Some properties of generalized self-reciprocal polynomials over finite fields

[a],[*]Ryul Kim, [b]Ok-Hyon Song, [c]Hyon-Chol Ri

[a,b]Faculty of Mathematics, **Kim Il Sung** University, DPR Korea
[c]Department of Mathematics, Chongjin University of Education No.2, DPR Korea
[*]Corresponding author. e-mail address: ryul_kim@yahoo.com

Abstract

Numerous results on self-reciprocal polynomials over finite fields have been studied. In this paper we generalize some of these to a-self reciprocal polynomials defined in [4]. We consider some properties of the divisibility of a-reciprocal polynomials and characterize the parity of the number of irreducible factors for a-self reciprocal polynomials over finite fields of odd characteristic.

1   Introduction

Self-reciprocal polynomials over finite fields are of interest both from a theoretical and a practical viewpoint, so they are widely studied by many authors (see, for example, [2, 3, 5]). Carlitz [3] proposed a formula on the number of self-reciprocal irreducible monic (srim) polynomials over finite fields and Meyn [7] gave a simpler proof of it. Recently Carlitz's result was generalized by Ahmadi [1] and similar explicit results have been obtained in [6, 8]. Using the Stickelberger-Swan theorem, Ahmadi and Vega [2] characterized the parity of the number of irreducible factors of a self-reciprocal polynomials over finite fields. In [10], Yucas and Mullen classified srim polynomials based on their orders and considered the weight of srim polynomials. The problem concerning to the existence of srim polynomials with prescribed coefficients has also been considered, see [5].

On the other hand, Fitzgerald and Yucas [4] introduced a new notion of generalized reciprocal polynomial over finite fields to give new descriptions of the factors of Dickson polynomials over finite fields. They characterized the generalized reciprocal polynomials by their roots and orders so that the results of [10] were generalized. The generalization of reciprocal polynomials gives a possibility to find new special types of irreducible polynomials over finite fields. This motivated us to consider the generalized reciprocal polynomials over finite fields. Consideration of the divisibility and the number of irreducible factors of a given polynomial is the first step to test its irreducibility.

In this work we find some properties for the divisibility of generalized reciprocal and generalized self-reciprocal polynomials for the purpose of characterizing a class of the generalized srim polynomials. First we characterize the generalized

reciprocal of the product of given polynomials, extend the notion of generalized self-reciprocal polynomial defined only for even degree in [4] to odd degree and obtain some new results on the divisibility of trivial or nontrivial generalized self-reciprocal polynomials. Next we determine the parity of the number of irreducible factors of generalized self-reciprocal polynomials which is a generalization of the results in [2]. In fact, we also have obtained an explicit formula on the number generalized srim polynomials but when we prepare for submission, a more generalized result in [1] came to our view, so the formula was omitted from this paper.

Throughout the paper, let $q = p^e$ be an odd prime power, $\mathbf{F}_q$ be a finite field containing q elements and $0 \neq a \in \mathbf{F}_q$. For $f(x) \in \mathbf{F}_q[x]$, a monic polynomial of degree n with $f(0) \neq 0$, $\hat{f}_a(x) := \frac{x^n}{f(0)} f\left(\frac{a}{x}\right)$ is called a-reciprocal of $f(x)$ [4]. That is, if $f(x) = \sum_{i=0}^{n} b_i x^i$ then $\hat{f}_a(x) = (1/b_0) \sum_{i=0}^{n} b_i a^i x^{n-i}$. $\hat{f}_a(x)$ is also monic and if α is a root of $f(x)$ then a/α is a root of $\hat{f}_a(x)$. The case $a = 1$ is the usual reciprocal in [2, 7, 10].

2 Divisibility of generalized reciprocal polynomials

In this section we summarize some properties for the divisibility of generalized reciprocal and generalized self-reciprocal polynomials over $\mathbf{F}_q$.

Theorem 1. *a-reciprocal of a product of two polynomials is the product of a-reciprocals of given polynomials.*

Proof. Let $f(x) = \sum_{i=0}^{n} b_i x^i$, $g(x) = \sum_{j=0}^{m} c_j x^j$, $(b_0 \neq 0, c_0 \neq 0)$. From the definition,

$$\hat{f}_a(x) = \frac{1}{b_0} \sum_{i=0}^{n} b_i a^i x^{n-i} = \frac{1}{b_0} \sum_{i=0}^{n} b_{n-i} a^{n-i} x^i,$$

$$\hat{g}_a(x) = \frac{1}{c_0} \sum_{j=0}^{m} c_j a^j x^{m-j} = \frac{1}{c_0} \sum_{j=0}^{m} c_{m-j} a^{m-j} x^j,$$

$$\hat{f}_a(x) \cdot \hat{g}_a(x) = \frac{1}{b_0 c_0} \sum_{k=0}^{n+m} \left[\sum_{i+j=k} \left(b_{n-i} a^{n-i} \right) \left(c_{m-j} a^{m-j} \right) \right] x^k$$

$$= \frac{1}{b_0 c_0} \sum_{k=0}^{n+m} \left(\sum_{i+j=k} b_{n-i} \cdot c_{m-j} \cdot a^{n+m-k} \right) x^k$$

and

$$f(x) \cdot g(x) = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} b_i c_j \right) x^k = \sum_{k=0}^{n+m} d_k x^k \left(d_k := \sum_{i+j=k} b_i c_j \right).$$

Therefore

$$\widehat{fg}_a(x) = \frac{1}{b_0 c_0} \sum_{k=0}^{n+m} d_k a^k x^{n+m-k} = \frac{1}{b_0 c_0} \sum_{k=0}^{n+m} d_{n+m-k} a^{n+m-k} x^k$$

We set $i' := n - i, j' := m - j$, then

$$d_{n+m-k} = \sum_{i'+j'=k} b_{n-i'} c_{m-j'}$$

and thus

$$\widehat{fg}_a(x) = \frac{1}{b_0 c_0} \sum_{k=0}^{n+m} \left(\sum_{i'+j'=k} b_{n-i'} \cdot c_{m-j'} \cdot a^{n+m-k} \right) x^k.$$

$\square$

It might be $\hat{f}_a(x) = \hat{f}_b(x)$ for nonzero distinct elements a, b in $\mathbf{F}_q$. For example, if $f(x) = x^2 + c \in \mathbf{F}_5[x]$, $c \neq 0$, then $\hat{f}_2(x) = \hat{f}_3(x)$.

A monic polynomial $f(x) \in \mathbf{F}_q[x]$ is said to be a-self reciprocal when $\hat{f}_a(x) = f(x)$. In [4], the notion of a-self reciprocal polynomial has been defined for only even degree. Note that $f(x) = \sum_{i=0}^{n} b_i x^i$ is a-self reciprocal if and only if for each i, $b_{n-i} b_0 = b_i a^i$. When $i = n$, we see that $b_0^2 = a^n$.

First consider a case when n is odd. If a^n and thus a is not a square in $\mathbf{F}_q$, then there is not any a-self reciprocal monic (srm) polynomial of degree n. When $0 \neq a \in \mathbf{F}_q$ is a square in $\mathbf{F}_q$, if $f(x)$ is a-srm polynomial then either $b_0 = \sqrt{a}^n$ or $b_0 = -\sqrt{a}^n$.

Theorem 2. *Let n be an odd, $0 \neq a \in \mathbf{F}_q$ be a square in $\mathbf{F}_q$ and $f(x) \in \mathbf{F}_q[x]$ be a-srm polynomial of degree n.*
  (1) If $b_0 = \sqrt{a}^n$ then $f(x)$ is divided by $x + \sqrt{a}$.
  (2) If $b_0 = -\sqrt{a}^n$ then $f(x)$ is divided by $x - \sqrt{a}$.

Proof. Suppose $b_0 = \sqrt{a}^n$. Then we have

$$f\left(-\sqrt{a}\right) = \left(-\sqrt{a}\right)^n + b_{n-1}\left(-\sqrt{a}\right)^{n-1} + \cdots + b_1\left(-\sqrt{a}\right) + \left(\sqrt{a}\right)^n$$

$$= b_{n-1}\left(-\sqrt{a}\right)^{n-1} + \cdots + b_1\left(-\sqrt{a}\right),$$

$$\hat{f}_a\left(-\sqrt{a}\right) = -\frac{1}{\left(-\sqrt{a}\right)^n}\left[\sqrt{a}^n\left(-\sqrt{a}\right)^n + \cdots + b_{n-1}a^{n-1}\left(-\sqrt{a}\right) + a^n\right]$$

$$= -\left[\sqrt{a}^n + b_1\left(-\sqrt{a}\right) + \cdots + b_{n-1}\left(-\sqrt{a}\right)^{n-1} + \left(-\sqrt{a}\right)^n\right]$$

$$= -\left[b_1\left(-\sqrt{a}\right) + \cdots + b_{n-1}\left(-\sqrt{a}\right)^{n-1}\right] = -f\left(-\sqrt{a}\right)$$

and from $f = \hat{f}_a$, $f\left(-\sqrt{a}\right) = -f\left(-\sqrt{a}\right)$ which implies that $f\left(-\sqrt{a}\right) = 0$. The second case follows similarly. $\square$

Corollary 1. *If $0 \neq a \in \mathbf{F}_q$ is a square in $\mathbf{F}_q$, then $x + \sqrt{a}$ and $x - \sqrt{a}$ are the only a-srim polynomials of odd degree over $\mathbf{F}_q$.*

Next let n be an even, that is, $n = 2m$. $f(x) = \sum_{i=0}^{2m} b_i x^i$ is said to be *trivial* or *nontrivial* respectively, according to $b_0 = -a^m$ or $b_0 = a^m$[4]. If $f(x)$ is a trivial a-srm polynomial, then $f\left(\sqrt{a}\right) = f\left(-\sqrt{a}\right) = 0$, hence $f(x)$ is a multiple of $x^2 - a$. Therefore $x^2 - a$ is the only trivial a-srim polynomial. From the definition, $b_m b_0 = b_m a^m$ and $b_0 = -a^m$, so that $b_m = 0$, hence trivial a-srm polynomials have always even terms.

Lemma 1. $x^2 - a$ *is a trivial a-srm polynomial and* $\left(x^2 - a\right)^2$ *is a nontrivial one.*

Lemma 2. *The product of two a-srm polynomials satisfies the following multiplication table.*

$\cdot$	trivial	nontrivial
trivial	nontrivial	trivial
nontrivial	trivial	nontrivial

The proof of the above lemmas are very simple so we omit.

Theorem 3. *If* $f(x) \in \mathbf{F}_q[x]$ *is a-srm polynomial of even degree, then it can be written as* $f(x) = \left(x^2 - a\right)^k \cdot g(x)$*, where* $g(x)$ *is a nontrivial a-srm polynomial not divided by* $x^2 - a$ *and*

$$k = \begin{cases} odd, & f(x) \text{ is trivial}, \\ even, & f(x) \text{ is nontrivial} \end{cases}.$$

Proof. Suppose that $x^2 - a$ divides $f(x)$. Then $f(x) = \left(x^2 - a\right) \cdot f_1(x)$ for some $f_1(x) \in \mathbf{F}_q[x]$. If $f(x)$ is trivial, then $f_1(x)$ is nontrivial by Theorem 1 and the above lemmas. And if $f(x)$ is nontrivial, then $f_1(x)$ is trivial, so it is divided by $x^2 - a$ and it can be written as $f(x) = \left(x^2 - a\right)^2 \cdot f_2(x)$. Again from the above lemmas $f_2(x)$ is nontrivial. Continuing this procedure implies the claim. □

If $f(x) \in \mathbf{F}_q[x]$ is divided by $x^2 - a$, then $\sqrt{a}$ and $-\sqrt{a}$ are roots of $f(x)$. If a is a square in $\mathbf{F}_q[x]$, then there might be an a-srm polynomial which is not divided by $x^2 - a$ but has a root $\sqrt{a}$ or $-\sqrt{a}$. For example, if $q = 5, a = 4$, then $\sqrt{a} = 2, -\sqrt{a} = 3$,

$$f(x) = x^6 + x^5 + 3x^4 + 4x^3 + 2x^2 + x + 4 \in \mathbf{F}_5[x]$$

is a nontrivial 4-srm polynomial which is not divided by $x^2 - 4$ but $f(2) = 0$ and

$$g(x) = x^6 + 3x^4 + 3x^3 + 2x^2 + 4 \in \mathbf{F}_5[x]$$

is a nontrivial 4-srm polynomial which is not divided by $x^2 - 4$ but $g(3) = 0$.

Theorem 4. *Let* $f(x) \in \mathbf{F}_q[x]$ *be a nontrivial a-srm polynomial of degree* $n = 2m$ *and* a *be a square in* $\mathbf{F}_q$*. If* $f(x)$ *is not divided by* $x^2 - a$ *and* $f\left(\sqrt{a}\right) = 0$*, then it can be written as* $f(x) = \left(x - \sqrt{a}\right)^k \cdot g(x)$*, where* k *is even and* $g(x)$ *is a nontrivial a-srm polynomial with* $g\left(\sqrt{a}\right) \neq 0$*.*

Proof. Let $f(x) = \sum_{i=0}^{n} b_i x^i$ then by assumption $b_0 = f(0) = a^m = \sqrt{a}^n$. Set

$$f_1(x) := \frac{f(x)}{x - \sqrt{a}} = x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1 x + c_0 \in \mathbf{F}_q[x].$$

Clearly $\left(-\sqrt{a}\right) \cdot c_0 = b_0 = \sqrt{a}^n$ which implies that $c_0 = -\sqrt{a}^{n-1}$. Then $f_1(x)$ is a-srm polynomial since $x - \sqrt{a}$ is a-srm polynomial. By Theorem 2, $f_1(x)$ is divided by $x - \sqrt{a}$ and thus we can write as $f(x) = \left(x - \sqrt{a}\right)^2 \cdot f_2(x)$. It is clear that $\left(x - \sqrt{a}\right)^2$ is a nontrivial a-srm polynomial, hence $f_2(x)$ is a nontrivial a-srm polynomial of degree $n - 2$. Continuing this procedure for $f_2(x)$ completes the proof. □

When a is a square in $\mathbf{F}_q$, from this theorem the consideration of nontrivial a-srm polynomials not divided by $x^2 - a$ is reduced to the case of ones without roots $\sqrt{a}$ and $-\sqrt{a}$.

3 The parity of the number of irreducible factors of generalized self-reciprocal polynomials

In this section we characterize the parity of the number of irreducible factors of the nontrivial a-srm polynomials over $\mathbf{F}_q$.

Theorem 5. *Let $f(x) \in \mathbf{F}_q[x]$ be a nontrivial a-srm polynomial of degree $2n$ with r pairwise distinct irreducible factors over $\mathbf{F}_q$. Then $r \equiv 0 \pmod 2$ if and only if $(-1)^n a^{n(n-2)} f\left(\sqrt{a}\right) f\left(-\sqrt{a}\right)$ is a square in $\mathbf{F}_q$, where $\sqrt{a}$ is a square root of a in an extension of $\mathbf{F}_q$.*

Proof. Let $f(x) = \sum_{i=0}^{2n} b_i x^i$, then $f(x) = x^n g\left(x + \frac{a}{x}\right)$, where $g(x) = b_n + \sum_{i=0}^{n-1} b_{2n-i} D_{n-i,a}(x)$ and $D_{n-i,a}(x)$ is the Dickson polynomial [4]. Clearly $f(0) = a^n \neq 0$ and by properties of the resultant, $R(f, f') = R(f, nf - xf')$. Since

$$f'(x) = nx^{n-1}g(x+a/x) + x^n g'\left(x + \frac{a}{x}\right)\left(1 - \frac{a}{x^2}\right)$$

$$= nx^{n-1}g\left(x + \frac{a}{x}\right) + x^{n-2}g'\left(x + \frac{a}{x}\right)(x^2 - a)$$

and

$$nf(x) - xf'(x) = -x^{n-1}g'\left(x + \frac{a}{x}\right)(x^2 - a),$$

we have

$$D(f) = (-1)^{n(2n-1)}R(f, f') = (-1)^n \cdot f(0)^{-1} \cdot R(f, nf - xf')$$

$$= (-1)^n \cdot a^{-n} \cdot R(f, x^2 - a) \cdot R\left(f, -x^{n-1}g'\left(x + \frac{a}{x}\right)\right)$$

$$= (-1)^n \cdot a^{-n} \cdot f\left(\sqrt{a}\right) f\left(-\sqrt{a}\right) \cdot R\left(f, -x^{n-1}g'\left(x + \frac{a}{x}\right)\right)$$

Let $x_0, \cdots, x_{n-1}, \frac{a}{x_0}, \cdots, \frac{a}{x_{n-1}}$ be the roots of $f(x)$ in some extension of $\mathbf{F}_q$. Then

$$R\left(f, -x^{n-1}g'\left(x + \frac{a}{x}\right)\right) = \prod_{i=0}^{n-1} x_i^{n-1}g'\left(x_i + \frac{a}{x_i}\right)\prod_{i=0}^{n-1}\left(\frac{a}{x_i}\right)^{n-1}g'\left(\frac{a}{x_i} + x_i\right)$$

$$= \prod_{i=0}^{n-1} x_i^{n-1}g'\left(x_i + \frac{a}{x_i}\right)\prod_{i=0}^{n-1} a^{n-1}x_i^{1-n}g'\left(x_i + \frac{a}{x_i}\right)$$

$$= a^{n(n-1)}\left[\prod_{i=0}^{n-1} g'\left(x_i + \frac{a}{x_i}\right)\right]^2.$$

On the other hand, since x_i is a root of $f(x)$ if and only if $x_i + \frac{a}{x_i}$ is a root of $g(x)$ and

$$D(g) = (-1)^{n(n-1)/2}R(g, g') = (-1)^{n(n-1)/2}\prod_{i=0}^{n-1} g'\left(x_i + \frac{a}{x_i}\right),$$

we have
$$D(f) = (-1)^n a^{n(n-2)} f\left(\sqrt{a}\right) f\left(-\sqrt{a}\right) \cdot D(g)^2.$$
Required result follows from Stickelberger theorem [9] (see also [2, Theorem 4]). $\square$

Let $f(x) = \sum_{i=0}^{2n} b_i x^i$ be as in Theorem 5, then

$$f(x) = \sum_{i=0}^{n} b_{2i} x^{2i} + \sum_{i=0}^{n-1} b_{2i+1} x^{2i+1}$$

and

$$f\left(\sqrt{a}\right) = \sum_{i=0}^{n} b_{2i} a^i + \sqrt{a} \sum_{i=0}^{n-1} b_{2i+1} a^i,$$

$$f\left(-\sqrt{a}\right) = \sum_{i=0}^{n} b_{2i} a^i - \sqrt{a} \sum_{i=0}^{n-1} b_{2i+1} a^i.$$

Denote

$$A := \sum_{i=0}^{n} b_{2i} a^i, \qquad B := \sum_{i=0}^{n-1} b_{2i+1} a^i$$

then $f\left(\sqrt{a}\right) f\left(-\sqrt{a}\right) = A^2 - aB^2$, which means $f\left(\sqrt{a}\right) f\left(-\sqrt{a}\right) \in \mathbf{F}_q$. Since $f(x)$ is nontrivial, $b_i = b_{2n-i} a^{n-i}$. Therefore if n is odd, then

$$A = 2 \sum_{i=0}^{(n-1)/2} b_{2n-2i} a^{n-i}, \quad B = 2 \sum_{i=0}^{(n-3)/2} b_{2n-2i-1} a^{n-i-1} + b_n a^{(n-1)/2},$$

and if n is even then

$$A = 2 \sum_{i=0}^{n/2-1} b_{2n-2i} a^{n-i} + b_n a^{n/2}, \quad B = 2 \sum_{i=0}^{n/2-1} b_{2n-2i-1} a^{n-i-1}.$$

For any monic polynomial $f(x) \in \mathbf{F}_q[x]$ of degree n, denote $f_a^Q(x) := x^n f\left(x + \frac{a}{x}\right)$. Then $f_a^Q(x)$ is a nontrivial a-srm polynomial of degree $2n$. This is a natural generalization of $f^Q(x)$ in [7] and it has been mentioned in [4], too.

Theorem 6. *Suppose that $f(x) \in \mathbf{F}_q[x]$ is a monic irreducible polynomial of degree $n (\geq 1)$ and $f\left(\sqrt{a}\right) f\left(-\sqrt{a}\right) \neq 0$. Then $f_a^Q(x)$ is either a-srim polynomial or a product of a-reciprocal pair of irreducible polynomials of degree n which are not a-self reciprocal.*

Proof. Let α be any root of $f_a^Q(x)$. Then $\beta = \alpha + \frac{a}{\alpha}$ is a root of $f(x)$, so $\beta^{q^n} = \beta$. Here n is the smallest positive integer k with $\beta^{q^k} = \beta$. Multiply α^{q^n} to both sides of the identity

$$\alpha^{q^n} + \frac{a}{\alpha^{q^n}} = \beta^{q^n} = \beta = \alpha + \frac{a}{\alpha},$$

then

$$\alpha^{2q^n} + a = \alpha^{q^n+1} + a\alpha^{q^n-1}$$

and so

$$\left(\alpha^{q^n+1} - a\right)\left(\alpha^{q^n-1} - 1\right) = 0.$$

Hence $\alpha^{q^n+1} = a$ or $\alpha^{q^n-1} = 1$. When $\alpha^{q^n+1} = a$, the irreducible factor $g(x)$ of $f_a^Q(x)$ with a root α has degree ≥ 2 because if $g(x)$ has degree 1, then a is a square in $\mathbf{F}_q$ and $g(x) = x \pm \sqrt{a}$ which contradicts to $f(\sqrt{a})\,f(-\sqrt{a}) \neq 0$. Therefore $g(x)$ is a nontrivial a-srm polynomial of degree $2d$ for a positive divisor of n. If we assume $d < n$ then $\alpha^{q^d+1} = a$, so $\beta^{q^d} = \beta$, a contradiction. Hence $d = n$ and $f_a^Q(x)$ is irreducible over $\mathbf{F}_q$. When $\alpha^{q^n-1} = 1$, the irreducible factor $g(x)$ of $f_a^Q(x)$ with a root α divides $x^{q^n} - x$ and the degree of $g(x)$ is n. Therefore $f_a^Q(x)$ is a product of two n-degree irreducible polynomials $g(x)$ and $h(x) = \frac{f_a^Q(x)}{g(x)}$. Suppose $g(x)$ is a nontrivial a-srim polynomial, then $\alpha^{q^{n/2}+1} - a = 0$ which contradicts to the minimality of n. So $g(x)$ and $h(x)$ are not a-self reciprocal. And if $f_a^Q(x)$ has a root α then it also has a root $\frac{a}{\alpha}$, which implies easily that $h(x)$ is a-reciprocal of $g(x)$. $\qquad\square$

Finally we prove that Theorem 5 is still valid when $f(x)$ has repeated irreducible factors.

Theorem 7. *Let $f(x) \in \mathbf{F}_q[x]$ be a nontrivial a-srm polynomial of degree $2n$ with $f(\sqrt{a})\,f(-\sqrt{a}) \neq 0$, and let r be the number of irreducible factors counted with multiplicity of $f(x)$. Then r is even if and only if $(-1)^n a^{n(n-2)} f(\sqrt{a})\,f(-\sqrt{a})$ is a square in $\mathbf{F}_q$.*

Proof. As in the proof of Theorem 5, there exists $g(x) \in \mathbf{F}_q[x]$ such that $f(x) = x^n g\left(x + \frac{a}{x}\right)$. Suppose that $g(x) = g_1(x) \cdots g_k(x)$ where $g_i(x) \in \mathbf{F}_q[x]$ is monic irreducible polynomial of degree n_i and $n_1 + \cdots + n_k = n$. Denote $f_i(x) := x^{n_i} g_i\left(x + \frac{a}{x}\right)$, then $f(x) = f_1(x) \cdots f_k(x)$ where every $f_i(x)$ is a nontrivial a-srm polynomial of degree $2n_i$ over $\mathbf{F}_q$. By Theorem 6, every $f_i(x)$ is either irreducible or a product of two distinct monic irreducible polynomials of degree n_i. Now suppose that the claim holds for two nontrivial a-srm polynomials $g(x)$, $h(x)$ of degree $2s$, $2t$ with r_s, r_h irreducible factors counted with multiplicity respectively over $\mathbf{F}_q$. If both r_s and r_h are odd, then neither $(-1)^s a^{s(s-2)} g(\sqrt{a})g(-\sqrt{a})$ nor $(-1)^t a^{t(t-2)} h(\sqrt{a})h(-\sqrt{a})$ is a square in $\mathbf{F}_q$, hence $(-1)^{s+t} a^{(s+t)(s+t-2)} g(\sqrt{a}) g(-\sqrt{a})h(\sqrt{a})h(-\sqrt{a})$ is a square in $\mathbf{F}_q$. Similar observation about other cases for r_s and r_h tells us the claim is still valid for $g(x)h(x)$. It is sufficient to apply Theorem 5 to complete the proof. $\qquad\square$

References

[1] O. Ahmadi, Generalization of a theorem of Carlitz. Finite Fields Appl. 17 (2011) 473-480.

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

[3] L. Carlitz, Some theorems on irreducible reciprocal polynomials over a finite field, J. reine Angew. Math. 227 (1967) 212-220.

[4] R.W. Fitzgerald, J.L. Yucas, Generalized reciprocals, factors of Dickson polynomials and generalized cyclotomic polynomials over finite fields, Finite Fields Appl. 13 (2007) 492-515.

[5] T. Garefalakis, G. Kapetanakis, On the Hansen-Mullen conjecture for self-reciprocal irreducible polynomials, Finite Fields Appl. 18 (2012) 832-841.

[6] T. Garefalakis, On the action of $GL_2(\mathbf{F}_q)$ on irreducible poynomials over $\mathbf{F}_q$, J. Pure Appl. Algebra. 215 (2011) 1835-1843.

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

[8] H. Stichtenoth, A. Topuzoğlu, Factorization of a class of polynomials over finite fields, Finite Fields Appl. 18 (2012) 108-122.

[9] L. Stickelberger, Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, Verhandlungen des ersten Internationalen Mathematiker-Kongresses, Zürich,(1897) 182-193.

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