On $k$-normal elements over finite fields

Lucas Reis

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa
ON (Canada), K1S 5B6

Abstract

The so called $k$-normal elements appear in the literature as a generalization of normal elements over finite fields. Recently, questions concerning the construction of $k$-normal elements and the existence of $k$-normal elements that are also primitive have attracted attention from many authors. In this paper we give alternative constructions of $k$-normal elements and, in particular, we obtain a sieve inequality for the existence of primitive, $k$-normal elements. As an application, we show the existence of primitive $k$-normals in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ in the case when $k$ lies in the interval $[1, n/4]$, $n$ has a special property and $q, n \geq 420$.

Keywords: primitive elements, normal bases, $k$-normal elements

2010 MSC: 12E20, 11T30, 12E20

1. Introduction

Let $\mathbb{F}_{q^n}$ be the finite field with $q^n$ elements, where $q$ is a prime power and $n$ is a positive integer. We have two special notions of generators in the theory of finite fields. The multiplicative group $\mathbb{F}_{q^n}^*$ is cyclic, with $q^n - 1$ elements, and any generator is called primitive. Also, $\mathbb{F}_{q^n}$ can be regarded as an $\mathbb{F}_q$-vector space over $\mathbb{F}_q$: its dimension is $n$ and, in particular, $\mathbb{F}_{q^n}$ is isomorphic to $\mathbb{F}_q^n$. An element $\alpha \in \mathbb{F}_{q^n}$ is said to be normal over $\mathbb{F}_q$ if $A = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$: $A$ is frequently called a normal basis. Due to their high efficiency, normal bases are frequently used in cryptography and computer algebra systems; sometimes it is also interesting to use normal bases composed by primitive elements. The Primitive Normal Basis Theorem states that for any extension field $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$, there exists a normal basis composed by primitive elements; this result was first proved by Lenstra and Schoof and a proof without the use of a computer was later given in [3].

1Permanent address: Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte MG (Brazil), 30123-970.
Recently, Huczynska et al.\[7\] introduce $k$-normal elements, extending the notion of normal elements. There are many equivalent definitions and here we present the most natural in the sense of vector spaces.

**Definition 1.1.** For $\alpha \in \mathbb{F}_{q^n}$, consider the set $S_\alpha = \{\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}\}$ comprising the conjugates of $\alpha$ by the action of the Galois Group of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The element $\alpha$ is said to be $k$-normal over $\mathbb{F}_q$ if the vector space $V_\alpha$ generated by $S_\alpha$ has dimension $n-k$, i.e., $V_\alpha \subseteq \mathbb{F}_{q^n}$ has co-dimension $k$.

From definition, 0-normal elements correspond to normal elements in the usual sense. Also, the concept of $k$-normal depends strongly on the base field that we are working. For this reason, unless otherwise stated, $\alpha \in \mathbb{F}_{q^n}$ is $k$-normal if it is $k$-normal over $\mathbb{F}_q$.

In \[7\], the authors find a formula for the number of $k$-normals and, consequently, obtain some results on the density of these elements. Motivated by the Primitive Normal Basis Theorem, they obtain an existence result on primitive, 1-normal elements.

**Theorem 1.2** (\[7\], Theorem 5.10). Let $q = p^e$ be a prime power and $n$ a positive integer not divisible by $p$. Assume that $n \geq 6$ if $q \geq 11$ and that $n \geq 3$ if $3 \leq q \leq 9$. Then there exists a primitive 1-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

In \[12\], we explore some ideas of \[7\] and, in particular, we obtain a characterization of $k$-normals in the case when $n$ is not divisible by $p$. In the same paper, we find some asymptotic results on the existence of $k$-normal elements that are primitive or have a reasonable high multiplicative order. In \[1\], the author obtains alternative characterizations of $k$-normals via some recursive constructions and, in particular, he presents a method for constructing 1-normal elements in even characteristic. Recently, Theorem 1.2 was extended to arbitrary $n \geq 3$ (see \[13\]), where the authors use many techniques for completing the case $\gcd(n, p) = 1$ and extending this existence result to the case when $n$ is divisible by $p$.

In this paper we deal with the general question concerning the existence of primitive, $k$-normal elements. We introduce a particular class of $k$-normal elements, obtained from normal elements, that removes the pertinent obstruction $n \equiv 0 \pmod{p}$. In particular, we obtain a character sum formula, derived from the Lenstra-Schoof method, for the number of certain primitive $k$-normals. As an application, we obtain some existence results on primitive $k$-normals in special extensions of $\mathbb{F}_q$. We also extend some results of \[13\] to $k$-normal elements.

2. Preliminaries

Here we introduce some basic definitions related to the $k$-normal elements, adding some recent results. We start with some arithmetic functions and their polynomial version.
Definition 2.1. (a) Let $f(x)$ be a monic polynomial with coefficients in $F_q$. The Euler Phi Function for polynomials over $F_q$ is given by

$$\Phi(f) = \left| \left( \frac{F_q[x]}{(f)} \right)^* \right|,$$

where $(f)$ is the ideal generated by $f(x)$ in $F_q[x]$.

(b) If $t$ is a positive integer (or a monic polynomial over $F_q$), $W(t)$ denotes the number of square-free (monic) divisors of $t$.

(c) If $f(x)$ is a monic polynomial with coefficients in $F_q$, the Polynomial Mobius Function $\mu_q$ is given by $\mu_q(f) = 0$ if $f$ is not square-free and $\mu_q(f) = (-1)^r$ if $f$ writes as a product of $r$ distinct irreducible factors over $F_q$.

2.1. $q$-polynomials and $k$-normals

For $f \in F_q[x]$, $f = \sum_{i=0}^{s} a_i x^i$, we set $L_f(x) = \sum_{i=0}^{s} a_i x^{q^i}$ as the $q$-associate of $f$. Also, for $\alpha \in F_q^n$, we set $f \circ \alpha = L_f(\alpha) = \sum_{i=0}^{s} a_i \alpha^{q^i}$.

As follows, we have some basic properties of the $q$-associates:

Lemma 2.2. ([3], Theorem 3.62) Let $f, g \in F_q[x]$. The following hold:

(i) $L_f(L_g(x)) = L_{fg}(x)$,

(ii) $L_f(x) + L_g(x) = L_{f+g}(x)$.

For $\alpha \in F_q^n$, we define $\mathcal{I}_\alpha$ as the subset of $F_q[x]$ comprising the polynomials $f(x)$ for which $f(x) \circ \alpha = 0$, i.e., $L_f(\alpha) = 0$. Notice that $x^n - 1 \in \mathcal{I}_\alpha$ and, from the previous Lemma, it can be verified that $\mathcal{I}_\alpha$ is an ideal of $F_q[x]$, hence $\mathcal{I}_\alpha$ is generated by a polynomial $m_\alpha(x)$. We can suppose $m_\alpha(x)$ monic. The polynomial $m_\alpha(x)$ is defined as the $F_q$-order of $\alpha$. This is a dual definition of multiplicative order in $F_q^*$.

Clearly $m_\alpha(x)$ is always a divisor of $x^n - 1$, hence its degree is $j$ for some $0 \leq j \leq n$. Notice that $j = 0$ if and only if $m_\alpha(x) = 1$, i.e., $\alpha = 0$. The following result shows a connection between $k$-normal elements and their $F_q$-order.

Proposition 2.3. ([3], Theorem 3.2) Let $\alpha \in F_q^n$. Then $\alpha$ is $k$-normal if and only if $m_\alpha(x)$ has degree $n - k$.

In particular, an element $\alpha$ is normal if and only if $m_\alpha(x) = x^n - 1$. We see that the existence of $k$-normals depends on the existence of a polynomial of degree $n - k$ dividing $x^n - 1$ over $F_q$; as follows, we have a formula for the number of $k$-normal elements.

Lemma 2.4. ([3], Theorem 3.5) The number $N_k$ of $k$-normal elements of $F_q^n$ over $F_q$ is given by

$$N_k = \sum_{\substack{h | x^n - 1 \text{ monic} \\ \deg(h) = n - k}} \Phi(h),$$

where the divisors are monic and polynomial division is over $F_q$. 

3
One of the main steps in the proof of the result above is the fact that, for each monic divisor $f(x)$ of $x^n - 1$, there exists $\Phi_q(f(x))$ elements $\alpha \in \mathbb{F}_{q^n}$ for which $m_\alpha(x) = f(x)$. This fact will be further used in this paper.

Since $\frac{x^n - 1}{x - 1}$ divides $x^n - 1$, there are 1-normal elements over any finite field extension. However, the sum in equality (1) can be empty: for instance, if $q = 5$ and $n = 7$:

$$x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

is the factorization of $x^7 - 1$ into irreducible factors over $\mathbb{F}_5$. In particular, there are no 2, 3, 4 or 5-normal elements of $\mathbb{F}_5$. More generally, if $n$ is a prime and $q$ is primitive mod $n$, $x^n - 1$ factors as $(x - 1)(x^{n-1} + \cdots + x + 1)$ and we do not have $k$-normal elements for any $1 < k < n - 1$. The existence of $k$-normals is not guaranteed for generic values of $k$.

As follows, we may construct $k$-normal elements from a given normal element.

**Lemma 2.5.** Let $\beta \in \mathbb{F}_{q^n}$ be a normal element over $\mathbb{F}_q$ and $f(x)$ be a polynomial of degree $k$ such that $f(x)$ divides $x^n - 1$. Then $\alpha = f(x) \circ \beta$ is $k$-normal.

**Proof.** We prove that $m_\alpha(x) = \frac{x^n - 1}{f(x)}$ and this implies the desired result. Notice that $\frac{x^n - 1}{f(x)} \circ \alpha = \frac{x^n - 1}{f(x)} \circ (f(x) \circ \beta) = (x^n - 1) \circ \beta = 0$, hence $m_\beta(x)$ divides $\frac{x^n - 1}{f(x)}$. It cannot divide strictly because $m_\beta(x) = x^n - 1$ and this completes the proof.

In particular, we have a method for constructing $k$-normal elements when they exist: if we find a divisor $f(x)$ of $x^n - 1$ of degree $k$ and a normal element $\beta \in \mathbb{F}_{q^n}$, the element $\alpha = f(x) \circ \beta$ is $k$-normal. There are many ways of finding normal elements in finite field extensions, including constructive and random methods; this is a classical topic in the theory of finite fields and the reader can easily find a wide variety of papers regarding those methods. For instance, see [6].

2.2. A characteristic equation for elements with prescribed $\mathbb{F}_{q^n}$-order

We have noticed that we may construct $k$-normal elements from the normal elements. However, it is not guaranteed that this method describes every $k$-normal in $\mathbb{F}_{q^n}$. For a polynomial $f$ dividing $x^n - 1$, set

$$\Psi_f(x) = \prod_{m_\alpha = f(x)} (x - \alpha),$$

the polynomial of least degree that vanishes in every element $\alpha \in \mathbb{F}_{q^n}$ with $m_\alpha = f(x)$. Clearly $m_\alpha = f$ if and only if $\Psi_f(\alpha) = 0$. Also, for $f(x) \in \mathbb{F}_q[x]$ and $\alpha \in \mathbb{F}_{q^n}$, we have $f(x) \circ \alpha = L_f(\alpha) = 0$ if and only if $m_\alpha$ divides $f(x)$. In particular, this shows that $L_f(x) = \prod_{g | f} \Psi_g(x)$. This identity is similar to the one describing cyclotomic polynomials

$$x^n - 1 = \prod_{n/d} \Phi_d(x).$$
From the Mobius Inversion formula, we may deduce \( \Phi_d(x) = \prod_{r|d}(x^r - 1)^{\mu(d/r)} \). This last equality describes the elements of multiplicative order \( d \) in finite fields.

Motivated by this characterization, we obtain the following:

**Proposition 2.6.** Let \( f(x) \) be any divisor of \( x^n - 1 \) over \( \mathbb{F}_q \). The following holds:

\[
\Psi_f(x) = \prod_{g|f} L_g(x)^{\mu_q(f/g)},
\]

where \( g \) is monic and polynomial division is over \( \mathbb{F}_q \).

**Proof.** Notice that

\[
\prod_{g|f} L_g(x)^{\mu_q(f/g)} = \prod_{g|f} L_{f/g}(x)^{\mu_q(g)},
\]

and, from \( L_{f/g}(x) = \prod_{h|f/g} \Psi_h(x) \), we obtain

\[
\prod_{g|f} L_{f/g}(x)^{\mu_q(g)} = \prod_{h|f} \Psi_h(x)^{\sum_{g|f/h} \mu_q(g)}.
\]

Writing \( f/h \) as product of irreducibles over \( \mathbb{F}_q \), we can easily see that

\[
\sum_{g|f/h} \mu_q(g) = \begin{cases} 
1 & \text{if } f/h = 1, \\
0 & \text{otherwise}.
\end{cases}
\]

This shows that

\[
\prod_{g|f} L_g(x)^{\mu_q(f/g)} = \Psi_f(x).
\]

Example 2.7. Suppose that \( q \equiv 3 \pmod{4} \) and \( n = 4 \). Then \( \Lambda_0(x) = x^{(q^2 - 1)(q^2 - 1)} \) if \( x^{q^2 - 1} \equiv 1 \pmod{4} \) and \( x^{q - 1} \equiv 1 \pmod{4} \). Hence, \( \alpha \in \mathbb{F}_{q^4} \) is normal if and only if

\[
\sum_{i=0}^{q^2 - 1} \alpha^{2i(q^2 - 1)} = 0.
\]
In general, we have shown that the $k$-normals can be described as the zeroes of a univariate polynomial over $F_q$; this polynomial can be computed from the factorization of $x^n - 1$ over $F_q$.

### 2.3. Some recent results

The proof of Theorem 1.2 is based on an application of the Lenstra-Schoof method, introduced in [8]; this method has been used frequently in the characterization of elements in finite fields with particular properties like being primitive, normal and of zero-trace. In particular, from Corollary 5.8 of [7], we can easily deduce the following:

**Lemma 2.8.** Suppose that $q$ is a power of a prime $p$, $n \geq 2$ is a positive integer not divisible by $p$ and $T(x) = x^n - 1$. If

$$W(T) \cdot W(q^n - 1) < q^{n/2 - 1},$$

(3)

there exist primitive, $1$-normal elements of $F_{q^n}$ over $F_q$.

Inequality (3) is an essential step in the proof of Theorem 1.2 and it was studied in [4]; if $n \geq 6$ for $q \geq 11$ and $n \geq 3$ for $3 \leq q \leq 9$, this inequality holds for all but a finite number of pairs $(q, n)$.

In [7], the authors propose an extension of the Theorem 1.2 for all pairs $(q, n)$ with $n \geq 3$ as a problem ([7], Problem 6.2); they conjectured that such elements always exist. This was recently proved in [13], where the authors use many different techniques to complete Theorem 1.2 in the case gcd($n, p$) = 1 and add the case when $p$ divides $n$.

In particular, when $n$ is divisible by $p^2$, they obtain the following:

**Lemma 2.9.** ([13], Lemma 5.2) Suppose that $F_q$ has characteristic $p$ and let $n = p^2 s$ for any $s \geq 1$. Then $\alpha \in F_{q^n}$ is such that $m_\alpha(x) = \frac{x^{p^2 s} - 1}{x - 1}$ if and only if $\beta = Tr_{q^n/q^{p^s}}(\alpha) = \sum_{i=0}^{p^s-1} \alpha^{p^{si}}$ satisfies $m_\beta(x) = \frac{x^{p^s-1}}{x-1}$.

Using the well-known result on the existence of primitive elements with prescribed trace due to Cohen (see [3]), they prove the existence of primitive 1-normals in the case when $p^2$ divides $n$. The case $n = ps$ with gcd($p, s$) = 1 is dealt in a similar way of [3].

As follows, we have a generalization of Lemma 2.9.

**Lemma 2.10.** ([13], Lemma 5.2) Suppose that $F_q$ has characteristic $p$ and let $n = p^2 s$ for any $s \geq 1$. Also, let $f(x)$ be a polynomial dividing $x^s - 1$. Then $\alpha \in F_{q^n}$ is such that $m_\alpha(x) = \frac{x^{p^2 s} - 1}{f(x)}$ if and only if $\beta = Tr_{q^n/q^{ps}}(\alpha) = \sum_{i=0}^{p^{-1}} \alpha^{p^{si}}$ satisfies $m_\beta(x) = \frac{x^{p^s-1}}{f(x)}$.

The proof is entirely similar to the proof of Lemma 2.9 (see [13]) so we will omit. Motivated by Theorem 5.3 of [13], we have the following.

**Theorem 2.11.** Suppose that $n = p^2 \cdot s$ and $x^s - 1$ is divisible by a polynomial of degree $k$. Then there exists a primitive, $k$-normal element over $F_q$. 

6
Proof. Let \( f(x) \) be a polynomial of degree \( k \) such that \( f(x) \) divides \( x^n - 1 \). In particular, \( f(x) \) divides \( x^{ps} - 1 \), i.e., \( g(x) = \frac{x^{ps} - 1}{f(x)} \) is a polynomial. Since \( g(x) \) divides \( x^{ps} - 1 \), we know that there exists an element \( \beta \in \mathbb{F}_{q^{ps}} \) such that the \( \mathbb{F}_q \)-order \( m_\beta(x) \) of \( \beta \) is \( g(x) \). Clearly \( g(x) \neq 1 \), hence \( \beta \neq 0 \). According to [3], there exists a primitive element \( x \in \mathbb{F}_{q^n} \) such that \( \text{Tr}_{q^n/q^m}(x) = \beta \) and then, from Lemma 2.10, it follows that such an \( x \) satisfies \( m_\alpha = \frac{x^n - 1}{f(x)} \), i.e., \( \alpha \) is a primitive, \( k \)-normal element. \( \square \)

3. Characteristic function for a class of primitive \( k \)-normals

In this section, we use the method of Lenstra and Schoof in the characterization of primitive and normal elements. This method has been used by many different authors in a wide variety of existence problems. For this reason, we skip some details, which can be found in [3]. We recall the notion of freeness.

**Definition 3.1.**

1. If \( m \) divides \( q^n - 1 \), an element \( \alpha \in \mathbb{F}_{q^n} \) is said to be \( m \)-free if \( \alpha = \beta^d \) for any divisor \( d \) of \( m \) implies \( d = 1 \).

2. If \( m(x) \) divides \( x^n - 1 \), an element \( \alpha \in \mathbb{F}_{q^n} \) is \( m(x) \)-free if \( \alpha = h \circ \beta \) for any divisor \( h(x) \) of \( m(x) \) implies \( h = 1 \).

It follows from definition that primitive elements correspond to the \((q^n - 1)\)-free elements. Also, \( \alpha \in \mathbb{F}_{q^n} \) is normal if and only if is \((x^n - 1)\)-free. The concept of freeness derives some characteristic functions for primitive and normal elements. We pick the notation of [3].

**Multiplicative Part:** \( \int_{d|m} \eta_d \) denotes \( \sum_{d|m} \frac{\mu(d)}{\varphi(d)} \sum_{(d)} \eta_d \), where \( \mu \) and \( \varphi \) are the Mobius and Euler functions for integers, respectively, \( \eta_d \) is a typical multiplicative character of \( \mathbb{F}_{q^n} \) of order \( d \), and the sum \( \sum_{(d)} \eta_d \) runs through all the multiplicative characters of order \( d \).

**Additive Part:** \( \chi \) denotes the canonical additive character on \( \mathbb{F}_{q^n} \), i.e.

\[
\chi(\omega) = \lambda \left( \sum_{i=0}^{n-1} \omega^i \right), \omega \in \mathbb{F}_{q^n},
\]

where \( \lambda \) is the canonical additive character of \( \mathbb{F}_q \) to \( \mathbb{F}_p \). If \( D \) is a monic polynomial dividing \( x^n - 1 \) over \( \mathbb{F}_q \), a typical character \( \chi_* \) of \( \mathbb{F}_{q^n} \) of \( \mathbb{F}_q \)-order \( D \) is one such that \( \chi_* (D \circ \gamma) \) is the trivial additive character in \( \mathbb{F}_{q^n} \) and \( D \) is minimal (in terms of degree) with this property. Let \( \Delta_D \) be the set of all \( \delta \in \mathbb{F}_{q^n} \) such that \( \chi_\delta \) has \( \mathbb{F}_{q^n} \)-order \( D \), where \( \chi_\delta(\omega) = \chi(\delta \omega) \) for any \( \omega \in \mathbb{F}_{q^n} \). For instance, \( \Delta_1 = \{0\} \) and \( \Delta_{x-1} = \mathbb{F}_{q^n} \).

In the same way of the multiplicative part, \( \int_{D|T} \chi_{D|T} \) denotes the sum

\[
\sum_{D|T} \frac{\mu_q(D)}{\Phi(D)} \sum_{(\delta|D)} \chi_{\delta|D},
\]
where \( \mu_q \) and \( \Phi \) are the Mobius and Euler functions for polynomials over \( \mathbb{F}_q \), respectively, \( \chi_{\delta_D} \) denotes a typical additive character of \( \mathbb{F}_{q^n} \) of \( \mathbb{F}_q \)-Order \( D \) and the sum \( \sum_{(\delta_D)} \chi_{\delta_D} \) runs through all the additive characters whose \( \mathbb{F}_q \)-order equals \( D \), i.e., \( \delta_D \in \Delta_D \).

For \( t \) dividing \( q^n - 1 \) and \( D \) dividing \( x^n - 1 \), set \( \theta(t) = \frac{\varphi(t)}{t} \) and \( \Theta(D) = \frac{\phi(D)}{q^{\deg D}} \).

**Theorem 3.2.** [7, Section 5.2]

1. For \( w \in \mathbb{F}_{q^n}^* \) and \( t \) be a positive divisor of \( q^n - 1 \),
   \[
   \omega_t(w) = \theta(t) \int_{d|t} \eta_d(w) = \begin{cases} 1 & \text{if } w \text{ is } t\text{-free}, \\ 0 & \text{otherwise.} \end{cases}
   \]

2. For \( w \in \mathbb{F}_{q^n} \) and \( D \) be a monic divisor of \( x^n - 1 \),
   \[
   \Omega_D(w) = \Theta(D) \int_{E|D} \chi_{\delta_E}(w) = \begin{cases} 1 & \text{if } w \text{ is } D\text{-free}, \\ 0 & \text{otherwise.} \end{cases}
   \]

In particular, for \( t = q^n - 1 \) and \( D = x^n - 1 \), we obtain characteristic functions for primitive and normal elements, respectively. We write \( \omega_{q^n - 1} = \omega \) and \( \Omega_{x^n - 1} = \Omega \). As usual, we may extend the multiplicative characters to 0 by setting \( \eta_1(0) = 1 \), where \( \eta_1 \) is the trivial multiplicative character and \( \eta(0) = 0 \) if \( \eta \) is not trivial.

We have seen that some \( k \)-normals arise from a normal element \( \beta \) via the composition \( f(x) \circ \beta \), where \( f(x) \) is a divisor of \( x^n - 1 \), \( \deg f = k \); more than that, \( \alpha = f(x) \circ \beta \) satisfies \( m_\alpha = \frac{x^{n-1}}{f(x)} \). In particular, we may obtain the characteristic function for the primitive elements arising from this construction: note that \( \Omega(w) \cdot \omega(L_f(w)) = 1 \) if and only if \( w \) is normal and \( L_f(w) = f(x) \circ w \) is primitive. This characteristic function describes a particular class of primitive \( k \)-normal elements. The following is straightforward.

**Proposition 3.3.** Let \( f(x) \) be a divisor of \( x^n - 1 \) of degree \( k \) and \( n_f \) be the number of primitive elements of the form \( f(x) \circ \alpha \), where \( \alpha \) is a normal element. The following holds:

\[
\frac{n_f}{\theta(q^n - 1) \Theta(x^n - 1)} = \sum_{w \in \mathbb{F}_{q^n}^* \substack{d|q^n - 1 \ D|x^n - 1}} \int \int \eta_d(L_f(w)) \chi_{\delta_D}(w). \tag{4}
\]

In particular, the number of primitive, \( k \)-normal elements in \( \mathbb{F}_{q^n} \) is at least \( n_f \).

### 3.1. Character sums and a sieve inequality

Here we make some estimates for the character sums that appear naturally from Eq. (4): note that \( \eta_d \) is the trivial multiplicative character if and only if \( d = 1 \). Also, \( \chi_{\delta_D} \) is the trivial additive character if and only if \( \delta_D = 0 \), i.e., \( D = 1 \).
As usual, we split the sum in Eq. (1) as Gauss sums types, according to the trivial and non-trivial characters. For each $d$ dividing $q^n - 1$ and $D$ dividing $x^n - 1$, set $G_f(\eta_d, \chi_D) = \sum_{w \in \mathbb{F}_{q^n}} \eta_d(L_f(w))\chi_D(w)$.

Note that, from Proposition 3.3

$$\frac{n_f}{\Theta(q^n - 1)\Theta(x^n - 1)} = s_0 + S_1 + S_2 + S_3,$$

where $s_0 = G_f(\eta_1, \chi_0)$, $S_1 = \int_{D|q^n-1} \int_{D|x^n-1} G_f(\eta_1, \chi_D)$, $S_2 = \int_{D|q^n-1} \int_{D|x^n-1} G_f(\eta_d, \chi_0)$ and

$$S_3 = \int_{D|q^n-1} \int_{D|x^n-1} G_f(\eta_d, \chi_D).$$

From definition, $s_0 = q^n$. Also, note that

$$G_f(\eta_1, \chi_D) = \sum_{w \in \mathbb{F}_{q^n}} \eta_1(L_f(w))\chi_D(w) = \sum_{w \in \mathbb{F}_{q^n}} \chi_D(w) = 0,$$

for any divisor $D$ of $x^n - 1$ with $D \neq 1$. In particular, $S_1 = 0$. For the quantities $S_2$ and $S_3$, we use some general bounds on character sums.

**Lemma 3.4.** ([2], Theorem 5.41) Let $\eta$ be a multiplicative character of $\mathbb{F}_{q^n}$ of order $r > 1$ and $f \in \mathbb{F}_{q^n}[x]$ be a monic polynomial of positive degree such that $f$ is not of the form $g(x)^r$ for some $g \in \mathbb{F}_{q^n}[x]$ with degree at least 1. Suppose that $e$ is the number of distinct roots of $f$ in its splitting field over $\mathbb{F}_{q^n}$. For every $a \in \mathbb{F}_{q^n}$,

$$\left| \sum_{c \in \mathbb{F}_{q^n}} \eta(ac(c)) \right| \leq (e - 1)q^{n/2}.$$

**Lemma 3.5.** ([4]) Let $\eta$ be a non-trivial multiplicative character of order $r$ and $\chi$ be a nontrivial additive character of $\mathbb{F}_{q^n}$. Let $f$ and $g$ be rational functions in $\mathbb{F}_{q^n}(x)$ such that $f$ is not of the form $y \cdot h^r$ for any $y \in \mathbb{F}_{q^n}$ and $h \in \mathbb{F}_{q^n}(x)$, and $g$ is not of the form $h^r - h + y$ for any $y \in \mathbb{F}_{q^n}$ and $h \geq \mathbb{F}_{q^n}(x)$. Then,

$$\left| \sum_{w \in \mathbb{F}_{q^n} \setminus S} \eta(f(w)) \cdot \chi(g(w)) \right| \leq (\deg(g)_{\infty} + m + m' - m'' - 2)q^{n/2},$$

where $S$ is the set of poles of $f$ and $g$, $(g)_{\infty}$ is the pole divisor of $g$, $m$ is the number of distinct zeros and finite poles of $f$ in the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$, $m'$ is the number of distinct poles of $g$ (including $\infty$) and $m''$ is the number of finite poles of $f$ that are poles or zeros of $g$.

Write $f(x) = \sum_{i=0}^{k} a_i x^i$. Note that, since $L_f$ is a $q$-polynomial, its formal derivative equals $a_0$. In particular, $L_f$ does not have repeated roots, hence cannot be of the form $y \cdot g(x)^r$ for some $r > 1$. 

9
Also, if \( f(x) \) divides \( x^n - 1 \) and has degree \( k \), we know that \( L_f = 0 \) has exactly \( q^k \) roots over \( \mathbb{F}_{q^n} \); these roots describe a \( k \)-dimensional \( \mathbb{F}_q \)-vector subspace of \( \mathbb{F}_{q^n} \). Finally, notice that \( g(x) = x \) cannot be written as \( h^p - h - y \) for any rational function \( h \in \mathbb{F}_{q^n}(x) \) and \( y \in \mathbb{F}_{q^n} \). From Lemma 3.3 we conclude that, for \( d > 1 \) a divisor of \( q^n - 1 \),

\[
|G_f(\eta_d, \chi_0)| = \left| \sum_{c \in \mathbb{F}_{q^n}} \eta_d(L_f(c)) \right| \leq (q^k - 1)q^{n/2}.
\]

From Lemma 3.3 it follows that, for any \( D \) divisor of \( x^n - 1 \) and \( d \) a divisor of \( q^n - 1 \), with \( D, d \neq 1 \),

\[
|G_f(\eta_d, \chi_{\delta_D})| = \left| \sum_{w \in \mathbb{F}_{q^n}} \eta_d(L_f(w))\chi_{\delta_D}(w) \right| \leq (1 + q^k + 1 - 0 - 2)q^{n/2} = q^{n/2+k}.
\]

Combining all the previous bounds, we obtain the following:

**Theorem 3.6.** Let \( f(x) \) be a divisor of \( x^n - 1 \) of degree \( k \) and let \( n_f \) be the number of primitive elements of the form \( f(x) \circ \alpha \), where \( \alpha \) is a normal element. The following holds:

\[
\frac{n_f}{\theta(q^n - 1)\Theta(x^n - 1)} > q^n - q^{n/2+k}W(q^n - 1)W(x^n - 1).
\]

In particular, if

\[
q^{n/2-k} \geq W(q^n - 1)W(x^n - 1),
\]

then there exist primitive \( k \)-normal elements in \( \mathbb{F}_{q^n} \).

**Proof.** We have seen that

\[
\frac{n_f}{\theta(q^n - 1)\Theta(x^n - 1)} = s_0 + S_1 + S_2 + S_3 = q^n + S_2 + S_3.
\]

In particular,

\[
\frac{n_f}{\theta(q^n - 1)\Theta(x^n - 1)} \geq q^n - |S_2| - |S_3|.
\]

Applying estimates to the sums \( S_2, S_3 \), we obtain

\[
|S_2| \leq (W(q^n - 1) - 1)(q^k - 1)q^{n/2}
\]

and

\[
|S_3| \leq (W(q^n - 1) - 1)(W(x^n - 1) - 1)q^{n/2+k},
\]

hence

\[
|S_1| + |S_2| < q^{n/2+k}W(q^n - 1)W(x^n - 1).
\]

In particular, if Eq. (5) holds, \( n_f > 0 \) and we know that the number of primitive \( k \)-normals is at least \( n_f \). This completes the proof.

\[\square\]

Notice that Eq. (5) generalizes the sieve inequality in Lemma 2.8
4. Existence of primitive $k$-normals

In this section, we discuss the existence of primitive $k$-normals in some special extensions of $\mathbb{F}_q$. Essentially, we explore the sieve inequality present in Theorem 3.6 and the result contained in Theorem 2.11.

We have seen that the existence of $k$-normals is not always ensured for generic values of $1 < k < n - 1$: from Lemma 2.4, the number of $k$-normals is strongly related to the factorization of $x^n - 1$ over $\mathbb{F}_q$. This motivates us to introduce the concept of practical numbers.

**Definition 4.1. (Practical numbers) A positive integer $n$ is said to be $\mathbb{F}_q$-practical if, for any $1 \leq k \leq n - 1$, $x^n - 1$ is divisible by a polynomial of degree $k$ over $\mathbb{F}_q$.**

Notice that, if $n$ is $\mathbb{F}_q$-practical, there exist $k$-normals in $\mathbb{F}_q^n$ for any $1 < k < n - 1$. This definition arises from the so called $\varphi$-practical numbers: they are the positive integers $n$ for which $x^n - 1 \in \mathbb{Z}[x]$ is divisible by a polynomial of degree $k$ for any $1 \leq k \leq n - 1$. These $\varphi$-practical numbers have been extensively studied in many aspects, such as their density over $\mathbb{N}$ and their asymptotic number. In particular, if $s(t)$ denotes the number of $\varphi$-practical numbers up to $t$, according to [11], there exists a constant $C > 0$ such that

$$\lim_{t \to \infty} \frac{s(t) \log t}{t} = C.$$ 

This shows that the $\varphi$-practical numbers behaves like the primes on integers and, in particular, their density in $\mathbb{N}$ is zero.

Notice that the factorization of $x^n - 1$ over $\mathbb{Z}$ also holds over any finite field: we take the coefficients (mod $p$) and recall that $\mathbb{F}_p \subseteq \mathbb{F}_q$. This shows that any $\varphi$-practical number is also $\mathbb{F}_q$-practical. In particular, the number of $\mathbb{F}_q$-practicals up to $t$ has growth at least $\frac{Ct}{\log t}$. The exact growth of the number of $\mathbb{F}_q$-practicals is still an open problem. However, we can find infinite families of such numbers.

**Proposition 4.2. ([12], Theorem 4.4) Let $q$ be a power of a prime $p$ and let $n$ be a positive integer such that every prime divisor of $n$ divides $p(q - 1)$. Then $n$ is $\mathbb{F}_q$-practical.**

From Theorem 2.11, we obtain the following.

**Corollary 4.3. Let $n = p^2s$, where $s$ is an $\mathbb{F}_q$-practical number. Then, for any $1 \leq k \leq s$, there exists a primitive, $k$-normal element of $\mathbb{F}_q^n$.**

The previous corollary ensures the existence of primitive $k$-normals for $k$ in the interval $[1, \frac{n}{p^2}]$. This corresponds to a proportion close to $1/p^2$ of the possible values of $k$.

In the rest of this paper, we explore Eq. (5) in extensions of degree $n$, where $n$ is an $\mathbb{F}_q$-practical number. Essentially, we obtain effective bounds on the functions $W(x^n - 1)$ and $W(q^n - 1)$. 

11
4.1. Some estimates for the square-free divisors counting

Here we obtain some estimates on the functions \( W(q^n - 1) \) and \( W(x^n - 1) \). We start with some general bounds. The bound \( W(x^n - 1) \leq 2^n = q^{n \log_q 2} \) is trivial. Also, we have a general bound for \( W(q^n - 1) \): if \( d(q^n - 1) \) denotes the number of divisors of \( q^n - 1 \), \( W(q^n - 1) \leq d(q^n - 1) \). For the number of divisors function, we have the following.

**Lemma 4.4.** If \( d(m) \) denotes the number of divisors of \( m \), then for all \( m \geq 3 \),

\[
d(m) \leq m^{\frac{1.06 \log 2}{\log \log m}} < m^{\frac{1.06}{\log \log m}}.
\]

**Proof.** This inequality is a direct consequence of the result in [10].

In particular, we can easily obtain \( W(q^n - 1) < q^{1.06 n \log \log(q^n - 1)} \). We now study the special case when \( n \) is a power of two.

**Lemma 4.5.** Suppose that \( q \) is odd. For any \( i \geq 1 \), if \( r_0 \) is an odd prime that divides \( q^{2^i} + 1 \), then \( r_0 \equiv 1 \pmod{2^{i+1}} \).

**Proof.** Let \( l \) be the least positive integer such that \( q^l \equiv 1 \pmod{r_0} \). Clearly \( l \) divides \( \varphi(r_0) = r_0 - 1 \). Also, \( r_0 \) divides \( q^{2^{i+1}} - 1 \) but not \( q^{2^i} - 1 \), it follows that \( l \) divides \( 2^{i+1} \) but not \( 2^i \). This shows that \( 2^{i+1} = l \), hence \( 2^{i+1} \) divides \( r_0 - 1 \).

In particular, we obtain the following.

**Proposition 4.6.** For any \( q \geq 3 \) odd and \( t \geq 2 \),

\[
W(q^{2^t} - 1) < 2q^{\frac{2^t}{2^t + 1}}.
\]

**Proof.** For \( 1 \leq i < t - 1 \), set \( d_i = q^{2^i} + 1 \). Note that \( W(q^{2^i} - 1) \leq W(q^{2^i} - 1) \cdot \prod_{i=2}^{t-1} W(d_i/2) \). For a fixed \( 2 \leq i \leq t \), let \( s_1 < \cdots < s_{d(i)} \) be the distinct odd primes that divide \( d_i \). Clearly \( W(d_i/2) = 2^{d(i)} \). As we have seen, \( s_j \equiv 1 \pmod{2^{i+1}} \), hence \( s_j > 2^{i+1} \) and then

\[
d_i > s_1 \cdots s_{d(i)} > 2^{(i+1) \cdot d(i)},
\]

hence \( 2^{d(i)} < q^{\frac{2^t}{2^t + 1}} \). It follows by induction that \( \sum_{i=1}^{t-1} \frac{2^i}{2^t + 1} \leq \frac{2^t}{2^t + 1} - 1 \) for \( t \geq 2 \). Moreover, we have the trivial bound \( W(q^{2^2} - 1) < 2q \). This completes the proof.

4.2. Applications of Theorem 3.6

The following is straightforward.

**Proposition 4.7.** Let \( n \) be an \( \mathbb{F}_q \)-practical number. If \( k \) is a positive integer such that

\[
k \leq n \cdot \left( \frac{1}{2} - \frac{1.06 \log 2}{\log \log(q^n - 1)} - \log 2 \frac{\log q}{\log q} \right),
\]

there exist primitive \( k \)-normals in \( \mathbb{F}_{q^n} \).
For $h(n, q) = \frac{1}{2} - \frac{1.06}{\log \log(q^n-1)} - \frac{\log 2}{\log q}$, we have $\lim_{q \to \infty} h(n, q) = 1/2$ uniformly on $n$. In particular, given $\epsilon > 0$, for $q$ sufficiently large, we can guarantee the existence of $k$-normals in the interval $[1, (1/2 - \epsilon)n]$ in the case when $n$ is $\mathbb{F}_q$-practical. In general, the bounds on character sums over $\mathbb{F}_q^n$ yield the factor $q^{n/2}$. In particular, this result is somehow sharp based on our character sums estimates. However, $h(n, q)$ goes to $1/2$ slowly and we do not have much control on $n$, since we are assuming that $n$ is $\mathbb{F}_q$-practical. Far from the extreme $n/2$, we have effective results:

**Corollary 4.8.** Let $q \geq 420$ be a power of a prime and let $n \geq 420$ be an $\mathbb{F}_q$-practical number. For any $k \in [1, n/4]$, there exist primitive $k$-normals in $\mathbb{F}_q^n$.

*Proof.* Note that $h(n, q)$ is an increasing function on $q$ and $n$. Also, $h(420, 420) > 1/4$ and the result follows.

The previous corollary gives a wide class of extensions having primitive $k$-normals in the interval $[1, n/4]$; for instance, we can consider $n = r^t$, $t \geq 1$, where $r \geq 420$ is a prime dividing $q - 1$. In the special case when $n$ is a power of two, we obtain the following.

**Corollary 4.9.** Set $n = 2^t$, $t \geq 2$ and let $q$ be a power of a prime. Additionally, suppose that $t \geq 9$ and $q \geq 259$ if $q$ is odd. Then, for $k \in [1, n/4]$, there exist primitive $k$-normal elements in $\mathbb{F}_q^n$.

*Proof.* Since 2 always divides $p(q - 1)$, from Proposition 4.2, $2^t$ is $\mathbb{F}_q$-practical. For $q$ even, the result follows from Corollary 4.3. Suppose that $q$ is odd. According to Proposition 4.6, $W(q^{2^t} - 1) < 2q^{2^{t-1}}$ and we have the trivial bound $W(x^{2^t} - 1) \leq 2^{2^t}$. We can verify that, for $t \geq 9$ and $q \geq 259$, $2^{2^{t+1}}q^{2^{t-1}} < q^{2^{t+1}}$ and the result follows from Theorem 3.6.

5. Conclusions and an additional remark

In this paper we have discussed the existence of primitive $k$-normal elements over finite fields. We recall some recent results on 1-normal elements and partially extend them to more general $k$-normals. In particular, we obtain a sieve inequality for the existence of primitive $k$-normal elements in extension fields that contains $k$-normals. As an application, we give some families of pairs $(q, n)$ for which we can guarantee the existence of $k$-normals in $\mathbb{F}_q^n$ for $k \in [1, n/4]$; this corresponds to the first quarter of the possible values of $k$. For $q$ large enough, we can extend the range of $k$ to $[1, (1/2 - \epsilon)n]$, where $\epsilon$ is close to 0: in other words, we can asymptotically reach the first half of the interval $[1, n]$. As we have pointed out, the typical bounds for our character sums always have the component $q^{n/2}$ and, for this reason, in order to obtain results on primitive $k$-normals for $k \in [n/2, n]$, we need methods beyond the approach of Lenstra and Schoof or even better character sums estimates.

13
Here we make a brief discussion on the existence of primitive $k$-normals for $k$ in the other extreme, i.e., $k$ close to $n$. We recall that $0 \in \mathbb{F}_{q^n}$ is the only $n$-normal element. Also, as pointed out in [7], there do not exist primitive $(n-1)$-normals in $\mathbb{F}_{q^n}$: in particular, a primitive element and its conjugates cannot all lie in a “line”.

For the special case $k = n - 2$ and $n > 2$, we consider the following: set $q = p$ a prime, $n = p$ and let $a$ be a primitive element of $\mathbb{F}_p$. It can be verified that $f(x) = x^p - x - a$ is irreducible over $\mathbb{F}_p$ and any root $\alpha \in \mathbb{F}_{p^p}$ of $f(x)$ satisfies $(x - 1)^2 \circ \alpha = 0$, i.e., $\alpha$ is $(n-2)$-normal. It is conjectured that such an $\alpha$ is always a primitive element of $\mathbb{F}_{p^p}$. This conjecture is verified for every $p \leq 100$ and some few primes $p > 100$. If this conjecture is true, we obtain an interesting example of a primitive element $\alpha$ of “low normalcy” (in the sense that $\alpha$ and their conjugates generates an $\mathbb{F}_q$-vector space of low dimension).

**Acknowledgments**

This work was conducted during a scholarship supported by the Program CAPES-PDSE (process - 88881.134747/2016-01) at Carleton University.

**References**

[1] M. Alizadeh, *Some notes on the $k$-normal elements and $k$-normal polynomials over finite fields*, Journal of Algebra and its Applications, 16 (2017), 11 pages.

[2] F.N. Castro, C.J. Moreno, *Mixed exponential sums over finite fields*, Proc. Am. Math. Soc. 128 (2000) 2529-2537.

[3] S.D. Cohen, S. Huczynska. *The primitive normal basis theorem - without a computer*, Journal of the London Mathematical Society 67 (2003) 41-56.

[4] S. D. Cohen, D. Hachenberger, *Primitive normal bases with prescribed trace*, Applicable Algebra in Engineering, Communication and Computing 9 (1999) 383-403.

[5] S. D. Cohen, *Primitive elements and polynomials with arbitrary trace*. Discrete Mathematics, 83 (1990), 1-7.

[6] J. von zur Gathen, M. Giesbrecht, *Constructing normal bases in finite fields*, Journal of Symbolic Computation 10 (1990) 547-570.

[7] 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.

[8] H.W. Lenstra, R. Schoof, *Primitive normal bases for finite fields*, Mathematics of Computation 48 (1987) 217-231.
[9] R. Lidl, H. Niederreiter, *Finite Fields: Encyclopedia of Mathematics and Its Applications*, vol. 20, 2nd ed. Cambridge University Pres, Cambridge, 1997.

[10] J.L. Nicolas, G. Robin, *Majorations explicites pour le nombre de diviseurs de N*, Canad. Math. Bull. 26 (1983) 485-492.

[11] C. Pomerance, L. Thompson, A. Weingartner, *On integers n for which $x^n - 1$ has a divisor of every degree*, Acta Arith. 175 (2016) 225-243.

[12] L. Reis, *Existence results on K-normal elements over finite fields*, Arxiv (2017) [https://arxiv.org/pdf/1612.05931.pdf](https://arxiv.org/pdf/1612.05931.pdf).

[13] L. Reis, D. Thomson, *Existence of primitive 1-normal elements in Finite Fields*, Arxiv (2017) [https://arxiv.org/pdf/1710.06131.pdf](https://arxiv.org/pdf/1710.06131.pdf).