Thai Journal of Mathematics
Volume 22 Number 1 (2024)
Pages 93–102
http://thaijmath.in.cmu.ac.th

ISSN 1686-0209

Annual Meeting in Mathematics 2023

Self-Conjugate-Reciprocal Polynomials over Finite Fields and Self-Conjugate-Reciprocal Transformation

Hataiwit Palasak*, **Ouamporn Phuksuwan and Tuangrat Chaichana**

Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Thailand
e-mail : hataiwit.p@gmail.com (H. Palasak); ouamporn.p@chula.ac.th (O. Phuksuwan); tuangrat.c@chula.ac.th (T. Chaichana)

Abstract An interesting class of polynomials over finite fields, namely self-conjugate-reciprocal polynomials, has been studied here. Some elementary properties on their roots and a way to find all self-conjugate-reciprocal irreducible monic polynomials of a given degree are provided. Moreover, in the last part, we define a map taking a polynomial over a finite field with some conditions to a self-conjugate-reciprocal polynomial. Certain properties of the polynomial obtained from this map are investigated.

MSC: 11T06
Keywords: self-conjugate-reciprocal polynomials; self-conjugate-reciprocal transformations; finite fields

Submission date: 02.06.2023 / Acceptance date: 31.08.2023

1. Introduction

Let $\mathbb{F}_q$ be the finite field of order q, where q is a prime power. For a polynomial $f(x)$ of degree n over $\mathbb{F}_q$ with nonzero constant term, its *reciprocal* is the polynomial

$$f^*(x) := x^n f(1/x).$$

A polynomial $f(x)$ is called *self-reciprocal* if $f^*(x) = f(x)$. Self-reciprocal polynomials were studied by many researchers in different aspects. In [8], Yucas and Mullen classified self-reciprocal irreducible monic (SRIM) polynomials and enumerated these polynomials. Due to the conjecture appearing in [3], infinite families of self-reciprocal irreducible polynomials were constructed under some conditions in [8].

Let $f(x)$ be a polynomial over $\mathbb{F}_q$ of degree n. Define a map ϕ to be

$$\phi : f(x) \mapsto f_R(x) := x^n f(x + 1/x).$$

The resulting polynomial $f_R(x)$ is self-reciprocal and the map ϕ is called a *self-reciprocal transformation*. A factorization of the polynomial $f_R(x)$ was studied by Meyn in [6], and later, by Kobayashi and Nogami in [4].

*Corresponding author.

Published by The Mathematical Association of Thailand.

Definition 1.1. Let $g(x)$ and $h(x)$ be polynomials over $\mathbb{F}_q$ with $g(0) \neq 0$ and $h(0) \neq 0$. They are called a *reciprocal pair* if there exist $\gamma \in \mathbb{F}_q^*$ such that

$$g^*(x) = \gamma h(x).$$

Theorem 1.2. [6] *If $f(x)$ is irreducible over $\mathbb{F}_q$ of degree $n > 1$, then either*

(i) *$f_R(x)$ is a SRIM polynomial of degree $2n$, or*

(ii) *$f_R(x)$ is the product of a reciprocal pair of irreducible polynomials of degree n which are not self-reciprocal.*

On the other hand, Ahmadi and Vega [1] proved that any self-reciprocal polynomial over $\mathbb{F}_q$ of even degree can be written in the form

$$x^n g(x + 1/x)$$

for some $g(x) \in \mathbb{F}_q[x]$ and obtained some results about the parity of the number of irreducible factors of self-reciprocal polynomials.

The concept of self-reciprocal polynomials is analogously extended to self-conjugate-reciprocal polynomials. Naturally, some properties of self-reciprocal polynomials have been investigated for self-conjugate-reciprocal polynomials.

Definition 1.3. Let $f(x) = a_0 + a_1x + ... + a_nx^n$ be a polynomial of degree n over $\mathbb{F}_{q^2}$ such that $a_0 \neq 0$. The *conjugate* of $f(x)$ is written as

$$\overline{f(x)} = \overline{a_0} + \overline{a_1}x + ... + \overline{a_n}x^n,$$

where $^- : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ is defined by $\alpha \mapsto \alpha^q$ for all $\alpha \in \mathbb{F}_{q^2}$. The *conjugate-reciprocal polynomial* of $f(x)$ is defined to be

$$f^\dagger(x) = \overline{a_0^{-1}x^n f(1/x)}$$

and the polynomial $f(x)$ is called *self-conjugate-reciprocal* if $f(x) = f^\dagger(x)$.

If $f(x)$ is self-conjugate-reciprocal, then its leading coefficient must be $\overline{a_0^{-1}a_0} = 1$ so it is monic.

Some properties related to this kind of polynomials can be found in e.g. [2] and [7].

Remark 1.4. (i) α is a root of $f(x)$ if and only if $\overline{\alpha^{-1}} = \alpha^{-q}$ is a root of $f^\dagger(x)$,

(ii) any self-conjugate-reciprocal irreducible monic (SCRIM) polynomials have odd degree,

(iii) a polynomial $f(x) = a_0 + a_1x + ... + a_nx^n$ is self-conjugate-reciprocal if and only if $a_i = \overline{a_0^{-1}a_{n-i}}$ for all $0 \leq i \leq n$,

(iv) for any $\alpha \in \mathbb{F}_{q^2}$, $\alpha \in \mathbb{F}_q$ if and only if $\overline{\alpha} = \alpha^q = \alpha$.

Moreover, Boripan [2] showed analogous results as those in [8] to characterize self-conjugate-reciprocal polynomials.

Definition 1.5. The *order* of a polynomial $f(x)$ over a finite field, denoted by $ord(f)$, is the smallest positive integer s such that $f(x)$ divides $x^s - 1$.

If $f(x)$ is an irreducible polynomial over $\mathbb{F}_q$, then one can see that $ord(f)$ is the order of any root of f in the multiplicative group $\mathbb{F}^*_{q^{\deg(f)}}$.

Theorem 1.6. [2] *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) $ord(f) \in D_n := \{d \in \mathbb{N} : d \mid (q^n+1)$ but $d \nmid (q^k+1)$ for all $0 \le k < n\}$,
(iii) $f(x) = f_\beta(x) := \prod_{i=0}^{n-1}(x - \beta^{q^{2i}})$ *for some primitive dth root of unity* β *with* $d \in D_n$.

Some parts of our earlier works in [7] showed a relation between self-conjugate-reciprocal polynomials and cyclotomic polynomials as in the following.

Theorem 1.7. [7] *For* $d \in D_n$*, the dth cyclotomic polynomial*

$$Q_d(x) := \prod_{\substack{s=1 \\ \gcd(s,d)=1}}^{d} (x - \beta^s),$$

where β *is a primitive dth root of unity, can be factored uniquely into the product of all self-conjugate-reciprocal irreducible polynomials over* $\mathbb{F}_{q^2}$ *of degree* n *and order* d.

Consequently, to find all SCRIM polynomials with a given degree, it is enough to find all irreducible factors of the corresponding cyclotomic polynomial. For example, to find all SCRIM polynomials over $\mathbb{F}_{2^2}$ of degree 5, first we consider

$$D_5 = \{d \in \mathbb{N} : d \mid (2^5+1) \text{ but } d \nmid (2^k+1) \text{ for all } 0 \le k < 5\} = \{11, 33\}.$$

Next, factorizing the dth cyclotomic polynomial $Q_d(x)$ for each $d \in D_5$ by letting $\alpha \in \mathbb{F}_{2^2}$ that satisfies $\alpha^2+\alpha+1=0$, we have

$$Q_{11}(x) = (x^5+\alpha x^4+x^3+x^2+(1+\alpha)x+1)(x^5+(1+\alpha)x^4+x^3+x^2+\alpha x+1), \text{and}$$

$$Q_{33}(x) = (x^5+x^4+\alpha x^3+x^2+\alpha x+\alpha)(x^5+x^4+(1+\alpha)x^3+x^2+(1+\alpha)x+(1+\alpha))$$
$$(x^5+\alpha x^4+\alpha x^3+x^2+x+\alpha)(x^5+(1+\alpha)x^4+(1+\alpha)x^3+x^2+x+(1+\alpha)).$$

The formula to count the number of all SCRIM polynomials degree n is given in [2], which is equal to $\frac{1}{n}\sum_{d\in D_n}\phi(d)$. Thus the number of all SCRIM polynomials of degee 5 is $\frac{1}{5}\sum_{d\in D_5}\phi(d) = 6$. They are listed in the following table separating for each order $d \in D_5$.

SCRIM polynomials	**order**
$x^5+\alpha x^4+x^3+x^2+(1+\alpha)x+1$	11
$x^5+(1+\alpha)x^4+x^3+x^2+\alpha x+1$	11
$x^5+x^4+\alpha x^3+x^2+\alpha x+\alpha$	33
$x^5+\alpha x^4+\alpha x^3+x^2+x+\alpha$	33
$x^5+x^4+(1+\alpha)x^3+x^2+(1+\alpha)x+(1+\alpha)$	33
$x^5+(1+\alpha)x^4+(1+\alpha)x^3+x^2+x+(1+\alpha)$	33

2. Results

Some elementary results about the roots of self-conjugate-reciprocal irreducible polynomials are given in the following lemmas.

Lemma 2.1. *Let* $\beta \in \mathbb{F}_{q^{2(2m+1)}}$ *be a root of a self-conjugate-reciprocal irreducible polynomial* $f(x)$ *over* $\mathbb{F}_{q^2}$ *of odd degree* $2m+1$*. Then*

(i) $\overline{\beta^{-1}}$ *is a root of* $f(x)$*, and*

(ii) *for each* $0 \le j \le 2m$, $\overline{(\beta^{q^{2j}})^{-1}} = \beta^{q^{2(m+j+1)}}$.

Proof. (i) It follows immediately from Remark 1.4 (i) and the fact that $f(x) = f^{\dagger}(x)$.
(ii) We know that $ord(f)$ divides $q^{2m+1}+1$ by Theorem 1.6. Then for each $0 \le j \le 2m$,

$$\overline{\beta^{q^{2j}}} \cdot \beta^{q^{2(m+j+1)}} = \beta^{q^{2j+1}+q^{2(m+j+1)}} = (\beta^{q^{2m+1}+1})^{q^{2j+1}} = 1.$$

Thus, $\overline{(\beta^{q^{2j}})^{-1}} = (\overline{\beta^{q^{2j}}})^{-1} = \beta^{q^{2(m+j+1)}}$. ∎

Lemma 2.2. *Let $f(x)$ be an irrducible polynomial over $\mathbb{F}_{q^2}$ of degree n and $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ the set of all distinct roots of $f(x)$. Then $\{\overline{\alpha_1^{-1}}, \overline{\alpha_2^{-1}}, ..., \overline{\alpha_n^{-1}}\}$ is the set of all distinct roots of $f^{\dagger}(x)$. Moreover, $f^{\dagger}(x)$ is also irreducible over $\mathbb{F}_{q^2}$.*

Proof. Note that $\overline{\alpha_1^{-1}}, \overline{\alpha_2^{-1}}, ..., \overline{\alpha_n^{-1}}$ are roots of $f^{\dagger}(x)$. To show that they are all distinct, suppose that $\overline{\alpha_i^{-1}} = \overline{\alpha_j^{-1}}$ for some $i, j \in \{1, 2, ..., n\}$. We then have $\alpha_i^{-q} = \alpha_j^{-q}$, and so $0 = \alpha_i^q - \alpha_j^q = (\alpha_i - \alpha_j)^q$. This implies that $\alpha_i - \alpha_j = 0$ and then $\alpha_i = \alpha_j$ and $i = j$. Since $\deg(f^{\dagger}) = n$, $\{\overline{\alpha_1^{-1}}, \overline{\alpha_2^{-1}}, ..., \overline{\alpha_n^{-1}}\}$ is the set of all distinct roots of $f^{\dagger}(x)$. ∎

Definition 2.3. A subset R of a finite field is said to be *closed under conjugate-inversion* if for any $a \in R$, $\overline{a^{-1}} \in R$.

Theorem 2.4. *Let $f(x)$ be an irreducible monic polynomial over $\mathbb{F}_{q^2}$. Then $f(x)$ is self-conjugate-reciprocal if and only if its set of all roots is closed under conjugate-inversion.*

Proof. Let R and R' be the set of all roots of $f(x)$ and $f^{\dagger}(x)$, respectively. By Lemma 2.1, if $f(x)$ is a SCRIM polynomial, then R is closed under conjugate-inversion. Conversely, assume that R is closed under conjugate-revision. We will show that $f(x) = f^{\dagger}(x)$ by considering their roots. Let $\beta \in R$. Then $\overline{\beta^{-1}} \in R'$. By assumption, $\{\overline{\beta^{-1}} : \beta \in R\} \subseteq R$. By Lemma 2.2, the set $\{\overline{\beta^{-1}} : \beta \in R\} = R'$. Hence $\deg(f) = \deg(f^{\dagger}) = |R'| \le |R| = \deg(f)$. It follows that $R = R'$. Since $f(x)$ and $f^{\dagger}(x)$ are monic, $f(x) = f^{\dagger}(x)$. ∎

Next, we give a relation between SCRIM polynomials over $\mathbb{F}_{q^2}$ of degree n and the polynomial of the form

$$H_{q,n}(x) := x^{q^n+1} - 1.$$

Based on this relation, another way to find all SCRIM polynomials of a given degree is obtained.

Lemma 2.5. [5] *Let $f(x)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree n. Then*

(i) *$f(x)$ has a root α in $\mathbb{F}_{q^n}$ and all the roots of $f(x)$ are given by the n distinct elements $\alpha, \alpha^q, ..., \alpha^{q^{n-1}}$, and*

(ii) *$f(x)$ divides $x^{q^m} - x$ if and only if n divides m.*

Theorem 2.6. *We have*

(i) *each SCRIM polynomial of odd degree n over $\mathbb{F}_{q^2}$ is a factor of the polynomial $H_{q,n}(x)$, and*

(ii) *each irreducible factor over $\mathbb{F}_{q^2}$ of $H_{q,n}(x)$ (where n is odd) is a SCRIM polynomial over $\mathbb{F}_{q^2}$ of degree d, where d divides n.*

Proof. (i) Let $f(x)$ be a SCRIM polynomial of degree $n = 2m+1$ over $\mathbb{F}_{q^2}$. Then $f(x)$ has a root in $\mathbb{F}_{q^{2n}}$, say α. By Lemma 2.5 (i), $\{\alpha, \alpha^{q^2}, \alpha^{q^4}, ..., \alpha^{q^{2(n-1)}}\}$ is the set of all roots of $f(x)$ in $\mathbb{F}_{q^{2n}}$. For each $0 \le j \le n-1$, $\overline{(\alpha^{q^{2j}})^{-1}}$ is a root of $f(x)$ and by Lemma 2.1 (ii),

$$\alpha^{-q^{2j+1}} = \overline{(\alpha^{q^{2j}})^{-1}} = \alpha^{q^{2(m+j+1)}}, \text{ so } 0 = \alpha^{q^{2(m+j+1)}+q^{2j+1}} - 1 = [\alpha^{q^{n+2j}+q^{2j}} - 1]^q.$$

Then $(\alpha^{q^{2j}})^{q^n+1} - 1 = 0$. Therefore, for each $0 \le j \le n-1$, $\alpha^{q^{2j}}$ is a root of $H_{q,n}(x)$. This implies $f(x)$ divides $H_{q,n}(x)$.

(ii) Write $n = 2m+1$ and let $g(x)$ be a monic irreducible factor of $H_{q,n}(x)$ with $\deg(g(x)) = d$ and α a root of $g(x)$. Then α is a root of $H_{q,n}(x)$. It means $\alpha^{q^n+1} - 1 = 0$, so

$$\alpha^{q^{2(m+1)}} - \overline{\alpha^{-1}} = \alpha^{q^{n+1}} - \alpha^{-q} = \alpha^{-q} \cdot (\alpha^{q^n+1} - 1)^q = 0.$$

Then $\overline{\alpha^{-1}} = \alpha^{q^{2(m+1)}}$. Moreover, we have $R := \{\alpha, \alpha^{q^2}, ..., \alpha^{q^{2(d-1)}}\}$ is the set of all roots of $g(x)$, and for each $0 \le j \le d-1$, $\overline{(\alpha^{q^{2j}})^{-1}} = \alpha^{q^{2(m+j+1)}}$, which is a root of $g(x)$. This implies that R is closed under conjugate-inversion. By Theorem 2.4, $g(x)$ is SCRIM. Then d is odd. Since q^n+1 divides $q^{2n}-1$, $H_{q,n}(x)$ divides $x^{q^{2n}-1}-1$. Thus $g(x)$ divides $x^{q^{2n}} - x$. By Lemma 2.5 (ii), d divides $2n$, so d divides n. ■

Denote $C_{q,n}(x)$ to be the product of all distinct SCRIM polynomials of degree n over $\mathbb{F}_{q^2}$.

Lemma 2.7. *For each $d_1, d_2 \in \mathbb{N}$ with $d_1 \ne d_2$, $\gcd(C_{q,d_1}(x), C_{q,d_2}(x)) = 1$.*

Proof. Let $d_1 \ne d_2$. Suppose that $\gcd(C_{q,d_1}(x), C_{q,d_2}(x)) \ne 1$. Then there exists an irreducible polynomial $p(x)$ over $\mathbb{F}_{q^2}$ such that $p(x)|C_{q,d_1}(x)$ and $p(x)|C_{q,d_2}(x)$. We know that $C_{q,d_i}(x) = \prod_{e \in D_{d_i}} Q_e(x)$ where $Q_e(x)$ is the eth cyclotomic polynomial. Then there exist $a \in D_{d_1}$ and $b \in D_{d_2}$ such that $p(x) \mid Q_a(x)$ and $p(x) \mid Q_b(x)$, respectively. By Theorem 1.7, we have $p(x)$ is a SCRIM polynomial of order a and b. It follows that $a = b$ which is impossible because $D_{d_1} \cap D_{d_2} = \emptyset$ when $d_1 \ne d_2$. ■

Theorem 2.8. *Let n be an odd positive integer. Then*

$$H_{q,n}(x) = \prod_{d|n} C_{q,d}(x).$$

Proof. We first note that $H_{q,n}(x)$ has no repeated root. Let

$$H_{q,n}(x) = f_1(x)f_2(x)\cdots f_k(x),$$

where $f_1(x), ..., f_k(x)$ are distinct irreducible monic polynomials over $\mathbb{F}_{q^2}$. By Theorem 2.6 (ii), for each $1 \le i \le k$, $f_i(x)$ is a SCRIM polynomial of degree d where $d|n$. Then $f_i(x)$ divides $\prod_{d|n} C_{q,d}(x)$, so $H_{q,n}(x)$ divides $\prod_{d|n} C_{q,d}(x)$ since $f_1(x), ..., f_k(x)$ are pairwise relatively prime.

Conversely, let $f(x)$ be a SCRIM polynomial of degree d where $d|n$. By Theorem 2.6 (i), $f(x)$ divides $H_{q,d}(x)$. Since $d \mid n$ and $\frac{n}{d}$ is odd, it follows that $(q^d+1) \mid (q^n+1)$. This implies that $H_{q,d}(x)$ divides $H_{q,n}(x)$. Thus $f(x)$ divides $H_{q,n}(x)$. Since any irreducible factors of $C_{q,d}(x)$ are pairwise relatively prime and by Lemma 2.7, it follows that $\prod_{d|n} C_{q,d}(x)$ divides $H_{q,n}(x)$. ■

Example 2.9. Considering the factorization of $H_{2,5}(x)$ over $\mathbb{F}_{2^2}$ where $\mathbb{F}_{2^2} = \mathbb{F}_2(\alpha)$ with $\alpha \in \mathbb{F}_{2^2}$ satisfying $\alpha^2 + \alpha + 1 = 0$ as follows

$$\begin{aligned} H_{2,5}(x) = &(x+1)(x+\alpha)(x+(1+\alpha))(x^5+x^4+\alpha x^3+x^2+\alpha x+\alpha)\\ &(x^5+x^4+(1+\alpha)x^3+x^2+(1+\alpha)x+(1+\alpha))\\ &(x^5+\alpha x^4+x^3+x^2+(1+\alpha)x+1)(x^5+(1+\alpha)x^4+x^3+x^2+\alpha x+1)\\ &(x^5+\alpha x^4+\alpha x^3+x^2+x+\alpha)(x^5+(1+\alpha)x^4+(1+\alpha)x^3+x^2+x+(1+\alpha))\\ = &C_{2,1}(x)C_{2,5}(x), \end{aligned}$$

we can find all SCRIM polynomials of degee 1 and 5 over $\mathbb{F}_{2^2}$.

degree	**SCRIM polynomials**
1	$x+1$ $x+\alpha$ $x+(1+\alpha)$
5	$x^5+\alpha x^4+x^3+x^2+(1+\alpha)x+1$ $x^5+(1+\alpha)x^4+x^3+x^2+\alpha x+1$ $x^5+x^4+\alpha x^3+x^2+\alpha x+\alpha$ $x^5+x^4+(1+\alpha)x^3+x^2+(1+\alpha)x+(1+\alpha)$ $x^5+\alpha x^4+\alpha x^3+x^2+x+\alpha$ $x^5+(1+\alpha)x^4+(1+\alpha)x^3+x^2+x+(1+\alpha)$

3. Self-Conjugate-Reciprocal Transformation

Analogously to the concept of self-reciprocal transformation, we need to define a map that generates self-conjugate-reciprocal polynomials.

Definition 3.1. For $A \subseteq \mathbb{F}_{q^2}[x]$, a map ψ from A to $\mathbb{F}_{q^2}[x]$ is called a *self-conjugate-reciprocal transformation* for A if $\psi(f(x))$ is a self-conjugate-reciprocal polynomial for all $f(x) \in A$.

For any polynomial $f(x)$ over $\mathbb{F}_{q^2}$ of degree n, define Ψ to be

$$\Psi : f(x) \mapsto F(x) := x^{nq} f(x^q + x^{-q}).$$

It is clear that the degree of the polynomial $F(x)$ is $2nq$ and its leading coefficient is equal to the leading coefficient of $f(x)$.

The resulting polynomial $F(x)$ obtained from Ψ may not be self-conjugate-reciprocal. This problem leads us to find the necessary and sufficient conditions to produce a self-conjugate-reciprocal polynomial $F(x)$.

Theorem 3.2. *Let $f(x) = \sum\limits_{i=0}^{n} a_i x^i \in \mathbb{F}_{q^2}[x]$ with $a_n, a_0 \neq 0$. Then $F(x)$ is self-conjugate-reciprocal if and only if $a_n = 1$ and $a_i \in \mathbb{F}_q$ for all $i = 0, 1, ..., n-1$.*

Proof. Let $f(x) = \sum\limits_{i=0}^{n} a_i x^i \in \mathbb{F}_{q^2}[x]$. Assume that $a_i \in \mathbb{F}_q$ for all $i = 0, 1, ..., n-1$ and $a_n = 1$. Then

$$F^{\dagger}(x) = \overline{x^{2nq} x^{-nq} f(x^q + x^{-q})} = x^{nq} \sum_{i=0}^{n} \overline{a_i}(x^q + x^{-q})^i = x^{nq} \sum_{i=0}^{n} a_i (x^q + x^{-q})^i = F(x).$$

Conversely, assume that $F(x) = \sum_{i=0}^{2n} b_{iq}x^{iq}$ is self-conjugate-reciprocal. Note that $F(x) = \sum_{i=0}^{n} a_i x^{nq}(x^q + x^{-q})^i$. For each $0 \leq i \leq n$, each term of $F(x)$ can be expressed as

$$a_i x^{nq}(x^q + x^{-q})^i = a_i x^{nq} \sum_{k=0}^{i} \binom{i}{k} (x^q)^{i-k}(x^{-q})^k = a_i \sum_{k=0}^{i} \binom{i}{k} x^{(n+i)q-2qk}.$$

Then for each $0 \leq k \leq i$, the coefficient of $x^{(n+i)q-2qk}$ and $x^{(n-i)q+2qk}$, which are $a_i\binom{i}{k}$ and $a_i\binom{i}{i-k}$, respectively, must equal. Moreover, these two terms appear only in the expansion of

$$a_{i+2t}x^{nq}(x^q + x^{-q})^{i+2t} = a_{i+2t} \sum_{k=0}^{i+2t} \binom{i+2t}{k} x^{q(n+i+2t)-2qk}$$

for all $0 \leq t \leq \lfloor \frac{n-i}{2} \rfloor$. We then have $b_0 = b_{2nq} = a_n$ and $b_q = b_{(2n-1)q} = a_{n-1}$. In general, for each $0 \leq i \leq n$,

$$b_{(2n-i)q} = b_{iq} = \begin{cases} a_{n-i} + a_{n-i+2}\binom{n-i+2}{1} + \ldots + a_n\binom{n}{\frac{i}{2}}, & \text{if } i \text{ is even,} \\ a_{n-i} + a_{n-i+2}\binom{n-i+2}{1} + \ldots + a_{n-1}\binom{n-1}{\frac{i-1}{2}}, & \text{if } i \text{ is odd.} \end{cases} \tag{3.1}$$

Since $F(x)$ is self-conjugate-reciprocal,

$$b_{2nq} = 1 \text{ and } b_{lq} = \overline{b_0^{-1}b_{(2n-l)q}}, \text{ for all } 0 \leq l \leq 2n.$$

It follows that $a_n = b_0 = b_{2nq} = 1$.

By the assumption, the coefficients of $x^{(2n-1)q}$ and x^q are given by $b_{(2n-1)q}$ and b_q, respectively. Moreover, these two terms appear only in the expansion of $a_{n-1}x^{nq}(x^q + x^{-q})^{n-1}$ and they have the same coefficient which is equal to a_{n-1}. These imply that $a_{n-1} = b_q = b_{(2n-1)q}$, and then $b_{(2n-1)q} = \overline{b_0^{-1}b_q} = \overline{a_{n-1}}$. Thus $a_{n-1} = \overline{a_{n-1}}$, so $a_{n-1} \in \mathbb{F}_q$. By (3.1), it can be proved inductively to obtain that $a_i \in \mathbb{F}_q$ for all i. ■

Remark 3.3. Ψ is a self-conjugate-reciprocal transformation for A where A is the set of all monic polynomials $f(x)$ over $\mathbb{F}_q$. From now on, we consider only all monic polynomials $f(x)$ over $\mathbb{F}_q$. We notice that

$$F(x) = x^{nq}f(x^q + x^{-q}) = [x^n f(x + x^{-1})]^q = (f_R(x))^q$$

where $f_R(x)$ is the resulting polynomial derived from the self-reciprocal transformation. Clearly, $F(x)$ is reducible. It is natural to investigate irreducible factors of the self-conjugate-reciprocal polynomial $F(x)$.

Lemma 3.4. *Let $f(x)$ be a monic polynomial over $\mathbb{F}_q$ with nonzero constant term. Then $f(0)^{-1}f(x)f^*(x)$ is both self-reciprocal and self-cojugate-reciprocal over $\mathbb{F}_q$.*

Proof. Let $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ be a polynomial of degree n over $\mathbb{F}_q$ with $a_0 \neq 0$. Then $f^*(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + 1$. Hence

$$\begin{aligned} f(0)^{-1}f(x)f^*(x) &= a_0^{-1}[(x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0) \\ &\qquad \cdot (a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + 1)] \\ &= a_0^{-1}[a_0x^{2n} + (a_1 + a_{n-1}a_0)x^{2n-1} + (a_2 + a_{n-1}a_1 + a_{n-2}a_0)x^{2n-2} \\ &\qquad + \ldots + (a_2 + a_1a_{n-1} + a_0a_{n-2})x^2 + (a_1 + a_0a_{n-1})x + a_0]. \end{aligned}$$

If we write $f(0)^{-1}f(x)f^*(x) = \sum_{i=0}^{2n} b_i x^i$ where $b_i \in \mathbb{F}_q$, then by comparing the coefficients, we have

$$\begin{aligned}
b_{2n} &= a_0^{-1}a_0 = 1 & b_0 &= a_0^{-1}a_0 = 1\\
b_{2n-1} &= a_0^{-1}[a_1 + a_{n-1}a_0] & b_1 &= a_0^{-1}[a_1 + a_0 a_{n-1}]\\
b_{2n-2} &= a_0^{-1}[a_2 + a_{n-1}a_1 + a_{n-2}a_0] & b_2 &= a_0^{-1}[a_2 + a_1 a_{n-1} + a_0 a_{n-2}]\\
&\vdots & &\vdots\\
b_{2n-i} &= a_0^{-1}\sum_{j=0}^{i} a_{n-j}a_{i-j} & b_i &= a_0^{-1}\sum_{j=0}^{i} a_{i-j}a_{n-j}\\
&\quad (i = 0, ..., n-1) & &\quad (i = 0, ..., n)\\
&\vdots & &\vdots\\
b_{2n-(n-1)} &= a_0^{-1}[a_{n-1} + a_{n-1}a_{n-2} + ... & b_{n-1} &= a_0^{-1}[a_{n-1} + a_{n-2}a_{n-1} + ...\\
&\qquad + a_2 a_1 + a_1 a_0] & &\qquad + a_1 a_2 + a_0 a_1]\\
& & b_n &= a_0^{-1}[a_n^2 + a_{n-1}^2 + ... + a_1^2 + a_0^2].
\end{aligned}$$

These imply that $b_{2n-i} = b_i$ for all $0 \le i \le 2n$. Thus $f(0)^{-1}f(x)f^*(x)$ is self-reciprocal. Moreover, $f(0)^{-1}f(x)f^*(x)$ is self-conjugate-reciprocal over $\mathbb{F}_q$ since $\overline{b_0^{-1}b_{2n-i}} = b_{2n-i} = b_i$ for all $0 \le i \le 2n$. ∎

Lemma 3.5. *Let $f(x)$ be a monic polynomial over $\mathbb{F}_q$ of degree n with nonzero constant term. Then $f(x)$ is self-conjugate-reciprocal over $\mathbb{F}_q$ if and only if $f^\dagger(x)$ is self-conjugate-reciprocal over $\mathbb{F}_q$.*

Proof. Let $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ be a monic polynomial over $\mathbb{F}_q$ of degree n with $a_0 \neq 0$. Then $f^\dagger(x) = x^n + a_0^{-1}a_1 x^{n-1} + ... + a_0^{-1}a_{n-1}x + a_0^{-1}$. It suffices to show that $(f^\dagger)^\dagger(x) = f(x)$. We have

$$\begin{aligned}
(f^\dagger)^\dagger(x) = (a_0^{-1})^{-1}x^n f^\dagger(1/x) &= a_0[a_0^{-1}x^n + a_0^{-1}a_{n-1}x^{n-1} + ... + a_0^{-1}a_1 x + 1]\\
&= x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = f(x)
\end{aligned}$$

as required. ∎

Definition 3.6. Let $g(x)$ and $h(x)$ be polynomials over $\mathbb{F}_q$ with $g(0) \neq 0$ and $h(0) \neq 0$. They are called a *conjugate-reciprocal pair* if there exists $\beta \in \mathbb{F}_q^*$ such that

$$g^\dagger(x) = \beta h(x).$$

Theorem 3.7. *Let $f(x)$ be a monic irreducible polynomial over $\mathbb{F}_q$ of degree n. Then either*

(i) *$F(x)$ is a qth power of an irreducible polynomial of degree $2n$ which is a self-conjugate-reciprocal polynomial over $\mathbb{F}_q$, or*

(ii) *$F(x)$ is a qth power of the product of a conjugate-reciprocal pair of irreducible polynomials over $\mathbb{F}_q$ of degree n.*

Proof. Let $f(x)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree n. We divide this proof into 2 cases according to Theorem 1.2 and Remark 3.3.

Case 1 $F(x) = [f_R(x)]^q$ where $f_R(x)$ is a SRIM polynomial of degree $2n$ over $\mathbb{F}_q$. In this case, it remains to show that $f_R(x)$ is self-conjugate-reciprocal over $\mathbb{F}_q$.

Let $f_R(x) = \sum_{i=0}^{2n} b_i x^i \in \mathbb{F}_q[x]$. Then $b_i = b_{2n-i}$ for all $0 \le i \le 2n$. Since $F(x)$ is self-conjugate-reciprocal, $F(0) = 1$. So,

$$1 = F(0) = (f_R(0))^q = f_R(0) = b_0.$$

Thus for each $0 \le i \le 2n$, $\overline{b_0^{-1} b_{2n-i}} = b_0^{-1} b_{2n-i} = b_i$. Therefore, $f_R(x)$ is self-conjugate-reciprocal over $\mathbb{F}_q$.

Case 2 $F(x) = [g(x)h(x)]^q$ where $g(x)$ and $h(x)$ are a reciprocal pair of monic irreducible polynomials over $\mathbb{F}_q$ of degree n, i.e., $g^*(x) = \gamma h(x)$ for some $\gamma \in \mathbb{F}_q^*$. We have $F(x) = [g(x)h(x)]^q = [g(x)\gamma^{-1} g^*(x)]^q$, and then

$$1 = F(0) = [g(0)\gamma^{-1} g^*(0)]^q = [g(0)\gamma^{-1}]^q = g(0)\gamma^{-1}.$$

Hence $\gamma = g(0)$. Now,

$$g^\dagger(x) = g(0)^{-1} g^*(x) = g(0)^{-1}\gamma h(x) = g(0)^{-1} g(0) h(x) = h(x).$$

Therefore, $g(x)$ and $h(x)$ are a conjugate-reciprocal pair. ■

From the proof of Theorem 3.7, we notice that if $f(x)$ is monic irreducible over $\mathbb{F}_q$ of degree n such that $F(x) = \Psi(f(x)) = [g(x)h(x)]^q$ where $g(x)$ and $h(x)$ are a conjugate-reciprocal pair of irreducible polynomials of degree n, then $h(x) = g^\dagger(x)$. Moreover, the product $g(x)h(x)$ is self-conjugate-reciprocal over $\mathbb{F}_q$ since $g(x)h(x) = g(x)g(0)^{-1}g^*(x)$ and $g(x)g(0)^{-1}g^*(x)$ is self-conjugate-reciprocal by Lemma 3.4.

For any polynomial over $\mathbb{F}_2$ with nonzero constant term, its constant term is always equal to 1, so we obtain the next corollary.

Corollary 3.8. *Let $f(x)$ be an irreducible polynomial over $\mathbb{F}_2$ of degree n. Then either*

(i) *$F(x)$ is a 2nd power of a irreducible polynomial of degree $2n$ which is a self-conjugate-reciprocal over $\mathbb{F}_2$, or*

(ii) *$F(x)$ is a 2nd power of the product of a conjugate-reciprocal pair of irreducible polynomials over $\mathbb{F}_2$ of degree n which are not self-conjugate-reciprocal.*

Proof. It remains to show that the conjugate-reciprocal pair appearing in (ii), say $g(x)$ and $h(x)$, are not self-conjugate-reciprocal polynomials. Write $g(x) = \sum_{i=0}^{n} a_i x^i$. By Theorem 1.2 (ii), $g(x)$ is not self-reciprocal. That is, there exists $i \in \{0, 1, ..., n\}$ such that $a_i \neq a_{n-i}$. So, $a_i \neq a_0^{-1} a_{n-i}$. This implies that $g(x)$ is not self-conjugate-reciprocal over $\mathbb{F}_2$. By Lemma 3.5, $g^\dagger(x)$ is not self-conjugate-reciprocal over $\mathbb{F}_2$. In fact, $h(x) = g^\dagger(x)$. It follows that $h(x)$ is not self-conjugate-reciprocal. ■

From above results, we have some properties of the factorization of $F(x)$ as follows.

Corollary 3.9. *If $f(x)$ is an irreducible polynomial over $\mathbb{F}_2$ then $F(x)$ is a 2nd power of SCRIM polynomial over $\mathbb{F}_2$ if and only if $f'(0) = 1$.*

Proof. By Remark 3.3 and Corollary 7 of [6]. ■

Corollary 3.10. *If $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ is a monic irreducible polynomial over $\mathbb{F}_{2^k} (k \ge 1)$ then $F(x)$ is a qth power of SCRIM polynomial over $\mathbb{F}_q$ if and only if $Tr_{\mathbb{F}_{2^k}}(a_1/a_0) = 1$.*

Proof. By Remark 3.3 and Theorem 6 of [6]. ■

Corollary 3.11. *Let q be an odd prime power. If $f(x)$ is an irreducible monic polynomial of degree n over $\mathbb{F}_q$ then $F(x)$ is a qth power of SCRIM polynomial over $\mathbb{F}_q$ if and only if $f(2)f(-2)$ is a non-square in $\mathbb{F}_q$.*

Proof. By Remark 3.3 and Theorem 8 of [6]. ∎

Acknowledgements

The authors would like to thank the referees for their comments and suggestions which helped improving the manuscript. The first author would like to thank the Science Achievement Scholarship of Thailand (SAST) for financial support throughout her Master's degree study at Chulalongkorn University.

References

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

[2] A. Boripan, Self-Conjugate-Reciprocal Irreducible Monic Polynomials over Finite Fields, Master's Thesis, Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, 2014.

[3] K.H. Hicks, G.L. Mullen, I. Sato, Distribution of irreducible polynomials over $\mathbb{F}_2$, In G.L. Mullen, H. Stichtenoth, H. Tapia-Recillas (eds.), Finite Fields with Applications in Coding Theory, Cryptography and Related Areas, Springer (2002), 177–186.

[4] S. Kobayashi, Y. Nogami, T. Sugimura, Generating irreducible self-reciprocal polynomials by using even polynomial over $\mathbb{F}_q$, In S. Taoka (ed.), Proceedings of the 23^{rd} International Technical Conference on Circuits Systems, Computers and Communications, Japan (2008) 121–124.

[5] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.

[6] H. Meyn, On the construction of irreducible self-reciprocal polynomials over finite fields, Appl. Algebra Engrg. Comm. Comput. 1 (1990) 43–53.

[7] H. Palasak, O. Phuksuwan, T. Chaichana, An existence of some class of self-conjugate-reciprocal irreducible polynomials over finite fields, In S. Piti et al. (eds.), Proceedings of Annual Pure and Applied Mathematics Conference 2017, Bangkok (2017) 234–240.

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