Applications and Applied Mathematics: An International Journal (AAM)

Volume 19
Issue 3 *Special Issue No. 12 (March 2024)*

Article 10

3-2024

Construction of Normal Polynomials using Composition of Polynomials over Finite Fields of Odd Characteristic

Shalini Gupta
Himachal Pradesh University

Manpreet Singh
Himachal Pradesh University

Rozy Sharma
Himachal Pradesh University

Available at
http://pvamu.edu/aam
Appl. Appl. Math.
ISSN: 1932-9466

Applications and Applied Mathematics:
An International Journal
(AAM)

Special Issue No. 12 (March 2024), Article 10, 11 pages

Construction of Normal Polynomials using Composition of Polynomials over Finite Fields of odd Characteristic

[1*]Shalini Gupta, [2]Manpreet Singh and [3]Rozy Sharma

[1,2,3]Department of Mathematics and Statistics
Himachal Pradesh University
Shimla, Himachal Pradesh, India
[1]shalini.garga1970@gmail.com; [2]ms44167@gmail.com; [3]sharmarozy0115@gmail.com

*Corresponding author

Received: May 1, 2023; Accepted: June 23, 2023

Abstract

A monic irreducible polynomial is known as a normal polynomial if its roots are linearly independent over Galois field. Normal polynomials over finite fields and their significance have been studied quite well. Normal polynomials have applications in different fields such as computer science, number theory, finite geometry, cryptography and coding theory. Several authors have given different algorithms for the construction of normal polynomials. In the present paper, we discuss the construction of the normal polynomials over finite fields of prime characteristic by using the method of composition of polynomials.

Keywords: Trace; Prime characteristic; Galois field; Irreducible polynomial; Linearized polynomial; Normal polynomial; Normal basis

MSC 2020 No.: 12E05, 12E10, 12E20

1. Introduction

The normal polynomials have vast applications in computer science, number theory, algebraic geometry, finite geometry, cryptography and coding theory. Construction of irreducible polynomials and normal polynomials have always been a focused area of research in recent times (see Alizadeh (2011), Alizadeh (2012), Alizadeh and Mehrabi (2016), Hou (2022), Menezes et al. (1993), Meyn (1995) and Schwartz (1988)). Recursive constructions of normal polynomials over the finite fields were discussed by Kyuregyan (2008) and Sharma et al. (2022). In 2002, Kyuregyan provided recurrent methods for the construction of irreducible polynomials over finite field of even characteristic. Kyuregyan (2004) proposed the iterated constructions of irreducible polynomials over finite fields of even characteristic. Sharma and Ashima (2022) constructed irreducible polynomials over finite field by using the method of composition of polynomials. Hou (2022) provided certain sufficient conditions for an irreducible polynomial over finite field to be normal. Meyn (1995) constructed explicit N-polynomials of 2-power degree over finite fields.

A monic irreducible polynomial of degree n is called k-normal polynomial over finite field if its roots are k-normal elements which are defined and characterized by Huczynska et al. (2013). Further, the k-normal elements and the construction of k-normal polynomials were studied by Alizadeh and Mehrabi (2016), Alizadeh et al. (2018) and Kim and Son (2020). Normal elements and normal bases are discussed in detail by Chapman (1997), Gao (1993), Lidl and Niederreiter (1994) and Menezes et al. (1993). Iterated constructions of normal bases over finite fields are considered by Scheerhorn (1994). The existence of trace orthogonal normal bases is discussed by Jungnickel (1993).

In the present paper, we construct the normal polynomials over finite fields using the composition of polynomials over finite fields of characteristic p which is the extension of work done by Alizadeh et al. (2011). The work done in the paper is divided into four sections. The subsequent section offers the necessary references to comprehend the paper's preliminaries and essential results for driving its main findings. In Section 3, construction of N-polynomials over finite fields of prime characteristic p is presented which is illustrated over the finite fields of characteristics 5 and 7, respectively. Section 4 concludes the work done in this paper.

2. Preliminaries

In this section, we first examine the concepts of irreduciblilty and normality of polynomials over finite fields. Several researchers have contributed valuable insights, definitions and various results for analyzing the behaviour of polynomials over finite fields, which led to the advancements in theoretical and practical domains. The trace function $Tr_{q^n|q}(\alpha)$ of α over $\mathbb{F}_q$ where $\alpha \in \mathbb{F}_q$ is defined in Lidl and Niederreiter (Definition 2.22). Also, the reciprocal polynomial $f^*(x)$ of $f(x)$ is defined in Lidl and Niederreiter (Definition 3.12), where $f(x)$ is a polynomial of degree n in $\mathbb{F}_q[x]$. Cohen in 1969 (Lemma 1) derived the condition for the irreducibility of composition of relatively prime polynomials $f(x), g(x) \in \mathbb{F}_q(x)$ and an irreducible polynomial $p(x) \in \mathbb{F}_q[x]$ of degree n. Linearized polynomials play a great role in checking the normality of polynomials over finite fields. These polynomials are defined in Lidl and Niederreiter (Definition 3.49). Schwartz (1988) provided condition for $\alpha \in F$ to be a generator of a normal basis of $\mathbb{F}_q(\alpha)$ over $\mathbb{F}_q$. Alizadeh (2011) (Theorem 1) presented new type of irreducible polynomial from composition of irreducible polynomial by giving condition on trace function. The construction of self reciprocal normal polynomial from normal polynomial is provided by Alizadeh and Mehrabi (2015).

3. Main Results

Alizadeh et al. (2011) constructed normal polynomial over finite field with characteristic 3. So, we generalize this result over finite field with odd prime characteristic p. To prove this result, we have used two results regarding irreducible polynomials using the method of composition of polynomials given by (Alizadeh (2011), Theorem 1) and the condition for the reciprocal of the composite polynomial to be a normal polynomial given by Menezes et al. (1993) (Theorem 4.18). In this section, we construct normal polynomials over finite fields of odd prime characteristic p using the method of composition of polynomials. The main result is presented in the form of following Theorem.

Theorem 3.1.

Let $I(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial of degree n, where

$$n = n_1 p^e = n_1 t \text{ and } \gcd(n_1, p) = 1,$$

over $\mathbb{F}_{p^s}$ and $I^*(x)$ be an N-polynomial over $\mathbb{F}_{p^s}$. Also, let

$$F(x) = (x^p - x + 1)^n I\left(\frac{x^p - x}{x^p - x + 1}\right).$$

Then, $F^*(x)$ is an N-polynomial of degree pn over $\mathbb{F}_{p^s}$ if and only if

$$\left(n + \frac{c_1}{c_0}\right) . Tr_{q|p}\left(\frac{I'(1)}{I(1)} - n\right) \neq 0.$$

Proof:

Consider an irreducible polynomial $I(x) = \sum_{i=0}^{n} c_i x^i$ of degree n over $\mathbb{F}_{p^s}$ and its reciprocal polynomial $I^*(x)$ is a normal polynomial over $\mathbb{F}_{p^s}$. Construct a composite polynomial

$$F(x) = (x^p - x + 1)^n\, I\left(\frac{x^p - x}{x^p - x + 1}\right), \tag{1}$$

which is irreducible over $\mathbb{F}_p$ by Alizadeh (2011) (Theorem 1). Also, from Lidl and Niederreiter (1983) (Corollary 3.79), we have

$$x^{pn} - 1 = [\varphi_1(x) \ldots \varphi_i(x)]^{pt}.$$

Here, $x^{pn} - 1$ factors in distinct irreducible factors $\varphi_r(x) \in \mathbb{F}_{p^s}[x]$.

Set

$$G_r(x) = \frac{x^{pn} - 1}{\varphi_r(x)} = \frac{(x^n - 1)(x^{(p-1)n} + x^{(p-2)n} + \ldots + x + 1)}{\varphi_r(x)}$$

$$= \sum_{m=0}^{v_r} t_{rm} x^m (x^{(p-1)n} + x^{(p-2)n} + \ldots + x^n + 1)$$

$$= \sum_{m=0}^{v_r} t_{rm} \left(x^{(p-1)n+m} + x^{(p-2)n+m} + ... + x^{n+m} + x^m \right). \tag{2}$$

Here,

$$\frac{x^n - 1}{\varphi_r(x)} = \sum_{m=0}^{v_r} t_{rm} x^m.$$

Let ρ_1 be a root of $F(x)$. Then, $\sigma_1 = \frac{1}{\rho_1}$ is a root of $F^*(x)$.

As discussed in Menezes et al. (1993) (Theorem 4.18), $F^*(x)$ is an N-polynomial if and only if

$$L_{G_r}(\sigma_1) \neq 0,$$

$$L_{G_r}(\sigma_1) = \sum_{m=0}^{v_r} t_{rm} \left[(\sigma_1)^{(p^s)^{(p-1)n+m}} + (\sigma_1)^{(p^s)^{(p-2)n+m}} + \cdots + (\sigma_1)^{(p^s)^{n+m}} + \ (\sigma_1)^{(p^s)^m} \right],$$

which gives

$$L_{G_r}(\sigma_1) = \sum_{m=0}^{v_r} t_{rm} \left[\left(\frac{1}{\rho_1}\right)^{p^{(p-1)sn}} + \left(\frac{1}{\rho_1}\right)^{p^{(p-2)sn}} + ... + \left(\frac{1}{\rho_1}\right)^{p^{sn}} + \left(\frac{1}{\rho_1}\right) \right]^{p^{sm}}. \tag{3}$$

From (1), we see that $\dfrac{\rho_1^p - \rho_1}{\rho_1^p - \rho_1 + 1}$ is a root of $I(x)$.

Let ρ be the root of $I(x)$, so

$$\rho = \frac{\rho_1^p - \rho_1}{\rho_1^p - \rho_1 + 1},$$

$$\rho - 1 = -\left[\rho_1^p - \rho_1 + 1\right]^{-1}, \tag{4}$$

$$\rho - 1 = \frac{-1}{\rho_1^p - \rho_1 + 1},$$

$$\rho_1^p - \rho_1 = \frac{-1}{\rho - 1} - 1 = \frac{-\rho}{\rho - 1},$$

$$\rho_1^p - \rho_1 = \frac{\rho}{1 - \rho}. \tag{5}$$

Powering p^{sn} on the both sides of (4), we obtain

$$(\rho - 1)^{p^{sn}} = -\left[\rho_1^p - \rho_1 + 1\right]^{-p^{sn}}.$$

Using $(a+b)^{p^n} = a^{p^n} + b^{p^n}$, we have

$$(\rho - 1) = -\left[\rho_1^{p^{sn+1}} - \rho_1^{p^{sn}} + 1\right]^{-1}. \tag{6}$$

Then, from (4) and (6), we obtain

$$\left[\rho_1^{p^{sn+1}} - \rho_1^{p^{sn}} + 1\right]^{-1} = \left[\rho_1^p - \rho_1 + 1\right]^{-1}.$$

We know that $(\rho_1^p - \rho_1 + 1)$ cannot be zero, otherwise our root of $I(x)$ will be undefined,

$$\rho_1^{p^{sn+1}} - \rho_1^{p^{sn}} + 1 = \rho_1^p - \rho_1 + 1,$$

$$\rho_1^{p^{sn+1}} - \rho_1^{p^{sn}} = \rho_1^p - \rho_1,$$

$$\left[\rho_1^{p^{sn}} - \rho_1\right]^p = \left[\rho_1^{p^{sn}} - \rho_1\right].$$

Let $\rho_1^{p^{sn}} - \rho_1 = \theta \in \mathbb{F}_p$ and by using induction, we have

$$\rho_1^{p^{ksn}} = \rho_1 + k\theta, \tag{7}$$

where, $k = 0, 1, ...v_r$.

So, from (3) and (7), we get

$$L_{G_r}(\sigma_1) = \sum_{m=0}^{v_r} t_{rm} \left[\left(\frac{1}{\rho_1 + (p-1)\theta}\right) + \left(\frac{1}{\rho_1 + (p-2)\theta}\right) + \cdots + \left(\frac{1}{\rho_1 + \theta}\right) + \left(\frac{1}{\rho_1}\right)\right]^{p^{sm}},$$

which gives

$$L_{G_r}(\sigma_1) = \sum_{m=0}^{v_r} t_{rm} \left(\frac{-1}{\rho_1^p - \rho_1}\right)^{p^{sm}}.$$

Then, by (5), we have

$$L_{G_r}(\sigma_1) = \sum_{m=0}^{v_r} t_{rm} \left[\frac{\rho - 1}{\rho}\right]^{p^{sm}} = \sum_{m=0}^{v_r} \left[1 - \frac{1}{\rho}\right]^{p^{sm}}.$$

Let $H(x) = I^*(x)$ be an N-polynomial. From the theorem's hypothesis and Menezes et al. (1993) (Theorem 4.18), $H(1-x)$ is an N-polynomial. But $\left(1 - \frac{1}{\rho}\right)$ is a root of $H(1-x)$. So, we get

$$\sum_{m=0}^{v_r} \left[1 - \frac{1}{\rho}\right]^{p^{sm}} \neq 0,$$

which concludes the proof. ■

Example 3.1.

Let $I(x) = x^5 + 4x^4 + 3x^3 + 4x + 1$ be an irreducible polynomial of degree 5 over $\mathbb{F}_{5^2}$ and $I^*(x)$ be an N-polynomial over $\mathbb{F}_{5^2}$.

Also, let

$$F(x) = \left(x^5 - x + 1\right)^5 I\left(\frac{x^5 - x}{x^5 - x + 1}\right).$$

Then, $F^*(x)$ is an N-polynomial of degree 25 over $\mathbb{F}_{5^2}$ if and only if

$$\left(5 + \frac{c_1}{c_0}\right) . Tr_{5^2|5}\left(\frac{I'(1)}{I(1)} - 5\right) \neq 0.$$

Proof:

Consider an irreducible polynomial $I\left(x\right)=x^5+4x^4+3x^3+4x+1$ of degree 5 over $\mathbb{F}_{5^2}$ and its reciprocal polynomial $I^*\left(x\right)$ is a normal polynomial over $\mathbb{F}_{5^2}$. Construct a composition polynomial

$$F\left(x\right)=\left(x^5-x+1\right)^5 I\left(\frac{x^5-x}{x^5-x+1}\right), \tag{8}$$

which is an irreducible polynomial over $\mathbb{F}_{5^2}$ from given hypothesis and Alizadeh (2011) (Theorem 1).

Also, by Lidl and Niederreiter (1983) (Corollary 3.79) we have,

$$x^{25}-1=\left[\varphi_1\left(x\right)\ldots\varphi_i\left(x\right)\right]^{5t}.$$

Here, $x^{25}-1$ factors in distinct irreducible factors $\varphi_r\left(x\right)\in\mathbb{F}_{5^2}[x]$.

Denote

$$G_r\left(x\right)=\frac{x^{25}-1}{\varphi_r(x)}=\frac{(x^5-1)(x^{4*5}+x^{3*5}+x^{2*5}+x^{1*5}+1)}{x-1}$$

$$=\sum_{m=0}^{4}x^m(x^{4*5}+x^{3*5}+x^{2*5}+x^5+1)$$

$$=\sum_{m=0}^{4}\left(x^{4*5+m}+x^{3*5+m}+x^{2*5+m}+x^{5+m}+x^m\right). \tag{9}$$

Here,

$$\frac{x^5-1}{\varphi_r(x)}=\sum_{m=0}^{4}x^m.$$

Let ρ_1 be a root of $F(x)$. Then, $\sigma_1=\frac{1}{\rho_1}$ is a root of $F^*(x)$.

To prove $F^*(x)$ is an N-polynomial, we must have

$$L_{G_r}\left(\sigma_1\right)\neq 0,$$

$$L_{G_r}\left(\sigma_1\right)=\sum_{m=0}^{4}\left[(\sigma_1)^{(5^2)^{4*5+m}}+(\sigma_1)^{(5^2)^{3*5+m}}+(\sigma_1)^{(5^2)^{2*5+m}}+(\sigma_1)^{(5^2)^{5+m}}+(\sigma_1)^{(5^2)^{m}}\right],$$

$$L_{G_r}\left(\sigma_1\right)=\sum_{m=0}^{4}\left[\left(\frac{1}{\rho_1}\right)^{5^{4*2*5}}+\left(\frac{1}{\rho_1}\right)^{5^{3*2*5}}+\left(\frac{1}{\rho_1}\right)^{5^{2*2*5}}+\left(\frac{1}{\rho_1}\right)^{5^{2*5}}+\left(\frac{1}{\rho_1}\right)\right]^{5^{2m}}. \tag{10}$$

From (8), we see that $\dfrac{\rho_1^5-\rho_1}{\rho_1^5-\rho_1+1}$ is a root of $I(x)$.

Let ρ be the root of $I(x)$, so

$$\rho = \frac{\rho_1^5 - \rho_1}{\rho_1^5 - \rho_1 + 1},$$

$$\rho - 1 = -\left[\rho_1^5 - \rho_1 + 1\right]^{-1}, \tag{11}$$

$$\rho - 1 = \frac{-1}{\rho_1^5 - \rho_1 + 1},$$

$$\rho_1^5 - \rho_1 = \frac{-1}{\rho - 1} - 1 = \frac{-\rho}{\rho - 1},$$

$$\rho_1^5 - \rho_1 = \frac{\rho}{1 - \rho}. \tag{12}$$

Therefore, by (11), we get

$$(\rho - 1)^{5^{2*5}} = -\left[\rho_1^{5^{2*5+1}} - \rho_1^{5^{2*5}} + 1\right]^{-1}.$$

Using $(a+b)^{p^n} = a^{p^n} + b^{p^n}$, we have

$$(\rho - 1) = -\left[\rho_1^{5^{2*5+1}} - \rho_1^{5^{2*5}} + 1\right]^{-1}. \tag{13}$$

Then, from (11) and (13), we have

$$\left[\rho_1^{5^{2*5+1}} - \rho + 1\right]^{-1} = \left[\rho_1^5 - \rho_1 + 1\right]^{-1},$$

$$\rho_1^{5^{2*5+1}} - \rho + 1 = \rho_1^5 - \rho_1 + 1,$$

$$\rho_1^{5^{2*5+1}} - \rho_1^{5^{2*5}} = \rho_1^5 - \rho_1,$$

$$\left[\rho_1^{5^{2*5}} - \rho_1\right]^5 = \left[\rho_1^{5^{2*5}} - \rho_1\right].$$

Let $\rho_1^{5^{2*5}} - \rho_1 = \theta \in \mathbb{F}_5$ and by using induction, we have

$$\rho_1^{5^{k*2*5}} = \rho + k\theta, \text{ where } k = 0, 1, ...4. \tag{14}$$

Therefore, from (10) and (14), we get

$$L_{G_r}(\sigma_1) = \sum_{m=0}^{4} \left[\left(\frac{1}{\rho_1 + 4\theta}\right) + \left(\frac{1}{\rho_1 + 3\theta}\right) + \left(\frac{1}{\rho_1 + 2\theta}\right) + \left(\frac{1}{\rho_1 + \theta}\right) + \left(\frac{1}{\rho_1}\right)\right]^{5^{2*m}}$$
$$= \sum_{m=0}^{4} \left(\frac{-1}{\rho_1^5 - \rho_1}\right)^{5^{2*m}}.$$

Then, by (5), we have

$$L_{G_r}(\sigma_1) = \sum_{m=0}^{4} \left[\frac{\rho - 1}{\rho}\right]^{5^{2*m}} = \sum_{m=0}^{4} \left[1 - \frac{1}{\rho}\right]^{5^{2*m}}.$$

Let $H\left(x\right)=I^{*}(x)$ be an N-polynomial. From Theorem 3.1 and Menezes et al. (1993) (Theorem 4.18), $H\left(1-x\right)$ is an N-polynomial. But $\left(1-\frac{1}{\rho}\right)$ is a root of $H\left(1-x\right)$, so we get

$$\sum_{m=0}^{4}\left[1-\frac{1}{\rho}\right]^{5^{2*m}}\neq 0.$$

Hence, it is proved. ■

Example 3.2.

Consider an irreducible polynomial $I\left(x\right)=2x^{7}+3x^{6}+6x^{5}+3x^{4}+2x^{3}+5x^{2}+4x+5$ of degree 7 over $\mathbb{F}_{7^2}$ and its reciprocal polynomial $I^{*}\left(x\right)$ is a normal polynomial over $\mathbb{F}_{7^2}$. Construct a composite polynomial

$$F\left(x\right)=\left(x^{7}-x+1\right)^{7}I\left(\frac{x^{7}-x}{x^{7}-x+1}\right), \tag{15}$$

which is irreducible over $\mathbb{F}_{7^2}$ by Alizadeh (2011) (Theorem 1). On the other side by Schwartz (1988), we have

$$x^{49}-1=\left[\varphi_{1}\left(x\right)\ldots\varphi_{i}\left(x\right)\right]^{7t}.$$

Here, $x^{49}-1$ factors in distinct irreducible factors $\varphi_{r}\left(x\right)\in\mathbb{F}_{7^2}[x]$.

Denote

$$\begin{aligned}G_{r}\left(x\right)&=\frac{x^{49}-1}{\varphi_{r}\left(x\right)}\\&=\frac{(x^{7}-1)(x^{6*7}+x^{5*7}+...+x^{7}+1)}{x-1}\\&=\sum_{m=0}^{6}x^{m}(x^{6*7}+x^{5*7}+...+x^{7}+1)\\&=\sum_{m=0}^{6}\left(x^{6*7+m}+x^{5*7+m}+...+x^{7+m}+x^{m}\right).\end{aligned} \tag{16}$$

Here,

$$\frac{x^{49}-1}{x-1}=\sum_{m=0}^{6}x^{m}.$$

Assume that ρ_1 be a root of $F(x)$. Then, $\sigma_1=\frac{1}{\rho_1}$ is a root of $F^{*}(x)$.

To prove $F^{*}(x)$ is an N-polynomial, we must have

$$L_{G_r}\left(\sigma_1\right)\neq 0,$$

$$L_{G_r}\left(\sigma_1\right)=\sum_{m=0}^{6}\left[\left(\sigma_1\right)^{(7^2)^{6*7+m}}+\left(\sigma_1\right)^{(7^2)^{5*7+m}}+\cdots+\left(\sigma_1\right)^{(7^2)^{7+m}}+\ \left(\sigma_1\right)^{(7^2)^{m}}\right],$$

$$L_{G_r}(\sigma_1) = \sum_{m=0}^{6}\left[\left(\frac{1}{\rho_1}\right)^{7^{2*6*7}} + \left(\frac{1}{\rho_1}\right)^{7^{2*5*7}} + \ldots + \left(\frac{1}{\rho_1}\right)^{7^{2*7}} + \left(\frac{1}{\rho_1}\right)\right]^{7^{2*m}}. \tag{17}$$

From (15), we may check that $\dfrac{\rho_1^7-\rho_1}{\rho_1^7-\rho_1+1}$ is a root of $I(x)$.

Let ρ be the root of $I(x)$, so

$$\rho = \frac{\rho_1^7-\rho_1}{\rho_1^7-\rho_1+1},$$

$$\rho - 1 \ = \ -\left[\rho_1^7-\rho_1+1\right]^{-1}, \tag{18}$$

$$\rho - 1 = \frac{-1}{\rho_1^7-\rho_1+1},$$

$$\rho_1^7-\rho_1 = \frac{-1}{\rho-1} - 1 = \frac{-\rho}{\rho-1},$$

$$\rho_1^7-\rho_1 = \frac{\rho}{1-\rho}, \tag{19}$$

$$(\rho-1)^{7^{2*7}} = -\left[\rho_1^{7^{2*7+1}} - \rho_1^{7^{2*7}} + 1\right]^{-1}.$$

Using$(a+b)^{p^n} = a^{p^n} + b^{p^n}$, we have

$$(\rho-1) = -\left[\rho_1^{7^{2*7+1}} - \rho_1^{7^{2*7}} + 1\right]^{-1}. \tag{20}$$

Then, from (18) and (20), we obtain

$$\left[\rho_1^{7^{2*7+1}} - \rho_1^{7^{2*7}} + 1\right]^{-1} = \left[\rho_1^7-\rho_1+1\right]^{-1},$$

$$\rho_1^{7^{2*7+1}} - \rho + 1 = \rho_1^7 - \rho_1 + 1,$$

$$\rho_1^{7^{2*7+1}} - \rho_1^{7^{2*7}} = \rho_1^7 - \rho_1,$$

$$[\rho_1^{7^{2*7}} - \rho]^7 = \left[\rho_1^{7^{2*7}} - \rho_1\right].$$

Let $\rho_1^{7^{2*7}} - \rho_1 = \theta \in \mathbb{F}_7$ and by using induction, we have

$$\rho_1^{7^{k*2*7}} = \rho + k\theta. \tag{21}$$

So, from (17) and (21), we get

$$\begin{aligned} L_{G_r}(\sigma_1) &= \sum_{m=0}^{6}\left[\left(\frac{1}{\rho_1+6\theta}\right) + \left(\frac{1}{\rho_1+5\theta}\right) + \cdots + \left(\frac{1}{\rho_1+\theta}\right) + \left(\frac{1}{\rho_1}\right)\right]^{7^{2*m}} \\ &= \sum_{m=0}^{6}\left(\frac{-1}{\rho_1^7-\rho}\right)^{7^{2*m}}. \end{aligned}$$

Then, by (12), we have

$$L_{G_r}(\sigma_1) = \sum_{m=0}^{6}\left[\frac{\rho-1}{\rho}\right]^{7^{2*m}} = \sum_{m=0}^{6}\left[1-\frac{1}{\rho}\right]^{7^{2*m}}.$$

Let $H(x) = I^*(x)$ be an N-Polynomial. From the given hypothesis inTheorem 3.1 and Menezes et al. (1993) (Theorem 4.18), $H(1-x)$ is an N-polynomial, but $\left(1-\frac{1}{\rho}\right)$ is a root of $H(1-x)$. We get

$$\sum_{m=0}^{6}\left[1-\frac{1}{\rho}\right]^{7^{2*m}} \neq 0.$$

Hence it is proved.

4. Conclusion

There are different ways to construct a normal polynomial over finite fields. In this paper, we constructed families of normal polynomials over the finite field of odd prime characteristic by using composition of polynomial. Further, we showed that the reciprocal of the composite polynomial is a normal polynomial of degree pn over finite field with some restrictions.

Acknowledgment:

The authors acknowledge the anonymous reviewers for their positive comments.

REFERENCES

Alizadeh, M. (2011). Constructing methods for irreducible polynomials, Mathematical Problems of Computer Science, Vol. 35, pp. 26-32.

Alizadeh, M. (2012). Some algorithms for normality testing irreducible polynomials and computing complexity of the normal polynomials over finite fields, Applied Mathematical Sciences, Vol. 6, No. 40, pp. 1997-2003.

Alizadeh, M., Abrahamyan, S., Mehrabi, S. and Kyuregyan, M. K. (2011). Constructing of N-polynomials over finite fields, International Journal of Algebra, Vol. 5, No. 29, pp. 1437-1442.

Alizadeh, M., Darafsheh, M. R. and Mehrabi, S. (2018). On the k-normal elements and polynomials over finite fields, Italian Journal of Pure and Applied Mathematics, Vol. 39, pp. 451-464.

Alizadeh, M. and Mehrabi, S. (2015). Construction of self- reciprocal normal polynomials over finite fields of even characteristic, Turkish Journal of Mathematics, Vol. 39, pp. 259-267.

Alizadeh, M. and Mehrabi, S. (2016). Recursive constructions of k-normal polynomials over finite fields, arXiv preprint arXiv:1610.05684.

Chapman, R. (1997). Completely normal elements in iterated quadratic extensions of finite fields, Finite Fields and Their Applications, Vol. 3, No. 1, pp. 1-10.

Cohen, S. D. (1969). On irreducible polynomials of certain types in finite fields, Mathematical Proceedings of the Cambridge Philosophical Society, Vol. 66, No. 2, pp. 335-344.

Gao, S. (1993). Normal bases over finite fields, Ph.D Thesis, Waterloo, Canada: University of Waterloo.

Hou, X. D. (2022). Normal polynomials over finite fields, arXiv preprint, arXiv:2212.04978.

Huczynska, S., Mullen, G. L., Panario, D. and Thomson, D. (2013). Existence and properties of k-normal elements over finite fields, Finite Fields and Their Applications, Vol. 24, pp. 170-183.

Jungnickel, D. (1993). Trace-orthogonal normal bases, Discrete Applied Mathematics, Vol. 47, No. 3, pp. 233-249.

Kim, R. and Son, H. S. (2020). Recursive constructions of k-normal polynomials using some rational transformations over finite fields, Journal of Algebra and its Applications, 2050210, pp. 1-16.

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

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

Kyuregyan, M. K. (2008). Recursive constructions of N-polynomials over $GF(2^s)$, Discrete Applied Mathematics, Vol. 156, No. 9, pp. 1554-1559.

Lidl, R. and Niederreiter, H. (1983). Finite Fields, *Encyclopedia of Mathematics and its Applications*, Addison-Wesley, Reading, MA, Vol. 20.

Lidl, R. and Niederreiter, H. (1994). *Introduction to Finite Fields and Their Applications*, Cambridge University Press.

Menezes, A. J., Blake, I. F., Gao, X., Mullin, R. C., Vanstone, S. A. and Yaghoobian, T. (1993). *Applications of Finite Fields*, Kluwer Academic Publishers, Boston.

Meyn, H. (1995). Explicit N-polynomials of 2-power degree over finite fields, Designs, Codes and Cryptography, Vol. 6, pp. 107-116.

Scheerhorn, A. (1994). Iterated constructions of normal bases over finite fields, In: Mullen, G. L. and Shiue, P. J. S., editors, *Finite Fields: Theory, Applications and Algorithms*, Contemporary Mathematics, American Mathematical Society, Providence, RI.

Schwartz, S. (1988). Irreducible polynomials over finite fields with linearly independent roots, Mathematica Slovaca, Vol. 38, No. 2, pp. 147-158.

Sharma, P. L. and Ashima. (2022). Construction of irreducible polynomials over finite fields, Asian-European Journal of Mathematics, Vol. 15, No. 7, 2250130.

Sharma, P. L., Ashima and Sharma, A. K. (2022). Recursive construction of normal polynomials over finite fields, Journal of Discrete Mathematical Sciences and Cryptography, Vol. 25, No. 8, pp. 2645-2660.