Journal of Mathematical Extension
Vol. 6, No. 2, (2012), 65-73

On the Irreducibility of Some Composite Polynomials

M. Alizadeh
Islamic Azad University-Ahvaz Branch

Abstract. In this paper we study the irreducibility of some composite polynomials, constructed by a polynomial composition method over finite fields. Finally, a recurrent method for constructing families of irreducible polynomials of higher degree from given irreducible polynomials over finite fields is given.

AMS Subject Classification: 12A20
Keywords and Phrases: Composition polynomial, finite fields, irreducible polynomial

1. Introduction

The problem of irreducibility of polynomials over Galois fields is a case of spacial interest and plays an important role in modern engineering. One of the methods to construct irreducible polynomials is the polynomial composition method that allows constructions of irreducible polynomials of higher degree from given irreducible polynomials over finite fields.

Let $\mathbb{F}_q$ be the Galois field of order $q = p^s$, where p is a prime and s is a natural number. For a finite field $\mathbb{F}_q$ we denote by $\mathbb{F}_q^*$ the multiplicative group of nonzero elements of $\mathbb{F}_q$. Recall that the trace function of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is defined by

$$Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i},\ \alpha \in \mathbb{F}_{q^n},$$

Received: June 2011; Accepted: January 2012

where $\mathbb{F}_{q^n}$ is an extension field of the finite field $\mathbb{F}_q$. For convince we denote $Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ by $Tr_{q^n|q}$. Notice also the transitivity of the trace in the sense that

$$Tr_{\mathbb{F}_{q^n}|\mathbb{F}_p}(\alpha) = Tr_{\mathbb{F}_q|\mathbb{F}_p}(Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha)), \qquad \alpha \in \mathbb{F}_{q^n}. \tag{1}$$

Suppose that $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial over $\mathbb{F}_q$ of degree n. Its reciprocal polynomial is defined as

$$P^*(x) = x^n P(1/x).$$

Some authors have been studied the irreducibility of the polynomial

$$F(x) = (dx^p - rx + h)^n P(\frac{ax^p - bx + c}{dx^p - rx + h}), \tag{2}$$

for some particular cases. Varshamov studied one case from (2) and gave the following proposition:

Proposition 1.1. ([10, Theorem 3.13]) *Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial over $\mathbb{F}_q$ and p be the characteristic of $\mathbb{F}_q$. Then the polynomial $P(x^p - x - \delta_0)$ is an irreducible polynomial over $\mathbb{F}_q$ if and only if*

$$Tr_{q|p}(n\delta_0 - c_{n-1}) \neq 0.$$

Also, for this case, Kyuregyan gave a recurrent method for constructing irreducible polynomials in the following proposition:

Proposition 1.2. (Kyuregyan [8, Theorem 2]) *Let $F(x) = \sum_{u=0}^{n} c_u x^u$ be an irreducible polynomial over $\mathbb{F}_q$ and suppose that there exist an element $\delta_0 \in \mathbb{F}_p$ such that $F(\delta_0) = a$, with $a \in \mathbb{F}_p^*$ and*

$$Tr_{q|p}(n\delta_0 - c_{n-1}) Tr_{q|p}(F'(\delta_0)) \neq 0.$$

Let $g_0(x) = x^p - x + \delta_0$ and $g_k(x) = x^p - x + \delta_k$, where $\delta_k \in \mathbb{F}_p^*$, $k \geqslant 1$. Define $F_0(x) = F(g_0(x))$, and $F_k(x) = F_{k-1}^*(g_k(x))$ for $k \geqslant 1$, where $F_{k-1}^*(x)$ is the reciprocal polynomial of $F_{k-1}(x)$. Then for each $k \geqslant 0$, the polynomial $F_k(x)$ is an irreducible polynomial of degree $n_k = np^{k+1}$ over $\mathbb{F}_q$.

We note that the above proposition is the generalization of Varshamov's theorem, that the reader can find it in [10]. He also gave another recurrent method for constructing irreducible polynomials in the following proposition:

Proposition 1.3. (Kyuregyan [7], Corollary 2) *Let s be odd integer, δ be any element of $\mathbb{F}_{2^s}^*$, and the sequence of functions $\varphi_m(x)$ be defined by*

$$\varphi_m(x) = a_m(x) + \delta b_m(x)$$

under the initial condition

$$\varphi_0(x) = x + \delta.$$

Then the polynomial $\varphi_m(x)$ of degree $2m$ defined by the recurrent relation

$$\varphi_m(x) = x^{2^{m-1}} \varphi_{m-1}(x + \frac{\delta^2}{x})$$

is an irreducible polynomial over $\mathbb{F}_{2^s}$, where

$$a_1(x) = x^2 + \delta^2, \quad b_1(x) = x$$

and

$$a_m(x) = a_{m-1}^2(x) + b_{m-1}^2(x)$$

and also

$$b_m(x) = a_{m-1}(x) b_{m-1}(x).$$

The aim of this paper is to determine under what conditions

$$F(x) = x^{2n} P(\frac{x^2 - \delta_0 x + \delta_1}{x^2}), \qquad \delta_0, \delta_1 \in \mathbb{F}_{2^s}^*$$

is an irreducible polynomial over $\mathbb{F}_{2^s}$, where $P(x)$ is an irreducible polynomial of degree n over $\mathbb{F}_{2^s}$, and also giving a recurrent method for constructing families of irreducible polynomials $F_k(x)$, for $k \geqslant 0$ over finite fields, when $F_0(x) = P(x)$. Such polynomials are used to implement arithmetic in extension fields and are found in many applications, including coding theory [1] and [6], cryptography [2], [4] and [5], computer algebra system [3].

In [9] Melsik K. Kyuregyan and Gohar M. Kyuregyan presented a new method for constructing irreducible polynomials over finite fields. They proved the following results which will be used in the proof of our results.

Proposition 1.4. (M. K. Kyuregyan and G. M. Kyureghyan [9], Lemma 1) *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 $\mathbb{F}_q(h_0, h_1, ..., h_k) = \mathbb{F}_{q^d}$ and $f(x) = \prod_{v=0}^{d-1} h^{(v)}(x)$ on $\mathbb{F}_{q^d}[x]$, where*

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

2. Irreducibility of Composition Polynomials

In this section we examine the irreducibility of composite polynomial $x^{2n} P(\frac{x^2-\delta_0 x+\delta_1}{x^2})$ over $\mathbb{F}_{2^s}$. We prove some results that will be helpful to construct sequences of high degree irreducible polynomials over a finite fields. The following proposition will be helpful to derive our results.

Proposition 2.1. *([10], Corollary 3.6) For $a, b \in \mathbb{F}_q^*$ the trinomial $x^p - ax - b$ is irreducible over $\mathbb{F}_q$ if and only if $a = A^{p-1}$, for some $A \in \mathbb{F}_q$ and $Tr_{q|p}(\frac{b}{A^p}) \neq 0$.*

Theorem 2.2. *Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial over $\mathbb{F}_{2^s}$ of degree n. Then*

$$F(x) = x^{2n} P(\frac{x^2 - \delta_0 x + \delta_1}{x^2}), \qquad \delta_0, \delta_1 \in \mathbb{F}_{2^s}^*$$

is an irreducible polynomial of degree $2n$ over F_{2^s} if and only if

$$Tr_{2^s|2}(\frac{\delta_1}{\delta_0^2}(\frac{P^{*\prime}(0)}{P^*(0)} + n)) \neq 0.$$

Proof. Let $\alpha \in \mathbb{F}_{2^{sn}}$ be a root of $P(x)$. Irreducibility of $P(x)$ over $\mathbb{F}_{2^s}$ implies that it can represented over $\mathbb{F}_{2^{sn}}$ as

$$P(x) = c_n \prod_{u=0}^{n-1} (x - \alpha^{2^{su}}).$$

By substituting $\frac{x^2-\delta_0 x+\delta_1}{x^2}$ for x and multiplying its both sides by x^{2n}, we get

$$\begin{aligned} F(x) &= x^{2n} P(\frac{x^2 - \delta_0 x + \delta_1}{x^2}) \\ &= c_n x^{2n} \prod_{u=0}^{n-1} (\frac{x^2 - \delta_0 x + \delta_1}{x^2} - \alpha^{2^{su}}) \\ &= c_n \prod_{u=0}^{n-1} (1 - \alpha^{2^{su}})(x^2 - (\frac{\delta_0}{1-\alpha})^{2^{su}} x - (\frac{\delta_1}{\alpha - 1})^{2^{su}}) \\ &= c_n (1-\alpha)^{\frac{2^{sn}-1}{2^s-1}} \prod_{u=0}^{n-1} (x^2 - (\frac{\delta_0}{1-\alpha})^{2^{su}} x - (\frac{\delta_1}{\alpha-1})^{2^{su}}). \end{aligned}$$

Proposition 4 implies that $F(x)$ is an irreducible polynomial over $\mathbb{F}_{2^s}$ if and only if

$$x^2 - \frac{\delta_0}{\alpha - 1} x - \frac{\delta_1}{\alpha - 1}$$

is an irreducible polynomial over $\mathbb{F}_{2^{sn}}$. Then by Proposition 5, $F(x)$ is an irreducible polynomial over $\mathbb{F}_{2^s}$ if and only if

$$Tr_{2^{sn}|2}(\frac{\frac{\delta_1}{\alpha-1}}{(\frac{\delta_0}{1-\alpha})^2}) = Tr_{2^{sn}|2}(\frac{\delta_1}{\delta_0^2}(\alpha - 1)) \neq 0.$$

On the other side by (1),

$$Tr_{2^{sn}|2}(\frac{\delta_1}{\delta_0^2}(\alpha - 1)) = Tr_{2^s|2}(Tr_{2^{sn}|2^s}(\frac{\delta_1}{\delta_0^2}(\alpha - 1))). \tag{3}$$

Recall that for an irreducible polynomial $f(x) = \sum_{i=0}^{n} a_i x^i$ of degree n over $\mathbb{F}_q$, we have

$$Tr_{q^n|q}(\beta) = -\frac{a_{n-1}}{a_n},$$

where $\beta \in \mathbb{F}_{q^n}$ is a root of $f(x)$(see [6], page 51). So

$$\begin{aligned} Tr_{2^{sn}|2^s}(\frac{\delta_1}{\delta_0^2}(\alpha-1)) &= \frac{\delta_1}{\delta_0^2} Tr_{2^{sn}|2^s}(\alpha-1) \\ &= \frac{\delta_1}{\delta_0^2}(Tr_{2^{sn}|2^s}(\alpha) - Tr_{2^{sn}|2^s}(1)) \\ &= \frac{\delta_1}{\delta_0^2}(\frac{c_{n-1}}{c_n} + n). \end{aligned} \tag{4}$$

Hence (3) and (4) imply that

$$Tr_{2^{sn}|2}(\frac{\delta_1}{\delta_0^2}(\alpha-1)) = Tr_{2^s|2}(\frac{\delta_1}{\delta_0^2}(\frac{c_{n-1}}{c_n} + n)).$$

By the given condition $Tr_{2^s|2}(\frac{\delta_1}{\delta_0^2}(\frac{P^{*\prime}(0)}{P^*(0)} + n)) \neq 0$, $F(x)$ is an irreducible polynomial over $\mathbb{F}_{2^s}$. $\square$

Example 2.3. Consider the irreducible polynomial $P(x) = x^2 + x + (\alpha+1)$ over the Galois field $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$, where α is a root of the irreducible polynomial $x^2 + x + 1$ over $\mathbb{F}_2$. According to Theorem 2.

$$\begin{aligned} F(x) &= x^4 P(\frac{x^2 - (\alpha+1)x + \alpha}{x^2}) \\ &= (x^2 - (\alpha+1)x + \alpha)^2 + x^2(x^2 - (\alpha+1)x + \alpha) + (\alpha+1)x^4 \\ &= (\alpha+1)x^4 + (\alpha+1)x^3 + (\alpha+1) \end{aligned}$$

is an irreducible polynomial over $\mathbb{F}_4$.

Corollary 2.4. *Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial over $\mathbb{F}_2$ of degree n. Then*

$$F(x) = x^{2n} P(\frac{x^2 - x + 1}{x^2})$$

is an irreducible polynomial of degree $2n$ over $\mathbb{F}_2$ if and only if

$$\frac{c_{n-1}}{c_n} + n \neq 0.$$

3. Recurrent Method

In this section we shall describe a computationally simple and explicit recurrent method for constructing higher degree irreducible polynomials over finite field $\mathbb{F}_{2^s}$ starting from an irreducible polynomial.

Theorem 3.1. *Let $P(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_{2^s}$. Define*

$$F_0(x) = P(x),$$

$$F_k(x) = x^{n2^k} F_{k-1}(\frac{x^2+x+1}{x^2}) \qquad k \geqslant 1. \tag{5}$$

Suppose that

$$Tr_{2^s|2}(\frac{P'(1)}{P(1)}) \cdot Tr_{2^s|2}(\frac{P^{*\prime}(0)}{P^*(0)} + n) \neq 0.$$

Then $(F_k(x))_{k\geqslant 1}$ is a sequence of irreducible polynomials over $\mathbb{F}_{2^s}$ of degree $n2^k$.

Proof. We start our proof by setting $\delta_0, \delta_1 = 1$ in Theorem 2.2. According to Theorem 2.2. and hypothesis of theorem , $F_1(x)$ is an irreducible polynomial over $\mathbb{F}_{2^s}$ of degree $2n$. Also by Theorem 2.2. for every $k \geqslant 2$, $F_k(x)$ is an irreducible polynomial over $\mathbb{F}_{2^s}$ if and only if $Tr_{2^s|2}(\frac{F_{k-1}^{*\prime}(0)}{F_{k-1}^*(0)}) \neq 0$. On the other hand, from (5), we have

$$\begin{aligned} F_k^*(x) &= x^{n2^k} F_k(\frac{1}{x}) \\ &= x^{n2^k} ((\frac{1}{x})^{n2^k} F_{k-1}(\frac{(\frac{1}{x})^2 - (\frac{1}{x}) + 1}{(\frac{1}{x})^2}) \\ &= F_{k-1}(x^2 - x + 1), \end{aligned} \tag{6}$$

for every $k \geqslant 1$. So

$$F_k^*(0) = F_{k-1}(1), \tag{7}$$

and

$$F_k^{*\prime}(0) = F'_{k-1}(1), \tag{8}$$

for every $k \geqslant 1$. On the other side

$$F'_k(x) = x^{n2^k-2} F'_{k-1}(\frac{x^2-x+1}{x^2}). \tag{9}$$

So

$$F'_k(1) = F'_{k-1}(1), \tag{10}$$

for every $k \geqslant 1$. Using (8) and (9), we get

$$F_k^{*\prime}(0) = P'(1). \tag{11}$$

Obviously by (5)

$$F_k(1) = F_{k-1}(1), \tag{12}$$

for every $k \geqslant 1$. So (7) and (12) imply that $F_k^*(0) = P(1)$, for every $k \geqslant 1$. Thus by hypothesis of theorem $F_k(x)$ is an irreducible polynomial over $\mathbb{F}_{2^s}$, for every $k \geqslant 2$, and the proof is completed. □

Corollary 3.2. *Consider the irreducible polynomial $F_0(x) = x^2 + x + 1$ over the Galois field $\mathbb{F}_2$. According to Theorem 3., for each $k \geqslant 1$,*

$$F_k(x) = x^{2^{k+1}} F_{k-1}(\frac{x^2-x+1}{x^2}),$$

is a sequence of irreducible polynomials over $\mathbb{F}_2$ of degree 2^{k+1}.

References

[1] E. R. Berlekamp, *Algebraic coding theory*, Mc Graw-Hill, New York, 1968.

[2] I. F. Blake, G. Seroussi, and N. P. Smart, *Elliptic curves in cryptography*, Cambridge University Press, Cambridge, reprinted, 2000.

[3] J. Calment, Algebraic algorithms in GF(q), *Discrete Math.,* 56 (1985), 101-109.

[4] B. Chor and R. Rivest, *Aknapsack-type public key cryptosystem based on arithmetic in finite fields*, IEEE Trans. Inform. Theory, 34 (1988), 901-909.

[5] N. Koblitz, *Algebraic a spects of cryptography*, Springer, Berlin, 1998.

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

[7] M. K. Kyuregyan, Recurrent methods for constructing irreducible polynomials over $GF(2^s)$, *Finite Fields and Their Applications,* 8 (2002), 52-68.

[8] M. K. Kyuregyan, Iterated constructions of irreducible polynomials over finite fields with linearly independent roots, *Finite Fields and Their Applications,* 10 (2004), 323-341.

[9] M. K. Kyuregyan and G. M. Kyureghyan, *Irreducible compositions of polynomials over finite fields*, Designs Codes and Cryptography, DOI: 10.1007/s 10623-010-9476-7.

[10] A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian, *Applications of finite fields*, Kluwer Academic publishers, Boston, Dordrecht, Lancaster, 1993.

Mahmood Alizadeh
Department of Mathematics
Assistant Professor of Mathematics
Islamic Azad University-Ahvaz Branch
Ahvaz, Iran
E-mail: alizadeh@iauahvaz.ac.ir