Parity of the Number of Irreducible Factors for Composite Polynomials

Ryul Kim[*] Wolfram Koepf[†]

Abstract

Various results on parity of the number of irreducible factors of given polynomials over finite fields have been obtained in the recent literature. Those are mainly based on Swan's theorem in which discriminants of polynomials over a finite field or the integral ring $\mathbb{Z}$ play an important role. In this paper we consider discriminants of the composition of some polynomials over finite fields. The relation between the discriminants of composed polynomial and the original ones will be established. We apply this to obtain some results concerning the parity of the number of irreducible factors for several special polynomials over finite fields.

Keywords: Discriminant, Swan's theorem, Composition, Finite field

1 Introduction

Irreducible polynomials over finite fields are widely used in many applications to codes, cryptography and computer algebra. The construction and distribution of irreducible and primitive polynomials over finite fields have been investigated by many researchers [5, 10, 12].

Swan's theorem [13] is an important tool for determining parity of the number of irreducible factors of a given polynomial and thus giving a necessary condition for irreducibility of polynomials over finite fields. Below we write PNIF simply for 'parity of the number of irreducible factors'. Some results similar as Swan's theorem have been obtained for various classes of polynomials over finite fields [1-3,6-8]. In these results the discriminants of polynomials over finite fields or the integral ring $\mathbb{Z}$ are needed to compute. Swan found an elegant formula for the discriminant of a general trinomial and applied it for the determination of the PNIF of trinomials over $\mathbb{F}_2$. In [4] the result for the discriminants of certain self-reciprocal quadrinomials was established. The authors of this paper derived a formula for the discriminant of composite polynomial $f(ax+b)$ for their results. Concerning the

[*] Faculty of Mathematics and Mechanics, Kim Il Sung University, Pyongyang, D.P.R.Korea

[†] Department of Mathematics, University of Kassel, Kassel, F. R. Germany

irreducibility of some composite polynomials obtained from irreducible polynomials over finite fields already various considerable results have been achieved [10]. It is desirable to investigate the relation between the PNIF of a composition of two polynomials and that of the original polynomials for the treatment of polynomials with unknown PNIF. In this paper we consider the discriminants of some composite polynomials over finite fields. Then we apply this to determine the PNIF for several special polynomials over finite fields.

2 Background results

In this section we give some results which will be used in the following sections. First recall the discriminant and the resultant of polynomials over a field. Let $\mathbb{K}$ be a field, and let $f(x) = a\prod_{i=0}^{n-1}(x-\alpha_i) \in \mathbb{K}[x]$ be a polynomial of degree n with leading coefficient a where $\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$ are the roots of $f(x)$ in a certain extension of $\mathbb{K}$. Then the discriminant $D(f)$ of f is defined as follows:

$$D(f) = a^{2n-2}\prod_{i<j}(\alpha_i-\alpha_j)^2 \tag{1}$$

Let $f(x)$ be the same as above and let $g(x) = b\prod_{j=0}^{m-1}(x-\beta_j) \in \mathbb{K}[x]$, where $\beta_0, \beta_1, \cdots, \beta_{m-1}$ are the roots of $g(x)$ in a certain extension of $\mathbb{K}$. The resultant $R(f,g)$ of $f(x)$ and $g(x)$ is

$$R(f,g) = (-1)^{mn}b^n\prod_{j=0}^{m-1} f(\beta_j) = a^m\prod_{i=0}^{n-1} g(\alpha_i) \tag{2}$$

The resultant has the following properties.

Lemma 1 $[9,13]1)R(f,g) = (-1)^{mn}R(g,f)$

2) *If* c *is a constant,* $R(f,c) = R(c,f) = c^n$

3) $R(x,g) = g(0),\ R(f,-x) = f(0)$

4) $R(f_1f_2,g) = R(f_1,g)R(f_2,g),\ R(f,g_1g_2) = R(f,g_1)R(f,g_2)$

5) *If* $f = gq + r,\ deg\ r = t,$ *then* $R(f,g) = (-1)^{m(n-t)}b^{n-t}R(r,g)$

Proof. We prove only 5).

$$R(f,g) = (-1)^{mn}b^n\prod_{j=0}^{m-1}\left[g(\beta_j)q(\beta_j)+r(\beta_j)\right] = (-1)^{mn}b^n\prod_{j=0}^{m-1} r(\beta_j)$$

$$= (-1)^{mn-mt}b^{n-t}\left[(-1)^{mt}b^t\prod_{j=0}^{m-1} r(\beta_j)\right] = (-1)^{m(n-t)}b^{n-t}R(r,g).\square$$

The discriminant of a polynomial f can be given in terms of the resultant by

$$D(f) = \frac{1}{a}(-1)^{n(n-1)/2}R\left(f,f'\right) \tag{3}$$

where f' is the derivative of f.

In [9] the following chain rule for resultants was proved.

Theorem 1 *Let $f(x), g(x)$ be the same as above, $h(x) \in \mathbb{K}[x]$ and h_0 be the leading coefficient of $h(x)$. Then*

$$R\left(f(h), g(h)\right) = [h_0^{mn} R(f, g)]^{deg\ h} \tag{4}$$

unless h is (a constant which is) a common root of f and g.

This result is our main tool for computing the discriminant of composite polynomials.

Next let us recall Swan's results [13].

Theorem 2 *Let $f(x)$ be a polynomial of degree n over a finite field $\mathbb{F}_q$ with no repeated root where q is an odd prime power. Let r be the number of irreducible factors of $f(x)$ over $\mathbb{F}_q$. Then $r \equiv n \pmod 2$ if and only if $D(f)$ is a square in $\mathbb{F}_q$.*

Theorem 3 *Let $f(x)$ be a polynomial of degree n over $\mathbb{F}_2$ with no repeated root and let r be the number of irreducible factors of $f(x)$ over $\mathbb{F}_2$. Let $F(x) \in \mathbb{Z}[x]$ be any monic lift of $f(x)$ to the integers. Then $D(F) \equiv 1$ or $5 \pmod 8$ and $r \equiv n \pmod 2$ if and only if $D(f) \equiv 1 \pmod 8$.*

Using these results we determine the PNIF of composite polynomials over finite fields in some special cases.

3 The PNIF of composite polynomials over finite fields

First we deal with the PNIF of $f\left(x^t\right)$ for an arbitrary polynomial $f(x)$.

Lemma 2 *Let $\mathbb{K}$ be a field, $f(x) \in \mathbb{K}[x]$ be a polynomial of degree n with a leading coefficient a and let t be a positive integer. Then*

$$D\left(f\left(x^t\right)\right) = (-1)^{n^2 t(t-1)/2} a^{t-1} t^{nt} f(0)^{t-1} D\left(f(x)\right)^t \tag{5}$$

Proof. By (3) and Lemma 1 we can write

$$\begin{aligned} D\left(f\left(x^t\right)\right) &= \frac{1}{a}(-1)^{nt(nt-1)/2} R\left(f\left(x^t\right), f'\left(x^t\right) t x^{t-1}\right) \\ &= \frac{1}{a}(-1)^{nt(nt-1)/2} R\left(f\left(x^t\right), f'\left(x^t\right)\right) R\left(f\left(x^t\right), t\right) \left[R\left(f\left(x^t\right), x\right)\right]^{t-1} \\ &= \frac{1}{a}(-1)^{nt(nt-1)/2} t^{nt} f(0)^{t-1} R\left(f\left(x^t\right), f'\left(x^t\right)\right) \end{aligned}$$

Put $h(x) = x^t$ and apply Theorem 1. Then we get

$$R\left(f\left(x^t\right), f'\left(x^t\right)\right) = \left[R\left(f(x), f'(x)\right)\right]^t$$

Therefore

$$\begin{aligned} &D\left(f\left(x^t\right)\right) = \\ &\quad = (-1)^{\frac{nt(nt-1)}{2}-\frac{nt(n-1)}{2}} a^{t-1} t^{nt} f(0)^{t-1} \left[(-1)^{n(n-1)/2}\frac{1}{a}R\left(f(x), f'(x)\right)\right]^t \\ &\quad = (-1)^{n^2t(t-1)/2} a^{t-1} t^{nt} f(0)^{t-1} D\left(f(x)\right)^t \ \square \end{aligned}$$

(5) shows that if $f(x)$ has repeated root, then $f\left(x^t\right)$ also has. But the inverse is not true. For example, $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{F}_2$, but $f(x^2) = x^4 + x^2 + 1 = \left(x^2 + x + 1\right)^2$. Below we consider the relation between the PNIF of $f(x)$ and $f\left(x^t\right)$ over $\mathbb{F}_2$.

Theorem 4 *Let $f(x)$ be a polynomial of degree n over $\mathbb{F}_2$ with no repeated root. Let t be any positive integer and assume that $f(0) \neq 0$. Then*

1) *$f\left(x^t\right)$ has repeated root if and only if t is even.*

2) *If n is even and t is odd, or n is odd and $t \equiv \pm 1 \pmod 8$, then the PNIF of $f\left(x^t\right)$ coincides with one of $f(x)$.*

3) *If n is odd and $t \equiv \pm 3 \pmod 8$, then the PNIF of $f\left(x^t\right)$ is opposite to one of $f(x)$.*

Proof. In this case (5) can be written as follows.

$$D\left(f\left(x^t\right)\right) = (-1)^{n^2t(t-1)/2} t^{nt} D\left(f(x)\right)^t$$

If t is even, then $D\left(f\left(x^t\right)\right) = 0$ in $\mathbb{F}_2[x]$, that is, $f\left(x^t\right)$ has a repeated root over $\mathbb{F}_2$ and vice versa. Let t be odd and put $C = (-1)^{n^2t(t-1)/2} t^{nt}$. Since a square of odd integer is congruent to 1 modulo 8, it can be easily seen

$$C \equiv \begin{cases} 1, & \text{if } n \text{ is even and } t \text{ is odd, or } n \text{ is odd and } t \equiv \pm 1 \pmod 8, \\ 5, & \text{if } n \text{ is odd and } t \equiv \pm 3 \pmod 8 \end{cases}$$

Let $F(x) \in \mathbb{Z}[x]$ be any monic lift of $f(x)$ to the integers. Since $f(x)$ has no repeated root, Theorem 3 implies that $D\left(F(x)\right) \equiv 1 \,\text{or}\, 5 \pmod 8$ and therefore $D\left(F(x)\right)^t \equiv D\left(F(x)\right) \pmod 8$ for t is odd. Thus $D\left(F\left(x^t\right)\right) \equiv C \cdot D\left(F(x)\right) \pmod 8$ which gives the assertion of the theorem. □

Next we consider $f\left(L(x)\right)$ over finite fields where $L(x)$ is a linearized polynomial. Let $\mathbb{F}_q$ be a finite field of characteristic p. A polynomial of the form

$$L(x) = \sum_{i=0}^{t} \beta_i x^{q^i}$$

with coefficients β_i from $\mathbb{F}_{q^n}$ is called *q-polynomial* over $\mathbb{F}_{q^n}$. For fixed q, $L(x)$ is called a *linearized polynomial* over $\mathbb{F}_{q^n}$. A polynomial of the form

$$A(x) = L(x) + \beta, \quad \beta \in \mathbb{F}_{q^n}$$

is called an *affine polynomial* over $\mathbb{F}_{q^n}$ [10].

Lemma 3 *Let $\mathbb{F}_q$ and $f(x) \in \mathbb{F}_q[x]$ be the same as above and let t be a positive integer divided by p. Let $h_1(x)$ be any polynomial over $\mathbb{F}_q$ and $h(x) = h_1^t(x) + cx + d$ be a polynomial of degree k. Then*

$$D\left(f\left(h(x)\right)\right) = (-1)^{n^2k(k-1)/2} a^{k-1} c^{nk} h_0^{n[k\cdot\deg f'-1]} D\left(f(x)\right)^k \tag{6}$$

where h_0 is a leading coefficient of $h(x)$.

The proof of this lemma is simple and similar with Lemma 2, so we omit it. The linearized polynomials and affine polynomials are special cases of the polynomial $h(x)$ in Lemma 3.

The next simpler case is $f(cx+d)$. Regarding $h_1 = 0$, namely $h(x) = cx + d$, we have from (6)

$$D\left(f(cx+d)\right) = c^{n\cdot\deg f'} D\left(f(x)\right) \tag{7}$$

over an arbitrary field which is the result in [4]. It shows that for any element d in a given field, the PNIF of $f(x+d)$ and $f(x)$ are equal. And if $a = h_0 = c = 1$, namely $f(x)$ and $h(x)$ are monic, then (6) has the following form

$$D\left(f\left(h(x)\right)\right) = (-1)^{\frac{n^2k(k-1)}{2}} D\left(f(x)\right)^k \tag{8}$$

This can be used to get a criterion for determining the PNIF of composite polynomials over finite fields.

Theorem 5 *Let $\mathbb{F}_q$ be a finite field of odd characteristic p and t be a positive integer divided by p. Let $h(x) = h_1^t(x) + x + d \in \mathbb{F}_q[x]$ be a monic polynomial of even degree k. Then*

1) $f\left(h(x)\right)$ has repeated root if and only if $f(x)$ has.

2) If $f(x)$ has no repeated root, then $f\left(h(x)\right)$ has an even number of irreducible factors over $\mathbb{F}_q$ if and only if $(-1)^{\frac{n^2k(k-1)}{2}}$ is a square in $\mathbb{F}_q$.

Proof. 1) is trivial by (8) and 2) follows directly from Theorem 2 with the condition of even k. □

In [1], the PNIF of weight-n polynomials over $\mathbb{F}_2$ was considered. Using this we determine the PNIF of a special type of pentanomials over $\mathbb{F}_2$.

Theorem 6 *For any positive integer $k \geq 3$ and $l \geq 1$, the pentanomial*

$$f(x) = x^{2^k-1} + x^{2^l+1} + x^{2^l} + x + 1 \in \mathbb{F}_2[x]$$

has always an odd number of irreducible factors over $\mathbb{F}_2$ with only one exception $k = 3$, $l = 2$.

Proof. Consider the weight-n polynomial

$$F_{n,m}(x) = \frac{x^{n+1}+1}{x+1} + x^m \in \mathbb{F}_2[x]$$

where n is odd. We have the composite polynomial in $\mathbb{F}_2[x]$

$$F_{n,m}(x+1) = \frac{(x+1)^{n+1}+1}{x} + (x+1)^m$$

Let $G(x) \in \mathbb{Z}[x]$ be a monic lift of $F_{n,m}(x)$ to the integers, then $G(x+1)$ (composition in $\mathbb{Z}[x]$) is a monic lift of $F_{n,m}(x+1)$ to the integers and by (7), $D\left(G(x+1)\right) = D\left(G(x)\right)$. Thus by Theorem 3 the PNIF of $F_{n,m}(x)$ and $F_{n,m}(x+1)$ over $\mathbb{F}_2$ are equal. Put $u = 2^k - 1, m = 2^l + 1$, then

$$F_{2^k-1,2^l+1}(x+1) = x^{2^k-1} + (x+1)(x+1)^{2^l} = x^{2^k-1} + x^{2^l+1} + x^{2^l} + x + 1 = f(x).$$

The conditions $k \geq 3, l \geq 1$ imply $n = 2^k - 1 \equiv 7 \pmod 8$ and $m \neq 2$. And $m = n-2$ if and only if $k = 3, l = 2$. Therefore the assertion follows from Theorem 5 in [1]. □

The pentanomial of Theorem 6 is a special case of so called type I pentanomial defined in [11] and we were not yet able to find any result dealing with the PNIF of this type of pentanomial in the literature.

Finally consider the PNIF of the composite polynomial $f(x^2+x+1)$. Let

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{Z}[x]$$

be a monic polynomial of degree n with integer coefficients. Consider a homogeneous polynomial in two variables

$$F(x,y) = x^n + a_1x^{n-1}y + \cdots + a_{n-1}xy^{n-1} + a_ny^n \in \mathbb{Z}[x,y]$$

derived from $f(x)$.

Lemma 4

$$D\left(f\left(x^2+x+1\right)\right) = (-1)^n \cdot F(3,4) \cdot D\left(f(x)\right)^2 \ .$$

Proof. Put $g(x) = f\left(x^2+x+1\right)$. Then by Lemma 1 and Theorem 1, we get

$$\begin{aligned} D\left(g(x)\right) &= (-1)^{2n(2n-1)/2} R\left(g(x), g'(x)(2x+1)\right) \\ &= (-1)^{n(2n-1)} R\left(g(x), g'(x)\right) R\left(g(x), 2x+1\right) \\ &= (-1)^n R\left(f(x), f'(x)\right)^2 R\left(g(x), 2x+1\right) \end{aligned}$$

Since there exists a polynomial $q(x)$ such that

$$g(x) = (2x+1)q(x) + g\left(-\frac{1}{2}\right) = (2x+1)q(x) + f\left(\frac{3}{4}\right),$$

we use Lemma 1 again to get

$$\begin{aligned} D\left(g(x)\right) &= (-1)^n D\left(f(x)\right)^2 \cdot R\left(g(x), 2x+1\right) \\ &= (-1)^n D\left(f(x)\right)^2 \cdot 4^n \cdot R\left(f\left(\frac{3}{4}\right), 2x+1\right) \\ &= (-1)^n \cdot F(3,4) \cdot D\left(f(x)\right)^2 \ \square \end{aligned}$$

Now consider a binary polynomial

$$f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n\in\mathbb{F}_2[x]\ . \tag{9}$$

Theorem 7 *If a polynomial* (9) *has no repeated root, then the composition* $f\left(x^2+x+1\right)\in\mathbb{F}_2[x]$ *also has no repeated root. In this case assume that* $f\left(x^2+x+1\right)$ *has* r *irreducible factors over* $\mathbb{F}_2$*. Then* r *is even if and only if* $(-1)^nF(3,4)\equiv 1 \pmod 8$ *where* F *is a homogeneous polynomial corresponding to the monic lift of* $f(x)$ *to the integers.*

Proof. Let $D(f),D(g)$ be the discriminants of $f(x),g(x)=f\left(x^2+x+1\right)\in\mathbb{F}_2[x]$ in $\mathbb{F}_2[x]$, respectively. Then we get $D(g)=(-1)^{n(3n-1)/2}D(f)$ in the same way as above lemma and this gives the first assertion. The second part of the theorem is followed from Lemma 4 and Theorem 3. □

Theorem 8 *Let* $f(x),r$ *and* F *be as in Theorem 7. Then*

$$r\equiv n+a_1 \pmod 2$$

Proof. Let D be a discriminant of the monic lift of $f\left(x^2+x+1\right)$ to the integers. From Lemma 4, it can be easily seen

$$D\equiv(-1)^n\cdot F(3,4)\equiv(-1)^n\cdot\left(3^n+4a_1\cdot 3^{n-1}\right)\equiv 1+4a_1+4n \pmod 8$$

On the other hand, it follows that $D\equiv 1+4r \pmod 8$ by Theorem 3 since $f\left(x^2+x+1\right)$ is of even degree. This means $r\equiv n+a_1 \pmod 2$ □
Theorem 8 shows that the PNIF of a composite polynomial $f\left(x^2+x+1\right)\in\mathbb{F}_2[x]$ depends only on the degree n and the coefficient of x^{n-1} of the original polynomial $f(x)$. From this we get the necessary condition for a composite polynomial $f\left(x^2+x+1\right)$ to be irreducible over $\mathbb{F}_2$.

Corollary 1 *For a polynomial* $f(x)\in\mathbb{F}_2[x]$ *if* $f\left(x^2+x+1\right)$ *is irreducible over* $\mathbb{F}_2$*, then*

$$tr(f)=\begin{cases}1, & \text{if } n \text{ is even}\\ 0, & \text{if } n \text{ is odd}\end{cases}$$

We apply Theorem 8 to trinomials over $\mathbb{F}_2$ to get the following.

Corollary 2 *Let* $f(x)=x^n+x^k+1\in\mathbb{F}_2[x]$*. If* $f(x)$ *has no repeated root, then* $f\left(x^2+x+1\right)$ *has an even number of irreducible factors over* $\mathbb{F}_2$ *in the following cases*

1) $n-k=1$ *and* n *is odd,*

2) $n-k\geq 2$ *and* n *is even.*

References

[1] O. Ahmadi and A. Menezes, Irreducible polynomials over maximum weight, Utilitas Mathematica **72** (2007), 111-123

[2] 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** (2008), 124-131

[3] A. Bluher, A Swan-like theorem, Finite Fields and Their Applications **12** (2006), 128-138

[4] K. Dilcher and K. B. Stolarsky, Resultants and discriminants of Chebyshev and related polynomials, Transactions of the American Mathematical Society **357** (2004), 965-981

[5] S. Fan and W. Han, Primitive Polynomials over Finite Fields of Characteristic Two, AAECC **14** (2004), 381-395

[6] A. Hales and D. Newhart, Swan's theorem for binary tetranomials, Finite Fields and Their Applications **12** (2006), 301-311

[7] J. von zur Gathen, Irreducible trinomials over finite fields, Mathematics of Computation **72** (2003), 1987-2000

[8] W. Koepf and R. Kim, The parity of the number of irreducible factors for some pentanomials, preprint (2008)

[9] J. H. McKay and S. Sui-Sheng Wang, A chain rule for the resultant of two polynomials, Archiv der Mathematik **53** (1989), 347-351

[10] A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone and T. Yaghoobian, *Applications of Finite Fields*, Kluwer, 1993

[11] F. Rodriguez-Henriquez and C. K. Koc, Parallel multipliers based on special irreducible pentanomials, IEEE Transactions on Computers **52** (2003), 1535-1542

[12] I. E. Shparlinski, Finding irreducible and primitive polynomials, AAECC **4** (1993), 263-268

[13] R. G. Swan, Factorization of polynomials over finite fields, Pacific Journal of Mathematics **12** (1962), 1099-1106