Finite Fields and Their Applications 16 (2010) 137–143

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Parity of the number of irreducible factors for composite polynomials

Ryul Kim [a,1], Wolfram Koepf [b,*]

[a] Faculty of Mathematics and Mechanics, Kim Il Sung University, Pyongyang, Democratic People's Republic of Korea
[b] Department of Mathematics, University of Kassel, Kassel, Germany

ARTICLE INFO

Article history:
Received 4 September 2009
Revised 11 December 2009
Available online 31 December 2009
Communicated by D. Panario

Keywords:
Discriminant
Stickelberger's theorem
Swan's theorem

ABSTRACT

Various results on the 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 Stickelberger's and 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. A relation between the discriminants of the 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 types of polynomials over finite fields.

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 [5,12,14].

Swan's theorem [16] is an important tool for determining the parity of the number of irreducible factors of a given polynomial, thus giving a necessary condition for irreducibility of polynomials over finite fields. Below we will write for 'parity of the number of irreducible factors' simply PNIF. Some results similar to 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. Swan found an elegant formula for the discriminant of a general trinomial and applied it to the determination of the PNIF of trinomials over $\mathbb{F}_2$. In [4] a result for the discriminant of cer-

* Corresponding author.
E-mail address: koepf@mathematik.uni-kassel.de (W. Koepf).

[1] Research supported by Deutscher Akademischer Austauschdienst (DAAD).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2009.12.002

tain self-reciprocal quadrinomials was established. The authors of this paper derive a formula for the discriminant of the composite polynomial $f(ax+b)$. Various considerable results have been achieved concerning the irreducibility of some composite polynomials obtained from irreducible polynomials over finite fields [12]. It is desirable to investigate the relation between the PNIF of the 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 types of composite polynomials over finite fields. Then we apply this to determine the PNIF for several special cases.

2. Background results

In this section we give some definitions and collect some results which will be used in the following sections. First recall the notions of resultant and discriminant.

Definition 1. (See [9,17].) 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 $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ are the roots of $f(x)$ (counted with multiplicity) in a certain extension of $\mathbb{K}$ and let $g(x) = b\prod_{j=0}^{m-1}(x-\beta_j) \in \mathbb{K}[x]$, where $\beta_0, \beta_1, \ldots, \beta_{m-1}$ 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 defined by

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

and the *discriminant* $D(f)$ of f is given as

$$D(f) = a^{2n-2}\prod_{i<j}(\alpha_i-\alpha_j)^2 = \frac{1}{a}(-1)^{n(n-1)/2}R\big(f,f'\big) \tag{2}$$

where f' denotes the derivative of f. Note that $R(f,g) \in \mathbb{K}$ and $D(f) \in \mathbb{K}$.

The resultant has the following well-known properties.

Lemma 1. *(See [9,17].)*

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

In [11] the following chain rule for resultants was proved.

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

$$R\big(f(h),g(h)\big) = \big(h_0^{mn}R\big(f(x),g(x)\big)\big)^{\deg h} \tag{3}$$

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

Theorem 1 will be our main tool for computing the discriminant of composite polynomials. Next let us recall the results due to Stickelberger ([15], see also Swan [16]).

Theorem 2. *Let $f(x)$ be a squarefree polynomial of degree n over a finite field $\mathbb{F}_q$ 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 squarefree polynomial of degree n over $\mathbb{F}_2$ 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, i.e. $F(x) \equiv f(x) \pmod 2$. 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 will 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 $f(x^t)$ for an arbitrary polynomial $f(x)$. For this purpose we apply Theorem 1 with $h(x) = x^t$.

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

$$D\big(f\big(x^t\big)\big) = (-1)^{n^2t(t-1)/2} a^{t-1} t^{nt} f(0)^{t-1} D\big(f(x)\big)^t. \tag{4}$$

Proof. By (2) and Lemma 1 we can write

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

We put $h(x) = x^t$, apply Theorem 1 and get

$$R\big(f\big(x^t\big), f'\big(x^t\big)\big) = \big[R\big(f(x), f'(x)\big)\big]^t.$$

Therefore

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

Eq. (4) shows that if $f(x)$ is not squarefree, then $f(x^t)$ is neither. But the converse is not true. For example, $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{F}_2$, but $f(x^2) = x^4 + x^2 + 1 = (x^2 + x + 1)^2$. Below we consider the relation between the PNIF of $f(x)$ and $f(x^t)$ over $\mathbb{F}_2$.

Theorem 4. *Let $f(x)$ be a squarefree polynomial of degree n over $\mathbb{F}_2$. Let t be any positive integer and assume that $f(0) \neq 0$. Then*:

(1) *$f(x^t)$ is not squarefree 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 $f(x^t)$ coincides with that of $f(x)$.*
(3) *If n is odd and $t \equiv \pm 3 \pmod 8$, then the PNIF of $f(x^t)$ is the opposite of that of $f(x)$.*

Proof. In this case (4) can be written as

$$D\big(f\big(x^t\big)\big) = (-1)^{n^2t(t-1)/2}t^{nt}D\big(f(x)\big)^t. \tag{5}$$

If t is even, then $D(f(x^t)) = 0$ in $\mathbb{F}_2[x]$, that is, $f(x^t)$ is not squarefree over $\mathbb{F}_2$. The converse follows from the factor $t^{nt} \equiv 0 \pmod 2$ in (5). Let t be odd and put $C = (-1)^{n^2t(t-1)/2}t^{nt}$. Since a square of an odd integer is congruent to 1 modulo 8, it can be easily seen that

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

Let $F(x) \in \mathbb{Z}[x]$ be any monic lift of $f(x)$ to the integers. Since $f(x)$ is squarefree, Theorem 3 implies that $D(F(x)) \equiv 1$ or $5 \pmod 8$ and therefore $D(F(x))^t \equiv D(F(x)) \pmod 8$ for t is odd. Thus $D(F(x^t)) \equiv C \cdot D(F(x)) \pmod 8$ which gives the assertion of the theorem. □

Let $\mathbb{F}_q$ be a finite field of characteristic p. Next we consider $f(L(x))$ where $L(x)$ is a linearized polynomial [10]: A polynomial of the form

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

with coefficients $\beta_i \in \mathbb{F}_{q^n}$ 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 $\mathbb{F}_{q^n}$ [12].

Lemma 3. *Let $f(x) \in \mathbb{F}_q[x]$ be the same as above and let t be a positive integer multiple of 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*

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

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

The proof of this lemma is simple and similar to 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 case we consider is $f(cx+d)$. Regarding $h_1 = 0$, namely $h(x) = cx + d$, we get from (6)

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

over an arbitrary field which is the result in [4]. This shows in particular 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

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

This relation 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) *$f(h(x))$ is squarefree if and only if $f(x)$ is.*
(2) *If $f(x)$ is squarefree, then $f(h(x))$ has an even number of irreducible factors over $\mathbb{F}_q$ if and only if $(-1)^{\frac{n^2k(k-1)}{2}} a^{k-1}$ is a square in $\mathbb{F}_q$.*

Proof. (1) is trivial by (8) and (2) follows directly from Lemma 3 with the condition that k is even. □

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 $k \geqslant 3$, $k > l$ and $l \geqslant 1$, 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 the only 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 and $m < n$. 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 any 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), $D(G(x+1)) = D(G(x))$. Thus by Theorem 3 the PNIF of $F_{n,m}(x)$ and of $F_{n,m}(x+1)$ over $\mathbb{F}_2$ are equal.

Put $n = 2^k - 1$, $m = 2^l + 1$, 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 $k \geqslant 3$, $l \geqslant 1$ 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 [1, Theorem 5] or [7, Theorem 2] but can also be checked by hand. □

The pentanomial of Theorem 6 is a special case of the so-called type I pentanomials defined in [13]. Note that 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

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{Z}[x]$$

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

$$F(x, y) = x^n + a_1 x^{n-1} y + \cdots + a_{n-1} x y^{n-1} + a_n y^n \in \mathbb{Z}[x, y]$$

derived from $f(x)$.

Lemma 4.

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

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

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

By polynomial division we find a polynomial $q(x)$ such that

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

and we use Lemma 1 again to get

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

Finally consider a binary polynomial

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{F}_2[x]. \tag{9}$$

Theorem 7. *If a polynomial* (9) *is squarefree, then the composition* $f(x^2+x+1) \in \mathbb{F}_2[x]$ *is squarefree, too. In this case assume that* $f(x^2+x+1)$ *has* r *irreducible factors over* $\mathbb{F}_2$*. Then* r *is even if and only if* $(-1)^n F(3,4) \equiv 1 \pmod 8$ *where* F *is the homogeneous polynomial corresponding to a monic lift of* $f(x)$ *to the integers.*

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

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 a monic lift of $f(x^2+x+1)$ to the integers. From Lemma 4, it can be easily seen

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

On the other hand, it follows that $D \equiv 1 + 4r \pmod 8$ by Theorem 3 since $f(x^2+x+1)$ has even degree. This means $r \equiv n + a_1 \pmod 2$. $\square$

Theorem 8 shows that the PNIF of a composite polynomial $f(x^2+x+1) \in \mathbb{F}_2[x]$ depends only on the degree n and on the coefficient of x^{n-1} of the original polynomial $f(x)$. From this we get the following necessary condition for a composite polynomial $f(x^2+x+1)$ to be irreducible over $\mathbb{F}_2$.

Corollary 1. *If for a polynomial $f(x) \in \mathbb{F}_2[x]$ the composition $f(x^2+x+1)$ is irreducible over $\mathbb{F}_2$, then*

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

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 $f(x)$ is squarefree, then $f(x^2+x+1)$ has an even number of irreducible factors over $\mathbb{F}_2$ in the following cases*:

(1) $n-k=1$ *and n is odd,*
(2) $n-k \geqslant 2$ *and n is even.*

References

[1] O. Ahmadi, A. Menezes, Irreducible polynomials of maximum weight, Util. Math. 72 (2007) 111–123.
[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] A. Bluher, A Swan-like theorem, Finite Fields Appl. 12 (2006) 128–138.
[4] K. Dilcher, K.B. Stolarsky, Resultants and discriminants of Chebyshev and related polynomials, Trans. Amer. Math. Soc. 357 (2004) 965–981.
[5] S. Fan, W. Han, Primitive polynomials over finite fields of characteristic two, Appl. Algebra Engrg. Comm. Comput. 14 (2004) 381–395.
[6] J. von zur Gathen, Irreducible trinomials over finite fields, Math. Comp. 72 (2003) 1987–2000.
[7] A. Hales, D. Newhart, Swan's theorem for binary tetranomials, Finite Fields Appl. 12 (2006) 301–311.
[8] W. Koepf, R. Kim, The parity of the number of irreducible factors for some pentanomials, Finite Fields Appl. 15 (2009) 585–603.
[9] W. Koepf, Computeralgebra, Springer, Berlin, 2008.
[10] R. Lidl, H. Niederreiter, Finite Fields, 2nd edition, Encyclopedia Math. Appl., vol. 20, Cambridge University Press, Cambridge, 1996.
[11] J.H. McKay, S. Sui-Sheng Wang, A chain rule for the resultant of two polynomials, Arch. Math. 53 (1989) 347–351.
[12] A.J. Menezes, I.F. Blake, X. Gao, R.C. Mullin, S.A. Vanstone, T. Yaghoobian, Applications of Finite Fields, Kluwer, 1993.
[13] F. Rodriguez-Henriquez, C.K. Koc, Parallel multipliers based on special irreducible pentanomials, IEEE Trans. Comput. 52 (2003) 1535–1542.
[14] I.E. Shparlinski, Finding irreducible and primitive polynomials, Appl. Algebra Engrg. Comm. Comput. 4 (1993) 263–268.
[15] L. Stickelberger, Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, in: Verh. I. Internat. Math.-Kongress Zürich, 1897, Leipzig, 1898, pp. 182–193.
[16] R.G. Swan, Factorization of polynomials over finite fields, Pacific J. Math. 12 (1962) 1099–1106.
[17] R. Zippel, Effective Polynomial Computation, Springer, 1993.