พหุนามโมนิกลดทอนไม่ได้ส่วนกลับสังยุคในตัวบนฟิลด์จำกัด

นางสาวอรุณวรรณ บริพันธ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2557

SELF-CONJUGATE-RECIPROCAL IRREDUCIBLE MONIC POLYNOMIALS OVER FINITE FIELDS

Miss Arunwan Boripan

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Mathematics
Department of Mathematics and Computer Science
Faculty of Science
Chulalongkorn University
Academic Year 2014

Thesis Title	SELF-CONJUGATE-RECIPROCAL IRREDUCIBLE MONIC POLYNOMIALS OVER FINITE FIELDS
By	Miss Arunwan Boripan
Field of Study	Mathematics
Thesis Advisor	Associate Professor Patanee Udomkavanich, Ph.D.
Thesis Co-Advisor	Somphong Jitman, Ph.D

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree.

.....Dean of the Faculty of Science

(Professor Supot Hannongbua, Dr.rer.nat.)

THESIS COMMITTEE

.....Chairman

(Assistant Professor Sajee Pianskool, Ph.D.)

.....Thesis Advisor

(Associate Professor Patanee Udomkavanich, Ph.D.)

.....Thesis Co-advisor

(Somphong Jitman, Ph.D.)

.....Examiner

(Ouamporn Phuksuwan, Ph.D.)

.....External Examiner

(Tippaporn Eungrasamee, Ph.D.)

อรุณวรรณ บริพันธ์ : พหุนามโมนิกลดทอนไม่ได้ส่วนกลับสังยุคในตัวบนฟิลด์จำกัด (SELF-CONJUAGTE-RECIPROCAL IRREDUCIBLE MONIC POLYNOMIALS OVER FINITE FIELDS) อ. ที่ปรึกษาวิทยานิพนธ์หลัก: รศ.ดร.พัฒนี อุดมกะวานิช, อ. ที่ปรึกษาวิทยานิพนธ์ร่วม: ดร.สมพงค์ จิตต์มั่น, 30 หน้า.

เราศึกษาพหุนามโมนิกลดทอนไม่ได้ส่วนกลับสังยุคในตัว (SCRIM) บนฟิลด์จำกัด พร้อมทั้งให้เงื่อนไขเพียงพอและจำเป็นที่ทำให้พหุนามโมนิกลดทอนไม่ได้เป็น SCRIM ยิ่งไปกว่านั้นเราได้คำนวณจำนวนพหุนาม SCRIM เมื่อกำหนดระดับขั้นให้

ภาควิชา คณิตศาสตร์และวิทยาการคอมพิวเตอร์ ลายมือชื่อนิสิต.....

ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

สาขาวิชา คณิตศาสตร์ ลายมือชื่อ อ.ที่ปรึกษาร่วม .....

ปีการศึกษา 2557

##5672143923 : MAJOR MATHEMATICS
KEYWORDS : ORDER / DEGREE / SCRIM POLYNOMIALS
ARUNWAN BORIPAN : SELF-CONJUGATE-RECIPROCAL
IRREDUCIBLE MONIC POLYNOMIALS OVER FINITE FIELDS.
ADVISOR : ASSOC. PROF. PATANEE UDOMKAVANICH, Ph.D.,
CO-ADVISOR : SOMPHONG JITMAN, Ph.D., 30 pp.

The class of self-conjugate-reciprocal irreducible monic (SCRIM) polynomials over finite fields is studied. Necessary and sufficient conditions for monic irreducible polynomials to be SCRIM are given. The number of SCRIM polynomials of a given degree is also determined.

Department : ...Mathematics and.....	Student's Signature : .....
...Computer Science...	Advisor's Signature : .....
Field of Study : .....Mathematics.....	Co-advisor's Signature : .....
Academic Year : .....2014.....	

ACKNOWLEDGEMENTS

I am deeply grateful to my thesis advisor, Associate Professor Dr. Patanee Udomkavanich, and my thesis co-advisor, Dr. Somphong Jitman, for their invaluable advice and constant encouragement throughout the course of this thesis. I am most grateful for their teaching and advice. I would not have achieved this far and this thesis would not have been completed without all the support that I have always received from them. Sincere thanks are also extended to Assistant Professor Dr. Sajee Pianskool, the chairman, Dr. Ouamporn Phuksuwan and Dr. Tippaporn Eungrasamee, the committee members, for their comments and suggestions.

Special thanks go to the Science Achievement Scholarship of Thailand (SAST) for financial aid to study.

Additionally, I would like to thank my family, my friends and those whose names are not mentioned here but have greatly inspired and encouraged me throughout the period of this research.

CONTENTS

CHAPTER I
INTRODUCTION

Self-reciprocal and self-reciprocal irreducible monic (SRIM) polynomials over finite fields have been studied and applied in various branches of Mathematics and Engineering. SRIM polynomials were used for characterizing and enumerating Euclidean self-dual cyclic codes over finite fields in [3] and for characterizing Euclidean complementary dual cyclic codes over finite fields in [7]. In [2], SRIM polynomials have been characterized up to their degrees. The order and the number of SRIM polynomials of a given degree over finite fields have been determined in [8].

Self-conjugate-reciprocal irreducible monic (SCRIM) polynomials, a generalization of SRIM polynomials, have been used for characterizing Hermitian self-dual cyclic codes in [4]. However, properties of SCRIM polynomials have not been well studied. Therefore, it is of natural interest to characterize and to enumerate such polynomials.

In Chapter II, some useful properties of the minimal polynomial of an element of a finite field and the order of a polynomial over finite field are recalled. Necessary and sufficient conditions for a monic irreducible polynomial to be SRIM are reviewed.

In Chapter III, we investigate SCRIM polynomials. Necessary and sufficient conditions for a monic irreducible polynomial to be SCRIM are given. Moreover, for any possible degrees, the order and the number of SCRIM polynomials over an appropriate finite field have been determined.

In Chapter IV, the definitions and some basic properties of cyclic codes and Hermitian complementary dual cyclic codes are recalled. We apply the results from chapter III to characterize and to enumerate Hermitian complementary dual codes over finite fields.

In Chapter V, remarks on definitions of SRIM and SCRIM polynomials are given.

CHAPTER II
PRELIMINARIES

In Section 2.1, the minimal polynomials of all nonzero elements of a finite field are given via the cyclotomic cosets. They are used for factorizing $x^n - 1$ as a product of monic irreducible polynomials over a given finite field. SRIM polynomials and their characterization are reviewed in Section 2.2.

2.1 Polynomials over Finite Fields and Their Orders

It is well-known that the multiplicative group $\mathbb{F}_q^*$ of a finite field $\mathbb{F}_q$ is cyclic. Its generator is called a *primitive element* of the field. Hence, an element of a finite field is a power of a primitive element of the field and it is a root of the polynomial $x^{q-1} - 1$. It is interesting to determine, for each $a \in \mathbb{F}_q^*$, a nonzero polynomial $f(x) \in \mathbb{F}_q[x]$ of the least degree such that a is a root (*i.e.*, $f(a) = 0$).

Definition 2.1. The *minimal polynomial* of an element $\alpha \in \mathbb{F}_{q^m}$ with respect to $\mathbb{F}_q$ is a nonzero monic polynomial $f(x)$ of the least degree in $\mathbb{F}_q[x]$ such that $f(\alpha) = 0$.

In order to determine the minimal polynomial of each element in $\mathbb{F}_q$, we will start with cyclotomic cosets.

Definition 2.2. Let n and q be positive integers with $\gcd(n, q) = 1$. For each $0 \leq i < n$, the *cyclotomic coset of q modulo n containing i* is defined to be the set

$$Cl_q(i) = \{iq^j \bmod n \mid j \in \mathbb{N}_0\}.$$

The next theorem relates our two previous definitions:

Theorem 2.3 ([6, Theorem 3.4.8]). *Let α be a primitive element of $\mathbb{F}_{q^m}$. Then the minimal polynomial of α^i with respect to $\mathbb{F}_q$ is*

$$M_{\mathbb{F}_q}^{(i)}(x) = \prod_{j \in Cl_q(i)} (x - \alpha^j),$$

where $Cl_q(i)$ is the cyclotomic coset of q modulo $q^m - 1$ containing nonnegative integer i.

For any polynomial $f(x)$ over $\mathbb{F}_q$, $f(x)$ divides $x^n - 1$ for some positive integer n. The smallest of such integers is called the *order* of $f(x)$, denoted by $\mathrm{ord}(f(x))$.

Remark 2.4. *It is well-known that if $f(x)$ is an irreducible polynomial over $\mathbb{F}_q$, then $f(x)$ divides $x^{\mathrm{ord}(f(x))} - 1$. Moreover, $x^{\mathrm{ord}(f(x))} - 1 = \prod_{i=1}^{t} M_{\mathbb{F}_q}^{(i)}(x)$, where t is the cardinality of the complete set of representative of cyclotomic cosets of q modulo $\mathrm{ord}(f(x))$ [6, Theorem 3.4.11]. It follows that any irreducible polynomials over $\mathbb{F}_q$ can be viewed as $M_{\mathbb{F}_q}^{(i)}(x)$ for some i.*

Remark 2.5. *$M_{\mathbb{F}_q}^{(i)}(x)$ in Theorem 2.3 will be referred to as a minimal polynomial defined corresponding to $Cl_q(i)$. It plays an important role later since a monic irreducible polynomial over $\mathbb{F}_q$ can be viewed as the minimal polynomial of an element in an extension field of $\mathbb{F}_q$.*

Example 2.1. Let α be a primitive element of $\mathbb{F}_{16}$. To determine the minimal polynomial over $\mathbb{F}_2$ of α^3, we begin with computing the cyclotomic cosets of 2 modulo 15.

$Cl_2(0) = \{0\}, Cl_2(1) = \{1, 2, 4, 8\}, Cl_2(3) = \{3, 6, 9, 12\}, Cl_2(5) = \{5, 10\},$
$Cl_2(7) = \{7, 11, 13, 14\}$.

By Theorem 2.3, $M_{\mathbb{F}_2}^{(3)}(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12}) = x^4+x^3+x^2+x+1$.

Next theorem gives the factorization of $x^n - 1$ as a product of irreducible polynomials over the finite field of interest.

Theorem 2.6 ([6, Theorem 3.4.11]). *Let n and q be positive integer with $\gcd(q, n) = 1$. Let $m \in \mathbb{N}$ satisfy $n|(q^m - 1)$ and α be a primitive element of $\mathbb{F}_{q^m}$ and let $M_{\mathbb{F}_q}^{(j)}(x)$*

be the minimal polynomial of α^j with respect to $\mathbb{F}_q$. Let $\{s_1, s_2, \ldots, s_t\}$ be a complete set of representatives of cyclotomic cosets of q modulo n. Then the polynomial $x^n - 1$ has a factorization into monic irreducible polynomials over $\mathbb{F}_q$ of the form

$$x^n - 1 = \prod_{i=1}^{t} M_{\mathbb{F}_q}^{\left(\frac{(q^m-1)s_i}{n}\right)}(x).$$

Example 2.2. We will factor $x^{21} - 1$ over $\mathbb{F}_2$. Since 21 is a divisor of $(2^6 - 1)$, we consider the field $\mathbb{F}_{64}$. The cyclotomic cosets of 2 modulo 63 containing $0, 3, 9, 15, 21$ and 27 are as follows:

$$\begin{aligned} &Cl_2(0) = \{0\}, && Cl_2(3) = \{3, 6, 12, 24, 48, 33\}, \\ &Cl_2(9) = \{9, 18, 36\}, && Cl_2(15) = \{15, 30, 60, 57, 51, 39\}, \\ &Cl_2(21) = \{21, 42\}, && Cl_2(27) = \{27, 54, 45\}. \end{aligned}$$

By Theorem 2.6, $x^{21} - 1 = M_{\mathbb{F}_2}^{(1)}(x) M_{\mathbb{F}_2}^{(3)}(x) M_{\mathbb{F}_2}^{(9)}(x) M_{\mathbb{F}_2}^{(15)} M_{\mathbb{F}_2}^{(21)} M_{\mathbb{F}_2}^{(27)}$, where

$$\begin{aligned} M_{\mathbb{F}_2}^{(1)}(x) &= x - 1, \\ M_{\mathbb{F}_2}^{(3)}(x) &= \prod_{j \in Cl_2(3)} (x - \alpha^j) = 1 + x^2 + x^4 + x^5 + x^6, \\ M_{\mathbb{F}_2}^{(9)}(x) &= \prod_{j \in Cl_2(9)} (x - \alpha^j) = 1 + x + x^3, \\ M_{\mathbb{F}_2}^{(15)}(x) &= \prod_{j \in Cl_2(15)} (x - \alpha^j) = 1 + x + x^2 + x^4 + x^6, \\ M_{\mathbb{F}_2}^{(21)}(x) &= \prod_{j \in Cl_2(21)} (x - \alpha^j) = 1 + x + x^2 \text{ and} \\ M_{\mathbb{F}_2}^{(27)}(x) &= \prod_{j \in Cl_2(27)} (x - \alpha^j) = 1 + x^2 + x^3. \end{aligned}$$

The order of $f(x)$ has been used for studying self-reciprocal irreducible polynomials over finite fields in [7]. It will be our important tool for investigating self-conjugate-reciprocal irreducible polynomials in the next chapter as well. The

property of the order of an irreducible polynomial has been mentioned in [7] without proof. For completeness, the proof is given now.

Lemma 2.7. *If $f(x)$ is an irreducible polynomial of degree n over $\mathbb{F}_q$, then* $\mathrm{ord}(f(x))$ *is the order of any root of $f(x)$ in the multiplicative group $\mathbb{F}_{q^n}^*$.*

Proof. Let α be a root of $f(x)$ in $\mathbb{F}_{q^n}^*$. For convenience, denote by $\mathrm{o}(\alpha)$ the order of α, the smallest positive integer t such that $\alpha^t = 1$. Then the distinct roots of $f(x)$ are $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$. Since $f(\alpha) = 0$ and $f(x)|(x^{\mathrm{ord}(f(x))} - 1)$, we have $\alpha^{\mathrm{ord}(f(x))} - 1 = 0$. Then $\mathrm{o}(\alpha)|\mathrm{ord}(f(x))$. Since $\mathrm{o}(\alpha)|(q^n - 1)$ and $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is the set of distinct roots of $f(x)$, we have $(x-\alpha^{q^i})|(x^{\mathrm{o}(\alpha)}-1)$ for all $i = 0, \ldots, n-1$.

Then $f(x) = \prod_{i=0}^{n-1}(x - \alpha^{q^i})$ is a divisor of $x^{\mathrm{o}(\alpha)} - 1$. Therefore, $\mathrm{ord}(f(x)) = \mathrm{o}(\alpha)$. □

2.2 SRIM Polynomials over Finite Fields

In this section, we review the results of SRIM polynomials. For more details, please see [8].

Let $f(x) = f_0 + f_1 x + \cdots + f_n x^n$ be a polynomial in $\mathbb{F}_q[x]$ with $f_0 \neq 0$ and $f_n \neq 0$. The *reciprocal polynomial* of $f(x)$, denoted by $f^*(x)$, is defined by $f^*(x) := x^n f_0^{-1} f\left(\frac{1}{x}\right)$. $f(x)$ is said to be *self-reciprocal* if $f(x) = f^*(x)$. If, in addition, $f(x)$ is monic and irreducible, $f(x)$ is refered to as a self-reciprocal irreducible monic (SRIM) polynomial.

Next lemma gives a relationship between a root of a polynomial and a root of its reciprocal.

Lemma 2.8 ([8])**.** *Let α be an element in an extension field of $\mathbb{F}_q$ and let $f(x) \in \mathbb{F}_q[x]$. Then α is a root of $f(x)$ if and only if α^{-1} is a root of $f^*(x)$.*

Proof. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}_q[x]$ and α be an element in an extension

field of $\mathbb{F}_q$. Then

$$\begin{aligned} f^*(\alpha^{-1}) &= \alpha^{-n} a_0^{-1} f(\frac{1}{\alpha^{-1}}) \\ &= \alpha^{-n} a_0^{-1} f(\alpha). \end{aligned}$$

Hence, the proof is complete. □

Next proposition gives a characterization of a SRIM polynomial. By Remark 2.5, it suffices to focus on $M_{\mathbb{F}_q}^{(i)}(x)$.

Proposition 2.9. *Let $M_{\mathbb{F}_q}^{(i)}(x)$ be a monic irreducible polynomial defined corresponding to $Cl_q(i)$. Then $M_{\mathbb{F}_q}^{(i)}(x)$ is self-reciprocal if and only if $Cl_q(i) = Cl_q(-i)$.*

Proof. Assume $M_{\mathbb{F}_q}^{(i)}(x) = M_{\mathbb{F}_q}^{*(i)}(x)$. Let α be a primitive element in an extension field of $\mathbb{F}_q$. Then α^i is a root of $M_{\mathbb{F}_q}^{*(i)}(x)$. Since $Cl_q(-i)$ is a class corresponding to $M_{\mathbb{F}_q}^{*(i)}(x)$, by Theorem 2.3, $i \in Cl_q(-i)$. Hence,

$$Cl_q(i) = Cl_q(-i).$$

Conversely, assume $Cl_q(i) = Cl_q(-i)$. Then

$$\begin{aligned} M_{\mathbb{F}_q}^{(i)}(x) &= \prod_{j \in Cl_q(i)} (x - \alpha^j), \\ &= \prod_{j \in Cl_q(-i)} (x - \alpha^j), \\ &= \prod_{j \in Cl_q(i)} (x - \alpha^{-j}). \end{aligned}$$

Since α^{-j} is a root of $M_{\mathbb{F}_q}^{(i)}(x)$ for all $j \in Cl_q(i)$, it follows that α^j is a root of $M_{\mathbb{F}_q}^{*(i)}(x)$ for all $j \in Cl_q(i)$. Therefore, $M_{\mathbb{F}_q}^{(i)}(x) = M_{\mathbb{F}_q}^{*(i)}(x)$ as desired. □

Example 2.3. The cyclotomic cosets of 3 modulo 8 are $Cl_3(0) = \{0\}$, $Cl_3(1) = \{1, 3\}$, $Cl_3(2) = \{2, 6\}$, $Cl_3(4) = \{4\}$ and $Cl_3(5) = \{5, 7\}$. Then, we have $Cl_3(2) = Cl_3(-2)$. Let α be a root of $2x^2 + 2x + 1$. We verify that α is a primitive element

of $\mathbb{F}_9$. Consider the minimal polynomial corresponding to $Cl_3(2)$, we have

$$\begin{aligned} M^{(2)}_{\mathbb{F}_3}(x) &= \prod_{j \in Cl_3(2)} (x - \alpha^j) \\ &= (x - \alpha^2)(x - \alpha^6) \\ &= x^2 + 1. \end{aligned}$$

Since $Cl_3(2) = Cl_3(-2)$, by Theorem 2.9,

$$M^{*(2)}_{\mathbb{F}_3}(x) = M^{(2)}_{\mathbb{F}_3}(x).$$

Hence, the minimal polynomial corresponding to $Cl_3(2)$ is a SRIM polynomial.

The next theorem has been mentioned in [8] without proof. Hence, we provide a proof of the theorem.

Theorem 2.10 ([8])**.** *If an irreducible polynomial $f(x)$ is a SRIM polynomial, then the degree of $f(x)$ must be 1 or even.*

Proof. Let $f(x)$ be a SRIM polynomial of degree n defined corresponding to $Cl_q(i)$. Suppose $n \neq 1$. Then, by Proposition 2.9, we have $Cl_q(i) = Cl_q(-i)$ and $|Cl_q(i)| = n > 1$. Then there exists $0 \leq j < n$ such that

$$\begin{aligned} -i &\equiv iq^j \bmod n \\ &\equiv (-iq^j)q^j \bmod n. \end{aligned}$$

It follows that $1 \equiv q^{2j} \bmod n$. Hence,

$$n | 2j.$$

Then,

$$n \leq 2j < 2n.$$

Hence, $n = 2j$ which is even. $\square$

CHAPTER III
SELF-CONJUGATE-RECIPROCAL IRREDUCIBLE POLYNOMIALS

In this chapter, we investigate SCRIM polynomials, a generalization of SRIM polynomials.

Let $f(x) = f_0 + f_1x + \cdots + f_nx^n$ be a polynomial of degree n over $\mathbb{F}_{q^2}$ with $f_0 \neq 0$. The *conjugate* of a polynomial $f(x) = \sum_{i=0}^{n} f_ix^i$ over $\mathbb{F}_{q^2}$ is defined to be $\overline{f(x)} = \overline{f_0}+\overline{f_1}x+\cdots+\overline{f_n}x^n$, where $\bar{}: \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ is defined by $\alpha \mapsto \alpha^q$ for all $\alpha \in \mathbb{F}_{q^2}$. The polynomial $f(x)$ over $\mathbb{F}_{q^2}$ (with $f(0) \neq 0$) is said to be *self-conjugate-reciprocal* if $f(x)$ equals its *conjugate-reciprocal polynomial* $f^\dagger(x) := \overline{f^*(x)}$. If, in addition, $f(x)$ is monic and irreducible, it is said to be *self-conjugate-reciprocal irreducible monic (SCRIM)*. SCRIM polynomials have been used for characterizing Hermitian self-dual cyclic codes in [4]. However, the properties of SCRIM polynomials have not been well studied. Therefore, it is of natural interest to characterize and to enumerate such polynomials.

We begin with giving a relationship between roots of $f(x)$ and $f^\dagger(x)$.

Lemma 3.1. *Let α be an element in an extension field of $\mathbb{F}_{q^2}$ and let $f(x) \in \mathbb{F}_{q^2}[x]$. Then α is a root of $f(x)$ if and only if α^{-q} is a root of $f^\dagger(x)$.*

Proof. Let $f(x) = a_0 + a_1(x) + \cdots + a_nx^n$. Then

$$\begin{aligned} f^\dagger(\alpha^{-q}) &= \alpha^{-qn}a_0^{-q}(a_0^q + \frac{a_1^q}{\alpha^{-q}} + \cdots + \frac{a_n^q}{\alpha^{-qn}}) \\ &= \alpha^{-qn}a_0^{-q}(a_0 + a_1\alpha + \cdots + a_n\alpha^n)^q \\ &= \alpha^{-qn}a_0^{-q}(f(\alpha))^q. \end{aligned}$$

Therefore, α is a root of $f(x)$ if and only if α^{-q} is a root of $f^\dagger(x)$. □

Next lemma gives necessary and sufficient conditions for an irreducible polynomial to be SCRIM. By Remark 2.5, it suffices to concentrate on $M^{(i)}_{\mathbb{F}_{q^2}}(x)$.

Proposition 3.2. *$M^{(i)}_{\mathbb{F}_{q^2}}(x)$ is self-conjugate-reciprocal if and only if $Cl_{q^2}(i) = Cl_{q^2}(-qi)$.*

Proof. Assume $M^{(i)}_{\mathbb{F}_{q^2}}(x) = M^{\dagger(i)}_{\mathbb{F}_{q^2}}(x)$. Then α^i is a root of $M^{\dagger(i)}_{\mathbb{F}_{q^2}}(x)$. Since $Cl_{q^2}(-qi)$ is a class corresponding to $M^{\dagger(i)}_{\mathbb{F}_{q^2}}(x)$. By Theorem 2.3, we have $i \in Cl_{q^2}(-qi)$. Hence,

$$Cl_{q^2}(i) = Ci_{q^2}(-qi).$$

Conversely, assume that $Cl_{q^2}(i) = Cl_{q^2}(-qi)$. Then

$$\begin{aligned} M^{(i)}_{\mathbb{F}_{q^2}}(x) &= \prod_{j \in Cl_{q^2}(i)} (x - \alpha^j) \\ &= \prod_{j \in Cl_{q^2}(-qi)} (x - \alpha^j) \\ &= \prod_{j \in Cl_{q^2}(i)} (x - \alpha^{-qj}). \end{aligned}$$

Since α^{-qj} is a root of $M^{(i)}_{\mathbb{F}_{q^2}}(x)$ for all $j \in Cl_{q^2}(i)$, it follows that α^j is a root of $M^{\dagger(i)}_{\mathbb{F}_{q^2}}(x)$ for all $j \in Cl_{q^2}(-qi)$. Therefore, $M^{(i)}_{\mathbb{F}_{q^2}}(x) = M^{\dagger(i)}_{\mathbb{F}_{q^2}}(x)$ as desired. □

Example 3.1. The cyclotomic cosets of 4 modulo 63 are

$$\begin{aligned} &Cl_4(0) = \{0\}, && Cl_4(1) = \{1, 4, 16\}, \\ &Cl_4(2) = \{2, 8, 32\}, && Cl_4(3) = \{3, 12, 48\}, \\ &Cl_4(5) = \{5, 20, 17\}, && Cl_4(6) = \{6, 24, 33\}, \\ &Cl_4(7) = \{7, 28, 49\}, && Cl_4(9) = \{9, 36, 18\}, \\ &Cl_4(10) = \{10, 40, 34\}, && Cl_4(11) = \{11, 44, 50\}, \\ &Cl_4(13) = \{13, 52, 19\}, && Cl_4(14) = \{14, 56, 35\}, \\ &Cl_4(15) = \{15, 60, 51\}, && Cl_4(21) = \{21\}, \end{aligned}$$

$$
\begin{aligned}
&Cl_4(22) = \{22, 25, 37\}, \quad Cl_4(23) = \{23, 29, 53\},\\
&Cl_4(26) = \{26, 41, 38\}, \quad Cl_4(27) = \{27, 45, 54\},\\
&Cl_4(30) = \{30, 57, 39\}, \quad Cl_4(42) = \{42\},\\
&Cl_4(43) = \{43, 46, 58\}, \quad Cl_4(47) = \{47, 62, 59\} \text{ and}\\
&Cl_4(61) = \{61, 55, 31\}.
\end{aligned}
$$

Since $Cl_4(7) = Cl_4((-2)7)$, $Cl_4(14) = Cl_4((-2)14)$, $Cl_4(21) = Cl_4((-2)21)$ and $Cl_4(42) = Cl_4((-2)42)$, we have that $M^{(7)}_{\mathbb{F}_4}(x) = (x - \alpha^7)(x - \alpha^{28})(x - \alpha^{49})$, $M^{(14)}_{\mathbb{F}_4}(x) = (x-\alpha^{14})(x-\alpha^{56})(x-\alpha^{35})$, $M^{(21)}_{\mathbb{F}_4}(x) = (x-\alpha^{21})$ and $M^{(42)}_{\mathbb{F}_4}(x) = (x-\alpha^{42})$ are SCRIM.

Theorem 3.3. *The degree of a SCRIM polynomial must be odd.*

Proof. Assume that $M^{(i)}_{\mathbb{F}_{q^2}}(x)$ has degree t. If $t = 1$, then the degree of $M^{(i)}_{\mathbb{F}_{q^2}}(x)$ is odd. Suppose $t \neq 1$. Then, by Proposition 3.2, we have $Cl_{q^2}(i) = Cl_{q^2}(-qi)$ and $|Cl_{q^2}(i)| = t > 1$. Then there exists $0 \leq j < t$ such that

$$i \equiv (-qi)q^{2j} \bmod t.$$

It follows that

$$
\begin{aligned}
-qi &\equiv (-q)(-qi)q^{2j} \bmod t\\
&\equiv iq^{2j+2} \bmod t,
\end{aligned}
$$

and hence,

$$
\begin{aligned}
i &\equiv iq^{2j+2}q^{2j} \bmod t\\
&\equiv iq^{2(2j+1)} \bmod t.
\end{aligned}
$$

It follows that

$$t|(2j + 1).$$

Then $t \leq 2j+1 < 2t$. Hence, $t = 2j+1$ which is odd. $\square$

Next, we determine the number of SCRIM polynomials of degree 1.

Proposition 3.4. *There are $q+1$ SCRIM polynomials of degree 1 over $\mathbb{F}_{q^2}$.*

Proof. Let $f(x)$ be a polynomial of degree 1 over $\mathbb{F}_{q^2}$. Then $f(x) = x + a$ for some $a \in \mathbb{F}_{q^2}$. Thus $f^\dagger(x) = x + a^{-q}$. The polynomial $f(x)$ is SCRIM if and only if $a = a^{-q}$. Equivalently, $a^{q+1} = 1$.

Since $(q+1)||\mathbb{F}_{q^2}^*|$ and $\mathbb{F}_{q^2}^*$ is a cyclic group, there exists a unique subgroup H of order $q+1$ of $\mathbb{F}_{q^2}^*$. Clearly, $a^{q+1} = 1$ if and only if $a \in H$. Hence, the number of SCRIM polynomials of degree 1 over $\mathbb{F}_{q^2}$ is $q+1$. $\square$

Example 3.2. By Proposition 3.4, there are 6 SCRIM polynomials of degree 1 over $\mathbb{F}_{25}$. In order to list all of them, we assume that $\mathbb{F}_{25}^* = \langle \alpha \rangle$. It can be easily seen that $1^6 = 1 = (\alpha^4)^6 = (\alpha^8)^6 = (\alpha^{12})^6 = (\alpha^{16})^6 = (\alpha^{20})^6$.

Hence, all SCRIM polynomials of degree 1 over $\mathbb{F}_{25}$ are $x+1$, $x+\alpha^4$, $x+\alpha^8$, $x+\alpha^{12}$, $x+\alpha^{16}$ and $x+\alpha^{20}$.

From now on, we assume that the polynomials have odd degree $n \geq 3$. We determine the number of SCRIM polynomials of degree $n \geq 3$ by using the orders of SCRIM polynomials of degree n over $\mathbb{F}_{q^2}$. The following three lemmas are important tools for determining the orders of SCRIM polynomials.

Lemma 3.5 ([8, Proposition 2])**.** *Suppose a, r and k are positive integers with r even. If a divides $q^r - 1$ and a divides $q^k + 1$, then a divides $q^{r/2^s} + 1$ for some positive integer s.*

Lemma 3.6 ([8, Proposition 1])**.** *Let a be a positive integer with $a > 2$. If m is the smallest positive integer such that a divides $q^m + 1$, then, for any positive integer s, the following statements hold.*

(i) a divides $q^s + 1$ if and only if s is an odd multiple of m.

(ii) a divides $q^s - 1$ if and only if s is an even multiple of m.

Lemma 3.7. *Let $f(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_{q^2}$ and $\alpha \in \mathbb{F}_{q^{2n}}$ be a root of $f(x)$. If k divides n and $\mathrm{o}(\alpha)$ divides q^k+1, then $k=n$.*

Proof. Since $\mathrm{o}(\alpha)$ divides q^k+1, $\mathrm{o}(\alpha)$ divides $q^{2k}-1$. Hence $\alpha \in \mathbb{F}_{q^{2k}}$. Let $f(x) = \prod_{i=0}^{n-1}(x-\alpha^{q^{2i}}) = g(x)h(x)$ where $g(x) = \prod_{i=0}^{k-1}(x-\alpha^{q^{2i}})$ and $h(x) = \prod_{i=k}^{n-1}(x-\alpha^{q^{2i}})$.

For $1 \leq j \leq n-1$, let $T_j : \mathbb{F}_{q^{2k}} \to \mathbb{F}_{q^2}$ be the *j-th* trace map defined for $\alpha \in \mathbb{F}_{q^{2k}}$ by

$$T_j(\alpha) = \sum_{0 \leq i_1 \leq i_2 \leq \cdots \leq i_j \leq k-1} \alpha^{q^{2i_1}} \alpha^{q^{2i_2}} \ldots \alpha^{q^{2i_j}}.$$

$T_j(\alpha)$ is the coefficient of x^{k-1-j} of $g(x)$. It follows that $g(x) \in \mathbb{F}_{q^2}[x]$. Moreover, $h(x) \in \mathbb{F}_{q^2}$. If $k < n$, then $f(x)$ is reducible. This is a contradiction.

□

Lemma 3.8. *If $f(x)$ is an irreducible polynomial of degree n over $\mathbb{F}_{q^2}$, then $\mathrm{ord}(f(x))$ is the order of any root of $f(x)$ in the multiplicative group $\mathbb{F}^*_{q^{2n}}$.*

Proof. Let α be a root of $f(x)$ in $\mathbb{F}^*_{q^{2n}}$. For convenience, denoted by $\mathrm{o}(\alpha)$, the order of α, is defined to be the smallest positive integer t such that $\alpha^t = 1$. Then the set of all distinct roots of $f(x)$ is $\{\alpha, \alpha^{q^2}, \ldots, \alpha^{q^{2(n-1)}}\}$. Since $f(\alpha) = 0$ and $f(x) | (x^{\mathrm{ord}(f(x))} - 1)$, we have $\alpha^{\mathrm{ord}(f(x))} - 1 = 0$. Then $\mathrm{o}(\alpha) | \mathrm{ord}(f(x))$. Since $\mathrm{o}(\alpha) | q^n - 1$ and $\{\alpha, \alpha^{q^2}, \ldots, \alpha^{q^{2n-1}}\}$ is the set of all distinct roots of $f(x)$, we have $(x - \alpha^{q^{2(i)}}) | x^{\mathrm{o}(\alpha)} - 1$ for all $i = 0, \ldots, n-1$.

Then $f(x) = \prod_{i=0}^{n-1}(x - \alpha^{q^{2i}})$. Therefore, $\mathrm{ord}(f(x)) | \mathrm{o}(\alpha)$. □

Let D_n be the set of all positive divisors of q^n+1 which do not divide q^k+1 for all $0 \leq k < n$.

Proposition 3.9. *Let $f(x)$ be a SCRIM polynomial of degree n over $\mathbb{F}_{q^2}$. Then $\mathrm{ord}(f(x)) \in D_n$. Moreover, if $\alpha \in \mathbb{F}_{q^{2n}}$ is a root of $f(x)$, then α is a primitive d-th root of unity for some $d \in D_n$.*

Proof. Let $\alpha \in \mathbb{F}_{q^{2n}}$ be a root of $f(x)$. Since $f(x)$ is SCRIM, by Lemma 3.1, $f(\frac{1}{\alpha^q}) = 0$ and we may write $\frac{1}{\alpha^q} = \alpha^{q^{2t}}$ for some positive integer t. Then $\alpha^{q^{2t}+q} = 1$

and thus $\mathrm{o}(\alpha)$ divides $q^{2t}+q$. Since $\gcd(q, \mathrm{o}(\alpha)) = 1$, we have $\mathrm{o}(\alpha)|(q^{2t-1}+1)$. Since $\alpha \in \mathbb{F}_{q^{2n}}$, $\mathrm{o}(\alpha)$ divides $q^{2n}-1$. By Lemma 3.5, we have that $\mathrm{o}(\alpha)$ divides $q^{2n/2^s}+1$ for some positive integer s. Since n is odd, it follows that $s = 1$. Then $\mathrm{o}(\alpha)|(q^n+1)$.

Let t be the smallest nonnegative integer such that $\mathrm{o}(\alpha)|(q^t+1)$. Since $\deg(f(x)) \geq 3$, we have $\mathrm{o}(\alpha) \geq 3$, and hence, $t \geq 1$. By Lemma 3.6, n is an odd multiple of t. Using Lemma 3.7, we have $n = t$. Therefore, $\mathrm{o}(\alpha) \nmid (q^k+1)$ for all $0 \leq k < n$. Hence, by Lemma 3.8, $\mathrm{ord}(f(x)) = \mathrm{o}(\alpha) \in D_n$. From this, it implies that α is a primitive *d-th* root of unity for some $d \in D_n$. □

The following corollary is key to prove the next proposition.

Corollary 3.10. *Let $f(x)$ be a SCRIM polynomial of degree n over $\mathbb{F}_{q^2}$. If α be a primitive element of $\mathbb{F}_{q^{2n}}$ and α^j is a root of $f(x)$, then*

$$\mathrm{ord}(f(x)) = \frac{q^{2n}-1}{\gcd(q^{2n}-1, j)}.$$

Proof. Let α be a primitive element of $\mathbb{F}_{q^{2n}}$ and α^j be a root of $f(x)$. Then

$$\mathrm{o}(\alpha^j) = \frac{q^{2n}-1}{\gcd(q^{2n}-1, j)}.$$

From Lemma 3.8, we know that if $f(x)$ is an irredeucible polynomial of degree n, then $\mathrm{ord}(f(x))$ is the order of any root of $f(x)$ in the multiplicative group $\mathbb{F}^*_{q^{2n}}$. Then $\mathrm{o}(\alpha^j) = \mathrm{ord}(f(x))$. Hence, $\mathrm{ord}(f(x)) = \mathrm{o}(\alpha^j) = \dfrac{q^{2n}-1}{\gcd(q^{2n}-1, j)}$. □

Proposition 3.11. *If $d \in D_n$ and β is a primitive d-th root of unity, then the set $\{\beta, \beta^{q^2}, \ldots, \beta^{q^{2(n-1)}}\}$ is a collection of n distinct primitive d-th roots of unity.*

Proof. Since $d|(q^n+1)$, we have $d|(q^{2n}-1)$. Let $0 \leq i \leq n-1$. From $d|(q^{2n}-1)$, it follows that $\gcd(d, q^{2i}) = 1$ and $\beta^{q^{2i}}$ is a primitive *d-th* root of unity. If $\beta^{q^{2i}} = \beta^{q^{2j}}$ for some $0 \leq i < j \leq n-1$, then $\beta^{q^{2i}-q^{2j}} = 1$ so that d divides $q^{2i}-q^{2j} = q^{2i}(q^{2(j-i)}-1)$. Since $\gcd(d, q^{2i}) = 1$, we see that d divides $q^{2(j-i)}-1$. Hence, by Lemma 3.6, $2(j-i) = kn$ for some even positive integer k. But then $j = \dfrac{kn}{2}+i \geq n$, a contradiction. Hence, $\beta^{q^{2i}}$ for $0 \leq i \leq n-1$ are all distinct. □

Let $d \in D_n$ and let β be a primitive *d-th* root of unity over $\mathbb{F}_{q^2}$. Define the polynomial $f_\beta(x) = \prod_{i=0}^{n-1}(x - \beta^{q^{2i}})$.

Proposition 3.12. *$f_\beta(x)$ is a SCRIM polynomial of degree n and order d.*

Proof. Using the definition of $f_\beta(x)$ and the fact that n is odd, we have

$$\begin{aligned} f_\beta^\dagger(x) &= \prod_{i=0}^{n-1}(x - \beta^{q^{2i}})^\dagger \\ &= \prod_{i=0}^{n-1}\left(x(-\beta^{q^{2i}})^{-q}(\frac{1}{x} - \beta^{q^{2i+1}})\right) \\ &= \prod_{i=0}^{n-1}(-\beta^{-q^{2i+1}})\prod_{i=0}^{n-1}(1 - \beta^{q^{2i+1}}x) \\ &= \prod_{i=0}^{n-1}(-\beta^{-q^{2i+1}})\prod_{i=0}^{n-1}\beta^{q^{2i+1}}\prod_{i=0}^{n-1}(\beta^{-q^{2i+1}} - x) \\ &= \prod_{i=0}^{n-1}(x - \beta^{-q^{2i+1}}). \end{aligned} \tag{3.1}$$

We claim that $\{\beta^{q^{2j}} \mid 0 \le j \le n-1\} = \{\beta^{-q^{2i+1}} \mid 0 \le i \le n-1\}$.

Let $\beta^{-q^{2s+1}} \in \{\beta^{-q^{2i+1}} \mid 0 \le i \le n-1\}$. Then

$$\beta^{-q^{2s+1}} = \beta^{q^{2s}(-q)} = (\beta^{-q})^{q^{2s}} = (\beta^{q^{n+1}})^{q^{2s}} = \beta^{q^{n+1+2s}}.$$

Since n is odd, we have $\beta^{-q^{2s+1}} = \beta^{q^{2l}}$ for some $0 \le l \le n-1$. Hence, $\beta^{-q^{2s+1}} \in \{\beta^{q^{2j}} \mid 0 \le j \le n-1\}$.

Let $\beta^{q^{2i}} \in \{\beta^{q^{2j}} \mid 0 \le j \le n-1\}$. Since n is odd, we have

$$\beta^{q^{2i}} = \beta^{q^{n+1+2s}} = (\beta^{q^{n+1}})^{q^{2s}} = (\beta^{-q})^{q^{2s}} = \beta^{q^{2s}(-q)} = \beta^{-q^{2s+1}}$$

for some $0 \le s \le n-1$. Hence, $\beta^{q^{2i}} \in \{\beta^{-q^{2i+1}} \mid 0 \le i \le n-1\}$. Therefore, $\{\beta^{q^{2j}} \mid 0 \le j \le n-1\} = \{\beta^{-q^{2i+1}} \mid 0 \le i \le n-1\}$ as desired.

From (3.1) and the fact that $\{\beta^{q^{2j}} \mid 0 \le j \le n-1\} = \{\beta^{-q^{2i+1}} \mid 0 \le i \le n-1\}$,

we have

$$\begin{aligned} f_\beta^\dagger(x) &= \prod_{i=0}^{n-1}(x - \beta^{-q^{2i+1}}) \\ &= \prod_{j=0}^{n-1}(x - \beta^{q^{2j}}) \\ &= f_\beta(x). \end{aligned}$$

Suppose that $f_\beta(x)$ is written as $f_\beta(x) = g(x)h(x)$, where $g(x)$ is an irreducible monic polynomial of degree r and $h(x)$ is a monic polynomial of degree $n - r$. Let α be a root of $g(x)$. Then

$$\alpha^{q^{2r}-1} = 1.$$

Since α is a root of $f_\beta(x)$, α is a *d-th* root of unity. Hence,

$$d|(q^{2r} - 1).$$

Since d divides $q^n + 1$, by Lemma 3.6, $2r$ is an even multiple of n. Since $r \leq n$, we have $r = n$ and $f_\beta(x) = g(x)$ is irreducible. □

The construction of a SCRIM polynomial $f_\beta(x)$ can be illustrate as follows.

Example 3.3. Let $n = 3$ and $q = 3$. Then $D_3 = \{7, 14, 28\}$. Assume that $\mathbb{F}_{729}^* = \langle\alpha\rangle$. Since the set $\{\alpha^{52}, \alpha^{468}, \alpha^{572}\}$ is a collection of 3 distinct primitive 14-*th* roots of unity, it follows that

$$f_{\alpha^{52}}(x) = f_{\alpha^{468}}(x) = f_{\alpha^{572}}(x) = (x - \alpha^{52})(x - \alpha^{468})(x - \alpha^{572}).$$

By Proposition 3.12, $f_{\alpha^{52}}(x)$ is a SCRIM polynomial.

Lemma 3.13 ([5, Theorem 2.45])**.** *Let $\mathbb{F}$ be a field of characteristic p, n be a positive integer not divisible by p, and ζ be a primitive d-th root of unity over $\mathbb{F}$.*

Then

$$x^n - 1 = \prod_{d|n} Q_d(x), \tag{3.2}$$

where $Q_d(x) = \prod_{s=1,\ \gcd(s,d)=1}^{n} (x - \zeta^s)$.

Note that $Q_d(x)$ can be viewed as

$$Q_d(x) = \prod_{\eta \in D} (x - \eta),$$

where D is the set of all primitive *d-th* roots of unity over $\mathbb{F}$.

Lemma 3.14 ([5, Theorem 2.47])**.** *The splitting field of* $x^n - 1$ *over a field* $\mathbb{F}_q$ *with* $\gcd(q, n) = 1$*,* $Q_n(x)$ *factors into* $\frac{\phi(n)}{d}$ *distinct monic irreducible polynomial over* $\mathbb{F}_q$ *of the same degree* d *where* d *is the least positive integer such that* $q^d \equiv 1 \bmod n$*.*

Theorem 3.15. *Let* $f(x)$ *be an irreducible monic polynomial of degree* n *over* $\mathbb{F}_{q^2}$*. Then the following statements are equivalent:*

(i) $f(x)$ *is self-conjugate-reciprocal,*

(ii) $\mathrm{ord}(f(x)) \in D_n$*,*

(iii) $f(x) = f_\beta(x)$ *for some primitive d-th root of unity* β *with* $d \in D_n$*.*

Proof. By Corollary 3.10 and Proposition 3.12, it remains to prove (ii) implies (iii). Assume $\mathrm{ord}(f(x)) \in D_n$. Let p be the characteristic of $\mathbb{F}_{q^2}$. Since $\gcd(p, \mathrm{ord}(f(x))) = 1$, by Lemma 3.13, we have $x^{\mathrm{ord}(f(x))} - 1 = \prod_{\ell|\mathrm{ord}(f(x))} Q_\ell(x)$. Since $f(x)|(x^{\mathrm{ord}(f(x))} - 1)$, we have $f(x)|Q_d(x)$ for some divisor d of $\mathrm{ord}(f(x))$. Then $d|(q^n + 1)$.

We claim that $d \in D_n$. Suppose $d|(q^k + 1)$ for some $k < n$. Then $d|(q^{2k} - 1)$, *i.e.*, $q^{2k} \equiv 1 \mod d$. From Lemma 3.14, n is the smallest positive integer such that $q^{2n} \equiv 1 \mod d$. Since $k < n$, we have a contradiction. Therefore, $d \in D_n$.

Let γ be a primitive *d-th* root of unity over $\mathbb{F}_{q^2}$. Since $q^{2n} \equiv 1 \mod d$ and $q^{2k} \not\equiv 1 \mod d$, for all $0 \le k < n$, it follows that $\gamma \in \mathbb{F}_{q^{2n}}$ but $\gamma \notin \mathbb{F}_{q^{2k}}$ for

all $0 \leq k < n$. Then the minimal polynomial of γ has degree n. Since $f(x)$ is irreducible and $f(x)|Q_d(x)$, there exists a primitive *d-th* root of unity δ such that its minimal polynomial equals $f(x)$.

Finally, we show that $f(x) = f_\delta(x)$. Since $f_\delta(x)$ and $f(x)$ are monic irreducible polynomials of the same degree n and δ is a root of $f_\delta(x)$, we have $f(x) = f_\delta(x)$. □

In next theorem, we determine the number of SCRIM polynomials of a given degree.

Theorem 3.16. *Let $n \geq 3$ be an odd positive integer. Then following statements hold.*

(i) For each $d \in D_n$, there are $\dfrac{\phi(d)}{n}$ SCRIM polynomials of degree n and order d over $\mathbb{F}_{q^2}$.

(ii) The number of SCRIM polynomials of degree n over $\mathbb{F}_{q^2}$ is $\dfrac{1}{n}\sum_{d \in D_n} \phi(d)$.

Proof. For each $d \in D_n$, there are $\phi(d)$ primitive *d-th* roots of unity. For each primitive *d-th* root of unity β, $f_\beta(x)$ has degree n by Lemma 3.14. Therefore, there are $\dfrac{\phi(d)}{n}$ SCRIM polynomials over $\mathbb{F}_{q^2}$ of degree n and order d. Hence, (i) is proved.

Next, we show that $d = \text{ord}(f_\beta(x))$. From the proof of Theorem 3.15, we know $d \leq \text{ord}(f_\beta(x))$. Since $f_\beta(x)|Q_d(x)$, we have $f_\beta(x)|(x^d - 1)$. It follows that $\text{ord}(f_\beta(x)) \leq d$. Hence, $d = \text{ord}(f_\beta(x))$.

The statement (ii) follows from (i) and the equivalence $(i) \Leftrightarrow (ii)$ in Theorem 3.15. □

Example 3.4. Let $q = 3$ and $n = 3$. Then $D_3 = \{7, 14, 28\}$. Let a be a primitive element of $\mathbb{F}_9$. Then, we have the following properties.

(i) If $d = 7$, there are 2 SCRIM polynomials over $\mathbb{F}_{3^2}$ of degree 3 and order 7 which are $x^3 + a^3x^2 + a^5x + 2$, and $x^3 + ax^2 + a^7x + 2$.

(ii) If $d = 14$, there are 2 SCRIM polynomials over $\mathbb{F}_{3^2}$ of degree 3 and order 14 which are $x^3 + a^5x^2 + a^7x + 1$ and $x^3 + a^7x^2 + a^5x + 1$.

(iii) If $d = 28$, there are 4 SCRIM polynomials over $\mathbb{F}_{3^2}$ of degree 3 and order 28 which are $x^3 + ax^2 + ax + a^6$, $x^3 + a^3x^2 + a^3x + a^2$, $x^3 + a^5x^2 + ax + a^2$ and $x^3 + a^7x^2 + a^3x + a^6$.

Table 3.1 displays the number of SCRIM polynomials of degree $n = 1, 3, 5, \ldots, 13$ over $\mathbb{F}_{q^2}$, where $q = 2, 3, 5, 7$.

q	n	The number of SCRIM polynomials of degree n over $\mathbb{F}_{q^2}$
2	1	3
	3	2
	5	6
	7	18
	9	56
	11	186
	13	630
3	1	4
	3	8
	5	48
	7	312
	9	2184
	11	16104
	13	122640
5	1	6
	3	40
	5	624
	7	1160
	9	217000
	11	4438920
	13	93900240
7	1	8
	3	112
	5	3360
	7	117648
	9	4483696
	11	179756976
	13	7453000800

Table 3.1*: The number of SCRIM polynomials of a given degree over $\mathbb{F}_{q^2}$.

The orders of SCRIM polynomials of degree $n = 11$ over $\mathbb{F}_4$ and $\mathbb{F}_9$ are listed in Table 3.2 and Table 3.3, respectively, together with the number of SCRIM polynomials of each order.

Order	The number of SCRIM polynomials of each order
99	4
331	22
993	44
2979	132
3641	220
10928	440
32769	1320
Total	2182

Table 3.2*: The number of SCRIM polynomials of degree 11 over $\mathbb{F}_4$.

Order	The number of SCRIM polynomials of each order
67	6
134	6
268	12
661	60
1322	60
2644	120
44287	3960
88574	3960
177148	7920
Total	16104

Table 3.3*: The number of SCRIM polynomials of degree 11 over $\mathbb{F}_9$.

*All the computation are prepared by using MAGMA [1].

CHAPTER IV
APPLICATIONS

In this chapter, it is shown how SCRIM polynomials are related to cyclic codes over a finite field $\mathbb{F}_{q^2}$.

Let us begin with basic definitions and properties of cyclic codes over finite fields. All properties are state without proof. For more details, please see [6].

A *linear code* C of length n and dimension k over $\mathbb{F}_q$ is a k-dimensional subspace of the vector space $\mathbb{F}_q^n$ over $\mathbb{F}_q$. It is known as an $[n,k]_q$ code. An element in C is called a *codeword* and written as a row vector $c = (c_o,\, c_1, ...,\, c_{n-1})$.

An $[n,k]_q$ code C is called a *cyclic code* if for each codeword $c = (c_o,\, c_1, ...,\, c_{n-1})$ in C, the vector $(c_{n-1},\, c_0, ...,\, c_{n-2})$ is also a codeword in C.

In order to convert the combinatorial structure of cyclic codes into an algebraic one, we consider the following correspondence:

$$\pi : \mathbb{F}_q^n \to \mathbb{F}_q[x]/\langle x^n - 1\rangle, \text{ defined by } \pi(c_o,\, c_1, ...,\, c_{n-1}) = c_o + c_1 x + ... + c_{n-1}x^{n-1}. \tag{4.1}$$

It is easy to see that π is a linear transformation. Hence, as a vector space over $\mathbb{F}_q$, they are isomorphic. On the other hand,

$$\mathbb{F}_q[x]/\langle x^n - 1\rangle = \{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} | a_i \in \mathbb{F}_q\}$$

is a ring under addition and multiplication modulo $x^n - 1$.

Theorem 4.1 ([6, Theorem 7.1.10]). *For a finite field $\mathbb{F}_q$ and for any positive integer n, $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ is a principal ideal ring.*

Example 4.1. Let $\mathbb{F}_2[x]/\langle x^3 - 1\rangle = \{0, 1, x, x^2, x+1, 1+x^2, x+x^2, 1+x+x^2\}$.

All ideals in ring $\mathbb{F}_2[x]/\langle x^3-1\rangle$ are

$$\begin{aligned}\langle 0\rangle &= \{0\},\\ \langle 1+x+x^2\rangle &= \{0, 1+x+x^2\},\\ \langle 1+x\rangle &= \{0, 1+x, x+x^2, 1+x^2\} \text{ and}\\ \langle 1\rangle &= \{0, 1, x, x^2, +x1, 1+x^2, x+x^2, 1+x+x^2\}.\end{aligned}$$

Next theorem gives a structure of cyclic codes in the ring $\mathbb{F}_q[x]/\langle x^n-1\rangle$.

Theorem 4.2 ([6, Theorem 7.2.1])**.** *Let $C \subseteq \mathbb{F}_q^n$ and π be a linear transformation defined in (4.1). Then C is a cyclic code if and only if $\pi(C)$ is an ideal of $\mathbb{F}_q[x]/\langle x^n-1\rangle$.*

Example 4.2. The code $C = \{000, 111, 222\}$ is a cyclic code over $\mathbb{F}_3$. The corresponding ideal in $\mathbb{F}_3[x]/\langle x^3-1\rangle$ is $\pi(C) = \{0, 1+x+x^2, 2+2x+2x^2\}$.

Definition 4.3. For a cyclic code C of length n over $\mathbb{F}_q$, the unique monic polynomial of the least degree in $\pi(C)$ is called the *generator polynomial* of C. The code C is said to be generated by $g(x)$.

Theorem 4.4 ([6, Theorem 7.2.9])**.** *There is a one-to-one correspondence between the cyclic codes of length n and the nonzero divisors of x^n-1 in $\mathbb{F}_q[x]$.*

Example 4.3. All nonzero divisors of x^3-1 in $\mathbb{F}_2[x]$ are $1, 1+x$ and $1+x+x^2$. Hence, there are three nonzero cyclic codes of length 3 as shown in the following table.

ideals in $\mathbb{F}_2[x]/\langle x^3-1\rangle$	cyclic codes C in $\mathbb{F}_2^3$
$\langle 1\rangle = \{0, 1, x, x^2, 1+x, 1+x^2,$ $x+x^2, 1+x+x^2\}$	{000, 100, 010, 001, 110, 101, 011, 111}
$\langle 1+x\rangle = \{0, 1+x, x+x^2, 1+x^2\}$	{000, 110, 011, 101}
$\langle 1+x+x^2\rangle = \{0, 1+x+x^2\}$	{000, 111}
$\langle 0\rangle = \{0\}$	{000}

The Hermitian inner product of $\mathbf{u} = (u_o, u_1, ..., u_{n-1})$ and $\mathbf{v} = (v_o, v_1, ..., v_{n-1})$ in $\mathbb{F}_{q^2}^n$ is defined to be

$$\langle \mathbf{u}, \mathbf{v} \rangle_H := \sum_{i=o}^{n-1} u_i v_i^q.$$

The Hermitian dual of a linear code C over $\mathbb{F}_{q^2}$ is defined to be the set

$$C^{\perp_H} = \{\mathbf{u} \in \mathbb{F}_{q^2}^n \mid \langle \mathbf{u}, \mathbf{v} \rangle_H = 0 \,\text{for all}\, \mathbf{v} \in C\}.$$

Theorem 4.5. *Let C be a cyclic code of length n over $\mathbb{F}_{q^2}$. Then*

(i) $C^{\perp_H}$ is a cyclic code of length n over $\mathbb{F}_{q^2}$,

(ii) if $g(x)$ is a generator polynomial of C and $h(x) = \dfrac{x^n - 1}{g(x)}$, then $h^\dagger(x)$ is a generator polynomial of $C^{\perp_H}$.

Definition 4.6. A cyclic code C is said to be a *Hermitian complementary dual* if $C \cap C^{\perp_H} = 0$.

Necessary and sufficient conditions for a cyclic code to be Hermitian complementary dual is given in the following theorem.

Lemma 4.7. *Let C be a cyclic code of length n generated by $g(x)$ and $h(x) = \dfrac{x^n - 1}{g(x)}$. Then C is Hermitian complementary dual if and only if* $\gcd(g(x), h^\dagger(x)) = 1$.

Proof. By Theorem 4.5(ii), $C^{\perp_H}$ is generated by $h^\dagger(x)$. Thus $C \cap C^{\perp_H}$ is generated by $f(x) = \text{lcm}(g(x), h^\dagger(x))$. Hence,
C is a Hermitian complementary dual $\Leftrightarrow f(x) = x^n - 1 \Leftrightarrow \gcd(g(x), h^\dagger(x)) = 1$.
□

Next proposition gives a very convenient tool to construct Hermitian complementary dual codes over a finite field.

Proposition 4.8. *Let c be a cyclic code of length n over $\mathbb{F}_{q^2}$ with generator polynomial $g(x)$. Assume that the characteristic of $\mathbb{F}_{q^2}$ does not divide n. Then C is Hermitian complementary dual if and only if $g(x) = g^\dagger(x)$.*

Proof. Write $x^n - 1 = g(x)h(x)$. Then

$$g(x)h(x) = x^n - 1 = g^\dagger(x)h^\dagger(x) \tag{4.2}$$

Assume that C is Hermitian complementary dual. By Lemma 4.7, $\gcd(g(x),\, h^\dagger(x)) = 1$. It follows from (4.2) that $g(x)$ divides $g^\dagger(x)$. Since $g(x)$ and $g^\dagger(x)$ are monic polynomial of the same degree, $g(x) = g^\dagger(x)$.

Conversely, assume that $g(x) = g^\dagger(x)$. By (4.2), $h(x) = h^\dagger(x)$. Since the characteristic of $\mathbb{F}_{q^2}$ does not divide n, every irreducible factor of $x^n - 1$ has multiplicity 1. Consequently,

$$1 = \gcd(g(x),\, h^\dagger(x)) = \gcd(g(x)^\dagger,\, h(x))$$

By Lemma 4.7, C is Hermitian complementary dual. □

Example 4.4. The polynomial $x^7 - 1$ over $\mathbb{F}_9 = \{0, 1, \alpha, \ldots, \alpha^7\}$ can be factored as

$$x^7 - 1 = (x-1)(x^3 + \alpha x^2 + \alpha^7 x + 2)(x^3 + \alpha^3 x^2 + \alpha^5 x + 2).$$

Since $x - 1$, $x^3 + \alpha x^2 + \alpha^7 x + 2$ and $x^3 + \alpha^3 x^2 + \alpha^5 x + 2$ are SCRIM polynomials. Then, all Hermitian complementary dual of length 7 over $\mathbb{F}_9$ are $\langle 0 \rangle$, $\langle (x-1) \rangle$, $\langle (x^3 + \alpha x^2 + \alpha^7 x + 2) \rangle$, $\langle (x^3 + \alpha^3 x^2 + \alpha^5 x + 2) \rangle$, $\langle (x-1)(x^3 + \alpha x^2 + \alpha^7 x + 2) \rangle$, $\langle (x-1)(x^3 + \alpha^3 x^2 + \alpha^5 x + 2) \rangle$ and $\langle (x^3 + \alpha x^2 + \alpha^7 x + 2)(x^3 + \alpha^3 x^2 + \alpha^5 x + 2) \rangle$.

CHAPTER V
CONCLUSION REMARKS

In this thesis, the definition of a SRIM polynomial is slightly different from that of Yucas and Mullen [8]. To be more precise, the reciprocal polynomial of $f(x) = f_0 + f_1x + \cdots + f_nx^n$ with $f_0 \neq 0$ is defined to be $f^*(x) := x^n f_0^{-1} f(\frac{1}{x})$. Where as in [8], $f^*(x) := x^n f(\frac{1}{x})$. This makes no harm to all work done on SRIM polynomials. We will show that these two definitions are equivalent.

Lemma 5.1. *If $Cl_q(i) = Cl_q(-i)$, then $-i = iq^{|Cl_q(i)|/2}$.*

Proof. Since $-i \in Cl_q(i) = Cl_q(-i)$, $-i = iq^j$ for some $j \in \{0, 1, \ldots, |Cl_q(i) - 1|\}$. Thus $i = -(-i) = -(iq^j) = iq^{2j}$, it follows that $|Cl_q(i)| \mid 2j$. Hence, $2j = |Cl_q(i)|$ because $0 < 2j < 2|Cl_q(i)|$. Therefore, $j = |Cl_q(i)|/2$. □

Theorem 5.2. *If $f(x) = f_0 + f_1x + \cdots + f_nx^n$ is a SRIM polynomial over $\mathbb{F}_q$, then $f_0 = 1$.*

Proof. By [8, Theorem 8], $f^*(x) = f(x) = f_\alpha(x) = \prod_{j \in Cl_q(i)} (x - \alpha^j)$ for some primitive *d-th* root of unity α with $d \in D_n$.

Claim $\prod_{j \in Cl_q(i)} \alpha^j = 1$.By Proposition 2.9, we have

$$\alpha^{\frac{i(q^n-1)}{q-1}} = \prod_{j \in Cl_q(i)} \alpha^j = \prod_{k \in Cl_q(-i)} \alpha^k = \alpha^{\frac{-i(q^n-1)}{q-1}}$$

i.e., $\left(\alpha^{\frac{i(q^n-1)}{q-1}}\right)^2 = 1$.

Hence, $\alpha^{\frac{i(q^n-1)}{q-1}} \in \{1, -1\}$.

Case 1, q is even. We are done.

Case 2, q is odd. Since $C_q(i) = C_q(-i)$, it follows that $i = -iq^{(\frac{n}{2})}$. Then,

$$i + q^{(\frac{n}{2})}i \equiv 0 \bmod (\, q^n - 1)$$
$$(q^{(\frac{n}{2})} + 1)i \equiv 0 \bmod (\, q^n - 1).$$

Thus, $i \equiv 0 \bmod (q^{(\frac{n}{2})} - 1)$.

Hence, $i \equiv 0 \bmod (q-1)$. Therefore $\alpha^{\frac{i(q^n-1)}{q-1}} = \left(\alpha^{q^n-1}\right)^{\frac{i}{q-1}} = 1$.

□

However, if $f(x)$ is SCRIM, f_0 does not need to be 1 as shown in the next example.

Example 5.1. Consider the polynomial $f(x) = x^3 + \alpha$ over $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$. Then

$f^\dagger := \overline{x^n f_0^{-1} f(\frac{1}{x})} = \overline{\alpha^2(x^3+1)} = \overline{\alpha^2 + x^3} = x^3 + \alpha$.

Hence, $f(x)$ is SCRIM and the constant term of $f(x)$ is not 1.

For this reason, we define the reciprocal polynomial of $f(x)$ to be $x^n f_0^{-1} f(\frac{1}{x})$ instead of $x^n f(\frac{1}{x})$.

REFERENCES

[1] Bosma, W., Cannon J.J., Playoust C.: The magma algebra system. I: the user lanquage, *J. symb. Comput.* **24**, 235–266 (1997).

[2] Hong, S.J., Bossen D.C.: On some preperties of self-reciprocal polynomials, *J. Korean Math. IEEE Trans. Infor. Try. IT.* **21**, 462–464 (1997).

[3] Jia, Y., Ling, S., Xing, C.: On self-dual cyclic codes over finite fields, *Information Theory, IEEE Transactions.* **57**(4), 2243–2251 (2011).

[4] Jitman, S., Ling, S., Solé, P.: Hermitian self-dual abelian codes, *Information Theory, IEEE Transactions.* **60**(3), 1496–1507 (2014).

[5] Lidl, R., Niederreiter, H.: *Finite fields*, Cambridege Univ. Press, Cambridege. (1997).

[6] Ling, S., Xing, C.: *Coding Theory: A First Course*, Cambridege Univ. Press, Cambridege. (2004).

[7] Xing, Y., Messay, J.L.: The condition for a cyclic code to have a complementary , *Discrete Mathematics.* **126**, 391–393 (1994).

[8] Yucas, J.L., Mullen, G.L.: Self-reciprocal irreducible polynomials over finite fields, *Designs, Codes and Cryptography.* **33**(3), 275–281 (2004).

VITA

Name	Miss Arunwan Boripan
Date of Birth	10 Febuary 1991
Place of Birth	Trang, Thailand
Education	B.Sc. (Mathematics), Prince of Songkla University, 2013
Scholarship	Science Achievement Scholarship of Thailand (SAST)