Chin. Ann. Math. Ser. B
41(5), 2020, 665–678
DOI: 10.1007/s11401-020-0226-5

Chinese Annals of Mathematics, Series B

A New Criterion on k-Normal Elements over Finite Fields*

Aixian ZHANG[1] Keqin FENG[2]

Abstract The notion of normal elements for finite fields extension was generalized as k-normal elements by Huczynska et al. (2013). Several methods to construct k-normal elements were presented by Alizadah et al. (2016) and Huczynska et al. (2013), and the criteria on k-normal elements were given by Alizadah et al. (2016) and Antonio et al. (2018). In the paper by Huczynska, S., Mullen, G., Panario, D. and Thomson, D. (2013), the number of k-normal elements for a fixed finite field extension was calculated and estimated. In this paper the authors present a new criterion on k-normal elements by using idempotents and show some examples. Such criterion was given for usual normal elements before by Zhang et al. (2015).

Keywords Normal basis, Finite field, Idempotent, Linearized polynomial, Gauss period
2000 MR Subject Classification 11T71, 13M06, 97H40

1 Introduction

Let $q = p^m$, where p is a prime number, $m \geq 1$, $\mathbb{F}_q$ a finite field with q elements, $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$. For $n \geq 1$ and $Q = q^n, \alpha \in \mathbb{F}_Q^*$ is called a normal element for extension $\mathbb{F}_Q/\mathbb{F}_q$ if $\mathrm{N} = \{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}\}$ is a basis of $\mathbb{F}_Q$ over $\mathbb{F}_q$ (N is called a normal basis for $\mathbb{F}_Q/\mathbb{F}_q$). For a normal element α of $\mathbb{F}_Q/\mathbb{F}_q$, the minimal polynomial $f_\alpha(x) \in \mathbb{F}_q[x]$ of α is called a normal polynomial for $\mathbb{F}_Q/\mathbb{F}_q$, which is a monic irreducible polynomial in $\mathbb{F}_q[x]$ with degree n. Normal bases have many applications including coding theory, cryptography and communication theory due to the efficiency of exponentiation (see [5–6]). It is proved that $\alpha \in \mathbb{F}_Q^*$ is a normal element for $\mathbb{F}_Q/\mathbb{F}_q$ if and only if

$$\gcd(g_\alpha(x), x^n - 1) = 1, \quad g_\alpha(x) = \sum_{i=0}^{n-1} \alpha^{q^i} x^{n-i-1} \tag{1.1}$$

(see [5, Theorem 2.39]).

The following definition given by Huczynska et al. [3] is a generalization of normal elements.

Definition 1.1 (see [3]) *Let $q = p^m, Q = q^n$ and $0 \leq k \leq n-1$. An element $\alpha \in \mathbb{F}_Q^*$ is called a k-normal element for $\mathbb{F}_Q/\mathbb{F}_q$ if the degree of $\gcd(g_\alpha(x), x^n - 1)$ is k.*

Manuscript received September 25, 2018.
[1]Department of Mathematical Sciences, Xi'an University of Technology, Xi'an 710054, China.
E-mail: zhangaixian1008@126.com
[2]Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China.
E-mail: kfeng@math.tsinghua.edu.cn
*This work was supported by the National Natural Science Foundation of China (No. 11571107) and the Natural Science Basic Research Plan of Shaanxi Province of China (No. 2019JQ-333).

With this terminology, a normal element is just 0-normal. As shown in the normal element case (see [6]), the k-normal elements can be used to reduce the multiplication process in finite fields. And another motivation for studying k-normal elements is due to the observation that they implicitly arise during the process of constructing quasi-normal bases of finite fields (see [7]).

The number of k-normal elements for extension $\mathbb{F}_Q/\mathbb{F}_q$ was calculated and estimated in [3] and several methods to construct k-normal elements were presented in [1–2]. As the normal element case, the k-normal elements can be characterized by using q-linearlized polynomial theory (see [2–3]). Now we briefly introduce such characterization.

A q-linearlized polynomial (q-polynomial in brief) is a polynomial in the following form:

$$L(x) = a_0x + a_1x^q + \cdots + a_mx^{q^m}, \quad a_i \in \mathbb{F}_q.$$

Let $\mathcal{F}_q[x]$ be the set of all q-polynomials. Then $\mathcal{F}_q[x]$ is a ring with respect to the ordinary addition and the following multiplication $\otimes$:

$$L(x) \otimes K(x) = L(K(x)), \quad \text{composition.}$$

One of the basic facts on $\mathcal{F}_q[x]$ is that the mapping

$$\varphi : \mathbb{F}_q[x] \longrightarrow \mathcal{F}_q[x], \quad \sum_{i=0}^{m} a_ix^i \mapsto \sum_{i=0}^{m} a_ix^{q^i}, \quad a_i \in \mathbb{F}_q \tag{1.2}$$

is an isomorphism of rings. Therefore $\mathcal{F}_q[x]$ is a principal ideal domain with identity x. We use the notation $\parallel$ to express the divisibility in $\mathcal{F}_q[x]$. Namely, for $L(x)$ and $M(x)$ in $\mathcal{F}_q[x]$, $L(x) \parallel M(x)$ means that $L(x) \neq 0$ and there exists $N(x) \in \mathcal{F}_q[x]$ such that $M(x) = L(x) \otimes N(x) = N(x) \otimes L(x)$.

Let $n \geq 1$ and $\alpha \in \mathbb{F}_Q^*$. The set

$$I_\alpha = \{M(x) \in \mathcal{F}_q[x] : M(\alpha) = 0\}$$

is a nonzero ideal of $\mathcal{F}_q[x]$ because $x^{q^n} - x \in I_\alpha$. The monic generator $M_\alpha(x)$ of the ideal I_α is called the minimal q-polynomial of α. Particularly, $M_\alpha(x)$ is an irreducible polynomial in $\mathcal{F}_q[x]$ and $M_\alpha(x) \parallel x^{q^n} - x$. Moreover for any $L(x) \in \mathcal{F}_q[x]$, $L(\alpha) = 0$ if and only if $M_\alpha(x) \parallel L(x)$.

Lemma 1.1 (see [3, Theorem 3.2]) *Let $q = p^m$, $Q = q^n$ and $0 \leq k \leq n-1$. The following statements for $\alpha \in \mathbb{F}_Q^*$ are equivalent to each other*:

(I) *α is a k-normal element for $\mathbb{F}_Q/\mathbb{F}_q$;*

(II) *The degree of the minimal q-polynomial $M_\alpha(x) \in \mathcal{F}_q[x]$ over $\mathbb{F}_q$ is q^{n-k};*

(III) *The dimension of the $\mathbb{F}_q$-vector subspace V_α of $\mathbb{F}_Q$ spanned by $\{\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}\}$ is $n-k$ and $\{\alpha, \alpha^q, \cdots, \alpha^{q^{n-k-1}}\}$ is an $\mathbb{F}_q$-basis of V_α.*

Let $n = p^tn'$, $p \nmid n'$. Then $x^n - 1$ is decomposed in $\mathbb{F}_q[x]$ as

$$x^n - 1 = (x^{n'} - 1)^{p^t} = (p_1(x)p_2(x)\cdots p_s(x))^{p^t}, \tag{1.3}$$

where $p_i(x)$ $(1 \leq i \leq s)$ are distinct monic irreducible polynomials in $\mathbb{F}_q[x]$. By the isomorphism φ in (1.2), $x^{q^n} - x$ has the following corresponding decomposition in $\mathcal{F}_q[x]$:

$$x^{q^n} - x = (P_1(x) \otimes P_2(x) \otimes \cdots \otimes P_s(x))^{p^t},$$

where $P_i(x) = \varphi(p_i(x))$ $(1 \le i \le s)$ are distinct monic irreducible q-polynomials in $\mathcal{F}_q[x]$ and for $L(x) \in \mathcal{F}_q[x]$ and $l \ge 1, L(x)^l$ means $L(x) \otimes L(x) \otimes \cdots \otimes L(x)$ (l copies).

For $\alpha \in \mathbb{F}_Q^*$, the minimal q-polynomial $M_\alpha(x)$ is a divisor of $x^{q^n} - x$ in $\mathcal{F}_q[x]$. Therefore $M_\alpha(x) = \varphi(m_\alpha(x))$ for a divisor $m_\alpha(x)$ of $x^n - 1$ in $\mathbb{F}_q[x]$. From the definition of $M_\alpha(x)$ and the isomorphism φ between $\mathbb{F}_q[x]$ and $\mathcal{F}_q[x]$ we get the following result.

Lemma 1.2 *Let x^n-1 be decomposed by formula* (1.3) *in $\mathbb{F}_q[x]$, and $m(x)$ is a monic divisor of $x^n - 1$ in $\mathbb{F}_q[x]$. Let $M(x) = \varphi(m(x))$ and $M_i(x) = \varphi(\frac{m(x)}{p_i(x)})$ if $p_i(x) \mid m(x)$. Then $M(x)$ is the minimal q-polynomial of α if and only if $M(\alpha) = 0$ and for each $p_i(x) \mid m(x)$, $M_i(\alpha) \ne 0$.*

Particularly, if $\gcd(n, p) = 1$, then the decomposition (1.3) becomes

$$x^n - 1 = p_1(x)p_2(x)\cdots p_s(x). \tag{1.4}$$

For $\alpha \in \mathbb{F}_Q^*$, the minimal q-polynomial $M_\alpha(x)$ has the form

$$M_\alpha(x) = M_\Delta(x) = \bigotimes_{i\in\Delta} P_i(x),$$

where Δ is a subset of $\{1, 2, \cdots, s\}$. In this case, $M_\alpha(x)$ can be described by the following way.

Lemma 1.3 *Suppose that $Q = q^n, (n, q) = 1$ and $x^n - 1$ has decomposition formula* (1.4) *where $p_i(x)$ $(1 \le i \le s)$ are distinct monic irreducible polynomials in $\mathbb{F}_q[x]$. Let*

$$m_i(x) = \frac{x^n - 1}{p_i(x)}, \quad M_i(x) = \varphi(m_i(x)), \quad 1 \le i \le s.$$

For $\alpha \in \mathbb{F}_Q^*$, let

$$\Delta = \Delta(\alpha) = \{i : 1 \le i \le s,\ M_i(\alpha) \ne 0\}.$$

Then the minimal q-polynomial $M_\alpha(x)$ of α is $M_\Delta(x) = \bigotimes\limits_{i\in\Delta} P_i(x)$ and α is a k-normal element for $\mathbb{F}_Q/\mathbb{F}_q$ where $k = n - \sum\limits_{i\in\Delta} \deg p_i(x)$.

Proof For each i, $1 \le i \le s$,

$$\begin{aligned} P_i(x) \| M_\alpha(x) &\iff M_\alpha(x) \nmid \frac{x^{q^n} - x}{P_i(x)} = M_i(x) \in \mathcal{F}_q[x] \ \left(\text{since } x^{q^n} - x = \bigotimes_{i=1}^{s} P_i(x)\right) \\ &\iff M_i(\alpha) \ne 0 \iff i \in \Delta. \end{aligned}$$

Therefore $M_\alpha(x) = \prod\limits_{i\in\Delta} P_i(x)$. Since $\deg M_\alpha(x) = \prod\limits_{i\in\Delta} \deg P_i(x) = q^{\sum\limits_{i\in\Delta} \deg p_i(x)}$, by Lemma 1.1 we know that α is a k-normal element for extension $\mathbb{F}_Q/\mathbb{F}_q$ where $k = n - \sum\limits_{i\in\Delta} \deg p_i(x) = \sum\limits_{\substack{i=1 \\ i\notin\Delta}}^{s} \deg p_i(x)$.

Lemma 1.3 presents a method to determine the normality k and the minimal q-polynomial of an element $\alpha \in \mathbb{F}_Q^*$ provided we know the decomposition formula (1.4) in the case $\gcd(n, q) = 1$. In this paper we present a new method to determine the normality and the minimal q-polynomial $M_\alpha(x)$ of $\alpha \in \mathbb{F}_Q^*$, essentially by the partition of $\mathrm{Z}_n = \mathbb{Z}/n\mathbb{Z}$ into q-classes without using the explicit form of the irreducible factors $p_i(x)$ $(1 \le i \le s)$ of $x^n - 1$. We explain this idempotent method in Section 2 and show several examples in Section 3.

2 Main Result

Let $q = p^m,\ Q = q^n$ and $\gcd(n, p) = 1$. A criterion on normal element for extension $\mathbb{F}_Q/\mathbb{F}_q$ was given in [6] by using idempotents in semisimple $\mathbb{F}_q$-algebra $A = \mathbb{F}_q[x]/(x^n - 1)$. In this section we generalize this method to determine the normality k and $M_\alpha(x)$ of any $\alpha \in \mathbb{F}_Q^*$.

By assumption $\gcd(n, p) = 1,\ x^n - 1$ has the decomposition (1.4) in $\mathbb{F}_q[x]$:

$$x^n - 1 = p_i(x)p_2(x)\cdots p_s(x),$$

where $p_i(x)\ (1 \le i \le s)$ are distinct monic irreducible polynomials in $\mathbb{F}_q[x]$. Let

$$n_i = \deg p_i(x), \quad l_i(x) = \frac{x^n - 1}{p_i(x)}, \quad L_i(x) = \varphi(l_i(x)), \quad 1 \le i \le s.$$

Then $n_1 + n_2 + \cdots + n_s = n,\ \deg L_i(x) = q^{n_i}\ (1 \le i \le s)$. By the Chinese Remainder Theorem, $A = \mathbb{F}_q[x]/(x^n - 1)$ is a direct sum of finite fields:

$$A \cong \bigoplus_{i=1}^{s} \frac{\mathbb{F}_q[x]}{(p_i(x))} \cong \bigoplus_{i=1}^{s} \mathbb{F}_{Q_i}, \quad Q_i = q^{n_i}.$$

It is well known that zeros and degree of $P_i(x)$ can be described by q-classes of $\mathrm{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

Definition 2.1 *Let $n \ge 2,\ q = p^m$ and $\gcd(n, p) = 1$. Two elements a and b in $\mathrm{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \cdots, n-1\}$ are called q-equivalent if there exists a positive $i \in \mathbb{Z}$ such that $a \equiv bq^i \pmod n$.*

This is an equivalent relation on Z_n and Z_n is partitioned into q-equivalent classes.

$$\begin{aligned}
&\mathcal{A}_1 = \{a_1 = 0\}, \quad |\mathcal{A}_1| = n_1 = 1,\\
&\mathcal{A}_2 = \{a_2, a_2q, \cdots, a_2q^{n_2-1}\}, \quad |\mathcal{A}_2| = n_2,\\
&\quad\ \vdots\\
&\mathcal{A}_s = \{a_s, a_sq, \cdots, a_sq^{n_s-1}\}, \quad |\mathcal{A}_s| = n_s,
\end{aligned}$$

where for $1 \le i \le s,\ n_i$ is the least positive integer such that $a_iq^{n_i} \equiv a_i \pmod n$.

Let α be a primitive n-th root of 1 in the algebraic closure of $\mathbb{F}_q$. Then for each $i,\ 1 \le i \le s$,

$$\mathcal{S}_i = \{\alpha^\lambda : \lambda \in \mathcal{A}_i\} = \{\alpha^{a_i}, \alpha^{a_iq}, \cdots, \alpha^{a_iq^{n_i-1}}\}$$

is the set of zeros of a monic irreducible polynomial $p_i(x)$ in $\mathbb{F}_q[x]$ with degree n_i. And $x^n - 1$ is decomposed in $\mathbb{F}_q[x]$ as (1.4).

Now we introduce the system of orthogonal (minimal) idempotents in ring

$$A = \mathbb{F}_q[x]/(x^n - 1).$$

Consider the natural isomorphism of rings

$$\begin{aligned}
&\pi : A \longrightarrow \frac{\mathbb{F}_q[x]}{(p_1(x))} \oplus \frac{\mathbb{F}_q[x]}{(p_2(x))} \oplus \cdots \oplus \frac{\mathbb{F}_q[x]}{(p_s(x))}, \quad \frac{\mathbb{F}_q[x]}{(p_i(x))} = \mathbb{F}_{Q_i},\ Q_i = q^{n_i}\\
&f(x) = (f(x) \pmod{p_1(x)}, f(x) \pmod{p_2(x)}, \cdots, f(x) \pmod{p_s(x)}).
\end{aligned}$$

Definition 2.2 *Let* $v_1 = (1, 0, \cdots, 0)$, $v_2 = (0, 1, \cdots, 0), \cdots$, $v_s = (0, 0, \cdots, 1)$ *be elements in*

$$\frac{\mathbb{F}_q[x]}{(p_1(x))} \oplus \frac{\mathbb{F}_q[x]}{(p_2(x))} \oplus \cdots \oplus \frac{\mathbb{F}_q[x]}{(p_s(x))} = \mathbb{F}_{Q_1} \oplus \mathbb{F}_{Q_2} \oplus \cdots \oplus \mathbb{F}_{Q_s}.$$

Let

$$e_i(x) = \pi^{-1}(v_i), \quad 1 \le i \le s.$$

Namely, $e_i(x)$ $(1 \le i \le s)$ *are determined by*

$$e_i(x) \equiv \delta_{ij} \pmod{p_j(x)}, \quad 1 \le j \le s, \tag{2.1}$$

where $\delta_{ij} = 1$ *for* $i = j$ *and* $\delta_{ij} = 0$ *otherwise.* $\{e_i(x)\ (1 \le i \le s)\}$ *is called the system of orthogonal* (*minimal*) *idempotents of* A, *because the following relationships hold*:

$$e_i(x)e_j(x) = \delta_{ij}e_i(x), \quad \sum_{i=1}^{s} e_i(x) = 1, \quad 1 \le i, j \le s.$$

Now we present our main result which shows that the minimum q-polynomial and the normality of $\alpha \in \mathbb{F}_Q^*$ can be determined by using $e_i(x)$ $(1 \le i \le s)$.

Theorem 2.1 *Let* $q = p^m$, $Q = q^n$ *and* $\gcd(n, p) = 1$. *Let* $x^n - 1$ *be decomposed as* $x^n - 1 = p_i(x)p_2(x)\cdots p_s(x)$ *in* $\mathbb{F}_q[x]$ *and the idempotents* $\{e_i(x)\ (1 \le i \le s)\}$ *be defined by congruence equation* (2.1). *Let* $E_i(x) = \varphi(e_i(x))$ *and* $P_i(x) = \varphi(p_i(x))$ $(1 \le i \le n)$. *For any* $\alpha \in \mathbb{F}_Q^*$, *let*

$$\Delta = \Delta(\alpha) = \{i : 1 \le i \le s,\ E_i(\alpha) \ne 0\}.$$

Then the minimal q*-polynomial of* α *is* $M_\Delta(x) = \bigotimes_{i \in \Delta} P_i(x)$ *and* α *is a* k*-normal element for extension* $\mathbb{F}_Q/\mathbb{F}_q$ *where* k (*the normality of* α) *is given by* $k = n - \sum_{i \in \Delta} \deg p_i(x)$.

Proof Let $m_i(x) = \frac{x^n - 1}{p_i(x)}$, $M_i(x) = \varphi(m_i(x))$ $(1 \le i \le s)$. It was proved in the proof of [8, Theorem 2] that for each $\alpha \in \mathbb{F}_Q^*$ and $1 \le i \le s$, $M_i(\alpha) \ne 0$ if and only if $E_i(\alpha) \ne 0$. Then the conclusion can be derived directly from Lemma 1.3. The idempotents $e_1(x), e_2(x), \cdots, e_s(x)$ are determined by the congruence equations (2.1), but the following method is easier to calculate $e_i(x)$ $(1 \le i \le s)$ in certain cases.

Theorem 2.2 (see [8,Theorem 3]) *Suppose that* $Q = q^n$, $\gcd(n, q) = 1$. *Let* $\mathcal{A}_i$ $(1 \le i \le s)$ *be* q*-classes of* Z_n, $e_i(x)$ *and* $p_i(x)$ $(1 \le i \le s)$ *be the corresponding idempotents of* $\mathbb{F}_q[x]/(x^n - 1)$ *and monic irreducible factors of* $x^n - 1$ *in* $\mathbb{F}_q[x]$. *Let* ζ *be a primitive* n*-th root of* 1 *in the algebraic closure of* $\mathbb{F}_q$. *For each* i $(1 \le i \le s)$, *we take* α_i *to be a zero of* $p_i(x)$ *which means* $\alpha_i = \zeta^{a_i}$ *for some* $a_i \in \mathcal{A}_i$. *Let*

$$\varepsilon_i(x) = \sum_{a \in \mathcal{A}_i} x^a, \quad 1 \le i \le s. \tag{2.2}$$

And $\mathbf{M}$ *is an* $s \times s$ *matrix over* $\mathbb{F}_q$ *defined by*

$$\mathbf{M} = (\varepsilon_i(\alpha_j))_{1 \le i,j \le s}.$$

Then $\det(\mathbf{M}) \neq 0$ *and*

$$\begin{pmatrix} e_1(x) \\ \vdots \\ e_s(x) \end{pmatrix} = \mathbf{M^{-1}} \begin{pmatrix} \varepsilon_1(x) \\ \vdots \\ \varepsilon_s(x) \end{pmatrix}.$$

By using the idempotents, a criterion on 0-normal elements was given in [8]: $\alpha \in \mathbb{F}_Q^*$ is a normal element for extension $\mathbb{F}_Q/\mathbb{F}_q$ ($Q = q^n$, $\gcd(n, q) = 1$) if and only if $E_i(\alpha) \neq 0$ ($1 \leq i \leq s$). Now we present such type of criterion on 1-normal elements as an application of Theorem 2.1.

By Theorem 2.1, $\alpha \in \mathbb{F}_Q^*$ is a 1-normal element for extension $\mathbb{F}_Q/\mathbb{F}_q$ ($Q = q^n$, $\gcd(n, q) = 1$) if and only if the minimal q-polynomial $M_\alpha(x)$ of α is $\varphi\big(\frac{x^n-1}{p_i(x)}\big)$ where $p_i(x)$ is a factor of $x^n - 1$ in $\mathbb{F}_q[x]$ with degree 1 so that $p_i(x) = x - c$ for some $c \in \mathbb{F}_q^*$, which means that $c^{q-1} = 1$. Moreover, $c^n = 1$ so that $c^d = 1$ where $d = \gcd(q - 1, n)$. Let γ be a primitive element of $\mathbb{F}_q$ so that $\mathbb{F}_q^* = \langle\gamma\rangle$. Let $n = ed$ and $\beta = \gamma^e$. Then the zeros of $x^n - 1$ in $\mathbb{F}_q$ are β^λ ($0 \leq \lambda \leq d - 1$) and the decomposition of $x^n - 1$ in $\mathbb{F}_q[x]$ is

$$x^n - 1 = p_1(x)p_2(x)\cdots p_d(x)p_{d+1}(x)\cdots p_s(x), \tag{2.3}$$

where $p_\lambda(x) = x - \beta^{\lambda-1}$ for $1 \leq \lambda \leq d$, and $\deg p_\lambda(x) \geq 2$ for $\lambda \geq d + 1$.

For $1 \leq \lambda \leq d$,

$$\begin{aligned} l_\lambda(x) = \frac{x^n - 1}{x - \beta^{\lambda-1}} &= \sum_{i=0}^{n-1} \beta^{(\lambda-1)(n-1-i)} x^i \\ &= \sum_{i=0}^{n-1} \beta^{(\lambda-1)(-1-i)} x^i \quad (\text{since } \beta^n = 1), \end{aligned}$$

and

$$L_\lambda(x) = \varphi(l_\lambda(x)) = \sum_{i=0}^{n-1} \beta^{(\lambda-1)(-1-i)} x^{q^i}.$$

Therefore

$$\begin{aligned} L_\lambda(\alpha) &= \sum_{l=0}^{e-1} \sum_{r=0}^{d-1} \beta^{(\lambda-1)(-1-r)} \alpha^{q^{dl+r}} \quad (\text{let } i = dl + r) \\ &= \sum_{r=0}^{d-1} \beta^{(\lambda-1)(-1-r)} (\mathrm{Tr}_d^n(\alpha))^{q^r}, \end{aligned}$$

where Tr_d^n is the trace mapping from $\mathbb{F}_Q = \mathbb{F}_{q^n}$ to $\mathbb{F}_{q^d}$. Particularly, $L_1(\alpha) = \sum_{r=0}^{d-1} (\mathrm{Tr}_d^n(\alpha))^{q^r} = \mathrm{Tr}_1^d(\mathrm{Tr}_d^n(\alpha)) = \mathrm{Tr}(\alpha)$ where $\mathrm{Tr} = \mathrm{Tr}_1^n$ is the trace mapping from $\mathbb{F}_Q$ to $\mathbb{F}_q$.

From these discussions we get the following result.

Theorem 2.3 *Suppose that* $Q = q^n$, $\gcd(n, q) = 1$. *Let* $\mathbb{F}_q^* = \langle\gamma\rangle$, $d = \gcd(n, q-1)$, $n = ed$ *and* $\beta = \gamma^e$. *Then* $x^n - 1$ *is decomposed in* $\mathbb{F}_q[x]$ *as formula* (2.3). *For any* $\alpha \in \mathbb{F}_Q^*$, *the following statements are equivalent to each other*:

(I) α *is a* 1*-normal element for extension* $\mathbb{F}_Q/\mathbb{F}_q$;

(II) *The minimum q-polynomial of* α *is* $L_\lambda(x) = \sum_{r=0}^{d-1} \beta^{(\lambda-1)(-1-r)}(\mathrm{Tr}_d^n(\alpha))^{q^r}$ *for some* $\lambda, 1 \le \lambda \le d$, *where* $\mathrm{Tr}_d^n(x) = \sum_{l=0}^{e-1} x^{q^{dl}}$;

(III) *There exists just one* λ *for* $1 \le \lambda \le d$ *such that* $\sum_{r=0}^{d-1} \beta^{(\lambda-1)(-1-r)}(\mathrm{Tr}_d^n(\alpha))^{q^r} = 0$ *and* $E_\lambda(\alpha) \neq 0$ *for all* $d+1 \le \lambda \le s$, *where* $E_i(x)$ *is the q-polynomial corresponding to the idempotent* $e_i(x)$;

(IV) *There exists just one* λ *for* $1 \le \lambda \le d$ *such that* $\sum_{r=0}^{d-1} \beta^{(\lambda-1)(-1-r)}(\mathrm{Tr}_d^n(\alpha))^{q^r} = 0$ *and* $\{\alpha, \alpha^q, \cdots, \alpha^{q^{n-2}}\}$ *is* $\mathbb{F}_q$*-linearly independent.*

Proof α is a 1-normal element of $\mathbb{F}_Q/\mathbb{F}_q$ if and only if the degree of the minimum q-polynomial $M_\alpha(x)$ of α is q^{n-1}. Namely, $M_\alpha(x) = L_\lambda(x) = \varphi(l_\lambda(x))$ where $l_\lambda(x) = \frac{x^n-1}{p_\lambda(x)}$ for some λ, $1 \le \lambda \le d$. Therefore (I) and (II) are equivalent. The other equivalent relations can be derived from Theorem 2.1.

Corollary 2.1 *Suppose that* $Q = q^n$ *and* $\gcd(n, q(q-1)) = 1$. *Then* $x^n - 1 = p_1(x)p_2(x)\cdots p_s(x)$ *where* $p_1(x) = x-1$ *and* $\deg p_\lambda \ge 2$ *for* $2 \le \lambda \le s$. *The following statements are equivalent to each other for* $\alpha \in \mathbb{F}_Q^*$:

(I) α *is a 1-normal element for extension* $\mathbb{F}_Q/\mathbb{F}_q$;

(II) *The minimum q-polynomial of* α *is* $\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{q^i}$;

(III) $\mathrm{Tr}(\alpha) = 0$ *and* $E_\lambda(\alpha) \neq 0$ *for all* $2 \le \lambda \le s$;

(IV) $\mathrm{Tr}(\alpha) = 0$ *and* $\{\alpha, \alpha^q, \cdots, \alpha^{q^{n-2}}\}$ *is* $\mathbb{F}_q$*-linearly independent.*

Proof By assumption $\gcd(n, q(q-1)) = 1$, we know that 1 is the only element c in $\mathbb{F}_q^*$ such that $c^n = 1$. Then the conclusion is derived from Theorem 2.3 directly.

3 Examples

In this section we present examples to determine the normality and the minimum q-polynomial of an element $\alpha \in \mathbb{F}_Q^*$ by using Lemma 1.3 and Theorem 2.1.

Example 3.1 Let p and n be prime numbers, $n \neq p$ and $q = p^m$. Suppose that the order of q in $\mathrm{Z}_n^\times$ is $\varphi(n) = n-1$. Namely, $\mathrm{Z}_n^\times = \langle q \rangle$. Then $x^n - 1 = p_1(x)p_2(x)$ where

$$p_1(x) = x - 1, \quad p_2(x) = x^{n-1} + x^{n-2} + \cdots + x + 1$$

are irreducible polynomials in $\mathbb{F}_q[x]$. We get

$$l_1(x) = \frac{x^n - 1}{p_1(x)}, \quad l_2(x) = \frac{x^n - 1}{p_2(x)} = p_1(x),$$

$$L_1(x) = \varphi(l_1(x)) = \sum_{i=0}^{n-1} x^{q^i} = \mathrm{Tr}(x), \quad L_2(x) = \varphi(l_2(x)) = x^q - x.$$

From Lemma 1.3 we get the following result.

Theorem 3.1 *Let* p *and* n *be prime numbers,* $n \neq p$, *and* $q = p^m$, $Q = q^n$. *Suppose that* $\mathrm{Z}_n^* = \langle q \rangle$. *For each* $\alpha \in \mathbb{F}_Q^*$, *let* $M_\alpha(x)$ *be the minimal q-polynomial of* α.

(I) *If* $\alpha \notin \mathbb{F}_q$ *and* $\mathrm{Tr}(\alpha) \neq 0$, *then* $M_\alpha(x) = x^{q^n} - x$ *and* α *is a* (0*-th*) *normal element for* $\mathbb{F}_Q/\mathbb{F}_q$.

(II) *If* $\alpha \notin \mathbb{F}_q$ *and* $\mathrm{Tr}(\alpha) = 0$, *then* $M_\alpha(x) = \mathrm{Tr}(x)$ *and* α *is a* 1*-normal element for* $\mathbb{F}_Q/\mathbb{F}_q$.

(III) *If* $\alpha \in \mathbb{F}_q^*$, *then* $\mathrm{Tr}(\alpha) = n\alpha \neq 0$ *so that* $M_\alpha(x) = x^q - x$ *and* α *is an* $(n-1)$*-normal element for* $\mathbb{F}_Q/\mathbb{F}_q$.

Example 3.2 Let p be a prime number, $q = p^m, n$ be an odd prime, $n \neq p$. Suppose that the order of q in $\mathrm{Z}_n^\times$ is $l = \frac{\varphi(n)}{2} = \frac{n-1}{2}$. Then there exists an integer g such that $\mathrm{Z}_n^\times = \langle g \rangle$ and $q = g^2 \in \mathrm{Z}_n^\times$. Then

$$D = \langle q \rangle = \{q^\lambda : 0 \leq \lambda \leq l-1\} = \{g^{2\lambda} : 0 \leq \lambda \leq l-1\}$$

is the subgroup of multiplicative group $\mathrm{Z}_n^\times$ and the other coset is $D' = gD = \{g^{2\lambda+1} : 0 \leq \lambda \leq l-1\}$. We have the decomposition

$$x^n - 1 = p_1(x)p_2(x)p_3(x)$$

in $\mathbb{F}_q[x]$, where

$$p_1(x) = x - 1, \quad p_2(x) = \prod_{a \in D}(x - \zeta^a), \quad p_3(x) = \prod_{a \in D'}(x - \zeta^a), \tag{3.1}$$

where ζ is an n-th primitive root of 1 in the algebraic closure of $\mathbb{F}_q$. It is not easy to get the polynomials $p_i(x) \in \mathbb{F}_q[x]$, $l_i(x) = \frac{x^n-1}{p_i(x)} \in \mathbb{F}_q[x]$ and $L_i(x) = \varphi(l_i(x)) \in \mathcal{F}_q[x]$ explicitly for $i = 2$ and 3. Now we use the idempotents. With the notations given in Section 2, we have

$$\varepsilon_1(x) = 1, \quad \varepsilon_2(x) = \sum_{r \in D} x^r, \quad \varepsilon_3(x) = \sum_{r \in D'} x^r,$$

$$\mathbf{M} = \begin{pmatrix} \varepsilon_1(1) & \varepsilon_1(\zeta) & \varepsilon_1(\zeta^g) \\ \varepsilon_2(1) & \varepsilon_2(\zeta) & \varepsilon_2(\zeta^g) \\ \varepsilon_3(1) & \varepsilon_3(\zeta) & \varepsilon_3(\zeta^g) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ l & C & B \\ l & B & C \end{pmatrix},$$

where $B = \sum_{r \in D'} \zeta^r \in \mathbb{F}_q$, $C = \sum_{r \in D} \zeta^r \in \mathbb{F}_q$. By Theorem 2.2, $\det(M) = n(B-C) \neq 0$. Then we get

$$\mathbf{M}^{-1} = \frac{1}{n(B-C)} \begin{pmatrix} B-C & B-C & B-C \\ l(B-C) & C-l & l-B \\ l(B-C) & l-B & C-l \end{pmatrix}$$

and

$$\begin{pmatrix} e_1(x) \\ e_2(x) \\ e_3(x) \end{pmatrix} = M^{-1} \begin{pmatrix} \varepsilon_1(x) \\ \varepsilon_2(x) \\ \varepsilon_3(x) \end{pmatrix}.$$

Namely, we get

$$\begin{aligned} e_1(x) &= \frac{1}{n}(\varepsilon_1(x) + \varepsilon_2(x) + \varepsilon_3(x)) = \frac{1}{n}\sum_{i=0}^{n-1} x^i, \\ e_2(x) &= \frac{1}{n(B-C)}[l(B-C) + (C-l)\varepsilon_2(x) + (l-B)\varepsilon_3(x)], \\ e_3(x) &= \frac{1}{n(B-C)}[l(B-C) + (l-B)\varepsilon_2(x) + (C-l)\varepsilon_3(x)]. \end{aligned} \tag{3.2}$$

Now we compute B and C by using the Legendre symbol

$$\Big(\frac{r}{n}\Big) = \begin{cases} 1, & \text{if } r \in D, \\ -1, & \text{if } r \in D'. \end{cases}$$

We have $B + C = \sum\limits_{r=1}^{n-1} \zeta^r = -1,\ B - C = \sum\limits_{r=1}^{n-1} (\frac{r}{n})\zeta^r \in \mathbb{F}_q$, where $B - C$ is the quadratic Gauss sum over $\mathbb{F}_n$, but valued in $\mathbb{F}_q$, instead of the complex number field $\mathbb{C}$. We calculated B and C in [8] as following result.

Case (I) $2 \nmid q$. Let $n^* = \big(\frac{-1}{n}\big)n$, then

$$B = \frac{1}{2}(-1 + \mu\sqrt{n^*}), \quad C = \frac{1}{2}(-1 - \mu\sqrt{n^*}), \quad \mu = 1 \text{ or } -1.$$

Then by (3.2) we get

$$n\mu\sqrt{n^*}e_2(x) = l\mu\sqrt{n^*} + \frac{n}{2}(\varepsilon_3(x) - \varepsilon_2(x)) - \frac{\mu\sqrt{n^*}}{2}(\varepsilon_3(x) + \varepsilon_2(x)),$$
$$n\mu\sqrt{n^*}e_3(x) = l\mu\sqrt{n^*} - \frac{n}{2}(\varepsilon_3(x) - \varepsilon_2(x)) - \frac{\mu\sqrt{n^*}}{2}(\varepsilon_3(x) + \varepsilon_2(x))$$

and

$$\begin{aligned} &nE_1(x) = \mathrm{Tr}(x), \\ &2n\sqrt{n^*}E_2(x) = n\sqrt{n^*}x - \mu n \sum_{r=1}^{n-1} \Big(\frac{r}{n}\Big)x^{q^r} - \sqrt{n^*}\mathrm{Tr}(x), \\ &2n\sqrt{n^*}E_3(x) = n\sqrt{n^*}x + \mu n \sum_{r=1}^{n-1} \Big(\frac{r}{n}\Big)x^{q^r} - \sqrt{n^*}\mathrm{Tr}(x). \end{aligned} \tag{3.3}$$

Case (II) $2 \mid q$. Then $B + C = B - C = 1$ and

$$\{B, C\} = \begin{cases} \{0, 1\}, & \text{if } n \equiv \pm 1 \pmod 8, \\ \{\omega, \omega + 1\}, & \text{if } n \equiv \pm 3 \pmod 8, \end{cases}$$

where $\omega \in \mathbb{F}_4 \backslash \{0, 1\}$. Then by (3.2) we get

$$ne_2(x) = l + (l + B)(\varepsilon_2(x) + \varepsilon_3(x)) + \varepsilon_2(x) = l\sum_{r=0}^{n-1} x^r + B\sum_{r=1}^{n-1} x^r + \sum_{r\in D} x^r,$$
$$ne_3(x) = l\sum_{r=0}^{n-1} x^r + C\sum_{r=1}^{n-1} x^r + \sum_{r\in D} x^r,$$

and

$$\begin{aligned} &nE_1(x) = \mathrm{Tr}(x), \\ &nE_2(x) = l\mathrm{Tr}(x) + B(\mathrm{Tr}(x) + x) + \sum_{r\in D} x^{q^r}, \\ &nE_3(x) = l\mathrm{Tr}(x) + C(\mathrm{Tr}(x) + x) + \sum_{r\in D} x^{q^r}, \quad C = B + 1. \end{aligned} \tag{3.4}$$

Now we determine the normality of any element $\alpha \in \mathbb{F}_Q^*$.

Theorem 3.2 *Let p and n be distinct prime numbers, $n \geq 3$, $q = p^m$, $Q = q^n$. Suppose that $\mathrm{Z}_n^\times = \langle g \rangle$ and $q = g^2 \in \mathrm{Z}_n^\times$ so that the order of q in the multiplicative group $\mathrm{Z}_n^\times$ is $l = \frac{n-1}{2}$. Let*

$$D = \langle q \rangle = \{g^{2\lambda} : 0 \leq \lambda \leq l-1\}.$$

Then $x^n - 1 = p_1(x)p_2(x)p_3(x)$ where $p_i(x)$ $(1 \leq i \leq 3)$ are the monic irreducible factors of $x^n - 1$ in $\mathbb{F}_q[x]$ defined by (3.1). Let $P_i(x) = \varphi(p_i(x))$ $(1 \leq i \leq 3)$. For $\alpha \in \mathbb{F}_Q^*$, let $M_\alpha(x)$ be the minimum q-polynomial of α, and α is a k-normal element for $\mathbb{F}_Q/\mathbb{F}_q$.

Case (I) $2 \nmid q$. *Let* $\delta = \sum_{r=0}^{n-1} (\frac{r}{n}) \alpha^{q^r}$.

(a) *If $\alpha \in \mathbb{F}_q^*$, then $M_\alpha(x) = x^q - x$ and $k = n-1$.*

(b) *Suppose that $\alpha \in \mathbb{F}_Q \backslash \mathbb{F}_q$ and $\mathrm{Tr}(\alpha) = 0$.*

If $\sqrt{n^*}\delta \notin \{\pm n\alpha\}$, then $M_\alpha(x) = \mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{q^i}$ and $k = 1$. Otherwise $M_\alpha(x) = P_2(x)$ or $P_3(x)$ and $k = l + 1 = \frac{n+1}{2}$.

(c) *Suppose that $\alpha \in \mathbb{F}_Q \backslash \mathbb{F}_q$ and $\mathrm{Tr}(\alpha) \neq 0$.*

If $\sqrt{n^*}\delta \notin \{\pm(n\alpha - \mathrm{Tr}(\alpha))\}$, then $M_\alpha(x) = x^{q^n} - x$ and $k = 0$ (α is a normal element for $\mathbb{F}_Q/\mathbb{F}_q$). Otherwise $M_\alpha(x) = P_i(x^q - x) = P_i(x)^q - P_i(x)$ for $i = 2$ or 3 and $k = l = \frac{n-1}{2}$.

Case (II) $2 \mid q$. *Let* $\varepsilon = \sum_{r \in D} \alpha^{q^r}$, $\omega \in \mathbb{F}_4 \backslash \{0, 1\}$ *and*

$$B = \begin{cases} 0, & \text{if } n \equiv \pm 1 \pmod 8, \\ \omega, & \text{if } n \equiv \pm 3 \pmod 8. \end{cases}$$

(a) *If $\alpha \in \mathbb{F}_q^*$, then $M_\alpha(x) = x^q - x$ and $k = n-1$.*

(b) *Suppose that $\alpha \in \mathbb{F}_Q \backslash \mathbb{F}_q$ and $\mathrm{Tr}(\alpha) = 0$. If $\varepsilon \notin \{B\alpha, (B+1)\alpha\}$, then $M_\alpha(x) = \mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{q^i}$ and $k = 1$. Otherwise $M_\alpha(x) = P_2(x)$ or $P_3(x)$ and $k = l + 1 = \frac{n+1}{2}$.*

(c) *Suppose that $\alpha \in \mathbb{F}_Q \backslash \mathbb{F}_q$ and $\mathrm{Tr}(\alpha) \neq 0$. If $\varepsilon \notin \{l\mathrm{Tr}(\alpha) + B(\mathrm{Tr}(\alpha) + \alpha), l\mathrm{Tr}(\alpha) + (B+1)(\mathrm{Tr}(\alpha) + \alpha)\}$, then $M_\alpha(x) = x^{q^n} - x$ and $k = 0$ (α is a normal element for $\mathbb{F}_Q/\mathbb{F}_q$). Otherwise $M_\alpha(x) = P_i(x)^q + P_i(x)$ for $i = 2$ or 3 and $k = l = \frac{n-1}{2}$.*

Proof (I) For $2 \nmid q$, $\alpha \in \mathbb{F}_Q^\times$, formula (3.3) gives

$$\begin{aligned} &E_1(\alpha) = 0 \Leftrightarrow \mathrm{Tr}(\alpha) = 0, \\ &E_2(\alpha) = 0 \Leftrightarrow n\alpha - \mathrm{Tr}(\alpha) - \mu\sqrt{n^*}\delta = 0, \\ &E_3(\alpha) = 0 \Leftrightarrow n\alpha - \mathrm{Tr}(\alpha) + \mu\sqrt{n^*}\delta = 0, \quad \mu = 1 \text{ or } -1. \end{aligned}$$

If $\alpha \in \mathbb{F}_q^*$, then $\mathrm{Tr}(\alpha) = n\alpha \neq 0$, $\delta = \sum_{r=0}^{n-1} \left(\frac{r}{n}\right) \alpha^{q^r} = \alpha \sum_{r=0}^{n-1} \left(\frac{r}{n}\right) = 0$. Therefore $E_1(\alpha) \neq 0$ and $E_2(\alpha) = E_3(\alpha) = 0$. By Theorem 2.1, $M_\alpha(x) = P_1(x) = x^q - x$ and $k = n-1$. If $\alpha \in \mathbb{F}_Q \backslash \mathbb{F}_q$, then $n\alpha - \mathrm{Tr}(\alpha) \neq 0$ $\big($otherwise $\alpha = \frac{1}{n}\mathrm{Tr}(\alpha) \in \mathbb{F}_q\big)$. If $E_2(\alpha) = E_3(\alpha) = 0$, then $n\alpha - \mathrm{Tr}(\alpha) = \sqrt{n^*}\delta = -\sqrt{n^*}\delta$ which implies that $\delta = 0$ and $n\alpha = \mathrm{Tr}(\alpha)$, contradiction.

Therefore at most one of $E_2(\alpha)$ and $E_3(\alpha)$ is zero. And $E_i(\alpha) = 0$ for $i = 2$ or 3 if and only if $\sqrt{n^*}\delta \in \{\pm(n\alpha - \mathrm{Tr}(\alpha))\}$. When $\mathrm{Tr}(\alpha) = 0$, then $E_1(\alpha) = 0$. If $\sqrt{n^*}\delta \notin \{\pm n\alpha\}$, then $E_2(\alpha) \neq 0 \neq E_3(\alpha)$ and $M_\alpha(x) = \varphi(p_2(x)p_3(x)) = \varphi\big(\sum_{i=0}^{n-1} x^i\big) = \sum_{i=0}^{n-1} x^{q^i}$, $k = n - (n-1) = 1$. If $\sqrt{n^*}\delta = n\alpha$ or $-n\alpha$ (namely, $\delta = \sqrt{n^*}\alpha$ or $-\sqrt{n^*}\alpha$), then $M_\alpha(x) = P_i(x)$ where $i = 2$ or

3 and $k = n - l = l + 1$. When $\mathrm{Tr}(\alpha) \neq 0$, we have $E_1(\alpha) \neq 0$. If $\sqrt{n^*}\delta \notin \{\pm(n\alpha - \mathrm{Tr}(\alpha))\}$, then $E_2(\alpha) \neq 0 \neq E_3(\alpha)$ and $M_\alpha(x) = \varphi(x^n - 1) = x^{q^n} - x,\ k = 0$. Otherwise $M_\alpha(x) = \varphi(p_i(x)p_1(x)) = P_i(x) \otimes (x^q - x) = P_i(x^q - x) = P_i(x)^q - P_i(x)$ for $i = 2$ or 3. This completes the proof of Case (I). Similarly we can prove Theorem 3.2 for Case (II) by using Theorem 2.1 and formula (3.4).

Example 3.3 (General Case) Let p and n be distinct prime numbers, $n \geq 3,\ q = p^m,\ Q = q^n$. Let f be the order of q in the multiplicative group $\mathrm{Z}_n^\times$. Then $n - 1 = ef$ and there exists $g \in \mathrm{Z}_n^\times$ such that $\mathrm{Z}_n^\times = \langle g \rangle$ and $q = g^e \in \mathrm{Z}_n^\times$. $C = \langle q \rangle$ is a subgroup of $\mathrm{Z}_n^\times$ and the cosets of C in $\mathrm{Z}_n^\times$ are

$$C_\lambda = g^\lambda C = \{g^{\lambda + ie} : 0 \leq i \leq f - 1\}, \quad 0 \leq \lambda \leq e - 1.$$

Let ζ be an n-th primitive root of 1, $\mathbb{F}_q(\zeta) = \mathbb{F}_{q^f}$. Then

$$x^n - 1 = p_*(x)p_0(x) \cdots p_{e-1}(x), \tag{3.5}$$

where $p_*(x) = x - 1$ and for $0 \leq \lambda \leq e - 1,\ p_\lambda = \sum\limits_{a \in C_\lambda} (x - \zeta^a)$ is an irreducible polynomial in $\mathbb{F}_q[x]$. Therefore

$$\varepsilon_* = 1, \quad \varepsilon_\lambda(x) = \sum_{a \in C_\lambda} x^a \ (\mathrm{mod}\, x^n - 1), \quad 0 \leq \lambda \leq e - 1. \tag{3.6}$$

Let $\varepsilon_\lambda = \varepsilon_\lambda(\zeta) = \sum\limits_{a \in C_\lambda} \zeta^a$ $(0 \leq \lambda \leq e - 1)$. We know that $\varepsilon_\lambda \in \mathbb{F}_q$ is the Gauss periods of order e and for $\alpha_j = \zeta^{g^j}$,

$$\varepsilon_\lambda(\alpha_j) = \sum_{a \in C_\lambda} \zeta^{ag^j} = \varepsilon_{\lambda + j}, \quad \lambda, j \in \mathrm{Z}_e.$$

Therefore

$$\mathbf{M} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ f & \varepsilon_0 & \varepsilon_1 & \cdots & \varepsilon_{e-1} \\ f & \varepsilon_1 & \varepsilon_2 & \cdots & \varepsilon_0 \\ \vdots & \vdots & \vdots & & \vdots \\ f & \varepsilon_{e-1} & \varepsilon_0 & \cdots & \varepsilon_{e-2} \end{pmatrix}.$$

By using the equalities

$$\sum_{\lambda=0}^{e-1} \varepsilon_\lambda = \sum_{\lambda=0}^{e-1} \sum_{a \in C_\lambda} \zeta^a = \sum_{a=0}^{n-1} \zeta^a = -1 \tag{3.7}$$

and

$$\begin{aligned} \sum_{\lambda=0}^{e-1} \varepsilon_\lambda \varepsilon_{\lambda+j} &= \sum_{\lambda=0}^{e-1} \sum_{a,b \in \mathrm{C}} \zeta^{ag^\lambda + bg^{\lambda+j}} \\ &= \sum_{\lambda=0}^{e-1} \sum_{a \in \mathrm{C}} \sum_{d \in \mathrm{C}} \zeta^{ag^\lambda(1+dg^j)} \quad (\text{let } d = ba^{-1}) \\ &= \begin{cases} n - f, & \text{if } -1 \in \mathrm{C_j} \text{ (namely, if } j = 0 \text{ for even } f \text{ and } j = \frac{e}{2} \text{ for odd } f), \\ -f, & \text{otherwise,} \end{cases} \end{aligned}$$

we get

$$\mathbf{M}^{-1} = \frac{1}{n}\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ f & \varepsilon_c & \varepsilon_{c+1} & \cdots & \varepsilon_{c-1} \\ f & \varepsilon_{c+1} & \varepsilon_{c+2} & \cdots & \varepsilon_c \\ \vdots & \vdots & \vdots & & \vdots \\ f & \varepsilon_{c-1} & \varepsilon_c & \cdots & \varepsilon_{c-2} \end{pmatrix},$$

where $c \equiv \frac{ef}{2} \pmod{e}$. Namely, $c = 0$ for even f and $c = \frac{f}{2}$ for odd f. By Theorem 2.2, we have for $\alpha \in \mathbb{F}_Q^*$ $(Q = q^n)$,

$$\begin{pmatrix} e_*(x) \\ e_0(x) \\ \vdots \\ e_{e-1}(x) \end{pmatrix} = \mathbf{M}^{-1}\begin{pmatrix} 1 \\ \varepsilon_0(x) \\ \vdots \\ \varepsilon_{e-1}(x) \end{pmatrix} = \frac{1}{n}\begin{pmatrix} \sum_{i=0}^{n-1} x^i \\ f + \sum_{\lambda=0}^{e-1} \varepsilon_\lambda(x)\varepsilon_{\lambda+c} \\ \vdots \\ f + \sum_{\lambda=0}^{e-1} \varepsilon_\lambda(x)\varepsilon_{\lambda+c-1} \end{pmatrix}.$$

Namely, $E_*(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i} = \mathrm{Tr}(\alpha)$ and for $0 \le i \le e-1$,

$$E_i(\alpha) = \frac{1}{n}\Big(f\alpha + \sum_{\lambda=0}^{e-1} \varepsilon_{\lambda+c+i} \sum_{a\in C_\lambda} \alpha^{q^a}\Big). \tag{3.8}$$

From these computations and Theorem 2.1, we get the following result.

Theorem 3.3 *Let p and n be distinct prime numbers, $n \ge 3$, $q = p^m$, $Q = q^n$. Let f be the order of q in the multiplicative group $\mathrm{Z}_n^\times$, $n - 1 = ef$. Then there exists $g \in \mathrm{Z}_n^\times$ such that $\mathrm{Z}_n^\times = \langle g\rangle$ and $q = g^e \in \mathrm{Z}_n^\times$. Let*

$$C = \langle q\rangle = \{q^i : 0 \le i \le f-1\} = \{g^{ie} : 0 \le i \le f-1\}$$

and $C_\lambda = g^\lambda C$ $(0 \le \lambda \le e-1)$ are the cyclotomic cosets of C in $\mathrm{Z}_n^\times$. Let ζ be an n-th primitive root of 1, $\mathbb{F}_q(\zeta) = \mathbb{F}_{q^f}$. Then $x^n - 1$ is decomposed in $\mathbb{F}_q[x]$ by

$$x^n - 1 = p_*(x)p_0(x)\cdots p_{e-1}(x),$$

where $p_*(x) = x - 1$ and for $0 \le \lambda \le e-1$, $p_\lambda = \sum_{a\in C_\lambda} (x - \zeta^a)$ is an irreducible polynomial in $\mathbb{F}_q[x]$, and $P_\lambda = \varphi(p_\lambda)$. Let

$$\varepsilon_\lambda = \sum_{a\in C_\lambda} \zeta^a,$$

$$c = \begin{cases} 0, & \text{if } f \text{ is even,} \\ \dfrac{e}{2}, & \text{if } f \text{ is odd.} \end{cases}$$

For $\alpha \in \mathbb{F}_Q^*$, let

$$\mathcal{S} = \Big\{i : 0 \le i \le e-1,\ \sum_{\lambda=0}^{e-1} \varepsilon_{\lambda+i+c} \sum_{a\in C_\lambda} \alpha^{q^a} \ne -fa\Big\}, \tag{3.9}$$

and let $M_\alpha(x)$ be the minimum q-polynomial of α and α be a k-normal element for $\mathbb{F}_Q/\mathbb{F}_q$.

(I) *When $\alpha \in \mathbb{F}_q^*$, then $M_\alpha(x) = x^q - x$ and $k = n-1$;*

(II) *When $\alpha \in \mathbb{F}_Q/\mathbb{F}_q$ and $\mathrm{Tr}(\alpha) = 0$, then $M_\alpha(x) = \bigotimes\limits_{\lambda\in\mathcal{S}} P_\lambda(x)$ and $k = n - f|\mathcal{S}| = f(e-|\mathcal{S}|)+1$;*

(III) *When $\alpha \in \mathbb{F}_Q/\mathbb{F}_q$ and $\mathrm{Tr}(\alpha) \neq 0$, then $M_\alpha(x) = \bigotimes\limits_{\lambda\in\mathcal{S}} P_\lambda(x^q - x)$ and $k = n-1-f|\mathcal{S}| = f(e-|\mathcal{S}|)$.*

Proof When $\alpha \in \mathbb{F}_q^*$, $E_* = \mathrm{Tr}(\alpha) = n\alpha \neq 0$ and for $0 \le i \le e-1$, by (3.8)

$$E_i(\alpha) = \frac{1}{n}\Big(f\alpha + \sum_{\lambda=0}^{e-1}\varepsilon_{\lambda+c+i}\sum_{a\in C_\lambda}\alpha^{q^a}\Big) = \frac{1}{n}\Big(f\alpha + f\alpha\sum_{\lambda=0}^{e-1}\varepsilon_\lambda\Big) = 0.$$

Therefore $M_\alpha(x) = P_1(x) = x^q - x$ and $k = n-1$.

When $\alpha \in \mathbb{F}_Q/\mathbb{F}_q$, $E_*(\alpha) = \mathrm{Tr}(\alpha)$ and for $1 \le i \le e-1$, by (3.8)–(3.9),

$$E_i(\alpha) \neq 0 \Longleftrightarrow i \in \mathcal{S}.$$

Therefore $M_\alpha(x) = \bigotimes\limits_{\lambda\in\mathcal{S}} P_\lambda(x)$ and $k = n - f|\mathcal{S}|$ if $\mathrm{Tr}(\alpha) = 0$ and $M_\alpha(x) = \big(\bigotimes\limits_{\lambda\in\mathcal{S}} P_\lambda(x)\big) \bigotimes P_1(x) = \bigotimes\limits_{\lambda\in\mathcal{S}} P_\lambda(x^q - x)$, $k = n - f|\mathcal{S}| - 1 = f(e-|\mathcal{S}|)$ if $\mathrm{Tr}(\alpha) \neq 0$.

Remark 3.1 (1) $\varepsilon_i = \sum\limits_{a\in C_1}\zeta^a$ $(0 \le i \le e-1)$ are Gauss periods of order e over $\mathbb{F}_n$, but valued in $\mathbb{F}_q$. They can be computed as usual Gauss periods valued in complex number field $\mathbb{C}$ for small e and semiprimitive case. For $e = 1$ and 2, we get Theorem 3.1 and 3.2 respectively.

(2) For $q = 2$, $(e,n) = (3,7),(5,31),(7,127)$ or $q = 4, e = 3, n = 7$, $\varepsilon_i \in \mathbb{F}_2$ and by (3.8),

$$\sum_{i=0}^{e-1}\varepsilon_i\varepsilon_{i+j} = \begin{cases} 1, & \text{if } j = 0,\\ 0, & \text{if } 1 \le j \le e-1, \end{cases}$$

which means that the circulant matrix over $\mathbb{F}_2$

$$\mathbf{M} = \begin{pmatrix} \varepsilon_0 & \varepsilon_1 & \cdots & \varepsilon_{e-1} \\ \varepsilon_1 & \varepsilon_2 & \cdots & \varepsilon_0 \\ \vdots & \vdots & & \vdots \\ \varepsilon_{e-1} & \varepsilon_0 & \cdots & \varepsilon_{e-2} \end{pmatrix}$$

is orthogonal. Jungnickel et al. [4] obtained a formula on the number of orthogonal circulant $e \times 2$ matrix over $\mathbb{F}_q$. From this formula we know that for $q = 2, (e,n) = (3,7),(5,31),(7,127)$ or $q = 4, (e,n) = (3,7)$, $(\varepsilon_0, \varepsilon_1, \cdots, \varepsilon_{e-1})$ is a cyclic shift of $(1,0,\cdots,0)$. Let $\varepsilon_t = 1$, then $\sum\limits_{\lambda=0}^{e-1}\varepsilon_{\lambda+i+c}\sum\limits_{a\in C_\lambda}\alpha^{q^a}\sum\limits_{a\in C_{\lambda'}}\alpha^{q^a}$ where $\lambda' = t+i+c$. Therefore let

$$\mathcal{S}' = \Big\{\lambda' : 0 \le \lambda' \le e-1, \sum_{a\in C_{\lambda'}}\alpha^{q^a}\Big\} \neq -fa.$$

Then $\mathcal{S}' = \mathcal{S} + t = \{s + t, s \in \mathcal{S}\}$, $|\mathcal{S}| = |\mathcal{S}'|$, and Theorem 3.3 can be stated in term of $\mathcal{S}'$ in stead of $\mathcal{S}$.

References

[1] Alizadah, M. and Mehrabi, S., Recursive constrctions of k-normal polymonials over finite fields, 2016. ArXiv: 1610.05684vl

[2] Antonio Sozaya-Chan, J. and Tapia-Recillas, H., On k-normal elements over finite fields, *Finite Fields Appl.*, **52**, 2018, 94–107.

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

[4] Jungnickel, D., Beth, T. and Geiseman, W., A note of orthogonal circulant matrices over finite fields, *Arch. Math.*, **62**, 1994, 120–133.

[5] Lidl, R. and Niederreiter, H., Finite Fields, 2nd ed., Encyclopedia of Mathematics and Its Applications, **20**, Cambridge University Press, Cambridge, 1997.

[6] Mullen, D. and Panario, D., Handbook of Finite Fields, CRC Press, Boca Baton, FL, 2013.

[7] Negre, C., Finite field arithmetic using quasi-normal bases, *Finite Fields Appl.*, **13**, 2007, 635–647.

[8] Zhang, A. and Feng, K., A new criterion on normal bases of finite field extensions, *Finite Fields Appl.*, **31**, 2015, 25–41.