

University of Kentucky

UKnowledge

---

Theses and Dissertations--Mathematics

Mathematics

---


2024

## Properties of Skew-Polynomial Rings and Skew-Cyclic Codes

Kathryn Hechtel

*University of Kentucky*, [kathrynhechtel@gmail.com](mailto:kathrynhechtel@gmail.com)

Author ORCID Identifier:

 <https://orcid.org/0009-0002-8922-650X>

Digital Object Identifier: <https://doi.org/10.13023/etd.2024.103>

[Right click to open a feedback form in a new tab to let us know how this document benefits you.](#)

### Recommended Citation

Hechtel, Kathryn, "Properties of Skew-Polynomial Rings and Skew-Cyclic Codes" (2024). *Theses and Dissertations--Mathematics*. 108.

[https://uknowledge.uky.edu/math\\_etds/108](https://uknowledge.uky.edu/math_etds/108)

This Doctoral Dissertation is brought to you for free and open access by the Mathematics at UKnowledge. It has been accepted for inclusion in Theses and Dissertations--Mathematics by an authorized administrator of UKnowledge. For more information, please contact [UKnowledge@lsv.uky.edu](mailto:UKnowledge@lsv.uky.edu).

## **STUDENT AGREEMENT:**

I represent that my thesis or dissertation and abstract are my original work. Proper attribution has been given to all outside sources. I understand that I am solely responsible for obtaining any needed copyright permissions. I have obtained needed written permission statement(s) from the owner(s) of each third-party copyrighted matter to be included in my work, allowing electronic distribution (if such use is not permitted by the fair use doctrine) which will be submitted to UKnowledge as Additional File.

I hereby grant to The University of Kentucky and its agents the irrevocable, non-exclusive, and royalty-free license to archive and make accessible my work in whole or in part in all forms of media, now or hereafter known. I agree that the document mentioned above may be made available immediately for worldwide access unless an embargo applies.

I retain all other ownership rights to the copyright of my work. I also retain the right to use in future works (such as articles or books) all or part of my work. I understand that I am free to register the copyright to my work.

## **REVIEW, APPROVAL AND ACCEPTANCE**

The document mentioned above has been reviewed and accepted by the student's advisor, on behalf of the advisory committee, and by the Director of Graduate Studies (DGS), on behalf of the program; we verify that this is the final, approved version of the student's thesis including all changes required by the advisory committee. The undersigned agree to abide by the statements above.

Kathryn Hechtel, Student

Dr. Heide Gluesing-Luerssen, Major Professor

Dr. Ben Braun, Director of Graduate Studies

Properties of Skew-Polynomial Rings and Skew-Cyclic Codes

---

DISSERTATION

---

A dissertation submitted in partial  
fulfillment of the requirements for  
the degree of Doctor of Philosophy  
in the College of Arts and Sciences  
at the University of Kentucky

By  
Kathryn M. Hechtel  
Lexington, Kentucky

Director: Dr. Heide Gluesing-Luerssen, Professor of Mathematics  
Lexington, Kentucky  
2024

Copyright© Kathryn M. Hechtel 2024  
<https://orcid.org/0009-0002-8922-650X>

## ABSTRACT OF DISSERTATION

### Properties of Skew-Polynomial Rings and Skew-Cyclic Codes

A skew-polynomial ring is a polynomial ring over a field, with one indeterminate  $x$ , where one must apply an automorphism to commute coefficients with  $x$ . It was first introduced by Ore in 1933 and since the 1980s has been used to study skew-cyclic codes. In this thesis, we present some properties of skew-polynomial rings and some new constructions of skew-cyclic codes. The dimension of a skew-cyclic code depends on the degree of its generating skew polynomial. However, due to the skew-multiplication rule, the degree of a skew polynomial can be smaller than its number of roots and hence tricky to predict. In Chapter 2, we introduce tools offered by Leroy in 2012 which connect the degree of a skew polynomial to linear independence of field elements which are related to the roots. In Chapter 3, we study a particular type of skew polynomial called a  $W$ -Polynomial. These are skew polynomials of smallest degree which vanish on some set of field elements. More specifically, we classify when skew polynomials of the form  $x^n - a$  are  $W$ -polynomials. In Chapter 4 we will make use of this work to study more general skew-cyclic codes than in the current literature and establish the skew-Roos bound for their distance. Finally, in Chapter 5, we study subfield subcodes of skew-cyclic codes, and compare skew-BCH codes of the first and second kind.

KEYWORDS: algebraic coding theory, skew-polynomial rings, skew-cyclic codes

---

Kathryn M. Hechtel

---

April 29, 2024

Properties of Skew-Polynomial Rings and Skew-Cyclic Codes

By  
Kathryn M. Hechtel

Dr. Heide Gluesing-Luerssen  
Director of Dissertation

Dr. Ben Braun  
Director of Graduate Studies

April 29, 2024  
Date

Dedicated to my parents Drs. Keith and Laura Hechtel.

## ACKNOWLEDGMENTS

First and foremost, I extend my deepest gratitude to my advisor, Dr. Heide Gluesing-Luerssen. Under her guidance, my abilities in writing, logic, and mathematical reasoning have grown profoundly. Her mentorship has been invaluable, and her wisdom will undoubtedly shape my journey in the years to come. I am also immensely thankful to Dr. Leah Marshall, my undergraduate professor, who dedicated countless office hours to teach me the art of proof-writing. Her enthusiasm for mathematics ignited my passion for the field and set me on the path I follow today. To all my other mathematics professors, thank you for enriching my academic journey. The diverse perspectives and teachings I received have been instrumental in shaping my scholarly perspective, and I consider myself fortunate to have learned from each of you.

My heartfelt thanks go to my family for their unwavering support and belief in my aspirations. To my parents, thank you for always encouraging me to reach for my dreams. To my brother KC, thank you for your constant faith in me and the joy you bring into my life. To my best friend Megan, thank you for keeping me grounded and reminding me of my capabilities when I needed it most. To my incredible fiancé, Tommy, thank you for standing by my side every day, and for always finding ways to lighten my days with laughter and love. I cannot wait for our next chapter together.

Lastly, I want to acknowledge the community of graduate students in the mathematics department. The camaraderie, support, and friendship I've experienced among you have been pivotal to my success. I truly couldn't have done this without you.

## TABLE OF CONTENTS

Acknowledgments . . . . .	iii
Chapter 1 Introduction . . . . .	1
Chapter 2 Skew-Polynomial Rings . . . . .	5
2.1 Properties of Skew-polynomial Rings . . . . .	5
2.2 Properties of the $(r, n)$ -th norm function . . . . .	12
2.3 Distance of Codes . . . . .	18
2.4 Properties of Skew-cyclic Codes . . . . .	20
Chapter 3 Noncommutative Polynomial Maps . . . . .	22
3.1 Semi Linear Maps . . . . .	22
3.2 Applications to W-Polynomials . . . . .	37
Chapter 4 W-Polynomials . . . . .	43
4.1 Vanishing set of $x^n - a$ . . . . .	43
4.2 Left and Right W-Polynomials . . . . .	47
4.3 W-polynomials in a Field Extension . . . . .	48
Chapter 5 Skew Roos Bound and the Arithmetic Progression Construction . . . . .	51
5.1 Skew Roos Bound . . . . .	51
5.2 Representative Defining Sets and Implications to MRD Codes . . . . .	55
5.3 Preliminary Results on Arithmetic Progressions . . . . .	58
5.4 Proof of Theorem 5.2.7 . . . . .	60
Chapter 6 Skew-Cyclic Subfield Subcodes . . . . .	62
6.1 Constructing Skew-Cyclic Codes over $\mathbb{F}_{q^s}$ . . . . .	62
6.2 Tapia-Tironi Theorems on Hamming Distance . . . . .	64
6.3 Comparison of skew-BCH Codes of the 1st and 2nd Kind . . . . .	69
Bibliography . . . . .	71



## Chapter 1 Introduction

In algebraic coding theory, we use vectors to represent shared information; any collection of such vectors is called a code. Often times, errors occur when these messages are sent along a noisy channel (e.g. satellite). In order to correct these errors, it can be very useful to know the distance between any two vectors in a message. Our work strives to guarantee a high minimum distance for a code. However, we would also prefer to have a code with a high dimension, so we can represent a larger amount of information. Naturally, in a higher dimensional code the vectors are closer together, so attaining a high dimensional code with a high minimum distance is nontrivial. Another task we focus on is constructing a code whose minimum distance reaches the upper bound placed by the dimension.

One class of codes that is known to have particularly nice error-correcting properties is cyclic codes. They were introduced by Prange in 1957 (see [19]) and they are given by ideals of the quotient ring  $\mathbb{F}_{q^s}[x]/(x^n - 1)$ . Here  $\mathbb{F}_{q^s}$  denotes the field of order  $q^s$  where  $q$  is a prime power (it will become clear later why we represent the finite field in this form). In the last decade, much work has been done to generalize classical cyclic codes to skew-cyclic codes (see [3]). The ambient space for skew-cyclic codes is given by the quotient module  $\mathbb{F}_{q^s}[x; \sigma]/\bullet(f)$  where  $\mathbb{F}_{q^s}[x; \sigma]$  is the skew-polynomial ring induced by an automorphism  $\sigma$  on  $\mathbb{F}_{q^s}$  (typically the  $q$ -Frobenius map), and  $\bullet(f)$  is the left ideal generated by a skew polynomial  $f$  of degree  $n$ . The quotient structure  $\mathbb{F}_{q^s}[x; \sigma]/\bullet(f)$  is isomorphic to the vector space  $\mathbb{F}_{q^s}^n$ . Hence, we are able to define skew-cyclic codes as follows. A linear code in  $\mathbb{F}_{q^s}^n$  is  $(\sigma, f)$ -skew-cyclic if it is a left submodule of the quotient structure  $\mathbb{F}_{q^s}[x; \sigma]/\bullet(f)$ .

One can easily show that each skew-cyclic code is generated by a right divisor,  $g$ , of the modulus  $f$ . Then, the dimension of the code is given by  $n - \deg(g)$ . In our work, we place conditions on the (right) roots of  $g$  to guarantee a minimum distance for the skew-cyclic code generated by  $g$ . Due to the skew-multiplication rule, a skew polynomial in  $\mathbb{F}_{q^s}[x; \sigma]$  may have more roots than suggested by its degree. Hence, the degree of the smallest skew polynomial  $g$  having a prescribed set of roots can be difficult to predict. However, this fact also tells us that the family of skew-cyclic codes is much larger than the family of classical cyclic codes.

This dissertation studies different properties of skew-polynomial rings and its impact on skew-cyclic codes. In Chapters 2, 3, and 4 we adapt and expand on skew-polynomial ring theory presented in [9], [14], [15], and [16]. In Chapters 5 and 6, we broaden some results from [1] and [20] which construct skew-cyclic codes of a prescribed distance (and in some cases, a prescribed dimension). Each chapter is described in more detail below.

In Chapter 2, we present background material on skew-polynomial rings and linear codes. Skew-polynomial rings were first introduced by Ore in his seminal paper from 1933 (see [18]). When the context is clear, we drop the prefix skew and refer to elements of  $\mathbb{F}_{q^s}[x; \sigma]$  as simply polynomials. Evaluation of these polynomials was presented by Lam in [12]. He makes use of the  $i$ -th norm function  $N_i : \mathbb{F}_{q^s} \rightarrow \mathbb{F}_{q^s}$  defined by  $N_i(a) = \prod_{j=0}^{i-1} \sigma^j(a)$ . In this chapter, we expand on some properties of this function. Most notably, for any  $\beta \in \mathbb{F}_{q^s}^*$  we classify the smallest value  $i$  where  $N_i(\beta) = 1$ . This property plays an important role in the distance theorems presented in Chapter 6.

For linear codes, we use two ways of measuring distance: the Hamming metric, and the rank metric. The Hamming distance,  $d_H$ , is measured by the number of non-zero components of a vector. The upper bound on the Hamming distance is known as the Singleton bound: for a code  $C \subset \mathbb{F}_{q^s}^n$  of dimension  $k$ , we have  $d_H(C) \leq n - k + 1$ . Codes that reach this upper bound are of particular significance and are called maximum distance separable (MDS). The rank distance,  $d_R$ , of a vector  $(v_1, \dots, v_n) \in \mathbb{F}_{q^s}^n$  is the dimension of the space  $\langle v_1, \dots, v_n \rangle_{\mathbb{F}_q}$ . There is also a Singleton-like bound for the rank metric (see Proposition 2.3.3). Codes that reach the Singleton-like bound for the rank metric are known as maximum rank distance (MRD) codes.

In Chapter 3, we present material from [16] in a slightly more streamlined way. This paper uses  $\sigma$ -semi-linear maps to develop the theory of  $\mathbb{F}_{q^s}[x; \sigma]$ -modules, such as the quotient structure we work with for skew-cyclic codes. One of the results of this paper connects the degree of a skew polynomial to linear independence of field elements related to its roots. Indeed, if we let  $\alpha_0, \dots, \alpha_{n-1}, \gamma \in \mathbb{F}_{q^s}^*$  and set  $p_i = \gamma \alpha_i^{q-1}$  for  $i = 0, \dots, n-1$ , then  $\alpha_0, \dots, \alpha_{n-1}$  are linearly independent over  $\mathbb{F}_q$  if and only if the smallest degree skew polynomial that vanishes on  $p_0, \dots, p_{n-1}$  has degree  $n$ . This tool helps us develop some of the theory for Chapter 4.

In Chapter 4, we work with a particular type of skew polynomial, namely a Wedderburn polynomial, or W-polynomial for short. First initiated by [14], a polynomial is a W-polynomial if it is the minimal polynomial for its set of roots. In particular, we determine the values of  $n \in \mathbb{N}$  and  $a \in \mathbb{F}_{q^s}^*$  for which polynomials of the form  $x^n - a$  are W-polynomials. For a  $(\sigma, f)$ -skew-cyclic code where  $f = x^n - a$ , the code is called a  $(\sigma, a)$ -skew-constacyclic code and has been studied extensively in [7]. This is also the modulus used for the codes described in Chapter 5. One nice fact about W-polynomials is that any monic factor (left, right or middle) of a W-polynomial is also a W-polynomial. This led us to investigate if any right W-polynomial (meaning it vanishes on right roots) is also a left W-polynomial (with respect to left roots). Lastly, we show that any W-polynomial will remain a W-polynomial when considered over a field extension.

There is a well-studied class of cyclic codes called BCH codes which were introduced independently by [10] and [2]. The theory states that the number of roots

forming an arithmetic progression for a generating polynomial  $g$  corresponds to a lower bound for the minimum Hamming distance of the code generated by  $g$ . In this context an arithmetic progression refers to the exponents of the roots with respect to a fixed primitive element of the field. In Chapter 5, we report on the skew Roos bound for both the Hamming distance and the rank distance presented in [1] which is a generalization of the BCH bound. In this paper, the authors provide criteria for constructing a code utilizing  $q$ -powers of a field element that are more general than in the form of an arithmetic progression. The minimal polynomial with these roots will generate a code with a known lower bound on both the minimum Hamming distance and the minimum rank distance. The authors use the modulus  $f = x^n - 1$ , where  $s$  divides  $n$ . We are able to generalize the modulus to  $x^n - a$  with  $a \in N_n(\mathbb{F}_{q^s})$  for the Hamming metric, and  $a \in N_n(\mathbb{F}_q)$  for the rank metric. In addition, we provide a counterexample illustrating that the skew Roos bound for the rank metric may not hold if  $a \in N_n(\mathbb{F}_{q^s} \setminus \mathbb{F}_q)$ .

Furthermore in [1], the authors provide conditions on the size of the set of roots of a generating polynomial which forces the resulting code to be MRD. After some work, we are able to show that any root set of this size must be in the form of an arithmetic progression. Any MRD code that satisfies the skew Roos bound is called a skew-BCH code of the second kind. The phrase the second kind refers to the fact that we are using  $q$ -powers of the field element. Skew-BCH codes of the first kind with regular exponents are studied in Chapter 6.

Even though we build skew-cyclic codes over the field  $\mathbb{F}_{q^s}$ , we will often allow the roots of the generating polynomial to come from an extension field  $\mathbb{F}_{q^{st}}$ . We can force any polynomial with roots in  $\mathbb{F}_{q^{st}}$  to be over  $\mathbb{F}_{q^s}$  by ensuring the set of roots is closed under  $\text{Aut}(\mathbb{F}_{q^{st}}/\mathbb{F}_{q^s})$ . This is something we will do often to guarantee our generating polynomial  $g$  is in  $\mathbb{F}_{q^s}[x; \sigma]$ , so that it generates a code over  $\mathbb{F}_{q^s}$ . Alternatively to get a code over  $\mathbb{F}_{q^s}$ , we could allow  $g$  and the skew-cyclic code it generates to be over  $\mathbb{F}_{q^{st}}$ , and then take its intersection with  $\mathbb{F}_{q^s}^n$ . In Chapter 6, we show that either method results in the same code. This smaller code over  $\mathbb{F}_{q^s}$  is called a skew-cyclic subfield subcode of some larger skew-cyclic code over  $\mathbb{F}_{q^{st}}$ .

In Chapter 6, our focus shifts to the examination of skew-cyclic codes, where the roots of the generating polynomial are not restricted to being  $q$ -powers of some field element. Instead, we employ roots whose regular exponents form an arithmetic progression. These codes are called skew-BCH codes of the first kind. As before, a root set with this regularity has implications for the lower bound of the minimum Hamming distance of the skew-cyclic code. This concept was initially introduced in [20]. Notably, our approach involves presenting the theorems using the minimal polynomial of the root set as the generating polynomial. By doing so, we ensure the code is constructed with the maximum achievable dimension for the chosen parameters. Additionally, we present proofs that are intended to be more intuitive compared to the computation-heavy proofs provided in [20]. Lastly, we compare the dimensions

of skew-BCH codes of the first and second kind with the same starting parameters. We are able to show that skew-BCH codes of the first kind have dimension at least as big as skew-BCH codes of the second kind.

## Chapter 2 Skew-Polynomial Rings

In a skew-polynomial ring, a skew polynomial may have more roots than its degree suggests. This lead to the use of skew polynomials in algebraic coding theory. These notes explain how we may construct skew-cyclic codes with a designed Hamming distance, and in some cases a designed rank distance.

### 2.1 Properties of Skew-polynomial Rings

In this section, we will introduce skew-polynomial rings and skew-cyclic codes. Many of the results of this section are presented in detail in [9]. Throughout, let  $q$  be a prime power and assume we have field extensions  $\mathbb{F}_{q^{st}}/\mathbb{F}_{q^s}/\mathbb{F}_q$ . Let  $\theta$  be the  $q$ -Frobenius automorphism of  $\mathbb{F}_{q^{st}}$  and let  $\sigma = \theta|_{\mathbb{F}_{q^s}}$ . Note that  $\theta$  will be different for different choices of  $q$ . For example, when we consider  $\mathbb{F}_{2^{12}}/\mathbb{F}_2$ , then  $\theta$  is given by  $a \mapsto a^2$  for  $a \in \mathbb{F}_{2^{12}}$ . However, for  $\mathbb{F}_{4^6}/\mathbb{F}_4$ , the  $q$ -Frobenius is given by  $a \mapsto a^4$  for  $a \in \mathbb{F}_{4^6}$ .

**Definition 2.1.1.** The skew-polynomial ring, denoted  $\mathbb{F}_{q^s}[x; \sigma]$ , is defined as the set

$$\left\{ \sum_{i=0}^N f_i x^i \mid N \in \mathbb{N}_0, f_i \in \mathbb{F}_{q^s} \right\}$$

with usual addition and multiplication given by the rule

$$xa = \sigma(a)x \quad \forall a \in \mathbb{F}_{q^s}.$$

**Remark 2.1.2.**

1.  $\mathbb{F}_{q^s}[x; \sigma]$  is a subring of  $\mathbb{F}_{q^{st}}[x; \theta]$ .
2. The center of the skew-polynomial ring  $\mathbb{F}_{q^s}[x; \sigma]$  is  $\mathbb{F}_q[x^s]$ . This is easily seen by using the fact that the fixed field of  $\sigma$  is  $\mathbb{F}_q$  and  $|\sigma| = s$ . Indeed, any  $f \in \mathbb{F}_q[x^s]$  satisfies  $xf = fx$  since the coefficients of  $f$  are invariant under  $\sigma$ . Moreover,  $af = fa$  for any  $a \in \mathbb{F}_{q^s}$  since  $\sigma^s(a) = a$ .

**Definition 2.1.3.** We say  $g$  right divides  $f$ , denoted  $g|_r f$ , if there exists  $h \in \mathbb{F}_{q^s}[x; \sigma]$  so that  $f = hg$ .

Skew-polynomial rings have many useful properties as seen here.

**Theorem 2.1.4.** [18, p. 483-486] *The skew-polynomial ring  $\mathbb{F}_{q^s}[x; \sigma]$  is a right Euclidean domain.*

1. *Right division with remainder:* For all  $f, g \in \mathbb{F}_{q^s}[x; \sigma]$  with  $g \neq 0$  there exists unique  $t, r \in \mathbb{F}_{q^s}[x; \sigma]$  such that  $f = tg + r$  and  $\deg(r) < \deg(g)$ .
2. For  $f_1, f_2 \in \mathbb{F}_{q^s}[x; \sigma]$  not both zero, there exists a unique monic polynomial  $d \in \mathbb{F}_{q^s}[x; \sigma]$  such that  $d|_r f_1$  and  $d|_r f_2$  and whenever  $h \in \mathbb{F}_{q^s}[x; \sigma]$  satisfies  $h|_r f_1$  and  $h|_r f_2$ , then  $h|_r d$ . The polynomial  $d$  is called the **greatest common right divisor** of  $f_1$  and  $f_2$ , denoted by  $\text{gcd}_r(f_1, f_2)$ . It also satisfies

$$d = uf_1 + vf_2 \quad \text{for some } u, v \in \mathbb{F}_{q^s}[x; \sigma].$$

3. For  $f_1, f_2 \in \mathbb{F}_{q^s}[x; \sigma]$  not both zero, there exists a unique monic polynomial  $l \in \mathbb{F}_{q^s}[x; \sigma]$  such that  $f_1|_r l$  and  $f_2|_r l$  and whenever  $h \in \mathbb{F}_{q^s}[x; \sigma]$  satisfies  $f_1|_r h$  and  $f_2|_r h$ , then  $l|_r h$ . The polynomial  $l$  is called the **least common left multiple** of  $f_1$  and  $f_2$ , denoted by  $\text{lclm}_r(f_1, f_2)$ . It also satisfies

$$l = uf_1 = vf_2 \quad \text{for some } u, v \in \mathbb{F}_{q^s}[x; \sigma].$$

4. For all nonzero  $f_1, f_2 \in \mathbb{F}_{q^s}[x; \sigma]$

$$\deg(\text{gcd}_r(f_1, f_2)) + \deg(\text{lclm}_r(f_1, f_2)) = \deg(f_1) + \deg(f_2).$$

5.  $\mathbb{F}_{q^s}[x; \sigma]$  is a left principal ideal ring. That is, for a left ideal  $I \subset \mathbb{F}_{q^s}[x; \sigma]$ , there exists  $f \in I$  where

$$I = \{gf : g \in \mathbb{F}_{q^s}[x; \sigma]\} := \bullet(f).$$

With the facts presented above, we easily get the following corollary.

**Corollary 2.1.5.** For any  $f, g \in \mathbb{F}_{q^s}[x; \sigma]$ , we have

$$\bullet(f) + \bullet(g) = \bullet(\text{gcd}_r(f, g)),$$

$$\bullet(f) \cap \bullet(g) = \bullet(\text{lclm}_r(f, g)).$$

Evaluating skew polynomials via the usual substitution of a field element in place of  $x$  will not respect the multiplication rule defined for a skew-polynomial ring. Hence, we define polynomial evaluation in the following way.

**Definition 2.1.6.** Let  $f \in \mathbb{F}_{q^s}[x; \sigma]$ , and let  $a \in \mathbb{F}_{q^s}$ .

1. We define  $f(a) = r$  where  $r$  is the remainder upon right division of  $f$  by  $x - a$ .
2. We say  $a$  is a right root of  $f$  if  $r = 0$ , that is,  $(x - a)|_r f$ .

3. For  $r, n \in \mathbb{N}$ , define the  $(r, n)$ -th norm function  $N_n^r : \mathbb{F}_{q^s} \rightarrow \mathbb{F}_{q^s}$  by  $N_0^r(a) = 1$  and

$$N_n^r(a) = \prod_{j=0}^{n-1} \sigma^{jr}(a) = a^{\frac{q^{nr}-1}{q^r-1}}.$$

If  $r = 1$ , then we use the notation  $N_n$  in place of  $N_n^1$ . More properties of the norm function are given in Section 2.2.

One may easily check the  $(r, n)$ -th norm function is multiplicative, and hence a group homomorphism on  $\mathbb{F}_{q^s}^*$ . Hence, for any  $a, b \in \mathbb{F}_{q^s}^*$ , we have

$$N_n^r(ab) = N_n^r(a)N_n^r(b). \quad (2.1)$$

Using right division with remainder to evaluate polynomials in a skew-polynomial ring can be quite computational and tedious. Luckily, the  $(r, n)$ -th norm function defined above allows us to evaluate polynomials in a more natural way.

**Proposition 2.1.7.** [13, Lem. 2.4] *Let  $f = \sum_{i=0}^N f_i x^i \in \mathbb{F}_{q^s}[x; \sigma]$  and  $a \in \mathbb{F}_{q^s}$ . Then*

$$f(a) = \sum_{i=0}^N f_i N_i(a).$$

While the number of roots of a polynomial may exceed the degree,  $\sigma$ -conjugacy classes can be useful for classification.

**Definition 2.1.8.** Let  $a, b \in \mathbb{F}_{q^s}$ .

1. For  $c \in \mathbb{F}_{q^s}^*$ , we define  $a^c := \sigma(c)ac^{-1}$ . We say  $a$  and  $b$  are  $\sigma$ -conjugates if  $b = a^c$  for some  $c \in \mathbb{F}_{q^s}^*$ . When  $\sigma$  is the  $q$ -Frobenius, this is simply  $a^c = c^{q-1}a$ . We call  $c$  the  $\sigma$ -conjugate exponent of  $b$ .
2. The  $\sigma$ -conjugacy class of  $a$  is

$$\Delta(a) = \{a^c \mid c \in \mathbb{F}_{q^s}^*\}.$$

**Remark 2.1.9.**

1. The nonzero conjugacy classes of  $\mathbb{F}_{q^s}$  are given by the cosets of  $\Delta(1) = \{c^{q-1} : c \in \mathbb{F}_{q^s}^*\}$ .
2. Furthermore, since  $|\Delta(1)| = \frac{q^s-1}{q-1}$ , there are  $q-1$  nonzero conjugacy classes in  $\mathbb{F}_{q^s}$ .

**Theorem 2.1.10.** [12, Thm. 2] Let  $f, g \in \mathbb{F}_{q^s}[x; \sigma]$  and let  $a \in \mathbb{F}_{q^s}$ . Then

$$(fg)(a) = \begin{cases} 0, & \text{if } g(a) = 0 \\ f(a^{g(a)})g(a) & \text{if } g(a) \neq 0. \end{cases}$$

The above theorem tell us that any root of  $g$  will be a root of any left multiple of  $g$ . Moreover, if  $a$  is a root of the product  $fg$ , but not  $g$ , then some conjugate of  $a$  is a root of  $f$ .

**Remark 2.1.11.** There is an analogous result for left roots. Indeed, if  $a$  is a left root of  $fg$  but not  $f$ , then some conjugate of  $a$  is a left root of  $g$ .

**Theorem 2.1.12.** [12, Thm. 4] Let  $f \in \mathbb{F}_{q^s}[x; \sigma]$  have degree  $n$ . Then the roots of  $f$  lie in at most  $n$  distinct  $\sigma$ -conjugacy classes. Furthermore, if  $f = (x - a_1) \dots (x - a_n)$  for some  $a_i \in \mathbb{F}_{q^s}$  and  $f(a) = 0$ , then  $a$  is  $\sigma$ -conjugate to some  $a_i$ .

**Proposition 2.1.13.** Let  $f \in \mathbb{F}_{q^s}[x; \sigma]$ ,  $a \in \mathbb{F}_{q^s}$  and assume  $f(a) \neq 0$ . Then,

$$\text{lclm}\{f, x - a\} = (x - a^{f(a)})f.$$

*Proof.* By the division algorithm, for some  $g \in \mathbb{F}_{q^s}[x; \sigma]$  we have  $f = g(x - a) + f(a)$ . Hence,

$$\begin{aligned} (x - a^{f(a)})f &= (x - a^{f(a)})g(x - a) + (x - a^{f(a)})f(a) \\ &= (x - a^{f(a)})g(x - a) + \sigma(f(a))(x - a). \end{aligned} \quad \square$$

**Definition 2.1.14.** Let  $A \subset \mathbb{F}_{q^s}$  and let  $d \in \mathbb{F}_{q^s}$ .

1. For any polynomial  $h \in \mathbb{F}_{q^s}[x; \sigma]$ , define the vanishing set of  $h$ , denoted  $V(h)$ , as the set of right roots of  $h$ , i.e.

$$V(h) = \{a \in \mathbb{F}_{q^s} : h(a) = 0\}.$$

2. The  $\sigma$ -minimal polynomial of  $A$ , denoted  $m_A$ , is the monic polynomial of smallest degree in  $\mathbb{F}_{q^s}[x; \sigma]$  such that  $A \subset V(m_A)$ . Clearly, if  $A = \{a_1, \dots, a_l\}$ , then

$$m_A = \text{lclm}\{x - a_i : i = 1, \dots, l\}.$$

3. The  $\sigma$ -rank of  $A$ , denoted  $\text{rk}_\sigma(A)$ , is the degree of  $m_A$ . Note that  $\text{rk}_\sigma(A) \leq |A|$ .
4. We say  $d$  is P-dependent on  $A$  if  $m_A = m_{A \cup \{d\}}$ .
5. We say  $A$  is P-independent if no element of  $a \in A$  is P-dependent on  $A \setminus \{a\}$ . Note that this is equivalent to  $\text{rk}_\sigma(A) = |A|$ .



6. We say  $B = \{p_1, \dots, p_r\} \subset A$  is a P-basis of  $A$  if  $B$  is a P-independent set, and for any  $d \in A \setminus B$  the set  $B \cup \{d\}$  is P-dependent.

The following is a direct result of Theorem 2.1.10.

**Corollary 2.1.15.** *Let  $A \subset \mathbb{F}_{q^s}$ , and let  $h \in \mathbb{F}_{q^s}[x; \sigma]$ , then  $A \subset V(h)$  if and only if  $m_A |_r h$ .*

With the following proposition, we are able to determine the minimal polynomial of some finite set using the least common left multiple of linear factors. We use this fact often to construct the minimal polynomial of some set.

**Proposition 2.1.16.** *[12, Prop. 6] Let  $A = \{a_1, \dots, a_n\} \subset \mathbb{F}_{q^s}$  and let  $r = \text{rk}_\sigma(A)$ . Then there exist a P-basis  $b_1, \dots, b_r \in A$  where  $m_A = \text{lcm}(x - b_1, \dots, x - b_r)$ .*

Another tool we often use is given by the following proposition. It allows us to force a polynomial over some smaller field with roots coming from a larger field by ensuring the root set is Galois closed. We will use this fact often in Section 6.

**Proposition 2.1.17.** *[5, Prop. 4] Fix  $A \subset \mathbb{F}_{q^{st}}$  and set*

$$\bar{A} = \{\alpha^{q^{sj}} : \alpha \in A, 0 \leq j \leq t-1\}.$$

*Then  $m_{\bar{A}}$  is a polynomial over  $\mathbb{F}_{q^s}$  rather than  $\mathbb{F}_{q^{st}}$ . It is the smallest degree monic polynomial over  $\mathbb{F}_{q^s}$  with vanishing set containing  $A$ . Conversely, let  $f \in \mathbb{F}_{q^s}[x; \sigma]$  and assume  $A = \{a \in \mathbb{F}_{q^{st}} : (x - a) |_r f\}$ . Then,  $\bar{A} = A$ .*

*Proof.* Assume  $m_{\bar{A}} = \sum_{i=0}^r h_i x^i$  with  $h_i \in \mathbb{F}_{q^{st}}$  and define  $h = \sum_{i=0}^r h_i^{q^s} x^i$ . Let  $\beta \in \bar{A}$  and note  $\beta^{q^{sj}} \in V(m_{\bar{A}})$  for all  $j$ . Then,

$$h(\beta) = \sum_{i=0}^r h_i^{q^s} N_i(\beta) = \left( \sum_{i=0}^r h_i N_i(\beta^{q^{-s}}) \right)^{q^s} = \left( m_{\bar{A}}(\beta^{q^{-s}}) \right)^{q^s} = 0.$$

Hence,  $\bar{A} \subset V(h)$ . This forces  $h = z m_{\bar{A}}$  for some  $z \in \mathbb{F}_{q^{st}}[x; \theta]$ . However, since  $m_{\bar{A}}$  and  $h$  are both monic of degree  $r$ , we have  $m_{\bar{A}} = h$ . Therefore,  $m_{\bar{A}} \in \mathbb{F}_{q^s}[x; \sigma]$ . Now, suppose  $g = \sum_{i=0}^l g_i x^i$  is the smallest degree monic polynomial over  $\mathbb{F}_{q^s}$  with a vanishing set containing  $A$ . Let  $\beta^{q^{sj}} \in \bar{A}$  where  $\beta \in A$  and  $j \in \{0, \dots, t-1\}$ , and consider

$$g(\beta^{q^{sj}}) = \sum_{i=0}^l g_i N_i(\beta^{q^{sj}}) = \left( \sum_{i=0}^l g_i N_i(\beta) \right)^{q^{sj}} = (g(\beta))^{q^{sj}} = 0.$$

This shows  $g$  also vanishes on  $\bar{A}$ . Since  $g$  is chosen to be monic and of smallest degree, we must have  $g = m_{\bar{A}}$ .

Conversely, assume  $f \in \mathbb{F}_{q^s}[x; \sigma]$  where  $f = \sum_{i=0}^r f_i x^i$  and let  $A = \{a \in \mathbb{F}_{q^{st}} : (x-a)|_r f\}$ . Note  $f_i^{q^{sj}} = f_i$  for any  $j = 0, \dots, t-1$  since  $f_i \in \mathbb{F}_{q^s}$ . Now let  $a \in A$  and let  $j \in \{0, \dots, t-1\}$  be arbitrary. Then

$$f(a^{q^{sj}}) = \sum_{i=0}^r f_i N_i(a^{q^{sj}}) = \left( \sum_{i=0}^r f_i N_i(a) \right)^{q^{sj}} = f(a)^{q^{sj}} = 0.$$

Hence,  $a^{q^{sj}} \in A$  for all  $a \in A$  and all  $j \in \{0, \dots, t-1\}$ . Therefore,  $A = \overline{A}$ .  $\square$

Not much is known about calculating the rank of an arbitrary subset of a finite field. However, the next few results give us an upper bound for the rank of any non-zero subset.

**Theorem 2.1.18.** [12, Thm. 22] *Let  $A, A' \subset \mathbb{F}_{q^s}$ , such that no element of  $A$  is  $\sigma$ -conjugate to any element of  $A'$ . Then,  $\text{rk}_\sigma(A \cup A') = \text{rk}_\sigma(A) + \text{rk}_\sigma(A')$ .*

In the following theorem, the author assumes  $q$  is prime. After careful review of the proof, it is clear this assumption is not necessary. This theorem is also stated in Section 3.2 to give the proof in that context (see Theorem 3.2.9).

**Theorem 2.1.19.** [16, Thm. 2.3] *Let  $\sigma$  be the  $q$ -Frobenius of  $\mathbb{F}_{q^s}/\mathbb{F}_q$ , then  $\text{rk}_\sigma(\mathbb{F}_{q^s}^*) = s(q-1)$ . As a result, for any  $A \subset \mathbb{F}_{q^s}^*$ ,  $\text{rk}_\sigma(A) \leq s(q-1)$ .*

The latter part of the above theorem also follows from work discussed in Section 2.2. The following is a direct result of the previous two theorems.

**Corollary 2.1.20.** *Let  $\sigma$  be the  $q$ -Frobenius of  $\mathbb{F}_{q^s}/\mathbb{F}_q$ , then  $\text{rk}_\sigma(\mathbb{F}_{q^s}) = s(q-1) + 1$ .*

**Lemma 2.1.21.** *For  $A \subset \mathbb{F}_{q^s}$  and  $\gamma \in \mathbb{F}_{q^s}^*$ , define  $\gamma A = \{\gamma a \mid a \in A\}$ . Then,  $\text{rk}_\sigma(A) = \text{rk}_\sigma(\gamma A)$ .*

*Proof.* Let  $r = \text{rk}_\sigma(A)$  and let  $m_A = \sum_{i=0}^r h_i x^i$ , with  $h_i \in \mathbb{F}_{q^s}$ . Define  $h(x) = \sum_{i=0}^r h_i (N_i(\gamma))^{-1} x^i$ . Then for  $a \in A$ ,

$$h(\gamma a) = \sum_{i=0}^r h_i (N_i(\gamma))^{-1} N_i(\gamma a) = \sum_{i=0}^r h_i N_i(a) = 0.$$

Hence,  $\gamma A \subset V(h)$ . By Corollary 2.1.15, this is equivalent to  $m_{\gamma A}|_r h$ . Therefore,  $\text{rk}_\sigma(\gamma A) \leq \text{rk}_\sigma(A)$ . Since  $A = \gamma^{-1}(\gamma A)$ , the same argument shows  $\text{rk}_\sigma(A) \leq \text{rk}_\sigma(\gamma A)$ .  $\square$

Luckily we are able to understand the rank of a set through the use of skew-Vandermonde matrices.

**Definition 2.1.22.** Let  $a_1, \dots, a_r \in \mathbb{F}_{q^s}$  and  $n \in \mathbb{N}$ . The  $n \times r$  skew-Vandermonde matrix in  $\text{Mat}_{n \times r}(\mathbb{F}_{q^s})$  is defined as

$$V_n(a_1, \dots, a_r) = \begin{pmatrix} 1 & \dots & 1 \\ N_1(a_1) & \dots & N_1(a_r) \\ \vdots & & \vdots \\ N_{n-1}(a_1) & \dots & N_{n-1}(a_r) \end{pmatrix}.$$

If  $A = \{a_1, \dots, a_r\}$ , we use the notation  $V_n(A)$  for  $V_n(a_1, \dots, a_r)$ . With this notation, the skew Vandermonde is only unique up to column ordering but that won't matter for our purposes.

**Remark 2.1.23.** For  $g(x) = \sum_{i=0}^{n-1} g_i x^i \in \mathbb{F}_{q^s}[x; \sigma]$  and  $a_1, \dots, a_r \in \mathbb{F}_{q^s}$ , we have

$$(g(a_1), \dots, g(a_r)) = (g_0, \dots, g_{n-1})V_n(a_1, \dots, a_r).$$

**Theorem 2.1.24.** [12, Thm. 8] Let  $A = \{a_1, \dots, a_n\} \subset \mathbb{F}_{q^s}$ . Then  $\text{rk}_\sigma(A) = \text{rk}(V_n(A))$  where  $\text{rk}(V_n(A))$  is the ordinary matrix rank of  $V_n(A)$ . Moreover, if  $\text{rk}_\sigma(A) = n$ , then  $\text{rk}_\sigma(B) = |B|$  for every  $B \subset A$ .

The following result is now obvious.

**Proposition 2.1.25.** [12, Prop. 17] Let  $A$  be a subset of  $\mathbb{F}_{q^s}$  and let  $d \in \mathbb{F}_{q^s}$ . Then  $d$  is  $P$ -dependent on  $A$  if and only if  $(1, N_1(d), \dots, N_{n-1}(d))^T$  is linearly dependent on  $\{(1, N_1(a), \dots, N_{n-1}(a))^T : a \in A\}$ .

The skew-Vandermonde does not need to be a square matrix to relate it to the rank of a set, as given by the next result.

**Theorem 2.1.26.** [12, Thm. 10] For a non-square Vandermonde matrix  $V_n(a_1, \dots, a_r)$ ,

$$\text{rk}(V_n(a_1, \dots, a_r)) = \min\{n, \text{rk}(V_r(a_1, \dots, a_r))\}.$$

**Remark 2.1.27.** It is well-known that a classical Vandermonde matrix has full rank if and only if the field elements are distinct in the first row. The same cannot be said for a skew-Vandermonde matrix. For the  $3 \times 3$  case, Lam showed in [12] that for distinct elements  $a, b, c \in \mathbb{F}_{q^s}$ , we have  $\text{rk}(V_3(a, b, c)) = 2$  if and only if  $a, b$ , and  $c$  satisfy  $(c - a)^{q-1}a = (b - a)^{q-1}b$ .

As we will see next, the skew-Vandermonde matrix is closely related to a Moore matrix [9, Ex. 5.10]. Hence, one can use information about a Moore matrix to draw conclusions about the elements in the skew-Vandermonde matrix. Indeed, let  $\alpha_0, \dots, \alpha_{s-1}, \gamma \in \mathbb{F}_{q^s}^*$ , and let  $p_i = \gamma\alpha_i^{q-1}$  for all  $i = 0, \dots, s-1$ . One may easily check that

$$V_s(p_0, \dots, p_{s-1}) = \text{diag}(1, N_1(\gamma), \dots, N_{s-1}(\gamma))V_s(\alpha_0^{q-1}, \dots, \alpha_{s-1}^{q-1}).$$

Let  $M = \left( \alpha_j^{q^i} \right)_{0 \leq i, j \leq s-1}$  be a Moore matrix, and note that

$$V_s(\alpha_0^{q-1}, \dots, \alpha_{s-1}^{q-1})\text{diag}(\alpha_0, \dots, \alpha_{s-1}) = M.$$

Therefore, we have

$$V_s(p_0, \dots, p_{s-1})\text{diag}(\alpha_0, \dots, \alpha_{s-1}) = \text{diag}(1, N_1(\gamma), \dots, N_{s-1}(\gamma))M. \quad (2.2)$$

It is well-known that a Moore matrix is invertible if and only if the elements of the first row are linearly independent over  $\mathbb{F}_q$  (see [17, Cor. 2.38]). This leads us to the next result.

**Corollary 2.1.28.** *Let  $\alpha_0, \dots, \alpha_{n-1}, \gamma \in \mathbb{F}_{q^s}^*$  and set  $p_i = \gamma\alpha_i^{q-1}$  for  $i = 0, \dots, n-1$ . Then  $\{\alpha_0, \dots, \alpha_{n-1}\}$  is linearly independent over  $\mathbb{F}_q$  if and only if  $\{p_0, \dots, p_{n-1}\}$  is P-independent.*

*Proof.* By Equation (2.2) and Theorem 2.1.24, we have  $\text{rk}(M) = \text{rk}(V_n(p_0, \dots, p_{n-1})) = \text{rk}_\sigma(\{p_0, \dots, p_{n-1}\})$ . Therefore,  $p_0, \dots, p_{n-1}$  are P-independent if and only if  $\text{rk}(M) = n$  which happens if and only if  $\alpha_0, \dots, \alpha_{n-1}$  are linearly independent over  $\mathbb{F}_q$ .  $\square$

The above Corollary also appears in Proposition 3.2.5 and a proof in the context of Chapter 3 is given.

## 2.2 Properties of the $(r, n)$ -th norm function

Recall the definition for the  $(r, n)$ -th norm function given in 2.1.6. In this section, we will give different properties of the norm function. We will also classify for a given  $\beta \in \mathbb{F}_{q^s}^*$  and  $m \in \mathbb{N}$  the smallest  $n \in \mathbb{N}$  where  $N_n(\beta^m) = 1$ . This work is relevant to the codes described in Theorem 6.2.1. Namely, it gives the maximum length of the codes described in the theorem. We begin with a recursive property which is used in Proposition 4.1.7.

**Lemma 2.2.1.** *Let  $n = kr$ . Then for all  $\beta \in \mathbb{F}_{q^s}^*$ ,*

$$N_n(\beta) = N_k^r(N_r(\beta)).$$

*Proof.* Consider the following.

$$N_k^r(N_r(\beta)) = N_k^r\left(\beta^{\frac{q^r-1}{q-1}}\right) = \left(\beta^{\frac{q^r-1}{q-1}}\right)^{\frac{q^{kr}-1}{q^r-1}} = \beta^{\frac{q^{kr}-1}{q-1}} = N_n(\beta). \quad \square$$

The following well-known result classifies when the  $s$ -th norm of  $\beta \in \mathbb{F}_{q^s}$  is 1.

**Theorem 2.2.2.** (*Hilbert's Theorem 90*) For  $\beta \in \mathbb{F}_{q^s}^*$ ,  $N_s(\beta) = 1$  if and only if  $\beta = \alpha^{q-1}$  for some  $\alpha \in \mathbb{F}_{q^s}$ . As a consequence,  $V(x^s - 1) = \{\alpha^{q-1} : \alpha \in \mathbb{F}_{q^s}^*\}$ .

*Proof.* First, assume  $\beta = \alpha^{q-1}$  for some  $\alpha \in \mathbb{F}_{q^s}$ . Then

$$N_s(\beta) = N_s(\alpha^{q-1}) = (\alpha^{q-1})^{\frac{q^s-1}{q-1}} = \alpha^{q^s-1} = 1.$$

Now assume  $N_s(\beta) = 1$ . Consider the map  $\varphi : \mathbb{F}_{q^s} \rightarrow \mathbb{F}_{q^s}$  where

$$\varphi = \sigma^0 + \beta\sigma + N_2(\beta)\sigma^2 + \cdots + N_{s-1}(\beta)\sigma^{s-1}.$$

Recall  $\sigma$  is defined to be the  $q$ -Frobenius. This map is non-zero due to Dedekind's Independence Theorem. Let  $\gamma \in \mathbb{F}_{q^s}^*$  and define  $\alpha := \varphi(\gamma)$ . Note that  $\beta\sigma(N_i(\beta)) = N_{i+1}(\beta)$ . Then

$$\alpha = \gamma + \beta\sigma(\gamma) + N_2(\beta)\sigma^2(\gamma) + \cdots + N_{s-1}(\beta)\sigma^{s-1}(\gamma).$$

Hence,

$$\begin{aligned} \beta\sigma(\alpha) &= \beta\sigma(\gamma) + \beta\sigma(\beta)\sigma^2(\gamma) + \beta\sigma(N_2(\beta))\sigma^3(\gamma) + \cdots + \beta\sigma(N_{s-1}(\beta))\sigma^s(\gamma) \\ &= \beta\sigma(\gamma) + N_2(\beta)\sigma^2(\gamma) + N_3(\beta)\sigma^3(\gamma) + \cdots + N_s(\beta)\sigma^s(\gamma) \\ &= \beta\sigma(\gamma) + N_2(\beta)\sigma^2(\gamma) + N_3(\beta)\sigma^3(\gamma) + \cdots + \gamma \\ &= \varphi(\gamma) \\ &= \alpha. \end{aligned}$$

This gives  $\beta\sigma(\alpha) = \alpha$ . Thus,  $\beta = \alpha^{1-q}$  as needed.  $\square$

Theorem 2.2.4 is a special case of Proposition 2.1.16 and is relevant for the background structure of the Roos Bound Theorems 5.1.3 and 5.1.4. We will see some more general results on the vanishing set of polynomials of the form  $x^n - a$  in Section 4.1. Before the theorem, we need a definition.

**Definition 2.2.3.** We call  $\alpha \in \mathbb{F}_{q^s}^*$  a normal element of  $\mathbb{F}_{q^s}$  if  $\{\alpha, \alpha^q, \dots, \alpha^{q^{s-1}}\}$  is a basis of  $\mathbb{F}_{q^s}/\mathbb{F}_q$ . A basis of this form is called normal.

**Theorem 2.2.4.** Let  $\alpha \in \mathbb{F}_{q^s}$  be a normal element of  $\mathbb{F}_{q^s}$  and set  $\beta = \alpha^{q-1}$ . Also let  $\gamma \in \mathbb{F}_{q^s}^*$ . Then

1.  $\Delta(\gamma) = V(x^s - N_s(\gamma))$ ,
2.  $B = \{\gamma\beta, \gamma\beta^q, \dots, \gamma\beta^{q^{s-1}}\}$  is a P-basis of  $V(x^s - N_s(\gamma))$ .

As a consequence,  $x^s - N_s(\gamma) = m_{\Delta(\gamma)}$ .

*Proof.*

1. Let  $b \in \mathbb{F}_{q^s}^*$ . By definition,  $b \in \Delta(\gamma)$  if  $b = c^{q-1}\gamma$  for some  $c \in \mathbb{F}_{q^s}^*$ . By Theorem 2.2.2, this happens if and only if  $N_s(b\gamma^{-1}) = 1$ . Since the  $n$ -th norm function is multiplicative, this is equivalent to  $N_s(b) = N_s(\gamma)$ , which happens if and only if  $b \in V(x^s - N_s(\gamma))$ .
2. Clearly  $m_{V(x^s - N_s(\gamma))} |_{\mathbb{F}}(x^s - N_s(\gamma))$ , so  $\text{rk}_\sigma(V(x^s - N_s(\gamma))) \leq s$ . We also know  $\gamma\beta^{q^i} \in \Delta(\gamma)$  since  $\gamma\beta^{q^i} = \gamma(\alpha^{q^i})^{q-1}$  for  $i = 0, \dots, s-1$ . By part 1, this forces  $B \subset V(x^s - N_s(\gamma))$ . By Corollary 2.1.28, we know  $\text{rk}_\sigma(B) = s$  which forces  $\text{rk}_\sigma(V(x^s - N_s(\gamma))) \geq s$ . Therefore,  $B$  is a P-basis for  $V(x^s - N_s(\gamma))$ . As a consequence, we have  $x^s - N_s(\gamma) = m_{V(x^s - N_s(\gamma))}$ .

From above, we have  $m_{\Delta(\gamma)} = m_{V(x^s - N_s(\gamma))} = x^s - N_s(\gamma)$ . □

**Corollary 2.2.5.** *For any nonzero  $\sigma$ -conjugacy class  $\Delta \subset \mathbb{F}_{q^s}$ , we have  $\text{rk}_\sigma(\Delta) = s$ .*

Now we will consider what we get when the  $i$ -th norm is not 1 for  $i = 1, \dots, n-1$ ,  $n \in \mathbb{N}$ .

**Proposition 2.2.6.** *Let  $n \in \mathbb{N}$  and let  $\beta \in \mathbb{F}_{q^s}$ . If  $N_i(\beta) \neq 1$  for  $i = 1, \dots, n-1$ , then  $1, N_1(\beta), \dots, N_{n-1}(\beta)$  are distinct.*

*Proof.* Suppose  $N_i(\beta) = N_j(\beta)$  for some  $j \leq i \leq n-1$ . Then

$$\begin{aligned} 1 &= N_i(\beta) (N_j(\beta))^{-1} = \prod_{k=0}^{i-1} \sigma^k(\beta) \prod_{l=0}^{j-1} \sigma^l(\beta^{-1}) \\ &= \prod_{k=j}^{i-1} \sigma^k(\beta) = \sigma^j(\beta) \dots \sigma^{i-1}(\beta). \end{aligned}$$

Thus,

$$1 = \sigma^{-j}(1) = \sigma^{-j}(\sigma^j(\beta) \dots \sigma^{i-1}(\beta)) = \beta \sigma(\beta) \dots \sigma^{i-j-1}(\beta) = N_{i-j}(\beta).$$

By the assumption, this forces  $i - j = 0$ , so we must have  $i = j$ . □

Having distinct  $N_1(\beta), \dots, N_{n-1}(\beta)$  for some  $\beta \in \mathbb{F}_{q^s}$  plays an important role in Theorem 6.2.1. For the rest of this section, we are working to establish the largest  $n$  for a given  $\beta$  in which this property is preserved.

**Lemma 2.2.7.** *Let  $d = \gcd(q-1, m)$ . Then,*

$$(q^s - 1) \mid m \left( \frac{q^{\frac{(q-1)s}{d}} - 1}{q-1} \right).$$

*Proof.* First note  $q^{\frac{(q-1)s}{d}} - 1 = (q^s - 1) \left( \sum_{j=0}^{\frac{q-1}{d}-1} q^{sj} \right)$ . Therefore,

$$m \left( \frac{q^{\frac{(q-1)s}{d}} - 1}{q-1} \right) = (q^s - 1) \frac{m \left( \sum_{j=0}^{\frac{q-1}{d}-1} (q^{sj} - 1) + \frac{q-1}{d} \right)}{q-1} = (q^s - 1) \left( \sum_{j=0}^{\frac{q-1}{d}-1} \frac{m(q^{sj} - 1)}{q-1} + \frac{m}{d} \right).$$

Since  $q-1 \mid q^{sj} - 1$  for all  $j$ , and  $d \mid m$ , the right most term is an integer as needed.  $\square$

As a result, we have the following useful fact. Note that the inequality in Theorem 2.1.19 follows immediately from this proposition.

**Proposition 2.2.8.** *For all  $\beta \in \mathbb{F}_{q^s}^*$ , we have  $N_{s(q-1)}(\beta) = 1$ .*

*Proof.* By Lemma 2.2.7 with  $m = 1$ , we know  $\frac{q^{s(q-1)} - 1}{q-1} = (q^s - 1)t$  for some  $t \in \mathbb{N}$ . Hence, for any  $\beta \in \mathbb{F}_{q^s}^*$ ,

$$N_{s(q-1)}(\beta) = \beta^{\frac{q^{s(q-1)} - 1}{q-1}} = \beta^{(q^s - 1)t} = 1^t = 1. \quad \square$$

Throughout the rest of this section let  $\omega$  be a primitive element of  $\mathbb{F}_{q^s}$ .

**Definition 2.2.9.** For  $\beta \in \mathbb{F}_{q^s}^*$ , define  $n(\beta) = \min\{n \in \mathbb{N} : N_n(\beta) = 1\}$ .

Now, we will put an upper bound on  $n(\beta)$  for  $\beta \in \mathbb{F}_{q^s}^*$ .

**Theorem 2.2.10.** *Let  $m \in \mathbb{N}$  and let  $\beta \in \mathbb{F}_{q^s}$ . Then,  $n(\beta^m) \leq \frac{(q-1)s}{\gcd(q-1, m)}$ . In particular,  $n(\beta) \leq (q-1)s$  for all  $\beta \in \mathbb{F}_{q^s}^*$ .*

*Proof.* Let  $d = \gcd(q-1, m)$ . By Lemma 2.2.7,  $(q^s - 1)t = m \left( \frac{q^{\frac{(q-1)s}{d}} - 1}{q-1} \right)$  for some  $t \in \mathbb{N}$ . Hence,

$$N_{\frac{(q-1)s}{d}}(\beta^m) = (\beta^m)^{\frac{q^{\frac{(q-1)s}{d}} - 1}{q-1}} = \beta^{(q^s - 1)t} = 1.$$

This forces  $n(\beta^m) \leq \frac{(q-1)s}{d}$ .  $\square$

Now, we will work to classify when we have equality in Theorem 2.2.10. Note that for  $r|s$ , the unique subfield  $\mathbb{F}_{q^r}$  of  $\mathbb{F}_{q^s}$  is given by

$$\mathbb{F}_{q^r} = \left\{ \omega^{\left(\frac{q^s-1}{q^r-1}j\right)} : 1 \leq j \leq q^r - 1 \right\} \cup \{0\}.$$

**Definition 2.2.11.** Let  $\beta \in \mathbb{F}_{q^s}$ , we say  $\beta$  is generic if  $\beta$  is not in a proper subfield of  $\mathbb{F}_{q^s}$ .

Luckily it does not matter what primitive element we start with, as discussed in the next remark.

**Remark 2.2.12.** Let  $m \in \mathbb{N}$ . Then,  $\omega^m$  is generic if and only if  $m \neq \frac{q^s-1}{q^r-1}j$  for all  $j \in \mathbb{N}$  and all  $r|s$  with  $r \neq s$ . As a consequence, if  $\hat{\omega}$  is another primitive element of  $\mathbb{F}_{q^s}$ , then  $\hat{\omega}^m$  is generic if and only if  $\omega^m$  is generic.

We may now state the result which gives equality in Theorem 2.2.10.

**Theorem 2.2.13.** Let  $m \in \mathbb{N}$  such that  $\omega^m$  is a generic element of  $\mathbb{F}_{q^s}$ , and assume  $\beta = \omega^l$  where  $\gcd(q^s - 1, l) = 1$ . Then  $n(\beta^m) = \frac{(q-1)s}{\gcd(q-1, m)}$ . In particular,  $n(\omega) = (q-1)s$  for any primitive element  $\omega \in \mathbb{F}_{q^s}$ .

Before the proof, we need some lemmas. For the rest of this section, assume  $m \in \mathbb{N}$  such that  $\omega^m$  is a generic element. Without loss of generality we may also assume  $m < q^s - 1$ .

**Lemma 2.2.14.** For all  $q, s, r \in \mathbb{N}$ ,  $\gcd(q^s - 1, q^r - 1) = q^{\gcd(s, r)} - 1$ .

*Proof.* Let  $d = \gcd(s, r)$  and let  $D = \gcd(q^s - 1, q^r - 1)$ . We will show  $D = q^d - 1$ . Since  $d|s$  and  $d|r$ , we have

$$q^d - 1 \mid q^s - 1 \quad \text{and} \quad q^d - 1 \mid q^r - 1.$$

Hence,  $(q^d - 1) \mid D$ . Conversely, note that

$$q^s \equiv 1 \pmod{D} \quad \text{and} \quad q^r \equiv 1 \pmod{D}.$$

So,  $q^{sx+ry} \equiv 1 \pmod{D}$  for all  $x, y \in \mathbb{N}_0$ . In particular,  $q^d \equiv 1 \pmod{D}$ . Hence,  $D \mid q^d - 1$ . Therefore,  $D = q^d - 1$ .  $\square$

**Lemma 2.2.15.** For all  $1 \leq r \leq s - 1$ ,  $(q^s - 1) \nmid m(q^r - 1)$ .



*Proof.* Assume for contradiction there exists  $\gamma \in \mathbb{N}_0$  such that  $(q^s - 1)\gamma = m(q^r - 1)$  for some  $r < s$  and let  $d = \gcd(r, s)$ . By Lemma 2.2.14,  $\gcd(q^s - 1, q^r - 1) = q^d - 1$ . Hence,

$$m = \frac{(q^s - 1)\gamma}{q^r - 1} = \frac{\frac{(q^s - 1)\gamma}{q^d - 1}}{\frac{q^r - 1}{q^d - 1}}.$$

Note that  $m < q^s - 1$  implies  $\gamma < q^r - 1$ . Since  $m$  must be an integer, and  $\gcd\left(\frac{q^s - 1}{q^d - 1}, \frac{q^r - 1}{q^d - 1}\right) = 1$ , the term  $\frac{q^r - 1}{q^d - 1}$  must divide  $\gamma$ . So, there exists  $\nu$  such that  $\frac{q^r - 1}{q^d - 1}\nu = \gamma$ . Note that  $\nu < q^d - 1$  since  $\gamma < q^r - 1$ . So,

$$m = \frac{(q^s - 1)\gamma}{q^r - 1} = \frac{\frac{q^s - 1}{q^d - 1}\gamma}{\frac{q^r - 1}{q^d - 1}} = \frac{q^s - 1}{q^d - 1}\nu.$$

Hence,  $\omega^m \in \mathbb{F}_{q^d}$ , contradicting that  $\omega^m$  is a generic field element.  $\square$

**Lemma 2.2.16.** *Let  $d = \gcd(m, q - 1)$ . Then*

$$(q^s - 1) \nmid m \frac{q^i - 1}{q - 1} \text{ for all } i = 1, \dots, \frac{(q - 1)s}{d} - 1.$$

*Proof.* By the division algorithm,  $i = sk + r$  for  $0 \leq k \leq \frac{q-1}{d} - 1$ ,  $0 \leq r \leq s - 1$ . Note since  $i \geq 1$ ,  $(k, r) \neq (0, 0)$ . Now, we compute

$$m \frac{q^i - 1}{q - 1} = \frac{m(q^{sk+r} - 1)}{q - 1} = \frac{mq^r(q^{sk} - 1) + m(q^r - 1)}{q - 1} = mq^r \left( \frac{q^{sk} - 1}{q - 1} \right) + \frac{m(q^r - 1)}{q - 1}.$$

For  $k = 0$ , the result follows from Lemma 2.2.15. So, assume  $k \geq 1$  and note that

$$\frac{q^{sk} - 1}{q - 1} = \frac{(q^s - 1) \left( \sum_{j=0}^{k-1} q^{sj} \right)}{q - 1} = \frac{(q^s - 1) \left( \sum_{j=0}^{k-1} (q^{sj} - 1) + k \right)}{q - 1} = (q^s - 1)M + \frac{k(q^s - 1)}{q - 1}$$

for some  $M \in \mathbb{N}$ . Now we have

$$m \frac{q^i - 1}{q - 1} = mq^r \left( (q^s - 1)M + \frac{k(q^s - 1)}{q - 1} \right) + \frac{m(q^r - 1)}{q - 1} = (q^s - 1)mq^r M + \frac{mkq^r(q^s - 1) + m(q^r - 1)}{q - 1}.$$

We need to show

$$(q^s - 1) \nmid \frac{mkq^r(q^s - 1) + m(q^r - 1)}{q - 1}.$$

If  $r = 0$ , the line above becomes

$$(q^s - 1) \nmid \frac{mk(q^s - 1)}{q - 1}.$$

For this case, it suffices to show  $\frac{mk}{q-1} \notin \mathbb{N}$ . Suppose for contradiction  $(q-1) \mid mk$ . Note that

$$\frac{mk}{q-1} = \frac{\frac{m}{d}k}{\frac{q-1}{d}}.$$

Since  $\gcd(\frac{m}{d}, \frac{q-1}{d}) = 1$ , this forces  $\frac{q-1}{d} \mid k$ . Hence,  $k = \frac{q-1}{d}\eta$  for some  $\eta \in \mathbb{N}$ , contradicting that  $1 \leq k \leq \frac{q-1}{d} - 1$ . Thus,  $\frac{mk}{q-1} \notin \mathbb{N}$ .

Now assume  $1 \leq r \leq s-1$ . By Lemma 2.2.15,  $q^s - 1 \nmid m(q^r - 1)$ . Hence,

$$(q^s - 1) \nmid mkq^r(q^s - 1) + m(q^r - 1).$$

By extension,  $q^s - 1$  cannot divide the fraction  $\frac{mkq^r(q^s-1)+m(q^r-1)}{q-1}$ . Therefore,

$$(q^s - 1) \nmid m \frac{q^i - 1}{q - 1} \text{ for all } i = 1, \dots, \frac{(q-1)s}{d} - 1. \quad \square$$

Now, we may go back to prove Theorem 2.2.13.

*Proof.* If  $\gcd(q^s - 1, l) = 1$ , then  $|w^l| = q^s - 1$ . Then, by Lemma 2.2.16,  $|w^l| \nmid m \frac{q^i - 1}{q-1}$  for  $i = 1, \dots, \frac{(q-1)s}{d} - 1$ , so  $N_i(\omega^{lm}) \neq 1$  for each  $i$  in this range. Therefore,  $n(\omega^{lm}) = \frac{(q-1)s}{d}$ .  $\square$

### 2.3 Distance of Codes

**Definition 2.3.1.** Let  $C \subset \mathbb{F}_{q^s}^n$  be a subspace and let  $x \in \mathbb{F}_{q^s}^n$ .

1. The Hamming weight of a vector  $x$  is the number of non-zero components of  $x$ , denoted  $w_H(x)$ .
2. The minimum Hamming distance of a code  $C$ , denoted  $d_H(C)$ , is defined as

$$d_H(C) = \min\{w_H(x) : x \in C, x \neq 0\}.$$

3. The rank weight over  $\mathbb{F}_q$  of a vector  $x = (x_1, \dots, x_n)$ , denoted  $w_R(x)$ , is defined as

$$w_R(x) = \dim_{\mathbb{F}_q} \langle x_1, \dots, x_n \rangle_{\mathbb{F}_q}.$$

4. The minimum rank distance of a code  $C$ , denoted  $d_R(C)$ , is defined as

$$d_R(C) = \min\{w_R(x) : x \in C, x \neq 0\}.$$

5. We call this subspace  $C$  a code with respect to the Hamming (or rank) distance. For brevity, we will simply use code from now on.

**Proposition 2.3.2** (The Singleton Bound). [11, Thm. 2.4.1] For a  $k$ -dimensional code  $C \subset \mathbb{F}_{q^s}^n$ , we have the bound

$$d_H(C) \leq n - k + 1.$$

When equality is obtained, we call this code *Maximum Distance Separable (MDS)*.

There is a similar bound for the rank metric.

**Proposition 2.3.3** (The Singleton-like Bound). [8, Lemma 1] For a code  $C \subset \mathbb{F}_{q^s}^n$ , let  $d = d_R(C)$  where the rank is over  $\mathbb{F}_q$ . Then

$$\dim_{\mathbb{F}_q}(C) \leq \max\{n, s\} (\min\{n, s\} - d + 1).$$

When equality occurs, we call this code *maximum rank distance (MRD)*.

Recall that  $\mathbb{F}_{q^s}^n \cong \mathbb{F}_q^{s \times n}$  as vector spaces over  $\mathbb{F}_q$ . For any  $\mathbb{F}_{q^s}$ -subspace  $C \subset \mathbb{F}_{q^s}^n$ , we know  $\dim_{\mathbb{F}_q}(C) = s \dim_{\mathbb{F}_{q^s}}(C)$ . So, the proposition above becomes

$$\begin{aligned} \dim_{\mathbb{F}_{q^s}}(C) &\leq \left\lfloor \frac{n}{s}(s - d + 1) \right\rfloor, & \text{if } s \leq n, \\ \dim_{\mathbb{F}_{q^s}}(C) &\leq n - d + 1, & \text{if } n \leq s. \end{aligned} \tag{2.3}$$

This bound will be used later on in Proposition 5.2.4. The Hamming metric and the rank metric are very closely related as seen here.

**Lemma 2.3.4.** Let  $C \subset \mathbb{F}_{q^s}^n$  be a code. Then,

$$d_R(C) = \min\{d_H(C \cdot M) : M \in GL_n(\mathbb{F}_q)\}.$$

*Proof.* Let  $d_r = d_R(C)$  and let  $d_h = \min\{d_H(C \cdot M) : M \in GL_n(\mathbb{F}_q)\}$ .

( $\leq$ ) For any  $c \in C$ ,  $M \in GL_n(\mathbb{F}_q)$ , clearly  $w_R(c) = w_R(cM) \leq w_H(cM)$ , so  $d_r \leq d_h$ .

( $\geq$ ) Let  $c \in C$  of min rank weight  $d_r$ . There exists  $M_0 \in GL_n(\mathbb{F}_q)$  where

$$cM_0 = (c_1, \dots, c_{d_r}, 0, \dots, 0).$$

Hence,  $d_r = w_H(cM_0) \geq \min_M(w_H(cM)) \geq d_h$ . □

The following topic will be discussed in detail in Section 6.

**Theorem 2.3.5.** [11, Thm. 3.8.4] Let  $C \subset \mathbb{F}_{q^{st}}^n$  be a code and let  $k = \dim_{\mathbb{F}_{q^{st}}}(C)$ . Then  $C \cap \mathbb{F}_{q^s}^n$  is a code over  $\mathbb{F}_{q^s}$  where

$$\dim_{\mathbb{F}_{q^s}}(C \cap \mathbb{F}_{q^s}^n) \leq k.$$

We call  $C \cap \mathbb{F}_{q^s}^n$  a subfield-subcode.

## 2.4 Properties of Skew-cyclic Codes

Throughout this section, let  $f \in \mathbb{F}_{q^s}[x; \sigma]$  where  $\deg(f) = n$ . This defines a left  $\mathbb{F}_{q^s}[x; \sigma]$ -module

$$\mathcal{R}_f = \mathbb{F}_{q^s}[x; \sigma] / \bullet(f).$$

For  $g \in \mathbb{F}_{q^s}[x; \sigma]$ , we use the notation  $\bar{g} := g + \bullet(f) \in \mathcal{R}_f$ . Then, for  $z \in \mathbb{F}_{q^s}[x; \sigma]$ , we have  $z\bar{g} = \overline{z}g$ .

Consider the  $\mathbb{F}_{q^s}$ -isomorphism of left vector spaces

$$\mathfrak{p}_f : \mathbb{F}_{q^s}^n \rightarrow \mathcal{R}_f, \quad (c_0, \dots, c_{n-1}) \mapsto \overline{\sum_{i=0}^{n-1} c_i x^i}.$$

Think of  $\mathfrak{p}_f$  as polynomialization, and  $\mathfrak{v}_f = \mathfrak{p}_f^{-1}$  as vectorization.

**Proposition 2.4.1.** [4] *If  $M$  is a left submodule of  $\mathcal{R}_f$ , then there exists a unique monic polynomial  $\bar{g} \in M$  of smallest degree such that  $M = \bullet(\bar{g})$ . Alternatively,  $g$  is the unique monic right divisor of  $f$  such that  $\bullet(\bar{g}) = M$ . We call  $g$  the generating polynomial of  $M$ .*

### Definition 2.4.2.

1. A subspace  $C \subset \mathbb{F}_{q^s}^n$  is called a  $(\sigma, f)$ -skew-cyclic code if  $\mathfrak{p}_f(C)$  is a submodule of  $\mathcal{R}_f$ .
2. For  $\bar{g} \in \mathcal{R}_f$ , we define the skew circulant matrix as

$$\Gamma_f^\sigma(\bar{g}) := \begin{pmatrix} \mathfrak{v}_f(\bar{g}) \\ \mathfrak{v}_f(x\bar{g}) \\ \vdots \\ \mathfrak{v}_f(x^{n-2}\bar{g}) \\ \mathfrak{v}_f(x^{n-1}\bar{g}) \end{pmatrix}.$$

For the rest of this document, assume  $\text{rs}(\cdot)$  denotes the row space and  $\ker_l(\cdot)$  denotes the left kernel.

**Proposition 2.4.3.** [7, Cor. 2.4] *Let  $M = \bullet(\bar{g}) \subseteq \mathcal{R}_f$ , where  $g \in \mathbb{F}_{q^s}[x; \sigma]$  has degree  $r$ . Then:*

1. For any  $u \in \mathbb{F}_{q^s}^n$ , we have  $\mathfrak{p}_f(u\Gamma_f^\sigma(\bar{g})) = \mathfrak{p}_f(u)\bar{g}$ .
2.  $\mathfrak{v}_f(M) = \text{rs}(\Gamma_f^\sigma(\bar{g}))$ .

3. Suppose in addition  $g|_r f$ . Then  $M$  is a left  $\mathbb{F}_{q^s}$ -vector space of dimension  $k := n - r$  with basis  $\{\bar{g}, \overline{xg}, \dots, \overline{x^{k-1}g}\}$ . As a consequence,  $\text{rk}(\Gamma_f^\sigma(\bar{g})) = k$  and  $\mathbf{v}_f(M) = \text{rs}(G)$  where  $G$  consists of the first  $k$  rows of the skew-circulant  $\Gamma_f^\sigma(\bar{g})$ , i.e.

$$G = \begin{pmatrix} \mathbf{v}_f(\bar{g}) \\ \mathbf{v}_f(x\bar{g}) \\ \vdots \\ \mathbf{v}_f(x^{k-1}\bar{g}) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \dots & g_r & & & & \\ & \sigma(g_0) & \sigma(g_1) & \dots & \sigma(g_r) & & & \\ & & \ddots & \ddots & & \ddots & & \\ & & & \sigma^{k-1}(g_0) & \sigma^{k-1}(g_1) & \dots & \sigma^{k-1}(g_r) & \end{pmatrix}.$$

**Remark 2.4.4.** Due to part 3 of the proposition above, the modulus  $f$  plays a very small role in the construction of skew-cyclic codes. We often choose  $f$  to be any monic left multiple of degree  $n$  of the generating function  $g$ .

**Proposition 2.4.5.** [6, Prop. 4] Let  $f \in \mathbb{F}_{q^s}[x; \sigma]$  be any monic modulus of degree  $n$  and let  $g \in \mathbb{F}_{q^s}[x; \sigma]$  be a monic right divisor of  $f$  of degree  $r$  where  $g = \text{lclm}\{x - a_i \mid i = 1, \dots, r\}$  for distinct  $a_1, \dots, a_r \in \mathbb{F}_{q^s}$ . Let  $V = V_n(a_1, \dots, a_r)$  be the skew-Vandermonde from Definition 2.1.22. Then  $C = \bullet(\bar{g})$  is given by

$$\mathbf{v}_f(C) = \ker_l(V) = \{c \in \mathbb{F}_{q^s}^n : cV = 0\}.$$

We call  $V = V_n(a_1, \dots, a_r)$  a parity check matrix for  $C$ .

## Chapter 3 Noncommutative Polynomial Maps

This chapter reports on the results derived in [16]. We present the material in a slightly more streamlined way, fill in various details, and simplify some of the arguments.

### 3.1 Semi Linear Maps

Throughout, let  $\mathbb{F}_{q^s}$  be a finite field, and let  $\sigma \in \text{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$ . Also let  $R = \mathbb{F}_{q^s}[x; \sigma]$ .

**Definition 3.1.1.** Let  $V$  be an  $\mathbb{F}_{q^s}$ -vector space. An additive map  $T : V \rightarrow V$  such that for any  $\alpha \in \mathbb{F}_{q^s}$  and  $v \in V$ ,

$$T(\alpha v) = \sigma(\alpha)T(v)$$

is called a  $\sigma$ -semi linear map ( $\sigma$ -SLM).

Note that any  $\sigma$ -SLM is  $\mathbb{F}_q$ -linear. For  $n, l \in \mathbb{N}$ , we will allow  $\sigma$  to be extended component-wise to  $\mathbb{F}_{q^s}^{n \times l}$ . It is well-known that extending  $\sigma$  to  $\mathbb{F}_{q^s}^{n \times l}$  entry-wise gives an  $\mathbb{F}_q$ -endomorphism, still denoted  $\sigma$ , on  $\mathbb{F}_{q^s}^{n \times l}$ . Moreover, this extended  $\sigma$  is a  $\sigma$ -SLM. This is used later on in Remark 3.1.11.

**Proposition 3.1.2.** *For an additive abelian group  $(V, +)$ , the following are equivalent:*

1.  $V$  is a left  $R$ -module.
2.  $V$  is an  $\mathbb{F}_{q^s}$ -vector space and there exists a  $\sigma$ -SLM  $T : V \rightarrow V$ .
3. There exists a ring homomorphism  $\Lambda : R \rightarrow \text{End}(V, +)$ .

*Proof.*

(1)  $\Rightarrow$  (2) Assume  $V$  is a left  $R$ -module. Then, since  $\mathbb{F}_{q^s} \subset R$ , clearly  $V$  is also an  $\mathbb{F}_{q^s}$ -vector space. Now consider the additive map  $T : V \rightarrow V$  where  $v \mapsto xv$ . This map is  $\sigma$ -semi linear since for  $\alpha \in \mathbb{F}_{q^s}$ , we have  $T(\alpha v) = x\alpha v = \sigma(\alpha)xv = \sigma(\alpha)T(v)$ .

(2)  $\Rightarrow$  (3) Assume  $V$  is an  $\mathbb{F}_{q^s}$ -vector space and  $T : V \rightarrow V$  is a  $\sigma$ -SLM. Consider the map

$$\Lambda : R \rightarrow \text{End}(V, +) \text{ where } \sum_i f_i x^i \mapsto \sum_i f_i T^i.$$

Then, one easily checks for  $f, g \in R$ , we have  $\Lambda(f + g) = \Lambda(f) + \Lambda(g)$  and  $\Lambda(fg) = \Lambda(f) \circ \Lambda(g)$ .

(3)  $\Rightarrow$  (1) Assume there exists a ring homomorphism  $\Lambda : R \rightarrow \text{End}(V, +)$ . For  $f \in R$  and  $v \in V$ , define  $f \cdot v := \Lambda(f)(v)$ . Then for  $g \in R$  and  $u \in V$ , we have

$$\begin{aligned} f \cdot (u + v) &= \Lambda(f)(u + v) = \Lambda(f)(u) + \Lambda(f)(v) = f \cdot u + f \cdot v \\ (f + g) \cdot (v) &= \Lambda(f + g)(v) = (\Lambda(f) + \Lambda(g))(v) = \Lambda(f)(v) + \Lambda(g)(v) = f \cdot v + g \cdot v \\ (fg) \cdot v &= \Lambda(fg)(v) = (\Lambda(f) \circ \Lambda(g))(v) = \Lambda(f)(\Lambda(g)(v)) = f \cdot (g \cdot v). \end{aligned}$$

Hence,  $V$  is an  $R$ -module. □

Using the homomorphism in Proposition 3.1.2  $\Lambda : R \rightarrow \text{End}(V, +)$ , for  $f = \sum_{i=0}^n a_i x^i \in R$ , and for a  $\sigma$ -SLM  $T : V \rightarrow V$ , we define the notation

$$f(T) := \Lambda(f) = \sum_{i=0}^n a_i T^i \in \text{End}(V, +).$$

With this notation, for any  $f, g \in R$  and any  $\sigma$ -SLM  $T$ , we have

$$(fg)(T) = f(T) \circ g(T).$$

The following is a result that appears in the proof of Proposition 3.1.2. In particular, part 3 below tells us for an  $R$ -module  $V$ , the  $R$ -module structure induced by  $T$  on  $V$  agrees with the existing structure.

**Corollary 3.1.3.**

1. Given a left  $R$ -module  $V$ , define  $T : V \rightarrow V$  where  $v \mapsto xv$ . Then  $T$  is a  $\sigma$ -SLM.
2. Conversely, let  $V$  be an  $\mathbb{F}_{q^s}$ -vector space and let  $T : V \rightarrow V$  be a  $\sigma$ -SLM. Then the  $R$ -module structure on  $V$  induced by  $T$  is given by  $f \cdot v = f(T)(v)$  for all  $v$  and all  $f \in R$ .
3. If  $V$  is an  $R$ -module and  $T$  is as in part 1, then  $fv = f(T)(v)$  for all  $v \in V$  and all  $f \in R$ .

For the next few results up to Example 3.1.10, assume  $V$  is an  $\mathbb{F}_{q^s}$ -vector space with basis  $\beta = \{v_1, \dots, v_n\}$ . Also, let  $\psi_\beta : V \rightarrow \mathbb{F}_{q^s}^n$  be the coordinate map for the basis  $\beta$  which maps  $v_i$  to  $e_i$  where  $e_i$  is the standard basis vector of  $\mathbb{F}_{q^s}^n$ .

**Definition 3.1.4.** For a map  $\tau \in \text{End}(V, +)$ , we define the representative matrix of  $\tau$  for the basis  $\beta$ , denoted  $[\tau]_\beta$ , as the matrix

$$[\tau]_\beta := \begin{bmatrix} \psi_\beta(\tau(v_1)) \\ \psi_\beta(\tau(v_2)) \\ \vdots \\ \psi_\beta(\tau(v_n)) \end{bmatrix} \in \mathbb{F}_{q^s}^{n \times n}.$$

Note that if  $\tau$  is a linear map, this is the standard definition for the matrix representation of a map. Hence, for a linear map  $\tau$ , it is a well-known from linear algebra that  $\psi_\beta(\tau(v)) = \psi_\beta(v)[\tau]_\beta$ . The analogue for  $\sigma$ -semi linear maps is given in the next proposition. Both facts will be used to prove Proposition 3.1.13 below.

**Proposition 3.1.5.** *Let  $T : V \rightarrow V$  be a  $\sigma$ -SLM. Then for any  $v \in V$ , the matrix  $C := [T]_\beta$  satisfies*

$$\psi_\beta(T(v)) = \sigma(\psi_\beta(v))C.$$

*Proof.* Let  $v \in V$  where  $v = \sum_{i=1}^n a_i v_i$  with  $a_i \in \mathbb{F}_{q^s}$ . Then note that  $T(v) = \sum_{i=1}^n \sigma(a_i)T(v_i)$ . Hence,

$$\begin{aligned} \psi_\beta(T(v)) &= \psi_\beta \left( \sum_{i=1}^n \sigma(a_i)T(v_i) \right) = \sum_{i=1}^n \sigma(a_i)\psi_\beta(T(v_i)) \\ &= (\sigma(a_1), \dots, \sigma(a_n))C = \sigma(\psi_\beta(v))C. \end{aligned} \quad \square$$

**Definition 3.1.6.** Let  $T : V \rightarrow V$  be  $\sigma$ -SLM, and let  $C := [T]_\beta$ . This gives rise to a new  $\sigma$ -SLM denoted  $T_C : \mathbb{F}_{q^s}^n \rightarrow \mathbb{F}_{q^s}^n$  where  $v \mapsto \sigma(v)C$ . We refer to this map  $T_C$  as the  $\sigma$ -SLM on  $\mathbb{F}_{q^s}^n$  corresponding to  $T$ .

Note that by Corollary 3.1.3(2), we now have a left  $R$ -module structure on  $\mathbb{F}_{q^s}^n$  (see also Proposition 3.1.18). By construction, the following diagram commutes,

$$\begin{array}{ccc} V & \xrightarrow{T} & V \\ \downarrow \psi_\beta & & \downarrow \psi_\beta \\ \mathbb{F}_{q^s}^n & \xrightarrow{T_C} & \mathbb{F}_{q^s}^n \end{array}$$

In fact, by extension the following also commutes for any  $f \in R$ ,

$$\begin{array}{ccc} V & \xrightarrow{f(T)} & V \\ \downarrow \psi_\beta & & \downarrow \psi_\beta \\ \mathbb{F}_{q^s}^n & \xrightarrow{f(T_C)} & \mathbb{F}_{q^s}^n \end{array}$$

We will now extend the definition of the norm function given in Definition 2.1.6 to matrices. This will allow us to evaluate polynomials on a matrices as follows.

**Definition 3.1.7.** Let  $C \in \mathbb{F}_{q^s}^{n \times n}$ .

1. Define  $N_0(C) = I_n$  and for  $i \geq 1$ ,

$$N_i(C) := \sigma^{i-1}(C)\sigma^{i-2}(C) \dots \sigma(C)C.$$



2. For  $g \in R$  where  $g = \sum_{i=0}^r g_i x^i$ , define

$$g(C) := \sum_{i=0}^r g_i N_i(C).$$

**Proposition 3.1.8.** *Let  $T : V \rightarrow V$  be a  $\sigma$ -SLM. Define  $C := [T]_\beta$  and let  $T_C : \mathbb{F}_{q^s}^n \rightarrow \mathbb{F}_{q^s}^n$  be given by  $u \mapsto \sigma(u)C$  as in Definition 3.1.6. Then, for  $u \in \mathbb{F}_{q^s}^n$ , and  $g \in R$  where  $g = \sum_{i=0}^r g_i x^i$ , we have*

1.  $g(T_C)(u) = \sum_{i=0}^r g_i \sigma^i(u) N_i(C)$ ,
2.  $g(C) = [g(T)]_\beta$ .

*Proof.*

1. It suffices to show this for  $g = x^i$ ,  $i \geq 0$ . We will proceed by induction on  $i$ . For the base case,  $T_C^0(u) = u = uI_n$  as expected. Now, for the inductive hypothesis assume  $T_C^i(u) = \sigma^i(u)N_i(C)$ . Then,

$$T_C^{i+1}(u) = T_C(T_C^i(u)) = T_C(\sigma^i(u)N_i(C)) = \sigma^{i+1}(u)\sigma(N_i(C))C = \sigma^{i+1}(u)N_{i+1}(C).$$

2. Recall by definition, row  $j$  of  $[g(T)]_\beta$  is given by  $\psi_\beta(g(T)(v_j))$ . By the commutative diagram following Definition 3.1.6 and by part (1) we have

$$\begin{aligned} \psi_\beta(g(T)(v_j)) &= g(T_C)(\psi_\beta(v_j)) = \sum_{i=0}^r g_i \sigma^i(\psi_\beta(v_j)) N_i(C) = \sum_{i=0}^r g_i \sigma^i(e_j) N_i(C) \\ &= \sum_{i=0}^r g_i e_j N_i(C) = e_j \sum_{i=0}^r g_i N_i(C) = e_j g(C). \quad \square \end{aligned}$$

The following is an example of the second part of Proposition 3.1.8.

**Example 3.1.9.** Let  $\alpha \in \mathbb{F}_{q^s}$  and let  $f = x^3 - \alpha \in R$ . Note that the  $R$ -module  $V = R/\bullet(f)$  is an  $\mathbb{F}_{q^s}$ -vector space with basis  $\beta = \{\bar{1}, \bar{x}, \bar{x}^2\}$  (see Section 2.4). Let  $T : V \rightarrow V$  be the  $\sigma$ -SLM given by left multiplication by  $x$ . Then,

$$\begin{aligned} T(\bar{1}) &= \bar{x}, \\ T(\bar{x}) &= \bar{x}^2, \\ T(\bar{x}^2) &= \bar{\alpha}. \end{aligned}$$

Hence, the matrix representation of  $T$  is

$$C = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \alpha & 0 & 0 \end{bmatrix}.$$

Now let  $g = x^2 + x \in R$  and consider

$$\begin{aligned} g(T)(\bar{1}) &= \overline{x + x^2}, \\ g(T)(\bar{x}) &= \overline{\alpha + x^2}, \\ g(T)(\overline{x^2}) &= \overline{\sigma(\alpha)x + \alpha}. \end{aligned}$$

So, we have

$$[g(T)]_\beta = \begin{bmatrix} 0 & 1 & 1 \\ \alpha & 0 & 1 \\ \alpha & \sigma(\alpha) & 0 \end{bmatrix}.$$

Now, using matrix evaluation we have

$$g(C) = N_2(C) + N_1(C) = \sigma(C)C + C = \begin{bmatrix} 0 & 1 & 1 \\ \alpha & 0 & 1 \\ \alpha & \sigma(\alpha) & 0 \end{bmatrix}.$$

Thus, one can see  $[g(T)]_\beta = g(C)$  as expected.

**Example 3.1.10.** As a special case of Definition 3.1.6, let  $a \in \mathbb{F}_{q^s}$  and consider  $V = R/\bullet(x - a)$ . Note  $V$  is a 1-dimensional  $\mathbb{F}_{q^s}$ -vector space, so let its basis be  $\beta = \{\bar{1}\}$ .

Let  $T : V \rightarrow V$  be the  $\sigma$ -SLM given by left multiplication by  $x$ . By Corollary 3.1.3,  $T$  induces an  $R$ -module structure on  $V$  that agrees with the natural structure on  $V$ . Hence, for an arbitrary  $f \in R$  we have the identity

$$f(T)(\bar{1}) = f(1 + \bullet(x - a)) = f + \bullet(x - a) = \overline{f(a)}.$$

Note that  $T(\bar{1}) = \bar{x} = \bar{a}$ . So, the representative matrix of  $T$  is the  $1 \times 1$  matrix  $[a]$ . Hence, the corresponding  $\sigma$ -SLM  $T_a : \mathbb{F}_{q^s} \rightarrow \mathbb{F}_{q^s}$  is given by  $\alpha \mapsto \sigma(\alpha)a$ . This map  $T_a$  is called the  $\sigma$ -SLM induced by  $a$ . By Proposition 3.1.2, the map  $T_a$  places an  $R$ -module structure on  $\mathbb{F}_{q^s}$ . Moreover, this  $R$ -module structure encompasses polynomial evaluation at  $x = a$  as we will see next.

If we consider both  $f(T)$  and  $f(T_a)$  on the basis element  $\bar{1}$ , we get

$$\psi_\beta(f(T)(\bar{1})) = \psi_\beta(\overline{f(a)}) = f(a)$$

and

$$f(T_a)(\psi_\beta(\bar{1})) = f(T_a)(1).$$

Therefore, since we know the diagram below Definition 3.1.6 is commutative, we know  $f(a) = f(T_a)(1)$ . Hence, polynomial evaluation on an element  $a$  can be done in  $\mathbb{F}_{q^s}$  using  $T_a$ .

This also exemplifies the connection between the above polynomial evaluation

$$f(a) = f(T_a)(1) = \sum_{i=0}^n f_i T_a^i(1)$$

and the evaluation given in Proposition 2.1.7:

$$f(a) = \sum_{i=0}^n f_i N_i(a)$$

where  $N_i$  is the  $i$ -th norm function defined on field elements such as the original definition given in 2.1.6. This is in fact a special case of Proposition 3.1.8, since  $T_a^i(1) = \sigma^i(1)N_i(a) = N_i(a)$ .

**Remark 3.1.11.**

1. The composition of two  $\sigma$ -SLMs is usually not a  $\sigma$ -SLM.
2. Let  ${}_A V_B$  be an  $(A, B)$ -bimodule where  $A$  and  $B$  are rings with unity and let  $\sigma$  be an endomorphism on  $A$ . Suppose  $S$  and  $T$  are  $\sigma$ -SLMs defined on  ${}_A V$  (which we define similar to  $\sigma$ -SLMs on vector spaces). Then for any  $b \in B$ , we may define a  $\sigma$ -SLM  $T_b$  as follows

$$T_b : {}_A V_B \rightarrow {}_A V_B \text{ where } v \mapsto S(v)b + T(v).$$

3. Let  $A = \mathbb{F}_{q^s}^{n \times n}$  and  $B = \mathbb{F}_{q^s}^{l \times l}$ . Then  $V = \mathbb{F}_{q^s}^{n \times l}$  is an  $(A, B)$ -bimodule. Let  $\sigma \in \text{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$  be extended entry-wise to  $A$ . Then as a special case of (2) with  $S = \sigma$ ,  $T = 0$  and any  $b \in \mathbb{F}_{q^s}^{l \times l}$ , we obtain the  $\sigma$ -SLM

$$T_b : \mathbb{F}_{q^s}^{n \times l} \rightarrow \mathbb{F}_{q^s}^{n \times l} \text{ where } v \mapsto \sigma(v)b.$$

4. Let  $A$  be a ring with unity and let  $\sigma$  be an endomorphism on  $A$ . Then, for a left  $A$ -module  $V$ , we have an  $(A, \text{End}_A(V))$ -bimodule structure on  $V$ . To see  $V$  is in fact a right  $\text{End}_A(V)$ -module, we define  $v\varphi := \varphi(v)$  for  $v \in V$  and  $\varphi \in \text{End}_A(V)$ . Then for  $\psi \in \text{End}_A(V)$ , we define composition of  $\varphi$  and  $\psi$  as  $\varphi\psi := \psi \circ \varphi$ , i.e. first apply  $\varphi$  and then apply  $\psi$ . As we will see next, these definitions respect the associativity rule for  $V$  as a right  $\text{End}_A(V)$ -module. Indeed,

$$(v\varphi)\psi = (\varphi(v))\psi = \psi(\varphi(v)) = v(\varphi\psi).$$

Now, we will see the associativity rule for  $V$  as an  $(A, \text{End}_A(V))$ -bimodule is also respected by this definition of  $v\varphi$ . For  $\alpha \in A$  and  $\varphi \in \text{End}_A(V)$  we have

$$(\alpha v)\varphi = \varphi(\alpha v) = \alpha(\varphi(v)) = \alpha(v\varphi).$$

We will now return to the notion that  $R = \mathbb{F}_{q^s}[x; \sigma]$  and that  $V$  is any left  $R$ -module. For the rest of this section, we will use the notation given in Remark 3.1.11(4) where  $v\varphi := \varphi(v)$  for  $v \in V$  and  $\varphi \in \text{End}_R(V)$ . Again, for  $\varphi, \psi \in \text{End}_R(V)$ , the composition  $\varphi\psi$  is given by first applying  $\varphi$  and then applying  $\psi$ . This gives rise to the following proposition.

**Proposition 3.1.12.** *Let  $T : V \rightarrow V$  be the  $\sigma$ -SLM given by left multiplication by  $x$ . Then, for any  $f \in R$ , the map  $f(T) \in \text{End}(V, +)$  is left  $\mathbb{F}_q$ -linear and right  $\text{End}_R(V)$ -linear.*

*Proof.* Recall any  $\sigma$ -SLM is left  $\mathbb{F}_q$ -linear. So clearly  $f(T)$  is left  $\mathbb{F}_q$ -linear. Now, let  $v \in V$  and let  $\varphi \in \text{End}_R(V)$ . Then,

$$\begin{aligned} f(T)(v\varphi) &= f(T)(\varphi(v)) = \sum_{i=0}^n f_i T^i(\varphi(v)) = \sum_{i=0}^n f_i x^i \varphi(v) = \sum_{i=0}^n \varphi(f_i x^i v) \\ &= \varphi \left( \sum_{i=0}^n f_i T^i(v) \right) = \varphi(f(T)(v)) = f(T)(v)\varphi. \end{aligned}$$

Note the equality at the end of the first line is given by  $\varphi$  being an  $R$ -endomorphism of  $V$ .  $\square$

As a result of Proposition 3.1.12,  $\ker(f(T))$  is a right  $\text{End}_R(V)$ -submodule of  $V$ . Indeed, for  $v \in \ker(f(T))$  and  $\varphi \in \text{End}_R(V)$ ,

$$f(T)(v\varphi) = f(T)(v)\varphi = \varphi(0) = 0.$$

For  $V = R/\bullet(x - a)$  with  $a \in \mathbb{F}_{q^s}$ , this module structure on  $\ker(f(T_a))$  will play a role later on in Corollary 3.1.21.

Recall a  $\sigma$ -SLM  $T_i$  defined on an  $\mathbb{F}_{q^s}$ -vector space  $V_i$  gives an  $(R, \text{End}_R(V_i))$ -bimodule structure on  $V_i$ . We will use this fact in the proposition below with  $i = 1, 2$ .

**Proposition 3.1.13.** *For  $i = 1, 2$ , let  $V_i$  be an  $\mathbb{F}_{q^s}$ -vector space with basis  $\beta_i$  and dimension  $n_i$ . Let  $T_i$  be a  $\sigma$ -SLM on  $V_i$  with representative matrix  $C_i \in \mathbb{F}_{q^s}^{n_i \times n_i}$  in the basis  $\beta_i$ . Suppose  $\varphi : V_1 \rightarrow V_2$  is an  $\mathbb{F}_{q^s}$ -linear map with representative matrix  $B \in \mathbb{F}_{q^s}^{n_1 \times n_2}$  in the corresponding bases  $\beta_1$  and  $\beta_2$ . Then, the following are equivalent.*

1.  $\varphi$  is an  $R$ -linear map.

2.  $(T_1(v))\varphi = T_2(v\varphi)$  for all  $v \in V_1$ , i.e. the diagram on the right commutes.

3.  $C_1 B = \sigma(B) C_2$ .

4.  $B \in \ker(T_{C_2} - L_{C_1})$  where

$$T_{C_2} : \mathbb{F}_{q^s}^{n_1 \times n_2} \rightarrow \mathbb{F}_{q^s}^{n_1 \times n_2} \text{ with } \Gamma \mapsto \sigma(\Gamma) C_2,$$

$$\begin{array}{ccc} V_1 & \xrightarrow{\varphi} & V_2 \\ \downarrow T_1 & & \downarrow T_2 \\ V_1 & \xrightarrow{\varphi} & V_2 \end{array}$$

and

$$L_{C_1} : \mathbb{F}_{q^s}^{n_1 \times n_2} \rightarrow \mathbb{F}_{q^s}^{n_1 \times n_2} \text{ with } \Gamma \mapsto C_1 \Gamma.$$

*Proof.*

(1)  $\Leftrightarrow$  (2) For  $v \in V_1$  we have  $(T_1(v))\varphi = (xv)\varphi$  and  $T_2(v\varphi) = x(v\varphi)$ . Hence,  $(T_1(v))\varphi = T_2(v\varphi)$  for all  $v \in V_1$  if and only if  $\varphi$  is  $R$ -linear.

(2)  $\Leftrightarrow$  (3) Recall from Proposition 3.1.5 that for any  $u \in V_i$ , we have

$$\psi_{\beta_i}(T_i(u)) = \sigma(\psi_{\beta_i}(u))C_i.$$

Also, since  $\varphi$  is  $\mathbb{F}_{q^s}$ -linear, we know for any  $v \in V_1$ ,

$$\psi_{\beta_2}(v\varphi) = \psi_{\beta_1}(v)B.$$

Hence, for any  $v \in V_1$  we have the following identities

$$\begin{aligned} \psi_{\beta_2}(T_2(v\varphi)) &= \sigma(\psi_{\beta_2}(v\varphi))C_2 = \sigma(\psi_{\beta_1}(v)B)C_2 = \sigma(\psi_{\beta_1}(v))\sigma(B)C_2, \\ \psi_{\beta_2}((T_1(v))\varphi) &= \psi_{\beta_1}(T_1(v))B = \sigma(\psi_{\beta_1}(v))C_1B. \end{aligned}$$

Therefore,  $(T_1(v))\varphi = T_2(v\varphi)$  for all  $v \in V_1$  if and only if  $\sigma(B)C_2 = C_1B$ .

(3)  $\Leftrightarrow$  (4) For any  $B \in \mathbb{F}_{q^s}^{n_1 \times n_2}$ ,

$$(T_{C_2} - L_{C_1})(B) = T_{C_2}(B) - L_{C_1}(B) = \sigma(B)C_2 - C_1B.$$

Hence,  $B \in \ker(T_{C_2} - L_{C_1})$  if and only if  $\sigma(B)C_2 = C_1B$ .  $\square$

Now we will turn to a particular  $R$ -module structure. Let  $f \in R$  where  $f = \sum_{i=0}^n f_i x^i$  is a monic polynomial of degree  $n$  and consider the left  $R$ -module  $V = R/\bullet(f)$ . Recall from Section 2.4,  $V$  is also an  $\mathbb{F}_{q^s}$ -vector space with basis  $\beta = \{\overline{1}, \overline{x}, \dots, \overline{x^{n-1}}\}$ . In Section 2.4, the isomorphism  $\psi_\beta$  is denoted by  $\mathbf{v}_f : R/\bullet(f) \rightarrow \mathbb{F}_{q^s}^n$  and is defined by

$$\overline{\sum_{i=0}^{n-1} g_i x^i} \mapsto (g_0, \dots, g_{n-1})$$

where  $\sum_{i=0}^{n-1} g_i x^i$  is the unique coset representative of degree less than  $n$ . The inverse of  $\mathbf{v}_f$  is denoted  $\mathbf{p}_f$ . We will use these notations in the next few results.

**Definition 3.1.14.** For  $V = R/\bullet(f)$ , let  $T : V \rightarrow V$  be the  $\sigma$ -SLM corresponding to left multiplication with  $x$ . The representative matrix of  $T$  in the basis  $\beta$  is called the companion matrix of  $f$  and is given by

$$C_f := \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ -f_0 & -f_1 & -f_2 & \dots & -f_{n-1} \end{pmatrix}.$$

Note the last line follows from  $x(\overline{x^{n-1}}) = \overline{x^n} = -\overline{\sum_{i=0}^{n-1} f_i x^i}$ .

The  $\sigma$ -SLM  $T_{C_f}$  on  $\mathbb{F}_{q^s}^n$  corresponding to  $T$  will be denoted as  $T_f$ . Now, the commutative diagram following Definition 3.1.6 becomes

$$\begin{array}{ccc} R/\bullet(f) & \xrightarrow{T} & R/\bullet(f) \\ \downarrow \mathfrak{v}_f & & \downarrow \mathfrak{v}_f \\ \mathbb{F}_{q^s}^n & \xrightarrow{T_f} & \mathbb{F}_{q^s}^n \end{array} .$$

We will make use of this diagram in Theorem 3.1.19 below.

**Corollary 3.1.15.** *Let  $f_1, f_2 \in R$  be monic of degree  $n$  with companion matrices  $C_1, C_2 \in \mathbb{F}_{q^s}^{n \times n}$ . Then  $R/\bullet(f_1) \cong R/\bullet(f_2)$  as  $R$ -modules if and only if there exists an invertible matrix  $B \in \mathbb{F}_{q^s}^{n \times n}$  such that  $C_1 B = \sigma(B) C_2$ .*

*Proof.* Given an invertible matrix  $B \in \mathbb{F}_{q^s}^{n \times n}$ , define  $\varphi : R/\bullet(f_1) \rightarrow R/\bullet(f_2)$  as  $\bar{g}\varphi := \mathfrak{p}_{f_2}(\mathfrak{v}_{f_1}(\bar{g})B)$  which is an  $\mathbb{F}_{q^s}$ -isomorphism. Then, by Proposition 3.1.13, we know  $B \in \mathbb{F}_{q^s}^{n \times n}$  satisfies  $C_1 B = \sigma(B) C_2$  if and only if  $\varphi$  is also  $R$ -linear.  $\square$

**Definition 3.1.16.**

1. The ideal  $\bullet(f)$  is two-sided in the ring

$$\text{Idl}(\bullet(f)) := \{g \in R : fg \in \bullet(f)\}$$

called the idealizer ring of  $\bullet(f)$ .

2. The quotient ring  $\text{Idl}(\bullet(f))/\bullet(f)$  is called the eigenring of  $\bullet(f)$ .

We will see next that the eigenring of  $\bullet(f)$  is isomorphic to  $\text{End}_R(R/\bullet(f))$ . Again, note that we must use the notation  $v\varphi := \varphi(v)$  for  $v \in V$  and  $\varphi \in \text{End}_R(V)$ .

**Proposition 3.1.17.** *Let  $V = R/\bullet(f)$ . Then we have*

$$\text{Idl}(\bullet(f))/\bullet(f) \cong \text{End}_R(V).$$

*Proof.* Consider the map

$$\eta : \text{Idl}(\bullet(f)) \rightarrow \text{End}_R(V) \quad \text{where } a \mapsto \psi_a$$

and  $\psi_a$  is given by  $\bar{g}\psi_a = \overline{ga}$ . Throughout let  $\bar{g}, \bar{h} \in V$ . First, we will check  $\psi_a$  is well defined. Assume  $\bar{g} = \bar{h}$ . Then  $g - h \in \bullet(f)$ , so  $g - h = tf$  for some  $t \in R$ . Now let  $a \in \text{Idl}(\bullet(f))$  so  $fa = \tilde{a}f$  for some  $\tilde{a} \in R$ . Then consider  $(g - h)a = tfa = t\tilde{a}f$ . Hence,  $\overline{ga} = \overline{ha}$  which gives  $\bar{g}\psi_a = \bar{h}\psi_a$  as needed.

Next, we will check  $\psi_a \in \text{End}_R(V)$ . For  $r \in R$ , we have

$$(r\bar{g} + \bar{h})\psi_a = \overline{rga + ha} = r\bar{g}a + \bar{h}a = r\bar{g}\psi_a + \bar{h}\psi_a.$$

Now, we must check  $\eta$  is a ring homomorphism. It is easy to check  $\eta$  is additive and maps  $\bar{1}$  to the identity map in  $\text{End}_R(V)$ . To check  $\eta$  is multiplicative, let  $a, b \in \text{Idl}(\bullet(f))$ . Then note

$$\bar{g}\psi_{ab} = \overline{gab} = \bar{g}a\psi_b = \bar{g}\psi_a\psi_b.$$

Hence,  $\eta(ab) = \eta(a)\eta(b)$  as needed. Next, we will show  $\ker(\eta) = \bullet(f)$ . For the forward containment, let  $a \in \ker(\eta)$  so that  $\psi_a$  is the zero map in  $\text{End}_R(V)$ . Then  $\bar{g}a = \bar{0}$ , so  $ga \in \bullet(f)$  for all  $g \in R$ . In particular, we get  $1a = a \in \bullet(f)$ . Conversely, assume  $a \in \bullet(f)$  so  $a = hf$  for some  $h \in R$ . Then, for any  $g \in R$ , we get  $\bar{g}\psi_a = \bar{g}a = \overline{ghf} = \bar{0}$ . This means  $\psi_a$  is the zero map in  $\text{End}_R(V)$ , so  $a \in \ker(\eta)$ . Therefore,  $\ker(\eta) = \bullet(f)$  as needed.

Lastly, we will show  $\eta$  is surjective. Let  $\psi \in \text{End}_R(V)$  and let  $\bar{b} := \bar{1}\psi$ . Note  $b \in \text{Idl}(\bullet(f))$  since

$$\bar{0} = \bar{0}\psi = \bar{f}\psi = (f\bar{1})\psi = f(\bar{1}\psi) = f\bar{b} = \bar{f}b.$$

Hence,  $fb \in \bullet(f)$  as needed. Therefore,  $\psi_b$  is well-defined. Then, for all  $\bar{g} \in V$ ,

$$\bar{g}\psi = g\bar{1}\psi = \bar{g}b = \bar{g}\psi_b.$$

Hence,  $\psi = \eta(b)$ . □

**Corollary 3.1.18.** *Let  $f \in R$  be a monic polynomial of degree  $n$  and let  $C = C_f$ . Then we have*

1. *As rings,  $\text{End}_R(R/\bullet(f))$  is isomorphic to  $C_f^\sigma := \{B \in \mathbb{F}_{q^s}^{n \times n} : CB = \sigma(B)C\}$ ,*
2.  *$\mathbb{F}_{q^s}^n$  has an  $(R, C_f^\sigma)$ -bimodule structure.*
3. *For  $g \in R$ , the map  $g(T_f) \in \text{End}(\mathbb{F}_{q^s}^n, +)$  is a right  $C_f^\sigma$ -linear map. In particular,  $\ker(g(T_f))$  is a right  $C_f^\sigma$ -submodule of  $\mathbb{F}_{q^s}^n$ .*

*Proof.*

1. Let  $V = R/\bullet(f)$ . This part follows directly from Proposition 3.1.13 since for any  $\varphi \in \text{End}_{\mathbb{F}_{q^s}}(V)$  with matrix representation  $B \in \mathbb{F}_{q^s}^{n \times n}$ , we know  $\varphi \in \text{End}_R(V)$  if and only if  $CB = \sigma(B)C$ . Moreover, the ring structure is preserved since it is a well-known fact that composition of linear maps is equivalent to multiplying the representative matrices.

2. By Proposition 3.1.2, the  $\sigma$ -SLM  $T_f : \mathbb{F}_{q^s}^n \rightarrow \mathbb{F}_{q^s}^n$  induces a left  $R$ -module structure on  $\mathbb{F}_{q^s}^n$ . Recall for  $g \in R$ , and  $v \in \mathbb{F}_{q^s}^n$ , we define  $g \cdot v := g(T_f)(v)$ . Furthermore, we have a right  $C_f^\sigma$ -module structure on  $\mathbb{F}_{q^s}^n$  where  $v \cdot B = vB$  using ordinary matrix-vector multiplication. Lastly, we need to check for  $B \in C_f^\sigma$  that  $(g \cdot v)B = g \cdot (vB)$ . Recall by Proposition 3.1.8  $T_f^i(v) = \sigma^i(v)N_i(C)$ . Then, the property  $CB = \sigma(B)C$ , leads to the fact  $T_f^i(v)B = T_f^i(vB)$ . Hence, for  $g = \sum_{i=0}^r g_i x^i$ , we get

$$(g \cdot v)B = \sum_{i=0}^r g_i T_f^i(v)B = \sum_{i=0}^r g_i T_f^i(vB) = g \cdot (vB).$$

3. For the third part, we need to show  $g(T_f) \in \text{End}(\mathbb{F}_{q^s}^n, +)$  is right  $C_f^\sigma$ -linear. This follows from the previous part since the property  $(g(T_f)(v))B = g(T_f)(vB)$  is equivalent to  $(g \cdot v)B = g \cdot (vB)$  which is given by the bimodule structure defined in part (2).  $\square$

Assume for the rest of this section that the standard basis for  $\mathbb{F}_{q^s}^n$  has indexing that starts at 0, so then  $e_0 = (1, 0, \dots, 0)$ ,  $e_1 = (0, 1, \dots, 0)$ , etc. This allows for easier mapping from the basis  $\{\bar{1}, \bar{x}, \dots, \bar{x}^{n-1}\}$  to the standard basis  $\{e_0, \dots, e_{n-1}\}$ .

**Theorem 3.1.19.** *Let  $f \in R$  be monic of degree  $n$  and consider  $R/\bullet(f)$ . Then, for  $g \in R$  we have*

1.  $\mathfrak{v}_f(\bar{g}) = g(T_f)(e_0)$ ,
2.  $\mathfrak{v}_f(\bar{gh}) = g(T_f)(\mathfrak{v}_f(\bar{h}))$  for any  $h \in R$ ,
3. there exists  $\mathbb{F}_q$ -isomorphisms between the  $\mathbb{F}_q$ -vector spaces

$$\ker(g(T_f)), \quad S := \{h \in R : \deg(h) < n, gh \in \bullet(f)\}, \quad \text{and } \text{Hom}_R(R/\bullet(g), R/\bullet(f)).$$

4.  $\text{Idl}(\bullet(f)) = \{g \in R : g(T_f)(e_0) \in \ker(f(T_f))\}$ .

*Proof.*

1. By the commutative diagram above, we know  $g(T_f) = \mathfrak{v}_f \circ g(T) \circ \mathfrak{p}_f$ . Hence,

$$g(T_f)(e_0) = (\mathfrak{v}_f \circ g(T) \circ \mathfrak{p}_f)(e_0) = \mathfrak{v}_f(g(T)(\bar{1})) = \mathfrak{v}_f(\bar{g}).$$

2. By part 1, for any  $h \in R$  we have

$$\mathfrak{v}_f(\bar{gh}) = (g(T_f) \circ h(T_f))(e_0) = g(T_f)(\mathfrak{v}_f(\bar{h})).$$



3. First, we will note that each of these sets are  $\mathbb{F}_q$ -vector spaces. The map  $g(T_f)$  is  $\mathbb{F}_q$ -linear, so  $\ker(g(T_f))$  is an  $\mathbb{F}_q$ -vector space. The set  $S$  is clearly additive,  $0 \in S$ , and for any  $\lambda \in \mathbb{F}_q$  and  $h \in S$ , we have  $g(\lambda h) = \lambda(gh) \in S$ . Thus, with the rest of the properties given by the ring structure on  $R$ , we know  $S$  is an  $\mathbb{F}_q$ -vector space. Lastly, since  $\text{Hom}_R(R/\bullet(g), R/\bullet(f))$  is an  $R$ -module and  $\mathbb{F}_q \subset R$ , we know that  $\text{Hom}_R(R/\bullet(g), R/\bullet(f))$  is an  $\mathbb{F}_q$ -vector space.

Now, consider  $\eta : \ker(g(T_f)) \rightarrow R$  where  $(v_0, \dots, v_{n-1}) \mapsto \sum_{i=0}^{n-1} v_i x^i$ . This map is clearly additive and injective. For any  $\lambda \in \mathbb{F}_q$  and  $u = (u_0, \dots, u_{n-1}) \in \ker(g(T_f))$ ,

$$\eta(\lambda u) = \sum_{i=0}^{n-1} \lambda u_i x^i = \lambda \sum_{i=0}^{n-1} u_i x^i = \lambda \eta(u).$$

Hence,  $\eta$  is  $\mathbb{F}_q$ -linear. We also claim the image of  $\eta$  is  $S$ . Indeed, let  $(v_0, \dots, v_{n-1}) \in \mathbb{F}_q^n$  and define  $h = \sum_{i=0}^{n-1} v_i x^i$ . Then

$$g(T_f)(v_0, \dots, v_{n-1}) = g(T_f)(\mathbf{v}_f(\bar{h})) = \mathbf{v}_f(\overline{gh}).$$

Thus,

$$v \in \ker(g(T_f)) \Leftrightarrow \mathbf{v}_f(\overline{gh}) = 0 \Leftrightarrow gh \in \bullet(f).$$

Next, consider the map  $\gamma : S \rightarrow \text{Hom}_R(R/\bullet(g), R/\bullet(f))$  where  $h \mapsto \psi_h$  given by

$$(a + \bullet(g))\psi_h = ah + \bullet(f).$$

To check  $\psi_h$  is a well-defined, let  $a + \bullet(g), b + \bullet(g) \in R/\bullet(g)$  where  $a + \bullet(g) = b + \bullet(g)$ . Then,  $a - b \in \bullet(g)$ , so  $(a - b) = tg$  for some  $t \in R$ . Now consider  $(a - b)h = tgh = tdf$  for some  $d \in R$  since  $h \in S$ . Hence,  $(a - b)h \in \bullet(f)$ , so  $(a + \bullet(g))\psi_h = (b + \bullet(g))\psi_h$  as needed.

One may easily check  $\psi_h$  is a  $R$ -linear, and that  $\gamma$  is additive and injective. Then, for  $\lambda \in \mathbb{F}_q$  and  $h \in S$ , we have  $\gamma(\lambda h) = \psi_{\lambda h} = \lambda(\psi_h) = \lambda\gamma(h)$ . Hence,  $\gamma$  is  $\mathbb{F}_q$ -linear. To see  $\gamma$  is also surjective, given  $\varphi \in \text{Hom}_R(R/\bullet(g), R/\bullet(f))$ , let  $h \in R$  of degree less than  $n$  such that  $h + \bullet(f) = (1 + \bullet(g))\varphi$ . Then, we claim  $\varphi = \psi_h$ . Indeed, for any  $a + \bullet(g) \in R/\bullet(g)$ ,

$$(a + \bullet(g))\varphi = a(1 + \bullet(g))\varphi = a(h + \bullet(f)) = ah + \bullet(f) = (a + \bullet(g))\psi_h.$$

Note that  $h \in S$  since  $0 + \bullet(f) = (0 + \bullet(g))\psi_h = gh + \bullet(f)$  which implies  $gh \in \bullet(f)$ .

4. By part 1 and 2, for  $g \in R$  we have

$$\mathbf{v}_f(\overline{fg}) = f(T_f)(\mathbf{v}_f(\bar{g})) = f(T_f)(g(T_f)(e_0)).$$

Hence,  $g \in \text{Idl}(\bullet(f))$  if and only if  $g(T_f)(e_0) \in \ker(f(T_f))$ . □

The following corollary makes use of the second part of Proposition 3.1.8 and Theorem 3.1.19.

**Corollary 3.1.20.** *Let  $f \in R$  be monic of degree  $n$ . Then, the following are equivalent.*

1.  $x \in \text{Idl}(\bullet(f))$
2. for any  $g \in R$ , we have  $g \in \bullet(f)$  if and only if  $g(C_f) = 0$
3.  $f(C_f) = 0$

*Proof.* Let  $\beta$  be the standard basis of  $\mathbb{F}_{q^s}^n$ .

(1)  $\Rightarrow$  (2) First note by Theorem 3.1.19(1), for  $i = 0, \dots, n-1$ , we have

$$e_i = \mathbf{v}_f(\overline{x^i}) = T_f^i(e_0).$$

Assume  $x \in \text{Idl}(\bullet(f))$  so that  $fx = tf$  for some  $t \in R$ . Then, inductively, for  $i = 0, \dots, n-1$ , we have  $fx^i = t^i f$ . Hence,  $x^i \in \text{Idl}(\bullet(f))$ . By Theorem 3.1.19(4), we know

$$0 = f(T_f)((T_f^i)(e_0)) = f(T_f)(e_i).$$

Now, suppose  $g \in \bullet(f)$  such that  $g = hf$  for some  $h \in R$ . Then, for  $i = 0, \dots, n-1$ ,

$$g(T_f)(e_i) = (hf)(T_f)(e_i) = h(T_f)(f(T_f)(e_i)) = h(T_f)(0) = 0.$$

Hence,  $0 = [g(T_f)]_\beta = g(C_f)$  as needed.

For the converse direction, assume  $g(C_f) = 0$ . Then,  $g(T_f)(e_i) = 0$  for all  $i = 0, \dots, n-1$ . In particular, by Theorem 3.1.19(1) we have  $0 = g(T_f)(e_0) = \mathbf{v}_f(\overline{g})$ . Hence,  $g \in \bullet(f)$  as needed.

(2)  $\Rightarrow$  (3) Since  $f \in \bullet(f)$ , (3) follows directly from (2).

(3)  $\Rightarrow$  (1) Assume  $f(C_f) = 0$ . Then, by Proposition 3.1.8  $[f(T_f)]_\beta = 0$ . In particular,  $f(T_f)(e_1) = 0$ . Hence,

$$(fx)(T_f)(e_0) = f(T_f)(T_f(e_0)) = f(T_f)(e_1) = 0.$$

This shows  $T_f(e_0) \in \ker(f(T_f))$ . Thus, by Theorem 3.1.19(4),  $x \in \text{Idl}(\bullet(f))$ .  $\square$

Recall from Definition 2.1.8 that for  $a \in \mathbb{F}_{q^s}$ , a conjugate of  $a$  is an element of the form  $a^c := \sigma(c)ac^{-1}$  for some  $c \in \mathbb{F}_{q^s}^*$ . Moreover, the conjugacy class of  $a$  is  $\Delta(a) := \{a^c : c \in \mathbb{F}_{q^s}^*\}$ . Now we will focus on the special case when  $V = R/\bullet(x-a)$  for some  $a \in \mathbb{F}_{q^s}$ . Recall from Example 3.1.10, the  $\sigma$ -SLM  $T_a : \mathbb{F}_{q^s} \rightarrow \mathbb{F}_{q^s}$  is given by  $\alpha \mapsto \sigma(\alpha)a$ . This map plays a large role in the following corollary.

**Corollary 3.1.21.** *Suppose  $a \in \mathbb{F}_{q^s}$  and  $g, h \in R$ .*

1. *The map  $\Lambda_a : R \rightarrow \text{End}(\mathbb{F}_{q^s}, +)$  defined by  $\Lambda_a(g) = g(T_a)$  is a ring homomorphism. Hence,*

$$(gh)(a) = g(T_a)(h(a)).$$

2. *Assume  $h(a) \neq 0$ , then we have,  $(gh)(a) = g(a^{h(a)})h(a)$  (This part is a restatement of Theorem 2.1.10 but is included here to be proven in this context). In particular, for  $b \in \mathbb{F}_{q^s}^*$  we have  $g(T_a)(b) = g(a^b)b$ .*

3. *If  $a \neq 0$ , then the field  $\text{Fix}_{\mathbb{F}_{q^s}}(\sigma)$  is ring isomorphic to  $\text{End}_R(\mathbb{F}_{q^s})$ .*

4. *Lastly, we have  $\ker(g(T_a)) = \{b \in \mathbb{F}_{q^s}^* : g(a^b) = 0\} \cup \{0\}$ .*

*Proof.* Let  $f = x - a$  and recall the map  $\mathbf{v}_f : R/\bullet(f) \rightarrow \mathbb{F}_{q^s}$  is an  $\mathbb{F}_{q^s}$ -isomorphism. Note that the companion matrix of  $f$  is the singleton matrix  $[a]$ . Hence, the  $\sigma$ -SLM  $T_f$  is the map  $T_a$  described above. By definition for any  $g \in R$ , we know  $\mathbf{v}_f(\bar{g}) = g(a)$ .

1. By Proposition 3.1.2,  $\Lambda_a$  is a ring homomorphism. Moreover, by Theorem 3.1.19(2),

$$(gh)(a) = \mathbf{v}_f(\overline{gh}) = g(T_a)(h(a)).$$

2. First we will show  $g(T_a)(b) = g(a^b)b$  for any  $b \in \mathbb{F}_{q^s}^*$ . Note that

$$(x - a^b)b = xb - \sigma(b)a = \sigma(b)(x - a).$$

Hence,  $\bullet((x - a^b)b) \subset \bullet(x - a)$ . Now, by definition,  $g - g(a^b) \in \bullet(x - a^b)$ , so clearly

$$gb - g(a^b)b = (g - g(a^b))b \in \bullet((x - a^b)b) \subset \bullet(x - a).$$

Then, we know  $\mathbf{v}_f(\overline{gb}) = g(a^b)b$ . Thus, by Theorem 3.1.19(2), we have

$$g(T_a)(b) = \mathbf{v}_f(\overline{gb}) = g(a^b)b.$$

For the other part, by Theorem 3.1.19(1) and setting  $b = h(a)$  in the above work, we have

$$(gh)(a) = g(T_a)(h(a)) = g(a^{h(a)})h(a).$$

3. From 3.1.18 with  $n = 1$ , we have

$$\text{End}_R(R/\bullet(x - a)) \cong \{b \in \mathbb{F}_{q^s} : ab = \sigma(b)a\} = \text{Fix}_{\mathbb{F}_{q^s}}(\sigma).$$

4. This part follows directly from part (2). □

Recall for  $f \in R$ , the set of right roots of  $f$  is denoted  $V(f)$ . So, for any  $a \notin V(f)$ , we set  $\Phi_f(a) := a^{f(a)}$ . With these notations, we have the following.

**Proposition 3.1.22.** *Let  $f, g \in R$  such that  $\gcd(f, g) = 1$  and let  $l = \text{lcm}(f, g)$ . Also let  $f', g' \in R$  be such that  $l = f'g = g'f$  and let  $T$  be a  $\sigma$ -SLM of any  $R$ -module  $V$ . Then,*

1.  $R/\bullet(f) \cong R/\bullet(f')$ ,
2.  $g(T)(\ker(f(T))) = \ker(f'(T))$ ,
3.  $\ker(l(T)) = \ker(f(T)) \oplus \ker(g(T))$ ,
4.  $V(f') = \Phi_g(V(f))$ .

*Proof.*

1. Note by the degree formula (2.1.4) we have  $\deg(f) + \deg(g) = \deg(1) + \deg(l)$ . Hence,  $\deg(f) = \deg(f')$ . Consider the map  $\varphi : R/\bullet(f') \rightarrow R/\bullet(f)$  where  $h + \bullet(f') \mapsto hg + \bullet(f)$ . To see this map is well defined let  $\bar{h}_1 = \bar{h}_2 \in R/\bullet(f')$  so that  $h_1 - h_2 = tf'$  for some  $t \in R$ . Then we have

$$(h_1 - h_2)g = tf'g = tg'f \in \bullet(f).$$

So,  $\varphi(\bar{h}_1) = \varphi(\bar{h}_2)$  as needed. This map is clearly  $R$ -linear, so to see it is injective consider  $\bar{h} \in \ker \varphi$ . Then we know  $hg = tf$  for some  $t$ , so in fact  $hg \in \bullet(l)$ . Then, for some  $k \in R$ , we have  $hg = kl = kf'g$ , which forces  $h = kf'$  as needed. Lastly, we know the map  $\varphi$  is surjective since  $R/\bullet(f)$  and  $R/\bullet(f')$  have the same cardinality.

2. We will prove this part by showing a number of subset containments. First let  $v \in \ker f(T)$ , and consider

$$f'(T)g(T)(v) = (f'g)(T)(v) = (g'f)(T)(v) = g'(T)f(T)(v) = 0.$$

Hence,

$$g(T)(\ker f(T)) \subset \ker f'(T).$$

Next, assume  $h + \bullet(f') = \varphi^{-1}(1 + \bullet(f))$ . Then

$$0 = \varphi^{-1}(f + \bullet(f)) = f\varphi^{-1}(1 + \bullet(f)) = fh + \bullet(f')$$

which gives  $fh \in \bullet(f')$ . Similar to the reasoning above, let  $v \in \ker(f'(T))$ . Then, for some  $k \in R$ , we have

$$(fh)(T)(v) = (kf')(T)(v) = 0.$$

Hence,

$$h(T)(\ker f'(T)) \subset \ker f(T).$$

Moreover, note that

$$gh + \bullet(f') = g\varphi^{-1}(1 + \bullet(f)) = \varphi^{-1}(g + \bullet(f)) = 1 + \bullet(f').$$

So  $gh - 1 \in \bullet(f')$ . This implies

$$(gh)(T)(\ker f'(T)) = \text{id}(\ker f'(T)) = \ker f'(T).$$

Therefore, in total we have

$$\ker f'(T) = (gh)(T)(\ker f'(T)) \subseteq g(T)(\ker f(T)) \subseteq \ker f'(T).$$

3. Clearly  $\ker g(T) + \ker f(T) \subseteq \ker l(T)$ . So, let  $v \in \ker l(T)$  and note

$$(f'g)(T)(v) = 0 = (g'f)(T)(v).$$

Hence,  $g(T)(v) \in \ker(f'(T)) = g(T)(\ker f(T))$  by part 2. So, there must be some  $w \in \ker f(T)$  where  $g(T)(v) = g(T)(w)$ . This implies  $v - w \in \ker g(T)$ . Therefore, we have  $v = v - w + w$  with  $v - w \in \ker g(T)$  and  $w \in \ker f(T)$  as needed. Lastly, we need to show  $\ker g(T) \cap \ker f(T) = \{0\}$ . Since  $\text{gcd}(f, g) = 1$ , there exists  $h, k \in R$  such that  $1 = hf + kg$ . Let  $v \in \ker f(T) \cap \ker g(T)$ . Then,

$$v = \text{id}(v) = (1)(T)(v) = (hf + kg)(T)(v) = (hf)(T)(v) + (kg)(T)(v) = 0.$$

4. Note that since  $\text{gcd}(f, g) = 1$ , we know  $g(a) \neq 0$  for any  $a \in V(f)$ . Hence, we have a well-defined set

$$\Phi_g(V(f)) = \{a^{g(a)} : a \in V(f)\}.$$

Now let  $a \in V(f)$  be arbitrary. By Corollary 3.1.21, we have

$$f'(a^{g(a)})g(a) = (f'g)(a) = (g'f)(a) = 0.$$

This shows  $\Phi_g(V(f)) \subset V(f')$ . To show the reverse containment, we need to show that for any  $a \in V(f')$  there is some  $b \in V(f)$  such that  $a = b^{g(b)}$ . By Example 3.1.10, we know  $0 = f'(a) = f'(T_a)(1)$ . So by part 2, we have  $1 \in \ker f'(T_a) = g(T_a) \ker f(T_a)$ . Therefore, there exists some nonzero  $c \in \ker f(T_a)$  such that  $g(T_a)(c) = 1$ . By Corollary 3.1.21,  $1 = g(T_a)(c) = g(a^c)c$ . Let  $b = a^c$  and note

$$b^{g(b)} = \sigma(g(b))b(g(b))^{-1} = \sigma(g(a^c)c) a (g(a^c)c)^{-1} = a.$$

Moreover,

$$f(b)c = f(a^c)c = f(T_a)(c) = 0.$$

Therefore,  $b \in V(f)$  as needed.  $\square$

### 3.2 Applications to W-Polynomials

Throughout this section, assume  $\sigma$  is the  $q$ -Frobenius. Recall the definition for the  $\sigma$ -minimal polynomial  $m_A$  for a set  $A \subset \mathbb{F}_{q^s}$  given in Definition 2.1.14. The following definition for W-polynomials is based on right roots. W-polynomials with left roots will be discussed in Section 4.2.

**Definition 3.2.1.** We say  $f$  is a W-polynomial if  $f$  is the minimal polynomial for its vanishing set, i.e.  $f = m_{V(f)}$ .

In the following equivalence for W-polynomials, we say  $g \in R$  is a factor of  $f \in R$  if  $f = f_1 g f_2$  for some  $f_1, f_2 \in R$ .

**Theorem 3.2.2.** [14, Prop. 3.4, Thm. 5.1] *Let  $f \in R$ . The following are equivalent.*

1.  $f$  is a W-polynomial.
2.  $f = m_\Delta$  for some  $\Delta \subset \mathbb{F}_{q^s}$ .
3.  $f$  splits completely and every monic factor of  $f$  is a W-polynomial.
4.  $f$  splits completely and every monic quadratic factor of  $f$  is a W-polynomial.
5.  $\text{rk}_\sigma(V(f)) = \deg(f)$ .

Now, let  $a \in \mathbb{F}_{q^s}^*$  and let  $T_a : \mathbb{F}_{q^s} \rightarrow \mathbb{F}_{q^s}$  be the  $\sigma$ -SLM given by  $\alpha \mapsto \sigma(\alpha)a$  as seen in Section 3.1. Then, by Proposition 3.1.2, the map  $T_a$  induces an  $R$ -module structure on  $\mathbb{F}_{q^s}$  where  $f \cdot b = f(T_a)(b)$  for any  $f \in R$  and  $b \in \mathbb{F}_{q^s}$ . Note also that  $f(T_a) \in \text{End}(\mathbb{F}_{q^s}, +)$  is an  $\mathbb{F}_q$ -linear map. We will assume  $\mathbb{F}_{q^s}$  has this  $R$ -module structure throughout the rest of this section.

**Proposition 3.2.3.** *If  $f$  is a W-polynomial, then*

$$\dim_{\mathbb{F}_q} \ker f(T_a) \leq \deg(f).$$

*Note that this is true for all  $a \in \mathbb{F}_{q^s}^*$ .*

*Proof.* Since  $f$  is a W-polynomial, we may assume  $f = (x - d_1) \dots (x - d_n)$  where  $d_i \in \mathbb{F}_{q^s}$  and  $n = \deg(f)$ . First we will show  $\dim_{\mathbb{F}_q} \ker(x - d_i)(T_a) \leq 1$  for all  $1 \leq i \leq n$ . Assume  $b \in \ker(x - d_i)(T_a)$ , so

$$0 = (x - d_i)(T_a)(b) = T_a(b) - d_i b = \sigma(b)a - d_i b.$$

Hence,  $d_i = a^b$ . So, for  $c \in \ker(x - d_i)(T_a)$ , we have  $a^c = d_i = a^b$ , which forces  $b^{q-1} = c^{q-1}$ . This means  $b = \lambda c$  for some  $\lambda \in \mathbb{F}_q$ . Therefore,  $\dim_{\mathbb{F}_q} \ker(x - d_i)(T_a) \leq 1$ . Now since

$$f(T_a) = (T_a - d_1 \text{id}) \circ \dots \circ (T_a - d_n \text{id})$$

we have

$$\dim_{\mathbb{F}_q} \ker f(T_a) \leq \sum_{i=1}^n \dim_{\mathbb{F}_q} \ker(x - d_i)(T_a) \leq n = \deg(f). \quad \square$$

The  $R$ -module structure placed on  $\mathbb{F}_{q^s}$  by the map  $T_a$  also implies the next result about  $R$ -linear maps involving  $\mathbb{F}_{q^s}$ .

**Lemma 3.2.4.** *Let  $p \in \mathbb{F}_{q^s}^*$ .*

1. *Assume there exists a nonzero  $R$ -linear map  $\Phi : R/\bullet(x-p) \rightarrow \mathbb{F}_{q^s}$ . Then, we have  $p = a^b$  where  $b = \Phi(1 + \bullet(x-p))$  and therefore  $\Phi(g + \bullet(x-p)) = g(T_a)(b)$  for all  $g \in R$ . Moreover,  $\Phi$  is an  $R$ -isomorphism.*
2. *Conversely, assume  $p = a^b$  for some  $b \in \mathbb{F}_{q^s}^*$ . Then, the map  $\Phi : R/\bullet(x-p) \rightarrow \mathbb{F}_{q^s}$  given by  $g + \bullet(x-p) \mapsto g(T_a)(b)$  is a well-defined  $R$ -linear isomorphism.*

*Proof.*

1. Note that  $p + \bullet(x-p) = x + \bullet(x-p)$ . Let  $b = \Phi(1 + \bullet(x-p))$  and note  $b$  is nonzero. Then

$$\begin{aligned}\Phi(p + \bullet(x-p)) &= p\Phi(1 + \bullet(x-p)) = pb \\ \Phi(x + \bullet(x-p)) &= x\Phi(1 + \bullet(x-p)) = x \cdot b = T_a(b) = \sigma(b)a.\end{aligned}$$

Since  $\Phi$  is well-defined, we must have  $pb = \sigma(b)a$ . Therefore,  $p = a^b$ . From the  $R$ -module structure on  $\mathbb{F}_{q^s}$ , for any  $g \in R$  we have

$$\Phi(g + \bullet(x-p)) = g\Phi(1 + \bullet(x-p)) = g \cdot b = g(T_a)(b).$$

Lastly, we will show  $\Phi$  is injective. Assume  $\Phi(f + \bullet(x-p)) = 0$  for some  $f \in R$ . Then, by Corollary 3.1.21,

$$0 = f\Phi(1 + \bullet(x-p)) = f \cdot b = f(T_a)(b) = f(a^b)b = f(p)b.$$

Since  $b \neq 0$ , we know  $f \in \bullet(x-p)$  as needed. Surjectivity follows immediately.

2. Now assume  $p = a^b$  for some  $b \in \mathbb{F}_{q^s}$ . Suppose for  $g, h \in R$  that  $g + \bullet(x-p) = h + \bullet(x-p)$ , so  $g - h = k(x-p)$  for some  $k \in R$ . Then consider

$$\begin{aligned}g(T_a)(b) - h(T_a)(b) &= (g - h)(T_a)(b) = k(x-p)(T_a)(b) \\ &= k(T_a)(T_a(b) - pb) = k(T_a)(\sigma(b)a - pb) = 0\end{aligned}$$

since  $p = \sigma(b)ab^{-1}$ . Therefore,  $\Phi(g + \bullet(x-p)) = \Phi(h + \bullet(x-p))$  as needed. Clearly,  $\Phi$  is additive since  $T_a$  is additive. Now assume  $g, h \in R$  are arbitrary. Then,

$$\begin{aligned}\Phi(gh + \bullet(x-p)) &= (gh)(T_a)(b) = g(T_a)(h(T_a)(b)) \\ &= g(T_a)(\Phi(h + \bullet(x-p))) = g \cdot \Phi(h + \bullet(x-p)).\end{aligned}$$

Hence,  $\Phi$  is an  $R$ -linear map. The fact that  $\Phi$  is an  $R$ -isomorphism follows from the first part.  $\square$

Recall the definition for  $P$ -dependence which is given in Definition 2.1.14. The following result is stated in Chapter 1 as Corollary 2.1.28, but it is included here to be proven in this context.

**Proposition 3.2.5.** For  $a \in \mathbb{F}_{q^s}^*$  and  $i = 1, \dots, n$ , assume  $p_i = a^{b_i}$  with  $p_i, b_i \in \mathbb{F}_{q^s}^*$ . Then,  $\{p_1, \dots, p_n\}$  is a P-dependent set if and only if  $\{b_1, \dots, b_n\}$  is linearly dependent over  $\mathbb{F}_q$ .

*Proof.* For  $i = 1, \dots, n$ , let

$$\Phi_i : R/\bullet(x - p_i) \rightarrow \mathbb{F}_{q^s}$$

be the isomorphism  $\Phi_i(g + \bullet(x - p)) = g(T_a)(b_i)$  as in Lemma 3.2.4. By the lemma, we have  $b_i = \Phi_i(1 + \bullet(x - p_i))$ .

( $\Leftarrow$ ) Assume  $b_n = \sum_{i=1}^{n-1} \lambda_i b_i$  for  $\lambda_i \in \mathbb{F}_q$ , and let

$$l' = \text{lcm}\{x - p_i : 1 \leq i \leq n-1\}.$$

Now consider

$$\begin{aligned} \Phi_n(l' + \bullet(x - p_n)) &= l' \cdot \Phi_n(1 + \bullet(x - p_n)) = l' \cdot b_n = l' \cdot \sum_{i=1}^{n-1} \lambda_i b_i \\ &= l'(T_a) \left( \sum_{i=1}^{n-1} \lambda_i b_i \right) = \sum_{i=1}^{n-1} \lambda_i l'(T_a)(b_i) = \sum_{i=1}^{n-1} \lambda_i l' \cdot \Phi_i(1 + \bullet(x - p_i)) \\ &= \sum_{i=1}^{n-1} \lambda_i \Phi_i(l' + \bullet(x - p_i)) = 0. \end{aligned}$$

Therefore,  $l'(p_n) = 0$  by injectivity. Now, since  $\deg(l') \leq n-1$ , we know  $\{p_1, \dots, p_n\}$  is a P-dependent set.

( $\Rightarrow$ ) Conversely, assume  $\{p_1, \dots, p_n\}$  is a P-dependent set and let

$$l = \text{lcm}\{x - p_i : 1 \leq i \leq n\}.$$

Note, by definition of a P-dependent set we know  $\deg(l) \leq n-1$ . Now consider

$$l(T_a)(b_i) = l \cdot b_i = l \cdot \Phi_i(1 + \bullet(x - p_i)) = \Phi_i(l + \bullet(x - p_i)) = 0.$$

Hence,  $\{b_1, \dots, b_n\} \subset \ker l(T_a)$ . By Proposition 3.2.3, since  $l$  is a W-polynomial,  $\dim_{\mathbb{F}_q} \ker l(T_a) \leq \deg(l) \leq n-1$ . Therefore,  $\{b_1, \dots, b_n\}$  is linearly dependent over  $\mathbb{F}_q$ .  $\square$

Assume  $0 = a_0, a_1, \dots, a_{q-1}$  are representatives of the  $\sigma$ -conjugacy classes of  $\mathbb{F}_{q^s}$ . Let

$$C_j = \{b \in \mathbb{F}_{q^s}^* : \sigma(b)a_j = a_j b\}.$$

Then, clearly  $C_0 = \mathbb{F}_{q^s}$  and  $C_j = \mathbb{F}_q$  for  $j \geq 1$ . Also note that  $T_{a_0}$  is the zero map, so  $\ker(T_{a_0}) = \mathbb{F}_{q^s}$ .



**Proposition 3.2.6.** *Let  $f \in R$  and let  $\Delta_j = V(f) \cap \Delta(a_j)$ , for  $j \in \{0, \dots, q-1\}$ . Then, if  $\Delta_j \neq \emptyset$ , we have*

$$\dim_{C_j} \ker f(T_{a_j}) = \text{rk}_\sigma(\Delta_j).$$

*Proof.* First note if  $\Delta_0 \neq \emptyset$ , then  $0 \in V(f)$ , so  $f$  must have no constant term. Hence,

$$\text{rk}_\sigma(\Delta_0) = 1 = \dim_{\mathbb{F}_{q^s}}(\mathbb{F}_{q^s}) = \dim_{\mathbb{F}_{q^s}} \ker f(T_{a_0})$$

as needed. Now fix  $j \geq 1$  and assume  $\Delta_j \neq \emptyset$ .

( $\geq$ ) Let  $\{p_1, \dots, p_n\}$  be a P-basis for  $\Delta_j$ . Note that for  $i = 1, \dots, n$  we have  $f(p_i) = 0$  and  $p_i = a_j^{b_i}$  for some  $b_i \in \mathbb{F}_{q^s}^*$ . By Proposition 3.2.5, we know  $\{b_1, \dots, b_n\}$  is linearly independent over  $\mathbb{F}_q$ . Moreover, by Corollary 3.1.21,

$$f(T_{a_j})(b_i) = f(a_j^{b_i})b_i = f(p_i)b_i = 0.$$

Therefore,  $\{b_1, \dots, b_n\} \subset \ker(f(T_{a_j}))$ , so  $\dim_{\mathbb{F}_q} \ker f(T_{a_j}) \geq n$ .

( $\leq$ ) Conversely, assume  $\{c_1, \dots, c_r\}$  is a basis for  $\ker f(T_{a_j})$  over  $\mathbb{F}_q$ . Then for  $i = 1, \dots, r$ ,

$$0 = f(T_{a_j})(c_i) = f(a_j^{c_i})c_i.$$

Hence,  $a_j^{c_i} \in \Delta_j$  since  $c_i \neq 0$ . Also, by Proposition 3.2.5, we know  $\{a_j^{c_1}, \dots, a_j^{c_r}\}$  are P-independent. Thus,  $r \leq \text{rk}_\sigma(\Delta_j)$ .  $\square$

Now for the main result.

**Theorem 3.2.7.** *Let  $f \in R$  be of degree  $n$ . Then*

1.  *$f$  has roots in at most  $n$   $\sigma$ -conjugacy classes say  $\{\Delta(a_{j_1}), \dots, \Delta(a_{j_r})\}$  with  $r \leq n$  (See Theorem 2.1.12).*
2.  $\sum_{i=1}^r \dim_{C_{j_i}} \ker(f(T_{a_{j_i}})) \leq n$ .

*Proof.*

1. We will show this part by induction on  $n$ . For the base case, assume  $n = 1$ , so then  $f = x - a$  for some  $a \in \mathbb{F}_{q^s}$ . Then clearly  $f$  has one root in one conjugacy class  $\Delta(a)$ .

Now, assume  $f \in R$  has degree  $n$  and let  $a \in \mathbb{F}_{q^s}$  be a root of  $f$ . Then  $f = g(x - a)$  for some  $g \in R$ . By the inductive hypothesis,  $g$  has roots in at most  $n - 1$   $\sigma$ -conjugacy classes, say  $\{\Delta(d_1), \dots, \Delta(d_r)\}$  with  $r \leq n - 1$ . By Theorem 2.1.10, if  $d \neq a$  is a root of  $f$ , then  $d^{d-a}$  is a root of  $g$ . Hence, all roots of  $f$  fall into at most  $n$  conjugacy classes

$$\{\Delta(d_1), \dots, \Delta(d_r), \Delta(a)\}.$$

2. Assume the roots of  $f$  fall into the  $\sigma$ -conjugacy classes  $\Delta(a_{j_1}), \dots, \Delta(a_{j_r})$ . Then, we can write  $V(f) = \cup_{i=1}^r \Delta_i$  where  $\Delta_i = V(f) \cap \Delta(a_{j_i})$ . Hence, by Theorem 2.1.18 and Proposition 3.2.6 we have

$$\mathrm{rk}_\sigma(V(f)) = \sum_{i=1}^r \mathrm{rk}_\sigma(\Delta_i) = \sum_{i=1}^r \dim_{C_{j_i}} \ker f(T_{a_{j_i}}).$$

Since  $m_{V(f)}$  right divides  $f$  we have  $\mathrm{rk}_\sigma(V(f)) \leq n$  and so the statement follows.  $\square$

**Remark 3.2.8.** Equality in the theorem above holds if and only if  $f = m_A$  for some  $A \subset \mathbb{F}_{q^s}$  i.e. if  $f$  is a W-polynomial.

Note that in [16], the author assumes  $q$  is prime in the following theorem. This assumption is not necessary as we will see in the subsequent proof.

**Theorem 3.2.9.** Consider  $R = \mathbb{F}_{q^s}[x; \sigma]$  where  $\sigma$  is the  $q$ -Frobenius.

1. We have  $l' := \mathrm{lcm}(x - a : a \in \mathbb{F}_{q^s}^*) = x^{(q-1)s} - 1$ .
2. We also have  $l := \mathrm{lcm}(x - a : a \in \mathbb{F}_{q^s}) = x^{(q-1)s+1} - x$ .
3. The ideal generated by  $l$  is two-sided.

*Proof.*

1. Let  $H = x^{(q-1)s} - 1$ . Recall from 2.2.8, we know  $N_{(q-1)s}(b) = 1$  for all  $b \in \mathbb{F}_{q^s}^*$ . Hence, for any  $b \in \mathbb{F}_{q^s}^*$ , we have  $H(b) = 0$ . Now, it suffices to show  $\deg(l') \geq (q-1)s$ . Let  $a_1, \dots, a_{q-1}$  be representatives of the nonzero  $\sigma$ -conjugacy classes of  $\mathbb{F}_{q^s}$ . By Corollary 3.1.21,

$$l'(T_{a_i})(b) = l'(a_i^b)b = 0$$

for all  $b \in \mathbb{F}_{q^s}^*$ . This shows  $\ker(l'(T_{a_i})) = \mathbb{F}_{q^s}$  for all  $i = 1, \dots, q-1$ . Therefore, by Theorem 3.2.7 we have

$$\deg(l') \geq \sum_{i=1}^{q-1} \dim_{C_i} \ker(l'(T_{a_i})) = \sum_{i=1}^{q-1} \dim_{\mathbb{F}_q}(\mathbb{F}_{q^s}) = (q-1)s.$$

Thus, we know  $l' = H$ .

2. Let  $G = x^{(q-1)s+1} - x$  and note that  $xl' = l'x$ . Hence,  $G$  annihilates any  $b \in \mathbb{F}_{q^s}$  since  $l'$  is a right divisor of  $G$  and clearly  $G(0) = 0$ . Since  $l'(0) \neq 0$ , we know  $\deg(l) > \deg(l')$ . Therefore,  $\deg(l) \geq (q-1)s + 1$ , so in fact  $l = G$ .
3. Since  $\sigma^s = \mathrm{id}$  we know  $la = \sigma(a)l$  for all  $a \in \mathbb{F}_{q^s}$ , and clearly  $xl = lx$ . Therefore,  $\bullet(l) = (l)\bullet$ .  $\square$

## Chapter 4 W-Polynomials

In a skew-polynomial ring, the skew-multiplication rule allows polynomials to pick up more roots than suggested by its degree. Hence, it has become of interest to classify when a polynomial is a W-polynomial, i.e. the minimal polynomial of its set of roots (see Definition 3.2.1). In this chapter, we will discuss when polynomials of the form  $x^n - a \in \mathbb{F}_{q^s}[x; \sigma]$  are W-polynomials. We will show that any right W-polynomial is also a left W-polynomial. Lastly, we will show any W-polynomial will remain a W-polynomial when considered over a field extension.

### 4.1 Vanishing set of $x^n - a$

There is a special kind of  $(\sigma, f)$ -skew-cyclic code called a  $(\sigma, a)$ -skew-constacyclic code where the modulus  $f$  is taken to be  $x^n - a \in \mathbb{F}_{q^s}[x; \sigma]$ . This type of skew-cyclic code was first introduced by [3] and later studied in detail by [4], [5], and [7]. In this section, we will identify the minimal polynomial for  $V(x^n - a)$ , thereby classifying for what  $n \in \mathbb{N}$  and  $a \in \mathbb{F}_{q^s}^*$ , the polynomial  $x^n - a$  is a W-polynomial.

Throughout, let  $\omega$  be a primitive element of  $\mathbb{F}_{q^s}$ , let  $\sigma$  be the  $q$ -Frobenius and let  $n \in \mathbb{N}$  where  $n \leq (q-1)s$ . Note that we have this upper bound on  $n$  since all minimal polynomials of subsets of  $\mathbb{F}_{q^s}^*$  have degree at most  $(q-1)s$  by Theorem 2.1.19.

Recall the definition for the  $(r, n)$ -th norm function given in 2.1.6. Note that  $N_n^r$  induces a group homomorphism on  $\mathbb{F}_{q^s}^*$ . Since  $\mathbb{F}_{q^s}^*$  is a cyclic group, we know  $\text{im}(N_n)$  and  $\text{ker}(N_n)$  are cyclic. This is made precise in the following proposition. For the rest of this section assume

$$d = \gcd(q^s - 1, \frac{q^n - 1}{q - 1}), \quad d' = \gcd(s(q-1), n), \quad \text{and} \quad \delta = \gcd(q^s - 1, \frac{q^{d'} - 1}{q - 1}). \quad (4.1)$$

**Proposition 4.1.1.** *The image and kernel of the  $n$ -th norm function are given by*

$$\text{im}(N_n) = \langle \omega^d \rangle \quad \text{and} \quad \text{ker}(N_n) = \langle \omega^{\frac{q^s - 1}{d}} \rangle.$$

*Proof.* Since  $\mathbb{F}_{q^s}^* = \langle \omega \rangle$ , clearly  $\text{im}(N_n) = \langle \omega^{\frac{q^n - 1}{q - 1}} \rangle$ . We also know that  $\langle \omega^{\frac{q^n - 1}{q - 1}} \rangle \subseteq \langle \omega^d \rangle$  since  $d$  divides  $\frac{q^n - 1}{q - 1}$ . Conversely, let  $u, v \in \mathbb{Z}$  where  $d = u(q^s - 1) + v(\frac{q^n - 1}{q - 1})$ . Then,

$$\omega^d = \omega^{u(q^s - 1) + v(\frac{q^n - 1}{q - 1})} = \omega^{v(\frac{q^n - 1}{q - 1})}.$$

Hence,  $\langle \omega^d \rangle \subseteq \langle \omega^{\frac{q^n - 1}{q - 1}} \rangle$ . Therefore,  $\text{im}(N_n) = \langle \omega^d \rangle$ .

The first isomorphism theorem for groups tells us,  $\text{ker}(N_n) = \langle \omega^{|\text{im}(N_n)|} \rangle$ . Hence, we have  $\text{ker}(N_n) = \langle \omega^{\frac{q^s - 1}{d}} \rangle$  as needed.  $\square$

Before we work more with the kernel and image of  $N_n$ , it is useful to have the following results on gcds. The first of which follows from elementary number theory.

**Lemma 4.1.2.** *Let  $\alpha, \beta, \gamma \in \mathbb{Z}$ . If  $\gamma \mid \gcd(\alpha, \beta)$ , then*

$$\gcd\left(\frac{\alpha}{\gamma}, \frac{\beta}{\gamma}\right) = \frac{\gcd(\alpha, \beta)}{\gamma}.$$

**Lemma 4.1.3.** *For  $d, \delta$  given in Equation 4.1, we have  $\delta = d$ .*

*Proof.* By Lemmas 2.2.14 and 4.1.2,

$$\frac{q^{d'} - 1}{q - 1} = \gcd\left(\frac{q^{(q-1)^s} - 1}{q - 1}, \frac{q^n - 1}{q - 1}\right).$$

Hence, for some  $u, v \in \mathbb{Z}$ ,

$$\begin{aligned} \frac{q^{d'} - 1}{q - 1} &= u \left( \frac{q^{(q-1)^s} - 1}{q - 1} \right) + v \left( \frac{q^n - 1}{q - 1} \right) \\ &= u \left( \frac{\sum_{i=0}^{q-2} (q^{is} - 1)}{q - 1} + \frac{q - 1}{q - 1} \right) (q^s - 1) + v \left( \frac{q^n - 1}{q - 1} \right) \\ &= dt \end{aligned}$$

for some  $t \in \mathbb{Z}$ . Thus, since  $d$  also divides  $q^s - 1$ , we know  $d$  divides  $\delta$ .

For some  $\nu, \zeta \in \mathbb{Z}$ , we have

$$\begin{aligned} d &= \nu(q^s - 1) + \zeta \left( \frac{q^n - 1}{q - 1} \right) \\ &= \nu(q^s - 1) + \zeta \left( \sum_{i=0}^{\frac{n}{d'} - 1} q^{d'i} \right) \left( \frac{q^{d'} - 1}{q - 1} \right) \\ &= k\delta \end{aligned}$$

for some  $k \in \mathbb{Z}$ . Therefore,  $\delta = d$ . □

The subsequent corollary follows immediately from Proposition 4.1.1 and Lemma 4.1.3.

**Corollary 4.1.4.** *For  $d'$  given in Equation (4.1),*

$$\ker(N_n) = \ker(N_{d'}).$$

**Lemma 4.1.5.** *The vanishing set of  $x^n - a$  is nonempty if and only if  $a \in \text{im}(N_n)$ .*

*Proof.* Let  $f = x^n - a$ . Recall from Proposition 2.1.7 that  $f(c) = N_n(c) - a$  for any  $c \in \mathbb{F}_{q^s}$ .  $\square$

**Remark 4.1.6.** Assume  $a = N_n(c)$  for some  $c \in \mathbb{F}_{q^s}^*$ . Then, the vanishing set of  $x^n - a$  is the coset of  $\ker(N_n)$  containing  $c$ . Indeed, for any  $b \in \mathbb{F}_{q^s}$ , we have  $b \in V(x^n - a)$  if and only if  $N_n(b) = N_n(c)$ . This is equivalent to  $bc^{-1} \in \ker(N_n)$ . Hence,  $b \in V(x^n - a)$  if and only if  $b$  and  $c$  are in the same coset of  $\ker(N_n)$ . Therefore,  $V(x^n - a)$  is precisely the coset of  $\ker(N_n)$  containing  $c$ .

In the following proposition, we will see that  $x^n - a$  factors in a nice way.

**Proposition 4.1.7.** *Assume  $n = \alpha\beta$ , and  $a = N_n(c)$  for some  $c \in \mathbb{F}_{q^s}^*$ . Define  $\hat{a} = N_\beta(c)$ . Then*

$$x^n - a = \left( \sum_{j=0}^{\alpha-1} \left( \prod_{i=j+1}^{\alpha-1} (\hat{a})^{q^{i\beta}} \right) x^{j\beta} \right) (x^\beta - \hat{a}).$$

*Proof.* If we carry out the multiplication on the right-hand side of the above identity, with the aid of Lemma 2.2.1 we get the following.

$$\begin{aligned} \text{RHS} &= \sum_{j=0}^{\alpha-1} \left( \prod_{i=j+1}^{\alpha-1} (\hat{a})^{q^{i\beta}} \right) x^{(j+1)\beta} - \sum_{j=0}^{\alpha-1} \left( \prod_{i=j}^{\alpha-1} (\hat{a})^{q^{i\beta}} \right) x^{j\beta} \\ &= \sum_{j=1}^{\alpha} \left( \prod_{i=j}^{\alpha-1} (\hat{a})^{q^{i\beta}} \right) x^{j\beta} - \sum_{j=0}^{\alpha-1} \left( \prod_{i=j}^{\alpha-1} (\hat{a})^{q^{i\beta}} \right) x^{j\beta} \\ &= x^{\alpha\beta} + \sum_{j=1}^{\alpha-1} \left( \prod_{i=j}^{\alpha-1} (\hat{a})^{q^{i\beta}} \right) x^{j\beta} - \left( \sum_{j=1}^{\alpha-1} \left( \prod_{i=j}^{\alpha-1} (\hat{a})^{q^{i\beta}} \right) x^{j\beta} + \prod_{i=0}^{\alpha-1} (\hat{a})^{q^{i\beta}} \right) \\ &= x^{\alpha\beta} - \prod_{i=0}^{\alpha-1} (\hat{a})^{q^{i\beta}} \\ &= x^{\alpha\beta} - N_\alpha^\beta(\hat{a}) \\ &= x^{\alpha\beta} - N_\alpha^\beta(N_\beta(c)) \\ &= x^{\alpha\beta} - N_n(c) \\ &= x^n - a. \end{aligned} \quad \square$$

**Corollary 4.1.8.** *Assume  $a = N_n(c)$  and let  $\hat{a} = N_\beta(c)$ . Then*

1.  $(x^{d'} - \hat{a})|_r (x^n - a)$ ,

$$2. (x^{d'} - \hat{a})|_r (x^{(q-1)s} - 1).$$

*Proof.* Part 1 follows immediately from Proposition 4.1.7. For part 2, recall from Proposition 2.2.8 that  $N_{(q-1)s}(c) = 1$  for any  $c \in \mathbb{F}_{q^s}^*$ . Hence, part 2 also follows immediately from Proposition 4.1.7 if we take  $a = 1$ .  $\square$

Now we have the main result of the section.

**Theorem 4.1.9.** *Let  $f = x^n - a \in \mathbb{F}_{q^s}[x; \sigma]$ . Assume  $a \in \text{im}(N_n)$  so  $a = N_n(c)$  for some  $c \in \mathbb{F}_{q^s}^*$ . Let  $\hat{a} = N_{d'}(c)$ . Then*

$$x^{d'} - \hat{a} = m_{V(f)},$$

where as before  $m_{V(f)}$  is the minimal polynomial of  $V(f)$ .

*Proof.* Let  $g = x^{d'} - \hat{a}$ . By Corollary 4.1.8(2), Theorem 3.2.2, and Theorem 3.2.9 we know  $g$  is a W-polynomial. By Corollary 4.1.8(1) and Corollary 2.1.15, we have  $V(g) \subseteq V(f)$ . Lastly, we need to show  $V(f) \subseteq V(g)$ . Let  $b \in V(f)$ . Then,  $N_n(b) = a = N_n(c)$ . Hence,  $bc^{-1} \in \ker(N_n)$ . By Corollary 4.1.4, we also have  $bc^{-1} \in \ker(N_{d'})$ . Therefore,  $N_{d'}(b) = N_{d'}(c) = \hat{a}$ . So,  $b \in V(g)$  as needed.  $\square$

As a corollary, we know the  $\sigma$ -rank of  $V(x^n - a)$  and we are able to classify exactly when  $x^n - a$  is a W-polynomial.

**Corollary 4.1.10.**

1. *If  $V(x^n - a) \neq \emptyset$ , then  $\text{rk}_\sigma(V(x^n - a)) = \gcd(s(q-1), n)$ .*
2. *The polynomial  $x^n - a$  is a W-polynomial if and only if  $n$  divides  $(q-1)s$  and  $a \in \text{im}(N_n)$ .*

In [12], the author states that  $x^s - a$  is a W-polynomial if and only if  $a \in \mathbb{F}_q^*$ . This is a special case of Corollary 4.1.10(1) since by Proposition 4.1.1,

$$\text{im}(N_s) = \langle \omega^{\frac{q^s-1}{q-1}} \rangle = \mathbb{F}_q^*.$$

This implies for any  $\gamma \in \mathbb{F}_{q^s}^*$ , we have  $N_s(\gamma) \in \mathbb{F}_q^*$ . Recall from Theorem 2.2.4 that  $x^s - N_s(\gamma)$  is the minimal polynomial of  $\Delta(\gamma)$ . Hence, we in fact have a one-to-one correspondence between the  $q-1$  non-zero elements of  $\mathbb{F}_q$ , and the  $q-1$  non-zero  $\sigma$ -conjugacy classes of  $\mathbb{F}_{q^s}$ .

**Remark 4.1.11.** Let  $\Delta$  be a nonzero  $\sigma$ -conjugacy class of  $\mathbb{F}_{q^s}$  with minimal polynomial  $m_\Delta = x^s - a$ . Recall from Remark 4.1.6 that  $V(m_\Delta)$  is a coset of  $\ker(N_s)$  and by Proposition 4.1.1 that  $\ker(N_s) = \langle \omega^{q-1} \rangle$ . Hence,  $|\ker(N_s)| = \frac{q^s-1}{q-1} = |\Delta|$ . This means  $V(m_\Delta) = \Delta$ . Any subset with this property is called full.

## 4.2 Left and Right W-Polynomials

By default, when we use the term W-polynomial, we assume we have a right W-polynomial, i.e. the right minimal polynomial of its set of right roots. A left W-polynomial is the left minimal polynomial for its set of left roots. In Theorem 3.2.2, we are given equivalent definitions for a W-polynomial involving its factors. In the theorem, we say  $g \in \mathbb{F}_{q^s}[x; \sigma]$  is a factor of  $f$  if  $f = f_1 g f_2$  for some  $f_1, f_2 \in \mathbb{F}_{q^s}[x; \sigma]$ . So, the term factor encompasses left, right, or middle factors. Hence, it is natural to ask if a right W-polynomial is also a left W-polynomial. In this section, we will use subscripts  $l$  and  $r$  to denote left or right vanishing sets, minimal polynomials, etc.

Throughout, assume  $\sigma$  is the  $q$ -Frobenius. From [14] we have the following useful fact about quadratic right or left W-polynomials.

**Proposition 4.2.1.** [14, Ex. 3.5] *A monic quadratic polynomial  $f \in \mathbb{F}_{q^s}[x; \sigma]$  is a right (left) W-polynomial if and only if  $f$  has at least two distinct right (left) roots.*

Now we will state what form any quadratic W-polynomial must have.

**Lemma 4.2.2.**

1. *If  $f \in \mathbb{F}_{q^s}[x; \sigma]$  is a quadratic right W-polynomial, then  $f = (x - b^{b-a})(x - a)$  for some  $a, b \in V_r(f)$  where  $a \neq b$ .*
2. *If  $f \in \mathbb{F}_{q^s}[x; \sigma]$  is a quadratic left W-polynomial, then  $f = (x - a)(x - \sigma^{-1}(b - a)b(b - a)^{-1})$  for some  $a, b \in V_l(f)$  where  $a \neq b$ .*

The lengthy expression in part 2 is a conjugate of  $b$  with respect to the automorphism  $\sigma^{-1}$ .

*Proof.*

1. Assume  $f$  is a quadratic right W-polynomial and let  $a, b \in V_r(f)$  where  $a \neq b$ . Note that  $a$  and  $b$  exist by Proposition 4.2.1. One can easily check the identity

$$(x - b^{b-a})(x - a) = (x - a^{a-b})(x - b). \quad (4.2)$$

Note that this result also follows directly from Theorem 2.1.10. Therefore,  $(x - b^{b-a})(x - a)$  must be the minimal polynomial of  $\{a, b\}$ . So, since  $f$  is a right W-polynomial, we have  $f = (x - b^{b-a})(x - a)$ .

2. This direction is analogous to part (1), since one can easily check the identity

$$(x - a)(x - \sigma^{-1}(b - a)b(b - a)^{-1}) = (x - b)(x - \sigma^{-1}(a - b)a(a - b)^{-1}). \quad (4.3)$$

Therefore, since  $f$  is a left W-polynomial, we have  $f = (x - a)(x - \sigma^{-1}(b - a)b(b - a)^{-1})$ .  $\square$

Before the main theorem, we need a lemma.

**Lemma 4.2.3.** *Let  $a, b \in \mathbb{F}_{q^s}$ . If  $a \neq b$ , then  $a^{a-b} \neq b^{b-a}$ . This is true for conjugation based on any  $\sigma \in \text{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$ .*

*Proof.* Let  $a, b \in \mathbb{F}_{q^s}$  where  $a \neq b$ . Then, we have

$$\sigma(a-b)a(a-b)^{-1} \neq \sigma(a-b)b(a-b)^{-1} = \sigma(b-a)b(b-a)^{-1}. \quad \square$$

Now we are able to state the main result of this section.

**Theorem 4.2.4.** *Let  $f \in \mathbb{F}_{q^s}[x; \sigma]$  be a monic of degree 2. Then  $f$  is a right W-polynomial if and only if it is a left W-polynomial.*

*Proof.* Assume  $f$  is a right W-Polynomial and let  $a, b \in V_r(f)$  be distinct. Then, by Lemma 4.2.2,  $f$  is of the form  $(x - a^{a-b})(x - b)$ . By Equation (4.2) and Lemma 4.2.3,  $f$  has  $a^{a-b}$  and  $b^{b-a}$  as distinct left roots. So, by Proposition 4.2.1,  $f$  must be a left W-polynomial. The converse direction can be shown via a symmetric argument that uses Equation (4.3) and applies Lemma 4.2.2 to  $\sigma^{-1}$ .  $\square$

As a result of the above theorem, we have the following.

**Corollary 4.2.5.** *Let  $f \in \mathbb{F}_{q^s}[x; \sigma]$ . Then  $f$  is a right W-polynomial if and only if it is a left W-polynomial.*

*Proof.* Recall from Theorem 3.2.2 that a polynomial  $f$  is a right (left) W-polynomial if and only if it splits completely, and every monic quadratic factor of  $f$  is a right (left) W-polynomial. By Theorem 4.2.4, a quadratic polynomial is left W-polynomial if and only if it is right W-polynomial. Hence, the result follows immediately.  $\square$

### 4.3 W-polynomials in a Field Extension

Consider fields  $\mathbb{F}_{q^{st}}/\mathbb{F}_{q^s}/\mathbb{F}_q$ , let  $\theta$  be the  $q$ -Frobenius of  $\mathbb{F}_{q^{st}}$  and let  $\sigma = \theta|_{\mathbb{F}_{q^s}}$ . In this section, we will see that a W-polynomial in  $\mathbb{F}_{q^s}[x; \sigma]$  will remain a W-polynomial when considered over a larger field  $\mathbb{F}_{q^{st}}$ , however the converse is not true.

Recall the vanishing set for a polynomial  $f$  is the set of roots of  $f$  (see Definition 2.1.14). For this section, we will use a subscript to indicate which field the roots are coming from, i.e. for  $f \in \mathbb{F}_{q^s}[x; \sigma]$ ,

$$\begin{aligned} V_{\mathbb{F}_{q^s}}(f) &= \{b \in \mathbb{F}_{q^s} : f(b) = 0\} \\ V_{\mathbb{F}_{q^{st}}}(f) &= \{b \in \mathbb{F}_{q^{st}} : f(b) = 0\} \end{aligned}$$



**Theorem 4.3.1.** *If  $f \in \mathbb{F}_{q^s}[x; \sigma]$  is a W-polynomial, then  $f$  is also a W-polynomial in  $\mathbb{F}_{q^{st}}[x; \theta]$ .*

*Proof.* Let  $f \in \mathbb{F}_{q^s}[x; \sigma]$  be a W-polynomial and let  $U = V_{\mathbb{F}_{q^s}}(f)$ , and  $V = V_{\mathbb{F}_{q^{st}}}(f)$ . Since  $f$  is a W-polynomial, we certainly have  $f = m_U$ . By Corollary 2.1.15, since  $U \subset V$ , we have  $f|_r m_V$ . By Theorem 2.1.10, since  $f$  vanishes on  $V$  we also have  $m_V|_r f$ . Therefore, we must have  $f = m_V$ , so  $f$  is a W-polynomial in  $\mathbb{F}_{q^{st}}[x; \theta]$ .  $\square$

**Remark 4.3.2.** Conversely, we may have a W-polynomial in  $\mathbb{F}_{q^{st}}[x; \theta]$  which is not a W-polynomial in  $\mathbb{F}_{q^s}[x; \sigma]$ . Recall from Corollary 4.1.10 that  $x^n - a \in \mathbb{F}_{q^s}[x; \sigma]$  is a W-polynomial if and only if  $n|(q-1)s$  and  $a \in \text{im}(N_n)$ . So, clearly if we let  $a \in N_n(\mathbb{F}_{q^s})$  and pick some  $n$  that divides  $(q-1)st$  but does not divide  $(q-1)s$ , then  $x^n - a$  is a W-polynomial in  $\mathbb{F}_{q^{st}}[x; \theta]$  but not  $\mathbb{F}_{q^s}[x; \sigma]$ .

For a polynomial  $f \in \mathbb{F}_{q^s}[x; \sigma]$ , we clearly have  $V_{\mathbb{F}_{q^s}}(f) \subseteq V_{\mathbb{F}_{q^{st}}}(f)$ . We will see next for certain W-polynomials we can have equality.

**Proposition 4.3.3.** *Let  $a = N_s(\gamma)$ ,  $\gamma \in \mathbb{F}_{q^s}^*$  and let  $f = x^s - a$ . Then we have  $V_{\mathbb{F}_{q^s}}(f) = V_{\mathbb{F}_{q^{st}}}(f)$ .*

*Proof.* Clearly we have  $V_{\mathbb{F}_{q^s}}(f) \subset V_{\mathbb{F}_{q^{st}}}(f)$ . To show the other direction, let  $\omega$  be a primitive element of  $\mathbb{F}_{q^{st}}$  and assume  $\gamma = \omega^{\frac{q^{st}-1}{q^s-1}k}$  for some  $k \in \mathbb{N}$ . Now let  $b \in V_{\mathbb{F}_{q^{st}}}(f)$  so that  $b\gamma^{-1} \in \ker(N_s)$ . Then by Proposition 4.1.1 applied to the group homomorphism  $N_s : \mathbb{F}_{q^{st}}^* \rightarrow \mathbb{F}_{q^s}^*$ , we have

$$b\gamma^{-1} = \omega^{\frac{q^{st}-1}{q^s-1}(q-1)j}$$

for some  $j \in \mathbb{N}$ . Therefore,

$$\begin{aligned} b &= \left( \omega^{\frac{q^{st}-1}{q^s-1}k} \right) \left( \omega^{\frac{q^{st}-1}{q^s-1}(q-1)j} \right) \\ &= \omega^{\left( \frac{q^{st}-1}{q^s-1} \right) (k+(q-1)j)} \in \mathbb{F}_{q^s}. \end{aligned}$$

So in fact  $b \in V_{\mathbb{F}_{q^s}}(f)$ . Thus,  $V_{\mathbb{F}_{q^{st}}}(f) = V_{\mathbb{F}_{q^s}}(f)$ .  $\square$

In general, W-polynomials in  $\mathbb{F}_{q^s}[x; \sigma]$  pick up roots when considered over  $\mathbb{F}_{q^{st}}$  as seen in the next example.

**Example 4.3.4.** Consider fields  $\mathbb{F}_{34}/\mathbb{F}_{32}/\mathbb{F}_3$  and assume  $\omega$  is a primitive element of  $\mathbb{F}_{34}$  which satisfies  $\omega^4 + 2\omega^3 + 2 = 0$ . Let  $f = x^2 - x + \omega^{30} \in \mathbb{F}_{32}[x; \sigma]$  and note that  $f$  is a W-polynomial over  $\mathbb{F}_{32}$ , and hence a W-polynomial over  $\mathbb{F}_{34}$ . When one

compares the vanishing set of  $f$  in  $\mathbb{F}_{3^2}$  with the vanishing set of  $f$  in  $\mathbb{F}_{3^4}$ , we see that  $f$  indeed has more roots in the larger field.

$$V_{\mathbb{F}_{3^2}}(f) = \{\omega^{50}, \omega^{60}\}$$

$$V_{\mathbb{F}_{3^4}}(f) = \{\omega^8, \omega^{50}, \omega^{60}, \omega^{72}\}$$

## Chapter 5 Skew Roos Bound and the Arithmetic Progression Construction

In [1], the authors showed a Roos-like bound for the minimum Hamming distance and rank distance of certain skew-cyclic codes. In their work, they take the modulus  $f = x^n - 1$ . We are able to show that the Roos-like bound on the minimum Hamming distance also holds for a more general modulus  $f = x^n - a$  with  $a \in N_n(\mathbb{F}_{q^s}^*)$ . If in fact  $a \in N_n(\mathbb{F}_q)$ , then it even holds for the minimum rank distance. In addition, we provide a counterexample illustrating that the last statement is not true if  $a \in N_n(\mathbb{F}_{q^s} \setminus \mathbb{F}_q)$ . Furthermore in [1], the authors provide conditions on the size of the set of roots of a generating polynomial which force the resulting code to be MRD. After some work, we are able to show that any root set of this size must be in the form of an arithmetic progression.

### 5.1 Skew Roos Bound

Throughout this section, let  $n = st$  and consider  $Z_n := (\{0, \dots, n-1\}, +)$  as an abelian group. For  $f = x^n - a$  with  $a \in N_n(\mathbb{F}_{q^s})$ , the skew-cyclic codes of interest for this section are submodules of the module

$$\mathbb{F}_{q^s}[x; \sigma] / \bullet (x^n - a) \cong \mathbb{F}_{q^s}^n.$$

**Definition 5.1.1.** Let  $\beta \in \mathbb{F}_{q^{st}}^*$  and  $\gamma \in \mathbb{F}_{q^s}^*$ . For  $g \in \mathbb{F}_{q^s}[x; \sigma]$ , the  $(\gamma, \beta)$ -defining set of  $g$  is

$$T_{\gamma, \beta}(g) := \{i \in Z_n : (x - \gamma\beta^{q^i}) \mid_r g\}.$$

Note that in particular  $\text{lcm}\{x - \gamma\beta^{q^i} : i \in T_{\gamma, \beta}(g)\} \mid_r g$ .

Considering  $(\gamma, \beta)$ -defining sets as a subsets of  $Z_n$  is well-defined because  $\beta^{q^{l+jn}} = \beta^{q^l}$  for any  $l \in \mathbb{N}$  and  $j \in \mathbb{Z}$ .

**Remark 5.1.2.** Let  $\gamma \in \mathbb{F}_{q^s}^*$  and  $\beta \in \mathbb{F}_{q^{st}}$  where  $\beta = \alpha^{q-1}$  for some normal element  $\alpha$  of  $\mathbb{F}_{q^{st}}$  (see Definition 2.2.3). Also let  $g \in \mathbb{F}_{q^s}[x; \sigma]$ .

1. The set  $T_{\gamma, \beta}(g)$  greatly depends on the choices of  $\gamma$  and  $\beta$ .
2. Let  $a = N_n(\gamma)$ . By Theorem 2.2.4, we know  $\gamma\beta^{q^i}$  is a root of  $x^n - a$  for  $i = 0, \dots, n-1$ . Hence, for any subset  $T \subset Z_n$ , we have

$$\text{lcm}\{x - \gamma\beta^{q^i} : i \in T\} \mid_r (x^n - a).$$

Now, we will state the Roos-like bound for the Hamming distance. The proof of the theorem presented here is the same as in [1] with small adjustments made to handle the more general modulus  $f$ . For the case where  $a = 1$ , see Theorem 13 in [1].

**Theorem 5.1.3** (Skew Roos Bound for the Hamming distance). *Let  $a \in N_n(\mathbb{F}_{q^s}^*)$  and  $f = x^n - a \in \mathbb{F}_{q^s}[x; \sigma]$ . Also let  $g \in \mathbb{F}_{q^s}[x; \sigma]$  be a right divisor of  $f$  and set  $C = \mathbf{v}_f(\bullet(\bar{g})) \subset \mathbb{F}_{q^s}^n$ . Suppose there exists parameters  $b, m, \delta, r, k_0, \dots, k_r \in \mathbb{N}_0$  such that*

1.  $m \neq 0$  and  $\gcd(m, n) = 1$ ,
2.  $k_0 < k_1 < \dots < k_r$  with  $k_r - k_0 \leq \delta + r - 2$ ,
3.  $\{b + mi + k_j : 0 \leq i \leq \delta - 2, 0 \leq j \leq r\} \subset T_{\gamma, \beta}(g)$  for some  $\gamma \in N_n^{-1}(a)$ , and  $\beta = \alpha^{q-1}$  for some normal element  $\alpha$  of  $\mathbb{F}_{q^{\text{st}}}$ , and where all elements are taken modulo  $n$ .

Then,  $d_H(C) \geq \delta + r$ .

*Proof.* Let  $w = \delta + r - 1$  and pick  $c \in C$  where  $w_H(c) \leq w$ . It suffices to show  $c = 0$ . Note that  $\mathbf{p}_f(c) = \sum_{h=1}^w c_{l_h} x^{l_h}$  for suitable  $\{l_1, \dots, l_w\} \subset \{0, \dots, n-1\}$ . So, for each  $0 \leq i \leq \delta - 2, 0 \leq j \leq r$  we know  $x - \gamma\beta^{q^{b+im+k_j}} |_{\mathbf{r}} \mathbf{p}_f(c)$ . Hence, for all  $i, j$ ,

$$0 = \sum_{h=1}^w c_{l_h} N_{l_h}(\gamma\beta^{q^{b+im+k_j}}) = \alpha^{-q^{b+im+k_j}} \sum_{h=1}^w c_{l_h} N_{l_h}(\gamma) \alpha^{q^{b+im+k_j+l_h}}.$$

This means  $\bar{c} = (c_{l_1} N_{l_1}(\gamma), \dots, c_{l_w} N_{l_w}(\gamma)) \in \ker(B)$  where

$$B = \left( A \mid A^{q^m} \mid \dots \mid A^{q^{(\delta-2)m}} \right)$$

and

$$A = \left( \alpha^{q^{b+l_h+k_j}} \right)_{\substack{1 \leq h \leq w \\ 0 \leq j \leq r}}.$$

By [1, Lemma 12], if we set  $t = \delta - 1$ , then we know  $\text{rk}(B) = w$  which forces  $\bar{c} = 0$ . Then, since  $N_{l_h}(\gamma) \neq 0$  for all  $1 \leq h \leq w$ , we must have  $c = 0$ .  $\square$

As we will see next, the Roos-like bound for the rank distance also holds with a general modulus  $f = x^n - a$  when  $a \in N_n(\mathbb{F}_q)$ . For the case where  $a = 1$ , see Theorem 22 in [1].

**Theorem 5.1.4** (Skew Roos Bound for the rank distance). *Let  $a \in N_n(\mathbb{F}_q)$  and  $f = x^n - a \in \mathbb{F}_q[x; \sigma]$ . Also let  $g \in \mathbb{F}_{q^s}[x; \sigma]$  be a right divisor of  $f$  and set  $C = \mathbf{v}_f(\bullet(\bar{g})) \subset \mathbb{F}_{q^s}^n$ . Suppose there exists parameters  $b, m, \delta, r, k_0, \dots, k_r \in \mathbb{N}_0$  such that*

1.  $m \neq 0$  and  $\gcd(m, n) = 1$ ,
2.  $k_0 < k_1 < \dots < k_r$  with  $k_r - k_0 \leq \delta + r - 2$ ,

3.  $\{b + mi + k_j : 0 \leq i \leq \delta - 2, 0 \leq j \leq r\} \subset T_{\gamma, \beta}(g)$  for some  $\gamma \in N_n^{-1}(a) \cap \mathbb{F}_q$ , and  $\beta = \alpha^{q^{-1}}$  for some normal element  $\alpha$  of  $\mathbb{F}_{q^{st}}$ , and where elements are taken modulo  $n$ .

Then,  $d_R(C) \geq \delta + r$ .

*Proof.* By Lemma 2.3.4, it suffices to show  $d_H(CM) \geq \delta + r$  for all  $M \in \text{GL}_n(\mathbb{F}_q)$ . Let  $M \in \text{GL}_n(\mathbb{F}_q)$  be arbitrary,  $w = \delta + r - 1$ , and  $c \in CM^{-1}$  such that  $w_H(c) \leq w$ . It suffices to show  $c = 0$ . Assume  $\mathfrak{p}_f(cM) = \sum_{h=0}^{n-1} p_h x^h$ . Then, for each  $0 \leq i \leq \delta - 2$ ,  $0 \leq j \leq r$  we know  $x - \gamma \beta^{q^{b+im+k_j}} \mid_r \mathfrak{p}_f(cM)$ . Hence, for all  $i, j$

$$0 = \sum_{h=0}^{n-1} p_h N_h(\gamma \beta^{q^{b+im+k_j}}) = \alpha^{-q^{b+im+k_j}} \sum_{h=0}^{n-1} p_h N_h(\gamma) \alpha^{q^{b+im+k_j+h}}.$$

Let  $D = \text{diag}(1, N_1(\gamma), \dots, N_{n-1}(\gamma))$ . Then, we have  $cMD \in \ker(B)$  where

$$B = \left( A \mid A^{q^m} \mid \dots \mid A^{q^{(\delta-2)m}} \right)$$

and

$$A = \left( \alpha^{q^{b+h+k_j}} \right)_{\substack{0 \leq h \leq n-1 \\ 0 \leq j \leq r}}.$$

Let  $L := \{l_1, \dots, l_w\} \subset \{0, \dots, n-1\}$  denote the non-zero components of  $c$  and set  $\bar{c} = (c_{l_1}, \dots, c_{l_w})$ . Denote by  $M_L$  the rows of  $M$  indexed by  $L$ . Then clearly  $cM = \bar{c}M_L$ , so we have  $\bar{c} \in \ker(M_L D B)$ . Since  $M_L D \in \mathbb{F}_q^{w \times n}$  and hence invariant under powers of  $q$ , we have

$$M_L D B = \left( M_L D A \mid (M_L D A)^{q^m} \mid \dots \mid (M_L D A)^{q^{(\delta-2)m}} \right)$$

Now we will show that

$$M_L D A = \left( \beta_h^{q^{k_j}} \right)_{\substack{1 \leq h \leq w \\ 0 \leq j \leq r}},$$

for linearly independent  $\beta_1, \dots, \beta_w$  where

$$\beta_h = M_{\{l_h\}} D [\alpha^{q^b}, \alpha^{q^{b+1}}, \dots, \alpha^{q^{b+n-1}}]^T.$$

Let  $M = (m_{ij})$ . Then for all  $1 \leq h \leq w$ ,  $0 \leq j \leq r$ , we have

$$\begin{aligned} (M_L D A)_{hj} &= \sum_{i=0}^{n-1} m_{l_h, i} N_i(\gamma) \alpha^{q^{b+k_j+i}} = \left( \sum_{i=0}^{n-1} m_{l_h, i} N_i(\gamma) \alpha^{q^{b+i}} \right)^{q^{k_j}} \\ &= \left( M_{\{l_h\}} D [\alpha^{q^b}, \alpha^{q^{b+1}}, \dots, \alpha^{q^{b+n-1}}]^T \right)^{q^{k_j}} = (\beta_h)^{q^{k_j}}. \end{aligned}$$

To show linear independence, assume that for  $x_1, \dots, x_w \in \mathbb{F}_q$  we have

$$\begin{aligned}
0 &= x_1\beta_1 + \dots + x_w\beta_w \\
&= \sum_{h=1}^w x_h \left( \sum_{i=0}^{n-1} m_{l_h,i} N_i(\gamma) \alpha^{q^{b+i}} \right) \\
&= \sum_{h=1}^w \sum_{i=0}^{n-1} x_h m_{l_h,i} N_i(\gamma) \alpha^{q^{b+i}} \\
&= \sum_{i=0}^{n-1} \left( \sum_{h=1}^w x_h m_{l_h,i} N_i(\gamma) \right) \alpha^{q^{b+i}} \\
&= \left( \sum_{i=0}^{n-1} \left( \sum_{h=1}^w x_h m_{l_h,i} N_i(\gamma) \right) \alpha^{q^i} \right)^{q^b}.
\end{aligned}$$

Since  $\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}$  are linearly independent over  $\mathbb{F}_q$ , we must have  $\sum_{h=1}^w x_h m_{l_h,i} N_i(\gamma) = 0$  for all  $i = 0, \dots, n-1$ . Then,

$$0 = \sum_{h=1}^w x_h m_{l_h,i} N_i(\gamma) = N_i(\gamma) \sum_{h=1}^w x_h m_{l_h,i}.$$

So, in fact  $\sum_{h=1}^w x_h m_{l_h,i} = 0$  for all  $i = 0, \dots, n-1$ . This forces  $(x_1, \dots, x_w)M_L = 0$ . Now, since  $M$  is invertible, we know  $\text{rk}(M_L) = w$ , so  $x_h = 0$  for all  $1 \leq h \leq w$ . Thus,  $\beta_1, \dots, \beta_w$  are linearly independent over  $\mathbb{F}_q$ . Therefore, by [1, Lemma 12], we have  $\text{rk}(M_L DB) = w$ . This forces  $\bar{c} = 0$  and hence  $c = 0$  as needed.  $\square$

Unfortunately, the Roos-like bound for the rank distance does not hold for  $\gamma \in \mathbb{F}_{q^s} \setminus \mathbb{F}_q$ . Indeed, the following is a counter-example to the Roos-like bound for the rank metric when  $\gamma \notin \mathbb{F}_q$ .

**Example 5.1.5.** Let  $n = s = 6$ ,  $t = 1$ , and consider fields  $\mathbb{F}_{3^6}/\mathbb{F}_3$ . Let  $\omega$  be a primitive element of  $\mathbb{F}_{3^6}$  which satisfies  $\omega^6 + 2\omega^4 + \omega^2 + 2\omega + 2 = 0$ . Note that  $\alpha = \omega^2$  generates a normal basis of  $\mathbb{F}_{3^6}$ , so set  $\beta = \omega^4$ . Pick  $\gamma = \omega^{11} \in \mathbb{F}_{3^6} \setminus \mathbb{F}_3$ . Then we have  $a = N_6(\gamma) = 2 \in \mathbb{F}_3$ , and note that  $a \notin N_6(\mathbb{F}_3^*)$ . Now choose parameters  $b = 1, m = 5, \delta = 3, r = 1, k_0 = 1, k_1 = 3$ , and let

$$g = \text{lclm}\{\gamma\beta^{q^{b+im+k_j}} : 0 \leq i \leq 1, 0 \leq j \leq 1\}.$$

For  $f = x^6 - 2$ , define  $C = \mathbf{v}_f(\bullet(\bar{g}))$ . Using SageMath software, one may easily see

$$v := (\omega^{203}, \omega, \omega^{31}, \omega^{397}, \omega^{667}, \omega^{321}) \in C$$

but  $\text{rk}(v) = 3 < \delta + r$ .

## 5.2 Representative Defining Sets and Implications to MRD Codes

In the previous section, we often have a generating polynomial  $g$  in  $\mathbb{F}_{q^s}[x; \sigma]$  even though the roots  $\gamma\beta^{qi}$  come from a field extension  $\mathbb{F}_{q^{st}}$ . As we will see, this puts a nice structure on sets of the form  $T_{\gamma, \beta}(g)$  which has implications as to when  $C = \mathbf{v}_f(\bullet(\bar{g}))$  is an MRD code.

Throughout this section, let  $n = st$  and recall  $Z_n := (\{0, \dots, n-1\}, +)$ . Then note  $sZ_n = \{0, s, \dots, s(t-1)\}$  is a subgroup of  $Z_n$ . Hence, we can write

$$Z_n = \bigsqcup_{j=0}^{s-1} (j + sZ_n).$$

**Definition 5.2.1.** A subset  $T \subset Z_n$  is called  $s$ -closed if for any  $i \in T$ , we also have  $i + s \in T$ .

With the same arguments as in the proof of Proposition 2.1.17, we have the following useful facts.

**Proposition 5.2.2.** Let  $\gamma \in \mathbb{F}_q^*$  and  $\beta \in \mathbb{F}_{q^{st}}$ .

1. If  $g \in \mathbb{F}_{q^s}[x; \sigma]$ , then  $T_{\gamma, \beta}(g)$  is  $s$ -closed.
2. Conversely, if  $T \subset Z_n$  is an  $s$ -closed set, then  $\text{lcm}\{x - \gamma\beta^{qi} : i \in T\}$  is a polynomial over  $\mathbb{F}_{q^s}$  rather than  $\mathbb{F}_{q^{st}}$ .

If  $g \in \mathbb{F}_{q^s}[x; \sigma]$ , then the above proposition allows us to work with a subset of the  $(\gamma, \beta)$ -defining set.

**Definition 5.2.3.** Let  $T \subset Z_n$  be an  $s$ -closed set. Define  $T^{(s)} := \{i_1, \dots, i_l\} \subset \{0, \dots, s-1\}$  such that

$$T = \bigsqcup_{j=1}^l (i_j + sZ_n).$$

Note that  $T^{(s)}$  is well-defined. We call  $T^{(s)}$  the  $s$ -representative set of  $T$ .

As we will show next, when  $g \in \mathbb{F}_{q^s}[x; \sigma]$  is in fact the minimal polynomial for its  $(\gamma, \beta)$ -defining set  $T$ , then the size of the  $s$ -representative set of  $T$  will have implications on when  $C = \mathbf{v}_f(\bullet(\bar{g}))$  is an MRD code. It comes from the Singleton-like bound for these particular skew-cyclic codes and is stated precisely in the following proposition. For the case where  $a = 1$ , see Proposition 26 in [1].

**Proposition 5.2.4.** *Let  $n = st$ . Choose  $a = N_n(\gamma)$ ,  $\gamma \in \mathbb{F}_q^*$  and let  $f = x^n - a$ . Also let  $\alpha$  be a normal element of  $\mathbb{F}_{q^{st}}$ , and set  $\beta = \alpha^{q-1}$ . Choose parameters  $b, m, \delta, r, k_0, \dots, k_r \in \mathbb{N}_0$  such that*

1.  $m \neq 0$  and  $\gcd(m, n) = 1$ ,
2.  $k_0 < \dots < k_r$  with  $k_r - k_0 \leq \delta + r - 2$ .
3. Set  $T = \{b + im + k_j : 0 \leq i \leq \delta - 2, 0 \leq j \leq r\} \subset Z_n$  and let  $\bar{T}$  be the  $s$ -closure of  $T$  in  $Z_n$ , where all elements are taken modulo  $n$ .

Now, set

$$g := \text{lcm}\{x - \gamma\beta^{q^\lambda} : \lambda \in \bar{T}\} \in \mathbb{F}_{q^s}[x; \sigma].$$

Then  $C := \mathbf{v}_f(\bullet(\bar{g}))$  satisfies

$$\delta + r \leq d_R(C) \leq |\bar{T}^{(s)}| + 1.$$

In particular, when  $|\bar{T}^{(s)}| = \delta + r - 1$ , then  $C$  is an MRD code with rank distance  $\delta + r$ .

*Proof.* The lower bound is given by Theorem 5.1.4. For the upper bound, recall that the Singleton-like bound for the rank metric (see Equation (2.3) following Proposition 2.3.3) is given by

$$d_R(C) \leq s - \frac{\dim_{\mathbb{F}_{q^s}}(C)}{t} + 1.$$

Also recall from Proposition 2.4.3 that  $\dim_{\mathbb{F}_{q^s}}(C) = n - \deg(g)$ . We will now show  $\deg(g) = |\bar{T}|$ . Clearly we have  $\deg(g) \leq |\bar{T}|$ . To show equality, first note that  $\bar{T} \subseteq Z_n$ , so all elements are taken modulo  $n$ . Therefore, all  $\alpha^{q^\lambda}$ ,  $\lambda \in \bar{T}$  are linearly independent over  $\mathbb{F}_q$  since  $\alpha$  is a normal element. Then, since  $\gamma\beta^{q^\lambda} = \gamma(\alpha^{q^\lambda})^{q-1}$ , we know all  $\gamma\beta^{q^\lambda}$ ,  $\lambda \in \bar{T}$  are P-independent by Corollary 2.1.28. Hence,  $\deg(g) = |\bar{T}|$ . Lastly, since  $|\bar{T}| = t|\bar{T}^{(s)}|$  we have

$$d_R(C) \leq s - \frac{n - t|\bar{T}^{(s)}|}{t} + 1 = |\bar{T}^{(s)}| + 1.$$

If in fact  $|\bar{T}^{(s)}| = \delta + r - 1$ , then  $d_R(C)$  is forced to be  $\delta + r$ . □

We will now look at a special case of Proposition 5.2.4. For the case where  $a = 1$ , see Corollary 28 in [1].

**Corollary 5.2.5.** *Let  $n = st$ . Choose  $a = N_n(\gamma)$ ,  $\gamma \in \mathbb{F}_q^*$  and let  $f = x^n - a$ . Also let  $\alpha$  be a normal element of  $\mathbb{F}_{q^{st}}$ , and set  $\beta = \alpha^{q-1}$ . Choose parameters  $b, m, \delta' \in \mathbb{N}_0$  such that  $m \neq 0$ ,  $\gcd(m, n) = 1$ , and  $2 \leq \delta' \leq s$ . Set*

1.  $T = \{b, b + m, \dots, b + (\delta' - 2)m\} \subset Z_n$ , where all elements are taken modulo  $n$ ,



2.  $\overline{T}$  be the  $s$ -closure of  $T$  in  $Z_n$ ,
3.  $g := \text{lclm}\{x - \gamma\beta^{q^\lambda} : \lambda \in \overline{T}\} \in \mathbb{F}_{q^s}[x; \sigma]$ .

Then  $C := \mathbf{v}_f(\bullet(\overline{g}))$  is an MRD code with rank distance  $\delta'$ . We call  $C$  a **skew-BCH Code of the second kind**.

*Proof.* First note that  $g$  is a right divisor of  $f$  by Remark 5.1.2. Therefore,  $C$  satisfies the parameters in Proposition 5.2.4 with  $r = k_0 = 0$ . Next we will show all the elements of  $T$  are distinct modulo  $s$ . Suppose there are  $0 \leq j \leq i \leq \delta' - 2$  such that  $b + im \equiv b + jm \pmod{s}$ . Then,  $s|m(i - j)$ , and since  $\gcd(m, s) = 1$ , we must have  $s|(i - j)$ . However, since  $i, j \leq \delta' - 2 < s$ , this forces  $i = j$ . Thus,  $|\overline{T}^{(s)}| = |T| = \delta' - 1$ . Hence, also by Proposition 5.2.4  $C$  is an MRD code with rank distance  $\delta'$ .  $\square$

We will see skew-BCH Codes of the first kind in Section 6.2. The set  $T$  in Corollary 5.2.5 above is in an important form which we will define next.

**Definition 5.2.6.** A set  $T = \{a_1, \dots, a_l\} \subset Z_n$  is an arithmetic progression with common difference  $m$  if there is an ordering of elements of  $T$ , say  $a_{i_1}, \dots, a_{i_l}$ , where  $a_{i_j} \equiv a_{i_{j-1}} + m \pmod{n}$  for all  $j = 2, \dots, l$ .

At the end of [1], the authors pose the question whether it is possible to construct skew-cyclic MRD codes where the  $s$ -representative set of the  $(\gamma, \beta)$ -defining set is not in the form of an arithmetic progression such as in Corollary 5.2.5. When  $m$  is prime, the authors used the Cauchy-Davenport Theorem to show the answer is no (see Proposition 30 in [1]). We were able to show for any  $m$ , the answer is no. The following is the statement of this result.

**Theorem 5.2.7.** Let  $n = st$ . Choose  $a = N_n(\gamma)$ ,  $\gamma \in \mathbb{F}_q^*$  and let  $f = x^n - a$ . Also let  $\alpha$  be a normal element of  $\mathbb{F}_{q^{st}}$ , and set  $\beta = \alpha^{q-1}$ . Choose parameters  $b, m, \delta \geq 3, r, k_0, \dots, k_r \in \mathbb{N}_0$  such that

1.  $m \neq 0$  and  $\gcd(m, n) = 1$ ,
2.  $k_0 < \dots < k_r$  with  $k_r - k_0 \leq \delta + r - 2$ .
3. Set  $T = \{b + im + k_j : 0 \leq i \leq \delta - 2, 0 \leq j \leq r\} \subset Z_n$  and let  $\overline{T}$  be the  $s$ -closure of  $T$  in  $Z_n$ , where all elements are taken modulo  $n$ .

If  $|\overline{T}^{(s)}| = \delta + r - 1$ , then  $\overline{T}^{(s)}$  is an arithmetic progression with common difference  $m$ . As a consequence, we are in the situation of Corollary 5.2.5 with  $\overline{T}^{(s)}$  in place of  $T$ .

The proof will be given in Section 5.4. We first need some set theoretic results.

### 5.3 Preliminary Results on Arithmetic Progressions

Throughout this section, consider the abelian group  $Z_s = (\{0, \dots, s-1\}, +)$  with addition taken modulo  $s$ . Let  $r, d \in \mathbb{Z}$  be positive integers such that  $d + r + 1 < s$ . Also let  $A := \{k_0, \dots, k_r\}$  with elements  $k_i$  that are distinct modulo  $s$ . Let  $B := \{0, m, \dots, dm\}$  where  $\gcd(m, s) = 1$ . Note that the elements of  $B$  are also distinct modulo  $s$ . Define  $A + B \subset Z_s$  by element wise addition where all the elements are taken modulo  $s$ . In this section, we will show  $|A + B| \geq d + r + 1$ , and in the case of equality  $A + B$  can be written as an arithmetic progression.

**Proposition 5.3.1.** *Define the map  $\varphi : Z_s \rightarrow Z_s$  where  $a \mapsto a + m$ . Then,  $\varphi$  is a cycle of length  $s$ . As a consequence, if  $K \subseteq Z_s$  and  $\varphi(K) \subset K$ , then  $K = Z_s$ .*

*Proof.* There are no fixed points of  $\varphi$  since  $m \neq 0$ . Consider a cycle  $(a, a + m, \dots, a + (l-1)m)$  contained in  $Z_s$  where  $a + lm = a$ , with  $l \leq s$ . Then,  $s|lm$ , so  $s|l$  since  $\gcd(m, s) = 1$ . Hence,  $l = s$ . As a consequence, if  $\varphi(K) \subset K$ , then  $K$  can be written as a cycle of length  $s$ . Hence,  $K = Z_s$ .  $\square$

**Lemma 5.3.2.** *For  $A + B$  defined above, we have  $|A + B| \geq d + r + 1$ .*

*Proof.* We will prove this by induction on  $d$ . For the base case, if  $d = 1$ , then  $B = \{0, m\}$ . By Proposition 5.3.1, we have

$$|A + B| = |A + \varphi(A)| \geq |A| + 1 = r + 2.$$

Now, assume  $B = \{0, m, \dots, dm\}$  and let  $B_1 = \{0, m, \dots, (d-1)m\}$ . By the inductive hypothesis,  $|A + B_1| \geq r + d$ . Let  $\hat{A} = A + B_1$ , and note  $A + B = \hat{A} + \{0, m\}$ . If  $|\hat{A}| \geq r + d + 1$ , then clearly  $|A + B| \geq r + d + 1$ . If  $|\hat{A}| = r + d$ , then

$$|A + B| = |\hat{A} + \{0, m\}| \geq |\hat{A}| + 1 = r + d + 1. \quad \square$$

For the rest of this section, assume  $|A + B| = d + r + 1$ . Recall that  $d \geq 1$  and therefore  $A + B \neq A$ .

**Definition 5.3.3.** Consider  $\mathcal{L} = \{(i_1, j_1), \dots, (i_d, j_d)\} : 0 \leq i_l \leq r, 1 \leq j_l \leq d\}$ .

1. We say  $L = \{(i_1, j_1), \dots, (i_d, j_d)\} \in \mathcal{L}$  is a representation of  $A + B$  if

$$A + B = \{k_0, \dots, k_r, k_{i_1} + j_1 m, \dots, k_{i_d} + j_d m\}.$$

2. We say  $(i_l, j_l)$  is equivalent to  $(i'_l, j'_l)$ , denoted  $(i_l, j_l) \sim (i'_l, j'_l)$ , if  $k_{i_l} + j_l m = k_{i'_l} + j'_l m$ .

3. For a representation  $L = \{(i_1, j_1), \dots, (i_d, j_d)\}$  of  $A + B$ , define  $\sigma(L) := \sum_{l=1}^d j_l$ .

**Lemma 5.3.4.** *Let  $L$  be a representation of  $A + B$  where  $\sigma(L)$  is minimal among all representations of  $A + B$ . Then,*

$$L = \{(0, 1), (0, 2), \dots, (0, d)\}.$$

*Proof.* By Proposition 5.3.1, we know  $\varphi(A + B) \not\subset A + B$  since  $|A + B| < s$ . We will show that in every representation of  $A + B$  there is some  $j_l$  equal to  $d$ . First note that  $\varphi(k_i + jm) \in A + B$  for all  $i$  and  $j < d$ . Assume for contradiction that  $j_l \neq d$  for all  $(i_l, j_l) \in L$ . Then for all  $0 \leq i \leq r$ ,

$$k_i + dm = k_{i_v} + j_v m$$

for some  $(i_v, j_v) \in L$ . However, then we have

$$\varphi(k_i + dm) = \varphi(k_{i_v} + j_v m) \in A + B$$

This forces  $\varphi(A + B) \subset A + B$ , a contradiction, so we may assume  $j_d = d$ . By re-indexing  $k_0, \dots, k_r$  we may also assume that  $i_d = 0$ . Thus,  $(0, d) \in L$ . Now suppose there is some  $1 \leq l < d$  where  $(0, l) \notin L$ . Then, since  $k_0 + lm \in A + B$ , we must have one of the following cases

1.  $k_0 + lm = k_i$  for some  $1 \leq i \leq r$ ,
2.  $k_0 + lm = k_{i_v} + j_v m$  for some  $(i_v, j_v) \in L$ .

Case 1: If  $k_0 + lm = k_i$ , then  $(0, d) \sim (i, d - l)$ . Hence, replacing  $(0, d)$  by  $(i, d - l)$  in  $L$  would lead to another representation  $L'$  of  $A + B$  with a smaller sum  $\sigma(L')$ .

Case 2: Suppose  $k_0 + lm = k_{i_v} + j_v m$ . We are assuming  $(0, l) \notin L$ , so clearly  $l \neq j_v$ . If  $j_v < l$ , then  $(0, d) \sim (i_v, d - l + j_v)$ . Hence, replacing  $(0, d)$  by  $(i_v, d - l + j_v)$  in  $L$  would be another representation of  $A + B$  that contradicts the minimality of  $\sigma(L)$ . If  $j_v > l$ , then  $(i_v, j_v) \sim (0, l)$  also giving a representation of  $A + B$  that contradicts the minimality of  $\sigma(L)$ .

Therefore,  $\{(0, l) \in L : 1 \leq l < d\} \subset L$ . Since  $|L| = d$ , we have  $L = \{(0, l) \in L : 1 \leq l \leq d\}$ .  $\square$

**Theorem 5.3.5.** *If we assume  $|A + B| = d + r + 1$ , then  $A + B$  can be written as an arithmetic progression with common difference  $m$ .*

*Proof.* By Lemma 5.3.4, we may assume that  $A + B$  is of the form

$$A + B = \{k_0, k_1, \dots, k_r, k_0 + m, \dots, k_0 + dm\}$$

where all elements listed are distinct. Let  $\varphi : Z_s \rightarrow Z_s$  be the map where  $a \mapsto a + m$ . Then, by Proposition 5.3.1,  $\varphi(\{k_1, \dots, k_r\}) \not\subset \{k_1, \dots, k_r\}$ . Since  $\varphi(\{k_1, \dots, k_r\}) \subset A + B$ , there must be some  $k_i \in \{k_1, \dots, k_r\}$  such that  $\varphi(k_i) \in \{k_0, k_0 + m, \dots, k_0 + dm\}$

$dm\}$ . If  $\varphi(k_i) = k_0 + lm$  where  $l \geq 1$ , then  $k_i = k_0 + (l-1)m$  contradictory to these elements being distinct. So  $\varphi(k_i) = k_0$ . WLOG assume  $\varphi(k_r) = k_0$ . Similarly,  $\varphi(\{k_1, \dots, k_{r-1}\}) \not\subseteq \{k_1, \dots, k_{r-1}\}$ , so there is some  $k_i \in \{k_1, \dots, k_{r-1}\}$ , where  $\varphi(k_i) \in \{k_r, k_0 + m, \dots, k_0 + dm\}$ . If  $\varphi(k_i) = k_0 + lm$  where  $l \geq 1$ , then  $k_i = k_0 + (l-1)m$ , a contradiction. Hence,  $\varphi(k_i) = k_r$ , wlog assume  $\varphi(k_{r-1}) = k_r$ .

Continuing in this fashion we obtain a chain of images under  $\varphi$

$$k_1 \mapsto k_2 \mapsto \dots \mapsto k_r \mapsto k_0.$$

We can now include the other elements of  $A + B$  in the natural way

$$k_1 \mapsto \dots \mapsto k_r \mapsto k_0 \mapsto k_0 + m \mapsto \dots \mapsto k_0 + dm.$$

Thus,  $A+B$  can be written as an arithmetic progression  $\{k_1 + jm : 0 \leq j \leq r+d\}$ .  $\square$

#### 5.4 Proof of Theorem 5.2.7

Now we are ready to prove Theorem 5.2.7 which is restated here for convenience.

**Theorem 5.2.7.** *Let  $n = st$ . Choose  $a = N_n(\gamma)$ ,  $\gamma \in \mathbb{F}_q^*$  and let  $f = x^n - a$ . Also let  $\alpha$  be a normal element of  $\mathbb{F}_{q^{st}}$ , and set  $\beta = \alpha^{q-1}$ . Choose parameters  $b, m, \delta \geq 3, r, k_0, \dots, k_r \in \mathbb{N}_0$  such that*

1.  $m \neq 0$  and  $\gcd(m, n) = 1$ ,
2.  $k_0 < \dots < k_r$  with  $k_r - k_0 \leq \delta + r - 2$ .
3. Set  $T = \{b + im + k_j : 0 \leq i \leq \delta - 2, 0 \leq j \leq r\} \subset Z_n$  and let  $\overline{T}$  be the  $s$ -closure of  $T$  in  $Z_n$ , where all elements are taken modulo  $n$ .

If  $|\overline{T}^{(s)}| = \delta + r - 1$ , then  $\overline{T}^{(s)}$  is an arithmetic progression with common difference  $m$ . As a consequence, we are in the situation of Corollary 5.2.5 with  $\overline{T}^{(s)}$  in place of  $T$ .

*Proof.* First, recall that we have a natural bound  $|\overline{T}| \leq n$ . With this we have

$$t(\delta + r - 1) = t|\overline{T}^{(s)}| = |\overline{T}| \leq n = st.$$

Hence, we must have  $\delta + r - 1 \leq s$ . If we have equality, then  $\overline{T}^{(s)} = Z_s$ . SO, with the help of Proposition 5.3.1,  $\overline{T}^{(s)}$  is an arithmetic progression with common difference  $m$ . Thus, we will assume  $\delta + r - 1 < s$ .

Next, consider the case when  $r = 0$ . In this case, we have  $T = \{b + k_0 + im : 0 \leq i \leq \delta - 2\}$ . We will show  $\overline{T}^{(s)}$  is also in the form of an arithmetic progression. Let  $\overline{T}^{(s)} = \{a_1, \dots, a_{\delta-1}\}$ . Then, by definition  $a_i \equiv b + k_0 + jm \pmod{s}$  for some  $j$ . Hence,

there is a re-ordering of  $\overline{T}^{(s)}$ , say  $a_{i_1}, \dots, a_{i_{\delta-1}}$  such that  $a_{i_j} \equiv b + k_0 + jm \pmod{s}$ . Then, we have

$$a_{i_{j+1}} \equiv b + k_0 + (j+1)m \pmod{s} \equiv a_{i_j} + m \pmod{s}.$$

So,  $\overline{T}^{(s)}$  is in fact an arithmetic progression with common difference  $m$ . For the rest of this proof, we may assume  $r \geq 1$ .

Let  $A := \{b + k_0, \dots, b + k_r\}$  and let  $B := \{0, m, \dots, (\delta - 2)m\}$ . We will show the elements of  $A$  and  $B$  are distinct when taken modulo  $s$ . Let  $b + k_i, b + k_j \in A$  such that  $b + k_i \equiv b + k_j \pmod{s}$ . Then  $s | (k_j - k_i)$  which forces  $i = j$  since  $k_j - k_i < \delta + r - 1 < s$  by assumption 2 above. We also know the elements of  $B$  are distinct modulo  $s$  since  $\gcd(m, s) = 1$ . Now define  $A + B$  by element wise addition where all elements are taken modulo  $s$ . By construction  $b + mi + k_j \pmod{s} \in \overline{T}^{(s)}$  for  $0 \leq i \leq \delta - 2, \leq j \leq r$ . Hence  $A + B \subset \overline{T}^{(s)}$ . By Lemma 5.3.2 (with  $d = \delta - 2 \geq 1$ ),  $|A + B| \geq r + \delta - 1 = |\overline{T}^{(s)}|$ . Thus,  $A + B = \overline{T}^{(s)}$ . Therefore, by Theorem 5.3.5, the set  $\overline{T}^{(s)}$  can be written as an arithmetic progression with common difference  $m$ . Lastly, note that  $\overline{T} = \overline{\overline{T}^{(s)}}$ . Thus, we are in the situation of Corollary 5.2.5 with  $\delta' = \delta + r$  and  $T = \overline{T}^{(s)}$ .  $\square$

## Chapter 6 Skew-Cyclic Subfield Subcodes

In [20], the authors relate the number of roots of a polynomial with the minimum Hamming distance of the skew-cyclic code generated by that polynomial. We will discuss constructing these skew-cyclic codes over  $\mathbb{F}_{q^s}$  while allowing the roots to come from some field extension  $\mathbb{F}_{q^{st}}$ . Hence, the smaller code over  $\mathbb{F}_{q^s}$  is a skew-cyclic subfield subcode of some larger skew-cyclic code over  $\mathbb{F}_{q^{st}}$ . There are two ways to get a subfield subcode over  $\mathbb{F}_{q^s}$ . As we will see, both methods produce the same code. We will also compare the dimension of BCH codes of the first and second kind.

### 6.1 Constructing Skew-Cyclic Codes over $\mathbb{F}_{q^s}$

Throughout, assume we have field extensions  $\mathbb{F}_{q^{st}}/\mathbb{F}_{q^s}/\mathbb{F}_q$ . Let  $\theta$  be the  $q$ -Frobenius automorphism of  $\mathbb{F}_{q^{st}}$  and let  $\sigma = \theta|_{\mathbb{F}_{q^s}}$ . Also let  $A \subset \mathbb{F}_{q^{st}}$  and let  $\overline{A}$  be the Galois closure of  $A$  under  $\text{Aut}(\mathbb{F}_{q^{st}}/\mathbb{F}_{q^s})$ . Consider the polynomials

$$m_A = \text{lcm}\{x - \gamma : \gamma \in A\} \in \mathbb{F}_{q^{st}}[x; \theta]$$

$$m_{\overline{A}} = \text{lcm}\{x - \alpha : \alpha \in \overline{A}\} \in \mathbb{F}_{q^s}[x; \sigma].$$

Indeed,  $m_{\overline{A}}$  has coefficients in  $\mathbb{F}_{q^s}$  since the set of roots,  $\overline{A}$ , is Galois closed (see Prop 2.1.17). Now, let  $n \in \mathbb{N}$  with  $n \geq \deg(m_{\overline{A}})$ . The largest option for  $n$  is described in detail in Section 2.2. Also, let  $\hat{f} \in \mathbb{F}_{q^{st}}[x; \theta]$  and  $f \in \mathbb{F}_{q^s}[x; \sigma]$  be left multiples of  $m_A$  and  $m_{\overline{A}}$  respectively, both monic of degree  $n$ . Then, we may define the modules

$$\mathcal{R} = \frac{\mathbb{F}_{q^s}[x; \sigma]}{\bullet(f)} \quad \text{and} \quad \mathcal{S} = \frac{\mathbb{F}_{q^{st}}[x; \theta]}{\bullet(\hat{f})}.$$

Recall, these modules are (left) isomorphic to the vector spaces  $\mathbb{F}_{q^s}^n$  and  $\mathbb{F}_{q^{st}}^n$  respectively. The  $\mathbb{F}_{q^s}$ -isomorphism is given by

$$\mathbf{p}_f : \mathbb{F}_{q^s}^n \rightarrow \mathcal{R} \quad \text{where} \quad (u_0, \dots, u_{n-1}) \mapsto \overline{\sum_{i=0}^{n-1} u_i x^i}.$$

Let  $\mathbf{v}_f = \mathbf{p}_f^{-1}$ . Similarly, we define the  $\mathbb{F}_{q^{st}}$ -isomorphism  $\mathbf{p}_{\hat{f}} : \mathbb{F}_{q^{st}}^n \rightarrow \mathcal{S}$ . Hence, we may identify skew-cyclic codes in  $\mathcal{R}$  (or  $\mathcal{S}$ ) as subspaces of  $\mathbb{F}_{q^s}^n$  (or  $\mathbb{F}_{q^{st}}^n$ ).

We will now discuss two constructions of skew-cyclic codes over  $\mathbb{F}_{q^s}$ . Define the codes

$$C_1 := \mathbf{v}_{\hat{f}}(\bullet(\overline{m_A})) \cap \mathbb{F}_{q^s}^n,$$

$$C_2 := \mathbf{v}_f(\bullet(\overline{m_{\overline{A}}}).$$

Then, by definition of  $m_A$  and  $m_{\bar{A}}$ , we have

$$C_1 = \ker_l(V_n(A)) \cap \mathbb{F}_{q^s}^n,$$

$$C_2 = \ker_l(V_n(\bar{A})) \cap \mathbb{F}_{q^s}^n.$$

**Proposition 6.1.1.** *Given the constructions above,  $C_1 = C_2$ .*

*Proof.* Since  $A \subset \bar{A}$ , we clearly have  $C_2 \subseteq C_1$ . Now we will show  $C_1 \subseteq C_2$ . Let  $h = (h_0, \dots, h_{n-1}) \in C_1$ , and let  $\alpha \in A$  so that  $\alpha^{q^{sj}} \in \bar{A}$  for any  $j \in \mathbb{N}$ . Then consider

$$\sum_{i=0}^{n-1} h_i N_i(\alpha^{q^{sj}}) = \left( \sum_{i=0}^{n-1} h_i N_i(\alpha) \right)^{q^{sj}} = 0.$$

Hence,  $h \in \ker_l(V_n(\bar{A}))$ . Since we also have  $h \in \mathbb{F}_{q^s}^n$ , we know  $h \in C_2$  as needed.  $\square$

We close the section with showing how to actually compute the intersection  $C \cap \mathbb{F}_{q^s}^n$  for any  $C \subset \mathbb{F}_{q^{st}}^n$ .

Let  $\{1, \gamma, \dots, \gamma^{t-1}\}$  be a basis for the extension  $\mathbb{F}_{q^{st}}/\mathbb{F}_{q^s}$ . Since the field extension is degree  $t$ , there exists unique  $a_j \in \mathbb{F}_{q^s}$  where  $\gamma^t = \sum_{j=0}^{t-1} a_j \gamma^j$ . Hence, we may define the block companion matrix

$$\Gamma = \begin{bmatrix} 0 & & I_{n(t-1)} & \\ a_0 I_n & a_1 I_n & \dots & a_{t-1} I_n \end{bmatrix} \in \mathbb{F}_{q^s}^{nt \times nt}.$$

Any vector  $v \in \mathbb{F}_{q^{st}}^n$  can be written  $v = \sum_{j=0}^{t-1} v_j \gamma^j$  with  $v_j \in \mathbb{F}_{q^s}^n$ . Define the  $\mathbb{F}_{q^s}$ -isomorphism

$$\psi : \mathbb{F}_{q^{st}}^n \rightarrow \mathbb{F}_{q^s}^{nt} \quad \text{where} \quad v \mapsto (v_0, \dots, v_{t-1}).$$

**Lemma 6.1.2.** *For any  $v \in \mathbb{F}_{q^{st}}^n$ , we have  $\psi(\gamma v) = \psi(v)\Gamma$ .*

*Proof.* Let  $v = \sum_{j=0}^{t-1} \gamma^j v_j$  with  $v_j \in \mathbb{F}_{q^s}^n$ . Then,

$$\begin{aligned} \gamma v &= \gamma v_0 + \gamma^2 v_1 + \dots + \gamma^{t-1} v_{t-2} + \gamma^t v_{t-1} \\ &= \gamma v_0 + \gamma^2 v_1 + \dots + \gamma^{t-1} v_{t-2} + \left( \sum_{j=0}^{t-1} a_j \gamma^j \right) v_{t-1} \\ &= a_0 v_{t-1} + (v_0 + a_1 v_{t-1})\gamma + (v_1 + a_2 v_{t-1})\gamma^2 + \dots + (v_{t-2} + a_{t-1} v_{t-1})\gamma^{t-1}. \end{aligned}$$

Thus,

$$\psi(\gamma v) = \begin{bmatrix} a_0 v_{t-1} & v_0 + a_1 v_{t-1} & v_1 + a_2 v_{t-1} & \dots & v_{t-2} + a_{t-1} v_{t-1} \end{bmatrix} = \psi(v)\Gamma. \quad \square$$

**Theorem 6.1.3.** Let  $C \subset \mathbb{F}_{q^{st}}^n$  with basis  $\{v_1, \dots, v_k\}$  over  $\mathbb{F}_{q^{st}}$ . Define the matrices  $\tilde{M} \in \mathbb{F}_{q^s}^{kt \times nt}$  and  $\tilde{I} \in \mathbb{F}_{q^s}^{n \times nt}$  as follows:

$$\tilde{M} = \begin{bmatrix} \psi(v_1) \\ \psi(v_1)\Gamma \\ \vdots \\ \psi(v_1)\Gamma^{t-1} \\ \psi(v_2) \\ \vdots \\ \psi(v_k)\Gamma^{t-1} \end{bmatrix}, \quad \text{and} \quad \tilde{I} = [ I_n \mid 0 \ \dots \ 0 ].$$

Then,

$$\psi(C \cap \mathbb{F}_{q^s}^n) = \text{rs}(\tilde{M}) \cap \text{rs}(\tilde{I}).$$

*Proof.* Let  $u \in \mathbb{F}_{q^s}^n$ . Then,  $u \in C$  if and only if  $u = \sum_{i=1}^k \left( \sum_{j=0}^{t-1} \alpha_{ij} \gamma^j \right) v_i$  for  $\alpha_{ij} \in \mathbb{F}_{q^s}$ . This is equivalent to

$$\psi(u) = \sum_{i=1}^k \sum_{j=0}^{t-1} \alpha_{ij} \psi(\gamma^j v_i) = \alpha \begin{bmatrix} \psi(v_1) \\ \psi(\gamma v_1) \\ \vdots \\ \psi(\gamma^{t-1} v_1) \\ \psi(v_2) \\ \vdots \\ \psi(\gamma^{t-1} v_k) \end{bmatrix}$$

where  $\alpha = (\alpha_{10}, \dots, \alpha_{1t-1}, \alpha_{20}, \dots, \alpha_{kt-1}) \in \mathbb{F}_{q^s}^{kt}$ . By lemma 6.1.2, the matrix on the RHS is equal to  $\tilde{M}$ . Hence,  $u \in C$  if and only if  $\psi(u) \in \text{rs}(\tilde{M})$ . Therefore,  $\psi(C) = \text{rs}(\tilde{M})$ . Similarly,  $\psi(\mathbb{F}_{q^s}^n) = \text{rs}(\tilde{I})$ . Since  $\psi$  is an  $\mathbb{F}_{q^s}$ -isomorphism, we now have

$$\psi(C \cap \mathbb{F}_{q^s}^n) = \text{rs}(\tilde{M}) \cap \text{rs}(\tilde{I}). \quad \square$$

The above theorem allows us to use the matrices  $\tilde{M}$  and  $\tilde{I}$  as described above when computing examples involving  $C \cap \mathbb{F}_{q^s}^n$  with  $C \in \mathbb{F}_{q^{st}}^n$ .

## 6.2 Tapia-Tironi Theorems on Hamming Distance

Throughout this section, assume we have field extensions  $\mathbb{F}_{q^{st}}/\mathbb{F}_{q^s}/\mathbb{F}_q$ . We will see that the number of roots of a generating polynomial  $g$  has implications on the lower bound of the minimum Hamming distance of the skew-cyclic code generated by  $g$ . The following theorems are from [20]. The first one is presented here using the minimal polynomial of the root set as the generating polynomial. This ensures we construct a code with the largest possible dimension given the parameters in the theorems. We give proofs below that we believe are more intuitive to the computation heavy ones given in [20].



**Theorem 6.2.1.** [20, Thm. 4.7] Let  $b, m, \delta \in \mathbb{N}_0$  with  $m \neq 0$ , and let  $\beta \in \mathbb{F}_{q^{st}}$ . Define

$$A = \{\beta^{b+im} : 0 \leq i \leq \delta - 2\}$$

and let  $\overline{A}$  be the Galois closure of  $A$  under  $\text{Aut}(\mathbb{F}_{q^{st}}/\mathbb{F}_{q^s})$ . Thus,  $m_{\overline{A}}$  is in  $\mathbb{F}_{q^s}[x; \sigma]$ . Pick  $n$  such that  $n > \max\{\deg(m_{\overline{A}}), \delta\}$  and  $N_i(\beta^m) \neq 1$  for  $i = 1, \dots, n-1$ . Lastly, let the modulus  $f \in \mathbb{F}_{q^s}[x; \sigma]$  be any monic left multiple of  $m_{\overline{A}}$  of degree  $n$  and set  $\mathcal{R} = \frac{\mathbb{F}_{q^s}[x; \sigma]}{\bullet(f)}$ . Then  $C := \mathbf{v}_f(\bullet(\overline{m_{\overline{A}}})) \subset \mathbb{F}_{q^s}^n$  satisfies  $d_H(C) \geq \delta$ . We call  $C$  a **skew-BCH code of the first kind**.

Note that the length  $n$  with the required conditions exists for suitable choices of  $\beta$ ,  $m$ , and  $\delta$ . For instance, if  $m = 1$  and  $\beta$  is a primitive element of  $\mathbb{F}_{q^{st}}$ , then Theorem 2.2.13 tells us that  $N_i(\beta^m) \neq 1$  for  $i = 1, \dots, (q-1)st - 1$ . Furthermore, by Theorem 2.1.19 the largest value for  $\deg(m_{\overline{A}})$  is  $(q-1)st - 1$  (unless the code is trivial) so we may choose  $n$  to be as large as  $(q-1)st$ .

*Proof.* Let  $V$  be the skew Vandermonde matrix

$$V = V_n(\beta^b, \beta^{b+m}, \dots, \beta^{b+(\delta-2)m}) = \begin{bmatrix} 1 & 1 & \dots & 1 \\ N_1(\beta^b) & N_1(\beta^{b+m}) & \dots & N_1(\beta^{b+(\delta-2)m}) \\ N_2(\beta^b) & N_2(\beta^{b+m}) & \dots & N_2(\beta^{b+(\delta-2)m}) \\ \vdots & \vdots & & \vdots \\ N_{n-1}(\beta^b) & N_{n-1}(\beta^{b+m}) & \dots & N_{n-1}(\beta^{b+(\delta-2)m}) \end{bmatrix}.$$

Since  $\beta^b, \beta^{b+m}, \dots, \beta^{b+(\delta-2)m}$  are roots of  $m_{\overline{A}}$ , we know  $C \subset \ker_l(V) \cap \mathbb{F}_{q^s}^n$ . Note that

$$V = \begin{bmatrix} 1 & & & \\ & N_1(\beta^b) & & \\ & & \ddots & \\ & & & N_{n-1}(\beta^b) \end{bmatrix} \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & N_1(\beta^m) & \dots & N_1(\beta^m)^{\delta-2} \\ 1 & N_2(\beta^m) & \dots & N_2(\beta^m)^{\delta-2} \\ \vdots & \vdots & & \vdots \\ 1 & N_{n-1}(\beta^m) & \dots & N_{n-1}(\beta^m)^{\delta-2} \end{bmatrix}.$$

The matrix on the right,  $\tilde{V}$ , is a classical Vandermonde matrix. By Proposition 2.2.6 the elements  $1, N_1(\beta^m), \dots, N_{n-1}(\beta^m)$  are distinct. Hence, any  $\delta - 1 \times \delta - 1$  minor of  $\tilde{V}$  is nonzero. Thus, the same must be true for  $V$ . Therefore, by Cor 1.4.14 in [11],  $d_H(C) \geq \delta$ .  $\square$

The following is a corollary of the above proof together with Theorem 2.1.24.

**Corollary 6.2.2.** Let  $A \subset \mathbb{F}_{q^{st}}$  be as described in Theorem 6.2.1. Then  $\text{rk}_\sigma(A) = \delta - 1$  and  $\text{rk}_\sigma(\overline{A}) \geq \delta - 1$ .

**Remark 6.2.3.** Let  $C := \mathbf{v}_f(\bullet(\overline{m_{\overline{A}}})) \subset \mathbb{F}_{q^s}^n$  be a code that satisfies the conditions of Theorem 6.2.1. Recall the Singleton bound is given by  $d_H(C) \leq n - \dim_{\mathbb{F}_{q^s}}(C) + 1$ , and we say  $C$  is MDS if we have equality. Since  $\dim_{\mathbb{F}_{q^s}}(C) = n - \text{rk}_{\sigma}(\overline{A})$ , this upper bound is equivalent to  $d_H(C) \leq \text{rk}_{\sigma}(\overline{A}) + 1$ . With the lower bound given in the theorem above, we now have

$$\delta \leq d_H(C) \leq \text{rk}_{\sigma}(\overline{A}) + 1.$$

Thus, if  $\text{rk}_{\sigma}(\overline{A}) = \delta - 1$ , we certainly have an MDS code with Hamming distance  $\delta$ .

As shown in the next example, the rank of  $\overline{A}$  depends on the choice of primitive element  $\omega$ . In the following example, we have one primitive element that generates an MDS code, and one that does not generate an MDS code with all other parameters identical.

**Example 6.2.4.** Consider  $\mathbb{F}_{3^6}/\mathbb{F}_{3^2}/\mathbb{F}_3$  with  $n = 6, b = 180, m = 2, \delta = 3$ , and  $\beta = \omega$  for a primitive element  $\omega \in \mathbb{F}_{3^6}$ ,

$$\overline{A} = \{\omega^{164}, \omega^{20}, \omega^{180}, \omega^{182}\}.$$

If  $\omega$  satisfies  $\omega^6 + \omega^5 + 2\omega^4 + \omega^3 + 2\omega^2 + \omega + 2 = 0$ , then  $\text{rk}_{\sigma}(\overline{A}) = 4$ , and  $d_H(\bullet(m_{\overline{A}})) = 4$ . Hence, the code is not MDS since the Singleton bound is 5. However, with the same parameters if  $\omega$  satisfies  $\omega^6 + \omega^5 + 2\omega^4 + 2\omega^3 + 2\omega^2 + 2 = 0$ , then  $\text{rk}_{\sigma}(\overline{A}) = 2$  and  $d_H(\bullet(m_{\overline{A}})) = 3$  so the code is MDS.

With Corollary 2.1.28, we are able to consider the  $\sigma$ -rank of  $\overline{A}$  through a new lens if  $\overline{A}$  is contained in a single  $\sigma$ -conjugacy class. In this case, we are able to relate P-independence of  $\overline{A}$  to linear independence over  $\mathbb{F}_q$  of the  $\sigma$ -conjugate exponents (see Definition 2.1.8). This is summed up in the following theorem.

**Theorem 6.2.5.** *Let*

$$\overline{A} = \{\beta^{(b+im)q^{sj}} : 0 \leq i \leq \delta - 2, 0 \leq j \leq t - 1\}.$$

for  $b, \delta, m, n \in \mathbb{N}_0$  and  $\beta \in \mathbb{F}_{q^{st}}$  satisfying the conditions in Theorem 6.2.1. Also, define

$$\Gamma = \langle \beta^{T_{ij}} : 0 \leq i \leq \delta - 2, 0 \leq j \leq t - 1 \rangle \quad \text{where} \quad T_{ij} = \frac{b(q^{sj} - 1) + imq^{sj}}{q - 1}.$$

If  $(q - 1) | m$ , then  $\overline{A} \subset \Delta(\beta^b)$  and  $\text{rk}_{\sigma}(\overline{A}) = \dim_{\mathbb{F}_q}(\Gamma)$ .

*Proof.* Assume  $(q - 1) | m$ , so that  $T_{ij}$  is an integer for all  $i = 0, \dots, \delta - 2$  and  $j = 0, \dots, t - 1$ . Now consider

$$\beta^{(b+im)q^{sj}} = \beta^b \beta^{b(q^{sj}-1)+imq^{sj}} = \beta^b \beta^{T_{ij}(q-1)} = (\beta^b)^{\beta^{T_{ij}}}.$$

Hence,  $\beta^{(b+im)q^{sj}} \in \Delta(\beta^b)$  for all  $i, j$  with  $\beta^{T_{ij}}$  as the  $\sigma$ -conjugate exponent. The last result follows immediately by Corollary 2.1.28.  $\square$

To reconcile the condition  $(q-1)|m$  with the conditions of Theorem 6.2.1, we need the following result.

**Lemma 6.2.6.** *Let  $\omega$  be a primitive element of  $\mathbb{F}_{q^{st}}$ . If  $st \geq 2$ , then  $\omega^{q-1}$  is a generic element of  $\mathbb{F}_{q^{st}}$  (see Definition 2.2.11).*

*Proof.* Assume  $r|st$  with  $r < st$ . Then, in fact  $r \leq \frac{st}{2}$ , so

$$(q^r - 1)(q - 1) = q^{r+1} - q - (q^r - 1) < q^{r+1} - 1 \leq q^{st} - 1.$$

Therefore, the order of  $\omega$  does not divide  $(q-1)(q^r-1)$ , so  $(\omega^{q-1})^{q^r-1} \neq 1$  for any  $r|st$ ,  $r < st$ . Thus,  $\omega^{q-1}$  is a generic element of  $\mathbb{F}_{q^{st}}$ .  $\square$

**Remark 6.2.7.** The conditions in Theorem 6.2.1 and Theorem 6.2.5 do not contradict. There are choices of  $m$  and  $\beta$  where  $(q-1)|m$  and  $N_i(\beta^m) \neq 1$  for  $i = 1, \dots, n-1$ . Indeed, we saw in Theorem 2.2.13 that if we choose  $m = \hat{m}(q-1)$  where  $\gcd(\hat{m}, q^{st} - 1) = 1$  and  $\beta = \omega$  a primitive element of  $\mathbb{F}_{q^{st}}$ , then  $n$  can be as large as  $st$  since  $\omega^{q-1}$  is generic by Lemma 6.2.6. Hence, it is possible to have parameters that satisfy both theorems.

**Remark 6.2.8.** Consider again the setting of Theorem 6.2.1. We will now make note of the role of the additive constant  $b$  in the exponent of the roots. In the proof of the Theorem, we see the matrix  $\text{diag}(1, N_1(\beta^b), \dots, N_{n-1}(\beta^b))$  is factored from the skew Vandermonde matrix  $V = V_n(\beta^b, \dots, \beta^{b+(\delta-2)m})$ . Since this  $n \times n$  diagonal matrix has full rank, the parameter  $b$  does not impact the lower bound on the Hamming distance of the code  $C$ . The parameter  $b$  plays a larger role on the dimension and the actual distance of  $C$ . For instance, assume sets

$$A = \{\beta^{b+im} : 0 \leq i \leq \delta - 2\} \quad \text{and} \quad A_0 = \{\beta^{im} : 0 \leq i \leq \delta - 2\}$$

satisfy the conditions of the theorem. Then, let  $C = \mathbf{v}_f(\bullet(\overline{m_A}))$  and let  $C_0 = \mathbf{v}_f(\bullet(\overline{m_{A_0}}))$ . The following is an example of very different codes  $C$  and  $C_0$ .

**Example 6.2.9.** Consider  $\mathbb{F}_{36}/\mathbb{F}_{33}/\mathbb{F}_3$  with  $n = 6$ ,  $b = 1$ ,  $m = 3$ ,  $\delta = 3$ , and  $\beta = \omega$ , where  $\omega$  is a primitive element of  $\mathbb{F}_{36}$  that satisfies  $\omega^6 + 2\omega^4 + \omega^2 + 2\omega + 2 = 0$ . Then,  $C$  is an  $[6, 2, 5]$  MDS code and  $C_0$  is an  $[6, 3, 3]$  code. They are clearly not the same code.

Theorem 6.2.1 above may be generalized to the following.

**Theorem 6.2.10.** *[20, Thm. 4.10] Let  $b, m_1, m_2, \delta, r \in \mathbb{N}_0$  with  $(m_1, m_2) \neq (0, 0)$  and let  $\beta \in \mathbb{F}_{q^{st}}$ . Define*

$$A = \{\beta^{b+i_1m_1+i_2m_2} : i_1 = 0, \dots, \delta - 2, i_2 = 0, \dots, r\},$$

and let  $\bar{A}$  be the Galois closure of  $A$  under  $\text{Aut}(\mathbb{F}_{q^{st}}/\mathbb{F}_{q^s})$ . Thus,  $m_{\bar{A}}$  is in  $\mathbb{F}_{q^s}[x; \sigma]$ . Pick  $n > \max\{\deg(m_{\bar{A}}), \delta + r\}$  such that  $N_i(\beta^{m_j}) \neq 1$  for  $i = 1, \dots, n-1$ ,  $j = 1, 2$ . Lastly, let the modulus  $f \in \mathbb{F}_{q^s}[x; \sigma]$  be any left multiple of  $m_{\bar{A}}$  of degree  $n$ . Then  $C := \mathbf{v}_f(\bullet(\overline{m_{\bar{A}}})) \subset \mathbb{F}_{q^s}^n$  satisfies  $d_H(C) \geq \delta + r$ . We call  $C$  a **skew-Hartmann Tzeng code of the first kind**.

*Proof.* Without loss of generality, we may assume  $b = 0$ . Let  $y_i = N_i(\beta)$  and let  $G = [G_0 \mid \dots \mid G_r]$  where

$$G_i = \begin{bmatrix} 1 & 1 & \dots & 1 \\ y_1^{im_2} & y_1^{im_2+m_1} & \dots & y_1^{im_2+(\delta-2)m_1} \\ \vdots & \vdots & & \vdots \\ y_{n-1}^{im_2} & y_{n-1}^{im_2+m_1} & \dots & y_{n-1}^{im_2+(\delta-2)m_1} \end{bmatrix}.$$

Note that  $G_i = D_i M_1$  where

$$D_i = \begin{bmatrix} 1 & & & \\ & y_1^{im_2} & & \\ & & \ddots & \\ & & & y_{n-1}^{im_2} \end{bmatrix} \quad \text{and} \quad M_1 = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & y_1^{m_1} & \dots & y_1^{(\delta-2)m_1} \\ \vdots & \vdots & & \vdots \\ 1 & y_{n-1}^{m_1} & \dots & y_{n-1}^{(\delta-2)m_1} \end{bmatrix}.$$

Let  $u = (u_0, \dots, u_{n-1}) \in C$  be nonzero, and note that  $uG = 0$  since  $C \subset \ker_l(G) \cap \mathbb{F}_{q^s}^n$ . Now, let

$$U_i = uD_i = (u_0, u_1 y_1^{im_2}, \dots, u_{n-1} y_{n-1}^{im_2}), \quad \text{for } i = 0, \dots, r$$

and consider

$$U = \begin{bmatrix} U_0 \\ U_1 \\ \vdots \\ U_{r-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & y_1^{m_2} & \dots & y_{n-1}^{m_2} \\ \vdots & \vdots & & \vdots \\ 1 & y_1^{rm_2} & \dots & y_{n-1}^{rm_2} \end{bmatrix} \begin{bmatrix} u_0 & & & \\ & u_1 & & \\ & & \ddots & \\ & & & u_{n-1} \end{bmatrix}.$$

Label the matrices on the right hand side  $M_2$  and  $D$  respectively. Then, we have

$$uG = 0 \iff UM_1 = 0 \iff M_2 D M_1 = 0.$$

Let  $\text{wt}(u) = w$ , and let the non-zero components of  $u$  be  $u_{a_1}, \dots, u_{a_w}$ . Also let  $\hat{D} = \text{diag}(u_{a_1}, \dots, u_{a_w})$ . We will use the notation  $M^{(i)}$  to represent the  $i$ -th row vector of a matrix  $M$ , and  $M_{(i)}$  to represent the  $i$ -th column vector of  $M$ . Now, define

$$\hat{M}_1 = \begin{bmatrix} M_1^{(a_1)} \\ \vdots \\ M_1^{(a_w)} \end{bmatrix}, \quad \text{and} \quad \hat{M}_2 = [M_{2(a_1)} \mid \dots \mid M_{2(a_w)}].$$

Since  $u \in C$ , we still have  $\hat{M}_2 \hat{D} \hat{M}_1 = 0$ . By Theorem 6.2.1, if we set  $i_2 = 0$  we get  $w \geq \delta$ , if  $i_1 = 0$  we have  $w \geq r + 2$  because  $C$  is contained in both the codes based on the sets  $\{\beta^{b+i_1 m_1} : i_1 = 0, \dots, \delta - 2\}$  and  $\{\beta^{b+i_2 m_2} : i_2 = 0, \dots, r\}$ . Hence, we can extend  $\hat{M}_1$  and  $\hat{M}_2$  to square matrices in  $\mathbb{F}_{q^{st}}^{w \times w}$

$$\tilde{M}_1 = \left[ \begin{array}{cccc|ccc} 1 & y_{a_1}^{m_1} & \dots & y_{a_1}^{(\delta-2)m_1} & y_{a_1}^{(\delta-1)m_1} & \dots & y_{a_1}^{(w-1)m_1} \\ 1 & y_{a_2}^{m_1} & \dots & y_{a_2}^{(\delta-2)m_1} & y_{a_2}^{(\delta-1)m_1} & \dots & y_{a_2}^{(w-1)m_1} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 1 & y_{a_w}^{m_1} & \dots & y_{a_w}^{(\delta-2)m_1} & y_{a_w}^{(\delta-1)m_1} & \dots & y_{a_w}^{(w-1)m_1} \end{array} \right]$$

$$\tilde{M}_2 = \left[ \begin{array}{cccc} 1 & 1 & \dots & 1 \\ y_{a_1}^{m_2} & y_{a_2}^{m_2} & \dots & y_{a_w}^{m_2} \\ \vdots & \vdots & & \vdots \\ y_{a_1}^{r m_2} & y_{a_2}^{r m_2} & \dots & y_{a_w}^{r m_2} \end{array} \right] \cdot \left[ \begin{array}{ccc} y_{a_1}^{(r+1)m_2} & y_{a_2}^{(r+1)m_2} & \dots & y_{a_w}^{(r+1)m_2} \\ \vdots & \vdots & & \vdots \\ y_{a_1}^{(w-1)m_2} & y_{a_2}^{(w-1)m_2} & \dots & y_{a_w}^{(w-1)m_2} \end{array} \right].$$

These matrices are classical Vandermonde matrices. Since  $y_0, \dots, y_{n-1}$  are distinct,  $\tilde{M}_1$  and  $\tilde{M}_2$  are invertible. Hence, the product  $\tilde{M}_2 \hat{D} \tilde{M}_1$  is invertible. As block matrices, this product is also

$$\tilde{M}_2 \hat{D} \tilde{M}_1 = \begin{bmatrix} \hat{M}_2 \hat{D} \hat{M}_1 & * \\ * & * \end{bmatrix} = \begin{bmatrix} 0_{(r+1) \times (\delta-1)} & * \\ * & * \end{bmatrix}.$$

The first  $\delta - 1$  columns must have full rank. This means  $w - (r + 1) \geq \delta - 1$ , so  $w \geq \delta + r$ .  $\square$

### 6.3 Comparison of skew-BCH Codes of the 1st and 2nd Kind

In Section 6.2, we presented results on the minimum Hamming distance of skew-BCH codes of the first kind from [20, Thm. 4.7]. In Section 5.1 we see BCH-codes of the second kind have a similar lower bound on the Hamming distance. Now, we will investigate the dimension of BCH codes of the first and second kind that have the same parameters, and hence the same lower bound on the minimum Hamming distance.

Throughout, let  $n = st$  and assume  $\{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$  is a normal basis of  $\mathbb{F}_{q^n}/\mathbb{F}_q$ . Then, set  $\beta = \alpha^{q-1}$ . Assume  $b, \delta, m \in \mathbb{N}_0$  with  $\delta \leq s$ ,  $m \neq 0$ ,  $\gcd(m, n) = 1$ , and  $N_i(\beta^m) \neq 1$  for  $i = 1, \dots, n - 1$ . Define the set

$$\overline{A_1} = \{\beta^{(b+im)q^{sj}} : 0 \leq i \leq \delta - 2, 0 \leq j \leq t - 1\}$$

and

$$\overline{A_2} = \{\beta^{q^{b+im+sj}} : 0 \leq i \leq \delta - 2, 0 \leq j \leq t - 1\}.$$

For  $l = 1, 2$  define  $g_l = m_{\overline{A_l}}$ . Let the modulus  $f_1 \in \mathbb{F}_{q^s}[x; \sigma]$  be any monic left multiple of  $g_1$  of degree  $n$ , and take  $f_2 = x^n - a \in \mathbb{F}_{q^s}[x; \sigma]$  for  $a \in N_n(\mathbb{F}_{q^s}^*)$ . Then, set  $C_1 = \mathbf{v}_{f_1}(\bullet(\overline{g_1}))$  and  $C_2 = \mathbf{v}_{f_2}(\bullet(\overline{g_2}))$ . As defined in Theorem 6.2.1 and Corollary 5.2.5, we call  $C_1$  a skew-BCH code of the first kind and call  $C_2$  a skew-BCH code of the second kind. Note since both sets are Galois closed under  $\text{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_{q^s})$ ,  $C_1$  and  $C_2$  are both contained in  $\mathbb{F}_{q^n}$ . Recall by Theorem 6.2.1 and Theorem 5.1.3, both  $C_1$  and  $C_2$  satisfy  $d_H(C_l) \geq \delta$ . However, as we see next,  $C_1$  performs better on dimension.

**Theorem 6.3.1.** *Given the constructions above,  $\dim(C_1) \geq \dim(C_2)$ .*

*Proof.* Since  $\dim(C_l) = n - \deg(g_l)$ , it suffices to show  $\deg(g_1) \leq \deg(g_2)$ . Recall by Proposition 2.1.16 the rank of a set is always bounded above by the size of the set. Hence,

$$\deg(g_1) = \text{rk}_\sigma(\overline{A_1}) \leq |\overline{A_1}| \leq (\delta - 1)t.$$

By Theorem 2.2.4, the proof of Corollary 5.2.5, and since  $|\overline{A_2}| = |\overline{A_2}^{(s)}|t$ , we have

$$\deg(g_2) = \text{rk}_\sigma(\overline{A_2}) = |\overline{A_2}| = (\delta - 1)t.$$

Therefore,  $\deg(g_1) \leq \deg(g_2)$ . □

**Remark 6.3.2.** If we take  $b = 0$ , then  $|\overline{A_1}| \leq (\delta - 2)t + 1 < (\delta - 1)t$ . Hence, we will have a strict inequality in the Theorem above.

## Bibliography

- [1] G. N. Alfarano, F. J. Lobillo, and A. Neri. Roos bound for skew cyclic codes in Hamming and rank metric. *Finite Fields and Their Applications*, 69, 2021.
- [2] R. C. Bose and D. K. Ray-Chaudhuri. On a class of error correcting binary group codes. *Information and control*, 3(1):68–79, 1960.
- [3] D. Boucher and F. Ulmer. Coding with skew polynomial rings. *Journal of Symbolic Computation*, 44(12):1644–1656, 2008.
- [4] D. Boucher and F. Ulmer. Codes as modules over skew polynomial rings. In *IMA International Conference on Cryptography and Coding*, pages 38–55, 2009.
- [5] D. Boucher and F. Ulmer. Linear codes using skew polynomials with automorphisms and derivations. *Designs, codes and cryptography*, 70:405–431, 2014.
- [6] M. Boulagouaz and A. Leroy.  $(\sigma, \delta)$ -codes. *Advances in Mathematics of Communications*, 7:463–474, 2013.
- [7] N. Fogarty and H. Gluesing-Luerssen. A circulant approach to skew-constacyclic codes. *Finite Fields and Their Applications*, 35:92–114, 2015.
- [8] E. M. Gabidulin. Theory of codes with maximum rank distance. *Problemy peredachi informatsii*, 21(1):3–16, 1985.
- [9] H. Gluesing-Luerssen. Introduction to skew-polynomial rings and skew-cyclic codes. In *Concise Encyclopedia of Coding Theory*, pages 151–180. 2021.
- [10] A. Hocquenghem. Codes correcteurs d’erreurs. *Chiffers*, 2:147–156, 1959.
- [11] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. Cambridge university press, 2010.
- [12] T.-Y. Lam. A general theory of Vandermonde matrices. *Expositiones Mathematicae*, 4:193–215, 1986.
- [13] T.-Y. Lam and A. Leroy. Vandermonde and Wronskian matrices over division rings. *Journal of Algebra*, 119:308–336, 1988.
- [14] T. Y. Lam and A. Leroy. Wedderburn polynomials over division rings, i. *Journal of Pure and Applied Algebra*, 186(1):43–76, 2004.
- [15] T. Y. Lam, A. Leroy, and A. Ozturk. Wedderburn polynomials over division rings, ii. *Contemporary Mathematics*, 456:73–98, 2008.
- [16] A. Leroy. Noncommutative polynomial maps. *Journal of Algebra and its Applications*, 11(4), 2012.

- [17] R. Lidl and H. Niederreiter. *Finite fields*. Cambridge university press, 1997.
- [18] O. Ore. Theory of non-commutative polynomials. *Annals of mathematics*, 34:480–508, 1933.
- [19] E. Prange. *Cyclic error-correcting codes in two symbols*. Air Force Cambridge Research Center, 1957.
- [20] L. F. Tapia Cuitiño and A. L. Tironi. Some properties of skew codes over finite fields. *Designs, Codes and Cryptography*, 85:359–380, 2017.



## Vita

Kathryn Mae Hechtel

### Place of Birth:

- Houston, TX

### Education:

- University of Kentucky, Lexington, KY  
M.A. in Mathematics, May. 2021
- George Washington University, Washington, D.C.  
B.S. in Mathematics, May. 2019

### Professional Positions:

- Graduate Teaching Assistant, University of Kentucky Fall 2019–  
Spring 2024

### Honors

- Diversity, Equity, and Inclusion Award 2023, University of Kentucky