TÜBİTAK

Turkish Journal of Mathematics

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

Research Article

Turk J Math
(2019) 43: 795 – 812

doi:10.3906/mat-1805-113

On the number of k-normal elements over finite fields

Zülfükar SAYGI*, Ernist TILENBAEV, Çetin ÜRTİŞ
Department of Mathematics, Faculty of Science, TOBB University of Economics and Technology, Ankara, Turkey

Received: 23.05.2018 • **Accepted/Published Online:** 11.02.2019 • **Final Version:** 27.03.2019

Abstract: In this article we give an explicit formula for the number of k-normal elements, hence answering Problem 6.1. of Huczynska et al. (Existence and properties of k-normal elements over finite fields, Finite Fields Appl 2013; 24: 170-183). Furthermore, for some cases we provide formulas that require the solutions of some linear Diophantine equations. Our results depend on the explicit factorization of cyclotomic polynomials.

Key words: Finite fields, normal bases, normal elements, k-normal elements

1. Introduction

Let q be a prime power. For a positive integer n let $\mathbb{F}_q$ and $\mathbb{F}_{q^n}$ denote finite fields of size q and q^n, respectively. $\mathbb{F}_{q^n}$ forms a vector space over $\mathbb{F}_q$ of dimension n. An element $\alpha \in \mathbb{F}_{q^n}$ is called a *normal element* if the set of conjugates $\mathcal{B} := \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ forms a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. In this case $\mathcal{B}$ is called a *normal basis* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Normal bases are widely used in areas such as cryptography, coding theory, and signal processing. They are practical in implementing finite field arithmetic, especially in multiplication and exponentiation due to the structure of finite fields (see, for example, [4, 8, 11, 14]). It is well known that there exists a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ (see [9, Theorem 2.35]). Furthermore, for some special values of q and n there exist normal bases allowing finite field arithmetic with low complexities called optimal normal bases and Gaussian normal bases; see [11, Theorem 3.1 and Theorem 3.2] and [4, Lemma 1].

Quasinormal bases were introduced in [12], which is a class of $\mathbb{F}_q$-bases of $\mathbb{F}_{q^n}$ that offer efficient multiplication in finite fields. These are useful when there is no optimal normal base for a given finite field and Gaussian normal bases of this field have high complexity. Extending the definition of normal elements, k-normal elements were first introduced in [7], which also arise implicitly in constructing quasinormal bases.

Structures of k-normal elements were studied and an implicit formula for the number of k-normal elements was given in [7] (see Theorem 2). To obtain the number of k-normal elements one needs an explicit factorization of cyclotomic polynomials. In this article we give some results concerning this problem. Let $Q_n(x)$ be the nth cyclotomic polynomial over the field $\mathbb{F}_q$. It is defined as the unique monic polynomial having exactly the nth primitive roots of unity as its zeros under the assumption that n is not divisible by the characteristic

*Correspondence: zsaygi@etu.edu.tr
2010 *AMS Mathematics Subject Classification:* 11T06, 12E20, 12Y05

of $\mathbb{F}_q$; that is,

$$Q_n(x) = \prod_{\substack{s=1 \\ \gcd(s,n)=1}}^{n} (x - \zeta^s),$$

where ζ is a primitive nth root of unity (see, for example, [9, Definition 2.44]). Factorization of $Q_n(x)$ was given in [9, Theorem 3.75] for the case $q \equiv 1 \pmod 4$ and $n = 2^m$. The case where q is prime, $q \equiv 3 \pmod 4$, and $n = 2^m$ was studied in [1] and generalization of this case, i.e. for a prime power $q \equiv 3 \pmod 4$ and $n = 2^m$, was done in [9, Theorem 3.76] and [10, Theorem 1], which gives the complete factorization of Q_n.

In [6] the authors studied the relationship between cyclotomic polynomials and Dickson polynomials. They studied the case where $n = 2^m r$, with r being an odd prime and $q \equiv \mp 1 \pmod r$. Hence, the complete factorization for the case $n = 2^m 3$ for any characteristic greater than 3 was obtained. The case $n = 2^m r$ in which q and r are odd with $\gcd(q, r) = 1$ was studied in [16] and complete factorization for the case $n = 2^m 5$ for any odd characteristic field was settled. Complete factorization for the case $n = 2^m 7$ for any characteristic was given in [5]. The relationship between cyclotomic polynomials $Q_{2^m r}$ and Q_r was given in [15] where r and q are odd. The work in [3] covers a complete factorization of Q_n where $n = 2^m p^k$, p being an odd prime such that $q \equiv 1 \pmod p$. Lastly, in [17], the authors studied the relationship between $Q_{p^m r}$ and Q_r, where r is odd. Furthermore, they gave a complete factorization for the cases $n = 3^m$, $n = 3^m 5$, and $n = 3^m 7$. We will exploit some of these results, while the remaining can be done similarly.

Four problems concerning k-normal elements were posed in [7]. In this article we investigate one of these problems (Problem 6.1 in [7]), given as follows:

> For which values of q, n, and k can "nice" formulae (in q and n) be obtained for the number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$?

We give an explicit formula for the number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ for some cases, hence answering the problem above and, furthermore, for some cases we provide formulas involving solutions of some linear Diophantine equations. Our results depend on the explicit factorizations of cyclotomic polynomials.

2. Preliminaries

In this section we give some notations and some preliminary results that will be used throughout the paper.

We denote the set of all nth roots of unity by $R(n)$ and the set of all primitive nth roots of unity by $\Omega(n)$. For $x, y \in \Omega(n)$, the relation $\sim$ defined by $x \sim y$ if and only if $x + x^{-1} = y + y^{-1}$ yields an equivalence relation on $\Omega(n)$. We denote the set of representatives of equivalence classes under this equivalence by $S(n)$.

For a prime r, let $v_r(n)$ be the r-adic valuation of n defined as the greatest integer power of r such that $r^{v_r(n)}$ divides n. Formally, for any positive integer n, $v_r(n)$ is defined as

$$v_r(n) = \max\{v \in \mathbb{N} : r^v \mid n\}.$$

In the following sections we present the factorization of the cyclotomic polynomial $Q_n(x)$ depending on the values of $v_r(q-1)$ for some specific r.

For $h \in \mathbb{F}_q[x]$, the Euler phi function $\Phi_q(h)$ gives the number of nonzero polynomials with degree smaller than the degree of h and that are relatively prime to h. If h is a nonzero constant, then it is assumed to be $\Phi_q(h) = 1$.

A well-known characterization of normal elements over finite fields (see [9, Theorem 2.39]) is given by the following result:

Theorem 1 *[9] For $\alpha \in \mathbb{F}_{q^n}, \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if the polynomials $x^n - 1$ and $\alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-1}}$ are relatively prime in $\mathbb{F}_{q^n}[x]$.*

As a consequence of this theorem, the notion of normal elements was extended in [7] as follows.

Definition 1 *[7] Let $\alpha \in \mathbb{F}_{q^n}$ and $g_\alpha(x) := \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-1}} = \sum_{i=0}^{n-1} \alpha^{q^i} x^{n-1-i} \in \mathbb{F}_{q^n}[x]$. If $\gcd(x^n - 1, g_\alpha(x))$ over $\mathbb{F}_{q^n}$ has degree k (where $0 \leq k \leq n-1$), then α is a k-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

Here we note that a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ becomes 0-normal in this definition. Therefore, the notion of k-normality generalizes the notion of normality. The following theorem gives the number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ implicitly. It depends on the factorization of $x^n - 1$, which in turn depends on the factorization of cyclotomic polynomials. To the best of our knowledge it is the only general but implicit result concerning the number of k-normal elements.

Theorem 2 *[7] The number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is given by*

$$\sum_{\substack{h | x^n - 1 \\ \deg(h) = n-k}} \Phi_q(h), \tag{1}$$

where divisors are monic and polynomial division is over $\mathbb{F}_q[x]$.

In this article, we give the exact number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ for some values of q and n. Furthermore, for some other values we will reduce the formula in Theorem 2 to a sum that depends on the solution of a certain linear Diophantine equation.

3. Number of k-normal elements

In this section we present explicit formulas for the number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ depending on the values of n and q. In our computations we mainly use the following useful result given in [9, Theorem 2.47].

Theorem 3 *[9] If $\gcd(q, n) = 1$, then $Q_n(x)$ factors into $\phi(n)/d$ distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of the same degree d, where d is the least positive integer such that $q^d \equiv 1 \mod n$.*

The main difficulty in Theorem 3 is to obtain the values of d depending on q and n. Once we obtain the values of d then one can get the number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ using Theorem 2. It is well known that $x^n - 1 = \prod_{m|n} Q_m(x)$, whenever $\mathrm{char}(\mathbb{F}_q)$ does not divide n and one needs to find d values corresponding to each Q_m as in Theorem 3.

First we present the following simple case. Assume that $n = p^m$, where $p = \mathrm{char}(\mathbb{F}_q)$. In this case

$$x^n - 1 = x^{p^m} - 1 = (x-1)^{p^m} = (x-1)^n. \tag{2}$$

Using this simple identity we get the following result on the number of k-normal elements.

Proposition 1 *Let $char(\mathbb{F}_q) = p$ and $n = p^m$ for some positive integer m. Then the number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is given by*

$$f(k) = (q-1)q^{n-k-1},$$

where $k = 0, 1, \ldots, n-1$.

Proof Since the characteristic of $\mathbb{F}_q$ is p, equation (2) gives

$$x^n - 1 = (x-1)^n.$$

Then by using Theorem 2 for $0 \leq k \leq n-1$ we get

$$\begin{aligned} f(k) &= \sum_{\substack{h \mid (x-1)^n,\ h-\text{monic} \\ \deg h = n-k}} \Phi_q(h) = \Phi_q\left((x-1)^{n-k}\right) \\ &= q^{n-k} - q^{n-k-1} = (q-1)q^{n-k-1}. \end{aligned}$$

□

Remark 1 *To consider the general case in which $\gcd(q, n) \neq 1$ we assume that $n = p^s \cdot n_0$ and $\gcd(q, n_0) = 1$ where $char(\mathbb{F}_q) = p$. Then we have $x^n - 1 = (x^{n_0} - 1)^{p^s}$. Therefore, one only needs to evaluate d values in Theorem 3 for n_0 and q. Combining this result with the proof of Proposition 1 one obtains the number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

In the following subsections we consider the values of $n = 2^m$, $n = 3^m$, $n = r^m$ for some prime $r \neq 2, 3$ and $n = 2^m \cdot r$ for some prime $r \neq 2$ separately and explicitly obtain the number of k-normal elements.

3.1. Case $n = 2^m$

Now let us consider one of the earliest results about factorization of cyclotomic polynomials. By using the following proposition we consider the extension fields of $\mathbb{F}_q$, where the degrees of the extensions are powers of 2. Here we note that the general form of the factors of cyclotomic polynomials in this case is presented in [6, Proposition 1] and it was obtained from the results of Theorem 3.35 and Theorem 2.47 in [9].

Proposition 2 *[6, Proposition 1] Let $q \equiv 1 \pmod 4$ be a prime power, $n = 2^m$ for some positive integer m and $L = v_2(q-1)$, i.e. $L \geq 2$. Then the cyclotomic polynomial Q_{2^m} factorizes over $\mathbb{F}_q$ as*

$$Q_{2^m}(x) = \begin{cases} \prod_{\zeta \in \Omega(2^m)} (x - \zeta), & \text{if } 2 \leq m \leq L, \\ \prod_{\zeta \in \Omega(2^L)} (x^{2^{m-L}} - \zeta), & \text{if } m > L. \end{cases}$$

Combining this result with Theorem 2, we obtain the following explicit result on the number of k-normal elements.

Theorem 4 *Let $q \equiv 1 \pmod 4$ be a prime power and $n = 2^m$ for some positive integer m. Let $L = v_2(q-1)$, i.e. $L \geq 2$. Then the number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is given as follows:*

$$f(k) = \begin{cases} \binom{n}{k}(q-1)^{n-k}, & \text{if } L \geq m \\ \sum \left[\prod_{i=1}^{m-L} \binom{2^{L-1}}{a_i} (q^{2^i}-1)^{a_i} \right] \binom{2^L}{b} (q-1)^b, & \text{if } L < m, \end{cases}$$

where the summation is over integers $0 \leq a_i \leq 2^{L-1}$ $(i = 1, \ldots, m-L)$, $0 \leq b \leq 2^L$, such that $n - k = 2^{m-L}a_{m-L} + \cdots + 2a_1 + b$.

Proof Let us consider the proof in two cases: $L \geq m$ and $L < m$.
First assume that $L \geq m$. From Proposition 2 we know the factorization of cyclotomic polynomials and hence we have

$$\begin{aligned} x^n - 1 &= x^{2^m} - 1 \\ &= Q_{2^m}(x)Q_{2^{m-1}}(x)\cdots Q_1(x) \\ &= \prod_{\zeta \in \Omega(2^m)} (x-\zeta) \prod_{\zeta \in \Omega(2^{m-1})} (x-\zeta) \cdots \prod_{\zeta \in \Omega(1)} (x-\zeta) \\ &= \prod_{\zeta \in R(2^m)} (x-\zeta) = \prod_{\zeta \in R(n)} (x-\zeta). \end{aligned}$$

In the last step, we use the fact that $R(n) = R(2^m) = \cup_{i=0}^{m} \Omega(2^i)$; that is, the union of all primitive 2^ith $(i = 0, \ldots, m)$ roots of unity gives the set of all 2^mth root of unity. Therefore, we see that $x^n - 1$ splits in $\mathbb{F}_q$ in this case. Now assume that $\{\zeta_1, \ldots, \zeta_{n-k}\} \subseteq R(2^m)$. Then the number of k-normal elements is given as follows:

$$\begin{aligned} f(k) &= \sum_{\substack{h \mid x^n - 1 \\ \deg h = n-k \\ h - \text{monic}}} \Phi_q(h) = \binom{n}{n-k} \Phi_q((x-\zeta_1)(x-\zeta_2)\cdots(x-\zeta_{n-k})) \\ &= \binom{n}{n-k} \Phi_q(x-\zeta_1)\Phi_q(x-\zeta_2)\cdots\Phi_q(x-\zeta_{n-k}) \\ &= \binom{n}{n-k}(q-1)^{n-k} = \binom{n}{k}(q-1)^{n-k}, \end{aligned}$$

which completes the first part of the proof.

Now we consider the case $L < m$. Again from Proposition 2 we have $Q_{2^i}(x) = \prod_{\zeta \in \Omega(2^i)}(x-\zeta)$, for $i =$

$0,1,\ldots,L$, and $Q_{2^i}(x)=\prod_{\zeta\in\Omega(2^L)}(x^{2^{i-L}}-\zeta)$, for $i=L+1,\ldots,m$. Hence, the factorization of x^n-1 becomes

$$\begin{aligned} x^{2^m}-1 &= Q_{2^m}(x)\cdots Q_{2^{L+1}}(x)Q_{2^L}(x)Q_{2^{L-1}}(x)\cdots Q_1(x) \\ &= \prod_{\zeta\in\Omega(2^L)}\left(x^{2^{m-L}}-\zeta\right)\cdots\prod_{\zeta\in\Omega(2^L)}(x^2-\zeta) \\ &\quad\times\prod_{\zeta\in\Omega(2^L)}(x-\zeta)\prod_{\zeta\in\Omega(2^{L-1})}(x-\zeta)\cdots\prod_{\zeta\in\Omega(1)}(x-\zeta) \\ &= \prod_{\zeta\in\Omega(2^L)}\left(x^{2^{m-L}}-\zeta\right)\cdots\prod_{\zeta\in\Omega(2^L)}(x^2-\zeta)\prod_{\zeta\in R(2^L)}(x-\zeta). \end{aligned} \tag{3}$$

Now that we know the factorization of x^n-1 from (3), we can assume that a divisor $h(x)$ of x^n-1 is of the form

$$h(x)=\prod_{\substack{\zeta\in A_{m-L}\subseteq\Omega(2^L)\\ |A_{m-L}|=a_{m-L}}}\left(x^{2^{m-L}}-\zeta\right)\cdots\prod_{\substack{\zeta\in A_1\subseteq\Omega(2^L)\\ |A_1|=a_1}}(x^2-\zeta)\prod_{\substack{\zeta\in A\subseteq R(2^L)\\ |A|=b}}(x-\zeta)$$

where the integers $a_i,\ i=1,\ldots,m-L$ and b comes from the the degree of $h(x)$, i.e.

$$n-k=2^{m-L}a_{m-L}+\cdots+2a_1+b$$

and

$$0\le b\le 2^L,\ 0\le a_i\le 2^{L-1},\quad i=1,\ldots,m-L.$$

Here we note that $A\subseteq R(2^L)$ and $|R(2^L)|=2^L$, which gives $|A|=b\le 2^L$. Similarly, for $i\in\{1,\ldots,m-L\}$ we have $A_i\subseteq\Omega(2^L)$ and $|\Omega(2^L)|=2^L-2^{L-1}=2^{L-1}$, which gives $|A_i|=a_i\le 2^{L-1}$. Then the Euler phi value

of $h(x)$ is evaluated as follows:

$$\begin{aligned}
\Phi_q(h(x)) &= \Phi_q\Bigg(\prod_{\substack{\zeta \in A_{m-L} \subseteq \Omega(2^L) \\ |A_{m-L}| = a_{m-L}}} \left(x^{2^{m-L}} - \zeta\right) \cdots \prod_{\substack{\zeta \in A_1 \subseteq \Omega(2^L) \\ |A_1| = a_1}} \left(x^2 - \zeta\right) \\
&\quad \times \prod_{\substack{\zeta \in A \subseteq R(2^L) \\ |A| = b}} (x - \zeta) \Bigg) \\
&= \prod_{\substack{\zeta \in A_{m-L} \subseteq \Omega(2^L) \\ |A_{m-L}| = a_{m-L}}} \Phi_q\left(x^{2^{m-L}} - \zeta\right) \cdots \prod_{\substack{\zeta \in A_1 \subseteq \Omega(2^L) \\ |A_1| = a_1}} \Phi_q\left(x^2 - \zeta\right) \\
&\quad \times \prod_{\substack{\zeta \in A \subseteq R(2^L) \\ |A| = b}} \Phi_q(x - \zeta) \\
&= \prod_{\substack{\zeta \in A_{m-L} \subseteq \Omega(2^L) \\ |A_{m-L}| = a_{m-L}}} \left(q^{2^{m-L}} - 1\right) \cdots \prod_{\substack{\zeta \in A_1 \subseteq \Omega(2^L) \\ |A_1| = a_1}} \left(q^2 - 1\right) \\
&\quad \times \prod_{\substack{\zeta \in A \subseteq R(2^L) \\ |A| = b}} (q - 1) \\
&= \left(q^{2^{m-L}} - 1\right)^{a_{m-L}} \cdots \left(q^2 - 1\right)^{a_1} (q - 1)^b . \qquad (4)
\end{aligned}$$

Here note that for fixed $a_{m-L}, \ldots, a_1$ and b, the number of monic $h(x)$ with degree $n-k$ is

$$\binom{2^{L-1}}{a_{m-L}} \cdots \binom{2^{L-1}}{a_1} \binom{2^L}{b} \qquad (5)$$

since $|\Omega(2^L)| = 2^L - 2^{L-1} = 2^{L-1}$, $|R(2^L)| = 2^L$, and for each different selection of the root of unity we obtain a different polynomial $h(x)$ having degree $n-k$. Therefore, applying (4) to the formula (1) and using (5) we find the number of k-normal elements as

$$\begin{aligned}
f(k) &= \sum_{h \mid x^n - 1,\ h - \text{monic},\ \deg h = n-k} \Phi_q(h) \\
&= \sum \left[\prod_{i=1}^{m-L} \binom{2^{L-1}}{a_i} (q^{2^i} - 1)^{a_i} \right] \binom{2^L}{b} (q-1)^b,
\end{aligned}$$

where the last summation is over $0 \le a_i \le 2^{L-1}$ $(i = 1, \ldots, m-L)$, $0 \le b \le 2^L$ satisfying $n - k = 2^{m-L} a_{m-L} + \cdots + 2a_1 + b$. This completes the proof. □

As an immediate consequence of Theorem 4 we have the following result on the number of 0-normal and 1-normal elements. Note that for each of these cases the Diophantine equation in Theorem 4 has a unique solution.

Corollary 1 *Let $q \equiv 1 \pmod 4$ be a prime power and $n = 2^m$ for some positive integer m. Then the number of 0-normal and 1-normal elements is given as follows:*

$$f(0) = \begin{cases} (q-1)^n, & \text{if } L \geq m, \\ (q^{2^{m-L}}-1)^a \cdots (q^2-1)^a (q-1)^b, & \text{if } L < m, \end{cases}$$

$$f(1) = \begin{cases} n(q-1)^{n-1}, & \text{if } L \geq m, \\ 2^L (q^{2^{m-L}}-1)^a \cdots (q^2-1)^a (q-1)^{b-1}, & \text{if } L < m, \end{cases}$$

where $L = v_2(q-1)$, $a = 2^{L-1}$, and $b = 2^L$. By taking the ratio we get

$$\frac{f(0)}{f(1)} = \begin{cases} \frac{q-1}{n}, & \text{if } L \geq m, \\ \frac{q-1}{2^L}, & \text{if } L < m. \end{cases}$$

Remark 2 *From Corollary 1 we see that $f(1) = f(0)$ whenever $q-1 = n$ and $L \geq m$ or $q-1 = 2^L$ and $L < m$. Furthermore, we know that there exist primitive normal elements for all finite fields. This suggests that it is highly probable that there exist primitive 1-normal elements for all finite fields $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that $q-1 = n$ and $L \geq m$ or $q-1 = 2^L$ and $L < m$.*

Now we present numerical examples related to our formulas in Theorem 4.

Example 1 (Case 1) *Let $q = 9$ and $n = 8$. Then we have $L = v_2(q-1) = 3$ and $m = 3$. In this case the formula for the number of k-normal elements becomes*

$$f(k) = \binom{8}{k} 8^{8-k}.$$

In Table 1 we give the number of k-normal elements evaluated in Magma [2]. They are consistent with the formula of Theorem 4.

Table 1. Number of k-normal elements of $\mathbb{F}_{9^8}$ over $\mathbb{F}_9$.

k	0	1	2	3	4	5	6	7
$f(k)$	16777216	16777216	7340032	1835008	286720	28672	1792	64

Example 2 (Case 2) *Now let us consider the finite field $\mathbb{F}_{5^8}$ over $\mathbb{F}_5$. In this case we have $q-1 = 5-1 = 4$ and $n = 2^m = 8$, and hence $L = v_2(q-1) = 2$ and $m = 3$. Then from Theorem 4 we have*

$$f(k) = \sum \binom{2}{a_1} \binom{4}{b} (q^2-1)^{a_1} (q-1)^b,$$

where $0 \leq a_1 \leq 2, 0 \leq b \leq 4$, and $8-k = 2a_1 + b$. We can compute $f(k)$ depending on the value of k and the solutions of the Diophantine equation given in Table 2.

Table 2. Integer solutions (a_1, b) of the equation $8 - k = 2a_1 + b$ where $0 \le a_1 \le 2, 0 \le b \le 4$.

$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$
(2,4)	(2,3)	(2,2) (1,4)	(2,1) (1,3)	(2,0),(1,2) (0,4)	(1,1) (0,3)	(1,0) (0,2)	(0,1)

Thus, the number of k-normal elements is as follows:

$$f(0) = (q^2-1)^2(q-1)^4,\ f(1) = 4(q^2-1)^2(q-1)^3,$$

$$f(2) = 6(q^2-1)^2(q-1)^2 + 2(q^2-1)(q-1)^4,\ f(3) = 4(q^2-1)^2(q-1) + 8(q^2-1)(q-1)^3,$$

$$f(4) = (q^2-1)^2 + 12(q^2-1)(q-1)^2 + (q-1)^4,$$

$$f(5) = 8(q^2-1)(q-1) + 4(q-1)^3,\ f(6) = 2(q^2-1) + 6(q-1)^2,\ f(7) = 4(q-1).$$

These values are consistent with the values computed with Magma given in Table 3.

Table 3. Number of k-normal elements of $\mathbb{F}_{5^8}$ over $\mathbb{F}_5$.

k	0	1	2	3	4	5	6	7
$f(k)$	147456	147456	67584	21504	5440	1024	144	16

For any positive integer $m \ge 2$ and for each $\zeta \in \Omega(2^m)$ we know that ζ^{-1} is also in $\Omega(2^m)$. Now assume that $\Omega(2^m) = \{\zeta_1, \zeta_1^{-1}, \zeta_2, \zeta_2^{-1}, \dots, \zeta_{2^{m-2}}, \zeta_{2^{m-2}}^{-1}\}$ and define $\Omega'(2^m) = \{\zeta_1, \zeta_2, \dots, \zeta_{2^{m-2}}\}$. We will use this set Ω' in the Proposition 3. The complete factorization of $x^{2^m}+1$ over $\mathbb{F}_q$ with $q \equiv 3 \pmod 4$ is given in [10, Theorem 1]. Using this factorization, we have the following result.

Proposition 3 *[10] Let $q \equiv 3 \pmod 4$ be a prime power, $n = 2^m$ for some positive integer m, and $L = v_2(q+1)$, i.e. $L \ge 2$. Then the cyclotomic polynomial Q_{2^m} factorizes over $\mathbb{F}_q$ as*

$$Q_{2^m}(x) = \begin{cases} \prod\limits_{\zeta \in \Omega'(2^m)} (x^2 + (\zeta + \zeta^{-1})x + 1), & \text{if } 2 \le m \le L, \\ \prod\limits_{\zeta \in \Omega(2^L)} (x^{2^{m-L}} + (\zeta - \zeta^{-1})x^{2^{m-L-1}} - 1), & \text{if } m > L. \end{cases}$$

Here we remark that the $m > L$ case of this result comes from the proof of [9, Theorem 3.76], which uses Waring's formula. Furthermore, this result was proven in [10, Theorem 1] by considering the polynomial factorization over the extension field $\mathbb{F}_{q^2}$ instead of $\mathbb{F}_q$. Combining Proposition 3 with Theorem 2, we again obtain the following explicit result on the number of k-normal elements. Here we assume that $\binom{r}{s} = 0$ if $r < s$.

Theorem 5 *Let $q \equiv 3 \pmod 4$ be a prime power and $n = 2^m$ for some positive integer m. Let $L = v_2(q+1)$, i.e. $L \ge 2$, $n_0 = n/2$, and $k_0 = \lfloor k/2 \rfloor$. Then the number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is given as follows:*

$$f(k) = \begin{cases} \binom{n_0-1}{n_0-1-k_0}(q^2-1)^{n_0-1-k_0}(q-1)^2 + \binom{n_0-1}{n_0-k_0}(q^2-1)^{n_0-k_0}, & \text{if } k \text{ is even}, \\ 2\binom{n_0-1}{n_0-1-k_0}(q^2-1)^{n_0-1-k_0}(q-1), & \text{if } k \text{ is odd}, \end{cases}$$

when $m \leq L$, *and for* $m > L$ *we have*

$$f(k) = \sum \left[\prod_{i=2}^{m-L} \binom{2^{L-1}}{a_i} (q^{2^i} - 1)^{a_i} \right] \binom{2^L - 1}{a} \binom{2}{b} (q^2 - 1)^a (q-1)^b,$$

where the sum is over $0 \leq b \leq 2$, $0 \leq a \leq 2^L - 1$, *and* $0 \leq a_i \leq 2^{L-1}$, $i = 2, \ldots, m-L$ *such that* $n - k = 2^{m-L} a_{m-L} + \cdots + 2^2 a_2 + 2a + b$.

Proof Here we omit the proof, which is very similar to the proof of Theorem 4. Note that in the proof of Theorem 4 the factors of $x^n - 1$ were linear and factors of the form $x^{2^{m-L}} - \zeta$ (see Proposition 2). Instead of these factors, here we deal with 2 linear factors $x-1$, $x+1$, $2^L - 1$ quadratic factors, and the other factors having degree 2^i $(i = 2, \ldots, m-L)$ of the polynomial $x^n - 1$ given in Proposition 3. □

Example 3 (Case 1) *Let* $q = 7$ *and* $n = 8$, *and then we have* $L = v_2(q+1) = 3$ *and* $m = 3$. *In this case the formula for the number of* k*-normal elements becomes*

$$f(k) = \begin{cases} \binom{3}{3-k_0}(q^2-1)^{3-k_0}(q-1)^2 + \binom{3}{4-k_0}(q^2-1)^{4-k_0}, & \text{is } k \text{ is even} \\ 2\binom{3}{3-k_0}(q^2-1)^{3-k_0}(q-1), & \text{if } k \text{ is odd,} \end{cases}$$

where $k_0 = \lfloor k/2 \rfloor$. *By counting all* k*-normal elements by Magma [2] we get Table 4, which is consistent with the formula given in Theorem 5.*

Table 4. Number of k-normal elements of $\mathbb{F}_{7^6}$ over $\mathbb{F}_7$.

k	0	1	2	3	4	5	6	7
$f(k)$	3981312	1327104	359424	82944	12096	1728	180	12

Example 4 (Case 2) *Now let us consider the finite field* $\mathbb{F}_{3^{16}}$ *over* $\mathbb{F}_3$. *In this case we have* $q+1 = 3+1 = 4$ *and* $n = 2^m = 16$, *and hence* $L = v_2(q+1) = 2$ *and* $m = 4$. *Then from Theorem 5 we have*

$$f(k) = \sum \binom{2}{a_2} \binom{3}{a} \binom{2}{b} (q^4-1)^{a_2} (q^2-1)^a (q-1)^b,$$

where $0 \leq a_2 \leq 2$, $0 \leq a \leq 3$, $0 \leq b \leq 2$, *and* $16 - k = 4a_2 + 2a + b$. *We can compute* $f(k)$ *depending on the value of* k. *Solutions* (a_2, a, b) *of the Diophantine equation* $0 \leq a_2 \leq 2$, $0 \leq a \leq 3$, $0 \leq b \leq 2$, *and* $16 - k = 4a_2 + 2a + b$ *are given in Table 5.*
By counting all k*-normal elements by Magma [2] we get Table 6, consistent with the formula given in Theorem 5.*

3.2. Case $n = 3^m$

Recently, the authors in [17] studied the factorization of cyclotomic polynomials for some cases. Using these results we will give an explicit formula for the number of k-normal elements. For the sake of completeness we

Table 5. Positive integer solutions (a_2, a, b) of the equation $16 - k = 4a_2 + 2a + b$.

$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$
(2,3,2)	(2,3,1)	(2,3,0) (2,2,2)	(2,2,1)	(2,2,0) (2,1,2) (1,3,2)	(2,1,1) (1,3,1)	(2,1,0) (2,0,2) (1,3,0) (1,2,2)	(2,0,1) (1,2,1)

$k=8$	$k=9$	$k=10$	$k=11$	$k=12$	$k=13$	$k=14$	$k=15$
(2,0,0) (1,2,0) (1,1,2) (0,3,2)	(1,1,1) (0,3,1)	(1,1,0) (1,0,2) (0,3,0) (0,2,2)	(1,0,1) (0,2,1)	(1,0,0) (0,2,0) (0,1,2)	(0,1,1)	(0,1,0) (0,0,2)	(0,0,1)

Table 6. Number of k-normal elements of $\mathbb{F}_{3^{16}}$ over $\mathbb{F}_3$.

$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$
13107200	13107200	8192000	4915200	2170880	942080	384000	148480

$k=8$	$k=9$	$k=10$	$k=11$	$k=12$	$k=13$	$k=14$	$k=15$
54528	17408	5760	1408	448	96	28	4

will state the result of [17] below. Let ζ be an element in some extension field of $\mathbb{F}_q$ and define $g_n(\zeta, x)$ as follows:

$$g_n(\zeta, x) = x^{2n} - (\zeta + \zeta^{-1})x^n + 1.$$

We use this polynomial in the following proposition.

Proposition 4 *[17] For a positive integer m the factorization of cyclotomic polynomial $Q_{3^m}(x)$ over $\mathbb{F}_q$ is given as follows:*

If $q \equiv 1 \pmod 3$, then when $m \leq v_3(q-1)$,

$$Q_{3^m}(x) = \prod_{\zeta \in \Omega(3^m)} (x - \zeta),$$

and when $m > v_3(q-1)$,

$$Q_{3^m}(x) = \prod_{\zeta \in \Omega(3^{v_3(q-1)})} \left(x^{3^{m-v_3(q-1)}} - \zeta\right).$$

If $q \equiv 2 \pmod 3$, then when $m \leq v_3(q+1)$,

$$Q_{3^m}(x) = \prod_{\zeta \in S(3^m)} g_1(\zeta, x),$$

and when $m > v_3(q+1)$,

$$Q_{3^m}(x) = \prod_{\zeta \in S(3^{v_3(q+1)})} g_{3^{m-v_3(q+1)}}(\zeta, x).$$

Combining Proposition 4 with Theorem 2, we obtain the number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ for $n = 3^m$. In this case we have two results depending on the value of $q \pmod 3$. For $q \equiv 1 \pmod 3$ the factorization of $Q_{3^m}(x)$ in Proposition 4 is very similar to the factorization of $Q_{2^m}(x)$ in Proposition 2. Furthermore, for the case $q \equiv 2 \pmod 3$ the factorization of $Q_{3^m}(x)$ in Proposition 4 is similar to the factorization of $Q_{2^m}(x)$ in Proposition 3. Therefore, we state our results without the proof, which is very similar to the proof given in the previous section.

Theorem 6 *Let $q \equiv 1 \pmod 3$ and $n = 3^m$ for some positive integer m. Then the number of k-normal elements is given by*

$$f(k) = \begin{cases} \binom{n}{k}(q-1)^{n-k}, & \text{if } L \geq m, \\ \sum \left[\prod_{i=1}^{m-L} \binom{2 \cdot 3^{L-1}}{a_i} (q^{3^i}-1)^{a_i} \right] \binom{3^L}{b} (q-1)^b, & \text{if } L < m, \end{cases}$$

where $L = v_3(q-1)$ and the sum in the last equation is over integers $a_{m-L}, \ldots, a_1, b$ such that $0 \leq a_i \leq 2 \cdot 3^{L-1}$ $(i = 1, \ldots, m-L)$, $0 \leq b \leq 3^L$, and $n - k = 3^{m-L}a_{m-L} + \cdots + 3a_1 + b$.

Before giving our next result we present some examples for the results in Theorem 6. In these examples we see that the summation given in terms of Diophantine equations is easy to compute. Results given in these examples are verified by evaluating k-normal elements in Magma [2].

Example 5 (Case 1) *Let us consider the finite field $\mathbb{F}_{19^3}$ over $\mathbb{F}_{19}$. In this case $m = 1$ and $v_3(q-1) = v_3(18) = 2$. Then from Theorem 6 we know that the number of k-normal elements equals $f(k) = \binom{n}{k}(q-1)^{n-k} = \binom{3}{k}18^{n-k}$ for $k = 0, 1, 2$. Evaluating with Magma we find that the number of k-normal elements $f(k)$ is given as in Table 7, and this is consistent with the formula given in Theorem 6.*

Table 7. Number of k-normal elements of $\mathbb{F}_{19^3}$ over $\mathbb{F}_{19}$.

k	0	1	2
$f(k)$	5832	972	54

Example 6 (Case 2) *Now let us consider the finite field $\mathbb{F}_{4^9}$ over $\mathbb{F}_4$. In this case we have $q - 1 = 3$ and $3^m = 9$, and hence $L = v_3(q-1) = 1$ and $m = 2$. Then from Theorem 6 we have*

$$f(k) = \sum \binom{2}{a_1} \binom{3}{b} (q^3-1)^{a_1} (q-1)^b,$$

where $0 \leq a_1 \leq 2, 0 \leq b \leq 3$, and $9 - k = 3a_1 + b$. We can compute $f(k)$ depending on the value of k and the solutions of the Diophantine equation given in Table 8.

Table 8. Positive integer solutions (a_1, b) of the equation $9 - k = 3a_1 + b$ where $0 \le a_1 \le 2$ and $0 \le b \le 3$.

$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	$k=8$
(2,3)	(2,2)	(2,1)	(2,0) (1,3)	(1,2)	(1,1)	(1,0) (0,3)	(0,2)	(0,1)

The number of k-normal elements is:

$$f(0) = (q^3-1)^2(q-1)^3,\ f(1) = 3(q^3-1)^2(q-1)^2,\ f(2) = 3(q^3-1)^2(q-1),$$
$$f(3) = (q^3-1)^2 + 2(q^3-1)(q-1)^3,\ f(4) = 6(q^3-1)(q-1)^2,$$
$$f(5) = 6(q^3-1)(q-1),\ f(6) = 2(q^3-1) + (q-1)^3,$$
$$f(7) = 3(q-1)^2,\ f(8) = 3(q-1).$$

These values are consistent with the values computed with Magma given in Table 9.

Table 9. Number of k-normal elements of $\mathbb{F}_{4^9}$ over $\mathbb{F}_4$.

k	0	1	2	3	4	5	6	7	8
$f(k)$	107163	107163	35721	7371	3402	1134	153	27	9

Example 7 *In this example we will consider the finite field $\mathbb{F}_{109^{3^6}}$ over $\mathbb{F}_{109}$. In this case we have $q-1 = 4\cdot 3^3$ and $3^m = 3^6$, and hence $L = v_3(q-1) = 3$ and $m = 6$. Then from Theorem 6 we have*

$$f(k) = \sum \binom{18}{a_1}\binom{18}{a_2}\binom{18}{a_3}\binom{27}{b}(q^{3^3}-1)^{a_3}(q^{3^2}-1)^{a_2}(q^3-1)^{a_1}(q-1)^b,$$

where $0 \le a_1, a_2, a_3 \le 18, 0 \le b \le 27$, and $729 - k = 27a_3 + 9a_2 + 3a_1 + b$. We can easily compute $f(k)$ depending on the value of k.

For instance, for $k = 0$ our Diophantine equation becomes $729 = 27a_3 + 9a_2 + 3a_1 + b$, which has unique solution $(a_3, a_2, a_1, b) = (18, 18, 18, 27)$. Hence, the number of 0-normal elements or normal elements is $f(0) = (q^{3^3}-1)^{18}(q^{3^2}-1)^{18}(q^3-1)^{18}(q-1)^{27} \approx 2^{4933.65} \approx q^{728.947}$ where $q^n = q^{729}$. Note that this number is more than half of $q^n - 1 \approx 2^{4934}$.

Similarly, for $k = 1$ our Diophantine equation becomes $728 = 27a_3 + 9a_2 + 3a_1 + b$, which has unique solution $(a_3, a_2, a_1, b) = (18, 18, 18, 26)$. Hence, the number of 1-normal elements is $f(1) = 27(q^{3^3}-1)^{18}(q^{3^2}-1)^{18}(q^3-1)^{18}(q-1)^{26} \approx 2^{4931.647}$.

For $k = 2$ we get the equation $727 = 27a_3 + 9a_2 + 3a_1 + b$, which has unique solution $(a_3, a_2, a_1, b) = (18, 18, 18, 25)$. Hence, the number of 2-normal elements is $f(2) = 351(q^{3^3}-1)^{18}(q^{3^2}-1)^{18}(q^3-1)^{18}(q-1)^{25} \approx 2^{4928.593}$.

Lastly, for $k = 3$, we obtain the equation $726 = 27a_3 + 9a_2 + 3a_1 + b$, which has two solutions $(a_3, a_2, a_1, b) \in \{(18, 18, 18, 24), (18, 18, 17, 27)\}$. Hence, the number of 3-normal elements is $f(3) = 2925(q^{3^3}-1)^{18}(q^{3^2}-1)^{18}(q^3-1)^{18}(q-1)^{24} + 18(q^{3^3}-1)^{18}(q^{3^2}-1)^{18}(q^3-1)^{17}(q-1)^{27} \approx 2^{4924.906}$.

By a similar argument as in Corollary 1, we have the following result using Theorem 6.

Corollary 2 *Let $q \equiv 1 \pmod 3$ be a prime power and $n = 3^m$ for some positive integer m. Then the ratio of the number of normal elements and 1-normal elements is*

$$\frac{f(0)}{f(1)} = \begin{cases} \frac{q-1}{n}, & \text{if } L \geq m, \\ \frac{q-1}{3^L}, & \text{if } L < m. \end{cases}$$

Again by combining Proposition 4 with Theorem 2, we obtain the number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ where $q \equiv 2 \pmod 3$ and $n = 3^m$.

Theorem 7 *Let $q \equiv 2 \pmod 3$ and $n = 3^m$ for some positive integer m. Then if $v_3(q+1) \geq m$, the number of k-normal elements is given by*

$$f(k) = \begin{cases} \binom{(n-1)/2}{(n-k-1)/2}(q^2-1)^{(n-k-1)/2}(q-1), & \text{if } k \text{ is even}, \\ \binom{(n-1)/2}{(n-k)/2}(q^2-1)^{(n-k)/2}, & \text{if } k \text{ is odd}, \end{cases}$$

and if $L = v_3(q+1) < m$ we have

$$f(k) = \sum \left[\prod_{i=1}^{m-L} \binom{3^{L-1}}{a_i} (q^{2\cdot 3^i}-1)^{a_i} \right] \binom{\frac{3^L-1}{2}}{a} (q^2-1)^a (q-1)^b,$$

where the sum is over $0 \leq a \leq (3^L-1)/2$, $0 \leq b \leq 1$, and $0 \leq a_i \leq 3^{L-1}$, $i = 1, \ldots, m-L$ such that $n - k = 2 \cdot 3^{m-L} a_{m-L} + \cdots + 2 \cdot 3a_1 + 2a + b$.

Now we present examples for Theorem 7 for the two cases separately.

Example 8 (Case 1) *Let $q = 53$ and $n = 3^2$. In this case we have $L = v_3(q+1) = 3$ and $m = 2$. Hence, the formula in Theorem 7 becomes*

$$f(k) = \begin{cases} \binom{4}{(8-k)/2}(53^2-1)^{(8-k)/2} \cdot 8, & \text{if } k \text{ is even}, \\ \binom{4}{(9-k)/2}(53^2-1)^{(9-k)/2}, & \text{if } k \text{ is odd}. \end{cases}$$

From this formula we get the number of k-normal elements given in Table 10.

Example 9 (Case 2) *Let $q = 17$ and $n = 3^3$. We get $L = v_3(q+1) = 2$ and $m = 3$. By the second part of Theorem 7 we have*

$$f(k) = \sum \binom{3}{a_1} \binom{4}{a} (17^{2\cdot 3}-1)^{a_1} (17^2-1)^a 16^b,$$

where the sum is over $0 \leq a \leq 4$, $0 \leq b \leq 1$, and $0 \leq a_1 \leq 3$, such that $9 - k = 2 \cdot 3a_1 + 2a + b$. Positive solutions (a_1, a, b) of this Diophantine equation are given in Table 11.

Table 10. Number of k-normal elements of $\mathbb{F}_{53^9}$ over $\mathbb{F}_{53}$.

k	0	1	2	3	4
$f(k)$	$2^{26}3^{24}13^9$	$2^{24}3^{24}13^8$	$2^{22}3^{18}13^7$	$2^{20}3^{18}13^6$	$2^{15}3^{13}13^5$

k	5	6	7	8
$f(k)$	$2^{13}3^{13}13^4$	$2^{10}3^6 13^3$	$2^8 3^6 13^2$	$2^2 13$

Table 11. Positive integer solutions (a_1, a, b) of the equation $9-k = 3a_1 + 2a + b$ where $0 \le a \le 4$, $0 \le b \le 1$, and $0 \le a_1 \le 3$.

$k=0$	$k=1$	$k=2$	$k=3$	$k=4$
(1,1,1) (0,4,1)	(1,1,0) (0,4,0)	(1,0,1) (0,3,1)	(1,0,0) (0,3,0)	(0,2,1)

$k=5$	$k=6$	$k=7$	$k=8$
(0,2,0)	(0,1,1)	(0,1,0)	(0,0,1)

Therefore, the number of k-normal elements is:

$$f(0) = 12(17^{2\cdot 3}-1)(17^2-1)16 + (17^2-1)^4 16,$$
$$f(1) = 12(17^{2\cdot 3}-1)(17^2-1) + (17^2-1)^4,$$
$$\vdots$$
$$f(8) = 16.$$

3.3. Case $n = p^m$

Proposition 4 was partially generalized by taking arbitrary odd prime p instead of 3 [17]. First we state this result for completeness and then find the number of k-normal elements in this case.

Proposition 5 *[17] Given a prime power q and an odd prime p such that $q \equiv 1 \pmod p$, let $n = p^m$ for some positive integer m and $L = v_p(q-1)$. Then the cyclotomic polynomial $Q_n(x)$ factorizes over $\mathbb{F}_q$ into irreducibles as follows:*

$$Q_n(x) = \begin{cases} \prod_{\zeta \in \Omega(n)} (x-\zeta), & \text{if } L \ge m, \\ \prod_{\zeta \in \Omega(p^L)} (x^{p^{m-L}} - \zeta), & \text{if } L < m. \end{cases}$$

Now using Proposition 5 we can extend our Theorem 4 and Theorem 6 to arbitrary characteristics p instead of 2 and 3. We will state it without the proof, since its proof is similar to the proof of Theorem 4.

Theorem 8 *Given a prime power q and an odd prime p such that $q \equiv 1 \pmod p$, let $n = p^m$ for some positive integer m and $L = v_p(q-1)$. Then the number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is given as*

follows:

$$f(k)=\begin{cases}\binom{n}{k}(q-1)^{n-k}, & \text{if } L\geq m,\\ \sum\left[\prod_{i=1}^{m-L}\binom{(p-1)p^{L-1}}{a_i}(q^{p^i}-1)^{a_i}\right]\binom{p^L}{b}(q-1)^b, & \text{if } L<m,\end{cases}$$

where the summation is over integers $0\leq a_i\leq (p-1)p^{L-1}$, $0\leq b\leq p^L$ *such that* $n-k=p^{m-L}a_{m-L}+\cdots+pa_1+b$.

Example 10 *Let* $q=251$ *and* $n=5^3$. *Then we have* $L=v_5(q-1)=3$ *and* $m=3$. *In this case the formula for the number of* k*-normal elements becomes*

$$f(k)=\binom{125}{k}250^{125-k}.$$

Example 11 *Let* $q=11$ *and* $n=5^2$. *Then we have* $L=v_5(q-1)=1$ *and* $m=2$. *In this case the formula for the number of* k*-normal elements becomes*

$$f(k)=\sum\binom{4}{a_1}\binom{5}{b}(11^5-1)^{a_1}10^b,$$

where the summation is over integers $0\leq a_1\leq 4$, $0\leq b\leq 5$ *such that* $25-k=5a_1+b$. *Taking* $k=0$ *we have unique solution* $(a_1,b)=(4,5)$ *and hence the number of 0-normal (normal) elements equals* $f(0)=(11^5-1)^4 10^5$. *Similarly, for* $k=1$, *we have unique solution* $(a_1,b)=(4,4)$ *and hence the number of 1-normal elements equals* $f(1)=5(11^5-1)^4 10^4$.

3.4. Case $n=2^m\cdot r$

In this section we consider the number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ where $n=2^m\cdot r$ for some odd prime r. In [6], using [9, Theorem 2.47, Theorem 3.35], the general forms of the factors of the cyclotomic polynomials were given depending on the values of $q\equiv\pm 1 \mod r$. Now we first present this factorization and then, combining this result, Proposition 2, and Proposition 3 with Theorem 2, we give our results.

Proposition 6 *[6] Let* $L=v_2(q^2-1)$.

1. *Suppose* $q\equiv 1 \mod r$. *Then:*
   (a) *For* $0\leq m\leq v_2(q-1)$, $Q_{2^m r}(x)$ *is a product of linear factors.*
   (b) *For* $v_2(q-1)<m\leq L$, $Q_{2^m r}$ *is a product of irreducible quadratic polynomials.*
   (c) *For* $m>L$, $Q_{2^m r}(x)=\prod f_i(x^{2^{m-L}})$, *where* $Q_{2^L r}=\prod f_i(x)$.
2. *Suppose* $q\equiv -1 \mod r$. *Then:*
   (a) *For* $0\leq m\leq L$, $Q_{2^m r}$ *is a product of irreducible quadratic factors.*
   (b) *For* $m>L$, $Q_{2^m r}(x)=\prod f_i(x^{2^{m-L}})$, *where* $Q_{2^L r}(x)=\prod f_i(x)$.

Theorem 9 *Let $q \equiv 1 \pmod r$ be a prime power and $n = 2^m r$ for some positive integer m and an odd prime r. Assume that $L_2 = v_2(q-1) \geq m$. Then the number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is*

$$f(k) = \binom{n}{k}(q-1)^{n-k}.$$

Remark 3 *In Theorem 9 we only considered $q \equiv 1 \pmod r$ and $m \leq v_2(q-1)$. In other cases due to the degrees of the factors of $x^n - 1$ there are many cases to be considered, and hence for these cases the formulas will not be that simple, which are not included here.*

4. Conclusion

In this paper, we give positive answers to Problem 6.1. in [7] by obtaining explicit formulas for the number of k-normal elements over finite fields under some conditions. In some cases, we show how to obtain explicit formulas requiring solutions of some linear Diophantine equations, which can be easily solved depending on values of n and k. For some special values of n and k these numbers can be evaluated explicitly.

Lastly, [13] deserves comment since it also considered the existence of k-normal elements over finite fields. The main problem considered in [13] is the existence of primitive k-normal elements over finite fields, which is not directly related to our main focus. On the other hand, [13, Section 5.2] has results that appear similar to ours. In fact, there is a little overlap, proved independently. The cases $v_2(q-1) \geq m$ in Theorem 4 and $v_3(q-1) \geq m$ in Theorem 6 were also obtained in [13, Corollary 5.7]. Furthermore, [13, Example 5.6] is equivalent to our Proposition 1.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments.

References

[1] Blake IF, Gao S, Mullin RC. Explicit factorization of $x^{2^k}+1$ over $\mathbb{F}_p$ with prime $p \equiv 3 \pmod 4$. Appl Algebra Eng Commun Comput 1993; 4: 89-94.

[2] Bosma W, Cannon J, Playoust C. The Magma algebra system. I. The user language. J Symb Comput 1997; 24: 235-265.

[3] Chen B, Li L, Tuerhong R. Explicit factorization of $x^{2^m p^n}-1$ over a finite field. Finite Fields Appl 2013; 24: 95-104.

[4] Dahab R, Hankerson D, Hu F, Long M, López J, Menezes A. Software multiplication using gaussian normal bases. IEEE T Comput 2006; 55: 974-984.

[5] Devi OR, Chanu TR. Explicit factorization of cyclotomic polynomials over finite fields. Int J Pure Appl Math 2013; 86: 585-592.

[6] Fitzgerald RW, Yucas JL. Explicit factorizations of cyclotomic and dickson polynomials over finite fields. In: International Workshop on the Arithmetic of Finite Fields, 2007.

[7] Huczynska S, Mullen GL, Panario D, Thomson D. Existence and properties of k-normal elements over finite fields. Finite Fields Appl 2013; 24: 170-183.

[8] Kızılkale C, Eğecioğlu Ö, Koç Ç. A matrix decomposition method for optimal normal basis multiplication. IEEE T Comput 2016; 65: 3239-3250.

[9] Lidl R, Niederreiter H. Finite Fields. 2nd ed. Cambridge, UK: Cambridge University Press, 1997.

[10] Meyn H. Factorization of the cyclotomic polynomial $x^{2^n}+1$ over finite fields. Finite Fields Appl 1996; 2: 439-442.

[11] Mullin RC, Onyszchuk IM, Vanstone SA, Wilson RM. Optimal normal bases in $GF(p^n)$. Discrete Appl Math 1989; 22: 149-161.

[12] Negre C. Finite field arithmetic using quasi-normal bases. Finite Fields Appl 2007; 13: 635-647.

[13] Reis L. Existence results on k-normal elements over finite fields. arXiv:1612.05931v3, 2018.

[14] Reyhani-Masoleh A. Efficient algorithms and architectures for field multiplication using gaussian normal bases. IEEE T Comput 2006; 55: 34-47.

[15] Tuxanidy A, Wang Q. Composed products and factors of cyclotomic polynomials over finite fields. Des Codes Cryptogr 2013; 69: 203-231.

[16] Wang L, Wang Q. On explicit factors of cyclotomic polynomials over finite fields. Des Codes Cryptogr 2012; 63: 87-104.

[17] Wu H, Zhu L, Feng R, Yang S. Explicit factorizations of cyclotomic polynomials over finite fields. Des Codes Cryptogr 2017: 83: 197-217.