error vector attains the unique decoding radius, the problem is converted to solving a quadratic polynomial, which ensures that the proposed decoding algorithm has polynomial-time complexity. This chapter is based on my work with Chunlei Li and Ferdinando Zullo [11].

4.1 Introduction

Rank metric codes were independently introduced by Delsarte [5], Gabidulin [7] and Roth [25]. Those rank metric codes that achieve Singleton-like bound are called *maximum rank distance (MRD) codes*. The well known family of MRD codes are the *Gabidulin codes*. Later this family was generalized by Kshevetskiy and Gabidulin [13] which is known as the *generalized Gabidulin (GG)* codes. These codes are linear over $\mathbb{F}_{q^n}$. Sheekey [28] introduced a large family of $\mathbb{F}_q$-linear MRD codes called *twisted Gabidulin (TG) codes*, which were extended to *generalized twisted Gabidulin (GTG) codes* by employing arbitrary automorphism [28, Remark 9],[17]. Later additive MRD codes were proposed by Otal and Özbudak [19] and they are known as *additive generalized twisted Gabidulin (AGTG) codes*. AGTG codes contain all the aforementioned MRD codes as subfamilies. There are also some other MRD codes that are not equivalent to the above codes, for instance the non-additive MRD codes by Otal and Özbudak [20], new MRD codes by Sheekey [29], *Trombetti-Zhou (TZ) codes* [32], etc. For more constructions of MRD codes, please refer to [27].

MRD codes have gained much interest in the last decades due to their wide applications in storage system [25], network coding [31] and cryptography [6]. Efficient decoding of MRD codes is critical for their applications. There are different decoding approaches for Gabidulin codes. Gabidulin [7] presented decoding based on a linearized equivalent of the Extended Euclidean Algorithm. The generalized Berlekamp-Massey algorithm was given by Richter and Plass in

[23]. Later Loidreau [16] proposed the Welch-Berlekamp like algorithm to decode Gabidulin codes. Nevertheless, the above algorithms can not be directly applied to the new MRD codes with twisted evaluation polynomials. Randrianarisoa and Rosenthal in [24] proposed a decoding method for a subfamily of TG codes. Randrianarisoa in [22] gave an interpolation-based decoding algorithm for GTG codes. He reduced the decoding problem to finding zeros of projective equations. Kadir and Li in [10] applied the interpolation approach to decoding AGTG codes and studied the final projective equations in greater depth. Li [14] used a similar idea in decoding the non-additive partition MRD codes in [20].

In this chapter we propose an interpolation-based decoding algorithm for TZ codes. We also compare the interpolation-based decoding algorithms for MRD codes when the rank of the error vector reaches the unique decoding radius, which shows that decoding TZ codes requires less operations than decoding GTG and AGTG codes as the problem can be reduced to solving a quadratic equation.

4.2 Preliminaries

Definition 38. *Let q be a power of prime p and $\mathbb{F}_{q^n}$ be an extension of the finite field $\mathbb{F}_q$. A q-polynomial is a polynomial of the form $L(x) = a_0x + a_1x^q + \cdots + a_{k-1}x^{q^{k-1}}$ over $\mathbb{F}_{q^n}$. If $a_{k-1} \neq 0$, then we say that $L(x)$ has q-degree $k-1$. The set of these polynomials is denoted by $\mathcal{L}_k(\mathbb{F}_{q^n})$.*

When q is fixed or the context is clear, it is also customary to speak of a *linearized polynomial* as it satisfies the linearity property: $L(c_1x+c_2y) = c_1L(x)+c_2L(y)$ for any $c_1, c_2 \in \mathbb{F}_q$ and any x, y in an arbitrary extension of $\mathbb{F}_{q^n}$. Hence a linearized polynomial $L(x) \in \mathcal{L}_k(\mathbb{F}_{q^n})$ defines an $\mathbb{F}_q$-linear transformation L from $\mathbb{F}_{q^n}$ to itself. The rank of a nonzero linearized polynomial $L(x) = \sum_{i=0}^{n} a_i x^{q^i}$ over $\mathbb{F}_{q^n}$ is given by $\mathrm{Rank}(L) = n - \dim_{\mathbb{F}_q}(\mathrm{Ker}(L))$, where $\mathrm{Ker}(L)$ is the kernel of $L(x)$.

Proposition 10. *Let $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ over $\mathbb{F}_{q^n}$ be a linearized polynomial with rank t. Then its associated Dickson matrix*

$$D = \left(a_{i-j(\mathrm{mod}n)}^{q^i}\right)_{n\times n} = \begin{pmatrix} a_0 & a_{n-1}^q & \cdots & a_1^{q^{n-1}} \\ a_1 & a_0^q & \cdots & a_2^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2}^q & \cdots & a_0^{q^{n-1}} \end{pmatrix}, \tag{4.1}$$

has rank t over $\mathbb{F}_{q^n}$. Moreover, any $t \times t$ submatrix formed by t consecutive rows and t consecutive columns in D is non-singular.

The first part of Prop. 10 is given in [33], whereas the second part can be found in [22] and [1].

4.3 Maximum rank distance (MRD) codes

The rank of a vector $a = (a_1, \ldots, a_n)$ in $\mathbb{F}_{q^m}^n$, denoted as $\mathrm{Rank}(a)$, is the number of its linearly independent components, that is the dimension of the vector space spanned by a_i's over $\mathbb{F}_q$. The rank distance between two vectors $a, b \in \mathbb{F}_{q^m}^n$ is defined as $d_R(a,b) = \mathrm{Rank}(a-b)$.

Definition 39. *A subset $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ with respect to the rank distance is called a rank metric code. When $\mathcal{C}$ contains at least two elements, the minimum rank distance of $\mathcal{C}$ is given by $d(\mathcal{C}) = \min_{A,B\in\mathcal{C},\, A\neq B}\{d_R(A,B)\}$. Furthermore, it is called a maximum rank distance (MRD) code if it attains the Singleton-like bound $|\mathcal{C}| \leq q^{\min\{m(n-d+1),n(m-d+1)\}}$.*

The most famous MRD codes are Gabidulin codes [7] which were further generalized in [13, 26]. The generalized Gabidulin (GG) codes $\mathcal{GG}_{n,k}$ with length $n \leq m$ and dimension k over $\mathbb{F}_{q^m}$ is defined by the evaluation of

$$\left\{ \sum_{i=0}^{k-1} f_i x^{q^{si}} \mid f_i \in \mathbb{F}_{q^m} \right\}, \tag{4.2}$$

where $(s,m) = 1$, on linearly independent points $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ in $\mathbb{F}_{q^m}$. The choice of α_i's does not affect the rank property and it is customary to exhibit Gabidulin codes and its generalized families without the evaluation points as in (4.2). For consistency with the parameters of MRD codes in [19, 28, 32], through what follows we always assume $n = m$.

For a linearized polynomial $L(x) = \sum_{i=0}^{k} l_i x^{q^i}$ over $\mathbb{F}_{q^n}$, it is clear that $\mathrm{Rank}(L) \geq n-k$ if $l_k \neq 0$. Gow and Quinlan in [9, Theorem 10] (see also [28]) characterize a necessary condition for $L(x)$ to have rank $n-k$ as below, see [3, 18] for other necessary conditions.

Lemma 5. *[9] Suppose a linearized polynomial $L(x) = l_0 x + l_1 x^q + \cdots + l_k x^{q^k}$, $l_k \neq 0$, in $\mathcal{L}_n(\mathbb{F}_{q^n})$ has q^k roots in $\mathbb{F}_{q^n}$. Then $\mathrm{Norm}_{q^n/q}(l_k) = (-1)^{nk}\mathrm{Norm}_{q^n/q}(l_0)$, where $\mathrm{Norm}_{q^n/q}(x) = x^{1+q+\cdots+q^{n-1}}$ is the norm function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$.*

According to Lemma 5, a linearized polynomial $L(x)$ of q-degree $k-1$ has rank at least $n-k+1$ if the condition in Lemma 5 is not met. Sheekey [28] applied Lemma 5 and constructed a new family of MRD codes, known as *twisted Gabidulin (TG) codes*, and the generalized TG codes are investigated in [17]. Later Otal and Özbudak [19] further generalized this family by manipulating some terms of linearized polynomials and constructed the *additive generalized twisted Gabidulin (AGTG) codes* which contains all the aforementioned MRD codes as subfamilies.

Below we recall from [32] the *Trombetti-Zhou (TZ) code*, which has been proved to be inequivalent to subfamilies of AGTG codes, further generalized twisted Gabidulin codes [21], Sheekey's new MRD codes [29] and those with minimum distance equals to $n-1$, such as [2, 4]. We are going to propose an interpolation-based decoding algorithm for TZ codes in the next section.

Proposition 11. *[32] Let $n,k,s \in \mathbb{Z}^+$ satisfying $(s,2n) = 1$ and let $\gamma \in \mathbb{F}_{q^{2n}}$ satisfy that $Norm_{q^{2n}/q}(\gamma)$ is a non-square element in $\mathbb{F}_q$. Then the set*

$$\mathcal{D}_{k,s}(\gamma) = \left\{ ax + \sum_{i=1}^{k-1} f_i x^{q^{si}} + \gamma b x^{q^{sk}} \mid f_i \in \mathbb{F}_{q^{2n}}, a, b \in \mathbb{F}_{q^n} \right\}$$

is an $\mathbb{F}_{q^n}$-linear MRD code of size q^{2nk} and minimum rank distance $2n-k+1$.

The first and the last coefficients of the above polynomial are chosen independently from the base field $\mathbb{F}_{q^n}$. If q is even, all the elements of $\mathbb{F}_q$ are square elements, so TZ codes exist only when the characteristic of $\mathbb{F}_q$ is odd.

4.4 Encoding and decoding of TZ codes

For the rest of this chapter, we will denote $[i] := q^{si}$ for $i = 0, \ldots, 2n-1$, where $(s, 2n) = 1$, for simplicity.

4.4.1 Encoding

For a TZ MRD code with evaluation points $\alpha_0, \alpha_1, \ldots, \alpha_{2n-1}$ that are linearly independent over $\mathbb{F}_q$, the encoding of a message $f = (f_0, \ldots, f_{k-1})$ is the evaluation of the following linearized polynomial at points $\alpha_0, \alpha_1, \ldots, \alpha_{2n-1}$:

$$f(x) = ax + \sum_{i=1}^{k-1} f_i x^{[i]} + \gamma b x^{[k]}, \tag{4.3}$$

where $(a,b) \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ corresponds to f_0 via an $\mathbb{F}_{q^n}$-basis of $\mathbb{F}_{q^{2n}}$. Let $\tilde{f} = (a, f_1, \ldots, f_{k-1}, \gamma b, 0, \ldots, 0)$ be a vector of length $2n$ over $\mathbb{F}_{q^{2n}}$ and $M = \left(\alpha_i^{[j]}\right)_{2n \times 2n}$ be the $2n \times 2n$ *Moore matrix* generated by α_i's, where $1 \leq i, j \leq 2n-1$. Then the encoding of TZ codes can be expressed as

$$(a, f_1, \ldots, f_{k-1}, \gamma b) \mapsto c = (f(\alpha_0), \ldots, f(\alpha_{2n-1})) = \tilde{f} M^T, \tag{4.4}$$

where M^T is the transpose of matrix M. Here it is worth noting that in encoding process, one actually only needs to calculate the multiplication of the $(k+1)$-tuple $(a, f_1, \ldots, f_{k-1}, \gamma b)$ and the first $k+1$ rows of M. Here we express it as in (4.4) for being consistent with the decoding procedure.

4.4.2 Decoding

For a received word $r = c + e$ with an error e added to the codeword c during transmission, when the error e has rank $t \leq \lfloor \frac{2n-k}{2} \rfloor$, the unique decoding task is to recover the unique codeword c such that $d_R(c, r) \leq \lfloor \frac{2n-k}{2} \rfloor$.

Suppose $g(x) = \sum_{i=0}^{2n-1} g_i x^{[i]}$ is an error interpolation polynomial such that

$$g(\alpha_i) = e_i = r_i - c_i, \quad i = 0, \ldots, 2n-1. \tag{4.5}$$

It is clear that the error vector e is uniquely determined by the polynomial $g(x)$ and denote $\tilde{g} = (g_0, \ldots, g_{2n-1})$. From (4.4) and (4.5) it follows that

$$r = c + e = (\tilde{f} + \tilde{g})M^T.$$

This is equivalent to

$$\begin{aligned} r \cdot (M^T)^{-1} =& (a, f_1, \ldots, f_{k-1}, \gamma b, 0, \ldots, 0) + \\ & (g_0, g_1, \ldots, g_{k-1}, g_k, g_{k+1}, \ldots, g_{2n-1}). \end{aligned}$$

Letting $\beta = (\beta_0, \ldots, \beta_{2n-1}) = r \cdot (M^T)^{-1}$, we obtain

$$(g_{k+1}, \ldots, g_{2n-1}) = (\beta_{k+1}, \ldots, \beta_{2n-1}) \tag{4.6}$$

and

$$\begin{cases} g_0 + a = \beta_0 \\ g_k + \gamma b = \beta_k \end{cases} \rightarrow \begin{cases} g_0 - \beta_0 = -a \\ \gamma^{-1}(g_k - \beta_k) = -b. \end{cases}$$

With $a, b \in \mathbb{F}_{q^n}$, one obtains

$$\begin{cases} (g_0 - \beta_0)^{[n]} = g_0 - \beta_0 \\ (\gamma^{-1}(g_k - \beta_k))^{[n]} = \gamma^{-1}(g_k - \beta_k). \end{cases} \tag{4.7}$$

which yields two linearized equations

$$\begin{cases} g_0^{[n]} - g_0 - \theta_1 = 0, & (4.8) \\ g_k^{[n]} - \gamma^{[n]-1} g_k - \theta_2 = 0, & (4.9) \end{cases}$$

where $\theta_1 = \beta_0^{[n]} - \beta_0,\ \theta_2 = \beta_k^{[n]} - \gamma^{[n]-1}\beta_k$.

Therefore, the task of correcting error e is equivalent to reconstructing $g(x)$ from the available information characterized in (4.6), (4.8) and (4.9). This reconstruction process heavily depends on the property of the associated Dickson matrix of $g(x)$ and will be discussed in Subsection 4.4.3.

4.4.3 Reconstructing the interpolation polynomial $g(x)$

The Dickson matrix associated with $g(x)$ can be given by

$$G = \left(g_{i-j \pmod{2n}}^{[j]} \right)_{2n \times 2n} = (G_0\ G_1\ \ldots\ G_{2n-1}), \tag{4.10}$$

where the indices i, j run through $\{0, 1, \ldots, 2n-1\}$ and G_j is the j-th column of G.

Since $\gcd(2n,s)=1$, Proposition 10 can be easily adapted for the Dickson matrix G in (4.10). Hence G has rank t and any $t\times t$ matrix formed by t successive rows and columns in G is nonsingular. Then G_0 can be expressed as a linear combination of $G_1,\ldots,G_t$, namely, $G_0=\lambda_1G_1+\lambda_2G_2+\cdots+\lambda_tG_t$, where $\lambda_1,\ldots,\lambda_t$ are elements in $\mathbb{F}_{q^{2n}}$. This yields the following recursive equations

$$g_i=\lambda_1g_{i-1}^{[1]}+\lambda_2g_{i-2}^{[2]}+\cdots+\lambda_tg_{i-t}^{[t]},\quad 0\le i<2n, \tag{4.11}$$

where the subscripts in g_i's are taken modulo $2n$. Recall that the elements $g_{k+1},\ldots,g_{2n-1}$ are known from (4.6). Hence we obtain the following linear equations with known coefficients and variables $\lambda_1,\ldots,\lambda_t$:

$$g_i=\lambda_1g_{i-1}^{[1]}+\lambda_2g_{i-2}^{[2]}+\cdots+\lambda_tg_{i-t}^{[t]},\ k+t+1\le i<2n. \tag{4.12}$$

The above recurrence gives a generalized version of q-linearized shift register as described in [30], where $(\lambda_1,\ldots,\lambda_t)$ is the connection vector of the shift register. It is the *key equation* for the decoding algorithm in this chapter, by which we shall reconstruct $g(x)$ in two major steps:

Step 1. derive $\lambda_1,\ldots,\lambda_t$ from (4.6)-(4.9), and (4.12);

Step 2. use $\lambda_1,\ldots,\lambda_t$ to compute $g_k,\ldots,g_0$ from (4.11).

Step 1 is the critical and challenging step in the decoding process, and Step 2 is simply a recursive process that can be done in linear time in $\mathbb{F}_{q^{2n}}$. The following discussion shows how the procedure of Step 1 works.

As discussed in the beginning of this section, for an error vector with $\mathrm{Rank}(e)=t\le\lfloor\frac{2n-k}{2}\rfloor$, i.e., $2t+k\le 2n$, we can divide the discussion into two cases.

Case 1: $2t+k<2n$. In this case, (4.12) contains $2n-k-t-1\ge t$ affine equations in variables $\lambda_1,\ldots,\lambda_t$, which has rank t. Hence the variables $\lambda_1,\ldots,\lambda_t$ can be uniquely determined. In this case, the code can be seen as a sub-code of an $\mathcal{GG}_{2n,k+1}$ code and any Gabidulin codes decoding algorithm is applicable. Here we assume the code has high code rate, for which the Berlekamp-Massey algorithm is more efficient. In addition it is consistent with the notation used in Case 2. Although the recurrence equation (4.12) is a generalized version of the ones in [23, 30], the modified Berlekamp-Massey algorithm can be applied here to recover the coefficients $\lambda_1,\ldots,\lambda_t$.

Case 2: $2t+k=2n$. In this case (4.12) gives $2n-k-t-1=t-1$ independent affine equations in variables $\lambda_1,\ldots,\lambda_t$. For such an under-determined system of linear equations, we will have a set of solutions $(\lambda_1,\ldots,\lambda_t)$ that has dimension 1 over $\mathbb{F}_{q^{2n}}$. Namely, the solutions will be of the form

$$\lambda+\omega\lambda'=(\lambda_1+\omega\lambda_1',\ldots,\lambda_t+\omega\lambda_t'),$$

where λ,λ' are fixed elements in $\mathbb{F}_{q^{2n}}^t$ and ω runs through $\mathbb{F}_{q^{2n}}$. As shown in [30, Th. 10], the solution can be derived from the modified BM algorithm with a free variable ω. Next we will show how the element ω is determined by other information in (4.6), (4.8) and (4.9).

Observe that in (4.11), by taking $i=0$ and $i=k+t$ and substituting the solution $\lambda+\omega\lambda'$, one

gets the following two equations

$$\begin{aligned} g_0 &= (\lambda_1 + \omega\lambda_1', \ldots, \lambda_t + \omega\lambda_t') \cdot (g_{2n-1}^{[1]}, \ldots, g_{2n-t}^{[t]})^T, \\ g_{k+t} &= (\lambda_1 + \omega\lambda_1', \ldots, \lambda_t + \omega\lambda_t') \cdot (g_{k+t-1}^{[1]}, \ldots, g_k^{[t]})^T, \end{aligned}$$

where g_0, g_k and ω are the only unknowns. Re-arranging the equations gives

$$g_0 = c_0 + c_1\omega, \tag{4.13}$$

and

$$g_{k+t} = c_2 + c_3\omega + (\lambda_t + \lambda_t'\omega)g_k^{[t]}, \tag{4.14}$$

where c_0, c_1, c_2, c_3 are derived from λ, λ' and the known coefficients g_i's. Furthermore, from (4.8) and (4.9) we have $g_0^{[n]} - g_0 + \theta_1 = 0$ and $g_k^{[n]} - \gamma^{[n]-1}g_k + \theta_2 = 0$. Substituting (4.13) in (4.8) gives

$$c_1\omega^{[n]} + \beta_1\omega + \beta_2 = 0. \tag{4.15}$$

If $\lambda_t + \lambda_t'\omega = 0$ then we have the solution $\omega = -\lambda_t/\lambda_t'$. This solution can be further checked in (4.14) by g_{k+1}, c_2 and c_3. Otherwise, one can raise both sides of (4.14) to the $[2n-t]$-th power and obtain

$$g_k = \frac{a_1 + a_2\omega^{[2n-t]}}{a_3 + a_4\omega^{[2n-t]}}. \tag{4.16}$$

Replacing this value in (4.9), raising it to the $[t]$-th power and rearranging the terms implies

$$\zeta_1\omega^{[n]+1} + \zeta_2\omega^{[n]} + \zeta_3\omega + \zeta_4 = 0, \tag{4.17}$$

where $\zeta_1 = (a_2^{[n]}a_4 + \theta_2 a_4^{[n+t]})^{[t]}$. Furthermore, by (4.15) and (4.17) we have the following quadratic equation over $\mathbb{F}_{q^{2n}}$

$$\zeta_1 x^2 + \zeta_5 x + \zeta_6 = 0. \tag{4.18}$$

When $\zeta_1 = 0$ and $\zeta_2 \neq 0$, the unknown ω can be uniquely determined. When $\zeta_1 \neq 0$, the above quadratic equation can be reduced to

$$x^2 + rx + s = 0, \tag{4.19}$$

where $r = \zeta_5/\zeta_1$ and $s = \zeta_6/\zeta_1$.

Since the characteristic of $\mathbb{F}_q$ is odd, Equation (4.19) can be solved explicitly as follows:

a) if $r^2 - 4s$ is a quadratic residue in $\mathbb{F}_{q^{2n}}$, then it has two solutions $x = \frac{-r \pm \sqrt{r^2-4s}}{2}$;

b) if $r^2 = 4s$, then it has a single solution $x = -r/2$;

c) it has no solution in $\mathbb{F}_{q^{2n}}$ otherwise.

Since the error e with rank $t = \frac{2n-k}{2} = \frac{d-1}{2}$ can be uniquely decoded, our quadratic equation should have roots w in $\mathbb{F}_{q^{2n}}$ that lead to solutions $\lambda + \omega\lambda'$ in (4.12) and (g_0, g_k) in (4.13). With the coefficients $\lambda_1, \ldots, \lambda_t$ in Step 1 and the initial state $g_{2n-1}, \ldots, g_{2n-t}$, one can recursively compute $g_0, \ldots, g_{k-1}$ according to (4.11) in Step 2. Note that even if the equation

(4.18) has two different solutions, they don't necessarily lead to correct coefficients of the error interpolation polynomial. In fact, by the expression of Dickson matrix of $g(x)$, the correct $g(x)$ should have the sequence $(g_{2n-1},\dots,g_{2n-t},\dots)$ generated from (4.11) has period $2n$. In other words, if the output sequence has period $2n$, we know that the corresponding polynomial $g(x)=\sum_{i=0}^{2n-1} g_i x^{[i]}$ is the desired error interpolation polynomial. For self-completeness, the decoding process of TZ codes is summarized in Algorithm 3.

Algorithm 3: Interpolation decoding of TZ codes

Input: A received word r with $t \le \lfloor \frac{2n-k}{2} \rfloor$ errors and linearly independent evaluation points $\alpha_1,\dots,\alpha_{2n}$

Output: The correct codeword $c \in \mathbb{F}_{q^{2n}}^n$ or "Decoding Failure"

Calculate $\beta(x)=\sum_{i=0}^{2n-1}\beta_i x^{[i]}$ such that $\beta(\alpha_i)=r_i$ for $i=1,\dots,2n$;
Apply modified BM algorithm to $(g_{k+1},\dots,g_{2n-1})=(\gamma_{k+1},\dots,\gamma_{2n-1})$ and output L, $\Lambda^{(2n-k-1)}(x)$, $B^{(2n-k-1)}(x)$;
if $L=(2n-k)/2$ **then**
    Denote $\Delta=\omega+\sum_{i=1}^{L}\Lambda_i^{(2n-k-1)} g_{2n-1-i}^{q^{si}}$ with $\omega\in\mathbb{F}_{q^{2n}}$;
    Express the coefficients of the polynomial

$$\Lambda^{(2n-k)}(x)=\Lambda^{(2n-k-1)}(x)-\frac{1}{\Delta}x^{q^s}\circ B^{(2n-k-1)}(x),$$

    Derive the vector $\lambda+\lambda'\omega$ by negating the coefficients of $\Lambda^{(2n-k)}(x)$;
    if $\lambda_t+\lambda_t'\omega=0$ **then**
        $\omega=-\lambda_t/\lambda_t'$;
    else
        Derive the polynomial $P(x)=\zeta_1x^2+\zeta_5x+\zeta_6$ as in (4.18);
        if $\zeta_1\neq 0$ **then**
            Solve $P(x)=0$ by Cases a)-c) after (4.19);
        else
            The zero of $P(x)$ is $x=\zeta_6/\zeta_5$;
        end
    end
    Set $(\lambda_1,\dots,\lambda_t)=\lambda+\omega\lambda'$ with ω as the zero of $P(x)$;
    Calculate g_0,g_k from (4.13) and (4.14);
end
for *each i in* $\{0,\dots,k\}$ **do**
    Calculate $g_i=\lambda_1 g_{i-1}^{[1]}+\cdots+\lambda_t g_{i-t}^{[t]}$, where the subscripts of g_j's are taken modulo $2n$;
end
if *The sequence* $g_0,\dots,g_{2n-1}$ *derived from* $\lambda_1,\dots,\lambda_t$ *has period* $2n$ **then**
    Return the codeword $c=(c_0,\dots,c_{2n-1})$ with $c_i=r_i-g(\alpha_i)$
else
    Return "Decoding Failure"
end

4.4.4 Complexity Analysis

As summarized in Algorithm 3, we have two major steps to construct the error interpolation polynomial $g(x)$. The first step is to use the modified BM algorithm for obtaining the coefficients $\lambda_1, \ldots, \lambda_t$. Calculating the interpolation polynomial at points (α_i, r_i) has complexity in the order of $\mathcal{O}(n^3)$, but according to [8], if $\alpha_0, \ldots, \alpha_{2n-1}$ is taken as a self-dual normal basis, M is orthogonal, which means $M^T = M^{-1}$ and computation of $(M^T)^{-1}$ is no longer required. So the complexity of computing polynomial β is reduced to $\mathcal{O}(n^2)$ over $\mathbb{F}_{q^{2n}}$. The second major component of the first step is the modified BM algorithm which is known to have complexity in the order of $\mathcal{O}(n^2)$ over $\mathbb{F}_{q^{2n}}$. The second step is to deal with the case $t = \lfloor (2n-k)/2 \rfloor$ by investigating the solutions of the equation (4.18). This step involves checking whether $(r^2 - 4s)$ is a quadratic residue or not. In order to check whether an element $a \in \mathbb{F}_{q^{2n}}$ is square or not, one calculates $a^{\frac{q^{2n}-1}{2}} = a^{\frac{q-1}{2} \cdot (q^{2n-1} + \cdots + q + 1)} = b^{q^{2n-1} + \cdots + q + 1}$ which has complexity $\mathcal{O}(n)$ over $\mathbb{F}_{q^{2n}}$, or directly check its exponent if in implementation an element in $\mathbb{F}_{q^{2n}}$ is represented in exponential form. As a result, the complexity of our decoding method is in the order of $\mathcal{O}(n^2)$ over $\mathbb{F}_{q^{2n}}$.

Therefore, the previous two sections imply the following result.

Theorem 29. *Consider the evaluation code obtained from $\mathcal{D}_{k,s}(\gamma)$ over an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^{2n}}$. Every received word can be uniquely decoded up to rank $t \leq \frac{2n-k}{2}$ errors in polynomial time.*

4.5 Comparing the known decoding algorithms

Known decoding algorithms for Gabidulin codes can be generally classified in two different approaches: syndrome decoding as in [6, 7, 23, 25] and interpolation-based decoding as in [10, 14, 15, 16, 22]. When the rank of the error vector reaches the maximal unique decoding radius, syndrome decoding approach works only for $\mathbb{F}_{q^n}$-linear MRD codes. Since Sheekey [28] introduced TG codes, which is not always $\mathbb{F}_{q^n}$-linear, a new (non syndrome) decoding algorithm for rank metric codes has been required for the extreme case when $t = \lfloor \frac{n-k}{2} \rfloor$. When the rank of the error is not the maximal unique decoding radius, i.e., $t < \lfloor \frac{n-k}{2} \rfloor$, the syndrome decoding algorithms are still applicable. Loidreau [16] proposed the first interpolation-based decoding approach for MRD codes and considered the analogue of Welch-Berlekamp algorithm, which was originally used to decode Reed-Solomon codes. Later Randrianarisoa [22] employed Berlekamp-Massey algorithm as the main seed and introduced a decoding algorithm for GTG codes. Later Kadir and Li [10, 15] used the same idea to decode AGTG codes. In the rest of this section, we compare the existing interpolation-based decoding algorithms for MRD codes when $t = \lfloor \frac{n-k}{2} \rfloor$.

The goal of the WB algorithm is to find two linearized polynomials V and N with q-degrees less than or equal to t and less than $k+t$, respectively, which satisfy the system of equations $V(r_i) - N(\alpha_i) = 0$ where $i = 1, \ldots, n$. The system is a linear system consists of n equations and $n+1$ unknowns. This is equivalent to interpolating two pairs of linearized polynomials (V_0, N_0) and (V_1, N_1). After an initialization step, the polynomials are interpolated via a loop with indices ranging from k to $n-1$. If one manages to bound the q-degree of the polynomials

as $\deg_q(V_j) \leq t$ and $\deg_q(N_j) \leq k+t-1$ for $j=0$ or 1, it is done. The complexity of the WB algorithm is in the order of $\mathcal{O}(n^2)$ over $\mathbb{F}_{q^n}$.

The decoding algorithms in [22] and [10] interpolated the polynomial $f(x)+g(x)$ where $f(x)$ and $g(x)$ correspond to message vector c and error vector e, respectively. The decoding problem is reduced to the problem of solving an under-determined system of linear equations with $t-1$ equations and t unknowns. This approach benefits from the properties of Dickson matrix associated with $g(x)$, known coefficients of $g(x)$ and the relation between f_0 and f_k which enable us to convert the system of equations to a single projective polynomials of the form $P(x) = x^{q^v+1} + u_1 x + u_2 = 0$ for GTG and AGTG codes. The zeros of this polynomial were discussed in [10] when $(v,n) = 1$. Very recently Kim *et al.*in [12] provide the complete solution of $P(x) = 0$ over $\mathbb{F}_{q^n}$ for any power prime q and any integers n and v. Note that the relation between the coefficients of the first and the last terms of $f(x)$ in the decoding algorithm for TZ codes provides more useful information than the corresponding equations for GTG and AGTG codes. It turns out that we only need to deal with a quadratic polynomial instead of a projective polynomial. This makes the decoding algorithm for TZ codes faster than decoding GTG and AGTG codes.

4.6 Conclusion

In this chapter we proposed an interpolation-based decoding algorithm for Trombetti-Zhou MRD codes. We have shown that the decoding algorithm has polynomial time complexity as low as $\mathcal{O}(n^2)$ over $\mathbb{F}_{q^{2n}}$. It involves Berlekamp-Massey algorithm similar to the decoding approaches in [10, 22] but end up with a quadratic polynomial, rather than a projective polynomial, which requires less operations ($\mathcal{O}(n)$) to compute the zeros.

Bibliography

[1] B. Csajbók. Scalar q-subresultants and dickson matrices. *Journal of Algebra*, 547:116–128, 2020.

[2] B. Csajbók, G. Marino, O. Polverino, and C. Zanella. A new family of MRD-codes. *Linear Algebra and its Applications*, 548:203 – 220, 2018.

[3] Bence Csajbók, Giuseppe Marino, Olga Polverino, and Ferdinando Zullo. A characterization of linearized polynomials with maximum kernel. *Finite Fields and Their Applications*, 56:109 – 130, 2019.

[4] Bence Csajbók, Giuseppe Marino, and Ferdinando Zullo. New maximum scattered linear sets of the projective line. *Finite Fields and Their Applications*, 54:133 – 150, 2018.

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

[6] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In Donald W. Davies, editor, *Advances in Cryptology – EUROCRYPT'91*, pages 482–489. Springer, 1991.

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

[8] Shuhong Gao. *Normal Bases over Finite Fields*. Phd thesis, University of Waterloo, Department of Combinatorics and Optimization, 1993.

[9] Rod Gow and Rachel Quinlan. Galois theory and linear algebra. *Linear Algebra and its Applications*, 430(7):1778 – 1789, 2009. Special Issue in Honor of Thomas J. Laffey.

[10] Wrya K. Kadir and Chunlei Li. On decoding additive generalized twisted Gabidulin codes. *Cryptography and Communications*, 12:987 – 1009, 2020.

[11] Wrya K. Kadir, Chunlei Li, and Ferdinando Zullo. On interpolation-based decoding of a class of maximum rank distance codes. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 31–36, 2021.

[12] Kwang Ho Kim, Jong Hyok Choe, and Sihem Mesnager. Complete solution over GFp^n of the equation $x^{p^k+1}+x+a=0$. *arXiv.org.*, abs/2101.01003, 2021.

[13] Alexander Kshevetskiy and Ernst Gabidulin. The new construction of rank codes. In *International Symposium on Information Theory, (ISIT)*, pages 2105–2108. IEEE, 2005.

[14] Chunlei Li. Interpolation-based decoding of nonlinear maximum rank distance codes. In *International Symposium on Information Theory (ISIT)*, 2019.

[15] Chunlei Li and Wrya K. Kadir. On decoding additive generalized twisted Gabidulin codes. *presented at the International Workshop on Coding and Cryptography (WCC)*, 2019.

[16] Pierre Loidreau. A Welch–Berlekamp like algorithm for decoding Gabidulin codes. In Øyvind Ytrehus, editor, *International Workshop on Coding and Cryptography (WCC)*, pages 36–45, Berlin, Heidelberg, 2006. Springer.

[17] G. Lunardon, R. Trombetti, and Y. Zhou. Generalized twisted Gabidulin codes. *Journal of Combinatorial Theory, Series A*, 159:79–106, 2018.

[18] Gary McGuire and John Sheekey. A characterization of the number of roots of linearized and projective polynomials in the field of coefficients. *Finite Fields and Their Applications*, 57:68 – 91, 2019.

[19] Kamil Otal and Ferruh Özbudak. Additive rank metric codes. *IEEE Transactions on Information Theory*, 63(1):164–168, 2017.

[20] Kamil Otal and Ferruh Özbudak. Some new non-additive maximum rank distance codes. *Finite Fields and Their Applications*, 50:293 – 303, 2018.

[21] Sven Puchinger, Johan Rosenkilde, and John Sheekey. Further generalisations of twisted Gabidulin codes. In *Proceedings of the 10th International Workshop on Coding and Cryptography*, 2017.

[22] Tovohery Hajatiana Randrianarisoa. A decoding algorithm for rank metric codes. *arXiv.org.*, abs/1712.07060, 2017.

[23] G. Richter and S. Plass. Fast decoding of rank-codes with rank errors and column erasures. In *International Symposium on Information Theory (ISIT)*, pages 398–398, June 2004.

[24] Joachim Rosenthal and Tovohery Hajatiana Randrianarisoa. A decoding algorithm for twisted Gabidulin codes. In *International Symposium on Information Theory (ISIT)*, pages 2771–2774. IEEE, 2017.

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

[26] Ron M Roth. Tensor codes for the rank metric. *IEEE Transactions on Information Theory*, 42(6):2146–2157, 1996.

[27] John Sheekey. MRD codes: Constructions and connections. *Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications, edited by Kai-Uwe Schmidt and Arne Winterhof, Berlin, Boston: De Gruyter, 2019, pp. 255-286*.

[28] John Sheekey. A new family of linear maximum rank distance codes. *Advances in Mathematics of Communications*, 10:475, 2016.

[29] John Sheekey. New semifields and new MRD codes from skew polynomial rings. *Journal of the London Mathematical Society*, 101(1):432–456, 2020.

[30] V. Sidorenko, G. Richter, and M. Bossert. Linearized shift-register synthesis. *IEEE Transactions on Information Theory*, 57(9):6025–6032, Sep. 2011.

[31] D. Silva, F. R. Kschischang, and R. Koetter. A rank-metric approach to error control in random network coding. *IEEE Transactions on Information Theory*, 54(9):3951–3967, Sept 2008.

[32] R. Trombetti and Y. Zhou. A new family of MRD codes in $\mathbb{F}_q^{2n\times 2n}$ with right and middle nuclei $\mathbb{F}_{q^n}$. *IEEE Transactions on Information Theory*, 65(2):1054–1062, 2019.

[33] Baofeng Wu and Zhuojun Liu. Linearized polynomials over finite fields revisited. *Finite Fields and Their Applications*, 22:79–100, 2013.

Chapter 5

New Communication Models and Decoding of Maximum Rank Distance Codes

In this chapter an interpolation-based decoding algorithm to decode Gabidulin codes transmitted through a new communication model is proposed. The algorithm is able to decode rank errors beyond half the minimum distance by one unit. Also the existing decoding algorithms for generalized twisted Gabidulin codes and additive generalized twisted Gabidulin codes are improved. This chapter is based on my work in [10].

5.1 Introduction

Delsarte [2], Gabidulin [5] and Roth [30] independently introduced *rank metric codes*. Those rank metric codes that achieve Singleton-like bound are called *maximum rank distance (MRD) codes*. Gabidulin codes are the most well known family of MRD codes. Later this family was generalized by Kshevetskiy and Gabidulin [14] to *generalized Gabidulin (GG)* codes. These codes are linear over $\mathbb{F}_{q^n}$. Sheekey in [33] defined *twsited Gabidulin (TG)* codes and established a way to generalize GG codes to linear MRD codes over a base fields and then he was followed by Lunardon *et al.*[20], Otal and Özbudak [23], Trombetti and Zhou [38] and Sheekey [35] to define *generalized twisted Gabidulin (GTG)* codes, *additive generalized twisted (AGTG)* codes, *Trombetti-Zhou (TZ)* codes and *new MRD codes by Sheekey*, repcetively. For more constructions of MRD codes, please refer to [34].

Efficient decoding is required for the wide range of applications of MRD codes in storage system [30], network coding [37] and cryptography [4]. There are plenty of algorithms that decode Gabidulin codes up to half the minimum distance [5, 17, 26, 28] and some which decode Gabidulin codes beyond half the minimum distance by considering restricted communication models [6, 7, 9, 25, 27]. The previously proposed restricted models, can generate error vectors that hold some structure and they do not look random.

Randrianarisoa in [26] gave an interpolation-based decoding algorithm for Gabidulin codes

and also for GTG codes. This idea is used later in [11],[15], [13] and [12] to decode AGTG [23], Non-additive partition MRD codes [24], TZ codes [38] and Hermitain Rank metric codes [32], respectively.

In this chapter we decode Gabidulin codes beyond half the minimum distance and also improve the decoding algorithms for GTG in [26] and AGTG codes in [11, 16] by making some delicate restrictions on the communication model. In the previously defined restricted models, the error vectors hold some specific structures, for instance symmetric error vectors [6], space-symmetric error vectors [9], but the channels in our model generate error vectors without any specific structure. Moreover, we use low rate GTG and AGTG codes at the end of this chapter to decode error vectors with rank $\leq k$ where k is the dimension of the code.

5.2 Preliminaries

Definition 40. *Let q be a power of prime p and $\mathbb{F}_{q^m}$ be an extension of the finite field $\mathbb{F}_q$. A q-polynomial is a polynomial of the form $L(x) = a_0x + a_1x^q + \cdots + a_{k-1}x^{q^{k-1}}$ over $\mathbb{F}_{q^m}$. If $a_{k-1} \neq 0$, then we say that $L(x)$ has q-degree $k-1$. The set of all linearized polynomials of the form $L(x)$ is denoted by $\mathcal{L}_k(\mathbb{F}_{q^m})$.*

When q is fixed or the context is clear, it is also customary to speak of a *linearized polynomial* as it satisfies the linearity property: $L(c_1x+c_2y) = c_1L(x)+c_2L(y)$ for any $c_1, c_2 \in \mathbb{F}_q$ and any x, y in an arbitrary extension of $\mathbb{F}_{q^m}$. Hence a linearized polynomial $L(x) \in \mathcal{L}_k(\mathbb{F}_{q^m})$ defines an $\mathbb{F}_q$-linear transformation L from $\mathbb{F}_{q^m}$ to itself. The rank of a nonzero linearized polynomial $L(x) = \sum_{i=0}^{n} a_i x^{q^i}$ over $\mathbb{F}_{q^m}$ is given by $\text{Rank}(L) = n - \dim_{\mathbb{F}_q}(\text{Ker}(L))$, where $\text{Ker}(L)$ is the kernel of $L(x)$.

Proposition 12. *Let $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ over $\mathbb{F}_{q^m}$ be a linearized polynomial with rank t. Then its associated Dickson matrix*

$$D = \left(a_{i-j(\text{mod}n)}^{q^i}\right)_{n\times n} = \begin{pmatrix} a_0 & a_{n-1}^q & \cdots & a_1^{q^{n-1}} \\ a_1 & a_0^q & \cdots & a_2^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2}^q & \cdots & a_0^{q^{n-1}} \end{pmatrix}, \tag{5.1}$$

has rank t over $\mathbb{F}_{q^m}$ [26]. Moreover, any $t \times t$ submatrix formed by t consecutive rows and t consecutive columns in D is non-singular [3, 22].

5.3 Maximum rank distance (MRD) codes

The rank of a vector $a = (a_1, \ldots, a_n)$ in $\mathbb{F}_{q^m}^n$, denoted as $\text{Rank}(a)$, is the number of its linearly independent components, that is the dimension of the vector space spanned by a_i's over $\mathbb{F}_q$. The rank distance between two vectors $a, b \in \mathbb{F}_{q^m}^n$ is defined as $d_R(a,b) = \text{Rank}(a-b)$.

Definition 41. *A subset $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ with respect to the rank distance is called a rank metric code. When $\mathcal{C}$ contains at least two elements, the minimum rank distance of $\mathcal{C}$ is given by*

$d(\mathcal{C}) = \min_{A,B\in\mathcal{C},\, A\neq B}\{d_R(A,B)\}$. *Furthermore, it is called a maximum rank distance (MRD) code if it attains the Singleton-like bound* $|\mathcal{C}| \leq q^{\min\{m(n-d+1),n(m-d+1)\}}$.

The most famous MRD codes are Gabidulin codes [5] which were further generalized in [14, 31]. The generalized Gabidulin (GG) codes $\mathcal{GG}_{n,k}$ with length $n \leq m$ and dimension k over $\mathbb{F}_{q^m}$ is defined by the evaluation of

$$\left\{ \sum_{i=0}^{k-1} f_i x^{q^{si}} \,|f_i \in \mathbb{F}_{q^m} \right\}, \tag{5.2}$$

where $(s,m) = 1$, on linearly independent points $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ in $\mathbb{F}_{q^m}$. The choice of α_i's does not affect the rank property and it is customary to exhibit Gabidulin codes and its generalized families without the evaluation points as in (5.2). For consistency with the parameters of MRD codes in [23, 33, 38], through what follows we always assume $n = m$.

For a linearized polynomial $L(x) = \sum_{i=0}^{k} l_i x^{q^i}$ over $\mathbb{F}_{q^n}$, it is clear that $\text{Rank}(L) \geq n-k$ if $l_k \neq 0$. Gow and Quinlan in [8, Theorem 10] (see also [33]) characterize a necessary condition for $L(x)$ to have rank $n-k$ as below, see [1, 21] for other necessary conditions.

Lemma 6. *[8] Suppose a linearized polynomial* $L(x) = l_0 x + l_1 x^q + \cdots + l_k x^{q^k}$, $l_k \neq 0$, *in* $\mathcal{L}_n(\mathbb{F}_{q^n})$ *has* q^k *roots in* $\mathbb{F}_{q^n}$. *Then* $\text{Norm}_{q^n/q}(l_k) = (-1)^{nk}\text{Norm}_{q^n/q}(l_0)$, *where* $\text{Norm}_{q^n/q}(x) = x^{1+q+\cdots+q^{n-1}}$ *is the norm function from* $\mathbb{F}_{q^n}$ *to* $\mathbb{F}_q$.

According to Lemma 6, a linearized polynomial $L(x)$ of q-degree k has rank at least $n-k+1$ if the condition in Lemma 6 is not met. Sheekey [33] applied Lemma 6 and constructed a new family of $\mathbb{F}_q$-linear MRD codes, known as *twisted Gabidulin (TG) codes*, and the generalized TG codes are investigated in [20] as follows:

$$\mathcal{H}_{k,s}(\varepsilon,h) = \left\{ \sum_{i=0}^{k-1} f_i x^{q^{si}} + \varepsilon f_0^{q^h} x^{q^{sk}} \mid f_i \in \mathbb{F}_{q^n} \right\}, \tag{5.3}$$

where n,k,s,h are positive integers such that $k < n$ and $(s,n) = 1$. Here ε is a nonzero element in $\mathbb{F}_{q^n}$ satisfying $\text{Norm}_{q^{sn}/q^s}(\varepsilon) \neq (-1)^{nk}$. Later Otal and Özbudak [23] further generalized this family by manipulating some terms of linearized polynomials and constructed the following $\mathbb{F}_{q_0}$-linear MRD codes, known as *additive generalized twisted Gabidulin (AGTG) codes*

$$\mathcal{A}_{k,s,q_0}(\varepsilon,h) = \left\{ \sum_{i=0}^{k-1} a_i x^{q^{si}} + \varepsilon a_0^{q_0^h} x^{q^{sk}} \mid a_i \in \mathbb{F}_{q^n} \right\}, \tag{5.4}$$

where $q = q_0^u$ and nonzero ε in $\mathbb{F}_{q^n}$ satisfies $\text{Norm}_{q_0^{snu}/q_0^s}(\varepsilon) \neq (-1)^{nku}$.

For the rest of this chapter, we use the notation $[i] := q^{si}$ for $i = 0, \ldots, n-1$, where $\gcd(s,n) = 1$, for simplicity.

5.4 New Communication Models

In this section we define two new communication models. The models contain two authorized parties as sender and receiver. The sender encodes his/her message and then an error vector with rank t is added to the encoded message. The receiver will be able to decode the error vector and recover the message. Each models uses a different form of interpolation polynomial to generate its corresponding error vector.

5.4.1 First Model

In this modes, a linearized polynomial of the form

$$e_{\theta_1,\theta_2}(x) = \sum_{i=0}^{n-1} z_i x^{[i]},\ z_i \in \mathbb{F}_{q^n}, \tag{5.5}$$

$$z_0^{[n/2]} - z_0 = \alpha_{\theta_1}, \tag{5.6}$$

$$z_{k-1}^{[n/2]} - z_{k-1} = \alpha_{\theta_2}, \tag{5.7}$$

is used as the error interpolation polynomial where $\theta_1, \theta_2 \in [0, n-1]$ are the models' public parameters. We denote this model by $\mathcal{Q}_{\theta_1,\theta_2}$.

5.4.2 Second Model

In this model we have two cases:

- **case 1.** Suppose n is an odd integer, then

$$b(x) = b_0 x^{[0]} + \sum_{i=1}^{\frac{n-1}{2}} (b_i x^{[i]} + (b_i x)^{[n-i]}), \tag{5.8}$$

  is the error interpolation polynomial where $\tilde{b} = (b_0, \ldots, b_{n-1})$, $b_i \in \mathbb{F}_{q^n}$ and

$$b_{n-i} = b_i^{[n-i]} \text{ for } i = 1, \ldots, \frac{n-1}{2}. \tag{5.9}$$

- **case 2.** Suppose n is an even integer, then

$$h(x) = h_0 x^{[0]} + \sum_{i=1}^{\frac{n}{2}-1} (h_i x^{[i]} + (h_i x)^{[n-i-1]}) + h_{n-1} x^{[n-1]}, \tag{5.10}$$

is the error interpolation polynomial where $\tilde{h} = (h_0, \ldots, h_{n-1})$, $h_i \in \mathbb{F}_{q^n}$, and

$$h_{n-i-1} = h_i^{[n-i-1]} \text{for } i = 1, \ldots, \frac{n}{2} - 1. \tag{5.11}$$

Suppose $s(x)$ be one of the polynomials $e_{\theta_1,\theta_2}, b(x)$ or $h(x)$. We use $s(x)$ such that

$$s(\alpha_i) = e_i, \quad i = 0, \ldots, n-1, \tag{5.12}$$

where $e = (e_0, \ldots, e_{n-1})$ is the error vector and $\alpha_0, \ldots, \alpha_{n-1}$ are ordered linearly independent points in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

5.5 Decoding Gabidulin codes beyond half the minimum distance

5.5.1 Encoding

Let $\mathcal{GG}_{n,k}$, where n is even and k is odd, be a Gabidulin code with ordered $\mathbb{F}_q$-linearly independent evaluation points $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$. The encoding of a message $m = (m_0, \ldots, m_{k-1})$ is the evaluation of the following linearized polynomial at points $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$:

$$f(x) = \sum_{i=0}^{k-1} m_i x^{[i]}, \tag{5.13}$$

Let $\tilde{m} = (m_0, m_1, \ldots, m_{k-1}, 0, \ldots, 0)$ be a vector of length n over $\mathbb{F}_{q^n}$ and $M = \left(\alpha_i^{[j]}\right)_{n\times n}$ be the *Moore matrix* generated by α_i's, where $1 \leq i, j \leq n-1$. Then the encoding of the message m can be expressed as

$$(m_0, m_1, \ldots, m_{k-1}) \mapsto c = (f(\alpha_0), \ldots, f(\alpha_{n-1})) = \tilde{m} \cdot M^T, \tag{5.14}$$

where M^T is the transpose of matrix M. In this process since only the first k components of $\tilde{m}$ are nonzero, so only the first k rows of M are involved.

5.5.2 Decoding errors with rank $t \leq \frac{n-k+1}{2}$

Let the error vector $e = (e_0, \ldots, e_{n-1})$ of rank t be added to the codeword $c = (c_0 \ldots, c_{n-1})$ during transmission and let $r = (r_0 \ldots, r_{n-1}) = c + e$ be the received vector.

Suppose we use the communication model $\mathcal{Q}_{\theta_1,\theta_2}$ and let e_{θ_1,θ_2} in (5.5) be the error interpolation polynomial such that

$$e_{\theta_1,\theta_2}(\alpha_i) = e_i = r_i - c_i, \quad i = 0, \ldots, n-1, \tag{5.15}$$

where $\alpha_0, \ldots, \alpha_{n-1}$ are ordered linearly independent points over $\mathbb{F}_q$ in $\mathbb{F}_{q^n}$. One can see that the

error vector e is uniquely determined by the polynomial $e_{\theta_1,\theta_2}(x)$ and denote $z=(z_0,\ldots,z_{n-1})$. From (5.14) and (5.15) it follows that

$$r=c+e=(\tilde{m}+z)\cdot M^T.$$

Since M is nonsingular, this can be rewritten as

$$\begin{aligned} r\cdot(M^T)^{-1} =&(c_0,c_1,\ldots,c_{k-1},0,\ldots,0)+\\ &(z_0,z_1,\ldots,z_{k-1},z_k,\ldots,z_{n-1}).\end{aligned}$$

Let $\tilde{r}=(\eta_0,\ldots,\eta_{n-1})=r\cdot(M^T)^{-1}$, then the known coefficients z_i's are

$$(z_k,\ldots,z_{n-1})=(\eta_k,\ldots,\eta_{n-1}), \tag{5.16}$$

and we also have the auxiliary equations (5.6) and (5.7) which we will use later.

5.5.3 Reconstructing the interpolation polynomial $e_{\theta_1,\theta_2}(x)$

Let

$$E=\left(z_{i-j\pmod n}^{[j]}\right)_{n\times n}=(E_0\,E_1\,\ldots\,E_{n-1}), \tag{5.17}$$

be the Dickson matrix associated with the linearized polynomial $e_{\theta_1,\theta_2}(x)$, where the indices i, j run through $\{0,1,\ldots,n-1\}$ and E_j is the j-th column of E.

According to Proposition 12, since $e_{\theta_1,\theta_2}(x)$ has rank t, so E has rank t and any $t\times t$ sub-miatrix of E which contains t consecutive rows and columns is nonsingular. Hence the first column E_0 can be written as the linear combination of columns $E_1\ldots,E_t$ as $E_0=\gamma_1E_1+\gamma_2E_2+\cdots+\gamma_tE_t$, where $\gamma_1,\ldots,\gamma_t$ are elements in $\mathbb{F}_{q^n}$. Then we can obtain the following recursive equations

$$z_i=\gamma_1z_{i-1}^{[1]}+\gamma_2z_{i-2}^{[2]}+\cdots+\gamma_tz_{i-t}^{[t]},\quad 0\le i<n. \tag{5.18}$$

Due to the relation in (5.16), we already know $z_k,\ldots,z_{n-1}$. These known coefficients leads us to the following linear recursive equation

$$z_i=\gamma_1z_{i-1}^{[1]}+\gamma_2z_{i-2}^{[2]}+\cdots+\gamma_tz_{i-t}^{[t]},\ k+t\le i<n, \tag{5.19}$$

where $\gamma_0\ldots,\gamma_t$ are unknowns. In [36], the q-linearized shift register is given and the above recursive relation (5.19) can be seen as its generalized version. Here $(\gamma_1,\ldots,\gamma_t)$ is the connection vector of the shift register. We call the equation (5.19) as the *key equation* for the decoding algorithm in this chapter and due to the properties of shift register, finding $\gamma_1,\ldots,\gamma_t$ leads us to find the unknown coefficients $z_0\ldots,z_{k-1}$, recursively. The most complex task in our decoding algorithm is finding $\gamma_1,\ldots,\gamma_t$ and then the remaining task (calculating unknown z_i's) will be a recursive process. We consider $\mathrm{Rank}(e)=t\le\frac{n-k+1}{2}$, i.e., $2t+k\le n+1$, and the task of finding $\gamma_1\ldots,\gamma_t$ via (5.19) is divided into two cases:

Case 1: If $2t+k<n+1$. In this case, (5.19) contains $n-k-t\ge t$ affine equations and t variables $\gamma_1,\ldots,\gamma_t$, which has rank t. Hence the variables $\gamma_1,\ldots,\gamma_t$ can be uniquely determined. Here any Gabidulin decoder can be applied, but here we assume the code has high

code rate, for which the Berlekamp-Massey algorithm is more efficient and it has polynomial time complexity.

Case 2: If $2t+k=n+1$. In this case (5.19) is an under-determined system of $n-k-t=t-1$ equations with t variables $\gamma_1,\ldots,\gamma_t$. A set of solutions $(\gamma_1,\ldots,\gamma_t)$ with dimension one can be expressed of the form

$$\gamma+X\gamma' = (\gamma_1+X\gamma'_1,\ldots,\gamma_t+X\gamma'_t), \tag{5.20}$$

where γ,γ' are fixed elements in $\mathbb{F}_{q^n}^t$ and X runs through $\mathbb{F}_{q^n}$. The modified BM algorithm in [36, Th. 10] can give the solution with a free variable X.

If we take $i=0$ and $i=k+t-1$ in (5.19) and substitute the solution (5.20), then we get

$$z_0 = \delta_0+\delta_1 X, \tag{5.21}$$

and

$$z_{k+t-1} = \delta_2+\delta_3 X+(\gamma_t+\gamma'_t X)z_{k-1}^{[t]}, \tag{5.22}$$

where in (5.21) and (5.22), z_0, z_{k-1} and X are the only unknowns and $\delta_0,\delta_1,\delta_2,\delta_3$ are derived from γ,γ' and known coefficients $z_k,\ldots,z_{n-1}$. $X=-\gamma_t/\gamma_t$ if $\gamma_t+\gamma'_t X=0$ and this solution can be verified by δ_2,δ_3 and a known coefficient z_i in (5.22). Substituting (5.21) in (5.6) gives

$$\tau_0 X^{[n/2]}+\tau_1 X+\tau_2 = 0. \tag{5.23}$$

As the next step, we rise both sides of (5.22) to the $[-t]$-th power and obtain

$$z_{k-1} = \frac{a_1+a_2X^{[-t]}}{a_3+a_4X^{[-t]}}. \tag{5.24}$$

We also substitute (4.16) in (5.7) and rise both sides to the $[t]$-th power to get

$$u_1X^{[n/2]+1}+u_2X^{[n/2]}+u_3X+u_4 = 0. \tag{5.25}$$

Finally, one can substitute (5.23) into (5.25) and obtain the following quadratic polynomial equation over $\mathbb{F}_{q^n}$

$$\mu_1X^2+\mu_2X+\mu_3 = 0. \tag{5.26}$$

If $\mu_1=0$, then $X=-\mu_3/\mu_2$ and if $\mu_1\neq 0$, equation (5.26) can be reduced to

$$X^2+rX+s = 0, \tag{5.27}$$

where $r=\mu_2/\mu_1$ and $s=\mu_3/\mu_1$. When the characteristic of $\mathbb{F}_q$ is odd, equation (5.27) can be solved explicitly as follows:

a) if r^2-4s is a quadratic residue in $\mathbb{F}_{q^n}$, then it has two solutions $X=\frac{-r\pm\sqrt{r^2-4s}}{2}$;

b) if $r^2=4s$, then it has a single solution $X=-r/2$;

c) it has no solution in $\mathbb{F}_{q^n}$ otherwise.

When the characteristic of $\mathbb{F}_q$ is two, we have the following cases:

1. if $r = 0$, it has a single solution $X = s^{2^{nl-1}}$, where $q = 2^l$;
2. if $r \neq 0$, the equation (5.27) can be reduced to $y^2 + y = \beta$, where $X = ry$ and $\beta = s/r^2$. Then $y^2 + y = \beta$ has
   - no zero if $\sum_{i=0}^{n-1} \beta^{2^i} = 1$;
   - two zeros of the form $W = \sum_{j=1}^{n-1} \beta^{2^j} (\sum_{k=0}^{j-1} c^{2^k})$ and $W + 1$ where $\sum_{i=0}^{n-1} \beta^{2^i} = 0$ and c is any fixed element such that $\sum_{i=0}^{n-1} c^{2^i} = 1$.

We expect our quadratic equation to have roots X in $\mathbb{F}_{q^n}$ that lead to solutions $\gamma + X\gamma'$ in (5.19) and z_0 in (5.21). With the coefficients $\gamma_1, \ldots, \gamma_t$ and also the initial state $z_{n-1}, \ldots, z_{n-t}$, one can recursively compute $z_1, \ldots, z_{k-1}$ according to (5.18). Note that even if the equation (5.26) has two different solutions, they don't necessarily lead to correct coefficients of the error interpolation polynomial. In fact, by the expression of the Dickson matrix of $e_{\theta_1,\theta_2}(x)$, the correct $e_{\theta_1,\theta_2}(x)$ should have the sequence $(z_{n-1}, \ldots, z_{n-t}, \ldots)$ with period n. In other words, if the output sequence has period n, we know that the corresponding polynomial $e_{\theta_1,\theta_2}(x)$ is the desired error interpolation polynomial.

5.6 An improvement of the decoding of GTG and AGTG codes

In the interpolation-based decodings of GTG and AGTG codes in [16, 26, 29] and[11], when the rank of the error vector e is $t < \frac{n-k}{2}$, one can use any decoder of a Gabidulin code $\mathcal{GS}_{n,k+1}$ to recover the message. But when $t = \frac{n-k}{2}$, the problem of decoding the error vector is transformed to the problem of solving the projective polynomial $P(x) = x^{q^w+1} + u_1 x + u_2 = 0$ over $\mathbb{F}_{q^n}$. In the following, we show that how one can decode GTG and AGTG codes more efficiently if he/she communicates via the communication model $\mathcal{Q}_{\theta_1,\theta_2}$. Moreover, we show that one will be able to decode any error vector with rank $t \leq k$ added to a low rate GTG and AGTG code if one uses the second communication model. In this chapter by a low rate code we mean a code with $k \leq \lceil \frac{n-1}{2} \rceil$.

5.6.1 Decoding GTG and AGTG codes

Here we explain an improvement of the decoding algorithm for GTG codes and the same procedure can be applied to AGTG codes with some minor differences. In this subsection we assume n as an even positive integer. To be self-contained, we recall the decoding algorithm from [11] where the general communication model is replaced by the communication model $\mathcal{Q}_{\theta_1,\theta_2}$.

Encoding

The encoding of a message $m = (m_0, \ldots, m_{k-1})$ is the evaluation of the following linearized polynomial at ordered points $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$:

$$f(x) = \sum_{i=0}^{k-1} m_i x^{[i]} + \varepsilon m_0^{q^h} x^{[k]}. \tag{5.28}$$

Then the encoding of GTG codes can be expressed as

$$(m_0, m_1, \ldots, m_{k-1}) \mapsto c = (f(\alpha_0), \ldots, f(\alpha_{n-1})) = \tilde{m} \cdot M^T, \tag{5.29}$$

where $\tilde{m} = (m_0, \ldots, m_{k-1}, \varepsilon m_0^{q^h}, 0, \ldots, 0)$.

Decoding

Let the error vector $e = (e_0, \ldots, e_{n-1})$ of rank t be added to the codeword $c = (c_0 \ldots, c_{n-1})$ during transmission and let $r = (r_0 \ldots, r_{n-1}) = c + e$ be the received vector. Take $e(x)$ be the error interpolation polynomial of the form given in (5.5) where instead of (5.7) we have

$$z_k^{[n/2]} - z_k = \alpha_{\theta_2}. \tag{5.30}$$

Then

$$e(\alpha_i) = e_i = r_i - c_i, \quad i = 0, \ldots, n-1. \tag{5.31}$$

As we mentioned before, e is uniquely determined by the polynomial $e(x)$ and denote $z = (z_0, \ldots, z_{n-1})$. From (5.14) and (5.15) it follows that

$$r = c + e = (\tilde{m} + z) \cdot M^T.$$

This is equivalent to

$$\begin{aligned} r \cdot (M^T)^{-1} =& (m_0, m_1, \ldots, m_{k-1}, \varepsilon m_0^{q^h}, 0, \ldots, 0) + \\ & (z_0, z_1, \ldots, z_{k-1}, z_k, z_{k+1}, \ldots, z_{n-1}). \end{aligned}$$

Letting $\tilde{r} = (\eta_0, \ldots, \eta_{n-1}) = r \cdot (M^T)^{-1}$, we obtain

$$(z_{k+1}, \ldots, z_{n-1}) = (\eta_{k+1}, \ldots, \eta_{n-1}), \tag{5.32}$$

and we also have the relations (5.6) and (5.30). In (5.32) we have $n-k-1$ known coefficients z_i's, while in (5.16) we had $n-k$ known coefficients '$_i$'s.

Reconstructing the interpolation polynomial $e(x)$

If we write the 0th column E_0 of the Dickson matrix associated to $e(x)$ as the linear combination of $E_1,\ldots,E_t$ we will get the recursive equation

$$z_i = \gamma_1 z_{i-1}^{[1]} + \gamma_2 z_{i-2}^{[2]} + \cdots + \gamma_t z_{i-t}^{[t]}, \quad 0 \le i < n, \tag{5.33}$$

same as (5.18), where the subscripts in z_i's are taken modulo n. Recall that the elements $z_{k+1},\ldots,z_{n-1}$ are known from (5.32). Hence we obtain the following linear equations to replace the key equation in (5.19), with known coefficients z_i and variables $\gamma_1,\ldots,\gamma_t$:

$$z_i = \gamma_1 z_{i-1}^{[1]} + \gamma_2 z_{i-2}^{[2]} + \cdots + \gamma_t z_{i-t}^{[t]}, \; k+t+1 \le i < n. \tag{5.34}$$

For an error vector with $\mathrm{Rank}(e) = t \le \frac{n-k}{2}$, i.e., $2t+k \le n$, we can divide the discussion into two cases.

Case 1: $2t+k < n$. In this case, (5.34) contains $n-k-t-1 \ge t$ affine equations in variables $\gamma_1,\ldots,\gamma_t$, which has rank t. Hence the variables $\gamma_1,\ldots,\gamma_t$ can be uniquely determined. Any Gabidulin $\mathcal{GG}_{n,k+1}$ decoder can be applied. Here we assume the code has high code rate, for which the Berlekamp-Massey algorithm gives a better complexity. Although the recurrence equation (5.34) is a generalized version of the ones in [28] and [36], the modified Berlekamp-Massey algorithm can be applied here to recover the coefficients $\gamma_1,\ldots,\gamma_t$.

Case 2: $2t+k = n$. In this case (5.34) gives $n-k-t-1 = t-1$ independent affine equations in variables $\gamma_1,\ldots,\gamma_t$. For such an under-determined system of linear equations, we will have a set of solutions $(\gamma_1,\ldots,\gamma_t)$ that has dimension 1 over $\mathbb{F}_{q^n}$. Namely, the solutions will be of the form

$$\gamma + X\gamma' = (\gamma_1 + X\gamma_1', \ldots, \gamma_t + X\gamma_t'),$$

where γ, γ' are fixed elements in $\mathbb{F}_{q^n}^t$ and X runs through $\mathbb{F}_{q^n}$. As shown in [36, Th. 10], the solution can be derived from the modified BM algorithm with a free variable X.

Observe that in (5.33), by taking $i = 0$ and $i = k+t$ and substituting the solution $\gamma + X\gamma'$, one gets the following two equations

$$z_0 = \delta_0' + \delta_1' X, \tag{5.35}$$

and

$$z_{k+t} = \delta_2 + \delta_3 X + (\gamma_t + \gamma_t' X) z_k^{[t]}, \tag{5.36}$$

where in (5.35) and (5.36), z_0, z_k and X are unknowns. Using equations (5.6),(5.30), (5.35) and (5.36) instead of (5.6),(5.7), (5.21) and (5.22) and going through the same procedure in Subsection 5.5.3, we can get a quadratic equation of the form

$$\mu_1 X^2 + \mu_2 X + \mu_3 = 0. \tag{5.37}$$

which can be solved in polynomial time as discussed in Subsection 5.5.3. Hence, if the communication parties use the model $\mathcal{Q}_{\theta_1,\theta_2}$ to transfer their messages, then GTG and AGTG codes can be decoded with less time complexity.

5.7 Decoding error rank vectors with any rank $t \leq k$

In this subsection we consider the second communication model described in 5.4.2 , but the generated error vectors are still look random and they can have any rank up to n.

In the decoding of GTG codes in Subsection 5.6.1, let $\tilde{r} = (\eta_0, \ldots, \eta_{n-1}) = r \cdot (M^T)^{-1}$, then we obtain

$$(z_{k+1}, \ldots, z_{n-1}) = (\eta_{k+1}, \ldots, \eta_{n-1}), \tag{5.38}$$

and also based on the definition of GTG codes we have an auxiliary equation

$$-\varepsilon z_0^{q^h} + z_k = \eta_k - \varepsilon \eta_0^{q^h}, \tag{5.39}$$

since $\varepsilon m_0^{q^h} + z_k = \eta_k$, and $m_0 + z_0 = \eta_0$. Let $k \leq \lceil \frac{n-1}{2} \rceil$. If we use (5.8) ((5.10)) as the error interpolation polynomial, one can employ (5.9) ((5.11)) and directly obtain $z_1, \ldots, z_k$ from the known coefficients in (5.38). The only remaining unknown coefficient z_0 can be calculated using the auxiliary equation (5.39) since z_k is already calculated.

Hence, by restricting the error interpolation polynomial we can decode any rank error vector with rank $t \leq k$ added to a low rate GTG (AGTG) code.

Remark 3. *In [9], an application of space-symmetric rank errors in code-based cryptography is proposed. But space-symmetric rank errors similar to symmetric rank errors [6], contain some structures and this may lead to a new structural attack. If we use rank error vectors defined in Subsection 5.7 instead of space-symmetric rank errors and use GTG codes instead of Gabidulin codes in GPT variants [18] and [19], we can avoid potential structural attacks and possibly get the same key size found in [9, Section VI.]. This will be investigated in future works.*

Remark 4. *The advantage of the model $\mathcal{Q}_{\theta_1,\theta_2}$ or even the second model 5.4.2 is that it can generate error vectors that do not carry a specific structure since the structured coefficients' vector of the error interpolation polynomial goes through an interpolation process on linearly independent points. Even in subsection VI. the error space has dimension $n/2$ but it contains error with high or low ranks with no specific structure. So based on this observation, to find more suitable rank-based scheme, besides looking for new MRD codes and find the most efficient one, one can also look for new communication models with higher error correctability.*

5.8 Conclusion

In this chapter we made some delicate restrictions on the communication model and decode Gabidulin codes beyond half the minimum distance by one unit in polynomial time. The error vectors which are added to the codewords in our model, do not carry a specific structure. Moreover, we improved the decoding algorithms for GTG and AGTG codes proposed in [26] and [11], if two parties communicate through the first defined models. We are also able to decode any error vector with any rank $t \leq k$ added to low rate ($k \leq \lceil \frac{n-1}{2} \rceil$) GTG and AGTG codes if we employ the second communication model.

Bibliography

[1] Bence Csajbók, Giuseppe Marino, Olga Polverino, and Ferdinando Zullo. A characterization of linearized polynomials with maximum kernel. *Finite Fields and Their Applications*, 56:109 – 130, 2019.

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

[3] L.E. Dickson. *Linear Groups, with an Exposition of the Galois Field Theory - Scholar's Choice Edition*. Creative Media Partners, LLC, 2015.

[4] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In Donald W. Davies, editor, *Advances in Cryptology – EUROCRYPT'91*, pages 482–489. Springer, 1991.

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

[6] Ernst M. Gabidulin and Nina I. Pilipchuk. Symmetric rank codes. *Problems of Information Transmission*, 40:103 – 117, 2004.

[7] Ernst M. Gabidulin and Nina I. Pilipchuk. Symmetric matrices and codes correcting rank errors beyond the $\lfloor (d-1)/2 \rfloor$ bound. *Discrete Applied Mathematics*, 154(2):305–312, 2006. Coding and Cryptography.

[8] Rod Gow and Rachel Quinlan. Galois theory and linear algebra. *Linear Algebra and its Applications*, 430(7):1778 – 1789, 2009. Special Issue in Honor of Thomas J. Laffey.

[9] Thomas Jerkovits, Vladimir Sidorenko, and Antonia Wachter-Zeh. Decoding of space-symmetric rank errors, 2021.

[10] Wrya K. Kadir. New communication models and decoding of maximum rank distance codes. In *2021 XVII International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY)*, pages 125–130, 2021.

[11] Wrya K. Kadir and Chunlei Li. On decoding additive generalized twisted Gabidulin codes. *Cryptography and Communications*, 12:987 – 1009, 2020.

[12] Wrya K. Kadir, Chunlei Li, and Ferdinando Zullo. Decoding a class of maximum hermitian rank metric codes. *Submitted to The 6th International Workshop on Boolean Functions and their Applications (BFA)*, 2021.

[13] Wrya K. Kadir, Chunlei Li, and Ferdinando Zullo. On interpolation-based decoding of a class of maximum rank distance codes. *in International Symposium on Information Theory (ISIT)*, 2021.

[14] Alexander Kshevetskiy and Ernst Gabidulin. The new construction of rank codes. In *International Symposium on Information Theory, (ISIT)*, pages 2105–2108. IEEE, 2005.

[15] Chunlei Li. Interpolation-based decoding of nonlinear maximum rank distance codes. In *International Symposium on Information Theory (ISIT)*, 2019.

[16] Chunlei Li and Wrya K. Kadir. On decoding additive generalized twisted Gabidulin codes. *presented at the International Workshop on Coding and Cryptography (WCC)*, 2019.

[17] Pierre Loidreau. A Welch–Berlekamp like algorithm for decoding Gabidulin codes. In Øyvind Ytrehus, editor, *International Workshop on Coding and Cryptography (WCC)*, pages 36–45, Berlin, Heidelberg, 2006. Springer.

[18] Pierre Loidreau. An evolution of gpt cryptosystem. In *Int. Workshop Alg. Combin. Coding Theory (ACCT)*, 2016.

[19] Pierre Loidreau. A new rank metric codes based encryption scheme. In *International Workshop on Post-Quantum Cryptography*, pages 3–17. Springer, 2017.

[20] G. Lunardon, R. Trombetti, and Y. Zhou. Generalized twisted gabidulin codes. *Journal of Combinatorial Theory, Series A*, 159:79–106, 2018.

[21] Gary McGuire and John Sheekey. A characterization of the number of roots of linearized and projective polynomials in the field of coefficients. *Finite Fields and Their Applications*, 57:68 – 91, 2019.

[22] Giampaolo Menichetti. Roots of affine polynomials. In A. Barlotti, M. Biliotti, A. Cossu, G. Korchmaros, and G. Tallini, editors, *Combinatorics '84*, volume 123 of *North-Holland Mathematics Studies*, pages 303–310. North-Holland, 1986.

[23] Kamil Otal and Ferruh Özbudak. Additive rank metric codes. *IEEE Transactions on Information Theory*, 63(1):164–168, 2017.

[24] Kamil Otal and Ferruh Özbudak. Some new non-additive maximum rank distance codes. *Finite Fields and Their Applications*, 50:293 – 303, 2018.

[25] Nina I. Pilipchuk and Ernst M. Gabidulin. On codes correcting symmetric rank errors. In Øyvind Ytrehus, editor, *Coding and Cryptography*, pages 14–21, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[26] Tovohery Hajatiana Randrianarisoa. A decoding algorithm for rank metric codes. *arXiv.org.*, abs/1712.07060, 2017.

[27] Julian Renner, Thomas Jerkovits, Hannes Bartz, Sven Puchinger, Pierre Loidreau, and Antonia Wachter-Zeh. Randomized decoding of gabidulin codes beyond the unique decoding radius. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography*, pages 3–19, Cham, 2020. Springer International Publishing.

[28] G. Richter and S. Plass. Fast decoding of rank-codes with rank errors and column erasures. In *International Symposium on Information Theory (ISIT)*, pages 398–398, June 2004.

[29] Joachim Rosenthal and Tovohery Hajatiana Randrianarisoa. A decoding algorithm for twisted Gabidulin codes. In *International Symposium on Information Theory (ISIT)*, pages 2771–2774. IEEE, 2017.

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

[31] Ron M Roth. Tensor codes for the rank metric. *IEEE Transactions on Information Theory*, 42(6):2146–2157, 1996.

[32] Kai-Uwe Schmidt. Hermitian rank distance codes. *Designs, Codes and Cryptography*, 86(7):1469–1481, 2018.

[33] John Sheekey. A new family of linear maximum rank distance codes. *Advances in Mathematics of Communications*, 10:475, 2016.

[34] John Sheekey. MRD codes: Constructions and connections. *arXiv.org.*, abs/1904.05813, 2019.

[35] John Sheekey. New semifields and new MRD codes from skew polynomial rings. *Journal of the London Mathematical Society*, 101(1):432–456, 2020.

[36] V. Sidorenko, G. Richter, and M. Bossert. Linearized shift-register synthesis. *IEEE Transactions on Information Theory*, 57(9):6025–6032, Sep. 2011.

[37] D. Silva, F. R. Kschischang, and R. Koetter. A rank-metric approach to error control in random network coding. *IEEE Transactions on Information Theory*, 54(9):3951–3967, Sept 2008.

[38] R. Trombetti and Y. Zhou. A new family of MRD codes in $\mathbb{F}_q^{2n\times 2n}$ with right and middle nuclei $\mathbb{F}_{q^n}$. *IEEE Transactions on Information Theory*, 65(2):1054–1062, 2019.

Chapter 6

Encoding and Decoding of Several Optimal Rank Metric Codes

This chapter presents encoding and decoding algorithms for several families of optimal rank metric codes whose codes are in restricted forms of symmetric, alternating and Hermitian matrices. First, we show the evaluation encoding is the right choice for these codes and then we provide easily reversible encoding methods for each family. Later unique decoding algorithms for the codes are described. The decoding algorithms are interpolation-based and can uniquely correct errors for each code with rank up to $\lfloor (d-1)/2 \rfloor$ in polynomial-time, where d is the minimum distance of the code. This chapter is based on my work with Chunlei Li and Ferdinando Zullo [13]. The sections related to the encoding and decoding algorithms for optimal Hermitian (Theorem 36) were presented in BFA 2021 conference [11].

6.1 Introduction

Rank metric codes were introduced first by Delsarte in [2], and independently by Gabidulin in [14] and Roth in [29]. They have been extensively investigated because of their applications in crisscross error correction [29], cryptography [7] and network coding [37]. The coding-theoretic properties of these codes have been studied in detail, and constructions of optimal codes with respect to a Singleton-like bound, known as MRD codes, have been found. An interested reader may refer to [8, 33] for more details.

Known decoding algorithms for MRD codes can be generally classified in two different approaches: syndrome-based decoding as in [5, 6, 27, 29] and interpolation-based decoding as in [9, 10, 15, 16, 18, 26]. Gabidulin in [6] solves the key equation in the decoding process by employing the linearized version of *extended Euclidean (LEE) algorithm*, while in [27], the key equation was solved by a linearized version of *Berlekamp-Massey (BM) algorithm*. The error values in both decoding algorithms in [6] and [27] are computed by an algorithm called *Gabidulin algorithm*. Loidreau in [18] proposed the first interpolation-based decoding approach for MRD codes and considered the analogue of *Welch-Berlekamp (WB) algorithm*, which was originally used to decode Reed-Solomon codes [40]. The algorithm directly gives the code's interpolation polynomial and computing the error vector is not required in the de-

coding process.

In [34], Sheekey proposed the first family of MRD codes over $\mathbb{F}_{q^n}$ which is linear over $\mathbb{F}_q$ (instead of $\mathbb{F}_{q^n}$ as the well-known Gabidulin codes) and his idea were used later to introduce new MRD codes that are linear over a sub-field of $\mathbb{F}_{q^n}$ [20, 22, 23, 24, 38]. When the rank of the error vector reaches the maximum unique decoding radius, the syndrome-based decoding approach works only for MRD codes that are linear over the main extension field. Randrianarisoa in [26, 28], gave an interpolation based decoding algorithm for twisted Gabidulin codes. Later this idea was adopted to decode additive generalized twisted Gabidulin codes and Trombetti-Zhou rank metric codes [10, 12]. Again BM algorithm is involved in the process of solving the key equations in [10] and [12] and it reduces the decoding problem to the problem of solving the projective polynomial equation $x^{q^\nu+1}+ax+b=0$ and quadratic polynomial equation $x^2+cx+d=0$ over $\mathbb{F}_{q^n}$, respectively. A similar idea is also used in [9] to decode Gabidulin codes beyond half the minimum distance. All the decoding algorithms described above have polynomial-time complexities. The result in [36] shows that when low-complexity normal basis are used, the complexity can be reduced even further. Solving the key equations carried out by BM or LEE algorithm are the most expensive steps in the above decoding algorithms.

Besides the aforementioned new MRD codes, there are also some restricted rank metric codes that are linear over a subfield of $\mathbb{F}_{q^n}$ which are not defined based on Sheekeys' idea. The study of subsets of *restricted* matrices equipped with rank metric was started in 1975 by Delsarte and Goethals in [3], in which they considered sets of alternating bilinear forms. The theory developed in [2] and [3] found applications also in the classical coding theory. Indeed, the evaluations of the forms found in [3] give rise to subcodes of the second-order Reed-Muller codes, including the Kerdock code and the chain of Delsarte–Goethals codes; see also [30].

Using the theory of association schemes, bounds, constructions and structural properties of restricted rank metric codes have been investigated in symmetric matrices [19, 31, 41], alternating matrices [3] and Hermitian matrices [32, 39].

In this chapter we will present both encoding and decoding algorithms for several optimal symmetric, alternating and Hermitian rank metric codes. Since the targeted codes are not linear over the extension field, syndrome-based decoding algorithms in [6] is not applicable. We choose interpolation-based decoding approach which is able to decode errors up to half of the minimum distance in polynomial time for all the aforementioned codes. A part of our work in this chapter responds to a suggestion in [1], where the authors suggested studying the decoding of Hermitian rank metric codes.

6.2 Preliminaries

Let $\mathbb{F}_\rho$ denote a finite field of ρ elements and $\mathbb{F}_\rho^{n\times n}$ be the set of the square matrices of order n defined over $\mathbb{F}_\rho$. We can equip $\mathbb{F}_\rho^{n\times n}$ with the following metric

$$d_r(A,B)=\mathrm{rk}(A-B),$$

where $\mathrm{rk}(A-B)$ is the rank of the difference matrix $A-B$. If $\mathcal{C}$ is a subset of $\mathbb{F}_{\rho}^{n\times n}$ with the property that

$$d = \min\{\mathrm{rk}(A-B)\colon A,B\in\mathcal{C}, A\neq B\},$$

then $\mathcal{C}$ is called a *rank metric code with minimum distance d*, or that $\mathcal{C}$ is a *d-code*, see e.g. [30]. A rank metric code $\mathcal{C}$ is said to be *additive* if it is closed under the classical matrix addition $+$ and said to be *linear* over a subfield $\mathbb{E}$ of $\mathbb{F}_{\rho}$ if it is closed under both matrix addition and scalar multiplication by any element in $\mathbb{E}$.

Let $\mathcal{L}_{n,\rho}$ denote the quotient $\mathbb{F}$-algebra of all *ρ-polynomials* over $\mathbb{F}_{\rho^n}$ with degree smaller than n , namely,

$$\mathcal{L}_{n,\rho} = \left\{ \sum_{i=0}^{n-1} a_i x^{\rho^i} \colon a_i \in \mathbb{F}_{\rho^n} \right\}.$$

It is well known that the $\mathbb{F}_{\rho}$-algebra $\mathcal{L}_{n,\rho}$ is actually isomorphic to the $\mathbb{F}_{\rho}$-algebra $\mathbb{F}_{\rho}^{n\times n}$. Hence many rank metric codes $\mathcal{C}\subseteq\mathbb{F}_{\rho}^{n\times n}$ are expressed in terms of ρ-polynomials in $\mathcal{L}_{n,\rho}$. If ρ is fixed or the context is clear, we can use the term *linearized polynomials* instead of ρ-polynomials.

Here we recall one important property of the Dickson matrix associated with ρ-polynomials which is critical for the decoding in this chapter.

Proposition 13. *Let $L(x)=\sum_{i=0}^{n-1} a_i x^{\rho^i}$ over $\mathbb{F}_{\rho^n}$ be a ρ-polynomial with rank t. Then its associated Dickson matrix*

$$D = \left(a_{i-j(\mathrm{mod}n)}^{\rho^i}\right)_{n\times n} = \begin{pmatrix} a_0 & a_{n-1}^{\rho} & \cdots & a_1^{\rho^{n-1}} \\ a_1 & a_0^{\rho} & \cdots & a_2^{\rho^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2}^{\rho} & \cdots & a_0^{\rho^{n-1}} \end{pmatrix}, \tag{6.1}$$

has rank t over $\mathbb{F}_{\rho^n}$ and any $t\times t$ submatrix formed by t consecutive rows and t consecutive columns in D is non-singular.

For the first part of the above result see [4, 21], whereas for the last part we refer to [26].

Below we shall introduce three families of rank metric codes whose codewords have restrictive forms. The first two consist of symmetric and alternating matrices over $\mathbb{F}_q$, respectively, and the third one consists of Hermitian matrices defined over $\mathbb{F}_{q^2}$, where q is a prime power.

Recall that a matrix $A\in\mathbb{F}_q^{n\times n}$ is said to be *symmetric* if $A^T=A$ and is said to be *alternating* if $A^T=-A$, where A^T is the transpose matrix of A. Let $\mathrm{S}_n(q)$ and $\mathrm{A}_n(q)$ be the set of all symmetric matrices and alternating matrices of order n over $\mathbb{F}_q$, respectively. Following the connection given in [19], the set $\mathrm{S}_n(q)$ can be identified as

$$\mathcal{S}_n(q) = \left\{ \sum_{i=0}^{n-1} c_i x^{q^i} \colon c_{n-i} = c_i^{q^{n-i}} \text{ for } i\in\{0,\ldots,n-1\} \right\} \subseteq \mathcal{L}_{n,q}.$$

The set $\mathrm{A}_n(q)$ can be identified as

$$\mathcal{A}_n(q) = \left\{ \sum_{i=0}^{n-1} c_i x^{q^i} : c_{n-i} = -c_i^{q^{n-i}} \text{ for } i \in \{0,\dots,n-1\} \right\} \subseteq \mathcal{L}_{n,q}.$$

Consider the conjugation map $\bar{\cdot}$ from $\mathbb{F}_{q^2}$ to itself: $x \mapsto \bar{x} = x^q$. For a matrix $A \in \mathbb{F}_{q^2}^{n\times n}$, we denote by A^* the conjugate transpose of A, which is obtained by applying the conjugate map to all entries of A^T. Recall that a matrix $A \in \mathbb{F}_{q^2}^{n\times n}$ is said to be *Hermitian* if $A = A^*$. Let $\mathrm{H}_n(q^2)$ be the set of all Hermitian matrices of order n over $\mathbb{F}_{q^2}$. Similarly, it can be identified as

$$\mathcal{H}_n(q^2) = \left\{ \sum_{i=0}^{n-1} c_i x^{q^{2i}} : c_{n-i+1} = c_i^{q^{2n-2i+1}} \text{ for } i \in \{0,\dots,n-1\} \right\} \subseteq \mathcal{L}_{n,q^2},$$

where the indices are taken modulo n. Note that if n is odd then $c_{(n+1)/2}$ belongs to $\mathbb{F}_{q^n}$.

It can be easily verified that these three sets, together with the classical sum of matrices and the scalar multiplication by elements in $\mathbb{F}_q$, are $\mathbb{F}_q$-vector spaces with dimensions

$$\dim_{\mathbb{F}_q}(\mathrm{S}_n(q)) = \frac{n(n+1)}{2},\ \dim_{\mathbb{F}_q}(\mathrm{A}_n(q)) = \frac{n(n-1)}{2},\ \dim_{\mathbb{F}_q}(\mathrm{H}_n(q^2)) = n^2.$$

A subset of $\mathrm{S}_n(q)$, $\mathrm{A}_n(q)$ or $\mathrm{H}_n(q^2)$ endowed with the rank distance will be termed a symmetric, alternating or Hermitian rank metric code, respectively, or symmetric, alternating or Hermitian d-code if d is the minimum distance of the considered code. With the isomorphism between $\mathbb{F}_\rho^{n\times n}$ and $\mathcal{L}_{n,\rho}$, $\rho \in \{q, q^2\}$, the codewords in these restricted rank metric codes will be represented in polynomials throughout this chapter. For simplicity, we will denote by $x^{[i]} := x^{q^i}$ and $x^{[\![i]\!]} := x^{q^{2i}}$ for any non-negative integer i.

6.2.1 Optimal Symmetric and Alternating d-Codes

For symmetric and alternating rank metric codes, the following bounds on their size have been established [3, 31].

Theorem 30. *[31, Theorem 3.3] Let $\mathcal{C}$ be a symmetric d-code in $\mathbb{F}_q^{n\times n}$. If d is even, suppose also that $\mathcal{C}$ is additive. Then*

$$\#\mathcal{C} \le \begin{cases} q^{n(n-d+2)/2} & \text{if } n-d \text{ is even,} \\ q^{(n+1)(n-d+2)/2} & \text{if } n-d \text{ is odd.} \end{cases}$$

Theorem 31. *[3, Theorem 4] Let $m = \lfloor \frac{n}{2} \rfloor$. Let $\mathcal{C}$ be an alternating $2e$-code in $\mathbb{F}_q^{n\times n}$. Then*

$$\#\mathcal{C} \le q^{\frac{n(n-1)}{2m}(m-e+1)}.$$

A symmetric (resp. alternating) d-code is said to be *optimal* if its parameters satisfy the equality in Theorem 30 (resp. Theorem 31). The following theorems present some instances of

optimal symmetric (resp. alternating) d-codes, where $\mathrm{Tr}_{q^n/q}(x) = x + x^q + \cdots + x^{q^{n-1}}$ is the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$.

Theorem 32. *[31, Theorem 4.4] Let n and d be two positive integers such that $1 \le d \le n$ and $n-d$ is even. The symmetric forms $S : \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \to \mathbb{F}_q$ given by $S(x,y) = \mathrm{Tr}_{q^n/q}(yL(x))$ with*

$$L(x) = b_0 x + \sum_{j=1}^{\frac{n-d}{2}} \left(b_j x^{q^j} + (b_j x)^{q^{n-j}} \right), \tag{6.2}$$

as $b_0, \ldots, b_{\frac{n-d}{2}}$ range over $\mathbb{F}_{q^n}$, form an additive optimal d-code in $\mathrm{S}_n(q)$.

In [31, Theorem 4.1] it has been shown that constructions of optimal symmetric d-codes with $n-d$ odd in $\mathrm{S}_n(d)$ can be obtained by puncturing the examples of optimal symmetric d-codes found in [31, Theorem 4.4].

Theorem 33. *[3, Theorem 7] Let n and e be two positive integers such that n is odd and $1 \le 2e \le n-1$, and let $d = 2e$. The alternating forms $A : \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \to \mathbb{F}_q$ given by $A(x,y) = \mathrm{Tr}_{q^n/q}(yL(x))$ with*

$$L(x) = \sum_{j=e}^{\frac{n-1}{2}} \left(b_j x^{q^j} - (b_j x)^{q^{n-j}} \right), \tag{6.3}$$

as $b_e, \ldots, b_{\frac{n-1}{2}}$ range over $\mathbb{F}_{q^n}$, form an additive optimal d-code in $\mathrm{A}_n(q)$.

6.2.2 Optimal Hermitian d-Codes

Schmidt characterized the upper bound on the size of Hermitian d-codes as follows [32, Theorem 1].

Theorem 34. *[32, Theorem 1] An additive Hermitian d-code $\mathcal{C}$ in $\mathbb{F}_{q^2}^{n \times n}$ satisfies*

$$\#\mathcal{C} \le q^{n(n-d+1)}.$$

Moreover, when d is odd, this upper bound holds also for non-additive Hermitian d-codes.

A Hermitian d-code is called a *optimal* Hermitian d-code if it attains the above bound. Schmidt in [32] also gave constructions for optimal Hermitian d-codes for all possible value of n and d, except if n and d are both even and $3 < d < n$. There are some examples of optimal Hermitian d-codes, see [32, 39]. We recall two examples given in [32, Theorems 4 and 5], where Tr_{q^{2n}/q^2} is the trace function from $\mathbb{F}_{q^{2n}}$ to $\mathbb{F}_{q^2}$.

Theorem 35. *[32, Theorem 4] Let n and d be integers of opposite parity satisfying $1 \le d \le n$. The Hermitian forms $H : \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}} \to \mathbb{F}_{q^2}$ given by $H(x,y) = \mathrm{Tr}_{q^{2n}/q^2}(y^q L(x))$ with*

$$L(x) = \sum_{j=1}^{\frac{n-d+1}{2}} \left((b_j x)^{q^{(2n-2j+2)}} + b_j^q x^{q^{(2j)}} \right), \tag{6.4}$$

as $b_1, \ldots, b_{\frac{n-d+1}{2}}$ range over $\mathbb{F}_{q^{2n}}$, form an additive optimal d-code in $\mathrm{H}_n(q^2)$.

Theorem 36. *[32, Theorem 5] Let n and d be odd integers satisfying $1 \leq d \leq n$. The Hermitian forms $H : \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}} \to \mathbb{F}_{q^2}$ given by $H(x,y) = \mathrm{Tr}_{q^{2n}/q^2}(y^q L(x))$ with*

$$L(x) = (b_0 x)^{q^{(n+1)}} + \sum_{j=1}^{\frac{n-d}{2}} \left((b_j x)^{q^{(n+2j+1)}} + b_j^q x^{q^{(n-2j+1)}} \right), \tag{6.5}$$

as b_0 ranges over $\mathbb{F}_{q^n}$ and $b_1, \ldots, b_{\frac{n-d}{2}}$ range over $\mathbb{F}_{q^{2n}}$, form an additive optimal d-code in $\mathrm{H}_n(q^2)$.

6.3 Encoding

In the literature, no encoding method has been given for symmetric, alternating and Hermitian d-codes. This section is dedicated to the encoding of these three types of restricted d-codes. As a matter of fact, the encoding of an optimal d-code $\mathcal{C}$ is mainly concerned with setting up a one-to-one correspondence between a message space of size $\#\mathcal{C}$ and the code $\mathcal{C}$ in an efficient way, which ideally also allows for an efficient decoding algorithm.

6.3.1 Encoding of symmetric d-codes

We start with the encoding of the optimal symmetric d-codes of size $q^{n(n-d+2)/2}$ in Theorem 32, where $n-d$ is even. The family of codes is linear over $\mathbb{F}_q$ and the message space is naturally a vector space over $\mathbb{F}_q$ with dimension $n(n-d+2)/2$. But we can represent each message in the form of a k-dimensional vector over $\mathbb{F}_{q^n}$ where $k = (n-d+2)/2$ and the set of all the message vectors are closed under $\mathbb{F}_q$-linear operations.

In order to present a polynomial-time decoding algorithm for the optimal symmetric d-codes in Theorem 32, we shall express their codewords as evaluations of certain polynomials at linearly independent points over $\mathbb{F}_q$. For this reason, we need to employ a pair of dual bases in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Recall that given an ordered $\mathbb{F}_q$-basis $(\alpha_1, \ldots, \alpha_n)$ of $\mathbb{F}_{q^n}$, its dual basis is defined as the ordered $\mathbb{F}_q$-basis $(\beta_1, \ldots, \beta_n)$ of $\mathbb{F}_{q^n}$ such that

$$\mathrm{Tr}_{q^n/q}(\alpha_i \beta_j) = \delta_{ij} \text{ for } i = 1, 2, \ldots, n,$$

where δ_{ij} denotes the Kronecker delta function. Note that a dual basis always exists for a given order basis $(\alpha_1, \ldots, \alpha_n)$ of $\mathbb{F}_{q^n}$ [17, Definition 2.30].

Let $(\alpha_1, \ldots, \alpha_n)$, $(\beta_1, \ldots, \beta_n)$ be a pair of dual bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. We will write $\mathrm{Tr}_{q^n/q}(x)$ as $\mathrm{Tr}(x)$ for simplicity when the context is clear. Let $L(x)$ be a linearized polynomial as in Theorem 32. For the symmetric form we have

$$S(x,y) = \mathrm{Tr}(xL(y)).$$

Now, we denote the associated matrix of S with respect to the ordered $\mathbb{F}_q$-basis $(\alpha_1, \ldots, \alpha_n)$ by

$\mathcal{S}$, of which the (i,j)-th entry $\mathcal{S}(i,j)$ is given by

$$\mathcal{S}(i,j) = S(\alpha_i, \alpha_j) = \mathrm{Tr}(\alpha_j L(\alpha_i)).$$

Furthermore, the codewords of the additive d-code in Theorem 32 can be expressed in the symmetric matrix form as follows: let $x, y \in \mathbb{F}_{q^n}$, then $x = \sum_{i=1}^{n} x_i \alpha_i$ and $y = \sum_{j=1}^{n} y_j \alpha_j$ for some $x_i, y_j \in \mathbb{F}_q$ and

$$\begin{aligned} S(x,y) &= \mathrm{Tr}\left(\Big(\sum_j y_j \alpha_j \Big) \sum_i x_i L(\alpha_i) \right) = \mathrm{Tr}\left(\sum_{i,j} x_i y_j \alpha_j L(\alpha_i) \right) \\ &= \sum_{i,j} x_i y_j \mathrm{Tr}\big(\alpha_j L(\alpha_i)\big) = \sum_{i,j} x_i \mathcal{S}(i,j) y_j = (x_1, \ldots, x_n) \cdot \mathcal{S} \cdot \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}, \end{aligned}$$

where $\mathcal{S}(i,j)$ is the (i,j)-th entry in $\mathcal{S}$.

In the following we show that the evaluation of the corresponding linearized polynomial at linearly independent elements $\alpha_1, \ldots, \alpha_n$ is a proper encoding method.

Define an n-dimensional vector over $\mathbb{F}_q$ as

$$s = (s_1, \ldots, s_n) = (\beta_1, \ldots, \beta_n) \cdot \mathcal{S}^T.$$

Since the i-th row of $\mathcal{S}$ is given by $(\mathrm{Tr}(\alpha_1 L(\alpha_i)), \ldots, \mathrm{Tr}(\alpha_n L(\alpha_i)))$ and since each $L(\alpha_i)$ can be written as $\sum_t c_t \beta_t$ for some $c_t \in \mathbb{F}_q$, we can write s_i as

$$\begin{aligned} s_i &= \sum_j \beta_j S(i,j) = \sum_j \beta_j \mathrm{Tr}(\alpha_j L(\alpha_i)) \\ &= \sum_j \beta_j \mathrm{Tr}\big(\alpha_j \sum_t c_t \beta_t\big) = \sum_j \beta_j \sum_t c_t \mathrm{Tr}(\alpha_j \beta_t) \\ &= \sum_j \beta_j c_j = L(\alpha_i) \end{aligned}$$

since $\mathrm{Tr}(x)$ is linear over $\mathbb{F}_q$ and $(\beta_1, \ldots, \beta_n)$ is the dual basis of $(\alpha_1, \ldots, \alpha_n)$. From the equality $s_i = L(\alpha_i)$, we see that the encoding of symmetric d-codes given by $\mathrm{Tr}(yL(x))$, as in Theorems 32 and 33, can be seen as the evaluation of $L(x)$ at the basis $(\alpha_1, \ldots, \alpha_n)$ of $\mathbb{F}_{q^n}$.

With the above preparation, we are now ready to look at the encoding of the optimal symmetric d-codes in Theorem 32 more explicitly.

Let $\omega_0, \ldots, \omega_{n-1}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. For optimal symmetric d-codes in Theorem 32, the linearized polynomial can be expressed as

$$L(x) = b_0 x + \sum_{j=1}^{k-1} \left(b_j x^{[j]} + (b_j x)^{[n-j]} \right),$$

where $k = (n-d+2)/2$. Then the encoding of a message $f = (f_0, \ldots, f_{k-1}) \in \mathbb{F}_{q^n}^k$ for the symmetric codes in Theorem 32 can be expressed as the evaluation of the following linearized polynomial at points $\omega_0, \ldots, \omega_{n-1}$:

$$L(x) = f_0 x + \left(\sum_{j=1}^{k-1} f_j x^{[j]} + (f_j x)^{[n-j]} \right) = \sum_{i=0}^{n-1} \tilde{f}_i x^{[i]},$$

where

$$\begin{aligned} \tilde{f} &= (\tilde{f}_0, \ldots, \tilde{f}_{k-1}, 0, \ldots, 0, \tilde{f}_{n-k+1}, \ldots, \tilde{f}_{n-1}) \\ &= (f_0, \ldots, f_{k-1}, 0, \ldots, 0, f_{k-1}^{[n-k+1]}, \ldots, f_1^{[n-1]}). \end{aligned} \tag{6.6}$$

Let $N = \left(\omega_i^{[j]} \right)_{n \times n}$ be the $n \times n$ *Moore matrix* generated by ω_i's. So the encoding of optimal symmetric and optimal alternating d-codes can be expressed as

$$(f_0, \ldots, f_{k-1}) \mapsto (L(\omega_0), \ldots, L(\omega_{n-1})) = \tilde{f} \cdot N^T, \tag{6.7}$$

where $\tilde{f} = (\tilde{f}_0, \ldots, \tilde{f}_{n-1})$ and N^T is the transpose of the matrix N. Note that the first k and the last $k-1$ elements of $\tilde{f}$ are nonzero. This means at most $n-d+1$ columns of the matrix N^T are involved in the encoding process.

6.3.2 Encoding of alternating d-codes

The encoding of alternating d-codes in Theorem 33 can be done similarly since the codewords in $A(x,y)$ has the same form $\mathrm{Tr}(yL(x))$ as in Theorem 32.

For alternating d-codes in Theorem 33, the linearized polynomial can be expressed as

$$L(x) = \sum_{j=e}^{\frac{n-1}{2}} \left(b_j x^{[j]} - (b_j x)^{[n-j]} \right).$$

Note that in Theorem 33, the parameters n is odd and $d = 2e$. The optimal alternating codes are $\mathbb{F}_q$-linear with dimension $n(n-d+1)/2$. For simplicity, we again consider the message vectors in the form of vectors over $\mathbb{F}_{q^n}$.

Let $(\omega_0, \ldots, \omega_{n-1})$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The encoding of a message $f = (f_0, \ldots, f_{k-1}) \in \mathbb{F}_{q^n}^k$ can be expressed as the evaluation of the following linearized polynomial at points $\omega_0, \ldots, \omega_{n-1}$:

$$L(x) = \left(\sum_{j=e}^{\frac{n-1}{2}} f_{j-e} x^{[j]} - (f_{j-e} x)^{[n-j]} \right) = \sum_{i=0}^{n-1} \tilde{f}_i x^{[i]},$$

where

$$\begin{aligned} \tilde{f} &= (0, \ldots, 0, \tilde{f}_e, \ldots, \tilde{f}_{\frac{n-1}{2}}, \tilde{f}_{\frac{n+1}{2}}, \ldots, \tilde{f}_{n-e}, 0, \ldots, 0) \\ &= (0, \ldots, 0, f_0, \ldots, f_{k-1}, -f_{k-1}^{[\frac{n+1}{2}]}, \ldots, -f_0^{[n-e]}, 0, \ldots, 0). \end{aligned} \tag{6.8}$$

Similarly, the encoding of optimal alternating d-code can be expressed as

$$(f_0,\dots,f_{k-1}) \mapsto (L(\omega_0),\dots,L(\omega_{n-1})) = \tilde{f}\cdot N^T, \tag{6.9}$$

where $\tilde{f} = (\tilde{f}_0,\dots,\tilde{f}_{n-1})$ and N^T is the transpose of the matrix N. As shown in (6.8), at most $n-d+1$ columns of the matrix N are involved in computation.

6.3.3 Encoding of Hermitian d-codes

This section is dedicated to the encoding of the optimal Hermitian d-codes of size $q^{n(n-d+1)}$ explained in Theorems 35 and 36. Given positive integers d,n with $1 \le d \le n$, for encoding of optimal Hermitian d-codes we are going to set up a one-to-one correspondence between a message space of size $q^{n(n-d+1)}$, and Hermitian optimal d-code, which later permits us to decode efficiently. Therefore, for a message space of size $q^{n(n-d+1)}$, we may assume its elements as vectors over $\mathbb{F}_{q^n}$ of dimension $k = n-d+1$.

For the optimal Hermitian d-codes in Theorems 35 and 36, we shall express their codewords as evaluations of certain polynomials at linearly independent points over $\mathbb{F}_{q^2}$. For this reason, we need to introduce the Hermitian variant of a basis in $\mathbb{F}_{q^{2n}}$ over $\mathbb{F}_{q^2}$. Given an ordered $\mathbb{F}_{q^2}$-basis $(\alpha_1,\dots,\alpha_n)$ of $\mathbb{F}_{q^{2n}}$, its *Hermitian dual basis* is defined as the ordered $\mathbb{F}_{q^2}$-basis $(\beta_1,\dots,\beta_n)$ of $\mathbb{F}_{q^{2n}}$ such that

$$\mathrm{Tr}_{q^{2n}/q^2}(\alpha_i^q\beta_j) = \delta_{ij} \text{ for } i = 1,2,\dots,n,$$

where Tr_{q^{2n}/q^2} is the relative trace function from $\mathbb{F}_{q^{2n}}$ to $\mathbb{F}_{q^2}$, namely, $\mathrm{Tr}_{q^{2n}/q^2}(x) = \sum_{i=0}^{n-1} x^{q^{2i}}$ and δ_{ij} denotes the Kronecker delta function. Note that such a Hermitian dual basis always exists for a given order basis $(\alpha_1,\dots,\alpha_n)$. Indeed, since there exist a dual basis $(\gamma_1,\dots,\gamma_n)$ for $(\alpha_1,\dots,\alpha_n)$ satisfying $\mathrm{Tr}_{q^{2n}/q^2}(\alpha_i\gamma_j) = \delta_{ij}$, one can simply takes $\beta_j = \gamma_j^{q^{2n-1}}$ for $j = 1,2,\dots,n$ and then the above Hermitian dual property follows. We shall also write $\mathrm{Tr}_{q^{2n}/q^2}()$ as $\mathrm{Tr}()$ for simplicity whenever there is no ambiguity.

Let $(\alpha_1,\dots,\alpha_n)$ be an $\mathbb{F}_{q^2}$-basis of $\mathbb{F}_{q^{2n}}$ and $(\beta_1,\dots,\beta_n)$ be its Hermitian dual as described above. Let $x,y \in \mathbb{F}_{q^{2n}}$, then $x = \sum_{i=1}^{n} x_i\alpha_i$ and $y = \sum_{i=1}^{n} y_i\beta_i$, for some $x_i,y_i \in \mathbb{F}_{q^2}$. It is clear that $\mathrm{Tr}(x^q y) = \sum_{i,j=1}^{n} x_i^q y_j \mathrm{Tr}(\alpha_i^q\beta_j) = \sum_{i=1}^{n} x_i^q y_i = \langle (x_1^q,\dots,x_n^q),(y_1,\dots,y_n)\rangle$.

Note that the Hermitian forms in Theorems 35 and 36 are of the form $H(x,y) = \mathrm{Tr}(x^q L(y))$. Now, we denote the associated matrix of H with respect to the ordered $\mathbb{F}_{q^2}$-basis $(\alpha_1,\dots,\alpha_n)$ by $\mathcal{H}$, of which the (i,j)-th entry $\mathcal{H}(i,j)$ is given by

$$\mathcal{H}(i,j) = H(\alpha_i,\alpha_j) = \mathrm{Tr}(\alpha_j^q L(\alpha_i)).$$

Furthermore, the codewords of the additive d-code in Theorem 36 can be expressed in the

Hermitian matrix form as follows

$$H(x,y) = \mathrm{Tr}\left(\Big(\sum_j y_j\alpha_j\Big)^q \sum_i x_i L(\alpha_i)\right) = \mathrm{Tr}\left(\sum_{i,j} x_i y_j^q \alpha_j^q L(\alpha_i)\right)$$
$$= \sum_{i,j} x_i y_j^q \mathrm{Tr}\left(\alpha_j^q L(\alpha_i)\right) = \sum_{i,j} x_i \mathcal{H}(i,j) y_j^q = (x_1,\ldots,x_n)\cdot\mathcal{H}\cdot\begin{pmatrix} y_1^q \\ y_2^q \\ \vdots \\ y_n^q \end{pmatrix},$$

where $\mathcal{H}(i,j)$ is an element in $\mathcal{H}$. In the following we show that the evaluation of the corresponding linearized polynomial at linearly independent elements $\alpha_1,\ldots,\alpha_n$ is a proper encoding method. Define an n-dimensional vector over $\mathbb{F}_{q^2}$ as

$$h = (h_1,\ldots,h_n) = (\beta_1,\ldots,\beta_n)\cdot\mathcal{H}^T.$$

Since the i-th row of $\mathcal{H}$ is given by $(\mathrm{Tr}(\alpha_1^q L(\alpha_i)),\ldots,\mathrm{Tr}(\alpha_n^q L(\alpha_i)))$ and since each $L(\alpha_i)$ can be written as $\sum_t c_t\beta_t$ for some $c_t \in \mathbb{F}_{q^2}$, we can write h_i as

$$\begin{aligned} h_i &= \sum_j \beta_j H(i,j) = \sum_j \beta_j \mathrm{Tr}(\alpha_j^q L(\alpha_i)) \\ &= \sum_j \beta_j \mathrm{Tr}\big(\alpha_j^q \sum_t c_t\beta_t\big) = \sum_j \beta_j \sum_t c_t \mathrm{Tr}(\alpha_j^q\beta_t) \\ &= \sum_t \beta_t c_t = L(\alpha_i), \end{aligned}$$

where the fourth and fifth equality signs hold because $\mathrm{Tr}(x)$ is linear over $\mathbb{F}_{q^2}$ and $(\beta_1,\ldots,\beta_n)$ is the Hermitian dual basis of $(\alpha_1,\ldots,\alpha_n)$. From the equality $h_i = L(\alpha_i)$, we see that the encoding of Hermitian d-codes given by $\mathrm{Tr}(y^q L(x))$, as in Theorems 35 and 36, can be seen as the evaluation of $L(x)$ at the basis $\alpha_1,\ldots,\alpha_n$ of $\mathbb{F}_{q^{2n}}$.

With the above preparation, we are now ready to look at the encoding of the Hermitian d-codes in Theorems 35 and 36 more explicitly.

Let $\kappa = \lceil\frac{n-d}{2}\rceil$ and H be the Hermitian form given in Theorem 35. The linearized polynomial in (6.4) can be written as

$$L(x) = \sum_{j=1}^{\kappa}\left((b_j x)^{[\![n+1-j]\!]} + b_j^q x^{[\![j]\!]}\right),$$

and assuming $m = \frac{n+1}{2}$, similarly one can write the linearized polynomial in (6.5) as

$$L(x) = (b_0 x)^{[\![m]\!]} + \sum_{j=1}^{\kappa}\left((b_j x)^{[\![m+j]\!]} + b_j^q x^{[\![m-j]\!]}\right).$$

Let $\{1,\eta\}$ be an $\mathbb{F}_{q^n}$-basis of $\mathbb{F}_{q^{2n}}$. Let $\alpha_0,\alpha_1,\ldots,\alpha_{n-1}$ be a basis of $\mathbb{F}_{q^{2n}}$ over $\mathbb{F}_{q^2}$. Raising all the basis elements α_i to the q^2-th power will still give a linearly independent set of elements in $\mathbb{F}_{q^{2n}}$. We use $\alpha_0^{q^2},\alpha_1^{q^2},\ldots,\alpha_{n-1}^{q^2}$ as the evaluation points for optimal Hermitian d-codes

in Theorem 35. The reason for this is to keep the consistent form $L(x) = l_0 x^{[\![0]\!]} + l_1 x^{[\![1]\!]} + \cdots + l_{n-1} x^{[\![n-1]\!]}$ for the linearized polynomial representation (employing $\alpha_0, \ldots, \alpha_{n-1}$ as the evaluation points for this codes will obligate us to use the linearized polynomial of the form $L(x) = l_0 x^{[\![1]\!]} + l_1 x^{[\![2]\!]} + \cdots + l_{n-1} x^{[\![n]\!]}$).

The encoding of a message $f = (f_0, \ldots, f_{k-1}) \in \mathbb{F}_{q^n}^k$ can be expressed as the evaluation of the following linearized polynomial at points $\alpha_0^{q^2}, \alpha_1^{q^2}, \ldots, \alpha_{n-1}^{q^2}$:

$$L(x) = \left(\sum_{j=0}^{\kappa-1} (f_j + \eta f_{\kappa+j})^q x^{[\![n-1-j]\!]} + (f_j + \eta f_{\kappa+j} x)^{[\![j]\!]} \right) = \sum_{i=0}^{n-1} \tilde{f}_i x^{[\![i]\!]}, \tag{6.10}$$

where

$$\begin{aligned} \tilde{f} &= (\tilde{f}_0, \ldots, \tilde{f}_{\kappa-1}, 0, \ldots, 0, \tilde{f}_{n-\kappa}, \ldots, \tilde{f}_{n-1}) = ((f_0 + \eta f_\kappa)^{[\![0]\!]}, \ldots, \\ &\quad (f_{\kappa-1} + \eta f_{2\kappa-1})^{[\![\kappa-1]\!]}, 0, \ldots, 0, (f_{\kappa-1} + \eta f_{2\kappa-1})^q, \ldots, (f_0 + \eta f_\kappa)^q), \end{aligned} \tag{6.11}$$

and $k = 2\kappa$. For the optimal Hermitian d-code in Theorem 36 and the evaluation points $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$, the encoding of a message $f = (f_0, \ldots, f_{k-1}) \in \mathbb{F}_{q^n}^k$ can be expressed as the evaluation of the following linearized polynomial at points $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$:

$$\begin{aligned} L(x) &= (f_0 x)^{[\![m]\!]} + \left(\sum_{j=1}^{\kappa} (f_j + \eta f_{\kappa+j})^q x^{[\![m-j]\!]} + ((f_j + \eta f_{\kappa+j}) x)^{[\![m+j]\!]} \right) \\ &= \sum_{i=0}^{n-1} \tilde{f}_i x^{[\![i]\!]}, \end{aligned} \tag{6.12}$$

where

$$\begin{aligned} \tilde{f} = &\ (0, \ldots, 0, \tilde{f}_{m-\kappa}, \ldots, \tilde{f}_{m-1}, \tilde{f}_m, \tilde{f}_{m+1}, \ldots, \tilde{f}_{m+\kappa}, 0, \ldots, 0) \\ = &\ (0, \ldots, 0, (f_\kappa + \eta f_{2\kappa})^q, \ldots, (f_1 + \eta f_{\kappa+1})^q, f_0^{[\![m]\!]}, \\ &\ (f_1 + \eta f_{\kappa+1})^{[\![m+1]\!]}, \ldots, (f_\kappa + \eta f_{2\kappa})^{[\![m+\kappa]\!]}, 0, \ldots, 0), \end{aligned} \tag{6.13}$$

and $k = 2\kappa + 1$.

Let $M_l = \left(\alpha_i^{[\![j+l]\!]} \right)_{n \times n}$ be the $n \times n$ *Moore matrix* generated by $\alpha_0^{q^{2l}}, \alpha_1^{q^{2l}}, \ldots, \alpha_{n-1}^{q^{2l}}$ where $l \in \{0, 1\}$. We take $l = 1$ when we consider $\alpha_0^{q^2}, \alpha_1^{q^2}, \ldots, \alpha_{n-1}^{q^2}$ as the evaluation points which is used in (6.10) and $l = 0$ when $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ are the evaluation points in (6.12).

So the encoding of the optimal Hermitian rank metric codes can be expressed as

$$(f_0, \ldots, f_{k-1}) \mapsto (L(\alpha_0^{q^{2l}}), \ldots, L(\alpha_{n-1}^{q^{2l}})) = \tilde{f} \cdot M_l^T, \tag{6.14}$$

where $\tilde{f} = (\tilde{f}_0, \ldots, \tilde{f}_{n-1})$ and M_l^T is the transpose of the matrix M_l.

When n, d are integers with opposite parities as shown in (6.10), only the first κ and the last κ elements of $\tilde{f}$ are nonzero. Also in the case when n, d are both odd integers, as can be seen in (6.12), the first $m - \kappa$ and the last $m - \kappa - 2$ elements of $\tilde{f}$ are zero. So we only use $n - d + 1$ columns of the Moore matrix in the encoding process.

In summary, the encoding of the optimal symmetric, alternating and Hermitian d-codes relies on converting the codewords of those codes to simplified linearized polynomials $L(x)$ under carefully-chosen base of the extension fields, which enables us to treat encoding of those codes as evaluations of $L(x)$ at linearly independent points.

6.4 Decoding

In Section 3 the encodings of symmetric, alternating and Hermitian d-codes are in the form of polynomial evaluation. In this section we will present interpolation-based decoding of those codes, which make use of some nice properties of Dickson matrices in Proposition 13.

6.4.1 Key equations for error interpolation polynomials

We start with the optimal symmetric and alternating d-codes in Theorems 32 and 33. Note that their codewords are in the form $\mathrm{Tr}(yL(x))$ and can be deemed as n-dimensional vectors $(L(\omega_0),\ldots,L(\omega_{n-1}))$ over $\mathbb{F}_{q^n}$. We assume errors that occur in transmission or storage medium are also vectors in $\mathbb{F}_{q^n}^n$.

Given a message $f=(f_0,\ldots,f_{k-1})\in\mathbb{F}_{q^n}^k$, its corresponding codeword $c=\tilde{f}\cdot N^T$, where $\tilde{f}$ and N^T are as given in Section 3. Let $r=(r_0,\ldots,r_{n-1})$ over $\mathbb{F}_{q^n}$ be a received word when the codeword $c\in\mathbb{F}_{q^n}^n$ is transmitted, namely, $r=c+e$ for certain error vector $e\in\mathbb{F}_{q^n}^n$. Suppose $g(x)=\sum_{i=0}^{n-1} g_i x^{[i]}$ is the error interpolation polynomial such that

$$g(\omega_i)=e_i=r_i-c_i,\quad i=0,\ldots,n-1. \tag{6.15}$$

Clearly the error vector e is uniquely determined by the error interpolation polynomial $g(x)$, and vice versa. Denote $\tilde{g}=(g_0,\ldots,g_{n-1})$. Then it follows that

$$r=c+e=(\tilde{f}+\tilde{g})N^T. \tag{6.16}$$

Denote by G the associated Dickson matrix of the q-polynomial $g(x)$, i.e.,

$$G=\left(g_{i-j\ (\mathrm{mod}\ n)}^{[j]}\right)_{n\times n}=(G_0\ G_1\ \ldots\ G_{n-1})=\begin{bmatrix} g_0 & g_{n-1}^{[1]} & \cdots & g_1^{[n-1]} \\ g_1 & g_0^{[1]} & \cdots & g_2^{[n-1]} \\ \vdots & \vdots & \ddots & \vdots \\ g_{n-1} & g_{n-2}^{[1]} & \cdots & g_0^{[n-1]} \end{bmatrix},$$

where the subscripts are taken modulo n. Suppose the error e has rank t, by Proposition 13 we know that G has rank t and any $t\times t$ submatrix formed by t consecutive rows and columns in G has rank t. Furthermore, the first column of G can be expressed as a linear combination of $G_1,\ldots,G_t$ as

$$G_0=\lambda_1 G_1+\cdots+\lambda_t G_t, \tag{6.17}$$

where $G_1, \ldots, G_t$ are linearly independent over $\mathbb{F}_{q^n}$.

In the following we will make use of the pattern of $L(x)$ in Theorems 32 and 33, which have consecutive $d-1$ zero coefficients (up to a cyclic shift on the coefficients), and the properties of G in recovering the vector $\tilde{g}$.

Optimal symmetric d-codes in Theorem 32

For optimal symmetric d-codes, by (6.6) we can rewrite (6.16) as

$$\begin{aligned} r \cdot (N^T)^{-1} =& (\tilde{f}_0, \ldots, \tilde{f}_{k-1}, 0, \ldots, 0, \tilde{f}_{n-k+1}, \ldots, \tilde{f}_{n-1}) \\ &+ (g_0, \ldots, g_{k-1}, g_k, \ldots, g_{n-k}, g_{n-k+1}, \ldots, g_{n-1}). \end{aligned}$$

where $\tilde{f}_0 = f_0^{[0]}$, $\tilde{f}_j = f_j$ and $\tilde{f}_j = \tilde{f}_{n-j}^{[n-j]}$ for $j = 1, \ldots, k-1$. Recall that $k = (n-d+2)/2$ for symmetric d-codes in Theorem 32. Letting $\beta = (\beta_0, \ldots, \beta_{n-1}) = r \cdot (N^T)^{-1}$, we obtain

$$g_i = \begin{cases} \beta_i & \text{for } i = k, \ldots, k+d-2, \\ \beta_i - \tilde{f}_i & \text{for } i = n-k+1, \ldots, n-2k+1, \end{cases} \tag{6.18}$$

where the subscripts are taken modulo n. Since the elements $g_k, \ldots, g_{n-k}$ are known, from (6.17) we can have the following system of linear equations:

$$g_i = \lambda_1 g_{i-1}^{[1]} + \lambda_2 g_{i-2}^{[2]} + \cdots + \lambda_t g_{i-t}^{[t]},\ k+t \le i \le n-k, \tag{6.19}$$

which contains t unknowns $\lambda_1, \ldots, \lambda_t$ in $d-1-t$ linear equations.

Optimal alternating d-codes in Theorem 33

From (6.8) it follows that (6.16) is equivalent to

$$\begin{aligned} r \cdot (N^T)^{-1} =& (0, \ldots, 0, \tilde{f}_e, \ldots, \tilde{f}_{n-e}, 0, \ldots, 0) \\ &+ (g_0, \ldots, g_{e-1}, g_e, \ldots, g_{n-e}, g_{n-e+1}, \ldots, g_{n-1}). \end{aligned}$$

where $\tilde{f}_{j+e} = f_j$ and $\tilde{f}_{n-e+j} = -f_j^{[n-e-j]}$ for $j = 0, \ldots, k$. Suppose we have $\beta = (\beta_0, \ldots, \beta_{n-1}) = r \cdot (N^T)^{-1}$, similarly we obtain

$$g_i = \begin{cases} \beta_i & \text{for } i = n-e+1, \ldots, n+e-1, \\ \beta_i - \tilde{f}_i & \text{for } i = e, \ldots, n-e, \end{cases} \tag{6.20}$$

where the subscripts are taken modulo n. Based on (6.20), we obtain the following linear system of equations

$$g_i = \lambda_1 g_{i-1}^{[1]} + \lambda_2 g_{i-2}^{[2]} + \cdots + \lambda_t g_{i-t}^{[t]},\ n-e+1+t \le i < n+e \mod n \tag{6.21}$$

with t unknowns $\lambda_1 \ldots, \lambda_t$ in $2e-1-t = d-1-t$ linear equations.

From the above analysis, one sees that the equations (6.19) and (6.21) are the key equations for decoding optimal symmetric and optimal alternating d-codes, respectively.

Optimal Hermitian d-codes

The approach of establishing the key equations in decoding Hermitian d-codes is similar to that for symmetric and alternating d-codes. Because Hermitian d-codes are defined over $\mathbb{F}_{q^2}$ instead of $\mathbb{F}_q$, we briefly describe the process in the sequel.

Suppose a Hermitian codeword $c \in \mathbb{F}_{q^{2n}}^n$ is transmitted and a word $r = c + e$, with an error e with rank t added to the codeword c, is received. Suppose $g(x) = \sum_{i=0}^{n-1} g_i x^{[\![i]\!]}$ is an error interpolation polynomial with rank t such that

$$g(\alpha_i^{[\![l]\!]}) = e_i = r_i - c_i, \quad i = 0, \ldots, n-1 \text{ and } l \in \{0, 1\}, \tag{6.22}$$

where we use $l = 1$ for the Hermitian d-codes in Theorem 35 and $l = 0$ for the codes in Theorem 36. It is clear that the error vector $e = (e_0, \ldots, e_{n-1})$ is uniquely determined by the polynomial $g(x)$. Denote by

$$G = (G_0, \ldots, G_{n-1}) = \left(g_{i-j \pmod n}^{[\![j]\!]} \right),$$

the Dickson matrix associated with $g(x)$, then G has rank t and we can express

$$G_0 = \lambda_1 G_1 + \cdots + \lambda_t G_t, \tag{6.23}$$

with unknown λ_i's in $\mathbb{F}_{q^{2n}}$.

Denote $\tilde{g} = (g_0, \ldots, g_{n-1})$. From (6.14) and (6.22) it follows that

$$r = c + e = (\tilde{f} + \tilde{g}) M_l^T. \tag{6.24}$$

Case 1. This case considers the optimal Hermitian d-codes in Theorem 35. Recall that in Theorem 35 the Hermitian d-codes have parameters n, d with opposite parities and the message space was represented in k-dimensional vectors over $\mathbb{F}_{q^n}$ which are closed under $\mathbb{F}_q$-linear operations. Denoting $\kappa = \lceil \frac{n-d}{2} \rceil$, we can rewrite (6.24) as

$$\begin{aligned} r \cdot (M_1^T)^{-1} =& (\tilde{f}_0, \ldots, \tilde{f}_{\kappa-1}, 0, \ldots, 0, \tilde{f}_{n-\kappa}, \ldots, \tilde{f}_{n-1}) \\ &+ (g_0, \ldots, g_{\kappa-1}, g_\kappa, \ldots, g_{n-\kappa-1}, g_{n-\kappa}, \ldots, g_{n-1}), \end{aligned}$$

where for $j = 0, 1, \ldots, \kappa - 1$, $\tilde{f}_{n-j-1} = (f_j + \eta f_{\kappa+j})^q$ and $\tilde{f}_j = \tilde{f}_{n-j-1}^{q^{2j+1}}$, and $\{1, \eta\}$ is an $\mathbb{F}_{q^n}$-basis of $\mathbb{F}_{q^{2n}}$.

Let $\beta = (\beta_0, \ldots, \beta_{n-1}) = r \cdot (M_1^T)^{-1}$. Since $2\kappa = n-d+1$, we have $n-\kappa-1 = \kappa+d-2$ and

$$g_i = \begin{cases} \beta_i & \text{for } i = \kappa, \ldots, \kappa+d-2 \\ \beta_i - \tilde{f}_i & \text{for } i = n-\kappa, \ldots, n+\kappa-1. \end{cases} \tag{6.25}$$

This together with (6.23) gives a system of $d-1-t$ linear equations over $\mathbb{F}_{q^{2n}}$ with t unknowns λ_i's in $\mathbb{F}_{q^{2n}}$.

Case 2. This case considers the optimal Hermitian d-codes in Theorem 36. In this case n, d are both odd integers. Denote $m = (n+1)/2$ and $\kappa = (n-d)/2$. Note that (6.24) is equivalent to

$$\begin{aligned} r \cdot (M_0^T)^{-1} =& (0, \ldots, 0, \tilde{f}_{m-\kappa}, \ldots, \tilde{f}_{m+\kappa}, 0, \ldots, 0) \\ &+ (g_0, \ldots, g_{m-\kappa-1}, g_{m-\kappa}, \ldots, g_{m+\kappa}, g_{m+\kappa+1}, \ldots, g_{n-1}). \end{aligned}$$

where $\tilde{f}_m = f_0^{[\![m]\!]}$ and for $j = 1, 2, \cdots, \kappa$, $\tilde{f}_{m-j} = (f_j + \eta f_{\kappa+j})^q$ and $\tilde{f}_{m+j} = \tilde{f}_{m-j}^{q^{n+2j}}$. Denote $\beta = (\beta_0, \ldots, \beta_{n-1}) = r \cdot (M_0^T)^{-1}$. Since $\kappa = (n-d)/2$, we have $n-1-(m+\kappa+1)+1+(m-\kappa) = n-2\kappa-1 = d-1$ known g_i's and we can obtain

$$g_i = \begin{cases} \beta_i & \text{for } i = m+\kappa+1, \ldots, m+\kappa+d-1 \\ \beta_i - \tilde{f}_i & \text{for } i = m-\kappa, \ldots, m+\kappa, \end{cases} \tag{6.26}$$

where the subscripts are taken modulo n. Similarly, this together with (6.23) gives a system of $d-1-t$ linear equations over $\mathbb{F}_{q^{2n}}$ with t unknowns λ_i's in $\mathbb{F}_{q^{2n}}$.

6.4.2 Reconstruction of the error polynomial

Recall that the error polynomials $g(x)$ for symmetric and alternating d-codes are q-polynomials over $\mathbb{F}_{q^n}$ and the one for Hermitian d-codes are q^2-polynomials over $\mathbb{F}_{q^{2n}}$. Despite the difference in representation, the approach used for recovering the coefficients will be the same for those error polynomials. This observation allows us to present the common procedure of reconstructing $g(x)$'s in a unified manner.

Let $\rho \in \{q, q^2\}$. Given an error polynomial $g(x) = \sum_{i=0}^{n-1} \in \mathbb{F}_{\rho^n}[x]$ with rank t, its associate Dickson matrix given by

$$G = (G_0, G_1, \ldots, G_{n-1}) = \left(g_{i-j(\bmod n)}^{\rho^i} \right)_{n \times n}$$

also has rank t and $G_0 = \lambda_1 G_1 + \cdots + \lambda_t G_t$ for t unknown λ_i's in $\mathbb{F}_{\rho^n}$, which gives rise to a linearized recurrence as

$$g_L = \lambda_1 g_{L-1}^{\rho} + \lambda_2 g_{L-2}^{\rho^2} + \cdots + \lambda_t g_{L-t}^{\rho^t} \text{ for } L = 0, 1, \ldots, n-1 \tag{6.27}$$

where the subscripts of g_i's are taken modulo n. For the optimal symmetric, alternating and Hermitian d-codes in Section 2, Section 4.1 has established a system of $d-1-t$ linear equations over $\mathbb{F}_{\rho^n}$ in t unknowns $\lambda_i \in \mathbb{F}_{\rho^n}$ for each of them.

According to the pattern in G, we have the following major steps for recovering the coefficients g_i's:

Step 1. derive the unknowns $\lambda_1, \ldots, \lambda_t$ from the $d-1-t$ linear equations given in Section 4.1 for each optimal d-code;

Step 2. use $\lambda_1, \ldots, \lambda_t$ to recursively compute unknown g_i's in G.

Step 1 is the critical step in the decoding process. In Step 1 one has a system of $d-1-t$ linear equations for each optimal d-codes with t unknowns. There are two options for solving the unknowns. The first option is simply applying Gaussian elimination algorithm on the equations; and the second option is to apply the modified Berlekamp-Massey algorithm in [35]. As a matter of fact, with the linearized recurrence in (6.27), the task of Step 1 becomes finding the coefficients of modified version of a linear shift register as in [35] for given $d-1$ consecutive inputs g_i's for each optimal d-codes.

For Step 2, with the recursive relation in (6.27), one can calculate the remaining unknown coefficients g_i's in a sequential order.

6.4.3 Reconstruction of the original message

Recall that for each optimal d-code, it is assumed that a codeword c is transmitted and a word $r = c + e$ is received. With the error polynomials $g(x)$ obtained in Section 4.2, we are directly able to derive the codeword $c = r - e$. With the codeword c, we can obtain the coefficient vector $\tilde{f}$ of the interpolation polynomial $f(x) = \sum_{i=0}^{n-1} \tilde{f}_i x^{q^{ui}}$ where $u \in \{1,2\}$. One can compute $\tilde{f} = (\tilde{f}_0, \ldots, \tilde{f}_{n-1}) = c \cdot (\mathcal{A}^T)^{-1}$ where $\mathcal{A}$ is the Moore matrix associated with the linearly independent evaluation points. When the $\tilde{f}$ is obtained, we can further reconstruct the original message $f = (f_0, \ldots, f_{k-1})$ according to the encoding for each optimal d-code as follows:

- **Symmetric d-codes.**
$$f = (f_0, \ldots, f_{k-1}) = (\tilde{f}_0, \ldots, \tilde{f}_{k-1}).$$
- **Alternating d-codes.**
$$f = (f_0, \ldots, f_{k-1}) = (\tilde{f}_e, \ldots, \tilde{f}_{\frac{n-1}{2}}).$$
- **Hermitian d-codes.**
  - Case 1. When n, d have different parities: for $j \in \{0, \ldots, \kappa - 1\}$ where $k = 2\kappa$ we have the following equations
$$\begin{cases} \tilde{f}_j & = (f_j + \eta f_{\kappa+j})^{q^{2j}} \\ \tilde{f}_{n-j-1} & = (f_j + \eta f_{\kappa+j})^{q}. \end{cases} \tag{6.28}$$

The unknown coefficients $f_j, f_{k+j} \in \mathbb{F}_{q^n}$ for $j \in \{0,\ldots,\kappa-1\}$ can be seen as the unique coordinate vector of $\tilde{f}_j^{q^{-2j}}$ (or $\tilde{f}_{n-j-1}^{q^{-1}}$) expressed with respect to the basis $\{1,\eta\}$ of $\mathbb{F}_{q^{2n}}$ over $\mathbb{F}_{q^n}$ and can be computed directly.

– Case 2. When n,d are both odd: for $j \in 1,\ldots,\kappa-1$ where $k = 2\kappa+1$ we have the following linear system of equations

$$\begin{cases} \tilde{f}_m & = f_0^{q^{2m}} \\ \tilde{f}_{m+j} & = (f_j + \eta f_{\kappa+j})^{q^{2(m+j)}} \\ \tilde{f}_{m-j} & = (f_j + \eta f_{\kappa+j})^{q}. \end{cases} \tag{6.29}$$

The coefficient f_0 can be computed from the first equation as $f_0 = \tilde{f}_m^{q^{-2m}}$. Similar to the Case 1, the unknown coefficients $f_j, f_{j+\kappa}$ can be seen as coordinate vector of $\tilde{f}_{m-j}^{q^{-1}}$ (or $\tilde{f}_{m+j}^{q^{-2(m+j)}}$) written with respect to the basis $\{1,\eta\}$. So we can compute all the unknown coefficients $f_0,\ldots,f_{k-1} \in \mathbb{F}_{q^n}$ and recover the message.

6.4.4 Summary

The decoding algorithms in Section 6.4 share some similarities and one can summarize the decoding algorithms for all the restricted codes as follows:

- **Input:** a received word $r = (r_0,\ldots,r_{n-1})$ with errors of $t \leq \frac{d-1}{2}$ rank and linearly independent points $\theta_0,\ldots,\theta_{n-1}$ in $\mathbb{F}_{q^{un}}$ where $u \in \{1,2\}$.
- **Idea:** Reconstructing the code's interpolation polynomial $f(x) = \sum_{i=0}^{n-1} \tilde{f}_i x^{q^{ui}}$ via the error interpolation polynomial $g(x) = \sum_{i=0}^{n-1} g_i x^{q^{ui}}$ where $f(\theta_i) + g(\theta_i) = c_i + e_i = r_i$.
- **Output:** The codeword $c = r - e$.

(1) Compute the coefficients β_i of the polynomial $\beta(x) = \sum_{i=0}^{n-1} \beta_i x^{q^{ui}}$ where $r_i = \beta(\theta_i)$. This is equivalent to $r \cdot (\mathcal{M}^T)^{-1}$, where $\mathcal{M}$ is the Moore matrix associated with θ_i's.

(2) Specify the known coefficients $(g_j,\ldots,g_{j+d-2}) = (\beta_j,\ldots,\beta_{j+d-2})$, where the subscripts are taken modulo n, based on the code.

(3) Use the $2t$ known coefficients g_i as the initial state in the BM algorithm and find the unique connection vector $\lambda = (\lambda_1,\ldots,\lambda_t)$.

(4) Let G be the Dickson matrix associated with $g(x)$ with rank t. Write the first column G_0 as the linear combination of the columns $G_1,\ldots,G_t$ which can be written as the following recursive equations

$$g_i = \lambda_1 g_{i-1}^{q^u} + \lambda_2 g_{i-2}^{q^{2u}} + \cdots + \lambda_t g_{i-t}^{q^{tu}}, \quad 0 \leq i < n. \tag{6.30}$$

(5) Find the remaining coefficients g_i using the recursive equation (6.30).

(6) Compute $\tilde{f} = (\beta_0, \ldots, \beta_{n-1}) - (g_0, \ldots, g_{n-1})$.

(7) Compute the codeword $c = \tilde{f} \cdot \mathcal{M}^{\mathcal{T}^{-1}}$.

The lines (1) and (7) in the above procedure need $\mathcal{O}(n^3)$ operations over $\mathbb{F}_{q^{un}}$ which can be optimized if one applies the ideas in [25]. The line (2) needs linear complexity while the line (3) dominates the complexity of the whole process. The BM algorithm has complexity in the order of $\mathcal{O}(n^2)$ operations over $\mathbb{F}_{q^{un}}$. The complexity of the the remaining steps can be neglected.

6.4.5 Examples

Example 2 (Symmetric d-Codes)**.** *Let C be an optimal symmetric d-code with minimum distance $d = 5$ and length $n = 7$ defined over $\mathbb{F}_{2^7}$. We consider a normal basis of $\mathbb{F}_{2^7}$ over $\mathbb{F}_2$ with normal element $w = z^{95}$ as the evaluation points. Here z is a primitive element in $\mathbb{F}_{2^7}^*$.*

Encoding: *Suppose Alice wants to transfer the message $f = (f_0, f_1) = (z^7, z^{13})$ to Bob via a noisy channel. The code's evaluation polynomial would have the coefficient vector $\tilde{f} = (f_0, f_1, 0, 0, 0, 0, f_1^{q^6}) = (z^7, z^{13}, 0, 0, 0, 0, z^{70})$ which gives the codeword*

$$c = \tilde{f}(\mathcal{M}^T) = (z^{108}, z^{36}, z^{11}, z^{12}, z^{57}, z^{24}, z) = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix},$$

in symmetric form.

Channel's transmission: *We assume that the noisy channel adds an error vector $e = (z^{63}, z^{126}, z^{126}, z^{63}, z^{126}, z^{126}, z^{126})$ with rank $t = 2$ to the codeword c and Bob receives the word*

$$r = c + e = (z^4, z^{45}, z^{124}, z^{52}, z^{37}, z^{104}, z^{13}).$$

Decoding: *Now Bob received r and he wants to recover the message f. He first computes $\beta = r \cdot (\mathcal{M}^T)^{-1} = (z^{17}, z^{51}, z^{98}, z^{124}, z^{100}, z^{83}, z^{86})$ and directly gets the coefficients $(g_2, g_3, g_4, g_5) = (\beta_2, \beta_3, \beta_4, \beta_5)$ where $g(x) = \sum_{i=0}^{6} g_i x^{2^i}$ is the error interpolation polynomial and $\tilde{g} = (g_0, \ldots, g_6)$. Then he submits (g_2, g_3, g_4, g_5) in the BM algorithm and obtains the unique connection vector $(\lambda_1, \lambda_2) = (z^{25}, z^{126})$. Now he uses both (g_2, g_3, g_4, g_5) and (λ_1, λ_2) as inputs for modified version of LFSR described in [35] and get the vector*

$$a = (g_2, g_3, g_4, g_5, g_6, g_0, g_1) = (z^{98}, z^{124}, z^{100}, z^{83}, z^{55}, z^{115}, z^{71}).$$

Now he can rearrange the components of a and gets $\tilde{g} = (z^{115}, z^{71}, z^{98}, z^{124}, z^{100}, z^{83}, z^{55})$. *Since he knows* β *and* $\tilde{g}$, *he is able to compute* $\tilde{f} = \beta - \tilde{g} = (z^7, z^{13}, 0, 0, 0, 0, z^{70})$ *and finally* $f = (\tilde{f}_0, \tilde{f}_1) = (z^7, z^{13})$.

Example 3 (Alternating d-Codes)**.** *Suppose* $D \in \mathbb{F}_{2^9}$ *be an alternating* d*-code with length* $n = 9$ *and minimum distance* $d = 6$. *Let* $w = z^{347}$ *be the normal element for our normal basis which is used as the interpolation points. For the received word* $r = (z^{293}, z^{389}, z^{430}, z^{227}, z^{481}, z^{445}, z^{426}, z^{404}, z^{339})$ *containing error of* $t = \lfloor (d-1)/2 \rfloor = 2$ *rank, we can compute* $\beta, (\lambda_1, \lambda_2), a, \tilde{g}, \tilde{f}, c$ *and* f *similar to Example 2 as follows:*

- $\beta = (z^{486}, z^{233}, z^{334}, z^{155}, z^{167}, z^{226}, z^{483}, z^{231}, z^{88})$,
- $(\beta_0, \beta_1, \beta_2, \beta_7, \beta_8) = (g_0, g_1, g_2, g_7, g_8)$.
- *BM algorithm input* $(\beta_7, \beta_8, \beta_0, \beta_1, \beta_2)$ *gives* $(\lambda_1, \lambda_2) = (z^{154}, z^{262})$,
- *modified LFSR input* $(\beta_7, \beta_8, \beta_0, \beta_1, \beta_2)$ *and* (λ_1, λ_2) *gives*

$$\begin{aligned} a &= (\beta_7, \beta_8, \beta_0, \beta_1, \beta_2, g_3, g_4, g_5, g_6) \\ &= (z^{231}, z^{88}, z^{486}, z^{233}, z^{334}, z^{505}, z^{113}, z^{265}, z^{425}), \end{aligned}$$

- $\tilde{g} = (z^{486}, z^{233}, z^{334}, z^{505}, z^{113}, z^{265}, z^{425}, z^{231}, z^{88})$,
- $\tilde{f} = \beta - \tilde{g} = (0, 0, 0, z^{77}, z^{397}, z^{440}, z^{329}, 0, 0)$,
- $c = \tilde{f} \cdot (\mathcal{M}^T) = (z^{244}, z^{412}, z^{364}, z^{400}, z^{368}, z^{161}, z^{122}, z^{59}, z^{122})$,
- $f = (f_0, f_1) = (\tilde{f}_3, \tilde{f}_4) = (z^{77}, z^{397})$.

Example 4 (Hermitian d-Codes)**.** *Suppose* $\mathcal{C} \in \mathbb{F}_{2^{14}}^7$ *be an optimal Hermitian* d*-code with length* $n = 7$, *minimum distance* $d = 5$ *and* $\eta = z$. *We use the normal basis* W *of* $\mathbb{F}_{2^{14}}$ *over* $\mathbb{F}_{2^2}$ *with normal element* $w = z^{8591}$ *as the evaluation points, where* z *is the primitive element in* $\mathbb{F}^*_{2^{10}}$. *Let* $r = (z^{3672}, z^{2957}, z^{1343}, z^{3039}, z^{10923}, z^{9913}, z^{1618})$ *be a received word with error of* $t = (d-1)/2 = 2$ *rank. Then* $\beta = r \cdot (\mathcal{M}^T)^{-1} = (z^{5036}, z^{5234}, z^{203}, z^{840}, z^{2939}, z^{13080}, z^{15830})$. *Let* $g(x) = \sum_{i=0}^{6} g_i x^{2^{2i}}$ *be the error interpolation polynomial. Due to the expected form of* $\tilde{f}$ *in optimal Hermitian* d*-codes we have* $(\beta_0, \beta_1, \beta_2, \beta_6) = (g_0, g_1, g_2, g_6)$. *Now we submit* $(\beta_6, \beta_0, \beta_1, \beta_2)$ *in the BM algorithm and get the output* $(\lambda_1, \lambda_2) = (z^{11141}, z^{14283})$. *using both* $(\beta_6, \beta_0, \beta_1, \beta_2)$ *and* (λ_1, λ_2) *as the input for the modified version of linear feedback shift register explained in [35], we get*

$$a = (\beta_6, \beta_0, \beta_1, \beta_2, g_3, g_4, g_5) = (z^{15830}, z^{5036}, z^{5234}, z^{203}, z^{12223}, z^{9784}, z^{1048}).$$

So $\tilde{g} = (z^{5036}, z^{5234}, z^{203}, z^{12223}, z^{9784}, z^{1048}, z^{15830})$ *and the code's evaluation polynomial has the coefficient vector* $\tilde{f} = (0, 0, 0, z^{4446}, z^{11481}, z^{15498}, 0)$. *Then the codeword is*

$$c = \tilde{f} \cdot \mathcal{M}^T = (z^{781}, z^{1313}, z^{4481}, z^{5130}, z^{1671}, z^{9656}, z^{1567})$$
$$= \begin{pmatrix} 1 & 0 & 0 & 1 & y & y^2 & 1 \\ 0 & 1 & 0 & y & y & y & 1 \\ 0 & 0 & 1 & 0 & y^2 & 0 & y^2 \\ 1 & y^2 & 0 & 0 & y^2 & y^2 & 0 \\ y^2 & y^2 & y & y & 1 & y & y^2 \\ y & y^2 & 0 & y & y^2 & 1 & 1 \\ 1 & 1 & y & 0 & y & 1 & 1 \end{pmatrix},$$

where y is the primitive element in $\mathbb{F}_{2^2}^*$ and the message is $f = (f_0, \ldots, f_{k-1}) = (l^{89}, l^{97}, l^{32})$ where l is the primitive element in $\mathbb{F}_{2^7}^*$.

6.5 Conclusion

This work proposes the first encoding and decoding methods for three restricted families of rank metric codes including optimal symmetric, optimal alternating and optimal Hermitian rank metric codes. We showed that the evaluation encoding is a right choice for the aforementioned families and the proposed encoding methods are easily reversible and efficient. We also introduce three interpolation-based decoding algorithms that are based on the properties of Dickson matrix associated with linearized polynomials. In the decoding process we reduced the rank decoding problem to the problem of solving a system of linear equations which can be solved by Gaussian elimination method or Berlekamp-Massey algorithm in polynomial time.

Bibliography

[1] Javier De La Cruz, Jorge Robinson Evilla, and Ferruh Özbudak. Hermitian rank metric codes and duality. *IEEE Access*, 9:38479–38487, 2021.

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

[3] Philippe Delsarte and Jean-Marie Goethals. Alternating bilinear forms over GF(q). *Journal of Combinatorial Theory, Series A*, 19(1):26–50, 1975.

[4] L.E. Dickson. *Linear Groups, with an Exposition of the Galois Field Theory - Scholar's Choice Edition*. Creative Media Partners, LLC, 2015.

[5] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In Donald W. Davies, editor, *Advances in Cryptology – EUROCRYPT'91*, pages 482–489. Springer, 1991.

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

[7] Ernst M Gabidulin, AV Paramonov, and OV Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In *Advances in Cryptology – EUROCRYPT'91*, pages 482–489. Springer, 1991.

[8] Elisa Gorla and Alberto Ravagnani. Codes endowed with the rank metric. In *Network Coding and Subspace Designs*, pages 03–23. Springer, 2018.

[9] Wrya K. Kadir. New communication models and decoding of maximum rank distance codes. In *2021 XVII International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY)*, pages 125–130, 2021.

[10] Wrya K. Kadir and Chunlei Li. On decoding additive generalized twisted Gabidulin codes. *Cryptography and Communications*, 12:987 – 1009, 2020.

[11] Wrya K. Kadir, Chunlei Li, and Ferdinando Zullo. Decoding a class of maximum hermitian rank metric codes. *Submitted to The 6th International Workshop on Boolean Functions and their Applications (BFA)*, 2021.

[12] Wrya K. Kadir, Chunlei Li, and Ferdinando Zullo. On interpolation-based decoding of a class of maximum rank distance codes. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 31–36, 2021.

[13] Wrya K Kadir, Chunlei Li, and Ferdinando Zullo. Encoding and decoding of several optimal rank metric codes. *Cryptography and Communications*, pages 1–20, 2022.

[14] Alexander Kshevetskiy and Ernst Gabidulin. The new construction of rank codes. *Proceedings. International Symposium on Information Theory, 2005*, pages 2105–2108, 2005.

[15] Chunlei Li. Interpolation-based decoding of nonlinear maximum rank distance codes. In *International Symposium on Information Theory (ISIT)*, 2019.

[16] Chunlei Li and Wrya K. Kadir. On decoding additive generalized twisted Gabidulin codes. *presented at the International Workshop on Coding and Cryptography (WCC)*, 2019.

[17] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2 edition, 1997.

[18] Pierre Loidreau. A Welch–Berlekamp like algorithm for decoding Gabidulin codes. In Øyvind Ytrehus, editor, *International Workshop on Coding and Cryptography (WCC)*, pages 36–45, Berlin, Heidelberg, 2006. Springer.

[19] Giovanni Longobardi, Guglielmo Lunardon, Rocco Trombetti, and Yue Zhou. Automorphism groups and new constructions of maximum additive rank metric codes with restrictions. *Discrete Mathematics*, 343(7):111871, 2020.

[20] Guglielmo Lunardon, Rocco Trombetti, and Yue Zhou. Generalized twisted Gabidulin codes. *Journal of Combinatorial Theory, Series A*, 159:79–106, 2018.

[21] Giampaolo Menichetti. Roots of affine polynomials. In A. Barlotti, M. Biliotti, A. Cossu, G. Korchmaros, and G. Tallini, editors, *Combinatorics '84*, volume 123 of *North-Holland Mathematics Studies*, pages 303–310. North-Holland, 1986.

[22] Kamil Otal and Ferruh Özbudak. Additive rank metric codes. *IEEE Transactions on Information Theory*, 63(1):164–168, 2017.

[23] Kamil Otal and Ferruh Özbudak. Constructions of cyclic subspace codes and maximum rank distance codes. In *Network Coding and Subspace Designs*, pages 43–66. Springer, 2018.

[24] Kamil Otal and Ferruh Özbudak. Some new non-additive maximum rank distance codes. *Finite Fields and Their Applications*, 50:293 – 303, 2018.

[25] Sven Puchinger and Antonia Wachter-Zeh. Fast operations on linearized polynomials and their applications in coding theory. *Journal of Symbolic Computation*, 89:194 – 215, 2018.

[26] Tovohery Hajatiana Randrianarisoa. A decoding algorithm for rank metric codes. *arXiv.org.*, abs/1712.07060, 2017.

[27] G. Richter and S. Plass. Fast decoding of rank-codes with rank errors and column erasures. In *International Symposium on Information Theory (ISIT)*, pages 398–398, June 2004.

[28] Joachim Rosenthal and Tovohery Hajatiana Randrianarisoa. A decoding algorithm for twisted Gabidulin codes. In *International Symposium on Information Theory (ISIT)*, pages 2771–2774. IEEE, 2017.

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

[30] Kai-Uwe Schmidt. Symmetric bilinear forms over finite fields of even characteristic. *Journal of Combinatorial Theory, Series A*, 117(8):1011–1026, 2010.

[31] Kai-Uwe Schmidt. Symmetric bilinear forms over finite fields with applications to coding theory. *Journal of Algebraic Combinatorics*, 42(2):635–670, 2015.

[32] Kai-Uwe Schmidt. Hermitian rank distance codes. *Designs, Codes and Cryptography*, 86(7):1469–1481, 2018.

[33] John Sheekey. MRD codes: Constructions and connections. *Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications, edited by Kai-Uwe Schmidt and Arne Winterhof, Berlin, Boston: De Gruyter, 2019, pp. 255-286.*

[34] John Sheekey. A new family of linear maximum rank distance codes. *Advances in Mathematics of Communications*, 10:475, 2016.

[35] V. Sidorenko, G. Richter, and M. Bossert. Linearized shift-register synthesis. *IEEE Transactions on Information Theory*, 57(9):6025–6032, Sep. 2011.

[36] Danilo Silva and Frank R Kschischang. Fast encoding and decoding of Gabidulin codes. In *International Symposium on Information Theory (ISIT)*, pages 2858–2862. IEEE, 2009.

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

[38] R. Trombetti and Y. Zhou. A new family of MRD codes in $\mathbb{F}_q^{2n\times 2n}$ with right and middle nuclei $\mathbb{F}_{q^n}$. *IEEE Transactions on Information Theory*, 65(2):1054–1062, 2019.

[39] Rocco Trombetti and Ferdinando Zullo. On maximum additive Hermitian rank-metric codes. *Journal of Algebraic Combinatorics*, pages 1–21, 2020.

[40] Lloyd R Welch and Elwyn R Berlekamp. Error correction for algebraic block codes, December 30 1986. US Patent 4,633,470.

[41] Yue Zhou. On equivalence of maximum additive symmetric rank-distance codes. *Designs, Codes and Cryptography*, 88(5):841–850, 2020.

Chapter 7

On cryptographic properties of the Welch permutation and a related conjecture

In this chapter, we determine the differential spectrum and the Walsh transform of the Welch permutation $g(x) = x^{2^{m+1}+1} + x^3 + x$ of $\mathrm{GF}_{2^{2m+1}}$, which was derived from the Welch APN power function x^{2^m+3}. As an application, the properties of $g(x)$ are used to partly resolve a conjecture by Ding [9] on a class of binary linear codes constructed from the Welch APN power functions. This chapter is based on my work with Yibo Wang, Chunlei Li and Yongbo Xia [14] which was presented at Sequences and Their Applications 2020 conference.

7.1 Introduction

Let GF_{2^n} denote the finite field of 2^n elements and $\mathrm{GF}_{2^n}^*$ be its multiplicative group. For a vectorial Boolean function $F(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$, denote

$$N_F(a,b) = |\{x \in \mathrm{GF}_{2^n} \,|\, F(x+a) + F(x) = b\}|. \tag{7.1}$$

The differential uniformity of $F(x)$ is defined by

$$\Delta_F = \max\left\{N_F(a,b) \mid a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}\right\}.$$

Nyberg defined a mapping $F(x)$ to be differentially δ-uniform if $\Delta_F = \delta$ [13]. Differential uniformity is one of the most important notions in symmetric cryptography. It quantifies the security of S-boxes used in block ciphers with respect to the differential attack. For practical applications, cryptographic functions are desirable to have low differential uniformity. It is clear that the equation $F(x+a) + F(x) = b$ have solutions in pairs. Thus, $\Delta_F = 2$ is the smallest possible value for the differential uniformity of $F(x)$. A function $F(x)$ is said to be almost perfect nonlinear (APN) if its differential uniformity is 2. Equivalently, a function $F(x)$ is APN if its derivative function $D_aF(x) := F(x+a) + F(x)$, for any $a \in \mathrm{GF}_{2^n}^*$, is a two-to-one function over GF_{2^n}. APN functions are of great interest due to their importance in the design of S-boxes in block ciphers and their close connection to optimal objects in coding theory and combinatorial theory. Constructing APN functions has been intensively studied in the last

three decades, and by far the known families of APN functions over GF_{2^n} can be found in the recent chapter [5]. Besides the differential uniformity, the differential spectrum of $F(x)$, namely the value distribution of $N_F(a,b)$ for $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, is also an important notion for estimating its resistance against variants of differential cryptanalysis [1, 2, 4, 7]. In addition to differential properties, nonlinearity and Walsh transform are important measurements to assess the properties of a vectorial Boolean function against linear cryptanalysis.

Nonlinear functions also have a number of applications in constructing error-correcting codes with good properties [6, 9]. An $[n,k,d]$ binary linear code $\mathcal{C}$ is a k-dimensional subspace of GF_2^n with minimum (Hamming) distance d. Let A_i denote the number of codewords with Hamming weight i in a code $\mathcal{C}$ of length n. The weight enumerator of $\mathcal{C}$ is defined by $1+A_1z+A_2z^2+\cdots+A_nz^n$. The sequence $(1,A_1,A_2,\ldots,A_n)$ is called the weight distribution of $\mathcal{C}$. Clearly, the weight distribution gives the minimum distance of the code, and thus the error correcting capability. In addition, the weight distribution of a code allows the computation of the error probability of error detection and correction with respect to some error detection and error correction algorithms. A binary code $\mathcal{C}$ is said to be a t-weight code if the number of nonzero A_i in the sequence $(A_1,A_2,\ldots,A_n)$ is equal to t. Binary linear codes with few weights have many applications [6, 9], including secret sharing schemes, authentication codes, association schemes and strongly regular graphs.

Ding et. al in [9, 10] introduced a generic construction of binary linear codes from a subset $D=\{d_1,d_2,\ldots,d_\ell\}$ of GF_{2^n} and the absolute trace function $\mathrm{Tr}_1^n(\cdot)$ from GF_{2^n} to GF_2 as

$$\mathcal{C}_D = \{\mathbf{c}_a = (\mathrm{Tr}_1^n(ad_1),\mathrm{Tr}_1^n(ad_2),\ldots,\mathrm{Tr}_1^n(ad_\ell)) : a \in \mathrm{GF}_{2^n}\}. \tag{7.2}$$

This construction is generic in the sense that many classes of known codes could be produced by selecting proper defining sets D. When the defining set D is properly chosen, the code $\mathcal{C}_D$ can have a few nonzero weights. In [9] Ding investigated the properties of binary linear codes from the images of certain functions on GF_{2^n} and proposed several conjectures on properties of the constructed codes, including the following one from the Welch APN power functions.

Conjecture 1. *[9, Conjecture 33] Let $n=2m+1$, $F(x)=x^{2^m+3}$, $f(x)=F(x)+F(x+1)+1$ and $D(f)=\{d_1,d_2,\ldots,d_\ell\}=\{f(x)\,|\,x\in\mathrm{GF}_{2^n}\}$. Define the binary code $\mathcal{C}_{D(f)}$ as*

$$\mathcal{C}_{D(f)} = \{\boldsymbol{c}_a = (\mathrm{Tr}_1^n(ad_1),\mathrm{Tr}_1^n(ad_2),\ldots,\mathrm{Tr}_1^n(ad_\ell)) : a \in \mathrm{GF}_{2^n}\}.$$

If $n\in\{5,7\}$, then $\mathcal{C}_{D(f)}$ is a three-weight code with length 2^{n-1} and dimension n. If $n\geq 9$, then $\mathcal{C}_{D(f)}$ is a five-weight code with length 2^{n-1} and dimension n.

In this chapter, we investigate certain cryptographic properties, namely, the differential spectrum and the Walsh spectrum, of the permutation polynomial $g(x)=x^{2^{m+1}+1}+x^3+x$ over $\mathrm{GF}_{2^{2m+1}}$ for a positive integer $m\geq 2$. Here we call $g(x)$ the Welch permutation polynomial since via it Dobbertion proved that the Welch power function $F(x)=x^{2^m+3}$ is APN [11]. Furthermore, based on an observation, the weight of a codeword in $\mathcal{C}_{D(f)}$ defined in Conjecture 1 can be expressed in terms of the Walsh transform of $g(x)$ at certain points. This enables us to show that the binary linear code $\mathcal{C}_{D(f)}$ has dimension n and at most five nonzero weights as described in Conjecture 1.

The remainder of this chapter is organized as follows. Section 2 introduces basic notation and

definitions. Section 3 studies the differential spectrum and Walsh transform of $g(x)$. Section 4 provides a positive answer to Conjecture 1.

7.2 Preliminaries

7.2.1 Cryptographic properties of vectorial Boolean functions

Definition 42. *Let $F(x)$ be a function from $\mathbb{F}_{2^n}$ to itself, and $N_F(a,b)$ be defined as in* (7.1)*. Denote*

$$\omega_i = |\{(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n} \mid N_F(a,b) = i\}|.$$

The differential spectrum of $F(x)$ is defined as the multi-set

$$\Omega_F = \{\omega_0, \omega_1, \ldots, \omega_\delta\}, \tag{7.3}$$

where δ is the differential uniformity of $F(x)$.

It is easily seen that $\omega_i = 0$ in the differential spectrum if i is odd. Moreover, we have the following identities

$$\sum_{i=0}^{\delta} \omega_i = 2^n(2^n-1) \text{ and } \sum_{i=0}^{\delta} (i \times \omega_i) = 2^n(2^n-1). \tag{7.4}$$

For any APN function over GF_{2^n}, there are only two possible values 0 and 2 in its differential spectrum. Thus, from the equalities in (7.4), the differential spectrum of an APN function over GF_{2^n} can be uniquely determined.

Another important criterion of a vectorial Boolean function $F(x)$ is its nonlinearity, which can be given in terms of the Walsh transforms of $F(x)$.

Definition 43. *Let $F(x)$ be a function from $\mathbb{F}_{2^n}$ to itself. The Walsh transform of $F(x)$ at (a,b) is defined by*

$$W_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(aF(x)+bx)} \tag{7.5}$$

for each $a,b \in \mathbb{F}_{2^n}$. The Walsh spectrum of $F(x)$ is the multi-set

$$\Lambda_F = \{W_F(a,b) : a,b \in \mathbb{F}_{2^n}, a \neq 0\}. \tag{7.6}$$

The nonlinearity of $F(x)$ is given by

$$NL(F) = 2^{n-1} - \frac{1}{2}\max\{|\, W_F(a,b) \,| : a,b \in \mathbb{F}_{2^n}, a \neq 0\}.$$

Given a quadratic Boolean function $Q(x)$ from GF_{2^n} to GF_2, the function $Q(x+z)+Q(x)+Q(z)$ is a bilinear function in x and z. Define

$$V_Q = \{x \in \mathrm{GF}_{2^n} \mid Q(x+z)+Q(x)+Q(z) = 0, \forall\, z \in \mathrm{GF}_{2^n}\}. \tag{7.7}$$

The rank of $Q(x)$ is defined by $\mathrm{Rank}(Q) = n - \dim_{\mathrm{GF}_2}(V_Q)$. Note that

$$\left(\sum_{x\in \mathrm{GF}_{2^n}} (-1)^{Q(x)}\right)^2 = \sum_{x\in \mathrm{GF}_{2^n}} (-1)^{Q(x)} \sum_{z\in \mathrm{GF}_{2^n}} (-1)^{Q(x+z)+Q(x)+Q(z)} = 2^n \sum_{x\in V_Q} (-1)^{Q(x)}, \quad (7.8)$$

where V_Q is the GF_2-linear space defined as in (7.7). It is readily seen that $Q(x)$ is linear over V_Q. Hence one has

$$\sum_{x\in \mathrm{GF}_{2^n}} (-1)^{Q(x)} = \begin{cases} \pm 2^{n-\mathrm{Rank}(Q)/2}, & \text{if } Q(x) = 0 \text{ for any } x \in V_Q, \\ 0, & \text{otherwise.} \end{cases}$$

This implies that the $\mathrm{Rank}(Q)$ is always an even number $2h$ with $2 \le 2h \le n$ [12].

For a quadratic Boolean function $Q(x)$ from GF_{2^n} to GF_2, the definition of its Walsh transform is modified slightly as

$$\widehat{Q}(\lambda) = \sum_{x\in \mathbb{F}_{2^n}} (-1)^{Q(x)+\mathrm{Tr}_1^n(\lambda x)}.$$

Moreover, when λ runs through $\mathbb{F}_{2^n}$, the distribution of $\widehat{Q}(\lambda)$ can be characterized below.

Lemma 7. *[12, Theorem 6.2] Let $Q(x)$ be a quadratic form on $\mathbb{F}_{2^n}$ to GF_2 with rank $2h$. Then its Walsh transform $\widehat{Q}(\lambda)$ has the following distribution*

$$\widehat{Q}(\lambda) = \sum_{x\in \mathbb{F}_{2^n}} (-1)^{Q(x)+\mathrm{Tr}_1^n(\lambda x)} = \begin{cases} \pm 2^{n-h}, & 2^{2h-1} \pm 2^{h-1} \text{ times}, \\ 0, & 2^n - 2^{2h} \text{ times}. \end{cases}$$

For cryptographic applications, a vectorial Boolean function is desired to have low differential uniformity and high nonlinearity [5].

7.2.2 The binary code from the Welch power function

Let $n = 2m+1$ for a positive integer m and $F(x) = x^{2^m+3}$. In Conjecture 1, the image of $f(x) = F(x+1) + F(x) + 1 = D_1F(x) + 1$ on GF_{2^n}, denoted by $D(f)$, is chosen as the defining set. Note that $f(x)$ is a two-to-one function on GF_{2^n}. Thus, the set $D(f)$ has size 2^{n-1}. Using the generic construction method in (7.2), the linear code $\mathcal{C}_{D(f)}$ in Conjecture 1 is obtained.

Let $\mathbf{c}_a$ be a codeword in $\mathcal{C}_{D(f)}$. Then, its weight is given by

$$\begin{aligned}\mathrm{wt}(\mathbf{c}_a) &= \left|\{1 \le i \le 2^{n-1} : \mathrm{Tr}_1^n(ad_i) = 1\}\right| \\ &= \frac{1}{2}\left(2^{n-1} - \sum_{d\in D(f)} (-1)^{\mathrm{Tr}_1^n(ad)}\right) \\ &= \frac{1}{2}\left(2^{n-1} - \frac{1}{2}\sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(af(x))}\right) \\ &= 2^{n-2} - \frac{1}{4}\sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(af(x))}.\end{aligned} \tag{7.9}$$

The above formula shows that for studying the Hamming weight properties of the code $\mathcal{C}_{D(f)}$, it is critical to investigate the Walsh transform of $f(x)$ at $(a,0)$, i.e., $W_f(a,0)$.

7.3 The differential spectrum and the Walsh spectrum of the Welch permutation

For the permutation $g(x) = x^{2^{m+1}+1} + x^3 + x$ over GF_{2^n} with $n = 2m+1$, this section will determine the differential spectrum Ω_g defined as in (7.3) and the Walsh spectrum Λ_g defined as in (7.6).

Theorem 37. *Let $n = 2m+1$ and $g(x) = x^{2^{m+1}+1} + x^3 + x$. Then $g(x)$ is differentially 4-uniform. Furthermore, its differential spectrum is given by*

$$\{\omega_0 = 2^{2n-1} + 2^{2n-3} - 3\cdot 2^{n-2}, \omega_2 = 2^{2n-2}, \omega_4 = 2^{2n-3} - 2^{n-2}\}.$$

Proof. Let $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$, and $N(a,b)$ be the number of solutions of $g(x+a) + g(x) = b$ in $\mathbb{F}_{2^n}$. Note that

$$\begin{aligned} & g(x+a) + g(x) + b \\ = \; & x^{2^{m+1}}a + xa^{2^{m+1}} + a^{2^{m+1}+1} + x^2a + xa^2 + a^3 + a + b \\ = \; & ax^{2^{m+1}} + ax^2 + (a^{2^{m+1}} + a^2)x + g(a) + b.\end{aligned}$$

Since $a \neq 0$, $g(x+a) + g(x) + b = 0$ is equivalent to that

$$x^{2^{m+1}} + x^2 + cx + d = 0, \tag{7.10}$$

where

$$c = a^{2^{m+1}-1} + a \text{ and } d = \frac{g(a)+b}{a}. \tag{7.11}$$

Note that $c = 0$ if and only if $a = 1$. Next we consider the following linearized polynomial

$$x^{2^{m+1}} + x^2 + cx = 0. \tag{7.12}$$

If $c = 0$ (i.e., $a = 1$), then (7.12) have two solutions in $\mathbb{F}_{2^n}$, which are 0 and 1. If $c \neq 0$ (i.e.,

$a \notin \mathbb{F}_2$), then by raising (7.12) to the power 2^m, we get

$$x + x^{2^{m+1}} + c^{2^m} x^{2^m} = 0. \tag{7.13}$$

Adding up (7.12) and (7.13), we get

$$c^{2^m} x^{2^m} + x^2 + (c+1)x = 0,$$

which implies

$$x^{2^m} = \frac{x^2}{c^{2^m}} + \frac{c+1}{c^{2^m}} x. \tag{7.14}$$

Substituting (7.14) into (7.13), we get

$$x^4 + (c^{2^{m+1}} + c^2 + 1)x^2 + c^{2^{m+1}+1} x = 0. \tag{7.15}$$

The above argument shows that if x is a solution of (7.12), it must be a solution of (7.15). Note that (7.15) is a linearized polynomial over $\mathbb{F}_{2^n}$ and the number of its solutions in $\mathbb{F}_{2^n}$ is 1, 2 or 4. Thus, we can conclude that the number of solutions of (7.12) in $\mathbb{F}_{2^n}$ is also 1, 2 or 4. Moreover, note that

$$c = a^{2^{m+1}-1} + a = \frac{a^{2^{m+1}} + a^2}{a}.$$

Thus, for any given $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$, $x = a$ must be a solution of (7.12). Thus, when $c \neq 0$, i.e., $a \notin \mathbb{F}_2$, the number of solutions of (7.12) in $\mathbb{F}_{2^n}$ is 2 or 4.

Denote by M_1 (resp. M_2) the number of $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$ such that (7.12) has two (resp. four) solutions in $\mathbb{F}_{2^n}$. In what follows, we need to determine M_1 and M_2. We further investigate the linearized polynomial (7.15). Since $x = 0$ and $x = a$ are its solutions, the polynomial on the left hand side of (7.15) has a factorization over $\mathbb{F}_{2^n}$ as follows

$$x^4 + (c^{2^{m+1}} + c^2 + 1)x^2 + c^{2^{m+1}+1} x = x(x+a)(x^2 + ax + \frac{c^{2^{m+1}+1}}{a}),$$

where $c = \frac{a^{2^{m+1}} + a^2}{a}$. (One can verify that $a^2 + \frac{c^{2^{m+1}+1}}{a} = c^{2^{m+1}} + c^2 + 1$.) To check the exact number of solutions of (7.12), we should investigate the solutions of the following quadratic equation

$$x^2 + ax + \frac{c^{2^{m+1}+1}}{a} = 0. \tag{7.16}$$

Note that

$$\begin{aligned}
& \mathrm{Tr}_1^n\left(\frac{c^{2^{m+1}+1}}{a^3}\right)\\
= \ & \mathrm{Tr}_1^n\left(\frac{a^2+a^{2^{m+2}}}{a^{2^{m+1}}}\cdot\frac{a^{2^{m+1}}+a^2}{a^4}\right)\\
= \ & \mathrm{Tr}_1^n\left(\frac{a^4+a^2\cdot a^{2^{m+1}}+a^{2^{m+2}}\cdot a^{2^{m+1}}+a^2\cdot a^{2^{m+2}}}{a^{2^{m+1}}\cdot a^4}\right)\\
= \ & \mathrm{Tr}_1^n\left(\frac{1}{a^{2^{m+1}}}+\frac{1}{a^2}+\frac{a^{2^{m+2}}}{a^4}+\frac{a^{2^{m+1}}}{a^2}\right)\\
= \ & \mathrm{Tr}_1^n\left(\tfrac{1}{a}\right)+\mathrm{Tr}_1^n\left(\tfrac{1}{a}\right)+\mathrm{Tr}_1^n\left(\frac{a^{2^{m+1}}}{a^2}\right)+\mathrm{Tr}_1^n\left(\frac{a^{2^{m+1}}}{a^2}\right)\\
= \ & 0.
\end{aligned}$$

Thus, (7.16) has two solutions in $\mathbb{F}_{2^n}$. This also shows that for any $a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2$, (7.15) always has four solutions in $\mathbb{F}_{2^n}$. By Theorem 1 in [8], one can get the solutions of (7.16), which are

$$x_1 = a\sum_{i=1}^{m}\left(\frac{c^{2^{m+1}+1}}{a^3}\right)^{2^{2i-1}}, \text{ and } x_2 = x_1+a.$$

Next the main task is to verify that whether x_1 is a solution of (7.12) or not.

Let $y=\frac{x_1}{a}$, then by (7.16) we have

$$y^2+y+\frac{c^{2^{m+1}+1}}{a^3}=0. \tag{7.17}$$

If x_1 is a solution of (7.12), we also have

$$y^{2^{m+1}}+\frac{a^2}{a^{2^{m+1}}}y^2+\frac{ca}{a^{2^{m+1}}}y=0. \tag{7.18}$$

Combining (7.17) and (7.18), we have

$$y^{2^{m+1}}+y+\left(\frac{c}{a}\right)^{2^{m+1}+1}=0. \tag{7.19}$$

On the other hand, by (7.17) we have

$$\begin{aligned}
& y^{2^{m+1}}+y \\
= & \sum_{i=0}^{m}\left(y^2+y\right)^{2^i} \\
= & \sum_{i=0}^{m}\left(\frac{c^{2^{m+1}+1}}{a^3}\right)^{2^i} \\
= & \sum_{i=0}^{m}\left(\frac{1}{a^{2^{m+1}}}+\frac{1}{a^2}+\frac{a^{2^{m+2}}}{a^4}+\frac{a^{2^{m+1}}}{a^2}\right)^{2^i} \\
= & \sum_{i=0}^{m}\left(\left(\frac{1}{a^2}\right)^{2^m}+\frac{1}{a^2}+\left(\frac{a^{2^{m+1}}}{a^2}\right)^2+\frac{a^{2^{m+1}}}{a^2}\right)^{2^i} \\
= & \mathrm{Tr}_1^n\left(\frac{1}{a^2}\right)+\frac{1}{a^{2^{m+1}}}+\frac{a^{2^{m+1}}}{a^2}+\left(\frac{a^{2^{m+1}}}{a^2}\right)^{2^{m+1}} \\
= & \mathrm{Tr}_1^n\left(\frac{1}{a^2}\right)+\frac{1}{a^{2^{m+1}}}+\frac{a^{2^{m+1}}}{a^2}+\frac{a^2}{a^{2^{m+2}}} \\
= & \mathrm{Tr}_1^n\left(\frac{1}{a^2}\right)+1+\left(\frac{a^{2^{m+1}}+a^2}{a^2}\right)^{2^{m+1}}\cdot\frac{a^{2^{m+1}}+a^2}{a^2} \\
= & \mathrm{Tr}_1^n\left(\frac{1}{a^2}\right)+1+\left(\frac{c}{a}\right)^{2^{m+1}+1}.
\end{aligned} \tag{7.20}$$

By (7.20) and (7.19), we can conclude that for each $a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2$, the solution x_1 of (7.16) is also a solution of (7.12) if and only if $\mathrm{Tr}_1^n\left(\frac{1}{a}\right)=1$. This means that for each $a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2$, (7.12) has two (resp. four) solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n\left(\frac{1}{a}\right)=0$ (resp. $\mathrm{Tr}_1^n\left(\frac{1}{a}\right)=1$). It is obvious that the number of $a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2$ such that $\mathrm{Tr}_1^n\left(\frac{1}{a}\right)=0$ (resp. $\mathrm{Tr}_1^n\left(\frac{1}{a}\right)=1$) is equal to $2^{n-1}-1$. Thus, we obtain that $M_1=M_2=2^{n-1}-1$.

For each given $a\in\mathbb{F}_{2^n}^*$, let $L_a(x)=x^{2^{m+1}}+x^2+cx$, and recall that $c=\frac{a^{2^{m+1}}+a^2}{a}$. Then, $L_a(x)$ is a linear transformation from $\mathbb{F}_{2^n}$ into itself. Let $A_i=\{a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2 \mid \mathrm{Tr}_1^n(\frac{1}{a})=i\}$, where $i=0,1$. Note that $\mathbb{F}_{2^n}^*=\{1\}\cup A_0\cup A_1$. The above arguments have shown that $L_a(x)=0$ has two solutions in $\mathbb{F}_{2^n}$ if $a\in\{1\}\cup A_0$ and has four solutions in $\mathbb{F}_{2^n}$ if $a\in A_1$. Moreover, when (7.12) has two (resp. four) solutions in $\mathbb{F}_{2^n}$, i.e., the kernel of $L_a(x)$ has cardinality two (resp. four), then by the homomorphism theorem the image of $L_a(x)$ has cardinality 2^{n-1} (resp. 2^{n-2}), and for each element d in the image, there exist exactly two (resp. four) elements x's in $\mathbb{F}_{2^n}$ such that $L_a(x)=d$.

For each $a\in\mathbb{F}_{2^n}^*$, let B_a denote the image of the linear transformation $L_a(x)=x^{2^{m+1}}+x^2+cx$. We have obtained that $|B_a|=2^{n-1}$ if $a\in\{1\}\cup A_0$ and $|B_a|=2^{n-2}$ if $a\in A_1$. By (7.11), for a given element $a\in\mathbb{F}_{2^n}^*$, the correspondence between d and b is one-to-one. Thus, we can conclude that for each $a\in\{1\}\cup A_0$ (resp. $a\in A_1$), $N(a,b)=2$ (resp. 4) if and only if $b\in aB_a+g(a)=\{ad+g(a)\mid d\in B_a\}$, where $N(a,b)$ denotes the number of solutions of (7.10) in $\mathbb{F}_{2^n}$. In other cases, we all have $N(a,b)=0$. Thus, the number of pairs $(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}$ such that $N(a,b)=2$ (resp. 4) is equal to $2^{n-1}\cdot 2^{n-1}$ (resp. $\left(2^{n-1}-1\right)\cdot 2^{n-2}$). This together with (7.4) gives the differential spectrum. □

Note that $\mathrm{Tr}_1^n(ag(x))=\mathrm{Tr}_1^n(a(x^{2^{m+1}+1}+x^3+x))$ is a quadratic Boolean function from GF_{2^n} to GF_2. According to Lemma 7, the Walsh transform of $\mathrm{Tr}_1^n(ag(x))$ heavily depends on its rank. Below is an auxiliary result for the rank of $\mathrm{Tr}_1^n(ag(x))$.

Lemma 8. *Let s, n, k be positive integers satisfying* $\gcd(s,n)=1$*, and without loss of generality we also assume that* $k \le n/2$*. Let*

$$Q(x)=\sum_{i=1}^{k} \mathrm{Tr}_1^n(c_i x^{2^{si}+1}),$$

where $c_i \in \mathbb{F}_{2^n}$ *and at least one* c_i *is nonzero for* $1 \le i \le k$*. Then, the rank* $2h$ *of* $Q(x)$ *is in the range* $n-2k \le 2h \le n$*.*

Proof. We consider the following equation

$$\begin{aligned} & Q(x)+Q(z)+Q(x+z) \\ = \ & \mathrm{Tr}_1^n\left(\sum_{i=1}^{k}\left(c_i x^{2^{si}} z + c_i x z^{2^{si}}\right)\right) \\ = \ & \mathrm{Tr}_1^n\left(\sum_{i=1}^{k}\left(c_i x^{2^{si}} z + c_i^{2^{-is}} x^{2^{-is}} z\right)\right) \\ = \ & \mathrm{Tr}_1^n\left(z\sum_{i=1}^{k}\left(c_i x^{2^{si}} + c_i^{2^{-is}} x^{2^{-is}}\right)\right) \\ = \ & 0 \end{aligned}$$

for all $z \in \mathbb{F}_{2^n}$. The above equation holds if and only if

$$\sum_{i=1}^{k}\left(c_i x^{2^{si}} + c_i^{2^{-is}} x^{2^{-is}}\right)=0,$$

which is equivalent to

$$\sum_{i=1}^{k}\left(c_i x^{2^{si}} + c_i^{2^{-is}} x^{2^{-is}}\right)^{2^{ks}} = \sum_{i=1}^{k}\left(c_i^{2^{ks}} x^{2^{s(k+i)}} + c_i^{2^{s(k-i)}} x^{2^{s(k-i)}}\right)=0. \tag{7.21}$$

We can rewrite (7.21) in the following form

$$\sum_{i=0}^{2k} a_i x^{2^{si}} = 0, \tag{7.22}$$

where $a_i = c_{k-i}^{2^{si}}$ for $i=0,1,\ldots,k-1$, $a_k=0$ and $a_i = c_{i-k}^{2^{ks}}$ for $i=k+1,k+2,\ldots,2k$. Since $\gcd(s,n)=1$, according to [3, Corollary 1], the equation (7.22) has at most 2^{2k} solutions in $\mathbb{F}_{2^n}$. The desired result then follows. □

With Theorem 7.3 and Lemma 8, we are ready to prove the following theorem.

Theorem 38. *Let* $n=2m+1$ *and* $g(x)=x^{2^{m+1}+1}+x^3+x$*. Then the Walsh spectrum of* $g(x)$ *is given in Table 7.1.*

Proof. It is easily seen that

Table 7.1: The Walsh spectrum of $x^{2^{m+1}+1}+x^3+x$

Value	Frequency
0	$9\cdot 2^{2n-4}+3\cdot 2^{n-3}-1$
$\pm 2^{m+1}$	$\frac{(5\cdot 2^{n-1}-2)}{3}\left(2^{n-2}\pm 2^{\frac{n-3}{2}}\right)$
$\pm 2^{m+2}$	$\frac{(2^{n-1}-1)}{3}\left(2^{n-4}\pm 2^{\frac{n-5}{2}}\right)$

$$W_g(0,b)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(bx)}=\begin{cases}2^n, \text{ if } b=0,\\ 0, \text{ if } b\neq 0.\end{cases}$$

When $a\neq 0$, $W_g(a,b)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(ax^{2^{m+1}+1}+ax^3+(a+b)x\right)}$, and $\mathrm{Tr}_1^n(ax^{2^{m+1}+1}+ax^3)$, denoted by $Q_a(x)$, is a quadratic form on $\mathbb{F}_{2^n}$. Note that

$$Q_a(x)=\mathrm{Tr}_1^n(ax^{2^{m+1}+1}+ax^3)=\mathrm{Tr}_1^n(a^{2^m}x^{2^m+1}+a^{2^{2m}}x^{2^{2m}+1}).$$

Then, by Lemma 8, the rank of $Q_a(x)$ is $n-3$ or $n-1$ since n is odd and $\gcd(m,n)=1$. When a runs through $\mathbb{F}_{2^n}^*$, assume that the number of $a\in\mathbb{F}_{2^n}^*$ such that $Q_a(x)$ has rank $n-(2i-1)$ is N_i, $i=1,2$. Then, by Lemma 7, when (a,b) runs through $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$, the Walsh transform $W_g(a,b)$ of $g(x)$ has the following distribution

$$W_g(a,b)=\begin{cases}0, & (2^n-1)+N_1(2^n-2^{n-1})+N_2(2^n-2^{n-3}) \text{ times},\\ \pm 2^{m+1}, & N_1(2^{n-2}\pm 2^{\frac{n-3}{2}}) \text{ times},\\ \pm 2^{m+2}, & N_2(2^{n-4}\pm 2^{\frac{n-5}{2}}) \text{ times}.\end{cases}$$

Next we calculate the fourth power sum of $W_g(a,b)$. On one hand, we have

$$\sum_{a,b\in\mathbb{F}_{2^n}}(W_g(a,b))^4=2^{4n}+2^{4m+4}\cdot 2^{n-1}\cdot N_1+2^{4m+8}\cdot 2^{n-3}\cdot N_2. \tag{7.23}$$

On the other hand, we have

$$\begin{aligned}&\sum_{a,b\in\mathbb{F}_{2^n}}(W_g(a,b))^4\\ =&\sum_{x,y,u,v\in\mathbb{F}_{2^n}}\sum_{b\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(b(x+y+u+v))}\sum_{a\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(a(g(x)+g(y)+g(u)+g(v)))} \qquad (7.24)\\ =&\ 2^{2n}T,\end{aligned}$$

where T denotes the number of $(x,y,u,v)\in(\mathbb{F}_{2^n})^4$ satisfying

$$\begin{cases}x+y+u+v=0,\\ g(x)+g(y)+g(u)+g(v)=0.\end{cases}$$

Let $N(a,b)$ be the number of solutions of $g(x+a)+g(x)=b$ in $\mathbb{F}_{2^n}$. Then, we have $T=\sum_{a,b\in\mathbb{F}_{2^n}} N(a,b)^2$. Using the notation and results in Theorem 37 and its proof, we have

$$T=\sum_{a,b\in\mathbb{F}_{2^n}} N(a,b)^2 = 2^{2n}+4\omega_2+16\omega_4 = 4\cdot\left(2^{2n}-2^n\right). \tag{7.25}$$

Combining (7.23), (7.24), (7.25) and the fact that $N_1+N_2=2^n-1$, we obtain the distribution of the Walsh transform of $g(x)$ as in Table 7.1. □

7.4 Binary codes from the Welch APN power function

For the Welch APN power function $F(x)=x^{2^m+3}$ and $f(x)=F(x+1)+F(x)+1$, it is easy to verify that

$$f(x)=F(x+1)+F(x)+1=(x+x^{2^m})(x^2+x+1)=g(x+x^{2^m}),$$

where $g(x)$ is the Welch permutation discussed in Section 3. With the properties of $g(x)$ presented in Section 3, we obtain the following result on the code $\mathcal{C}_{D(f)}$ constructed in Conjecture 1.

Theorem 39. *Let $n=2m+1$ with a positive integer $m\geq 2$. The binary linear code $C_{D(f)}$ defined in Conjecture 1 has length 2^{n-1}, dimension n and its nonzero weights are contained in the following set:*

$$\left\{2^{n-2}, 2^{n-2}\pm 2^{\frac{n-3}{2}}, 2^{n-2}\pm 2^{\frac{n-1}{2}}\right\}.$$

Proof. It is clear that the length of $\mathcal{C}_{D(f)}$ is 2^{n-1}. As for the dimension, since $\mathcal{C}_{D(f)}$ is linear, we need to consider the number of $a\in \mathrm{GF}_{2^n}$ such that $\mathrm{Tr}_1^n(af(x))=0$ for any $x\in \mathrm{GF}_{2^n}$, equivalently, $\sum_{x\in \mathrm{GF}_{2^n}}(-1)^{\mathrm{Tr}_1^n(af(x))}=2^n$.

Define $T_0=\{x+x^{2^m}\,|\,x\in \mathrm{GF}_{2^n}\}$ and $T_1=\{x+1\,|\,x\in T_0\}$. Note that $x+x^{2^m}$ is a two-to-one function over $\mathbb{F}_{2^n}$. Thus $T_0\cup T_1=\mathrm{GF}_{2^n}$. Since n is odd, we have $\mathrm{Tr}_1^n(1)=1$ and $\mathrm{Tr}_1^n(x)=1$ for any $x\in T_1$. Since $g(x)$ is a permutation of GF_{2^n}, one has

$$\sum_{z\in T_0}(-1)^{\mathrm{Tr}_1^n(bg(z))}+\sum_{z\in T_1}(-1)^{\mathrm{Tr}_1^n(bg(z))}=\sum_{z\in \mathrm{GF}_{2^n}}(-1)^{\mathrm{Tr}_1^n(bg(z))}=0.$$

Table 7.2: Some numerical results

Value of n	Weight enumerator of $\mathcal{C}_{D(f)}$
5	$1+6x^{10}+16x^8+10x^6$
7	$1+64x^{32}+36x^{28}+28x^{36}$
9	$1+x^{144}+108x^{120}+286x^{128}+108x^{136}+9x^{112}$
11	$1+440x^{496}+408x^{528}+22x^{480}+1156x^{512}+22x^{544}$

Then for any $a \in \mathrm{GF}_{2^n}^*$,

$$\begin{aligned}\sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(af(x))} &= 2\sum_{z\in T_0} (-1)^{\mathrm{Tr}_1^n(ag(z))} \\ &= \sum_{z\in T_0} (-1)^{\mathrm{Tr}_1^n(ag(z))} + \sum_{z\in T_0} (-1)^{\mathrm{Tr}_1^n(ag(z+1)+1)} \\ &= \sum_{z\in T_0} (-1)^{\mathrm{Tr}_1^n(ag(z)+z)} + \sum_{z\in T_0} (-1)^{\mathrm{Tr}_1^n(ag(z+1)+z+1)} \\ &= \sum_{z\in T_0} (-1)^{\mathrm{Tr}_1^n(ag(z)+z)} + \sum_{z\in T_1} (-1)^{\mathrm{Tr}_1^n(ag(z)+z)} \\ &= \sum_{x\in \mathrm{GF}_{2^n}} (-1)^{\mathrm{Tr}_1^n(ag(x)+x)}.\end{aligned} \tag{7.26}$$

By the Walsh spectrum of $g(x)$ in Theorem 38, it is clear that $W_f(a,0) = W_g(a,1) \neq 2^n$ for any nonzero $a \in \mathrm{GF}_{2^n}$. This implies that $\mathcal{C}_{D(f)}$ has dimension n. Furthermore, it follows from (7.9) that

$$\mathrm{wt}(\mathbf{c}_a) = 2^{n-2} - \frac{1}{4}\sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(ag(x)+x)}. \tag{7.27}$$

From the Walsh spectrum of $g(x)$ in Table 7.1, the possible nonzero weights of the code $\mathcal{C}_{D(f)}$ can be directly determined. □

With the help of Magma, we obtain some numerical results list in Table 7.2 , which are in accordance with Theorem 39.

Bibliography

[1] Céline Blondeau, Anne Canteaut, and Pascale Charpin. Differential properties of power functions. *International Journal of Information and Coding Theory*, 1(2):149–170, 2010.

[2] Céline Blondeau, Anne Canteaut, and Pascale Charpin. Differential properties of $x \mapsto x^{2^t-1}$. *IEEE Transactions on Information Theory*, 57(12):8127–8137, 2011.

[3] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. Determining the nonlinearity of a new family of apn functions. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 72–79. Springer, 2007.

[4] Carl Bracken and Gregor Leander. A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree. *Finite Fields and Their Applications*, 16(4):231–242, 2010.

[5] Lilya Budaghyan, Marco Calderini, and Irene Villa. On equivalence between known families of quadratic apn functions. *Finite Fields and Their Applications*, 66:101704, 2020.

[6] Claude Carlet, Cunsheng Ding, and Jin Yuan. Linear codes from perfect nonlinear mappings and their secret sharing schemes. *IEEE Transactions on Information Theory*, 51(6):2089–2102, 2005.

[7] Pascale Charpin, Gohar M Kyureghyan, and Valentin Suder. Sparse permutations with low differential uniformity. *Finite Fields and Their Applications*, 28:214–243, 2014.

[8] Chin-Long Chen. Formulas for the solutions of quadratic equations over gf(2^m)(corresp.). *IEEE Transactions on Information Theory*, 28(5):792–794, 1982.

[9] Cunsheng Ding. A construction of binary linear codes from boolean functions. *Discrete mathematics*, 339(9):2288–2303, 2016.

[10] Cunsheng Ding and Harald Niederreiter. Cyclotomic linear codes of order 3. *IEEE transactions on information theory*, 53(6):2274–2277, 2007.

[11] Hans Dobbertin. Almost perfect nonlinear power functions on GF(2^n): the welch case. *IEEE Transactions on Information Theory*, 45(4):1271–1275, 1999.

[12] Tor Helleseth. Sequences with low correlation. *Handbook of coding theory*, 1998.

[13] Kaisa Nyberg. Differentially uniform mappings for cryptography. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 55–64. Springer, 1993.

[14] Yibo Wang, Wrya K. Kadir, Chunlei Li, and Yongbo Xia. On cryptographic properties of the welch permutation and a related conjecture.

Chapter 8

Characterisation of the parameters of MWS codes according to their spread

We introduce the concept of spread of a code, and we specialize it to the case of maximum weight spectrum (MWS) codes. We classify two newly-defined sub-families of MWS codes according to their weight distributions, and completely describe their fundamental parameters. We focus on one of these families, the strictly compact MWS codes, proving their optimality as MWS codes and linking them to known codes. This chapter is based on my work with Alessio Meneghetti [9] which was presented at Sequences and Their Applications 2020 conference.

8.1 Introduction

Let $\mathbb{F}_q$ be a finite field with q elements. A $[n,k]_q$ linear code is a k-dimensional subspace of $\mathbb{F}_q^n$. The (Hamming) weight $w(x)$ of a vector $x \in \mathbb{F}_q^n$ is defined to be the number of nonzero components of x. The minimum of weights where $x \neq 0$ is the minimal distance d of the code. A linear code $[n,k]_q$ whose the minimum distance is d shall be denoted by $[n,k,d]_q$. A generator matrix for an $[n,k]_q$ linear code C is a $k \times n$ matrix over $\mathbb{F}_q$ whose row vectors generate C. Let $(n+1)$-tuples $\{A_0, A_1, \ldots, A_n\}$ be the weight distribution of an $[n,k,d]_q$ linear code C where A_i is the number of codewords in C with weight i. We denote by $S(C)$ the set of non-zero weights of a linear code C, i.e. $s \in S(C)$ if there exists $c \in C \setminus \{0\}$ such that $\mathrm{w}(c) = s$.

The weight distribution of linear codes has been appeared in many works over the years. MacWilliams in [7] constructed linear codes by employing the elements of a given weight set. She also proved that the weight set of a linear code can be derived from the weight set of its dual. Delsarte in [4] discussed some properties of codes using their weight distributions. In particular an upper bound

$$|C| \leq \sum_{i=0}^{r} \binom{n}{i} (q-1)^i$$

on the size of a q-ary code C with r nonzero distinct weights was proposed. In addition, a lower bound on the size of C was obtained using the number of distinct nonzero weights of its dual code $C^{\perp}$. More bounds on $|C|$ can be found in [5].

The concept of binary linear codes with distinct weights has been firstly proposed and fully characterised in [6]. In this work, the authors define a *distinct weight* (DW) code as a binary code whose weight distribution is of the form $A_i \in \{0,1\}$ for each i. Other than providing an infinite family of DW codes they study the automorphism group of DW codes.

Definition 44. *We denote by B_k the $[2^k-1,k,1]_2$ DW code defined by the generator matrix*

$$G = \begin{bmatrix} 1_1^{(k)} \\ 1_2^{(k)} \\ \vdots \\ 1_k^{(k)} \end{bmatrix}$$

where $1_i^{(k)}$ for $i = 1,\ldots,k$ is the (2^k-1)-bits row vector whose first 2^i-1 bits are equal to 1 and the remaining are equal to 0, e.g.

$$\begin{cases} 1_1^{(3)} = (1,0,0,0,0,0,0) \\ 1_2^{(3)} = (1,1,1,0,0,0,0) \\ 1_3^{(3)} = (1,1,1,1,1,1,1) \end{cases} \Rightarrow \begin{bmatrix} 1_1^{(3)} \\ 1_2^{(3)} \\ 1_3^{(3)} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Due to [6], there exist binary linear codes in which no two distinct codewords have the same Hamming weight and they are called distinct weight codes. Recently, independently from [6], the authors of [12] proposed the problem of determining the maximum possible number of distinct weights in a block code over any finite field $\mathbb{F}_q$. Other than providing a complete solution in the general nonlinear q-ary case, they showed a construction for binary linear codes attaining the maximum possible number of distinct weights. This family coincides with the family B_k recalled in Definition 44. In the same work, the authors proposed a bound and conjectured that the maximum number of distinct nonzero weights that a k-dimensional q-ary code can have is $\frac{q^k-1}{q-1}$. This work opened several lines of research, starting from two independent works providing solutions for the conjecture [2], [8]. Following the notation established in [2], the codes that attain this upper bound are now known as *maximum weight spectrum* (MWS) codes. Observe that DW codes are a particular case of MWS codes. Shorter codes with maximum number of weights for a given dimension were later discussed in [1, 3]. In [11], the authors discussed the largest number of nonzero weights a cyclic code of dimension k over $\mathbb{F}_q$ can have.

Theorem 40. *[12] Let C be a k-dimensional q-ary linear code. Then the maximum possible number q_k of distinct non-zero weights in C equals $q_k = \frac{q^k-1}{q-1}$.*

Definition 45. *[2] An $[n,k]_q$ code C such that $|S(C)| = \frac{q^k-1}{q-1}$ is called maximum weight spectrum (MWS) codes.*

We recall another important example of MWS code.

Definition 46. *We denote with D_q the $[\frac{q(q+1)}{2}, 2, \frac{q(q-1)}{2}]_q$ code generated by*

$$G' = \begin{bmatrix} \underbrace{\begin{matrix} 1 \\ \alpha^1 \end{matrix}}_{1} & \underbrace{\begin{matrix} 1 & 1 \\ \alpha^2 & \alpha^2 \end{matrix}}_{2} & \cdots & \underbrace{\begin{matrix} 1 & \cdots & 1 \\ \alpha^{q-1} & \cdots & \alpha^{q-1} \end{matrix}}_{q-1 \text{ times}} & \underbrace{\begin{matrix} 1 & \cdots & 1 \\ 0 & \cdots & 0 \end{matrix}}_{q \text{ times}} \end{bmatrix},$$

where α is a primitive element of $\mathbb{F}_q$.

Observe that for $k = 2$ and $q = 2$, the codes B_k and D_q coincide. This is a hint that there exists a family of MWS codes sharing the same structure and properties which will be named as *strictly compact* MWS codes and denoted by $\mathcal{SC}_{q,k}$ later.

Subsequent works propose several constructions for new families of codes [2, 3, 10], trying in particular to obtain tight bounds on the minimum possible length of MWS codes. Another related open question is whether, given two integers k and s, there exists a linear code with dimension k and exactly s distinct weights. A positive answer has been provided in [8] for the particular case of binary codes, while the q-ary case is left as a conjecture.

Due to [2], the minimum possible length of an $[n,k,d]_q$ MWS code is $n = \frac{q}{2} \cdot \frac{q^k-1}{q-1}$. An $[n,k,d]_q$ MWS code achieves this length if it has codewords of every Hamming weight from d to n and we call it *strictly compact* (Definition 47) MWS code. An $[m,l,s]_q$ *compact* (Definition 47) MWS code has codewords of every Hamming weight from s to $s + \frac{q^l-1}{q-1} - 1$.

In this work we investigate the parameters of MWS codes according to new classifications. The properties and parameters of MWS codes, strictly compact MWS codes and compact MWS codes are discussed. In particular, the codes B_k and D_q are strictly compact, and, as all strictly compact codes, they are optimal MWS codes (we will prove this in Corollary 2). We introduce the concept of *spread* (Definition 48) of a code, a sort of distance between the weight distribution of a code from a reference one. We use strictly compact codes as a reference code to measure the spread of MWS codes, namely, the spread of a MWS code C is the distance between its weight distribution and the one of a hypothetical strictly compact MWS code with equal length (see Definition 49). This choice is based upon the optimality of strictly compact codes, and it turns out that the spread is deeply linked with the length of MWS. Moreover, we investigate bounds on the minimum distance and the spread of known MWS codes.

8.2 Notation and remarks

In this section we discuss the parameters of MWS codes according to their weight distribution. In particular we will see how length, dimension and minimum distance of MWS codes are related to their weight distribution. Particular emphasis will be put on the parameters of the family $\mathcal{SC}_{q,k}$ briefly introduced in Section 8.1. The following lemma is a direct consequence of the definition of linear codes, hence we recall it without providing a proof.

Lemma 9. *Let $\{A_i\}_{i\in\{0,\dots,n\}}$ be the weight distribution of an $[n,k,d]_q$ linear code C. If C has no coordinate position is identically 0 (non-degenerate), then*

$$n = \frac{\sum_i A_i i}{q^k - q^{k-1}}.$$

We introduce some useful definitions to classify MWS codes according to their weight distribution.

Definition 47. *An MWS $[n,k,d]_q$ code C is compact if its set of weights $S(C)$ is $S(C) = \{d, d+1, \ldots, d+q_k-1\}$ where $q_k = \frac{q^k-1}{q-1}$, and it is strictly compact if it is compact and $n \in S(C)$. $\mathcal{SC}_{q,k}$ denotes a strictly compact MWS code with dimension k over $\mathbb{F}_q$.*

Proposition 14. *B_k and D_q in Definitions 44 and 46 are strictly compact for respectively any choice of k and q. In particular*

$$S(B_k) = \{1,\ldots,n\} = \{\underbrace{1\ ,\ 2\ ,\ \ldots\ ,\ 2^k-2\ ,\ 2^k-1}_{q_k \text{ consecutive integers}}\},$$

and

$$S(D_q) = \{d,\ldots,n\} = \left\{\underbrace{\frac{q(q-1)}{2}\ ,\ \ldots\ ,\ \frac{q(q+1)}{2}}_{q_k \text{ consecutive integers}}\right\}.$$

Proof. It follows from computation. □

Equivalent to Definition 47, an MWS is compact if its weight distribution is

$$\{A_i\}_{i\in\{0,\ldots,n\}} = \{1,\ \underbrace{0,\ldots,0}_{1\le i\le d-1}\ ,\ \underbrace{q-1,\ldots,q-1}_{d\le i\le d+q_k-1}\ ,\ \underbrace{0,\ldots,0}_{i>d+q_k-1}\}$$

while it is strictly compact if

$$\{A_i\}_{i\in\{0,\ldots,n\}} = \{1,\ \underbrace{0,\ldots,0}_{1\le i\le d-1}\ ,\ \underbrace{q-1,\ldots,q-1}_{i\ge d}\}.$$

Observe that for a strictly compact MWS we can write

$$S(C) = \{d,d+1,\ldots,n\} = \{n-q_k+1,\ldots,n-1,n\} = \{n-i \mid i = 0,1,\ldots,q_k-1\}\ ,$$

and in the general case, we can write the set of weights of an MWS code as

$$S(C) = \{n-s_0,\ldots,n-s_{q_k-1}\}. \tag{8.1}$$

A strictly compact MWS code with $d=1$ is called *full weight spectrum* (FWS) code in [1].

Definition 48. *Let C and $\bar{C}$ be two q-ary codes with the same length n and dimension k. We define the spread of C w.r.t a target code $\bar{C}$ as the value*

$$\Delta_{\bar{C}}(C) = \frac{1}{q-1}\sum_{i=1}^{M}(\bar{w}_i - w_i)\ ,$$

where $\{w_1,\ldots,w_M\}$ and $\{\bar{w}_1,\ldots,\bar{w}_M\}$ are the multiset of all non-zero weights of C and $\bar{C}$.

We remark that $\Delta_{\bar{C}}(C)$ is therefore equal to $\frac{1}{q-1}\left(\sum_{i=1}^{n} i\bar{A}_i - \sum_{j=1}^{n} jA_j\right)$, with $\bar{A}_i$ and A_j the weight distributions of $\bar{C}$ and C respectively. Observe that $\Delta_{\bar{C}}(C) = -\Delta_C(\bar{C})$.
For our purposes, we specialize Definition 48 to the case of MWS codes, using a hypothetical strictly compact MWS code as the target code. In this case we can therefore omit to specify

the target code, since given the $[n,k]_q$ MWS code C we know exactly the weight distribution of a strictly compact $[n,k]_q$ MWS code.

Definition 49. *The spread of an MWS code C with $S(C) = \{n-s_0,\dots,n-s_{q_k-1}\}$ is the value*

$$\Delta(C) = (s_0-0)+(s_1-1)+\cdots+(s_{q_k-1}-q_k+1) = \sum_{i=0}^{q_k-1}(s_i-i). \tag{8.2}$$

With this definition, $\Delta(C)$ can be thought as a measure of how much the weight distribution of an MWS code is spread across the entire set $\{1,\dots,n\}$, in terms of the distance from the weight distribution of a hypothetical strictly compact MWS code of length n. Due to Definition 49, we can equivalently define a strictly compact MWS code C as an MWS code with spread $\Delta(C) = 0$. As we will see, strictly compact MWS codes are optimal codes, namely, there exist no MWS code with equal dimension and length strictly less than their length. To prove this claim, the next section deals with the characterisation of the parameters of strictly compact MWS codes and their comparison with general MWS codes.

8.3 Strictly Compact MWS codes

In this section we use the notation introduced in previous section to discuss the parameters of MWS codes, with a focus on strictly compact codes. We prove in particular the link between length and spread of MWS codes, implying the optimality of strictly compact codes.

Theorem 41. *Let $\mathcal{SC}_{q,k}$ be a strictly compact MWS code of dimension k over $\mathbb{F}_q$. Then its parameters are*

$$\left[\ \frac{q}{2}\,q_k\ ,\ k\ ,\ \left(\frac{q}{2}-1\right)q_k+1\ \right]_q.$$

Proof. A strictly compact $[n,k,d]_q$ MWS code C is by definition a code with spread $\Delta(C) = 0$. In particular

$$S(C) = \{n, n-1,\dots,n-q_k+1\},\ \text{ and }\ A_i = q-1, i \in S(C). \tag{8.3}$$

By Lemma 9 we have $n = \frac{\sum_i A_i i}{q^k-q^{k-1}}$, which, due to Equation (8.3), can be written as

$$n = \frac{\sum_{i=0}^{q_k-1}(q-1)(n-i)}{q^k-q^{k-1}} = \frac{n\cdot q_k - \sum_{i=0}^{q_k-1} i}{q^{k-1}} = \frac{n\cdot q_k - \frac{(q_k-1)q_k}{2}}{q^{k-1}},$$

hence

$$n\left(q_k - q^{k-1}\right) = \frac{(q_k-1)\,q_k}{2} \tag{8.4}$$

We observe that on the left-hand side of Equation (8.4), the coefficient of n is $q_k - q^{k-1} = q_{k-1}$, while on the right-hand side we have $q_k - 1 = q\cdot q_{k-1}$. By substitution, we deduce

$$nq_{k-1} = \frac{(q\cdot q_{k-1})\,q_k}{2}, \tag{8.5}$$

which leads to the claimed length of C.
The proof that $d = \left(\frac{q}{2} - 1\right) q_k + 1$ is then a direct consequence of C being a strictly compact MWS code, since in this case the minimum weight is $n - q_k + 1$. □

Example 5. *As expected, if we use $q = 2$, then the parameters are $[2^k - 1, k, 1]_2$, namely the parameters of the known code $\mathcal{SC}_{2,k}$. Similarly, if we use $k = 2$, the parameters listed in Theorem 41 become $\left[\frac{q}{2} q_2 \, , \, 2 \, , \, \left(\frac{q}{2} - 1\right) q_2 + 1 \right]_q = \left[\frac{q}{2} (q+1) \, , \, 2 \, , \, \frac{q}{2}(q-1) \right]_q$, i.e. the parameters of $\mathcal{SC}_{q,2}$.*

Example 6. *Consider $q = 4$ and $k = 3$, namely the smallest case with q even which are not covered by $\mathcal{SC}_{2,k}$ or $\mathcal{SC}_{q,2}$. If a strictly compact MWS code would exists, then it would be a $[42, 3, 22]_4$ code.*

Theorem 42. *Let C be an MWS code. Then $n = \frac{q}{2} q_k + \frac{\Delta(C)}{q_{k-1}}$.*

Proof. We proceed similarly to the proof of Theorem 41, where Equation (8.3) is substituted by Equation (8.1). This implies, after some computation, that Equation (8.4) becomes

$$n \left(q_k - q^{k-1} \right) = \frac{(q_k - 1) q_k}{2} + \sum_{i=0}^{q_k - 1} (s_i - i) .$$

We recall that by Equation (8.2) the sum on the right-hand side is $\Delta(C)$. In this way, instead of Equation (8.5) we have $n q_{k-1} = \frac{(q \cdot q_{k-1}) q_k}{2} + \Delta(C)$. □

Corollary 2. *Strictly compact MWS codes are optimal among MWS codes.*

Proof. It follows from Theorem 41 and Theorem 42. The spread of an MWS code is indeed equal to zero if and only if the code is strictly compact, and the length of an MWS code grows together with its spread. □

8.4 On the parameters of MWS codes

In this section we consider again general MWS codes, and we use strictly compact MWS codes to obtain a characterization of their parameters.

Corollary 3. *Let C be an MWS code with q odd and odd dimension k. Then $\Delta(C) > 0$. In particular, there does not exist a strictly compact MWS code $\mathcal{SC}_{q,k}$ for q and k both odd.*

Proof. If $\Delta(C) = 0$ then C is a strictly compact MWS code, hence by Theorem 41 we know that its length is $n = \frac{q}{2} q_k \in \mathbb{Z}$. We have two possible cases: either q is even, or q_k is. Observe that if q is odd, the latter is true if and only if k is even. □

Corollary 4. *Let C be an $[n, k, d]_q$ MWS code.*

1. *Let $q \cdot k$ be even. Then $\Delta(C) = h q_{k-1}$, with h a non-negative integer.*

2. *Let $q \cdot k$ be odd. Then $\Delta(C) = \frac{2h+1}{2} q_{k-1}$, for some positive integer h.*

Proof. The length of C is equal to $\frac{q}{2} q_k + \frac{\Delta(C)}{q_{k-1}} \in \mathbb{Z}$.

1. If $q \cdot k$ is even, then either q is even or q_k is. This implies that $\frac{q}{2} q_k \in \mathbb{Z}$, and since $n \in \mathbb{Z}$, so has to be $n - \frac{q}{2} q_k = \frac{\Delta(C)}{q_{k-1}}$.

2. If both q and k are odd, then $\frac{q}{2} q_k$ is not an integer. However, since $n \in \mathbb{Z}$, $\frac{\Delta(C)}{q_{k-1}}$ is equal to $\frac{2h+1}{2}$ for a positive integer h. This implies that the spread of C is $\Delta(C) = \frac{2h+1}{2} q_{k-1}$.

□

Example 7. *Consider an MWS code C of dimension $k = 3$ over $\mathbb{F}_3$, so that by Corollary 4 C has spread $\Delta(C) = \frac{2h+1}{2} q_{k-1} = 2(2h+1) \geq 6$. If we assume $\Delta(C) = 6$ then we can apply Theorem 42 to deduce that the length of C is*

$$n = \frac{q}{2} \cdot \frac{q^k - 1}{q - 1} + \frac{q-1}{q^{k-1} - 1} \cdot 6 = \frac{3}{2} \cdot \frac{3^3 - 1}{2} + \frac{2}{3^2 - 1} \cdot 6 = \frac{3}{2} \cdot \frac{26}{2} + \frac{3}{2} = \frac{39}{2} + \frac{3}{2} = 21.$$

Some possible sets of non-zero weights of such an MWS code are

$$\{3, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21\}$$
$$\{4, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21\}$$
$$\{5, 8, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21\}$$
$$\{6, 7, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21\}$$
$$\{7, 8, 9, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21\}.$$

Proposition 15. *Let C be an $[n, k, d]_q$ MWS code.*

1. *If either q or k are even, then*

$$\begin{cases} n = \frac{q}{2} q_k + h \\ d \geq q_k(\frac{q}{2} - 1) + h(\frac{q^{k-1}}{q_k} - q_{k-1}) + 1 \\ d \leq q_k(\frac{q}{2} - 1) + h\frac{q^{k-1}}{q_k} + 1 \end{cases}$$

   where h is a non-negative integer.

2. *If both q and k are odd, then*

$$\begin{cases} n = \frac{q}{2} q_k + h + \frac{1}{2} \\ d \geq q_k(\frac{q}{2} - 1) + (\frac{2h+1}{2} q_{k-1})(\frac{1}{q_k} - 1) + 1 \\ d \leq q_k(\frac{q}{2} - 1) + (\frac{2h+1}{2})(\frac{q^{k-1}}{q_k}) + 1 \end{cases}$$

where h is a positive integer.

Proof. It follows from Corollary 4, noticing that the minimum distance is linked to the spread of the code, which in turn depends on h. □

8.5 Compact MWS codes

In this section we focus on the parameters of compact MWS codes, which are MWS codes whose set of weights is of the form $\{d, d+1, \ldots, d+q_k-1\}$.
Let us start with considering a code with either q odd and k even or with q even, i.e. as in Corollary 4, case 1, so that the spread is hq_{k-1} and the length is $n = \frac{q}{2}q_k + h$.
If we suppose that $A_n = 0$, then the spread has to be at least q_k, and this implies $h \geq \frac{q_k}{q_{k-1}}$. As a consequence $n \geq \frac{q}{2}q_k + \frac{q_k}{q_{k-1}}$.
Suppose now the maximum weight in C is $n-j$, namely $A_{n-j} \neq 0$ and $A_i = 0$ for any $i > n-j$. Similarly to above, $h \geq j\frac{q_k}{q_{k-1}}$. In this case we have obtained that $n \geq \frac{q}{2}q_k + j\frac{q_k}{q_{k-1}}$. We obtain the following complete characterization of the parameters of compact MWS codes.

Corollary 5. *Consider an $[n,k,d]_q$ compact MWS code C. Then*

1. *if $q \cdot k$ is even, then the parameters of C are*

$$\left[(\frac{q}{2} + \frac{j}{q_{k-1}})q_k \, , \, k \, , \, q_k(\frac{q}{2}-1) + j(\frac{q_k}{q_{k-1}} - 1) + 1 \right] ,$$

   where $q_{k-1} | j$.

2. *if $q \cdot k$ is odd, then the parameters of C are*

$$\left[(\frac{q}{2} + \frac{j}{q_{k-1}})q_k \, , \, k \, , \, q_k(\frac{q}{2}-1) + j(\frac{q_k}{q_{k-1}} - 1) + 1 \right] ,$$

   where $j = \frac{2r+1}{2}q_{k-1}$ and $r \in \mathbb{N}$.

Proof. If $q \cdot k$ is even, which was already introduced in the discussion above, we consider a code with maximum weight $n-j$, and we assume it is compact. Then the length is $n = \frac{q}{2}q_k + j\frac{q_k}{q_{k-1}}$ and therefore the distance is

$$d = n - j - q_k + 1 = \frac{q}{2}q_k + j\frac{q_k}{q_{k-1}} - j - q_k + 1 = q_k(\frac{q}{2} - 1) + j(\frac{q_k}{q_{k-1}} - 1) + 1$$

The case in which $q \cdot k$ is odd, namely as in Corollary 4, case 2, is very similar, since if the maximum weight is $n-j$, the spread is $hq_{k-1} + \frac{1}{2} \geq jq_k$, then $h \geq j\frac{q_k}{q_{k-1}} - \frac{1}{2}$. As a consequence, the length is $n \geq \frac{q}{2}q_k + j\frac{q_k}{q_{k-1}} + \frac{1}{2}$: which coincides with the bound in the first case and this bound is attained with equality if the code is compact.

□

As a consequence of Corollary 5 we have the following result.

Corollary 6. *The only compact MWS code with $d = 1$ is the binary full weight spectrum code.*

8.6 Known codes

MWS codes have been studied in [2, 8], where the authors also presented some bounds on the length of $[n,k]_q$ MWS codes. In this section we investigate bounds on the minimum distance and the spread of known MWS $[n,k,d]_q$ codes. In this section, by vector $A = [a_1,\ldots,a_k]$ we mean a nonzero element of $\mathbb{F}_q^k$ up to projective equivalence. We only consider *non-degenerate* $[n,k]_q$ codes. Let us first give some definitions and a simple observation.

Definition 50. *Let $m_1,\ldots,m_k$ be elements in $\mathbb{F}_q$ not all equal to zero. The set $\mathcal{H}$ consisting of all vectors $X = [x_1,\ldots,x_k]$ such that*

$$m_1x_1 + \cdots + m_kx_k = c \ , \quad \text{for } c \in \mathbb{F}_q \ ,$$

is called a hyperplane, which is a $(k-1)$-dimensional subspace of $(\mathbb{F}_q)^k$.

The number of the 1-dimensional vector spaces in $(\mathbb{F}_q)^k$ is equal to $\frac{q^k-1}{q-1} = q_k$ which coincides with the number of $(k-1)$-dimensional subspaces (hyperplanes) of $(\mathbb{F}_q)^k$. Consequently, every hyperplane contains $\frac{q^{k-1}-1}{q-1} = q_{k-1}$ k-vectors over $\mathbb{F}_q$. Any pair of distinct hyperplanes in $(\mathbb{F}_q)^k$ intersects in a $(k-2)$-dimensional subspace over $\mathbb{F}_q$.

Definition 51. *Let C be an $[n,k]_q$ code with generator matrix G where M is the (multi)set of columns of G and A is a subspace in $(\mathbb{F}_q)^k$. Then $Char_G(A)$ is the number, including multiplicity, of k-vectors in the (multi)set $M \cap A$. We denote by $m(v)$ the multiplicity of the vector v in M.*

Remark 5. *Let G be a generating matrix of an $[n,k]_q$ code C. For any non-zero vector $m = (m_1,\ldots,m_k) \in (\mathbb{F}_q)^k$, the hyperplane $m_1x_1 + \cdots + m_kx_k = 0$ contains $n-s$ columns (with multiplicity) of G if and only if the codeword mG has weight s. So we have a hyperplane with $Char_G(H) = n-s$ if and only if there is a codeword $c \in C$ with weight s.*

Theorem 43. *There exists an $[n,k,d]_q$ MWS code for each prime power q and $k \geq 2$, where*

$$n = 2^{q_k} - 1 \quad \text{and} \quad d = 2^{q^{k-1}-1} - 1.$$

Proof. The geometric construction given in [2, Theorem 3.4] leads to an $[n,k,d]_q$ code of length $n = 2^{q_k} - 1$. In the proof the characters of different hyperplanes are ranged from $2^{q_{k-1}} - 1$ to $2^{q_k} - 2^{q^{k-1}-1}$. So the minimum distance is $n - 2^{q_k} - 2^{q^{k-1}-1} = 2^{q^{k-1}-1} - 1$. □

Lemma 10. *If C is an $[n,k,d]_q$ MWS code with $k \geq 2$, then*

$$n \geq \lceil \frac{q}{2}q_k \rceil \ , \ \ d \geq \lceil \frac{q}{2}q_k - q_k + 1 \rceil \ \text{ and } \ \Delta(C) \geq 0.$$

Proof. The lower bound for n was proven in [2, Lemma 5.1] and also can be seen as a consequence of Theorem 42 and the bound for minimum distance is already given in Proposition 15. Finally the bound for $\Delta(C)$ comes from its definition. □

Proposition 16. *For $k = 2$ the bounds in Lemma 10 are tight for all prime powers q.*

Proof. The proof follows from Definition 46, Proposition 14 and [2, Proposition 5.4]. □

Remark 6. *Let $\beta \in \mathbb{F}_q$ and let $c = (c_1, \ldots, c_n)$ be a vector in $(\mathbb{F}_q)^n$. The number of coordinates of c equal to β is denoted by $c[\beta]$, namely $c[\beta] = |\{i \in \{1, \ldots, n\} \mid c_i = \beta\}|$. In [2] the authors considered codes with the following property:*

$$\text{There exists } \beta \in \mathbb{F}_q,\ \beta \neq 0, \text{ such that, for } a, b \in C,\ a[\beta] = b[\beta] \text{ only if } a = b. \qquad \text{(A)}$$

Due to [2, Corollary 5.2], if an $[n,k,d]_q$ MWS code C satisfy property (A)*, then $n \geq \lceil \frac{q \cdot q_{k+1}}{2} \rceil$. This follows by applying the bound in the Lemma 10 to the $[2n+1, k+1, d']_q$ MWS code $\bar{C}$ arisen from the construction given in [2, Proposition 4.1]. Using the same strategy we can get*

$$\Delta(c) \geq \frac{(q-2)(q^k - q)(q^{k+1} - 1)}{4(q-2)^2 \cdot q}.$$

In this setting the q_k smallest elements in $S(\bar{C})$ are exactly the elements in $S(C)$. So the minimum distance of the new $[2n+1, k+1, d']_q$ MWS code $\bar{C}$ coincides with the minimum distance of $[n,k,d]_q$ code C which means $d' = d$.

Proposition 17. *There exists an $[7,3]_2$ strictly compact MWS code C, and there exists an $[32,3]_3$ MWS code C' which is not strictly compact.*

Proof. The generator matrix of an $[7,3]_2$ is a matrix $G \in \mathbb{F}_2^{3 \times 7}$ where the (multi)set of columns M can be generated by 3 linearly independent vectors v_1, v_2, v_3 in $\mathbb{F}_2^3$ where $m(v_i) = 2^i$. $\mathbb{F}_2^3$ contains $q_3 = 7$ hyperplanes (2-dimensional subspaces) with characters $\{0, 1, \ldots, 6\}$. Due to Remark 5, the set of nonzero weights is $S(C) = \{1, 2, \ldots, 7\}$. It is easy to verify that $d = 1$, $\Delta(C) = 0$, $|S(C)| = q_k$ and $n \in S(C)$. So C is a strictly compact MWS code. The existence of $[7,3]_2$ MWS code is also shown in [2, 12].

The second part was also proven in [2]. Using the set of characters of hyperplanes, we can determine $S(C') = \{10, 14, 16, 19, 20, 21, 22, 24, 26, 27, 28, 30, 31\}$, $d = 10$ and $\Delta(C') = 50$. All the parameters satisfy the bounds given in the Lemma 10. Moreover, we already proved that there is no strictly compact MWS code when $q.k$ is odd. □

Proposition 18. *For each $k \geq 2$ there exists an MWS code C of length, minimum distance and spread*

$$n = q_{k-1} \binom{q_k}{2}\ ,\ d = q^{k-2} \left[\binom{q_k - 1}{2} - q_k + 1 \right] \text{ and } \Delta(C) = \frac{q_k \cdot q_{k-1}(q_k \cdot q_{k-1} - q_{k-1} - q)}{2}.$$

Proof. Let $\{H_0, \ldots, H_{q_{k-1}}\}$ be the set of hyperplanes in $(\mathbb{F}_q)^k$. Define the generating matrix G as follows. For each vector $v \in \mathbb{F}_q^k$, let $m(v) = \sum_{v \in H_i} i$. For $k = 2$, a hyperplane is just a single vector of length k over $\mathbb{F}_q$, so two hyperplanes might coincide or disjoint. If $k = 3$, then two distinct hyperplanes have intersection in a 1-dimensional subspace. So for $k \geq 3$, a

pair of distinct hyperplanes have intersection in a $k-2$-subspace. As a result, for $k \geq 2$ and $0 \leq s \leq \frac{q^k-1}{q-1} - 1 = q_k - 1$ we have

$$\mathrm{Char}_G(H_s) = q_{k-2}\binom{q_k}{2} + (q_{k-1} - q_{k-2}) \cdot s,$$

which tells the minimum distance is $d = n - \mathrm{Char}_G(H_{q_k-1}) = q^{k-2}\left[\binom{q_k-1}{2} - q_k + 1\right]$ and the number of columns of G should be $n = q_{k-1}\binom{q_k}{2}$. The rest follows by applying Theorem 42. □

The above length was given in [1, Proposition 3.3] and in [2, Corollary 5.9] the existence of MWS codes with length $n < q^{\frac{k^2+k-4}{2}}$ and dimension $k \geq 3$ is proven. The later gives a shorter length than the length in Proposition 18 where $k = 3$.

8.7 Conclusions

In this work we introduce the notion of spread of a code, a tool to study the fundamental parameters of a code w.r.t the weight distribution of a target code. More precisely, the spread is a measure of how much the weight distribution of a a code C is distant from the weight distribution of a target code. We focus here on MWS codes, a class of codes studied in the past few years by several authors, and we apply our methods to study the parameters of known examples of MWS codes. As a result of our approach, we are able to completely characterise the length of MWS codes according to the their spread and to provide bounds on their minimum distances (Proposition 15). Moreover, we specialise our results to two sub-families, namely to compact (Corollary 5) and strictly-compact (Theorem 41) MWS codes. We believe that the results obtained for MWS codes are a hint for the usefulness of analysing the parameters of families of codes according to their spread.

Bibliography

[1] Tim Alderson. A note on full weight spectrum codes. *Transactions on Combinatorics*, 8(3):15–22, 2019.

[2] Tim Alderson and Alessandro Neri. Maximum weight spectrum codes. *Advances in Mathematics of Communications*, 13(1):101–119, 2019.

[3] Gérard D. Cohen and Ludo Tolhuizen. Maximum weight spectrum codes with reduced length. *CoRR*, abs/1806.05427, 2018.

[4] Philippe Delsarte. Four fundamental parameters of a code and their combinatorial significance. *Information and Control*, 23(5):407 – 438, 1973.

[5] H. Enomoto, P. Frankl, N. Ito, and K. Nomura. Codes with given distances. *Graphs and Combinatorics*, 3:25–38, 1987.

[6] Abdelfattah Haily and Driss Harzalla. On the automorphism group of distinct weight codes. *Intelligent Information Management*, 7(02):80, 2015.

[7] Jessie MacWilliams. A theorem on the distribution of weights in a systematic code. *The Bell System Technical Journal*, 42(1):79–94, 1963.

[8] Alessio Meneghetti. On linear codes and distinct weights. *arXiv preprint arXiv:1804.04373*, 2018.

[9] Alessio Meneghetti and Wrya K Kadir. Characterisation of the parameters of maximum weight spectrum codes according to their spread. *arXiv preprint arXiv:2006.04567*, 2020.

[10] Nupur Patanker and Sanjay Kumar Singh. Weight distribution of a subclass of z2-double cyclic codes. *Finite Fields and Their Applications*, 57:287–308, 2019.

[11] Minjia Shi, Xiaoxiao Li, Alessandro Neri, and Patrick Solé. The largest number of weights in cyclic codes. *CoRR*, abs/1807.08418, 2018.

[12] Minjia Shi, Hongwei Zhu, Patrick Solé, and Gérard D Cohen. How many weights can a linear code have? *Designs, Codes and Cryptography*, 87(1):87–95, 2019.

Chapter 9

Conclusion

The main goal of this PhD project was to provide efficient decoding algorithms for the new defined families of rank metric codes. Beside our main research topic, we have also worked on two other problems in Hamming metric. The work presented in the included Chapters illustrates our results to this end. In particular, in Chapter 3, we have introduced an interpolation-based decoding algorithm for AGTG codes and it is able to decode rank errors of rank up to half the minimum distance. The decoding problem of AGTG codes has been reduced to the problem of solving a projective polynomial equation of the form $p(x) = u_0 x^{q^r+1} + u_1 x + u_2 = 0$ over $\mathbb{F}_{q^n}$. We have investigated the solutions of this equation when $gcd(n,r) = 1$ and proposed a deterministic method to compute zeros of a linearized polynomial which has a close connection with the zeros of $p(x)$. Very recently, Kim, Choe and Mesnager provided a complete solution for $p(x) = 0$ [4] and employing their result enables us to decode AGTG codes for all the possible values under the condition of knowing a single solution of $p(x) = 0$.

In Chapter 4, a decoding algorithm for another new family of MRD codes called Trombetti-Zhou codes [11] is provided. We used a similar interpolation-based approach as we used in Chapter 3 but we managed to reduce the decoding problem to the problem of solving a quadratic polynomial equation $q(x) = x^2 + ax + b = 0$ over $\mathbb{F}_{q^{2n}}$. This equation can be solved with linear-time complexity and the complexity of the whole decoding algorithm is dedicated by the complexity of Berlekamp-Massey algorithm which is $\mathcal{O}(n^2)$.

In Chapter 5, two new communication models which employ particular families of linearized polynomials as error interpolation polynomial are introduced. We managed to decode Gabidulin codes and go beyond the unique decoding radius by one unit. Using our models, we are also able to reduce the complexity of decoding GTG and AGTG codes. Moreover, we showed that one can define more constraints on error interpolation polynomials and decode any errors of rank $\leq k$, where k is the dimension of the code, added to GTG and AGTG codes.

Chapter 6 deals with different classes of rank metric codes that are not MRD but they are optimal with respect to different Singleton-like bounds. Efficient encoding and decoding algorithms were proposed for Hermitian, symmetric and alternating optimal rank metric codes. In Chapters 3-5 we used the relations between the coefficients of the codes evaluation polynomials but in this work we did not use the present symmetric relations and if someone manage to involve them, it may lead them to go further and decode optimal codes beyond the unique decoding radius.

Chapter 7 is dedicated to the properties of Welch permutation polynomial $g(x) = x^{2^{n+1}+1} + x^3 + x$ over $\mathbb{F}_{2^{2n+1}}$ where $n \geq 2$. We have derived the differential spectrum and Walsh transform of $g(x)$ which consequently lead us to compute the weight distribution of the code constructed in [1, Conjecture 33].

Chapter 8 studied a class of linear codes named as maximum weight spectrum (MWS) codes and they are linear codes with maximum number of distinct non-zero weights. We have introduced two new sub-families of MWS codes called compact and strictly compact MWS codes and studied the properties of these subfamilies. We also defined a new parameter called spread for MWS codes and we proved that strictly compact MWS codes are optimal codes among all MWS codes since they have spread equal to zero.

For future work on the the area of new optimal rank metric codes, the following research questions are interesting to explore.

- Gabidulin codes has been used as an alternative for Goppa code in McElice cryptosystem [2] and they have been shown to be vulnerable against structural attacks [7, 8]. With our efficient decoding algorithms for the new MRD codes AGTG and TZ codes, one may think of employing them to replace Gabidulin codes in GPT cryptosystem. So far only one of the generalized versions of Gabidulin codes [10] has been used to replace Gabidulin codes in [9].
- One can also use rank error vectors defined in Chapter 5 (first model) instead of space-symmetric rank errors in [3] and use GTG (or AGTG) codes instead of Gabidulin codes in GPT variants [5] and [6] then we may avoid potential structural attacks and possibly get the same key size found in [3, Section VI.].
- Due to the symmetric and Hermitian properties of the codes investigated in Chapter 6, there are some internal relations between the codewords components but in our decoding algorithms non of these internal relations have been used and investigating the existing relations may lead us to some new applications.

Bibliography

[1] Cunsheng Ding. A construction of binary linear codes from boolean functions. *Discrete mathematics*, 339(9):2288–2303, 2016.

[2] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In Donald W. Davies, editor, *Advances in Cryptology – EUROCRYPT'91*, pages 482–489. Springer, 1991.

[3] Thomas Jerkovits, Vladimir Sidorenko, and Antonia Wachter-Zeh. Decoding of space-symmetric rank errors, 2021.

[4] Kwang Ho Kim, Jong Hyok Choe, and Sihem Mesnager. Complete solution over GFp^n of the equation $x^{p^k+1}+x+a=0$. *arXiv.org.*, abs/2101.01003, 2021.

[5] Pierre Loidreau. An evolution of gpt cryptosystem. In *Int. Workshop Alg. Combin. Coding Theory (ACCT)*, 2016.

[6] Pierre Loidreau. A new rank metric codes based encryption scheme. In *International Workshop on Post-Quantum Cryptography*, pages 3–17. Springer, 2017.

[7] Raphael Overbeck. Extending gibson's attacks on the gpt cryptosystem. In *International Workshop on Coding and Cryptography*, pages 178–188. Springer, 2005.

[8] Raphael Overbeck. Structural attacks for public key cryptosystems based on Gabidulin codes. *Journal of cryptology*, 21(2):280–301, 2008.

[9] Sven Puchinger, Julian Renner, and Antonia Wachter-Zeh. Twisted Gabidulin codes in the gpt cryptosystem. *arXiv preprint arXiv:1806.10055*, 2018.

[10] Sven Puchinger and John Sheekey. Generalised twisted Gabidulin codes. *arXiv preprint arXiv:1703.08093*, 2017.

[11] R. Trombetti and Y. Zhou. A new family of MRD codes in $\mathbb{F}_q^{2n\times 2n}$ with right and middle nuclei $\mathbb{F}_{q^n}$. *IEEE Transactions on Information Theory*, 65(2):1054–1062, 2019.

Errata for "Decoding and constructions of codes in rank and Hamming metric"

"Wrya K. Kadir"

Thesis for the degree philosophiae doctor (PhD)

at the University of Bergen

_____ _____

(date and sign. of candidate) (date and sign. of faculty)

Errata

Page vii “Wrya K. Kadir, Chunlei Li, and Ferdinando Zullo. "Encoding and decoding of several optimal rank metric codes." arXiv.org., abs/2202.03009, 2022.” - corrected to “Wrya K. Kadir, Chunlei Li, and Ferdinando Zullo. "Encoding and decoding of several optimal rank metric codes." Cryptography and Communications (2022): 1-20.”

Page 41 Incorrect phrasing: “a work I did with” - corrected to “my work with”

Page 94 Missing article: “syndrome-based” - corrected to “the syndrome-based”

Page 94 Unnecessary space: “[26,28] ,” - corrected to “[26,28] ,”

Page 96 Removing word: “It is can” - corrected to “It can”

Page 96 Removing word: “that that” – corrected to “that”

Page 96 Incorrect phrasing: “any integer”- corrected to “any non-negative integer”

Page 98 Incorrect article: “a optimal”- corrected to “an optimal”

Page 98 Incorrect phrasing: “Theorems 32”-corrected to “Theorem 32”

Page 98 Incorrect notation: “F” - corrected to “F_q”

Page 98 Incorrect equation: “$(n - d + 2/2)$” – corrected to “$(n - d + 2)/2$”

Page 98 Incorrect phrasing: “dual base” - corrected to “dual bases”

Page 98 Incorrect phrasing: “dual base” - corrected to “dual bases”

Page 99 Missing parentheses: “$\alpha_1, \dots, \alpha_n$” – corrected to “$(\alpha_1, \dots, \alpha_n)$”

Page 100 Missing parentheses: “$\omega_0, \dots, \omega_{n-1}$” - corrected to “$(\omega_0, \dots, \omega_{n-1})$”

Page 101 Incorrect phrasing: “d-codes” – corrected to “d-code”

Page 102 Removing Word: “where and the” corrected to “where the”

Page 103 Misspelling: “Employing” – corrected to “employing”

Page 103 Misspelling: “non zero” – corrected to “nonzero”

Page 105 Punctuation: “$n + e - 1$” – corrected to “$n + e - 1$,”

Page 106 Misspelling: “rewritten” – corrected to “rewrite”

Page 106 Punctuation: “g_{n-1}).” - corrected to “g_{n-1}),”

Page 107 Punctuation: "$n + \kappa - 1$," – corrected to "$n + \kappa - 1$."

Page 107 Misspelling: "recover" – corrected to "recovering"

Page 107 Wrong notation: "q" – corrected to "ρ"

Page 108 Incorrect phrasing: "(6.27) can" corrected to "(6.27), one can"

Page 109 Punctuation: "Case1.," – corrected to "Case1,"

Page 110 Missing article: "BM" – corrected to "The BM"

Page 110 Punctuation: "$F_{2^7}^*$" – corrected as "$F_{2^7}^*$."

Page 113, Reference [8], "Greferath M., Pavcevic M., Silberstein N., Vázquez-Castro M.(eds) Network Coding and Subspace Designs. Signals and Communication Technology. Springer, Cham., 2018" – corrected to "In Network Coding and Subspace Designs, pages 03–23. Springer, 2018"

Page 113 Reference [12] "Submitted to International Symposium on Information Theory (ISIT), 2021" - corrected to "In 2021 IEEE International Symposium on Information Theory (ISIT), pages 31–36, 2021."

Page 113 Reference [13] "Wrya K. Kadir, Chunlei Li, and Ferdinando Zullo. Encoding and decoding of several optimal rank metric codes. arXiv.org., abs/2202.03009, 2022" - corrected to "Wrya K Kadir, Chunlei Li, and Ferdinando Zullo. Encoding and decoding of several optimal rank metric codes. Cryptography and Communications, pages 1–20, 2022."

Graphic design: Communication Division, UiB / Print: Skipnes Kommunikasjon AS

uib.no

ISBN: 9788230849118 (print)
9788230868959 (PDF)