Gen. Math. Notes, Vol. 10, No. 1, May 2012, pp.51-57
ISSN 2219-7184; Copyright ©ICSRS Publication, 2012
www.i-csrs.org
Available free online at http://www.geman.in

On the Reducibility of Some Composite Polynomials over Finite Fields

Saeid, Mehrabi[1] and Mohammad Javad, Ataei[2]

[1]The Holy Prophet Higher Education Complex
Esfahan, Iran
E-mail: saeid_mehrabi@yahoo.com
[2]Department of Mathematics Payame Noor University
Tehran, Iran
E-mail: ataeymj@pnu.ac.ir

(Received: 12-4-12/Accepted: 30-5-12)

Abstract

This paper presents the reducibility of some composite polynomials and explicitly determines the factorization over finite fields.

Keywords: *Galois fields, irreducible polynomial, composition method.*

1. Introduction

Let $\mathbb{F}_q$ be a Galois field with $q = p^s$ elements of characteristic p, and $\mathbb{F}_q^*$ is multiplicative group of $\mathbb{F}_q$. The problem of irreducibility of polynomials and determining the reducibility of a given polynomial stems both from mathematical theory and applications. At mathematical aspects determining the reducibility of a polynomial often appears in number theory, combinatorics and algebraic geometries. The study of irreducible polynomials is an old but currently still active subject. One of the methods for constructing irreducible polynomials is composition method. Probably the most powerful result in this area is the following theorem by S. Cohen that states as follows.

Theorem 1. *(Cohen [1]) Let $f(x), g(x) \in \mathbb{F}_q[x]$, and let $P(x) \in \mathbb{F}_q[x]$ is an irreducible polynomial of degree n. Then $F(x) = g(x)^n P(\frac{f(x)}{g(x)})$ is irreducible* *over $\mathbb{F}_q$ if and only if $f(x)-\alpha g(x)$ is irreducible over $\mathbb{F}_{q^n}$ for some root $\alpha \in \mathbb{F}_{q^n}$ of $P(x)$.*

The trace function of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is

$$Tr_{q^n|q}(\alpha) = \sum_{i=0}^{n} \alpha^{q^i}, \quad \alpha \in \mathbb{F}_{q^n}$$

It is clear that the trace function is a linear functional from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$. Also for a polynomial $f(x)$ over $\mathbb{F}_q$ of degree n its reciprocal polynomial is $f^*(x) = x^n f(\frac{1}{x})$. Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree n, then the least positive integer e for which $f(x)$ divides $x^e - 1$ is called the order of f and denoted by $ord(f)$. From [4] we have $ord(f)$ divides $q^n - 1$. If $ord(f) = q^n - 1$ then we call $f(x)$ is a primitive polynomial over $\mathbb{F}_q$. Also $ord(f)$ is equal to the order of any root of f in the multiplicative group $\mathbb{F}_q^*$, namely $ord(f) = ord(\alpha)$ for any root $\alpha \in \mathbb{F}_{q^n}$ of $f(x)$.
Recently, M. Kyuregyan and G. Kyuregyan [3] presented the following theorem for constructing irreducible polynomials which in our considering we apply this theorem and is a powerful tool in constructing in the present paper.

Theorem 2. *(M.K.Kyuregyan and G.M.Kyureguan) A monic polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $n = dk$ is irreducible over $\mathbb{F}_q$ if and only if there is a monic irreducible polynomial $h(x) = \sum_{i=0}^{k} h_i x^i$ over $\mathbb{F}_{q^d}$ of degree k such that $\mathbb{F}_q(h_0, ..., h_k) = \mathbb{F}_{q^d}$ and $f(x) = \prod_{v=0}^{d-1} h^{(v)}(x)$ on $\mathbb{F}_{q^d}[x]$, where*

$$h^{(v)}(x) = \sum_{i=0}^{k} h_i^{q^v} x^i$$

(Note that notation $h^{(0)}(x) = h(x)$ is used)
Indeed by using this theorem, they provide a short proof for the Cohen's Theorem. This time, we mention some propositions that we will need in the next section. The following propositions are well known and can be found in [2].
Proposition 1. For $x^q - x - b$ with $b \in \mathbb{F}_q^*$, the following factorization over $\mathbb{F}_q$ is complete.

$$x^q - x - b = \prod_{j=1}^{\frac{q}{p}} (x^p - b^{p-1}x - b^p \beta_j)$$

where β_j are the distinct elements of $\mathbb{F}_q$ with $Tr_{q|p}(\beta_j) = 1$.
Proposition 2. For $a, b \in \mathbb{F}_q$ with $a \neq 0, 1$, the following factorization is complete.

$$x^q - ax - b = (x - \frac{b}{1-a}) \prod_{j=1}^{\frac{q-1}{t}} ((x - \frac{b}{1-a})^t - \beta_j)$$

where $t = ord(a)$ and the β_j are all $\frac{q-1}{t}$ distinct roots of $x^{\frac{q-1}{t}} - a$.

Through this paper we always assume that $P(x)$ is monic. For this matter define

$$H(a,d) = \begin{cases} a^n & \text{for } \; d = 0, \\ d^n P(\frac{a}{d}) & \text{for } \; d \neq 0. \end{cases}$$

In the present paper we consider the factorization of some composition polynomials when assumptions on the Cohen's Theorem fail to hold and in particular, we obtain explicit family of irreducible polynomials of degree $n(q^n - 1)$ over $\mathbb{F}_q$ from a given primitive polynomial of degree n over $\mathbb{F}_q$.

2. Reducibility of Composite Polynomials of the Form $(dx^{q^n} - rx + h)^n P(\frac{ax^{q^n} - bx + c}{dx^{q^n} - rx + h})$

Let $P(x)$ is an irreducible polynomial of degree n over $\mathbb{F}_q$, then it can be represented in $\mathbb{F}_{q^n}[x]$ as

$$P(x) = \prod_{u=0}^{n-1} (x - \alpha^{q^u}),$$

where $\alpha \in \mathbb{F}_{q^n}$ is a root of $P(x)$. Suppose $ax^{q^n} - bx + c,\ dx^{q^n} - rx + h$ be relatively prime polynomials from $\mathbb{F}_q[x]$ with a or d bing non-zero. Set

$$F(x) = (dx^{q^n} - rx + h)^n P(\frac{ax^{q^n} - bx + c}{dx^{q^n} - rx + h}) = H(a,d) \prod_{u=0}^{n-1} h^{(u)}(x)$$

where

$$h^{(u)}(x) = x^{q^n} - (\frac{b - \alpha r}{a - \alpha d})^{q^u} x - (\frac{\alpha h - c}{a - \alpha d})^{q^u}$$

$$= (x^{q^n} - Ax - B)^{(u)} \in \mathbb{F}_{q^n}[x], \quad u = 0, ..., n-1, \tag{1}$$

and

$$A = \frac{b - \alpha r}{a - \alpha d}, \quad B = \frac{\alpha h - c}{a - \alpha d}.$$

We will consider separately 2 cases for this problem.

2.1 Reducibility of composite polynomial of the form

$$(x^{q^n} - x + \delta_1)^n P(\frac{x^{q^n} - x + \delta_0}{x^{q^n} - x + \delta_1})$$

In this subsection suppose in relation (1) $A = 1$ and as a typically, consider reducibility

$$F(x) = (x^{q^n} - x + \delta_1)^n P(\frac{x^{q^n} - x + \delta_0}{x^{q^n} - x + \delta_1}) = P(1) \prod_{u=0}^{n-1} h^{(u)}(x), \qquad (2)$$

where $\delta_0,\ \delta_1 \in \mathbb{F}_q,\ \delta_0 \neq \delta_1$ and

$$h^{(u)}(x) = x^{q^n} - x - B^{q^u} \in \mathbb{F}_{q^n}[x], \quad B = \frac{\delta_1 \alpha - \delta_0}{1 - \alpha}.$$

Let γ be a root of $h(x) = x^{q^n} - x - B$, so the conjugates of γ over $\mathbb{F}_{q^n}$ are $\gamma, \gamma^{q^n}, ..., \gamma^{q^{(p-1)n}}$. On the other hand $\lambda_k = \gamma + kB,\ \ k = 0, 1, ..., p-1$ are roots of minimal polynomial γ. Hence

$$m_\gamma(x) = \prod_{k=0}^{p-1}(x - (\gamma + kB)) = B^p \prod_{k=0}^{p-1}(\frac{x - \gamma}{B} - k)$$

$$= B^p((\frac{x-\gamma}{B})^p - (\frac{x-\gamma}{B})) = x^p - B^{p-1}x + \gamma B^{p-1} - \gamma^p \in \mathbb{F}_{q^n}[x].$$

So an irreducible factor of $h(x) = x^{q^n} - x - B \in \mathbb{F}_{q^n}[x]$ is of the form

$$x^p - B^{p-1}x - \beta, \quad \beta \in \mathbb{F}_{q^n}. \qquad (3)$$

Let θ be a root of (3) in some extension field of $\mathbb{F}_{q^n}$. Then we obtain

$$(\frac{\theta}{B^p})^{p^i} - (\frac{\theta}{B})^{p^{i-1}} = (\frac{\beta}{B^p})^{p^{i-1}} \quad i = 1, ..., ns \ (q = p^s). \qquad (4)$$

Summing (4) yields

$$\theta^{q^n} - \theta = BTr_{q^n|p}(\frac{\beta}{B^p})$$

On the other side $h(\theta) = 0$, or $\theta^{q^n} - \theta = B$. Therefore

$$Tr_{q^n|p}(\frac{\beta}{B^p}) = 1$$

We know that there are $\frac{q^n}{p}$ elements β in $\mathbb{F}_{q^n}$ with trace 1.
So that we obtain, $x^p - B^{p-1}x - B^p\beta_j$ where $Tr_{q^n|p}(\beta_j) = 1$ are factors of $h(x)$. It implies that

$$h(x) = x^{q^n} - x - B = \prod_{i=1}^{\frac{q^n}{p}}(x^p - B^{p-1}x - B^p\beta_i) = \prod_{i=1}^{\frac{q^n}{p}} s_i(x).$$

The same reasoning shows that for every $u = 1, 2, ..., n-1$ we have

$$h^{(u)}(x) = x^{q^n} - x - B^{q^u} = \prod_{i=1}^{\frac{q^n}{p}} (x^p - B^{p-1}x - B^p\beta_i)^{(u)} = \prod_{i=1}^{\frac{q^n}{p}} s_i^{(u)}(x). \qquad (5)$$

According to (2) and (5) we thus obtain

$$F(x) = P(1)\prod_{u=0}^{n-1} h^{(u)}(x) = P(1)\prod_{u=0}^{n-1}\prod_{i=1}^{\frac{q^n}{p}} s_i^{(u)}(x)$$

$$= P(1)\prod_{i=1}^{\frac{q^n}{p}}\prod_{u=0}^{n-1} s_i^{(u)}(x) = P(1)\prod_{i=1}^{\frac{q^n}{p}} k_i(x),$$

where $k_i(x)$ is an irreducible polynomial of degree np over $\mathbb{F}_q$. We formulate this result as below theorem.

Theorem 3. *Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial of degree n over $\mathbb{F}_q$ and $\delta_0, \delta_1 \in \mathbb{F}_q, \delta_0 \neq \delta_1$. Then*

$$F(x) = (x^{q^n} - x + \delta_1)^n P(\frac{x^{q^n} - x + \delta_0}{x^{q^n} - x + \delta_1})$$

decompose as a product of $\frac{q^n}{p}$ irreducible polynomials of degree np over $\mathbb{F}_q$.

Let's suppose $f(x) \in \mathbb{F}_q[x]$ be a primitive polynomial of degree n and set

$$P_1^*(x) = f(x+1), \quad P(x) = P_1(x-1).$$

So if α be some root of $P(x)$ then $\frac{\alpha}{\alpha-1}$ is some root of $f(x)$ and thus element $\frac{\alpha}{\alpha-1}$ is a primitive element in $\mathbb{F}_{q^n}$. Now in special case define

$$F(x) = (x^{q^n} - x + \delta_1)^n P(\frac{x^{q^n} + \delta_0}{x^{q^n} - x + \delta_1}).$$

Therefore

$$F(x) = P(1)\prod_{u=0}^{n-1} h^{(u)}(x),$$

where

$$h^{(u)}(x) = \left(x^{q^n} - (\frac{\alpha}{\alpha-1})x - \frac{\alpha\delta_1 - \delta_0}{1-\alpha}\right)^{(u)}, \ u = 0, 1, ..., n-1.$$

In view of Proposition 2, we obtain

$$h(x) = x^{q^n} - (\frac{\alpha}{\alpha - 1})x - \frac{\alpha\delta_1 - \delta_0}{1 - \alpha} = (x - \lambda)s(x),$$

so that

$$\lambda = \alpha\delta_1 - \delta_0 \in \mathbb{F}_{q^n},$$

and $s(x)$ is an irreducible polynomial of degree $q^n - 1$ over $\mathbb{F}_q$. Then it can be derived that

$$F(x) = P(1)\prod_{u=0}^{n-1} h^{(u)}(x) = P(1)\prod_{u=0}^{n-1}(x - \lambda^{q^u})s^{(u)}(x) = m_\lambda(x)g(x),$$

where by Theorem 2, $g(x)$ is an irreducible polynomial of degree $n(q^n - 1)$ over $\mathbb{F}_q$ and $m_\lambda(x)$ is minimal polynomial $\lambda \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$. It can be shown that

$$m_\lambda(x) = P(\frac{x + \delta_0}{\delta_1}).$$

This proves the validity of the below theorem.

Theorem 4. *Let $\delta_0,\ \delta_1 \in \mathbb{F}_{q^n}$. Suppose $f(x)$ be a primitive polynomial of degree n over $\mathbb{F}_q$. Set*

$$P_1^*(x) = f(1 + x), \quad P(x) = P_1(x - 1).$$

Then the polynomial

$$g(x) = (x^{q^n} - x + \delta_1)^n P(\frac{x^{q^n} + \delta_0}{x^{q^n} - x + \delta_1}) \left(P(\frac{x + \delta_0}{\delta_1})\right)^{-1},$$

is an irreducible polynomial of degree $n(q^n - 1)$ over $\mathbb{F}_q$.

2.2 Reducibility of composite polynomials of the form

$$(x^{q^n} - \delta_2 x + \delta_1)^n P(\frac{x^{q^n} - \delta_2 x + \delta_0}{x^{q^n} - \delta_2 x + \delta_1})$$

Now let's suppose in relation (1) $A \neq 1$ and consider $F(x)$ as follows:

$$F(x) = (x^{q^n} - \delta_2 x + \delta_1)^n P(\frac{x^{q^n} - \delta_2 x + \delta_0}{x^{q^n} - \delta_2 x + \delta_1}) = P(1)\prod_{u=0}^{n-1} h^{(u)}(x),$$

where $\delta_0,\ \delta_1, \delta_2 \in \mathbb{F}_{q^n},\ \delta_0 \neq \delta_1, \delta_2 \neq 0, 1$ and

$$h^{(u)}(x) = x^{q^n} - \delta_2 x - B^{q^u} \in \mathbb{F}_{q^n}[x], \quad B = \frac{\delta_1\alpha - \delta_0}{1 - \alpha}.$$

Let $t = ord(\delta_2)$, so in view of Proposition 2, we obtain

$$h(x) = x^{q^n} - \delta_2 x - \frac{\alpha\delta_1 - \delta_0}{1-\alpha} = (x-\lambda)\prod_{j=1}^{\frac{q^n-1}{t}} w_j(x),$$

where

$$\lambda = \frac{\alpha\delta_1 - \delta_0}{(1-\alpha)(1-\delta_2)} \in \mathbb{F}_{q^n}.$$

Also one can show that

$$h^{(u)}(x) = (x - \lambda^{q^u})\prod_{j=1}^{\frac{q^n-1}{t}} w_j^{(u)}(x).$$

Therefore

$$F(x) = P(1)\prod_{u=0}^{n-1} h^{(u)}(x) = P(1)m_\lambda(x)\prod_{j=1}^{\frac{q^n-1}{t}} s_j(x),$$

where $s_j(x)$ is an irreducible polynomial of degree nt over $\mathbb{F}_q$ and $m_\lambda(x)$ is minimal polynomial $\lambda \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$. It can be shown that

$$m_\lambda(x) = P_1^*\left(\frac{(1-\delta_2)x + \delta_1}{\delta_1 - \delta_0}\right),$$

where $P_1(x) = P(1-x)$. It follows the below theorem.

Theorem 5. *Let $\delta_0,\ \delta_1, \delta_2 \in \mathbb{F}_q,\ \delta_0 \neq \delta_1, \delta_2 \neq 0, 1$. Suppose $P(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_q$. Then the polynomial*

$$F(x) = (x^{q^n} - \delta_2 x + \delta_1)^n P(\frac{x^{q^n} - \delta_2 x + \delta_0}{x^{q^n} - \delta_2 x + \delta_1}),$$

decompose as a product of one irreducible polynomial of degree n and $\frac{q^n-1}{t}$ irreducible polynomials of degree nt over $\mathbb{F}_q$ where $t = ord(\delta_2)$.

References

[1] S.D. Cohen, On irreducible polynomials of certain types in finite fields, *Proc. Cambridge Philos. Soc.*, 66(1969), 335-344.

[2] S. Gao, Normal bases over finite fields, *Ph.D Thesis*, Waterloo, (1993).

[3] M.K. Kyuregyan and G.M. Kyuregyan, Irreducible compositions of polynomials over finite fields, http://www.arXiv:1008.1863.

[4] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, (1987).