TÜBİTAK

Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2013) 37: 874 – 883

doi:10.3906/mat-1201-53

Factorization of composite polynomials over finite fields

Saeid MEHRABI*
Farhangian University, Tehran, Iran

Received: 28.01.2012 • **Accepted:** 01.10.2012 • **Published Online:** 26.08.2013 • **Printed:** 23.09.2013

Abstract: This paper presents the reducibility of some composite polynomials and explicitly determines the factorization over finite fields. Also families of irreducible polynomials over finite fields are introduced.

Key words: 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 $\mathbb{F}_q^*$ be a multiplicative group of $\mathbb{F}_q$. The problem of irreducibility of polynomials and determining the reducibility of a given polynomial stems from both mathematical theory and applications. 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 the composition method. Probably the most powerful result in this area is the following theorem of Cohen.

Theorem 1.1 *(Cohen [1]) Let $f(x), g(x) \in \mathbb{F}_q[x]$, and $P(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree n. Then $F(x) = g(x)^n P\left(\frac{f(x)}{g(x)}\right)$ 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 and norm functions of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ are

$$Tr_{q^n|q}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i}, \; N_{q^n|q}(\alpha) = \prod_{i=0}^{n-1} \alpha^{q^i}, \quad \alpha \in \mathbb{F}_{q^n}.$$

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 $f^*(x) = x^n f(\frac{1}{x})$. For $\alpha \in \mathbb{F}_q$, the least positive integer t for which $\alpha^t = \alpha$ is called the order of α and denoted by $t = ord(\alpha)$. From [3] we know that $ord(\alpha)$ divides $q-1$. If $ord(f) = q-1$, then we say α is a primitive element in $\mathbb{F}_q$.

Recently, M. Kyuregyan and G. Kyuregyan [2] presented the following theorem for constructing irreducible polynomials, which is a powerful tool for constructions in the present paper.

*Correspondence: saeid_mehrabi@yahoo.com
2000 *AMS Mathematics Subject Classification:* 53A, 53C.

Theorem 1.2 *(M. Kyuregyan and G. Kyureguan [2]) 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 Cohen's Theorem. The following proposition will be used in the next section.

Proposition 1 (Lidl and Niederreiter [3] Theorem 2.26). Let K be a finite field. Let F be a finite extension of K and E a finite extension of F. Then

$$Tr_{E|K}(\alpha) = Tr_{F|K}\left(Tr_{E|F}(\alpha)\right), \quad \alpha \in E.$$

In this paper we always assume that $P(x)$ is monic. For this matter we 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 Cohen's Theorem fail. Furthermore, we obtain explicit families of irreducible polynomials of degree np over $\mathbb{F}_q$ from a given irreducible polynomial of degree n over $\mathbb{F}_q$.

2. Reducibility of composite polynomials of the form

$$(dx^q - rx + h)^n P\left(\frac{ax^q - bx + c}{dx^q - rx + h}\right)$$

Let $P(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_q$. Then $P(x)$ can be represented in $\mathbb{F}_{q^n}$ by

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

for $\alpha \in \mathbb{F}_{q^n}$, some root of $P(x)$. Suppose that $ax^q - bx + c$ and $dx^q - rx + h$ are relatively prime polynomials in $\mathbb{F}_q[x]$ with a or d being non-zero. Set

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

where

$$\begin{aligned} h^{(u)}(x) &= x^q - \left(\frac{b - \alpha r}{a - \alpha d}\right)^{q^u} x - \left(\frac{\alpha h - c}{a - \alpha d}\right)^{q^u} \\ &= (x^q - Ax - B)^{(u)} \in \mathbb{F}_{q^n}[x], \quad u = 0, ..., n-1, \end{aligned}$$

and

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

(Note that notation $h^{(0)}(x) = h(x)$ is used.)
If $ar = bd$, then

$$h^{(u)}(x) = \left(x^q - \frac{r}{d}x - \frac{\alpha h - c}{a-\alpha d}\right)^{(u)} = (x^q - Ax - B)^{(u)}, \tag{2.1}$$

where

$$A = \frac{r}{d} \in \mathbb{F}_q, \quad B = \frac{\alpha h - c}{a-\alpha d} \in \mathbb{F}_{q^n}.$$

For this problem we will consider two separate cases.

2.1. Reducibility of composite polynomials of the form

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

In this subsection we assume in (2.1) that $A = \frac{r}{d} = 1$, and consider $F(x)$ as follows:

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

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

$$h^{(u)}(x) = x^q - x - B^{q^u}, \quad B = \frac{\delta_1\alpha - \delta_0}{1-\alpha}.$$

Let γ be a root of $h(x)$, namely $h(\gamma) = 0$ or $\gamma^q = \gamma + B$. Then we obtain

$$\gamma^{q^n} = \gamma + Tr_{q^n|q}(B). \tag{2.2}$$

In view of (2.2), suppose that $Tr_{q^n|q}(B) = 0$. Then γ as a root of $h(x)$ is in $\mathbb{F}_{q^n}$ and further the roots of $h(x)$ are $\lambda_k = \gamma + \theta_k$, where $\theta_k \in \mathbb{F}_q$, $k = 1, \ldots, q$, i.e. $h(x)$ splits in $\mathbb{F}_{q^n}$. It follows that

$$h(x) = \prod_{k=1}^{q}(x - \lambda_k).$$

One can show that $\lambda_k^{q^u}$ $(k = 1, 2, \ldots, q)$ are the roots of $h^{(u)}(x)$. Therefore

$$h^{(u)}(x) = \prod_{k=1}^{q}(x - \lambda_k^{q^u}), \ \textit{for every } u = 0, 1, \ldots, n-1.$$

Hence we obtain

$$F(x) = P(1)\prod_{u=0}^{n-1} h^{(u)}(x) = P(1)\prod_{u=0}^{n-1}\left(\prod_{k=1}^{q}(x - \lambda_k^{q^u})\right)$$

$$= P(1)\prod_{k=1}^{q}\left(\prod_{u=0}^{n-1}(x - \lambda_k^{q^u})\right) = P(1)\prod_{k=1}^{q} m_{\lambda_k}(x),$$

where $m_{\lambda_k}(x)$ is the minimal polynomial of $\lambda_k \in \mathbb{F}_{q^n}$ of degree n over $\mathbb{F}_q$. So we obtain the following theorem.

Theorem 2.1 *Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial of degree n over $\mathbb{F}_q$ and $\delta_0, \delta_1 \in \mathbb{F}_q, \delta_0 \neq \delta_1$. Suppose that $n\delta_1 + (\delta_0 - \delta_1)\frac{P'(1)}{P(1)} = 0$. Then*

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

is decomposed as a product of q irreducible polynomial of degree n over $\mathbb{F}_q$.

Proof We only need to compute $Tr_{q^n|q}(B)$, where $B = \frac{\delta_1\alpha - \delta_0}{1-\alpha}$. For this purpose we have

$$B = \frac{\delta_1\alpha - \delta_0}{1-\alpha} = -\delta_1 + \frac{\delta_1 - \delta_0}{1-\alpha}.$$

Hence

$$Tr_{q^n|q}(B) = -n\delta_1 + (\delta_1 - \delta_0)Tr_{q^n|q}(\frac{1}{1-\alpha}).$$

If we set $P_1(x) = P(1-x) = \sum_{i=0}^{n} d_i x^i$, then $\frac{1}{1-\alpha}$ is some root of $P_1^*(x)$ and so

$$Tr_{q^n|q}(\frac{1}{1-\alpha}) = -\frac{d_1}{d_0} = \frac{P'(1)}{P(1)}.$$

This completes the proof. □

Now assume in (2.2) that $Tr_{q^n|q}(B) \neq 0$. Then, γ as a root of $h(x)$ is not in $\mathbb{F}_{q^n}$ and thus

$$\gamma^{q^{np}} = \gamma + pTr_{q^n|q}(B) = \gamma.$$

Then $\gamma \in \mathbb{F}_{q^{np}}$ and therefore conjugates of γ over $\mathbb{F}_{q^n}$ are $\gamma, \gamma^{q^n}, \ldots, \gamma^{q^{(p-1)n}}$. If we set $Tr_{q^n|q}(B) = b \in \mathbb{F}_q^*$, then we have

$$\gamma^{q^{in}} = \gamma + ib, \quad i = 0, 1, \ldots, p-1.$$

Therefore the minimal polynomial of $\gamma \in \mathbb{F}_{q^{np}}$ over $\mathbb{F}_{q^n}$ of degree p is as follows:

$$m_\gamma(x) = \prod_{i=0}^{p-1}(x - (\gamma + ib)) = b^p \prod_{i=0}^{p-1}\left(\frac{x-\gamma}{b} - i\right)$$
$$= b^p\left(\left(\frac{x-\gamma}{b}\right)^p - \left(\frac{x-\gamma}{b}\right)\right) = x^p - b^{p-1}x + \gamma b^{p-1} - \gamma^p \in \mathbb{F}_{q^n}[x].$$

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

$$x^p - b^{p-1}x - \beta, \quad \beta \in \mathbb{F}_{q^n}. \tag{2.3}$$

Now let θ be a root of (2.3) in some extension field of $\mathbb{F}_{q^n}$. Then we obtain

$$\left(\frac{\theta}{b^p}\right)^{p^i} - \left(\frac{\theta}{b}\right)^{p^{i-1}} = \left(\frac{\beta}{b^p}\right)^{p^{i-1}}, \quad i = 1, \ldots, s \ (q = p^s). \tag{2.4}$$

Summing (2.4) yields

$$\theta^q - \theta = b\left(\frac{\beta}{b^p} + \left(\frac{\beta}{b^p}\right)^p + \ldots + \left(\frac{\beta}{b^p}\right)^{\frac{q}{p}}\right).$$

On the other hand, we have $h(\theta) = 0$, or $\theta^q - \theta = B$. Thus

$$\frac{\beta}{b^p} + \left(\frac{\beta}{b^p}\right)^p + \ldots + \left(\frac{\beta}{b^p}\right)^{\frac{q}{p}} = Bb^{-1}$$

By Theorem 3.50 in [3], equation $X + X^p + \ldots + X^{\frac{q}{p}} = Bb^{-1}$ has $\frac{q}{p}$ distinct roots. So we have

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

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

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

Then

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

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

Since for every constant i, $s_i^{(u)}(x)$, $u = 0, 1, \ldots, n-1$ are irreducible polynomials of degree p over $\mathbb{F}_{q^n}$ and β_i is a proper element in $\mathbb{F}_{q^n}$, then by Theorem (1.2) $k_i(x)$ is an irreducible polynomial of degree np over $\mathbb{F}_q$. Then we obtain the following theorem.

Theorem 2.2 *Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial of degree n over $\mathbb{F}_q$ and $\delta_0, \delta_1 \in \mathbb{F}_q, \delta_0 \neq \delta_1$. Suppose that $n\delta_1 + (\delta_0 - \delta_1)\frac{P'(1)}{P(1)} \neq 0$. Then*

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

is decomposed as a product of $\frac{q}{p}$ irreducible polynomial of degree np over $\mathbb{F}_q$.

In a special case if we set

$$F(x) = (x^p - x + \delta_1)^n P\left(\frac{x^p - x + \delta_0}{x^p - x + \delta_1}\right),$$

where $P(x)$ is an irreducible polynomial of degree n over $\mathbb{F}_q$ then we obtain

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

Let γ be some root of $h(x)$. Then

$$\gamma^p = \gamma + B \to \gamma^{p^{ns}} = \gamma^{q^n} = \gamma + Tr_{q^n|p}(B). \tag{2.5}$$

If we assume in (2.5) that $Tr_{q^n|p}(B) = 0$, then $\gamma \in \mathbb{F}_{q^n}$ and in this case $\lambda_k = \gamma + k \in \mathbb{F}_{q^n}$, $k = 0, 1, \ldots, p-1$ are the roots of $h(x)$. Hence,

$$h(x) = \prod_{k=0}^{p-1}(x - \lambda_k),$$

and

$$h^{(u)}(x) = \prod_{k=0}^{p-1}(x - \lambda_k^{q^u}).$$

Finally we derive

$$\begin{aligned} F(x) = P(1)\prod_{u=0}^{n-1} h^{(u)}(x) &= P(1)\prod_{u=0}^{n-1}\left(\prod_{k=0}^{p-1}(x - \lambda_k^{q^u})\right) \\ &= P(1)\prod_{k=0}^{p-1}\left(\prod_{u=0}^{n-1}(x - \lambda_k^{q^u})\right) = P(1)\prod_{k=0}^{p-1} m_{\lambda_k}(x), \end{aligned}$$

where $m_{\lambda_k}(x)$ is the minimal polynomial of $\lambda_k \in \mathbb{F}_{q^n}$ of degree n over $\mathbb{F}_q$. This implies the following corollary.

Corollary 1 Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial of degree n over $\mathbb{F}_q$ and $\delta_0, \delta_1 \in \mathbb{F}_q, \delta_0 \neq \delta_1$. Suppose that $Tr_{q|p}\left(n\delta_1 + (\delta_0 - \delta_1)\frac{P'(1)}{P(1)}\right) = 0$. Then

$$F(x) = (x^p - x + \delta_1)^n P\left(\frac{x^p - x + \delta_0}{x^p - x + \delta_1}\right),$$

is decomposed as a product of p irreducible polynomials of degree n over $\mathbb{F}_q$.

Proof By the above discussions it is sufficient to compute $Tr_{q^n|p}(B)$, where

$$B = \frac{\delta_1\alpha - \delta_0}{1 - \alpha} = -\delta_1 + \frac{\delta_1 - \delta_0}{1 - \alpha}.$$

But by Proposition 1, we have

$$Tr_{q^n|p}(B) = Tr_{q|p}\left(Tr_{q^n|q}(B)\right) = Tr_{q|p}\left(-n\delta_1 + (\delta_1 - \delta_0)\frac{P'(1)}{P(1)}\right).$$

Thus, the proof is complete. □

Now if in (2.5), $Tr_{q^n|p}(B) \neq 0$, then $h(x) = x^p - x - B \in \mathbb{F}_{q^n}[x]$ is irreducible over $\mathbb{F}_{q^n}$ [3]. Moreover $h^{(u)}(x) = x^p - x - B^{q^u} \in \mathbb{F}_{q^n}[x]$ is irreducible. Hence by Theorem (1.2), $F(x) = P(1)\prod_{u=0}^{n-1} h^{(u)}(x)$ is an irreducible polynomial of degree np over $\mathbb{F}_q$. This yields the following corollary.

Corollary 2 Let $P(x)=\sum_{i=0}^{n}c_ix^i$ be an irreducible polynomial of degree n over $\mathbb{F}_q$ and $\delta_0,\delta_1\in\mathbb{F}_q,\delta_0\neq\delta_1$. Suppose that $Tr_{q|p}\left(n\delta_1+(\delta_0-\delta_1)\frac{P'(1)}{P(1)}\right)\neq 0$. Then

$$F(x)=(x^p-x+\delta_1)^nP\left(\frac{x^p-x+\delta_0}{x^p-x+\delta_1}\right)$$

is an irreducible polynomial of degree np over $\mathbb{F}_q$.

2.2. Reducibility of composite polynomials of the form

$$(x^q-\delta_2x+\delta_1)^nP\left(\frac{x^q-\delta_2x+\delta_0}{x^q-\delta_2x+\delta_1}\right).$$

In this subsection we suppose that in (2.1) $A=\frac{r}{d}\neq 1$ and consider $F(x)$ as follows:

$$F(x)=(x^q-\delta_2x+\delta_1)^nP\left(\frac{x^q-\delta_2x+\delta_0}{x^q-\delta_2x+\delta_1}\right)=P(1)\prod_{u=0}^{n-1}h^{(u)}(x),$$

where $\delta_0,\delta_1,\delta_2\ \in\mathbb{F}_q,\delta_0\neq\delta_1,\delta_2\neq 0,1$ and

$$h^{(u)}(x)=x^q-\delta_2x-B^{q^u},\quad B=\frac{\delta_1\alpha-\delta_0}{1-\alpha}\in\mathbb{F}_{q^n}.$$

Let $ord(\delta_2)=t$ and also $gcd(n,q-1)=1$. Set

$$h(x)=x^q-\delta_2x-B\in\mathbb{F}_{q^n}[x],\quad g(x)=x^q-\delta_2x\in\mathbb{F}_q[x],$$

and claim that $h(x)$ has exactly one root in $\mathbb{F}_{q^n}$ and other roots of $h(x)$ are in $\mathbb{F}_{q^{nt}}$.

Since $gcd(h(x),h'(x))=1$, then $h(x)$ has no multiple roots. Let $\alpha_1,\alpha_2,...,\alpha_q$ be its roots in an extension of $\mathbb{F}_{q^n}$. It is clear that for each $1\leq i\leq q$, $\gamma_i=\alpha_i^{q^n}-\alpha_i$ is a root of $g(x)=x^q-\delta_2x$ or $\gamma_i^q=\delta_2\gamma_i$. But

$$\gamma_i^q=\delta_2\gamma_i,\quad \gamma_i^{q^2}=\delta_2^2\gamma_i,\ldots,\quad \gamma_i^{q^t}=\gamma_i,$$

implies that roots of $g(x)$ are of degree t over $\mathbb{F}_q$. Now we show that $\gamma_1,\gamma_2,...,\gamma_q$ are pair-wise distinct. On the contrary, suppose that we have $1\leq i\neq j\leq q$ so that $\gamma_i=\gamma_j$, namely $\alpha_i^{q^n}-\alpha_i=\alpha_j^{q^n}-\alpha_j$ and then $\alpha_i-\alpha_j\in\mathbb{F}_{q^n}$. Moreover, α_i and α_j are roots of $h(x)$ and so $\alpha_i-\alpha_j$ is a root of $g(x)$; it follows that $\alpha_i-\alpha_j\in\mathbb{F}_{q^t}$. But $gcd(n,t)=1$ so we get $\alpha_i-\alpha_j\in\mathbb{F}_q$, which yields $\delta_2=1$, and this result is not true. So the roots of $g(x)$ are pair-wise distinct. In view of the fact that zero is one root of $g(x)$, there is an index i such that $\gamma_i=\alpha_i^{q^n}-\alpha_i=0$. Therefore α_i as a root of $h(x)$ is in $\mathbb{F}_{q^n}$ and denote this root α_i by λ. On the other hand,

$$\lambda+\gamma_j,\quad j=1,2,\ldots,q,$$

are roots of $h(x)$, so that $\lambda\in\mathbb{F}_{q^n}$, $\gamma_j\in\mathbb{F}_{q^t}$ and $gcd(n,t)=1$. It implies $\lambda+\gamma_j\in\mathbb{F}_{q^{nt}}$ and thus $w_j(x)$ as the minimal polynomial of $\lambda+\gamma_j$ over $\mathbb{F}_{q^n}$ is of degree t. Then we can write

$$h(x)=(x-\lambda)\prod_{j=1}^{\frac{q-1}{t}}w_j(x),\quad w_j(x)\in\mathbb{F}_{q^n}[x].$$

One can show that for every $u = 1, 2, \ldots, n-1$,

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

Therefore

$$F(x) = P(1) \prod_{u=0}^{n-1} h^{(u)}(x) = P(1) \prod_{u=0}^{n-1} \left((x - \lambda^{q^u}) \prod_{j=1}^{\frac{q-1}{t}} w_j^{(u)}(x) \right)$$

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

where $s_j(x)$ is an irreducible polynomial of degree nt over $\mathbb{F}_q$ and $m_\lambda(x)$ is the minimal polynomial of $\lambda \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$. This proves the validity of the following theorem.

Theorem 2.3 *Let $\delta_0,\ \delta_1, \delta_2 \in \mathbb{F}_q,\ \delta_0 \neq \delta_1, \delta_2 \neq 0, 1$. Suppose that $P(x)$ is an irreducible polynomial of degree n over $\mathbb{F}_q$ and $gcd(n, q-1) = 1$. Then the composite polynomial*

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

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

In a special case we set

$$F(x) = (x^p - \delta_2 x + \delta_1)^n P\left(\frac{x^p - \delta_2 x + \delta_0}{x^p - \delta_2 x + \delta_1} \right) = P(1) \prod_{u=0}^{n-1} h^{(u)}(x), \tag{2.6}$$

where

$$h(x) = x^p - \delta_2 x - B \in \mathbb{F}_{q^n}[x], \quad B = \frac{\delta_1 \alpha - \delta_0}{1 - \alpha} \in \mathbb{F}_{q^n}. \tag{2.7}$$

By Corollary (3.6) of [4], $h(x)$ is an irreducible polynomial over $\mathbb{F}_{q^n}$ if and only if $\delta_2 = A^{p-1}$ for some $A \in \mathbb{F}_{q^n}$ and $Tr_{q^n|p}\left(\frac{B}{A^p}\right) \neq 0$. If in Corollary (3.6) of [4], we add the extra condition $Nq|p(\delta_2) = 1$ or equivalently $\delta_2^{\frac{q-1}{p-1}} = 1$, then we can obtain $\delta_2 = A^{p-1}$ for some $A \in \mathbb{F}_q$. Now by this additional assumption and Proposition 1, we get

$$Tr_{q^n|p}\left(\frac{B}{A^p}\right) = Tr_{q|p}\left(Tr_{q^n|q}\left(\frac{B}{A^p}\right)\right) = Tr_{q|p}\left(\frac{1}{A^p} Tr_{q^n|q}(B)\right) = Tr_{q|p}\left(\frac{z}{A^p}\right),$$

where

$$z = Tr_{q^n|q}(B) = -n\delta_1 + (\delta_1 - \delta_0)\frac{P'(1)}{P(1)}.$$

By definition of the trace function we have

$$Tr_{q|p}\left(\frac{z}{A^p}\right) = \frac{z}{A^p} + \frac{z^p}{A^{p^2}} + \ldots + \frac{z^{p^{s-1}}}{A^{p^{p^s}}}$$
$$= \frac{1}{A}\left(\frac{z}{\delta_2} + \frac{z^p}{\delta_2^{1+p}} + \ldots + \frac{z^{p^{s-1}}}{\delta_2^{1+p+\ldots+p^{s-1}}}\right).$$

We formulate this result as follows.

Corollary 3 Let $P(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_q$, $\delta_0, \delta_1, \delta_2 \in \mathbb{F}_q, \delta_0 \neq \delta_1, \delta_2 \neq 0, 1$ and $Nq|p(\delta_2) = 1$. Then the polynomial

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

of degree np is irreducible over $\mathbb{F}_q$ if and only if the following relation holds

$$\sum_{u=0}^{s-1} z^{p^u} \delta_2^{\frac{p^{u+1}-1}{1-p}} \neq 0, \tag{2.8}$$

where $z = -n\delta_1 + (\delta_1 - \delta_0)\frac{P'(1)}{P(1)}$. Otherwise $F(x)$ factors as the product of p irreducible polynomials of degree n.

Proof By hypothesis of Corollary 3, $h^{(u)}(x)$, $u = 0, 1, \ldots, n-1$ are irreducible polynomials of degree p over $\mathbb{F}_{q^n}$ and $B = \frac{\delta_1\alpha - \delta_0}{1-\alpha}$ is a proper element in $\mathbb{F}_{q^n}$. So by Theorem (1.2), $F(x)$ is an irreducible polynomial of degree np over $\mathbb{F}_q$.

Now suppose that (2.8) failed. So by [3], $h(x)$ in (2.7) splits in $\mathbb{F}_{q^n}$ as follows:

$$h(x) = \prod_{i=1}^{p}(x - \lambda_i),$$

where $\lambda_i \in \mathbb{F}_{q^n}$. It can be shown that

$$h^{(u)}(x) = \prod_{i=1}^{p}(x - \lambda_i^{q^u}).$$

So by (2.6) and the above relation we obtain

$$F(x) = P(1)\prod_{u=0}^{n-1} h^{(u)}(x) = P(1)\prod_{u=0}^{n-1}\left(\prod_{i=1}^{p}(x - \lambda_i^{q^u})\right)$$
$$= P(1)\prod_{i=1}^{p}\left(\prod_{u=o}^{n-1}(x - \lambda_i^{q^u})\right) = P(1)\prod_{i=1}^{p} m_{\lambda_i}(x),$$

where $m_{\lambda_i}(x)$ is the minimal polynomial of $\lambda_i \in \mathbb{F}_{q^n}$ over F_q of degree n. Thus the proof is complete. □

Acknowledgments

I would like to thank the anonymous referee for carefully reading my manuscript and for his very detailed comments. His many helpful suggestions and corrections allowed me to improve the presentation of the paper and improve its readability.

References

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

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

[3] Lidl, R., Niederreiter, H.: Finite Fields. Cambridge University Press, 1987.

[4] Menezes, A., Blake, I. F., Gao, X., Mullin, R. C., Vanstone, S. A., Yaghoobian, T.: Applications of Finite Fields, Kluwer Academic Publishers, Boston-Dordrecht-Lancaster, 1993.