Turkish Journal of Mathematics

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

Research Article

Turk J Math
(2015) 39
© TÜBİTAK
doi:10.3906/mat-1407-32

Construction of self-reciprocal normal polynomials over finite fields of even characteristic

Mahmood ALIZADEH[1,*], **Saeid MEHRABI**[2]
[1]Department of Mathematics, College of Science, Ahvaz Branch, Islamic Azad University, Ahvaz, Iran
[2]Department of Mathematics, Farhangian University, Tehran, Iran

Received: 11.07.2014 • **Accepted:** 14.01.2015 • **Published Online:** 23.02.2015 • **Printed:** 20.03.2015

Abstract: In this paper, a computationally simple and explicit construction of some sequences of normal polynomials and self-reciprocal normal polynomials over finite fields of even characteristic are presented.

Key words: Finite fields, normal polynomial, self-reciprocal

1. Introduction

Let $\mathbb{F}_q$, be the Galois field of order $q = p^s$, where p is a prime and s is a natural number, and $\mathbb{F}_q^*$ be its multiplicative group. Let $P(x)$ be a monic irreducible polynomial of degree n over $\mathbb{F}_q$ and β be a root of $P(x)$. The field $\mathbb{F}_q(\beta) = \mathbb{F}_{q^n}$ is an n-dimensional extension of $\mathbb{F}_q$ and can be considered as a vector space of dimension n over $\mathbb{F}_q$. The Galois group of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is cyclic and is generated by the Frobenius mapping $\sigma(\alpha) = \alpha^q$, $\alpha \in \mathbb{F}_{q^n}$. A *normal* basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a basis of the form $N = \{\alpha, \alpha^q, ..., \alpha^{q^{n-1}}\}$, i.e. a basis that consists of the algebraic conjugates of a fixed element $\alpha \in \mathbb{F}_{q^n}^*$. Recall that an element $\alpha \in \mathbb{F}_{q^n}$ is said to generate a normal basis over $\mathbb{F}_q$ if its conjugates form a basis of $\mathbb{F}_{q^n}$ as a vector space over $\mathbb{F}_q$. For our convenience we call a generator of a normal basis a *normal* element. A monic irreducible polynomial $F(x) \in \mathbb{F}_q[x]$ is called *normal polynomial* or *N-polynomial* if its roots form a normal basis or, equivalently, if they are linearly independent over $\mathbb{F}_q$. The elements in a normal basis are exactly the roots of some N-polynomial. Hence, an N-polynomial is just another way of describing a normal basis. It is well known that such a basis always exists and any element of N is a generator of N (the normal basis theorem, see [4], Theorem 1.4.1).

The construction of N-polynomials over any finite field is a challenging mathematical problem. Interest in N-polynomials stems both from mathematical theory and practical applications such as coding theory and several cryptosystems using finite fields. The problem in general is: given an integer n and the ground field $\mathbb{F}_q$, construct a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, or, equivalently, construct an N-polynomial in $\mathbb{F}_q[x]$ of degree n by providing an efficient construction method.

Some results regarding constructions of special sequences $(F_k(x))_{k\geq 0}$ of normal polynomials over $\mathbb{F}_q$ can be found in [2, 4, 6, 7, 9] and [10, 11]. All constructions are considered as computationally easy and explicit. Cohen [3] and McNay [8] gave iterative constructions of irreducible polynomials of 2-power degree over finite

*Correspondence: alizadeh@iauahvaz.ac.ir

2010 *AMS Mathematics Subject Classification:* 12Y05.

fields of odd characteristics. Meyn [10] and Chapman [2] showed that these polynomials are N-polynomials. Another family of N-polynomials of degree 2^k was suggested by Gao [4], who constructed specific sequences $(F_k(x))_{k\geq 0}$ of N-polynomials of degree p^{k+2} over $\mathbb{F}_p$. In these constructions he used substitutions introduced earlier by Varshamov [13]. Kyuregyan in [6, 7] proposed a rather more general iterative technique of constructing sequences $(F_k(x))_{k\geq 0}$ of N-polynomials of degree p^{k+2} over $\mathbb{F}_q$ compared with the ones given by Gao [4] and Scheerhorn [11]. While in the constructions of N-polynomials over $\mathbb{F}_{2^S}$ suggested by Gao [4] and Scheerhorn [11] the initial polynomial is a quadratic normal polynomial, in constructions suggested by Kyuregyan in [7] the initial polynomial is a normal polynomial of arbitrary degree.

In this paper, a computationally simple and explicit construction of sequences $(F_k(x))_{k\geq 0}$ of normal polynomials and $(F_k(x+1))_{k\geq 0}$ of self-reciprocal normal polynomials over $\mathbb{F}_{2^s}$ is presented. For this, we will show that all members of the sequence $(F_k(x))_{k\geq 0}$ defined by polynomials $F_k(x) \in \mathbb{F}_{2^s}[x]$ of degree $n2^k$ that are constructed by iterated application of the polynomial composition $F_k(x) = x^{n2^k} F_{k-1}(\frac{x^2+x+1}{x^2}), \quad k \geq 0$, for a suitable chosen initial normal polynomial $F_0(x) \in \mathbb{F}_{2^s}[x]$ of degree n, for which the polynomial $F_0(x+1)$ is a self-reciprocal normal polynomial, are N-polynomials and the polynomials $F_k(x+1)$ are self-reciprocal normal polynomials over $\mathbb{F}_{2^s}$. Such a sequence of polynomials define a sequence of extension fields $\mathbb{F}_{2^{sn2^k}}$ whose union is denoted by $\mathbb{F}_{2^{sn2^\infty}} = \cup_{k\geq 0}\mathbb{F}_{2^{sn2^k}}$.

2. Preliminary notes

We need the following normality results for our further study.

Let p denote the characteristic of $\mathbb{F}_q$ and let $n = n_1 p^e = n_1 t$, with $gcd(p, n_1) = 1$, and suppose that $x^n - 1$ has the following factorization in $\mathbb{F}_q[x]$:

$$x^n - 1 = (x^{n_1} - 1)^t = (\varphi_1(x)\varphi_2(x)\cdots\varphi_r(x))^t, \tag{1}$$

where $\varphi_i(x) \in \mathbb{F}_q[x]$ are the distinct irreducible factors of $x^{n_1} - 1$. For $1 \leq i \leq r$, let

$$\phi_i(x) = \frac{x^n - 1}{\varphi_i(x)}. \tag{2}$$

We assume that $\phi_i(x)$ has degree m_i for $1 \leq i \leq r$. Furthermore, we will need Schwartz's theorem in [12] (see also [9], Theorem 4.18), which allows us to check whether an irreducible polynomial is N-polynomial.

Proposition 2.1 *([9], Theorem 4.18) Let $F(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_q$ and α be a root of $F(x)$. Let $x^n - 1$ factor as (1) and let $\phi_i(x)$ be as in (2). Then $F(x)$ is N-polynomial over $\mathbb{F}_q$ if and only if*

$$L_{\phi_i}(\alpha) \neq 0 \ for \ i = 1, 2, \ldots, r$$

where $L_{\phi_i}(x)$ is the linearized polynomial defined by

$$L_{\phi_i}(x) = \sum_{v=0}^{m_i} t_{iv} x^{q^v} \ if \ \phi_i(x) = \sum_{v=0}^{m_i} t_{iv} x^v.$$

A result by Jungnickel in [5] states when an element of $\mathbb{F}_q$ is a normal bases generator. We can restate it as follows.

Lemma 2.2 *Let* $f(x) = \sum_{i=0}^{n} c_i x^i$ *be* N*-polynomial of degree* n *over* $\mathbb{F}_q$. *Suppose* $g(x) = f(\frac{x-a}{b})$, *where* $a, b \in \mathbb{F}_q$ *and* $b \neq 0$. *Then* $g(x)$ *is* N*-polynomial if and only if* $na - b\frac{c_{n-1}}{c_n} \neq 0$.

Proof Let $n = n_1 p^e = n_1 t$, and then by (1), $x^n - 1$ has the following factorization in $\mathbb{F}_q[x]$:

$$x^n - 1 = (x^{n_1} - 1)^t = (\varphi_1(x)\varphi_2(x)\cdots\varphi_r(x))^t,$$

where $\varphi_1(x) = x - 1$. Set for $i = 2, 3, \ldots, r$

$$\begin{aligned}\phi_i(x) &= \frac{x^n - 1}{\varphi_i(x)} \\ &= (x-1)^t s_i(x) \\ &= (x-1)s_i'(x),\end{aligned}$$

where

$$s_i'(x) = (x-1)^{t-1} s_i(x) = \sum_{v=0}^{m_i'} t_{iv}' x^v.$$

Hence,

$$\phi_i(x) = \sum_{v=0}^{m_i'} t_{iv}' x^{v+1} - \sum_{v=0}^{m_i'} t_{iv}' x^v.$$

Since $f(x)$ is N-polynomial, then by Proposition 2.1 we have $L_{\phi_i}(\alpha) \neq 0$ for each $i = 1, 2, \ldots, r$, where α is a root of $f(x)$. We need to show that $L_{\phi_i}(a + b\alpha) \neq 0$ is also true for each $i = 2, 3, \ldots, r$, where $a + b\alpha$ is a root of $g(x)$. Since

$$L_{\phi_i}(a + b\alpha) = \sum_{v=0}^{m_i'} t_{iv}'(a + b\alpha)^{q^{v+1}} - \sum_{v=0}^{m_i'} t_{iv}'(a + b\alpha)^{q^v},$$

we have

$$\begin{aligned}L_{\phi_i}(a + b\alpha) &= a\sum_{v=0}^{m_i'} t_{iv}' + b\sum_{v=0}^{m_i'} t_{iv}'\alpha^{q^{v+1}} - a\sum_{v=0}^{m_i'} t_{iv}' - b\sum_{v=0}^{m_i'} t_{iv}'\alpha^{q^v} \\ &= b(\sum_{v=0}^{m_i'} t_{iv}'\alpha^{q^{v+1}} - \sum_{v=0}^{m_i'} t_{iv}'\alpha^{q^v}) \\ &= bL_{\phi_i}(\alpha) \neq 0, \end{aligned} \tag{3}$$

and hence, for $g(x)$ to be an N-polynomial, it suffices to solve the condition $L_{\phi_1}(a + b\alpha) \neq 0$. On the other hand, we have

$$\phi_1(x) = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1 = \sum_{i=0}^{n-1} x^i.$$

So:

$$\begin{aligned} L_{\phi_1}(a+b\alpha) &= \sum_{i=0}^{n-1}(a+b\alpha)^{q^i} \\ &= \sum_{i=0}^{n-1} a + b\sum_{i=0}^{n-1}\alpha^{q^i} \\ &= na + bTr_{q^n|q}(\alpha) = na - b\frac{c_{n-1}}{c_n}, \end{aligned} \tag{4}$$

which is nonzero by hypothesis. This completes the proof. □

In the following propositions a family of irreducible polynomials of degree $n2^k$ over $\mathbb{F}_{2^s}$ is suggested. We will use them in the proof of our results.

Proposition 2.3 *([1], Theorem 2.2) Recalling the definitions of P^* and $P^{*'}$, 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

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

Proposition 2.4 *([1], Theorem 3.1) Let $P(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_{2^s}$. Define*

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

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

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

3. Construction of N-polynomials over finite fields

In this section we establish theorems that will show how Propositions 2.3 and 2.4 can be applied to produce N-polynomials over $\mathbb{F}_{2^s}$.

Theorem 3.1 *Let $P(x) = \sum_{i=0}^n c_i x^i$, with $P(x) \neq x$ an N-polynomial of degree n over $\mathbb{F}_{2^s}$ such that $P(x+1)$ is a self-reciprocal polynomial over $\mathbb{F}_{2^s}$. Also let*

$$F(x) = x^{2n}P(\frac{x^2+x+1}{x^2}). \tag{6}$$

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

$$Tr_{2^s|2}(\frac{c_{n-1}}{c_n}+n)\neq 0.$$

Proof Recall the definition of $Ord_{\alpha,\sigma}$. Since $P(x)$ is an irreducible polynomial over $\mathbb{F}_{2^s}$, Proposition 2.3 and the hypothesis imply that $F(x)$ is irreducible over $\mathbb{F}_{2^s}$. Let $\alpha\in\mathbb{F}_{2^{sn}}$ be a root of $P(x)$. Since $P(x)$ is an N-polynomial of degree n over $\mathbb{F}_{2^s}$ by the hypothesis, $\alpha\in\mathbb{F}_{2^{sn}}$ is a normal element over $\mathbb{F}_{2^s}$ and hence has order $Ord_{\alpha,\sigma}(x)=x^n-1$.

Let $n=n_1 2^e$, where n_1 is a nonnegative integer with $gcd(n_1,2)=1$ and $e\geq 0$. For convenience we denote 2^e by t. Let x^n-1 have the following factorization in $\mathbb{F}_{2^s}[x]$:

$$x^n-1=(\varphi_1(x)\varphi_2(x)\cdots\varphi_r(x))^t, \tag{7}$$

where the polynomials $\varphi_i(x)\in\mathbb{F}_q[x]$ are the distinct irreducible factors of $x^{n_1}-1$. Set

$$\phi_i(x)=\frac{(x^n-1)}{\varphi_i(x)}=\sum_{v=0}^{m_i}t_{iv}x^v, i=1,2,\ldots,r. \tag{8}$$

By the hypothesis $\frac{c_{n-1}}{c_n}+n\neq 0$, and so by Lemma 2.2, $P(x+1)$ is a normal polynomial.

Now we proceed by proving that $F(x)$ is a normal polynomial. Let α_1 be a root of $F(x)$.

We only need to show that the σ-order of α_1 is

$$Ord_{\alpha_1,\sigma}(x)=x^{2n}-1.$$

Note that by (7) the polynomial $x^{2n}-1$ has the following factorization in $\mathbb{F}_{2^s}[x]$:

$$x^{2n}-1=(\varphi_1(x)\cdot\varphi_2(x)\cdot\cdots\cdot\varphi_r(x))^{2t},$$

where $\varphi_i(x)\in\mathbb{F}_{2^s}[x]$ are distinct irreducible factors of $x^{n_1}-1$. Let

$$H_i(x)=\frac{x^{2n}-1}{\varphi_i(x)},$$

or

$$H_i(x)=\frac{x^{2n}-1}{\varphi_i(x)}=(x^n+1)\cdot\frac{x^n-1}{\varphi_i(x)}.$$

By (8) we obtain

$$H_i(x)=(x^n+1)\cdot\phi_i(x).$$

Hence, since $\phi_i(x)=\sum_{v=0}^{m_i}t_{iv}x^v$, $i=1,2,\ldots,r$, we have

$$H_i(x)=\sum_{v=0}^{m_i}t_{iv}(x^{n+v}+x^v).$$

It follows that

$$L_{H_i}(\alpha_1)=\sum_{v=0}^{m_i}t_{iv}({\alpha_1}^{2^{sn}}+\alpha_1)^{2^{sv}}. \tag{9}$$

Note that, according to Proposition 2.1, to complete the proof of the theorem we only need to show that

$$L_{H_i}(\alpha_1) \neq 0 \; for\ each\ i = 1, 2, \ldots, r.$$

From (6), if α_1 is a zero of $F(x)$, then $\frac{{\alpha_1}^2+\alpha_1+1}{{\alpha_1}^2}$ is a zero of $P(x)$. It may thus be assumed that

$$\alpha = \frac{{\alpha_1}^2 + \alpha_1 + 1}{{\alpha_1}^2},$$

where α is a root of $P(x)$. It follows that

$$\alpha + 1 = \frac{\alpha_1 + 1}{{\alpha_1}^2} = \frac{1}{\alpha_1} + \frac{1}{{\alpha_1}^2}. \tag{10}$$

Now, by (10) and observing that $P(x)$ is an irreducible polynomial of degree n over $\mathbb{F}_{2^s}$, we obtain

$$\alpha + 1 = (\alpha + 1)^{2^{sn}} = (\frac{1}{\alpha_1} + \frac{1}{{\alpha_1}^2})^{2^{sn}}. \tag{11}$$

It follows from (10) and (11) that

$$(\frac{1}{\alpha_1} + (\frac{1}{\alpha_1})^{2^{sn}})^2 = (\frac{1}{\alpha_1} + (\frac{1}{\alpha_1})^{2^{sn}}). \tag{12}$$

It is clear that $(\frac{1}{\alpha_1} + (\frac{1}{\alpha_1})^{2^{sn}}) \neq 0$.

Hence, it follows from (12) that $\frac{1}{\alpha_1} + (\frac{1}{\alpha_1})^{2^{sn}} = 1$. Therefore,

$${\alpha_1}^{2^{sn}} = \frac{\alpha_1}{1 + \alpha_1}. \tag{13}$$

Now by (10) and (13), we can obtain

$${\alpha_1}^{2^{sn}} + \alpha_1 = \frac{1}{\alpha + 1}. \tag{14}$$

Thus, by (9) and (14), we have

$$L_{H_i}(\alpha_1) = \sum_{v=0}^{m_i} t_{iv} (\frac{1}{\alpha + 1})^{2^{sv}}. \tag{15}$$

Since $\frac{1}{\alpha+1}$ is a zero of the normal polynomial $(P(x+1))^*$, therefore $L_{H_i}(\alpha_1) \neq 0$. Hence, $F(x)$ is a normal polynomial of degree $2n$ over $\mathbb{F}_{2^s}$, and the proof is completed. □

4. Recurrent methods for constructing normal polynomials

In this section we describe a computationally simple and explicit recurrent method for constructing higher degree normal polynomials over finite fields $\mathbb{F}_{2^s}$ starting from a normal polynomial. We begin by establishing the following theorem.

Theorem 4.1 *Let $P(x) = \sum_{i=0}^{n} c_i x^i$, with $P(x) \neq x$ an N-polynomial of degree n over $\mathbb{F}_{2^s}$ such that $P(x+1)$ is a self-reciprocal polynomial over $\mathbb{F}_{2^s}$. Define*

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

$$F_k(x) = x^{n2^k} F_{k-1}(\frac{x^2+x+1}{x^2}) \qquad k \geq 1. \tag{16}$$

Then $(F_k(x))_{k\geq 0}$ and $(F_k(x+1))_{k\geq 0}$ are the sequences of N-polynomials and self-reciprocal N-polynomials of degree $n2^k$ over $\mathbb{F}_{2^s}$, respectively, if and only if

$$Tr_{2^s|2}(\frac{P'(1)}{P(1)}) \cdot Tr_{2^s|2}(\frac{c_{n-1}}{c_n} + n) \neq 0,$$

where $P^{'}(1)$ is the formal derivative of $P(x)$ at point 1.

Proof It is easy to check that the polynomial $F_k(x+1)$, for each $k \geq 1$, is self-reciprocal by using the definitions. According to Proposition 2.4 for each $k \geq 1$, $F_k(x)$ is an irreducible polynomial over $\mathbb{F}_{2^s}$. Consequently, $(F_k(x+1))_{k\geq 0}$ is a sequence of irreducible polynomials over $\mathbb{F}_{2^s}$. The proof of normality of the irreducible polynomial $F_k(x)$ for each $k \geq 1$ is done by mathematical induction on k.

For $k = 1$, $F_1(x)$ is a normal polynomial according to Theorem 3.1.

For $k \geq 2$, we show that $F_k(x)$ is also a normal polynomial. To this end we need to show that the hypothesis of Theorem 3.1 is satisfied. However, by induction hypothesis, we have $F_{k-1}(x)$ as a normal polynomial and $F_{k-1}(x+1)$ as a self-reciprocal polynomial. Thus, by Theorem 3.1, $F_k(x)$ is a normal polynomial if and only if

$$Tr_{2^s|2}(\frac{{F^*_{k-1}}'(0)}{F^*_{k-1}(0)} + 2^{k-1}n) \neq 0,$$

or

$$Tr_{2^s|2}(\frac{{F^*_{k-1}}'(0)}{F^*_{k-1}(0)}) \neq 0.$$

However, from (16), we have

$$\begin{aligned} F^*_{k-1}(x) &= x^{n2^{(k-1)}} F_{k-1}(\frac{1}{x}) \\ &= x^{n2^{(k-1)}} ((\frac{1}{x})^{n2^{(k-1)}} F_{k-2}(\frac{(\frac{1}{x})^2 + (\frac{1}{x}) + 1}{(\frac{1}{x})^2}) \\ &= F_{k-2}(x^2+x+1). \end{aligned} \tag{17}$$

So

$$F^*_{k-1}(0) = F_{k-2}(1) \tag{18}$$

and

$${F^*_{k-1}}'(0) = F'_{k-2}(1). \tag{19}$$

On the other hand:

$$F'_{k-1}(x) = x^{n2^{(k-1)}-2} F'_{k-2}(\frac{x^2+x+1}{x^2}). \tag{20}$$

So

$$F'_{k-1}(1) = F'_{k-2}(1). \tag{21}$$

Using (19) and (21), we get

$${F^*_{k-1}}'(0) = P'(1). \tag{22}$$

Obviously by (16)

$$F_{k-1}(1) = F_{k-2}(1). \tag{23}$$

So (18) and (23) imply that

$$F^*_{k-1}(0) = P(1). \tag{24}$$

Hence, by (22) and (24) we obtain

$$Tr_{2^s|2}(\frac{{F^*_{k-1}}'(0)}{F^*_{k-1}(0)}) = Tr_{2^s|2}(\frac{P'(1)}{P(1)}), \tag{25}$$

which is not equal to zero by the hypothesis of the theorem and so $(F_k(x))_{k\geq 0})$ is a sequence of N-polynomials of degree $n2^k$ over $\mathbb{F}_{2^s}$. Finally, we note that by Lemma 2.2, for every $k \geq 1$, $F_k(x+1)$ is an N-polynomial if and only if ${F_k^*}'(0) \neq 0$. Thus, (22) and the hypothesis of the theorem imply that $(F_k(x+1))_{k\geq 0}$ is a sequence of self-reciprocal N-polynomials of degree $n2^k$ over $\mathbb{F}_{2^s}$. The theorem is proved. □

Example 4.2 *Consider the normal polynomial $P(x) = x^2+x+1$ over $\mathbb{F}_2$. It is easy to see that the assumptions of Theorem 4.1 are fulfilled. Therefore, the composite polynomials*

$$F_1(x) = x^4 P(\frac{x^2+x+1}{x^2}) = x^4+x^3+1$$

and

$$\begin{aligned} F_2(x) &= x^8 F_1(\frac{x^2+x+1}{x^2}) \\ &= x^8+x^7+x^5+x^4+x^3+x^2+1 \end{aligned}$$

are normal polynomials over $\mathbb{F}_2$. Furthermore, the polynomials

$$F_1(x+1) = x^4+x^3+x^2+x+1$$

and

$$F_2(x+1) = x^8+x^7+x^6+x^4+x^2+x+1$$

are self-reciprocal normal polynomials over $\mathbb{F}_2$. Obviously, Theorem 4.1 describes a computationally simple and explicit recurrent method for constructing normal and self-reciprocal normal polynomials, so computing the normal and self-reciprocal normal polynomials $F_k(x)$ and $F_k(x+1)$, respectively, for $k \geq 3$ is not a complex problem.

Acknowledgment

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

References

[1] Alizadeh M. On the irreducibility of some composite polynomials. Journal of Mathematical Extension 2012; 6: 65–73.

[2] Chapman R. Completely normal elements in iterated quadratic extensions of finite fields. Finite Fields Appl 1997; 3: 3–10.

[3] Cohen S. D. The explicit constructions of irreducible polynomials over finite fields. Designs Code Cryptogr 1992; 2: 169–174.

[4] Gao S. Normal bases over finite fields. PhD, University of Waterloo, Waterloo, Canada, 1993.

[5] Jungnickel D. Trace-orthogonal normal basis. Discrete Appl Math 1993; 47: 233–249.

[6] Kyuregyan MK. Iterated construction of irreducible polynomials over finite fields with linearly independent roots. Finite Fields Appl 2004; 10: 323–341.

[7] Kyuregyan MK. Recursive construction of N-polynomials over $GF(2^s)$. Discrete Appl Math 2008; 156: 1554–1559.

[8] McNay G. Topics in finite fields. PhD, University of Glasgow, Glasgow, UK, 1995.

[9] Menezes AJ, Blake IF, Gao X, Mullin RC, Vanstone SA, Yaghoobian T. Applications of Finite Fields. Dordrecht, the Netherlands: Kluwer Academic, 1993.

[10] Meyn H. Explicit N-polynomials of 2-degree over finite fields. Designs Code Cryptogr 1995; 6: 107–116.

[11] Scheerhorn A. Iterated constructions of normal bases over finite fields. In: Mullen GL, Shiue PJS, editors. Finite Fields: Theory, Applications and Algorithms. Providence, RI, USA: American Mathematical Society, 1994, pp. 309–325.

[12] Schwartz S. Irreducible polynomials over finite fields with linearly independent roots. Math Slovaca 1988; 38: 147–158.

[13] Varshamov RR. A general method of synthesizing irreducible polynomials over Galois fields. Soviet Math Dokl 1984; 29: 334–336.