Generalization of a theorem of Carlitz

Omran Ahmadi

Claude Shannon Institute, University College Dublin, Dublin 4, Ireland

A R T I C L E I N F O	A B S T R A C T

We generalize Carlitz' result on the number of self-reciprocal monic irreducible polynomials over finite fields by showing that similar explicit formula holds for the number of irreducible polynomials obtained by a fixed quadratic transformation. Our main tools are a combinatorial argument and Hurwitz genus formula.

© 2011 Elsevier Inc. All rights reserved.

1. Introduction

Let $\mathbb{F}_q$ denote the finite field with q elements, where q is a prime power, and let $\mathbb{F}_q[x]$ denote the polynomial ring over $\mathbb{F}_q$. For $f(x)$, a polynomial of degree m over $\mathbb{F}_q$ whose constant term is nonzero, its *reciprocal* is the polynomial $f^*(x) = x^m f(1/x)$ of degree m over $\mathbb{F}_q$. A polynomial $f(x)$ is called *self-reciprocal* if $f^*(x) = f(x)$. The reciprocal of an irreducible polynomial is also irreducible. The roots of the reciprocal polynomial are the reciprocals of the roots of the original polynomial, and hence, any self-reciprocal irreducible monic (*srim*) polynomial of degree greater than one must have even degree, say $2n$.

Self-reciprocal irreducible polynomials over finite fields have been studied by many authors. Carlitz [3] counted the number of srim polynomials of degree $2n$ over a finite field for every n. He showed the following.

E-mail address: omran.ahmadi@ucd.ie.

Theorem 1. *(See [3].) Let SRIM$(2n, q)$ denote the number of srim polynomials of degree $2n$ over $\mathbb{F}_q$. Then*

$$SRIM(2n, q) = \begin{cases} \frac{1}{2n}(q^n - 1), & \text{if } q \text{ is odd and } n = 2^m, \\ \frac{1}{2n} \sum_{\substack{d|n, \\ d \text{ odd}}} \mu(d) q^{n/d}, & \text{otherwise.} \end{cases}$$

In [4,6], Cohen and Meyn, respectively, obtained the same result by methods simpler than that was used by Carlitz in [3].

In [1], it has been shown that if K is a field and $p(x) \in K[x]$ is a self-reciprocal polynomial of degree $2n$, then for some $f(x) \in K[x]$ of degree n, we have

$$p(x) = x^n f(x + x^{-1}) = x^n f\left(\frac{x^2 + 1}{x}\right). \tag{1}$$

This implies that self-reciprocal irreducible monic polynomials can be studied in the context of quadratic transformation of irreducible polynomials. A quadratic transformation of an irreducible polynomial $f(x)$ of degree n over $\mathbb{F}_q$ is the polynomial

$$p(x) = h(x)^n f\left(\frac{g(x)}{h(x)}\right), \tag{2}$$

where $g(x)$ and $h(x) \in \mathbb{F}_q[x]$ are coprime polynomials with

$$\max(\deg(g), \deg(h)) = 2.$$

Now it is natural to ask whether there exists a similar explicit formula for the number of irreducible polynomials of a fixed degree which have been obtained from other irreducible polynomials by applying a fixed quadratic transformation. In this paper we show that in fact this is the case and for any fixed quadratic transformation, we determine the number of irreducible polynomials of degree n over a finite field whose transformation is also irreducible. Our result generalizes Carlitz's result—Carlitz's formula for the number of srim polynomials can be recovered from our result. It should also be mentioned that in [7], the authors have developed a general framework for counting some families of irreducible polynomials including srim polynomials over finite fields. The results of [7] have some overlap with results of this paper although techniques are quite different.

The remainder of this paper is organized as follows. In Section 2, we state the main result of the paper. In Section 3, we gather some preliminary results which will be used in Section 4 which contains the proof of the main result. Finally we conclude by Section 5 which contains some remarks and comments.

In this paper $\mathcal{T}(m, q)$ denotes the set of elements from $\mathbb{F}_{q^m}$ which are not in any proper subfield of $\mathbb{F}_{q^m}$.

2. Main result

Throughout this section and Section 4 we assume that $g(x) = a_1 x^2 + b_1 x + c_1$ and $h(x) = a_2 x^2 + b_2 x + c_2$.

Theorem 2. *Let q be a prime power, and let $g(x)$ and $h(x) \in \mathbb{F}_q[x]$ be relatively prime polynomials with $\max(\deg(g), \deg(h)) = 2$. Also let $I_{(n,g,h)}$ be the set of monic irreducible polynomials $f(x)$ of degree $n > 1$ over $\mathbb{F}_q$ whose quadratic transformation by $g(x)$ and $h(x)$, i.e. $p(x) = h(x)^n f(\frac{g(x)}{h(x)})$, is irreducible over $\mathbb{F}_q$. Then*

$$\#I_{(n,g,h)} = \begin{cases} 0, & \text{if } b_1 = b_2 = 0 \text{ and } q = 2^l, \\ \frac{1}{2n}(q^n - 1), & \text{if } q \text{ is odd and } n = 2^m, \ m \geqslant 1, \\ \frac{1}{2n} \sum\limits_{\substack{d \mid n, \\ d \text{ odd}}} \mu(d)q^{n/d}, & \text{otherwise.} \end{cases}$$

Notice that Carlitz' result follows from the above theorem for $g(x) = x^2 + 1$ and $h(x) = x$.

3. Preliminaries

In this section we gather some results which will be used in the rest of the paper to prove the main result of the paper.

3.1. Polynomial transformation of irreducible polynomials

The following lemma is known as Capelli's lemma and can be found in [4] too.

Lemma 3. *Let $f(x)$ be a degree n irreducible polynomial over $\mathbb{F}_q$, and let $g(x), h(x) \in \mathbb{F}_q[x]$. Then $p(x) = h(x)^n f(g(x)/h(x))$ is irreducible over $\mathbb{F}_q$ if and only if for any root α of $f(x)$ in $\mathbb{F}_{q^n}$, $g(x) - \alpha h(x)$ is an irreducible polynomial over $\mathbb{F}_{q^n}$. In fact in order to show that $p(x)$ is irreducible over $\mathbb{F}_q$, it suffices to show that $g(x) - \alpha h(x)$ is an irreducible polynomial over $\mathbb{F}_{q^n}$ for some root α of $f(x)$ in $\mathbb{F}_{q^n}$.*

3.2. Resultant and discriminant

We begin this section by recalling the *Resultant* of polynomials over a field K. For a more detailed treatment see [5, Chapter 1, pp. 35–37].

Let $F(x)$ and $G(x) \in K[x]$ and suppose $F(x) = a \prod_{i=0}^{s-1}(x - x_i)$ and $G(x) = b \prod_{j=0}^{t-1}(x - y_j)$, where $a, b \in K$ and $x_0, x_1, \ldots, x_{s-1}, \ y_0, y_1, \ldots, y_{t-1}$ are in some extension of K. Then the *Resultant*, $\mathrm{Res}(F, G)$, of $F(x)$ and $G(x)$ is

$$\mathrm{Res}(F, G) = (-1)^{st} b^s \prod_{j=0}^{t-1} F(y_j) = a^t \prod_{i=0}^{s-1} G(x_i). \tag{3}$$

Notice that $\mathrm{Res}(F, G) = 0$ if and only if $F(x)$ and $G(x)$ have a common root in some extension of K. Thus if $\mathrm{Res}(F, G) \neq 0$, then $F(x)$ and $G(x)$ are coprime. There is another formulation of resultant of two polynomials which is easier to compute with as follows. Suppose $g(x) = a_1 x^2 + b_1 x + c_1$ and $h(x) = a_2 x^2 + b_2 x + c_2$ (for the formula for polynomials of higher degrees see [5, Chapter 1, pp. 35–37]). Then

$$\mathrm{Res}(g, h) = \begin{vmatrix} a_1 & b_1 & c_1 & 0 \\ 0 & a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 & 0 \\ 0 & a_2 & b_2 & c_2 \end{vmatrix}. \tag{4}$$

The following lemma which is probably already somewhere in the literature will be needed later. It follows from direct calculations. The right-hand side of (5) can be calculated using (4), and the left-hand side can be calculate using the usual formula for the discriminant of quadratic polynomials, and then equality of two sides can be checked.

Lemma 4. *Suppose $g(x) = a_1 x^2 + b_1 x + c_1$, $h(x) = a_2 x^2 + b_2 x + c_2$ and let y be an indeterminate. Then*

$$\mathrm{Disc}_y\big(\mathrm{Disc}_x\big(g(x) - yh(x)\big)\big) = 16\,\mathrm{Res}(g, h), \tag{5}$$

where Disc_x and Disc_y indicate that discriminant is taken with respect to variables x and y, respectively.

3.3. Hurwitz genus formula

Lemma 5. *(See [8, Theorem 5.9].)* Let $\mathbb{P}^1(\overline{\mathbb{F}_q})$ denote the one-dimensional projective space over $\overline{\mathbb{F}_q}$ (algebraic closure of $\mathbb{F}_q$), and let $\phi : \mathbb{P}^1(\overline{\mathbb{F}_q}) \to \mathbb{P}^1(\overline{\mathbb{F}_q})$ be a non-constant separable map. Then

$$2 \deg \phi - 2 \geqslant \sum_{P \in \mathbb{P}^1} \left(e_\phi(P) - 1\right),$$

where $e_\phi(P)$ is the ramification index of ϕ at P. Equality holds if and only if $e_\phi(P)$ is not divisible by the characteristic of $\mathbb{F}_q$ for all $P \in \mathbb{P}^1(\overline{\mathbb{F}_q})$.

4. Proof of the main theorem

Proof. Let $f(x)$ be a monic irreducible polynomial of degree n over $\mathbb{F}_q$. Using Lemma 3, $p(x)$ is irreducible over $\mathbb{F}_q$ if and only if for any root α of $f(x)$ in $\mathbb{F}_{q^n}$, $g(x) - \alpha h(x)$ is irreducible over $\mathbb{F}_{q^n}$. Thus in order to compute the number of irreducible polynomials $p(x) = h(x)^n f(\frac{g(x)}{h(x)})$ over $\mathbb{F}_q$ it suffices to compute the number of elements $\beta \in \mathcal{T}(n, q)$ for which

$$r_\beta(x) = g(x) - \beta h(x)$$

is irreducible in $\mathbb{F}_{q^n}[x]$ and divide the result by n.

Now for $m = 1, 2, 3, \ldots$, let

$$U(m, q) = \left\{\beta : \beta \in \mathcal{T}(m, q), \ r_\beta(x) \text{ is irreducible and quadratic over } \mathbb{F}_{q^n}\right\}. \tag{6}$$

Notice that

$$\#I_{(n,g,h)} = \frac{1}{n} \#U(n, q).$$

It turns out that we first need to compute the number of elements of some auxiliary sets. Thus let

$$\overline{U}(n, q) = \left\{\beta : \beta \in \mathbb{F}_{q^n}, \ r_\beta(x) \text{ is irreducible and quadratic over } \mathbb{F}_{q^n}\right\}, \tag{7}$$

and

$$V(n, q) = \left\{\beta : \beta \in \mathbb{F}_{q^n} \text{ and } \exists \gamma \in \mathbb{F}_{q^n} \text{ s.t. } g(\gamma) = \beta h(\gamma)\right\}. \tag{8}$$

If for $\beta \in \mathbb{F}_{q^n}$, $r_\beta(x)$ is not a constant polynomial over $\mathbb{F}_{q^n}$, then it is either irreducible over $\mathbb{F}_{q^n}$ or it has exactly two roots in $\mathbb{F}_{q^n}$ and gets factored as a product of two linear polynomials over $\mathbb{F}_{q^n}$. Thus if we let c be the number of $\beta \in \mathbb{F}_{q^n}$ for which $r_\beta(x)$ is a constant polynomial over $\mathbb{F}_{q^n}$, then

$$\#V(n, q) = q^n - c - \#\overline{U}(n, q). \tag{9}$$

In order to compute $\#V(n, q)$ we do a double counting as follows. Suppose that

$$W(n, q) = \left\{(\gamma, \beta) : \gamma, \beta \in \mathbb{F}_{q^n}; \ g(\gamma) = \beta h(\gamma)\right\}. \tag{10}$$

For every $\gamma \in \mathbb{F}_{q^n}$, there is a unique $\beta \in \mathbb{F}_{q^n}$ so that $g(\gamma) = \beta h(\gamma)$ unless γ is a root of $h(x) = 0$. Now let the number of roots of $h(x) = 0$ be a. Since $\deg(h(x)) \leqslant 2$, we have $a \leqslant 2$. Thus

$$\#W(n,q) = q^n - a; \quad a \leqslant 2. \tag{11}$$

On the other hand for every $\beta \in V(n,q)$ there are either one or two $\gamma \in \mathbb{F}_{q^n}$ such that $g(\gamma) = \beta h(\gamma)$. In order to compute $\#V(n,q)$ we need to know how many elements in $V(n,q)$ have exactly one preimage and how many have exactly two preimages. We deal with the fields of odd and even characteristic separately:

- Fields of even characteristic: we have two cases:
  - $b_1 = b_2 = 0$: for every $\beta \in V(n,q)$ there is exactly one $\gamma \in \mathbb{F}_{q^n}$ such that $g(\gamma) = \beta h(\gamma)$. In fact in this case $p(x)$ is always a square of a polynomial over $\mathbb{F}_q$ and hence the transformation by $g(x)$ and $h(x)$ does not result in any irreducible polynomial. This proves one of the cases of the main theorem. So in the rest of the paper we prove the remaining cases.
  - Either b_1 or b_2 is nonzero: for every $\beta \in V(n,q)$ the equation

    $$r_\beta(x) = g(x) - \beta h(x) = (a_1 - \beta a_2)x^2 + (b_1 - \beta b_2)x + (c_1 - \beta c_2) = 0$$

    has exactly two solutions in $\mathbb{F}_{q^n}$ unless either $r_\beta(x)$ is a linear polynomial or $b_1 - \beta b_2 = 0$. Each case can happen for at most one value of β.
- Fields of odd characteristic: for every $\beta \in V(n,q)$ there are exactly two γ such that $g(\gamma) = \beta h(\gamma)$, unless either

  $$r_\beta(x) = (a_1 - \beta a_2)x^2 + (b_1 - \beta b_2)x + (c_1 - \beta c_2)$$

  is a linear polynomial, or it is a quadratic polynomial with a repeated root and hence its discriminant

  $$w(\beta) = \mathrm{Disc}(h)\beta^2 + (4a_1c_2 + 4c_1a_2 - 2b_1b_2)\beta + \mathrm{Disc}(g) \tag{12}$$

  is zero. The linear case can happen for at most one value of β. In the quadratic case with repeated roots, we claim that Eq. (12) can be zero for at most two values of β. It suffices to show that $w(\beta)$ is not identically zero. Suppose that $w(\beta)$ is identically zero. Then all the coefficients of $w(\beta)$ are zero and hence $\mathrm{Disc}(w(\beta)) = 0$. But using Lemma 4 we have

  $$\mathrm{Disc}\big(w(\beta)\big) = 16\,\mathrm{Res}(g,h).$$

  This is a contradiction since we have assumed that $g(x)$ and $h(x)$ are relatively prime and do not have a common root.

Now if we let d be the number of β for which $r_\beta(x)$ is a linear polynomial and b be the number of β for which $r_\beta(x)$ is a quadratic polynomial and β has one preimage, then $d \leqslant 1$ and the above arguments show that $b \leqslant 2$. From this fact and Eq. (11) we deduce that

$$\#V(n,q) = \frac{\#W(n,q) + b + d}{2} = \frac{q^n - a + b + d}{2}$$

or equivalently

$$\#\overline{U}(n,q) = \frac{q^n + a - b - d - 2c}{2} = \frac{q^n + a - b - 2c - d}{2}. \tag{13}$$

Having computed $\#\overline{U}(n,q)$ we can compute $\#U(n,q)$. We claim that

$$\#\overline{U}(n,q) = \sum_{\substack{d|n \\ d \text{ odd}}} \#U(n/d,q). \tag{14}$$

Notice that if $\beta \in U(m,q)$ and $m \mid n$, then $\beta \in \overline{U}(n,q)$ if and only if n/m is an odd number since otherwise $\mathbb{F}_{q^n}$ contains a quadratic extension of $\mathbb{F}_{q^m}$ and hence $r_\beta(x)$ is not irreducible over $\mathbb{F}_{q^n}$ any more. This proves (14).

Using (13) and applying Möbius inversion we get

$$\#U(n,q) = \frac{1}{2} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d)\bigl(q^{n/d} + a - b - 2c - d\bigr)$$

$$= \frac{1}{2} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d)q^{n/d} + \frac{a-b-2c-d}{2} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d). \tag{15}$$

Now if n is not a power of two and hence has at least two odd positive divisors, then we have

$$\sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) = 0,$$

and thus

$$\#U(n,q) = \frac{1}{2} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d)q^{n/d}.$$

This finishes the proof for the case of n not being a power of two. On the other hand if $n = 2^m$ for some $m \geqslant 1$, then

$$\#U(n,q) = \frac{1}{2}\bigl(q^n + a - b - 2c - d\bigr).$$

In the sequel, we show that $a - b - 2c - d = -1$ if $\mathbb{F}_q$ is of odd characteristic and $a - b - 2c - d = 0$ if $\mathbb{F}_q$ is of even characteristic. In order to prove this we can use elementary arguments and consider many cases but here we use Hurwitz genus formula, Theorem 5, to give a shorter proof.

Now let Φ be a map defined over one-dimensional projective space over $\overline{\mathbb{F}_q}$ as follows

$$\Phi : \mathbb{P}^1(\overline{\mathbb{F}_q}) \to \mathbb{P}^1(\overline{\mathbb{F}_q}),$$
$$\Phi\bigl([X:Y]\bigr) = \bigl[a_1 X^2 + b_1 XY + c_1 Y^2 : a_2 X^2 + b_2 XY + c_2 Y^2\bigr].$$

Over the fields of odd characteristic, Φ is obviously separable and non-constant and furthermore since over fields of even characteristic we have assumed that either b_1 or b_2 is nonzero, it is separable over the fields of even characteristic, too. Thus one can apply Theorem 5 to the map Φ and conclude that over fields of odd characteristic Φ has two ramification points and over fields of even characteristic it has just one ramification point.

Now in order to avoid confusion in the rest of the proof, let ∞_1 and ∞_2 denote the points at infinity at the domain and range of the map Φ, respectively. In this setting, as we are assuming that

$n = 2^m$ for some $m \geqslant 1$, all the x and β related to a, b, c, d are in $\mathbb{F}_{q^2}$ and thus a is the number of finite preimages of ∞_2, b is the number of finite ramification points with finite image, c is one if ∞_1 is a ramification point and it image is finite and zero otherwise, and d is the number of finite points which have two preimages one of them being ∞_1.

Suppose that $\mathbb{F}_q$ is of odd characteristic. If ∞_2 is a branch point (its preimage is a ramification point), then its preimage $\Phi^{-1}(\infty_2)$ is either ∞_1 or finite. If $\Phi^{-1}(\infty_2)$ is ∞_1, then $a = 0$, $b = 1$ as we can have one more ramification point, $c = 0$ as there is no finite branch point having ∞_1 as preimage and $d = 0$ as there is no finite non-branch point having ∞_1 as preimage. If $\Phi^{-1}(\infty_2)$ is finite, then $a = 1$ and there is one more ramification point. If ∞_1 is ramified, then it is mapped to a finite point and hence $b = 0$, $c = 1$ and $d = 0$. If ∞_1 is unramified, then its image is finite and hence $b = 1$ as there should be two ramified points, $c = 0$ and $d = 1$.

If ∞_2 is not a branch point, then either it has two finite preimages or it has one finite preimage. If it has two finite preimages, then $a = 2$, either $b = 1$, $c = 1$ and $d = 0$ if ∞_1 is a ramification point or $b = 2$, $c = 0$ and $d = 1$ if ∞_1 is not a ramification point. If ∞_2 has one finite preimage, then $a = 1$, $b = 2$, $c = 0$ and $d = 0$.

We see that in all the cases if the characteristic of $\mathbb{F}_q$ is an odd number, then $a - b - 2c - d = -1$.

Similar arguments show that in the case of fields of even characteristic $a - b - 2c - d = 0$. This finishes the proof as if $n = 2^m$ and q is a power of two then

$$\frac{1}{2} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) q^{n/d} = \frac{1}{2} q^n. \qquad \square$$

5. Comments

5.1. Alternative proof approach

Since $r_\beta(x)$ is irreducible over fields of odd characteristic if and only if its discriminant is a non-square in $\mathbb{F}_{q^n}$, another approach that can be used to prove the main result for fields of odd characteristic is to see for how many β the discriminant of $r_\beta(x)$ is a non-square and for how many β it is a square in $\mathbb{F}_{q^n}$. This can be done using the following well-known lemma. The following lemma implies that a quadratic polynomial over a finite field of odd characteristic is a square almost as many times as it is a non-square.

Lemma 6. *(See [5, Theorem 5.48].) Let q be an odd prime power, and let $f(x) = a_2 x^2 + a_1 x + a_0 \in \mathbb{F}_q[x]$ where $a_2 \neq 0$. Let η be the quadratic character of $\mathbb{F}_{q^n}$. If $\mathrm{Disc}(f) \neq 0$, then $\sum_{c \in \mathbb{F}_{q^n}} \eta(f(c)) = -\eta(a_2)$.*

5.2. Palindromic primes

It is well known that the number $I(2n, q)$ of irreducible polynomials of degree $2n$ over $\mathbb{F}_q$ is

$$I(2n, q) = \frac{1}{2n} \sum_{d|2n} \mu(d) q^{2n/d},$$

and the probability that a random monic polynomial of degree $2n$ is irreducible over $\mathbb{F}_q$ is roughly $\frac{1}{2n}$. On the other hand, the number of polynomials of degree $2n$ obtained from a fixed quadratic transformation is q^n. Thus Carlitz' result and our result implies that the number of irreducible polynomials among the polynomials obtained by a quadratic transformation is roughly what one would expect. In [2], it was shown that

$$\frac{\text{Number of palindromic primes} \leqslant x \text{ written in base } g}{\text{Number of palindromic numbers} \leqslant x \text{ written in base } g} = O\left(\frac{\log\log\log x}{\log\log x}\right)$$

where the implied constant depends only on the base g and conjectured that

$$\frac{\text{Number of palindromic primes} \leqslant x \text{ written in base } g}{\text{Number of palindromic numbers} \leqslant x \text{ written in base } g} \sim C \frac{1}{\log x}$$

or roughly speaking palindromic numbers with respect to primality behave like random integers. Carlitz' result can be viewed as an affirmative answer to their conjecture in the finite field setting. Now we wonder what the analogue of our result is for the integer numbers and if one can establish results similar to those of [2]?

Acknowledgments

References

[1] O. Ahmadi, G. Vega, On the parity of the number of irreducible factors of self-reciprocal polynomials over finite fields, Finite Fields Appl. 14 (1) (2008) 124–131.
[2] W.D. Banks, D.N. Hart, M. Sakata, Almost all palindromes are composite, Math. Res. Lett. 11 (5–6) (2004) 853–868.
[3] L. Carlitz, Some theorems on irreducible reciprocal polynomials over a finite field, J. Reine Angew. Math. 227 (1967) 212–220.
[4] S.D. Cohen, On irreducible polynomials of certain types in finite fields, Proc. Cambridge Philos. Soc. 66 (1969) 335–344.
[5] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia Math. Appl., vol. 20, Addison–Wesley Publ. Co., Advanced Book Program, Reading, MA, 1983, with a foreword by P.M. Cohn.
[6] H. Meyn, On the construction of irreducible self-reciprocal polynomials over finite fields, Appl. Algebra Engrg. Comm. Comput. 1 (1) (1990) 43–53.
[7] R.C. Mullin, J.L. Yucas, G.L. Mullen, A generalized counting and factoring method for polynomials over finite fields, J. Combin. Math. Combin. Comput. 72 (2010) 121–143.
[8] J.H. Silverman, The Arithmetic of Elliptic Curves, Grad. Texts in Math., vol. 106, Springer-Verlag, New York, 1992, corrected reprint of the 1986 original.