ON THE k-NORMAL ELEMENTS AND POLYNOMIALS OVER FINITE FIELDS

Mahmood Alizadeh*
Department of Mathematics
Ahvaz Branch
Islamic Azad University
Ahvaz
Iran
alizadeh@iauahvaz.ac.ir

Mohammad Reza Darafsheh
School of Mathematics
Statistics and Computer Science College of Science
University of Tehran
Tehran
Iran
darafsheh@ut.ac.ir

Saeid Mehrabi
Department of Mathematics
Farhangian University
Tehran
Iran
saeid_mehrabi@yahoo.com

Abstract. An element $\alpha \in \mathbb{F}_{q^n}$ is normal over $\mathbb{F}_q$ if the set $\{\alpha, \alpha^q, ..., \alpha^{q^{n-1}}\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The k-normal elements over finite fields are defined and characterized by Huczynska, Mullen, Panario and Thomson (2013). For $0 \leq k \leq n-1$, the element $\alpha \in \mathbb{F}_{q^n}$ is said to be a k-normal element if $gcd(x^n - 1, \sum_{i=0}^{n-1} \alpha^{q^i} x^{n-1-i})$ has degree k. It is well known that a 0-normal element is a normal element. So, the k-normal elements are a generalization of normal elements. By analogy with the case of normal polynomials, a monic irreducible polynomial of degree n is called a k-normal polynomial if its roots are k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. In this paper, a new characterization and construction of k-normal elements and polynomials over finite fields are given.
Keywords: finite field, normal basis, k-normal element, k-normal polynomial.

1. Introduction

Let $\mathbb{F}_q$ be the Galois field of order $q = p^m$, where p is a prime and m is a natural number, and $\mathbb{F}_q^*$ be its multiplicative group. 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 $\alpha \in \mathbb{F}_{q^n}^*$. Such an element $\alpha \in \mathbb{F}_{q^n}$ is

$*$. Corresponding author

said to generate a normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and for convenience called a *normal element*.

A monic irreducible polynomial $F(x) \in \mathbb{F}_q[x]$ is called *normal polynomial* or *N-polynomial* if its roots are linearly independent over $\mathbb{F}_q$. Since the elements in a normal basis are exactly the roots of some N-polynomials, there is a canonical one-to-one correspondence between N-polynomials and normal bases. Normal bases have many applications, including coding theory, cryptography and computer algebra systems. For further details, see [9].

Recently, the k-normal elements over finite fields are defined and characterized by Huczynska et al [8]. For $0 \leq k \leq n-1$, the element $\alpha \in \mathbb{F}_{q^n}$ is called a k-normal element if $deg(gcd(x^n - 1, \sum_{i=0}^{n-1} \alpha^{q^i} x^{n-1-i})) = k$.

By analogy with the case of normal polynomials, a monic irreducible polynomial $P(x) \in \mathbb{F}_q[x]$ of degree n is called a k-normal polynomial (or N_k-polynomial) over $\mathbb{F}_q$ if its roots are k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Here, $P(x)$ has n distinct conjugate roots, of which $(n-k)$ are linearly independent. Recall that an element $\alpha \in \mathbb{F}_{q^n}$ is called a proper element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if $\alpha \notin \mathbb{F}_{q^v}$ for any proper divisor v of n. So, the element $\alpha \in \mathbb{F}_{q^n}$ is a proper k-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if α is a k-normal and proper element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Using the above mention, a normal polynomial (or element) is a 0-normal polynomial (or element). Since the proper k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ are the roots of a k-normal polynomial of degree n over $\mathbb{F}_q$, hence the k-normal polynomials of degree n over $\mathbb{F}_q$ is just another way of describing the proper k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Some results on the constructions of special sequences of k-normal polynomials over $\mathbb{F}_q$, in the cases $k = 0$ and 1 can be found in [2, 4, 5, 10, 11] and [6], respectively.

In this paper, in Sec. 2 some definitions, notes and results which are useful for our study have been stated. Section 3 is devoted to characterization and construction of k-normal elements. Finally, in Sec. 4 a recursive method for constructing k-normal polynomials of higher degree from a given k-normal polynomial is given.

2. Preliminary notes

We use the definitions, notations and results given by Huczynska [8], Gao [7] and Kyuregyan [10, 11], where similar problems are considered. We need the following results for our further study.

The trace of α in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, is given by $Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i}$. For convenience, $Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ is denoted by $Tr_{q^n|q}$.

Let $\mathbb{F}$ be a field and $f(x) = \Sigma_{i=0}^{n} f_i x^i$ and $g(x) = \Sigma_{j=0}^{m} g_j x^j$ with all $f_i, g_j \in \mathbb{F}$. The Sylvester matrix $S_{f,g}$ is the $(m+n) \times (m+n)$ matrix given by:

$$S_{f,g} = \begin{pmatrix} f_n & f_{n-1} & \dots & f_1 & f_0 & \dots & \dots \\ 0 & f_n & \dots & \dots & \dots & f_0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & f_n & \dots & \dots & \dots & f_0 \\ g_m & g_{m-1} & \dots & g_1 & g_0 & \dots & \dots \\ 0 & g_m & g_{m-1} & \dots & \dots & g_0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & g_m & \dots & \dots & \dots & g_0 \end{pmatrix} \tag{1}$$

Proposition 2.1 ([8]). *Let $\mathbb{F}$ be a field. For two non-zero polynomials $f, g \in \mathbb{F}[x]$, we have*

$$rank(S_{f,g}) = deg(f) + deg(g) - deg(gcd(f, g)).$$

Proposition 2.2 ([8]). *Let $\alpha \in \mathbb{F}_{q^n}$. Then the following properties are equivalent:*

i) α is k-normal over $\mathbb{F}_q$;

ii) α gives rise to a basis $\{\alpha, \alpha^q, ..., \alpha^{q^{n-k-1}}\}$ of a q-modules of degree $n-k$ over $\mathbb{F}_q$;

iii) $rank(A_\alpha) = n - k$, where

$$A_\alpha = \begin{pmatrix} \alpha & \alpha^q & \dots & \alpha^{q^{n-1}} \\ \alpha^q & \alpha^{q^2} & \dots & \alpha \\ \vdots & \vdots & \vdots & \vdots \\ \alpha^{q^{n-1}} & \alpha & \dots & \alpha^{q^{n-2}} \end{pmatrix}.$$

Proposition 2.3 ([6]). *Let p divide n, then $n = n_1 p^e$, for some $e \geq 1$ and $a, b \in \mathbb{F}_q^*$. Theefore the element α is a proper k-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $a + b\alpha$ is a proper k-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

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 $\mathbb{F}_q[x]$:

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

where $\varphi_i(x) \in \mathbb{F}_q[x]$ are the distinct irreducible factors of $x^n - 1$. For each s, $0 \leq s < n$, let there is a $u_s > 0$ such that $R_{s,1}(x)$, $R_{s,2}(x)$, $\cdots$, $R_{s,u_s}(x)$ are all of the s degree polynomials dividing $x^n - 1$. So, from (2) we can write $R_{s,i}(x) = \prod_{j=1}^{r} \varphi_j{}^{t_{ij}}(x)$, for each $1 \leq i \leq u_s$, $0 \leq t_{ij} \leq t$. Let

$$\phi_{s,i}(x) = \frac{x^n - 1}{R_{s,i}(x)}, \tag{3}$$

for $1 \leq i \leq u_s$. Then, there is a useful characterization of the k-normal polynomials of degree n over $\mathbb{F}_q$ as follows:

Proposition 2.4 ([6]). *Let $F(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_q$ and α be a root of it. Let $x^n - 1$ factor as (2) and let $\phi_{s,i}(x)$ be as in (3). Then $F(x)$ is a N_k-polynomial over $\mathbb{F}_q$ if and only if, there is j, $1 \leq j \leq u_k$, such that*

$$L_{\phi_{k,j}}(\alpha) = 0,$$

and also

$$L_{\phi_{s,i}}(\alpha) \neq 0,$$

for each s, $k < s < n$, and $1 \leq i \leq u_s$, where u_s is the number of all s degree polynomials dividing $x^n - 1$ and $L_{\phi_{s,i}}(x)$ is the linearized polynomial defined by

$$L_{\phi_{s,i}}(x) = \sum_{v=0}^{n-s} t_{iv} x^{q^v} \ if \ \phi_{s,i}(x) = \sum_{v=0}^{n-s} t_{iv} x^v.$$

The following propositions and lemma are useful for constructing N_k-polynomials over $\mathbb{F}_q$.

Proposition 2.5 ([3]). *Let $x^p - \delta_2 x + \delta_0$ and $x^p - \delta_2 x + \delta_1$ be relatively prime polynomials in $\mathbb{F}_q[x]$ and $P(x) = \sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial of degree $n \geq 2$ over $\mathbb{F}_q$, and let $\delta_0, \delta_1 \in \mathbb{F}_q$, $\delta_2 \in \mathbb{F}_q^*$, $(\delta_0, \delta_1) \neq (0,0)$. Then*

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

is an irreducible polynomial of degree np over $\mathbb{F}_q$ if and only if $\delta_2^{\frac{q-1}{p-1}} = 1$ and

$$Tr_{q|p}\left(\frac{1}{A^p}\left((\delta_1 - \delta_0)\frac{P'(1)}{P(1)} - n\delta_1\right)\right) \neq 0,$$

where $A^{p-1} = \delta_2$, for some $A \in \mathbb{F}_q^*$.

Proposition 2.6 ([1]). *Let $x^p - x + \delta_0$ and $x^p - x + \delta_1$ be relatively prime polynomials in $\mathbb{F}_q[x]$ and let $P(x)$ be an irreducible polynomial of degree $n \geq 2$ over $\mathbb{F}_q$, and $0 \neq \delta_1, \delta_0 \in \mathbb{F}_p$, such that $\delta_0 \neq \delta_1$. Define*

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

$$F_k(x) = (x^p - x + \delta_1)^{t_{k-1}} F_{k-1}\left(\frac{x^p - x + \delta_0}{x^p - x + \delta_1}\right), \qquad k \geq 1$$

where $t_k = np^k$ denotes the degree of $F_k(x)$. Suppose that

$$Tr_{q|p}\left(\frac{(\delta_1 - \delta_0)F_0'(1) - n\delta_1 F_0(1)}{F_0(1)}\right) \cdot Tr_{q|p}\left(\frac{(\delta_1 - \delta_0)F_0'(\frac{\delta_0}{\delta_1}) + n\delta_1 F_0(\frac{\delta_0}{\delta_1})}{F_0(\frac{\delta_0}{\delta_1})}\right) \neq 0.$$

Then $(F_k(x))_{k\geq 0}$ is a sequence of irreducible polynomials over $\mathbb{F}_q$ of degree $t_k = np^k$, for every $k \geq 0$.

Lemma 2.7. *Let γ be a proper element of $\mathbb{F}_{q^n}$ and $\theta \in \mathbb{F}_p^*$, where $q = p^m$, ($m \in \mathbb{N}$). Then we have*

$$\sum_{j=0}^{p-1} \frac{1}{\gamma + j\theta} = -\frac{1}{\gamma^p - \gamma}. \tag{4}$$

Proof. By observing that

$$\sum_{j=0}^{p-1} \frac{1}{\gamma + j\theta} = \frac{1}{\gamma^p - \gamma} \left(\sum_{j=0}^{p-1} \frac{\gamma^p - \gamma}{\gamma + j\theta} \right),$$

it is enough to show that

$$\sum_{j=0}^{p-1} \frac{\gamma^p - \gamma}{\gamma + j\theta} = -1.$$

We note that

$$\begin{aligned} \sum_{j=0}^{p-1} \frac{\gamma^p - \gamma}{\gamma + j\theta} &= \sum_{j=0}^{p-1} \Big((\gamma + j\theta)^{p-1} - 1 \Big) \\ &= \sum_{j=0}^{p-1} (\gamma + j\theta)^{p-1} \\ &= \sum_{j=1}^{p-1} \theta^j \binom{p-1}{j} \left(\sum_{i=1}^{p-1} i^j \right), \end{aligned} \tag{5}$$

where

$$\binom{p-1}{j} = \frac{(p-1)!}{(p-1-j)!j!}, \quad j \in \mathbb{F}_p^*.$$

On the other side, we know that

$$\sum_{i=1}^{p-1} i^j = \begin{cases} 0 \pmod{p}, & \text{if p-1} \nmid j \\ -1 \pmod{p}, & \text{if p-1} \mid j \end{cases} \tag{6}$$

and also $\theta^{p-1} = 1$. Thus by (5) and (6), the proof is completed. □

3. Characterization and construction of k-normal elements

In this section, we extend some existence results on the characterization and construction of normal elements into k-normal elements over finite fields. In the case $k = 0$, the following theorems had been obtained in [7] and [13].

Theorem 3.1. *Suppose that α is a proper element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Let $\alpha_i = \alpha^{q^i}$ and $t_i = Tr_{q^n|q}(\alpha_0\alpha_i)$, $0 \leq i \leq n-1$. Then α is a k-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $deg(gcd(g(x), x^n - 1)) = k$, where $g(x) = \Sigma_{i=0}^{n-1} t_i x^i$.*

Proof. Let

$$A_\alpha = \begin{pmatrix} \alpha & \alpha^q & \dots & \alpha^{q^{n-1}} \\ \alpha^q & \alpha^{q^2} & ... & \alpha \\ \vdots & \vdots & \vdots & \vdots \\ \alpha^{q^{n-1}} & \alpha & \dots & \alpha^{q^{n-2}} \end{pmatrix}.$$

So, by setting

$$\triangle = A_\alpha {A_\alpha}^T = \begin{pmatrix} Tr_{q^n|q}(\alpha_0\alpha_0) & Tr_{q^n|q}(\alpha_0\alpha_1) & \dots & Tr_{q^n|q}(\alpha_0\alpha_{n-1}) \\ Tr_{q^n|q}(\alpha_1\alpha_0) & Tr_{q^n|q}(\alpha_1\alpha_1) & ... & Tr_{q^n|q}(\alpha_1\alpha_{n-1}) \\ \vdots & \vdots & \vdots & \vdots \\ Tr_{q^n|q}(\alpha_{n-1}\alpha_0) & Tr_{q^n|q}(\alpha_0\alpha_0) & \dots & Tr_{q^n|q}(\alpha_{n-1}\alpha_{n-1}) \end{pmatrix}$$

$$= \begin{pmatrix} t_0 & t_1 & \dots & t_{n-1} \\ t_{n-1} & t_0 & ... & t_{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ t_1 & t_2 & \dots & t_0 \end{pmatrix},$$

we get

$$rank(A_\alpha {A_\alpha}^T) = rank(A_\alpha) = rank(\triangle).$$

Now, it is enough to show that $deg(gcd(\Sigma_{i=0}^{n-1} t_i x^i, x^n - 1)) = k$ if and only if the matrix $\triangle$ has rank $n-k$. The Sylvester matrix $S_{f,g}$ (see Equation 1) with $f(x) = x^n - 1$ can be converted, by a sequence of column operations, into the block matrix

$$\begin{pmatrix} I_{n-1} & 0_{n-1} \\ 0_{n-1} & \triangle \end{pmatrix}.$$

From this block decomposition, it follows that

$$rank(S_{f,g}) = rank(\triangle) + rank(I_{n-1}) = rank(\triangle) + (n-1).$$

By Proposition 2.1,

$$rank(S_{f,g}) = n + (n-1) - deg(gcd(f(x), g(x)).$$

Combining these two expressions yields

$$deg(gcd(f(x), g(x)) = n - rank(\triangle).$$

The proof is complete. □

Theorem 3.2. *Let α be a k-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then the element $\gamma = \Sigma_{i=0}^{n-1} a_i \alpha^{q^i}$, where $a_i \in \mathbb{F}_q$, is a k-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if the polynomial $\gamma(x) = \Sigma_{i=1}^{n-1} a_i x^i$ is relatively prime to $x^n - 1$.*

Proof. Since α is a k-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, so by Proposition 2.2, $rank(A_\alpha) = n - k$, where

$$A_\alpha = \begin{pmatrix} \alpha & \alpha^q & \dots & \alpha^{q^{n-1}} \\ \alpha^q & \alpha^{q^2} & \dots & \alpha \\ \vdots & \vdots & \vdots & \vdots \\ \alpha^{q^{n-1}} & \alpha & \dots & \alpha^{q^{n-2}} \end{pmatrix}.$$

Let

$$A_\gamma = \begin{pmatrix} \gamma & \gamma^q & \dots & \gamma^{q^{n-1}} \\ \gamma^q & \gamma^{q^2} & \dots & \gamma \\ \vdots & \vdots & \vdots & \vdots \\ \gamma^{q^{n-1}} & \gamma & \dots & \gamma^{q^{n-2}} \end{pmatrix}.$$

By Proposition 2.2, it is enough to show that $rank(A_\gamma) = n - k$. We note that $A_\gamma = A \cdot A_\alpha$, where

$$A = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_1 & a_2 & \dots & a_0 \\ \vdots & \vdots & \vdots & \vdots \\ a_{n-1} & a_0 & \dots & a_{n-2} \end{pmatrix}.$$

Since $\gamma(x) = \Sigma_{i=0}^{n-1} a_i x^i$ is relatively prime to $x^n - 1$, thus A is non-singular and so

$$rank(A_\gamma) = rank(A \cdot A_\alpha) = rank(A_\alpha) = n - k.$$

The proof is complete. □

Theorem 3.3. *Let t and v are two positive integers with $1 < t < v < 2t$ and α is a k-normal element of $\mathbb{F}_{q^{vt}}$ over $\mathbb{F}_q$ for $v - t \le k \le t - 1$. If $\gamma = Tr_{q^{vt}|q^t}(\alpha)$ is a proper element of $\mathbb{F}_{q^t}$ over $\mathbb{F}_q$, then γ is a proper k-normal element of $\mathbb{F}_{q^t}$ over $\mathbb{F}_q$.*

Proof. Since α is a k-normal element of $\mathbb{F}_{q^{vt}}$ over $\mathbb{F}_q$, so by Proposition 2.2 the elements α, α^q, α^{q^2}, ... , $\alpha^{q^{vt-k-1}}$ form a basis for a q-module of degree $vt - k$ over $\mathbb{F}_q$. By hypothesis and considering $\gamma = Tr_{q^{vt}|q^t}(\alpha)$, the elements γ, γ^q, ... , $\gamma^{q^{v-k-1}}$ are non-overlapping sums of the $vt - k$ conjugates of α, which are assumed to be linearly independent over $\mathbb{F}_q$. So the $v - k$ conjugates of γ are linearly independent over $\mathbb{F}_q$. On the other side, for each $0 \le s \le k - 1$,

$$\begin{aligned} \gamma^{q^{v-k+s}} &= \Sigma_{i=1}^{v} \alpha^{q^{vt-k+(v+s-it)}} \\ &= \Sigma_{i=1}^{vt-k} c_i \alpha^{q^{vt-k-i}}, \quad c_i \in \mathbb{F}_q \\ &= \Sigma_{j=1}^{v-k} d_j \gamma^{q^{v-k-j}}, \quad d_j \in \mathbb{F}_{q^t}. \end{aligned}$$

So γ gives rise to a basis $M = \{\gamma, \gamma^q, ..., \gamma^{q^{v-k-1}}\}$ of a q-modules of degree $v - k$ over $\mathbb{F}_q$. By Proposition 2.2, the proof is complete. □

Theorem 3.4. *Let t and v are two positive integers with $gcd(v,t) = 1$ and α is a k-normal element of $\mathbb{F}_{q^v}$ over $\mathbb{F}_q$, for $0 \leq k \leq v-1$. Then α is also a k-normal element of $\mathbb{F}_{q^{vt}}$ over $\mathbb{F}_{q^t}$.*

Proof. Since α is a k-normal element of $\mathbb{F}_{q^v}$ over $\mathbb{F}_q$, so by Proposition 2.2, $rank(A_\alpha) = v - k$, where

$$A_\alpha = \begin{pmatrix} \alpha & \alpha^q & \dots & \alpha^{q^{v-1}} \\ \alpha^q & \alpha^{q^2} & \dots & \alpha \\ \vdots & \vdots & \vdots & \vdots \\ \alpha^{q^{v-1}} & \alpha & \dots & \alpha^{q^{v-2}} \end{pmatrix}.$$

The element α is also a k-normal element of $\mathbb{F}_{q^{vt}}$ over $\mathbb{F}_{q^t}$ if $rank(A'_\alpha) = v - k$, where

$$A'_\alpha = \begin{pmatrix} \alpha & \alpha^{q^t} & \dots & \alpha^{q^{(v-1)t}} \\ \alpha^{q^t} & \alpha^{q^{2t}} & \dots & \alpha \\ \vdots & \vdots & \vdots & \vdots \\ \alpha^{q^{(v-1)t}} & \alpha & \dots & \alpha^{q^{(v-2)t}} \end{pmatrix}.$$

Since $gcd(v,t) = 1$, when j runs through 0,1,2, ... , $v-1$ *modulo* v, tj also runs through 0,1,2, ... , $v-1$ *modulo* v. Note that since $\alpha \in \mathbb{F}_{q^v}$, we have $\alpha^{q^v} = \alpha$ and thus $\alpha^{q^{jt}} = \alpha^{q^{k_j}}$ whenever $jt \equiv k_j \ (mod\ v)$ and k_j runs through 0,1,2, ... , $v-1$. So $rank(A'_\alpha) = rank(A_\alpha) = v - k$ and the proof is complete. □

4. Recursive construction N_k-polynomials

In this section we establish theorems which will show how propositions 2.4, 2.5 and 2.6 can be applied to produce infinite sequences of N_k-polynomials over $\mathbb{F}_q$. Recall that, the polynomial $P^*(x) = x^n P\left(\frac{1}{x}\right)$ is called the reciprocal polynomial of $P(x)$, where n is the degree of $P(x)$. In the case $k = 0$, some similar results of the following theorems have been obtained in [2], [4] and ([5], Theorems 3.3.1 and 3.4.1). We use of an analogous technique to that used in the above results, where similar problems are considered.

Theorem 4.1. *Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be an N_k-polynomial of degree n over $\mathbb{F}_q$, for each $n = rp^e$, where $e \in \mathbb{N}$ and r equals 1 or is a prime different from p and q a primitive element modulo r. Suppose that $\delta \in \mathbb{F}_q^*$ and*

$$F(x) = (x^p - x + \delta)^n P^*\left(\frac{x^p - x}{x^p - x + \delta}\right). \tag{7}$$

Then $F^*(x)$ is an N_k-polynomial of degree np over $\mathbb{F}_q$ if $k < p^e$ and

$$Tr_{q|p}\left(\delta \frac{P^{*\prime}(1)}{P^*(1)}\right) \neq 0.$$

Proof. Since $P^*(x)$ is an irreducible polynomial over $\mathbb{F}_q$, so Proposition 2.5 and theorem's hypothesis imply that $F(x)$ is irreducible over $\mathbb{F}_q$.
Let $\alpha \in \mathbb{F}_{q^n}$ be a root of $P(x)$. Since $P(x)$ is an N_k-polynomial of degree n over $\mathbb{F}_q$ by theorem's hypothesis, then $\alpha \in \mathbb{F}_{q^n}$ is a proper k-normal element over $\mathbb{F}_q$.

Since q is a primitive modulo r, so in the case $r > 1$ the polynomial $x^{r-1} + \cdots + x + 1$ is irreducible over $\mathbb{F}_q$. Thus $x^n - 1$ has the following factorization in $\mathbb{F}_q[x]$:

$$x^n - 1 = (\varphi_1(x) \cdot \varphi_2(x))^t, \tag{8}$$

where $\varphi_1(x) = x - 1$, $\varphi_2(x) = x^{r-1} + \cdots + x + 1$ and $t = p^e$.

Letting that for each $0 \leq s < n$ and $1 \leq i \leq u_s$, $R_{s,i}(x)$ is the s degree polynomial dividing $x^n - 1$, where u_s is the number of all s degree polynomials dividing $x^n - 1$. So, from (8), we can write $R_{s,i}(x) = (x-1)^{s_{1,i}} \cdot (x^{r-1} + \cdots + x + 1)^{s_{2,i}}$, where $s = s_{1,i} + s_{2,i} \cdot (r-1)$ for each $0 \leq s_{1,i}, s_{2,i} \leq t$, except when $s_{1,i} = s_{2,i} = t$. So, we have

$$\phi_{s,i}(x) = \frac{x^n - 1}{R_{s,i}(x)} = \frac{x^n - 1}{(x-1)^{s_{1,i}} \cdot (x^{r-1} + \cdots + x + 1)^{s_{2,i}}} = \sum_{v=0}^{n-s} t_{s,i,v} x^v. \tag{9}$$

Since $P(x)$ is an N_k-polynomial of degree n over $\mathbb{F}_q$, so by Proposition 2.4, there is a j, $1 \leq j \leq u_k$, such that

$$L_{\phi_{k,j}}(\alpha) = 0,$$

and also

$$L_{\phi_{s,i}}(\alpha) \neq 0,$$

for each $k < s < n$ and $1 \leq i \leq u_s$. Further, we proceed by proving that $F^*(x)$ is a k-normal polynomial. Let α_1 be a root of $F(x)$. Then $\beta_1 = \frac{1}{\alpha_1}$ is a root of its reciprocal polynomial $F^*(x)$. Note that by (8), the polynomial $x^{np} - 1$ has the following factorization in $\mathbb{F}_q[x]$:

$$x^{np} - 1 = (\varphi_1(x) \cdot \varphi_2(x))^{pt}, \tag{10}$$

where $\varphi_1(x) = x - 1$, $\varphi_2(x) = x^{r-1} + \cdots + x + 1$ and $t = p^e$.

Letting that for each $0 \leq s' < np$ and $1 \leq i' \leq u'_{s'}$, $R'_{s',i'}(x)$ is the s' degree polynomial dividing $x^{np} - 1$, where $u'_{s'}$ is the number of all s' degree polynomials dividing $x^{np} - 1$. So, from (10) we can write $R'_{s',i'}(x) = (x-1)^{s'_{1,i'}} \cdot (x^{r-1} + \cdots + x + 1)^{s'_{2,i'}}$, where $s' = s'_{1,i'} + s'_{2,i'} \cdot (r-1)$ for each $0 \leq s'_{1,i'}, s'_{2,i'} \leq pt$, except when $s'_{1,i'} = s'_{2,i'} = pt$. Therefore by considering

$$H'_{s',i'}(x) = \frac{x^{np} - 1}{R'_{s',i'}(x)}, \tag{11}$$

and Proposition 2.4, $F^*(x)$ is an N_k-polynomial of degree np over $\mathbb{F}_q$ if and only if there is a j', $1 \leq j' \leq u'_k$, such that

$$L_{H'_{k,j'}}(\beta_1) = 0,$$

and also

$$L_{H'_{s',i'}}(\beta_1) \neq 0,$$

for each $k < s' < np$ and $1 \leq i' \leq u'_{s'}$. Consider

$$H_{s,i}(x) = \frac{x^{np}-1}{R_{s,i}(x)} = \frac{x^n-1}{R_{s,i}(x)}\left(\sum_{j=0}^{p-1} x^{jn}\right), \tag{12}$$

for each $0 \leq s < n$ and $1 \leq i \leq u_s$. By (9) we obtain

$$H_{s,i}(x) = \phi_{s,i}(x)\left(\sum_{j=0}^{p-1} x^{jn}\right) = \sum_{v=0}^{n-s} t_{s,i,v}\left(\sum_{j=0}^{p-1} x^{jn+v}\right).$$

It follows that

$$L_{H_{s,i}}(\beta_1) = \sum_{v=0}^{n-s} t_{s,i,v}\left(\sum_{j=0}^{p-1} (\beta_1)^{p^{jmn}}\right)^{p^{mv}},$$

or

$$L_{H_{s,i}}(\beta_1) = L_{H_{s,i}}\left(\frac{1}{\alpha_1}\right) = \sum_{v=0}^{n-s} t_{s,i,v}\left(\sum_{j=0}^{p-1} \left(\frac{1}{\alpha_1}\right)^{p^{jmn}}\right)^{p^{mv}}. \tag{13}$$

From (7), if α_1 is a zero of $F(x)$, then $\frac{\alpha_1{}^p-\alpha_1+\delta}{\alpha_1{}^p-\alpha_1}$ is a zero of $P(x)$, and therefore it may assume that

$$\alpha = \frac{\alpha_1{}^p - \alpha_1 + \delta}{\alpha_1{}^p - \alpha_1},$$

or

$$\frac{\alpha - 1}{\delta} = (\alpha_1{}^p - \alpha_1)^{-1}. \tag{14}$$

Now, by (14) and observing that $P(x)$ is an irreducible polynomial of degree n over $\mathbb{F}_q$, we obtain

$$\frac{\alpha-1}{\delta} = \left(\frac{\alpha-1}{\delta}\right)^{p^{mn}} = \left(\alpha_1{}^{p^{mn+1}} - \alpha_1{}^{p^{mn}}\right)^{-1}. \tag{15}$$

It follows from (14) and (15) that

$$\left(\alpha_1{}^{p^{mn+1}} - \alpha_1{}^{p^{mn}}\right)^{-1} = (\alpha_1{}^p - \alpha_1)^{-1}. \tag{16}$$

Also observing that $F(x)$ is an irreducible polynomial of degree np over $\mathbb{F}_q$, we have $({\alpha_1}^p - \alpha_1) \neq 0$ and $({\alpha_1}^{p^{mn+1}} - {\alpha_1}^{p^{mn}}) \neq 0$. Hence by (16)

$$({\alpha_1}^{p^{mn}} - \alpha_1)^p = ({\alpha_1}^{p^{mn}} - \alpha_1). \tag{17}$$

It follows from (17) that ${\alpha_1}^{p^{mn}} - \alpha_1 = \theta \in \mathbb{F}_p^*$. Hence ${\alpha_1}^{p^{mn}} = \alpha_1 + \theta$ and

$$ {\alpha_1}^{p^{2mn}} = (\alpha_1 + \theta)^{p^{mn}} = {\alpha_1}^{p^{mn}} + \theta^{p^{mn}} = \alpha_1 + \theta + \theta = \alpha_1 + 2\theta. $$

It is easy to show that ${\alpha_1}^{p^{jmn}} = \alpha_1 + j\theta$, for $1 \leq j \leq p-1$, or

$$\left(\frac{1}{\alpha_1}\right)^{p^{jmn}} = \frac{1}{\alpha_1 + j\theta}, \quad for \;\; 1 \leq j \leq p-1. \tag{18}$$

From (13) and (18), we immediately obtain

$$L_{H_{s,i}}(\beta_1) = \sum_{v=0}^{n-s} t_{s,i,v} \left(\sum_{j=0}^{p-1} \frac{1}{\alpha_1 + j\theta} \right)^{p^{mv}}. \tag{19}$$

Thus, by (14), (19) and Lemma 2.7 we have

$$\begin{aligned} L_{H_{s,i}}(\beta_1) &= \sum_{v=0}^{n-s} t_{s,i,v} \left(-\frac{1}{\alpha_1^p - \alpha_1} \right)^{p^{mv}} \\ &= \frac{1}{\delta} \sum_{v=0}^{n-s} t_{s,i,v} (1-\alpha)^{p^{mv}} = L_{\phi_{s,i}} \left(\frac{1-\alpha}{\delta} \right). \end{aligned} \tag{20}$$

Since α is a zero of $P(x)$, then α will be a k-normal element in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Thus according to Proposition 2.3, the element $\frac{1-\alpha}{\delta}$ will also be a k-normal element. since $\frac{1-\alpha}{\delta}$ is a root of $P(-\delta x + 1)$, so by (20) and Proposition 2.4, there is a j, $1 \leq j \leq u_k$, such that $L_{H_{k,j}}(\beta_1) = 0$, and also $L_{H_{s,i}}(\beta_1) \neq 0$, for each s, $k < s < n$ and $1 \leq i \leq u_s$. So, there is a j', $1 \leq j' \leq u'_k$, such that, $L_{H'_{k,j'}}(\beta_1) = L_{H_{k,j}}(\beta_1) = 0$. On the other side, by (11) and (12), for each s', $k < s' < np$ and $1 \leq i' \leq u'_{s'}$, there is s, $k < s < n$ and $1 \leq i \leq u_s$ such that $H'_{s',i'}(x)$ divide $H_{s,i}(x)$. It follows that $L_{H'_{s',i'}}(\beta_1) \neq 0$, for each s', $k < s' < np$ and $1 \leq i' \leq u'_{s'}$. The proof is completed. $\square$

In the following theorem, a computationally simple and explicit recurrent method for constructing higher degree N_k-polynomials over $\mathbb{F}_q$ starting from an N_k-polynomial is described.

Theorem 4.2. *Let $P(x)$ be an N_k-polynomial of degree n over $\mathbb{F}_q$, for each $n = rp^e$, where $e \in \mathbb{N}$ and r equals 1 or is a prime different from p and q a primitive element modulo r. Define*

$$F_0(x) = P^*(x)$$

$$F_u(x) = (x^p - x + \delta)^{np^{u-1}} F_{u-1}\left(\frac{x^p - x}{x^p - x + \delta}\right), \tag{21}$$

where $\delta \in \mathbb{F}_p^*$. Then $(F_u^*(x))_{u\geq 0}$ is a sequence of N_k-polynomials of degree np^u over $\mathbb{F}_q$ if $k < p^e$ and

$$Tr_{q|p}\left(\frac{{P^*}'(0)}{P^*(0)}\right) \cdot Tr_{q|p}\left(\frac{{P^*}'(1)}{P^*(1)}\right) \neq 0,$$

where ${P^*}'(0)$ and ${P^*}'(1)$ are the formal derivative of $P^*(x)$ at the points $x = 0$ and $x = 1$, respectively.

Proof. By Proposition 2.6 and hypotheses of theorem for each $u \geq 1$, $F_u(x)$ is an irreducible polynomial over $\mathbb{F}_q$. Consequently, $(F_u^*(x))_{u\geq 0}$ is a sequence of irreducible polynomials over $\mathbb{F}_q$. The proof of k-normality of the irreducible polynomials $F_u^*(x)$, for each $u \geq 1$ is implemented by mathematical induction on u. In the case $u = 1$, by Theorem 4.1 ${F_1}^*(x)$ is a k-normal polynomial.

For $u = 2$ we show that ${F_2}^*(x)$ is also a k-normal polynomial. To this end we need to show that the hypothesis of Theorem 4.1 are satisfied. By Theorem 4.1, ${F_2}^*(x)$ is a k-normal polynomial if

$$Tr_{q|p}\left(\frac{F_1'(1)}{F_1(1)}\right) \neq 0,$$

since $\delta \in \mathbb{F}_p^*$. We apply (21) to compute

$$F_u(0) = F_u(1) = \delta^{un} P^*(0), \quad u = 1, 2, \ldots. \tag{22}$$

We calculate the formal derivative of $F_1'(x)$ at the points $x = 0$ and $x = 1$. According to (21) the first derivative of $F_1(x)$ is

$$\begin{aligned}
{F_1}'(x) &= -n(x^p - x + \delta)^{n-1} {F_0}'\left(\frac{x^p - x}{x^p - x + \delta}\right) \\
&\quad + (x^p - x + \delta)^n \cdot \left(\frac{(px^{p-1} - 1)(x^p - x + \delta) - (px^{p-1} - 1)(x^p - x)}{(x^p - x + \delta)^2}\right) \\
&\quad \cdot {F_0}'\left(\frac{x^p - x}{x^p - x + \delta}\right) \\
&= -\delta(x^p - x + \delta)^{n-2} \cdot {P^*}'\left(\frac{x^p - x}{x^p - x + \delta}\right),
\end{aligned}$$

and at the points $x = 0$ and $x = 1$

$${F_1}'(0) = -{F_1}'(1) = -\delta^{n-1} {P^*}'(0) \tag{23}$$

which is not equal to zero by the condition $Tr_{q|p}\left(\frac{{P^*}'(0)}{P^*(0)}\right) \neq 0$ in the hypothesis of theorem, since $\delta \in \mathbb{F}_p^*$. From (23) and (22)

$$Tr_{q|p}\left(\frac{F_1'(1)}{F_1(1)}\right) = Tr_{q|p}\left(\frac{-\delta^{n-1}{P^*}'(0)}{\delta^n P^*(0)}\right) = -\frac{1}{\delta} Tr_{q|p}\left(\frac{{P^*}'(0)}{P^*(0)}\right), \tag{24}$$

which is not equal to zero by hypothesis of theorem. Hence the polynomial $F_2^*(x)$ is a k-normal polynomial. If induction holds for $u-1$, then it must hold also for u, that is by assuming that $F_{u-1}^*(x)$ is a k-normal polynomial, we show that $F_u^*(x)$ is also a k-normal polynomial.
Let $u \geq 3$. By Theorem 4.1, $F_u^*(x)$ is a k-normal polynomial if

$$Tr_{q|p}\left(\frac{F'_{u-1}(1)}{F_{u-1}(1)}\right) \neq 0,$$

since $\delta \in \mathbb{F}_p^*$. We calculate the formal derivative of $F'_{u-1}(x)$ at the points 1 and 0. By (21) the first derivative of $F_{u-1}(x)$ is

$$\begin{aligned} F'_{u-1}(x) &= (x^p - x + \delta)^{np^{u-2}} \left(\frac{(px^{p-1}-1)(x^p - x + \delta) - (px^{p-1}-1)(x^p - x)}{(x^p - x + \delta)^2}\right) \\ &\cdot F'_{u-2}\left(\frac{x^p - x}{x^p - x + \delta}\right) \\ &= -\delta(x^p - x + \delta)^{np^{u-2}-2} F'_{u-2}\left(\frac{x^p - x}{x^p - x + \delta}\right), \end{aligned}$$

and at the point $x = 0$ and $x = 1$

$$F'_{u-1}(0) = F'_{u-1}(1) = -\delta^{np^{u-2}-1} F'_{u-2}(0) = -\delta^{n-1} F'_{u-2}(0).$$

So we have

$$F'_{u-1}(0) = F'_{u-1}(1) = (-1)^{u-2} \delta^{(n-1)(u-2)} F'_1(0),$$

which is not equal to zero by (23) and the condition $Tr_{q|p}\left(\frac{{P^*}'(0)}{P^*(0)}\right) \neq 0$ in the hypothesis of theorem, since $\delta \in \mathbb{F}_p^*$. Also

$$Tr_{q|p}\left(\frac{F'_{u-1}(1)}{F_{u-1}(1)}\right) = (-1)^{u-2} \frac{1}{\delta^{(u-2)}} Tr_{q|p}\left(\frac{F'_1(1)}{F_1(1)}\right),$$

which is not equal to zero by (24) and hypothesis of theorem. The theorem is proved. $\square$

References

[1] S. Abrahamyan, M. K. Kyureghyan, *A recurrent method for constructing irreducible polynomials over finite fields,* Proceeding of the 13th international conference on computer algebra in scientific computing, 2011, 1-9.

[2] S. Abrahamyan, M. K. Kyureghyan, *New recursive construction of normal polynomials over finite fields,* Proceeding of the 11th international conference on finite fields and their applications, 2013, 1-10.

[3] S. Abrahamyan, M. Alizadeh, M. K. Kyureghyan, *Recursive constructions of irreducible polynomials over finite fields*, Finite Fields Appl., 18 (2012), 738-745.

[4] M. Alizadeh, S. Abrahamyan, S. Mehrabi, M. K. Kyuregyan, *Constructing of N-polynomials over finite fields,* International Journal of Algebra, (5) 29, (2011), 1437-1442.

[5] M. Alizadeh, *Construction of Irreducible and Normal Polynomials over Finite Fields*, Ph.D. Thesis, National Academy of Sciences of Armenia, Yerevan, 2013.

[6] M. Alizadeh, *Some notes on the k-normal elements and k-normal polynomials over finite fields,* Journal of Algebra and Its Applications, Vol. 16, No. 1, 1750006, (11 pages), 2017.

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

[8] S. Huczynska, G. L. Mullen, D. Panario and D. Thomson, *Existence and properties of k-normal elements over finite fields,* Finite Fields Appl., 24 (2013), 170-183.

[9] D. Jungnickel, *Finite Fields: Structure and Arithmetics*, Wissenschaftsverlag, (Mannheim), 1993.

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

[11] M. K. Kyuregyan, *Recursive construction of N-polynomials over $GF(2^s)$,* Discrete Applied Mathematics, 156 (2008), 1554-1559.

[12] H. W. Lenstra and R. Schoof, *Primitive normal bases for finite fields*, Mathematics of Computation, 48 (1987), 217-231.

[13] S. Perlis, *Normal bases of cyclic fields of prime-power degree,* Duke Math. J., 9 (1942), 507-517.

[14] S. Schwartz, *Irreducible polynomials over finite fields with linearly independent roots*, Math. Slovaca, 38 (1988), 147-158.

Accepted: 5.09.2017