Self-Conjugate-Reciprocal Irreducible Monic Polynomials over Finite Fields

Arunwan Boripan, Somphong Jitman and Patanee Udomkavanich

Abstract

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

Keywords: order, degree, SCRIM polynomials
2010 Mathematics Subject Classification: 11T55

1 Introduction

A polynomial \( f(x) \) of degree \( n \) over a finite field \( \mathbb{F}_q \) (with \( f(0) \neq 0 \)) is said to be self-reciprocal if \( f(x) \) equals its reciprocal polynomial \( f^*(x) := x^n f(0)^{-1} f \left( \frac{1}{x} \right) \). A polynomial is said to be self-reciprocal irreducible monic (SRIM) if it is self-reciprocal, irreducible and monic. SRIM and self-reciprocal 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].

In this paper, we focus on a generalization of a SRIM polynomial over finite fields, namely, a self-conjugate-reciprocal irreducible monic (SCRIM) polynomial. The conjugate of a polynomial \( f(x) = \sum_{i=0}^{n} f_i x^i \) over \( \mathbb{F}_{q^2} \) is defined to be \( \overline{f(x)} = f_0 + f_1 x + \cdots + f_n x^n, \) where \( \overline{\alpha} : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2} \) is defined by \( \alpha \mapsto \alpha^q \) for all \( \alpha \in \mathbb{F}_{q^2} \). A 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 \( f^!(x) := \overline{f^*(x)} \). 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, properties of SCRIM polynomials have not been well studied. Therefore, it is of natural interest to characterize and to enumerate such polynomials.
2 Preliminaries

In this section, basic properties of polynomials that are important tools for studying SCRIM polynomials are recalled.

Let \( q \) be a prime power and let \( n \) be a positive integer such that \( \gcd(n, q) = 1 \). For each \( 0 \leq i < n \), the cyclotomic coset of \( q \) modulo \( n \) containing \( i \) is defined to be the set

\[
Cl_q(i) = \{ iq^j \mod n \mid j \in \mathbb{N}_0 \}.
\]

A 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 least degree in \( \mathbb{F}_q[x] \) such that \( f(\alpha) = 0 \).

**Theorem 2.1** ([6, Theorem 3.48]). Let \( n \in \mathbb{N} \) be such that \( \gcd(n, q) = 1 \). Let \( m \in \mathbb{N} \) satisfying \( n | (q^m - 1) \) and \( \alpha \) be a primitive element of \( \mathbb{F}_{q^m} \). Then

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

is the minimal polynomial of \( \alpha^i \).

**Remark 2.2.** The polynomial \( M_{\mathbb{F}_q}^{(i)}(x) \) in Theorem 2.1 will be referred to as the minimal polynomial of \( \alpha^i \) defined corresponding to \( Cl_q(i) \).

The order of a polynomial \( f(x) \), denoted by \( \ord(f(x)) \), is defined to be the smallest positive integer \( s \) such that \( f(x) \) divides \( x^s - 1 \).

**Remark 2.3.** It is well know that if \( f(x) \) is an irreducible polynomial over \( \mathbb{F}_q \), then \( f(x) \mid (x^{\ord(f(x))} - 1) \). Moreover, we have

\[
x^{\ord(f(x))} - 1 = \prod_{i=1}^{t} M_{\mathbb{F}_q}^{(i)}(x)^f
\]

where \( t \) is the cardinality of a complete set of representatives of the cyclotomic cosets of \( q \) modulo \( \ord(f(x)) \) [6, Theorem 3.48]. It follows that any irreducible polynomials over \( \mathbb{F}_q \) can be viewed as \( M_{\mathbb{F}_q}^{(i)}(x) \) for some \( i \).

The following property of the order mentioned in [8] and [9] is helpfull.

**Lemma 2.4** ([8, Theorem 3.3]). If \( f(x) \) is an irreducible polynomial of degree \( n \) over \( \mathbb{F}_q \), then \( \ord(f(x)) \) is the order of any root of \( f(x) \) in the multiplicative group \( \mathbb{F}_q^* \).

3 Self-Conjugate-Reciprocal Irreducible Polynomials

In this section, we study self-conjugate-reciprocal irreducible monic (SCRIM) polynomials over finite fields. Since a SCRIM polynomial is defined over a finite field whose order is a square, for notation simplicity, we focus on polynomials in \( \mathbb{F}_{q^2}[x] \). We determine the orders and the number of SCRIM polynomials of a given degree.
Lemma 3.1. Let \( \alpha \) be an element in an extension field of \( \mathbb{F}_{q^2} \) and let \( f(x) \in \mathbb{F}_{q^2}[x] \). Then \( \alpha \) is a root of \( f(x) \) if and only if \( \alpha^{-q} \) is a root of \( f^1(x) \).

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

\[
f^1(\alpha^{-q}) = \alpha^{-qn}(a_0^{q} + \frac{a_1}{\alpha^{-q}} + \cdots + \frac{a_n}{\alpha^{-qn}}) = \alpha^{-qn}(a_0 + a_1 \alpha + \cdots + a_n \alpha^n)^q = \alpha^{-qn}(f(\alpha))^q.
\]

Therefore, \( \alpha \) is a root of \( f(x) \) if and only if \( \alpha^{-q} \) is a root of \( f^1(x) \). \( \square \)

Next lemma gives a necessary and sufficient condition for an irreducible polynomial to be SCRIM. By Remark 2.3, it suffices to concentrate on \( M_{\mathbb{F}_{q^2}}^{(i)}(x) \).

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

Proof. Assume \( M_{\mathbb{F}_{q^2}}^{(i)}(x) = M_{\mathbb{F}_{q^2}}^{(i)}(x) \). Then \( x^i \) is a root of \( M_{\mathbb{F}_{q^2}}^{(i)}(x) \). Since \( Cl_{q^2}(-qi) \) is a class corresponding to \( M_{\mathbb{F}_{q^2}}^{(i)}(x) \), By Theorem 2.1, \( i \in Cl_{q^2}(-qi) \). Hence,

\[
Cl_{q^2}(i) = Cl_{q^2}(-qi).
\]

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

\[
M_{\mathbb{F}_{q^2}}^{(i)}(x) = \prod_{j \in Cl_{q^2}(i)} (x - \alpha^j) = \prod_{j \in Cl_{q^2}(-qi)} (x - \alpha^j) = \prod_{j \in Cl_{q^2}(i)} (x - \alpha^{-qj}).
\]

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

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

Proof. Assume that \( M_{\mathbb{F}_{q^2}}^{(i)}(x) \) has degree \( t \). If \( t = 1 \), then the degree of \( M_{\mathbb{F}_{q^2}}^{(i)}(x) \) is odd. Suppose \( t \neq 1 \). Then, by Lemma 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

\[
i \equiv (-qi)^j \quad (\text{mod} \ t).
\]

It follows that

\[
-qj \equiv (-q)(-qi)^j \quad (\text{mod} \ t)
\]

\[
i q^{2j+2} \quad (\text{mod} \ t),
\]

3
and hence,

\[ i \equiv iq^{2j+2}q^{2j} \pmod{t} \]
\[ \equiv iq^{2(2j+1)} \pmod{t}. \]

It follows that

\[ t \mid (2j+1). \]

Then \( 2j+1 = kt \) for some positive integer \( k \). Since \( 0 \leq j < t \), we have \( kt \leq 2j+1 < 2t \).

It follows that \( k = 1 \), and hence, \( t = 2j+1 \) which is odd.

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

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

**Proof.** Let \( f(x) \) be a polynomial over \( \mathbb{F}_{q^2} \) of degree 1. Then \( f(x) = x + a \) for some \( a \in \mathbb{F}_{q^2} \). Thus \( f^t(x) = x + a^{-q} \). 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 \( q+1 \).

**Example 3.5.** 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 \( 1^6 = 1 = (\alpha^3)^6 = (\alpha^8)^6 = (\alpha^{12})^6 = (\alpha^{20})^6 \).

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 order of SCRIM polynomial.

**Lemma 3.6 (\cite{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 \( q^{r/2} + 1 \) for some positive integer \( s \).

**Lemma 3.7 (\cite{8}, Proposition 1).** Let \( a \) be a positive integers 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.

1. \( a \) divides \( q^s + 1 \) if and only if \( s \) is an odd multiple of \( m \).
2. \( a \) divides \( q^s - 1 \) if and only if \( s \) is an even multiple of \( m \).

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 3.8.** Let \( f(x) \) be a SCRIM polynomial of degree \( n \) over \( \mathbb{F}_{q^2} \). Then \( \text{ord}(f(x)) \in D_n \). Moreover, if \( \alpha \in \mathbb{F}_{q^2} \) is a root of \( f(x) \), then \( \alpha \) 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, \( f\left( \frac{1}{\alpha^t} \right) = 0 \) and we may write \( \frac{1}{\alpha^t} = \alpha^{2^t} \) for some positive integer \( t \). Then \( \alpha^{2^t+q} \) divides \( q^{2^n} + q \). Since \( \gcd(q, \text{ord}(\alpha)) = 1 \), we have \( \text{ord}(\alpha) | (q^{2t+1} + 1) \). From \( \alpha \in \mathbb{F}_{q^{2n}} \), then \( \text{ord}(\alpha) \) divides \( q^{2n} - 1 \). By Lemma 3.6 we have that \( \text{ord}(\alpha) \) divides \( q^{2n/2^t} + 1 \) for some positive integer \( s \). Since \( n \) is odd, it follows that \( s = 1 \). Then \( \text{ord}(\alpha) | (q^n + 1) \).

Let \( t \) be the smallest nonegative integer such that \( \text{ord}(\alpha) | (q^t+1) \). Since \( \deg(f(x)) \geq 3 \), we have \( \text{ord}(\alpha) \geq 3 \), and hence, \( t \geq 1 \). By Lemma 3.7, \( n \) is an odd multiple of \( t \). Using arguments similar to those in the proof of [8, Proposition 4], we have \( n = t \). Therefore, \( \text{ord}(\alpha) \nmid (q^k + 1) \) for all \( 0 \leq k < n \). Hence, by Lemma 3.4, \( \text{ord}(f(x)) = \text{ord}(\alpha) \in D_n \). From this, it can implies that \( \alpha \) is a primitive \( d \)-th root of unity for some \( d \in D_n \).

Corollary 3.9. Let \( f(x) \) be a SCRIM polynomial of degree \( n \) over \( \mathbb{F}_{q^2} \). If \( \alpha \) is a primitive element of \( \mathbb{F}_{q^{2n}} \) and \( \alpha^j \) is a root of \( f(x) \), then

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

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

\[
\text{ord}(\alpha^j) = \frac{q^{2n} - 1}{\gcd(q^{2n} - 1, j)}.
\]

From Lemma 3.4, we know that if \( f(x) \) is irreducible of degree \( n \), then \( \text{ord}(f(x)) \) is the order of any root of \( f(x) \) in the multiplicative group \( \mathbb{F}_{q^{2n}}^{*} \), so \( \text{ord}(\alpha^j) = \text{ord}(f(x)) \).

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

Proposition 3.10. If \( d \in D_n \) and \( \beta \) is a primitive \( d \)-th root of unity, then the set \( \{ \beta, \beta^2, ..., \beta^{q^{2n} - 1} \} \) 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 \( \gcd(d, q^i) = 1 \) and \( \beta^i \) is a primitive \( d \)-th root of unity. If \( \beta^{2i} = \beta^{2j} \) for some \( 0 \leq i < j \leq n - 1 \), then \( \beta^{2i} - \beta^{2j} = 1 \) so that \( d \) divides \( q^{2i} - q^{2j} = q^{2i} (q^{2(j-i)} - 1) \). Since \( \gcd(d, q^2) = 1 \), we see that \( d \) divides \( q^{2(j-i)} - 1 \). Hence, by Lemma 3.7, \( 2(j-i) = kn \) for some even positive integer \( k \). But then \( j = \frac{kn}{2} + i \geq n \), a contradiction. Hence, \( \beta^{2i} \)'s are distinct.

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

Proposition 3.11. \( f_\beta(x) \) is a SCRIM polynomials of degree \( n \) and order \( d \).
Proof. Using the definition of \( f_β(x) \) and the fact that \( n \) is odd, we have

\[
f_β^1(x) = \prod_{i=0}^{n-1} (x - \beta^{2i})^\dagger
\]

\[
= \prod_{i=0}^{n-1} x(-\beta^{2i})^{-q(\frac{1}{x} - \beta^{2i+1})}
\]

\[
= \prod_{i=0}^{n-1} (\beta^{-q^{2i+1}}) \prod_{i=0}^{n-1} (1 - \beta^{2i+1} x)
\]

\[
= \prod_{i=0}^{n-1} (\beta^{-q^{2i+1}}) \prod_{i=0}^{n-1} (\beta^{q^{2i+1}} - x)
\]

\[
= \prod_{i=0}^{n-1} (x - \beta^{-q^{2i+1}}).
\] (3.1)

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

Let \( \beta^{-q^{2i+1}} \in \{\beta^{-q^{2i+1}} \mid 0 \leq i \leq n - 1\} \). Then

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

Since \( n \) is odd, we have \( \beta^{-q^{2i+1}} = \beta^{q^l} \) for some \( 0 \leq l \leq n - 1 \). Hence, \( \beta^{-q^{2i+1}} \in \{\beta^{q^l} \mid 0 \leq j \leq n - 1\} \).

Let \( \beta^{q^s} \in \{\beta^{q^l} \mid 0 \leq j \leq n - 1\} \). Since \( n \) is odd, we have

\[
\beta^{q^s} = \beta^{q^{n+1+2s}} = (\beta^{q^{n+1}})q^{2s} = (\beta^{-q}q^{2s}) = \beta^{q^{2s}(-q)}
\]

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

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

\[
f_β^1(x) = \prod_{i=0}^{n-1} (x - \beta^{-q^{2i+1}})
\]

\[
= \prod_{j=0}^{n-1} (x - \beta^{q^j})
\]

\[
f_β(x).
\]

Suppose that \( f_β(x) \) is written as \( f_β(x) = g(x)h(x) \), 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

\[
α^{q^{2r} - 1} = 1.
\]

Since \( α \) is a root of \( f_β(x) \), \( α \) is a \( d \)-th-root of unity. Hence,

\[
d((q^{2r} - 1)).
\]

Since \( d \) divides \( q^n + 1 \), by Lemma 3.7, \( 2r \) is an even multiple of \( n \). Since \( r \leq n \), we have \( r = n \) and \( f_β(x) = g(x) \) is irreducible. \( \square \)
The construction of a SCRIM polynomial \( f_\beta(x) \) can be illustrated as follows.

**Example 3.12.** Let \( n = 3 \) and \( q = 3 \). Then \( D_3 = \{7, 14, 28\} \). Assume that \( \mathbb{F}_{29} = \langle \alpha \rangle \). 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 Theorem 3.11, \( f_{\alpha^{52}}(x) \) is a SCRIM polynomial.

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

\[
x^n - 1 = \prod_{d \mid n} Q_d(x),
\]

(3.2)

where \( Q_d(x) = \prod_{s=1, \gcd(s,n)=1} \) (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 \( \mathbb{F} \).

**Theorem 3.14.** Let \( f(x) \) be an irreducible monic polynomial of degree \( n \) over \( \mathbb{F}_{q^2} \). Then the following statements are equivalent:

1) \( \text{ord}(f(x)) \) is self-conjugate-reciprocal.

2) \( \text{ord}(f(x)) \in D_n \).

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

**Proof.** By Corollary 3.9 and Proposition 3.11 it remains to prove 2) implies 3). Assume \( \text{ord}(f(x)) \in D_n \). Let \( p \) be the characteristic of \( \mathbb{F}_{q^2} \). Since \( \gcd(p, \text{ord}(f(x))) = 1 \), by Lemma 3.13, we have

\[
x^{\text{ord}(f(x))} - 1 = \prod_{\ell \mid \text{ord}(f(x))} Q_\ell(x).
\]

Since \( f(x)|(x^{\text{ord}(f(x))} - 1) \), we have \( f(x)|Q_d(x) \) for some divisor \( d \) of \( \text{ord}(f(x)) \). 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., \( \delta^{2k} \equiv 1 \pmod{d} \). From [5] Theorem 2.47, \( n \) is the smallest positive integer such that \( q^{2n} \equiv 1 \pmod{d} \). Since \( k < n \), we have a contradiction. Therefore, \( d \in D_n \).

Let \( \gamma \) be a primitive \( d \)-th root of unity over \( \mathbb{F}_{q^2} \). Since \( q^{2n} \equiv 1 \pmod{d} \) and \( q^{2k} \not\equiv 1 \pmod{d} \), for all \( 0 \leq k < n \), it follows that \( \gamma \in \mathbb{F}_{q^{2n}} \) but \( \gamma \not\in \mathbb{F}_{q^{2k}} \) for all \( 0 \leq k < n \). Then the minimal polynomial of \( \gamma \) has degree \( n \). Since \( f(x) \) is irreducible and \( f(x)|Q_d(x) \), there exists a primitive \( d \)-th root of unity \( \delta \) 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 \( \delta \) is a root of \( f_\delta(x) \), we have \( f(x) = f_\delta(x) \). \( \square \)
In the next theorem, we determine the number of SCRIM polynomials of a given degree.

**Theorem 3.15.** Let $n \geq 3$ be an odd positive integer. Then following statements hold.

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

2) The number of SCRIM polynomials over $\mathbb{F}_{q^2}$ of degree $n$ is

$$\frac{1}{n} \sum_{d \in D_n} \phi(d).$$

**Proof.** For each $d \in D_n$, there are $\phi(d)$ primitive $d$-th root of unity. For each primitive $d$-th root of unity $\beta$, $f_\beta(x)$ has degree $n$ by [5, Theorem 2.47]. Therefore, there are $\frac{\phi(d)}{n}$ SCRIM polynomials over $\mathbb{F}_{q^2}$ of degree $n$ and order $d$. Hence, 1) is proved.

Next, we show that $d = \text{ord}(f_\beta(x))$. From the proof of Theorem 3.14 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 2) follows from 1) and the equivalence of the statements 1) and 2) in Theorem 3.14. \[\square\]

**Example 3.16.** Let $q = 3$ and $n = 3$. Then $D_3 = \{7, 14, 28\}$. Let $\alpha$ be defined as in Example 3.12. Then, we have the following properties.

1) 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 $x^3 + ax^2 + a^7x + 2$.

2) 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 $x^3 + a^7x^2 + a^5x + 1$.

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

Table 3.1 displays the number of SCRIM polynomials of degree $n = 1, 3, 7, \ldots, 15$ over $\mathbb{F}_{q^2}$, where $q = 2, 3, 5$.

The order of SCRIM polynomials of degree $n = 11$ over $\mathbb{F}_4$ are listed in Table 3.2 together with the number of SCRIM polynomials of degree $n = 11$ over $\mathbb{F}_4$ of a given order.

**Acknowledgements**

The authors would like to thank the anonymous referees for helpful comments and suggestions.
The number of SCRIM polynomials of degree $n$ over $\mathbb{F}_{q^2}$

| $q$ | $n$ | The number of SCRIM polynomials |
|-----|-----|-------------------------------|
| 2   | 1   | 3                             |
|     | 3   | 2                             |
|     | 5   | 6                             |
|     | 7   | 18                            |
|     | 9   | 56                            |
|     | 11  | 186                           |
|     | 13  | 630                           |
|     | 15  | 2182                          |
| 3   | 1   | 4                             |
|     | 3   | 8                             |
|     | 5   | 48                            |
|     | 7   | 312                           |
|     | 9   | 2184                          |
|     | 11  | 16104                         |
|     | 13  | 122640                        |
|     | 15  | 956576                        |
| 5   | 1   | 6                             |
|     | 3   | 40                            |
|     | 5   | 624                           |
|     | 7   | 1160                          |
|     | 9   | 217000                        |
|     | 11  | 4438920                       |
|     | 13  | 93900240                      |
|     | 15  | 2034504992                    |

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

| 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 15 over $\mathbb{F}_4$.

References

[1] O. Ahmadi and G. Vega, On the parity of the number of irreducible factors of self-reciprocal polynomials over finite fields, *Finite Fields and Their Applications*, 14(1) (2008), 124–131.

[2] S. J. Hong and D. C. Bossen, On some properties of self-reciprocal polynomials, *IEEE Transactions on Information Theory*, 21 (1975), 462–464.
[3] Y. Jia, S. Ling, and C. Xing, On self-dual cyclic codes over finite fields, *IEEE Transactions on Information Theory*, **57**(4) (2011), 2243–2251.

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

[5] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, Cambridge, 1997.

[6] S. Ling and C. Xing, *Coding Theory: A First Course*, Cambridge Univ. Press, Cambridge, 2004.

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

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