Existence and properties of k-normal elements over finite fields

S. Huczynska[a], G. L. Mullen[b], D. Panario and D. Thomson[c,1]

[a]*School of Mathematics and Statistics, University of St. Andrews, St. Andrews, Fife, U.K., KY16 9SS.*
[b]*Department of Mathematics, The Pennsylvania State University, University Park, PA, U.S.A., 16802.*
[c]*School of Mathematics and Statistics, Carleton University, 1125 Colonel By Dr., Ottawa, ON, Canada, K1S 5B6.*

Abstract

An element $\alpha \in \mathbb{F}_{q^n}$ is *normal* over $\mathbb{F}_q$ if $\{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$ is a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. It is well-known that $\alpha \in \mathbb{F}_{q^n}$ is normal over $\mathbb{F}_q$ if and only if the polynomials $g_\alpha(x) = \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-2}} x + \alpha^{q^{n-1}}$ and $x^n - 1$ are relatively prime over $\mathbb{F}_{q^n}$, that is, the degree of their greatest common divisor in $\mathbb{F}_{q^n}[x]$ is 0. An element $\alpha \in \mathbb{F}_{q^n}$ is *k-normal* over $\mathbb{F}_q$ if the greatest common divisor of the polynomials $g_\alpha(x)$ and $x^n - 1$ in $\mathbb{F}_{q^n}[x]$ has degree k; so an element which is normal in the usual sense is 0-normal. This paper introduces and characterizes k-normal elements, establishes a formula and numerical bounds for the number of k-normal elements and demonstrates the existence of primitive 1-normal elements.

Keywords: Finite field, normal basis, k-normal element, primitive element
2000 MSC: 11T30, 11T06, 12E20

1. Introduction

Let q be a prime power and $n \in \mathbb{N}$. An element $\alpha \in \mathbb{F}_{q^n}$ yields a *normal basis* for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if $B = \{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$ is a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$; such an α is a *normal element* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. For any $\alpha \in \mathbb{F}_{q^n}$ and $0 \le i \le n-1$, α^{q^i} is the i-th *conjugate* of α. Since $\alpha^{q^n} = \alpha$ for all $\alpha \in \mathbb{F}_{q^n}$, any element of B and its distinct conjugates comprise all of B, and we say that $\alpha \in B$ *generates* B.

Normal bases are widely used in applications such as cryptography and signal processing due to the efficiency of exponentiation. In particular, q-th powers of field elements represented using a normal basis are given by a cyclic shift. For further details, see [9].

The existence of normal elements over every finite field extension is well-known [11, Theorem 2.35]. In addition, the existence of primitive normal elements, normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ which also generate the multiplicative group $\mathbb{F}_{q^n}^*$, was established in [1] and [2] for sufficiently large q and n. The so-called "Primitive Normal Basis Theorem" was established for all q and n in [10] and a proof without the use of a computer was later given in [3].

An element $\alpha \in \mathbb{F}_{q^n}[x]$ is normal if and only if the polynomial $g_\alpha(x) = \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-2}} x + \alpha^{q^{n-1}}$ and $x^n - 1$ are relatively prime over $\mathbb{F}_{q^n}$ [11, Theorem 2.39]. With this as motivation, we define *k-normal* elements as those elements for which the greatest common divisor of g_α and $x^n - 1$ over $\mathbb{F}_{q^n}$ has degree k. Thus, elements which are normal in the usual sense are 0-normal.

Additional motivation for studying k-normal elements is given by the observation that they implicitly arise during the process of constructing *quasi-normal* bases of finite fields [12]. These bases are a class of $\mathbb{F}_q$-bases of $\mathbb{F}_{q^n}$ which offer efficient multiplication in $\mathbb{F}_{q^n}$.

The structure of this paper is as follows. In Section 2, we introduce and characterize k-normal elements. In Section 3, we give a formula for the number of k-normal elements in terms of the Euler Phi function for polynomials. Section 4 contains numerical bounds on the number of k-normal elements. Finally, we establish the existence of primitive 1-normal elements for sufficiently large q^n in Section 5.

Email addresses: sophieh@mcs.st-and.ac.uk (S. Huczynska), mullen@math.psu.edu (G. L. Mullen), {daniel,dthomson}@math.carleton.ca (D. Panario and D. Thomson)

[1] These authors are supported in part by NSERC of Canada.

2. Introducing k-normal elements

A well-known criterion for checking whether an element generates a normal basis is given by the following theorem.

Theorem 2.1. *[11, Theorem 2.39] 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 $\alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-1}}$ in $\mathbb{F}_{q^n}[x]$ are relatively prime.*

Motivated by this, we make the following definition.

Definition 2.2. *Let $\alpha \in \mathbb{F}_{q^n}$. Denote by $g_\alpha(x)$ the polynomial $\sum_{i=0}^{n-1} \alpha^{q^i} x^{n-1-i} \in \mathbb{F}_{q^n}[x]$. 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 $\mathbb{F}_q$.*

Using this terminology, a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is 0-normal.

It is well known that the number of normal elements of $\mathbb{F}_{q^n}$ is $\Phi_q(x^n - 1)$, where Φ_q is the Euler Phi function for polynomials [11, Theorem 3.73]. Numerical bounds on the density of normal elements in $\mathbb{F}_{q^n}$ are given in [7].

We next give a characterization of k-normal elements in terms of the rank of a Sylvester matrix. We require the following terminology.

Definition 2.3. *Let $\mathbb{F}$ be a field and let $f, g \in \mathbb{F}[x]$ with $f(x) = \sum_{0 \leq j < n} f_j x^j$ and $g(x) = \sum_{0 \leq j < m} g_j x^j$ with all $f_j, g_j \in \mathbb{F}$. The Sylvester matrix $S_{f,g}$ is the $(m+n) \times (m+n)$ matrix given by:*

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

The determinant of the Sylvester matrix $S_{f,g}$ is the *resultant*, denoted $R(f,g)$, of f and g. We have $R(f,g) = 0$ if and only if $f, g \in \mathbb{F}[x]$ have a common divisor of positive degree. For more details, see [8].

Lemma 2.4. *Let $\mathbb{F}$ be a field. For two non-zero polynomials $f, g \in \mathbb{F}[x]$,*

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

Proof. By [8, Exercise 6.16], $\dim(\ker(S_{f,g})) = \deg(\gcd(f,g))$. The result follows by applying the Rank-Nullity Theorem and rearranging. □

We now provide our first characterization of k-normal elements (we note that this result may also be obtained as a consequence of Theorem 1 of [5]).

Theorem 2.5. *Let $\alpha \in \mathbb{F}_{q^n}$ and let*

$$A_\alpha = \begin{pmatrix} \alpha & \alpha^q & \alpha^{q^2} & \cdots & \alpha^{q^{n-1}} \\ \alpha^{q^{n-1}} & \alpha & \alpha^q & \cdots & \alpha^{q^{n-2}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \cdots & \alpha \end{pmatrix}. \tag{1}$$

Then α is k-normal over $\mathbb{F}_q$ if and only if $\operatorname{rank}(A_\alpha) = n - k$.

Proof. We prove that $\gcd(x^n-1, g_\alpha(x))$ (over $\mathbb{F}_{q^n}$) has degree k if and only if the matrix A_α has rank $n-k$. The Sylvester matrix S_{f,g_α} with $f(x) = x^n - 1$ and $g_\alpha(x) = \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-1}}$ can be converted, by a sequence of column operations, into the block matrix

$$\begin{pmatrix} I_{n-1} & 0_{n-1,n} \\ 0_{n,n-1} & A_\alpha \end{pmatrix}$$

where $0_{i,j}$ is the $i \times j$ all-zero matrix and I_{n-1} is the $(n-1) \times (n-1)$ identity matrix. From this block decomposition, it follows that

$$\operatorname{rank}(S_{f,g_\alpha}) = \operatorname{rank}(A_\alpha) + \operatorname{rank}(I_{n-1}) = \operatorname{rank}(A_\alpha) + (n-1).$$

By Lemma 2.4,

$$\operatorname{rank}(S_{f,g_\alpha}) = n + (n-1) - \deg(\gcd(f, g_\alpha)).$$

Combining these two expressions yields

$$\deg(\gcd(f, g_\alpha)) = n - \operatorname{rank}(A_\alpha),$$

as required. □

The following are immediate consequences of Theorem 2.5. First, let $f \in \mathbb{F}_{q^n}[x]$ have degree n. Denote the *reverse* (or *reciprocal*) polynomial of f by $f^*(x) = x^n f(1/x)$.

Corollary 2.6. *Let $\alpha \in \mathbb{F}_{q^n}$. Then*

(i) $\gcd(x^n - 1, g_\alpha(x)) = \gcd(x^n - 1, g^*_\alpha(x))$*;*

(ii) if α is k-normal over $\mathbb{F}_q$, then any conjugate of α is k-normal over $\mathbb{F}_q$.

3. The number of k-normal elements

In this section, we establish a formula for the number of k-normal elements. First, we review some terminology (more details can be found in [11, Chapter 4]).

A polynomial of the form $L(x) = \sum_{i=0}^{d} \alpha_i x^{q^i}$ with coefficients in $\mathbb{F}_{q^n}$ is a *q-polynomial* over $\mathbb{F}_{q^n}$ (or a *linearized polynomial* over $\mathbb{F}_{q^n}$). Given a non-zero q-polynomial L over $\mathbb{F}_{q^n}$, a root α of L is a *q-primitive root* over $\mathbb{F}_{q^n}$ if it is not a root of any non-zero q-polynomial of lower degree. Conversely, the monic q-polynomial over $\mathbb{F}_{q^n}$ of least positive degree having α as a root is the *minimal q-polynomial* of α over $\mathbb{F}_{q^n}$. The polynomials $l(x) = \sum_{i=0}^{d} \alpha_i x^i$ and $L(x) = \sum_{i=0}^{d} \alpha_i x^{q^i}$ over $\mathbb{F}_{q^n}$ are *q-associates* of each other. If $\mathbb{F}_{q^s}$ contains all the roots of L, then these roots form a subspace of the vector space $\mathbb{F}_{q^s}$ over $\mathbb{F}_q$.

We now consider q-polynomials over $\mathbb{F}_q$. A finite dimensional vector space $\mathcal{M}$ over $\mathbb{F}_q$ is a *q-modulus* if it is contained in some extension field of $\mathbb{F}_q$ and has the property that the q-th power of every element of $\mathcal{M}$ also lies in $\mathcal{M}$. From [11, Theorem 3.65], the monic polynomial L is a q-polynomial over $\mathbb{F}_q$ if and only if each root of L has the same multiplicity (1 or a power of q) and its roots form a q-modulus.

Following [10], the $\mathbb{F}_q$-Order of an element γ is defined to be the (unique) monic polynomial $f(x) = \sum f_i x^i \in \mathbb{F}_q[x]$ of least degree such that $\sum f_i \gamma^{q^i} = 0$. Thus, if γ is a q-primitive root of a monic q-polynomial L over $\mathbb{F}_q$ and l is the q-associate of L, then γ has $\mathbb{F}_q$-Order l and we write $\operatorname{Ord}(\gamma) = l$. Clearly $\operatorname{Ord}(\gamma)$ divides $x^n - 1$ if and only if $\gamma \in \mathbb{F}_{q^n}$.

Lemma 3.1. *Let $\alpha \in \mathbb{F}_{q^n}$. Let A_α be the matrix given by Equation* (1)*. Denote by M the vector space* $\operatorname{Span}\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ *over $\mathbb{F}_q$. Then* $\operatorname{rank} A_\alpha = \dim(M)$*.*

Proof. The column-space of A_α is given by $\operatorname{Span}\{C_0, C_1, \ldots, C_{n-1}\}$, where each column C_i is given by the transpose of $\left[\alpha^{q^i}, (\alpha^{q^i})^{q^{n-1}}, (\alpha^{q^i})^{q^{n-2}}, \ldots, (\alpha^{q^i})^q\right]$. Suppose M has dimension m as a vector space over $\mathbb{F}_q$; then a basis for the column-space of A_α is given by the set of m columns of A_α whose first entries are the basis elements of M. Conversely, given a basis of the column-space of A_α, a basis of M is immediately obtainable by taking the first entry of each column. □

Theorem 3.2. *Let $\alpha \in \mathbb{F}_{q^n}$. Then the following three properties are equivalent:*

(i) α *is* k*-normal over* $\mathbb{F}_q$*;*

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

(iii) $\deg(\mathrm{Ord}(\alpha)) = n-k$.

Proof. Let $\alpha \in \mathbb{F}_{q^n}$. We prove $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)$. For $(i) \Rightarrow (ii)$, suppose that $\alpha \in \mathbb{F}_{q^n}$ is k-normal. By Theorem 2.5, the matrix A_α has rank $n-k$, and so by Lemma 3.1, the vector space M also has dimension $n-k$ over $\mathbb{F}_q$. It may be verified that $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-k-1}}\}$ forms a basis for M. If $\beta \in M$ then $\beta^q \in M$, and so M is a q-modulus of dimension $n-k$ over $\mathbb{F}_q$.

For (ii) ⇒ (iii), suppose $B = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-k-1}}\}$ is the basis of a q-modulus N of dimension $n-k$ over $\mathbb{F}_q$. Let $L(x) = \prod_{\beta \in N}(x-\beta)$; then by [11, Theorem 3.65], L is a (monic) q-polynomial of degree q^{n-k} over $\mathbb{F}_q$. Since $\alpha \in N$, L has α as a root. Since the elements of B are linearly independent, α cannot satisfy a q-polynomial of degree less than q^{n-k}. Hence α is a q-primitive root of L, and $\mathrm{Ord}(\alpha) = l$ where l is the q-associate of L, of degree $n-k$.

Finally, for (iii) ⇒ (i), suppose $\mathrm{Ord}(\alpha)$ has degree $n-k$, that is α is a q-primitive root of a q-polynomial L over $\mathbb{F}_q$ of degree q^{n-k}. Then $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-k-1}}\}$ forms a basis for M. By Lemma 3.1, A_α has rank $n-k$ and thus α is k-normal over $\mathbb{F}_q$. □

The following result, due to Ore [13], allows us to use the preceding theorem to obtain a formula for the number of k-normal elements.

Lemma 3.3. *Let $f \in \mathbb{F}_q[x]$ be monic and relatively prime to x. Then the number of α in the algebraic closure of $\mathbb{F}_q$ with $\mathrm{Ord}(\alpha) = f$ equals $\Phi_q(f)$.*

Theorem 3.4. *The number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ equals 0 if there is no $h \in \mathbb{F}_q[x]$ of degree $n-k$ dividing x^n-1; otherwise it is given by*

$$\sum_{\substack{h \mid x^n-1,\\ \deg(h)=n-k}} \Phi_q(h), \tag{2}$$

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

Proof. Using criteria (iii) of Theorem 3.2, combined with Ore's result from Lemma 3.3, the total number of k-normal elements $\alpha \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is given by

$$\sum_{\substack{h \mid x^n-1,\\ \deg(h)=n-k}} \Phi_q(h). \qquad \square$$

We emphasize that the factorization of x^n-1 in Equation (2) is the $\mathbb{F}_q$-factorization of x^n-1. We further note that when $k=0$, that is, when counting the number of normal elements, the above summation reduces to $\Phi_q(x^n-1)$, as expected.

4. Bounds on the number of k-normal elements

Suppose $f \in \mathbb{F}_q[x]$ has degree n and let $\kappa(f) = q^{-n}\Phi_q(f)$ where, as usual, Φ_q denotes Euler's Phi function for polynomials over $\mathbb{F}_q$. The measure $\kappa(x^n-1)$ gives the density of normal elements over $\mathbb{F}_q$. Bounds on $\kappa(f)$, for general f, are obtained in [7]. Additionally, lower bounds for the density of normal elements are given in [7] as well as an upper-bound on the density of normal elements for infinitely many n. These results are improved in [6] for the specific polynomial $f(x) = x^n-1$.

Recall from Theorem 3.4, that the number of k-normal elements is given by

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

Suppose L and U are lower and upper bounds, respectively, for $\Phi_q(h)$, where h is any monic divisor of x^n-1 over $\mathbb{F}_q$ with degree $n-k$. Thus,

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

Let c_{n-k} be the number of divisors of x^n-1 with degree $n-k$. Then

$$c_{n-k}L \le |\{\alpha \in \mathbb{F}_{q^n} : \alpha \text{ is } k\text{-normal over } \mathbb{F}_q\}| \le c_{n-k}U.$$

By [11, Theorem 2.45(i)], if n is a positive integer not divisible by the characteristic of $\mathbb{F}_q$, we have $x^n-1=\prod_{d|n}Q_d(x)$, where Q_d is the d-th cyclotomic polynomial. The polynomial Q_d has degree $\phi(d)$, where ϕ is the Euler totient function. Thus c_{n-k} can be determined by the number of ways of writing $n-k$ as the sum of terms of the form $\phi(d)$, where d is a divisor n.

We note that c_{n-k} could be 0. For example, if the factorization of x^n-1 into irreducibles over $\mathbb{F}_q$ is $x^n-1=(x-1)(x^{n-1}+x^{n-2}+\cdots+x+1)$, then $c_n=c_{n-1}=c_1=1$, and $c_j=0$, for all other j.

4.1. Lower bounds

We state the explicit lower bound in [7] for $\kappa(f)$, for any $f\in\mathbb{F}_q[x]$.

Theorem 4.1. *[7] For any $f\in\mathbb{F}_q[x]$ of degree n with $f(0)\neq 0$, if $n\ge q$, then*

$$\kappa(f) \ge \frac{1}{e^{0.83}(1+\log_q(n))},$$

and if $n<q$, then $\kappa(f)>1/e$.

Thus, for any h of degree $n-k$, $\kappa(h)\ge 1/\left(e^{0.83}(1+\log_q(n-k))\right)$. However, the lower bound on the density of normal elements was improved in [6] by considering the particular case $f(x)=x^n-1$.

Theorem 4.2. *[6] There is a constant c such that, for all $q,n\ge 2$,*

$$\kappa(x^n-1)\ge c\frac{1}{\sqrt{\log_q(n)}}.$$

This bound is not explicit, but it is shown to be optimal in the sense that

$$\liminf_{n\to\infty}\kappa(x^n-1)\ge\frac{0.28477}{\sqrt{\log_q(n)}}.$$

We use a multiplicative form of $\Phi_q(f)$, which can be found in [11, Theorem 3.69].

Theorem 4.3. *Let $f\in\mathbb{F}_q[x]$ and suppose f has complete factorization $f=\prod_{i=1}^t f_i^{e_i}$ over $\mathbb{F}_q$ (that is, the irreducible factors f_i,f_j are distinct when $i\neq j$). Then*

$$\kappa(f)=\prod_{i=1}^t\left(1-\frac{1}{q^{n_i}}\right),$$

where n_i is the degree of f_i, and $n\ge 1$ is the degree of f.

We follow [6, Section 3] to give a strong lower bound on the number of k-normal elements. First, denote by $I_q(d;f)$ the number of irreducible factors of f having degree d, and denote by $I_q^*(d;f)$ the number of irreducible factors of f, not counting the single factor x, having degree d. In most cases, $I_q=I_q^*$.

For the remainder of this section, let f be any divisor of $x^n - 1$ of degree $n-k$. We define the values $A^{(f)}_{q,n,k}$ to be the set of those degrees $d \in \{1, 2, \ldots, n-k\}$ for which

$$I^*_q(d; f) > \frac{q^d - 1}{2d^2}$$

and $B^{(f)}_{q,n,k}$ to be the set of those degrees $d \in \{1, 2, \ldots, n-k\}$ for which $I^*_q(d, f) \leq \frac{q^d-1}{2d^2}$.

We show that we can ignore the contribution from the entries in $B^{(f)}_{q,n,k}$. The proof is very similar to [6, Lemma 8]; the difference in our case is that we consider any f dividing $x^n - 1$ rather than $x^n - 1$ itself, and our sets $A^{(f)}_{q,n,k}$ and $B^{(f)}_{q,n,k}$ replace the sets $A_{q,n}$ and $B_{q,n}$, respectively, from [6].

Lemma 4.4. *Let $f, A^{(f)}_{q,n,k}$ and $B^{(f)}_{q,n,k}$ be defined as above. Then*

$$\kappa(f) \geq \begin{cases} e^{-\zeta(2)/2} \approx 0.43935 & \text{if } A^{(f)}_{q,n,k} = \emptyset, \\ e^{-\gamma} \cdot \frac{e^{\left(|A^{(f)}_{q,n,k}|-1\right)}}{\left|A^{(f)}_{q,n,k}\right|} & \text{otherwise,} \end{cases}$$

where γ is Euler's constant and ζ is the zeta function.

The remaining lemmata in [6, Section 3] provide upper-bounds for $|A_{q,n}|$ $\left(\text{respectively, } \left|A^{(f)}_{q,n,k}\right|\right)$. The proofs of our case also follow directly from [6] and so we state our analogous results without proof.

Lemma 4.5. *For any finite set of natural numbers A, denote by $\operatorname{lcm}_{d\in A}$ the least common multiple of the elements of A. We have the following three assertions:*

1. $I^*_q(d, f) \leq \gcd(q^d - 1, n)/d$,
2. $n \geq \operatorname{lcm}_{d\in A^{(f)}_{q,n,k}}(q^d - 1)/\prod_{d\in A^{(f)}_{q,n,k}}(2d)$,
3. *if A is a finite set of natural numbers, then* $\operatorname{lcm}_{d\in A}(q^d - 1)/\prod_{d\in A}(2d) \geq q^{c|A|^2 - o(|A|^2)}$, *where* $c = \zeta(6)/(2\zeta(2)\zeta(3)) \approx 0.25726$.

We now combine all of the previous results to give a lower-bound on the number of k-normal elements.

Theorem 4.6. *There is a constant c such that for all $q \geq 2$ and $n > q^c$, the number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is at least*

$$0.28477 \cdot q^{n-k} \frac{c_{n-k}}{\sqrt{\log_q(n)}}.$$

Proof. (Sketch) First, suppose $A^{(f)}_{q,n,k} = \emptyset$. Then, we have that $\kappa(f) \geq e^{-\zeta(2)/2}$, and so

$$\Phi_q(f) \geq q^{n-k} e^{-\zeta(2)/2} \approx 0.43935 q^{n-k}.$$

Thus, the number of k-normal elements in this case is at least $0.43935 q^{n-k} c_{n-k}$, where c_{n-k} is the number of ways of writing $n-k$ as the sum of terms of the form $\phi(d)$, where d is a divisor of n.

The proof of the case when $A^{(f)}_{q,n,k} \neq \emptyset$ follows from [6]. Where our proof differs from [6] is that we apply Lemma 4.5 to the set $A^{(f)}_{q,n,k}$, where f is a divisor of $x^n - 1$. This corresponds to the set $A_{q,n}$ and the polynomial $f(x) = x^n - 1$. Hence, as in [6], we get the expression

$$\kappa(f) \geq e^{-\gamma}\sqrt{c'}\frac{1}{\log_q(n)},$$

where $e^{-\gamma}\sqrt{c'} > 0.28477$. Summing over all such f and expanding $\kappa(f)q^{n-k} = \Phi_q(f)$ gives that the number of k-normal elements is at least $0.28477 \cdot c_{n-k} q^{n-k}/\log_q(n)$. □

4.2. Upper bounds for infinitely many n

Upper bounds for $\kappa(x^n-1)$ are given in [6, 7] for an infinite family of n. In general, non-trivial upper bounds for $\kappa(x^n-1)$ are not known. In order to obtain upper-bounds on the number of k-normal elements, we note that if h divides x^n-1, then $\Phi_q(h) \leq \Phi_q(x^n-1)$.

Theorem 4.7. *Let*

$$n_k = \mathrm{lcm}_{1\leq d\leq k}(q^d-1),$$

then for every prime power q and any integer k,

$$\kappa(x^{n_k}-1) < 0.61910\frac{1}{\sqrt{\log_q(n_k)}}.$$

Corollary 4.8. *For any integer k, let n_k be as in Theorem 4.7. Then the number of k-normal elements of $\mathbb{F}_{q^{n_k}}$ is at most*

$$0.61910 \cdot q^{n-k}\frac{c_{n_k-k}}{\sqrt{\log_q(n_k)}}.$$

5. Primitive *k*-normal elements

An important extension of the normal basis theorem is the primitive normal basis theorem, which establishes that a normal basis $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ always exists with α primitive. We ask whether an analogous claim can be made about k-normal elements for certain values of k. In particular, when $k=1$, does there always exist a primitive 1-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$? We use the methods introduced in Carlitz [1] and Davenport [4] and then refined in Lenstra and Schoof [10] to determine the existence of primitive 1-normal elements. In this section, we closely follow [10].

For given q and n, let f be a monic divisor of x^n-1 of degree $n-1$ and define $A = \{\alpha \in \mathbb{F}_{q^n} : \mathrm{Ord}(\alpha) = x^n-1\}$, $A_\zeta = \{\alpha \in \mathbb{F}_{q^n} : \mathrm{Ord}(\alpha) = (x^n-1)/(x-\zeta)\}$ and $B = \{\alpha \in \mathbb{F}_{q^n}^* : \mathrm{ord}(\alpha) = q^n-1\}$. We also use the following terminology: for a divisor m of q^n-1, we call $\alpha \in \mathbb{F}_{q^n}$ m-free if $\alpha = \beta^d$ for any divisor d of m implies $d=1$. Furthermore, for any divisor M of x^n-1, we call α M-free if $\alpha = H(\beta)$, where H is the q-associate of a divisor h of $(x^n-1)/\mathrm{Ord}(\alpha)$, implies $h=1$. Normal elements are those which are (x^n-1)-free and primitive elements are those which are (q^n-1)-free. In what follows, we are interested in elements that are simultaneously (q^n-1)-free and $\frac{x^n-1}{x-\zeta}$-free for some appropriate ζ.

We define additive and multiplicative characters which determine when an element is (q^n-1)-free and f-free, respectively. We note that the multiplicative characters of $\mathbb{F}_{q^n}$ form a $\mathbb{F}_q[x]$-module by defining $\lambda^f(\alpha) = \lambda(f \circ \alpha)$, where the composition is given by $x \circ \alpha = \alpha^q$. Thus, we define $\mathrm{Ord}(\lambda)$ as the annihilator of λ.

For $\alpha \in \mathbb{F}_{q^n}^*$, we define

$$\omega(\alpha) = \sum_{d|q^n-1}\frac{\mu(d)}{\phi(d)}\sum_{\chi,\mathrm{ord}(\chi)=d}\chi(\alpha),$$

where μ is the Möbius function, and we also define

$$\Omega_1(\alpha) = \sum_{g|f}\frac{M(g)}{\Phi_q(g)}\sum_{\lambda,\mathrm{Ord}(\lambda)=g}\lambda(\alpha),$$

where M is the Möbius function for polynomials.

Lemma 5.1. [10] *Let q, n and ω be defined as above. Then, for $\alpha \in \mathbb{F}_{q^n}^*$, $\omega(\alpha) = 0$, if $\alpha \notin B$.*

Lemma 5.2. *Let q, n and Ω_1 be defined as above. Then, for $\alpha \in \mathbb{F}_{q^n}$, $\Omega_1(\alpha) = 0$ if $\alpha \notin A \cup A_\zeta$.*

Proof. We note that exactly $\Phi_q(g)$ characters have $\mathbb{F}_q$-Order g, see [13], and re-write Ω_1 as the product

$$\begin{aligned}\Omega_1(\alpha) &= \prod_{\ell \mid f, \ell \text{ irred}} \left(1 - \frac{1}{\Phi_q(\ell)} \sum_{\lambda, \operatorname{Ord}(\lambda)=\ell} \lambda(\alpha)\right) \\ &= \prod_{\ell \mid f, \ell \text{ irred}} \left(\frac{\Phi_q(\ell)+1}{\Phi_q(\ell)} - \frac{1}{\Phi_q(\ell)} \sum_{\lambda, \lambda^{\ell}=1} \lambda(\alpha)\right).\end{aligned}$$

The set $\{\lambda : \lambda^{\ell} = 1\}$ can be identified with the dual of the subgroup $\mathbb{F}_{q^n}/(\ell \circ \mathbb{F}_{q^n})$; in particular, it is a group and

$$\sum_{\lambda^{\ell}=1} \lambda(\alpha) = \begin{cases} \Phi_q(\ell) + 1 & \text{if } \alpha = \ell \circ \beta,\ \beta \in \mathbb{F}_{q^n}, \\ 0 & \text{otherwise.} \end{cases}$$

□

We extend the characters to all of $\mathbb{F}_{q^n}$ by defining $\chi(0) = 0$ for $\chi \neq 1$ and $1(0) = 1$.

Theorem 5.3. *There exists a primitive* 1*-normal element of* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$ *for sufficiently large* q *and* n*.*

Proof. We note that there are $\gcd(n, q-1)$ roots $\zeta \in \mathbb{F}_q$ of $x^n - 1$, but Lemma 5.2 does not depend on the choice of ζ (except for the choice of f). In order to prove existence of primitive 1-normal elements, it is enough to show the existence of at least one element which is $(q^n - 1)$-free and $\frac{x^n-1}{x-\zeta}$-free, for some ζ, but not $(x^n - 1)$-free. Suppose now that $f(x) = \frac{x^n-1}{x-\zeta}$ for a fixed n-th root of unity ζ. Thus, there exists a primitive 1-normal element if for some such f we have

$$\sum_{\alpha \in \mathbb{F}_{q^n}} \omega(\alpha)\Omega_1(\alpha) - \sum_{\alpha \in \mathbb{F}_{q^n}} \omega(\alpha)\Omega(\alpha) \neq 0,$$

where, as in [10],

$$\Omega(\alpha) = \sum_{g \mid x^n - 1} \frac{M(g)}{\Phi_q(g)} \sum_{\lambda, \operatorname{Ord}(\lambda)=g} \lambda(\alpha).$$

Suppose there is no primitive f-free element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then

$$\begin{aligned} 0 = &\sum_{d \mid q^n-1} \sum_{g \mid f} \frac{\mu(d)M(g)}{\phi(d)\Phi_q(g)} \sum_{\chi, \operatorname{ord}(\chi)=d} \sum_{\lambda, \operatorname{Ord}(\lambda)=g} \tau(\chi, \lambda) \\ &- \sum_{d \mid q^n-1} \sum_{g \mid x^n-1} \frac{\mu(d)M(g)}{\phi(d)\Phi_q(g)} \sum_{\chi, \operatorname{ord}(\chi)=d} \sum_{\lambda, \operatorname{Ord}(\lambda)=g} \tau(\chi, \lambda), \end{aligned}$$

where $\tau(\chi, \lambda) = \sum_{\alpha \in \mathbb{F}_{q^n}} \chi(\alpha)\lambda(\alpha)$. As in [10], the Gauss sum τ satisfies

$$\begin{aligned} &\tau(1, 1) = q^n, \\ &\tau(1, \lambda) = 0 \text{ for } \lambda \neq 1, \\ &\tau(\chi, 1) = 0 \text{ for } \chi \neq 1 \end{aligned}$$

and $|\tau(\chi, \lambda)| = q^{n/2}$ if $\chi \neq 1$ and $\lambda \neq 1$. Removing the trivial characters gives

$$\begin{aligned} -q^n = &\sum_{\substack{d \mid q^n-1, \\ d \neq 1}} \sum_{g \mid f, g \neq 1} \frac{\mu(d)M(g)}{\phi(d)\Phi_q(g)} \sum_{\chi, \operatorname{ord}(\chi)=d} \sum_{\lambda, \operatorname{Ord}(\lambda)=g} \tau(\chi, \lambda) \\ &- \sum_{\substack{d \mid q^n-1, \\ d \neq 1}} \sum_{\substack{g \mid x^n-1, \\ g \neq 1}} \frac{\mu(d)M(g)}{\phi(d)\Phi_q(g)} \sum_{\chi, \operatorname{ord}(\chi)=d} \sum_{\lambda, \operatorname{Ord}(\lambda)=g} \tau(\chi, \lambda) \\ = &- \sum_{\substack{d \mid q^n-1, \\ d \neq 1}} \sum_{\substack{g \mid x^n-1 \\ g \nmid f, g \neq 1}} \frac{\mu(d)M(g)}{\phi(d)\Phi_q(g)} \sum_{\chi, \operatorname{ord}(\chi)=d} \sum_{\lambda, \operatorname{Ord}(\lambda)=g} \tau(\chi, \lambda). \end{aligned}$$

Let s be the number of distinct prime factors of q^n-1 and let t be the number of monic irreducible factors of f. Taking absolute values we find, as in [3],

$$\begin{aligned} q^n &\leq q^{n/2} \sum_{\substack{d|q^n-1,\\ d\neq 1}} \sum_{\substack{g|x^n-1\\ g\nmid f, g\neq 1}} |\mu(d)M(g)| \\ &\leq q^{n/2}(2^s-1)(2^t-1). \end{aligned}$$

By [3, Lemma 3.3], we have $2^s \leq c_s(q^n-1)^{1/4}$ where c_s is a constant at most 4.9. Furthermore, $\deg(f) = n-1$ and so $t \leq n-1$. Thus,

$$q^n < 5q^{n/2} \cdot q^{n/4} \cdot 2^{n-1},$$

which is a contradiction if $5 \cdot 2^{n-1} < q^{n/4}$; for example, when $q > 2^5$ and $n > 8$. □

6. Conclusions and open problems

In this paper, we have generalized the concept of normal elements to that of k-normal elements, with the classical normal elements being 0-normal. We have characterized k-normal elements and given a formula for the number of such elements in terms of Euler's Phi function for polynomials. We have also given both upper and lower numerical bounds on their number. The primitive normal basis theorem proves the existence of primitive 0-normal elements over any finite field; we have obtained an asymptotic result which establishes the existence of primitive 1-normal elements.

Here we present some problems, motivated both by theoretical considerations and by data obtained through computer search of small finite fields.

Problem 6.1. *For which values of q, n and k can "nice" explicit formulae (in q and n) be obtained for the number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$?*

This question is closely related to being able to determine the factorization of x^n-1 into irreducibles over $\mathbb{F}_q$.

Problem 6.2. *Show that primitive 1-normal elements exist for all degrees n over all finite fields (with or without a computer).*

Table 1 gives the number of k-normal and primitive k-normal elements over some small finite fields.

	$q=2$, $n=6$			$q=5$, $n=6$			$q=5$, $n=7$	
k	# k-norm.	# pr. k-norm.	k	# k-norm.	# pr. k-norm.	k	# k-norm.	# pr. k-norm.
0	24	18	0	9216	2568	0	62496	31248
1	12	12	1	4608	1320	1	15624	7811
2	18	5	2	1344	360	2	0	0
3	3	0	3	384	71	3	0	0
4	5	0	4	64	0	4	0	0
5	1	0	5	8	0	5	0	0
						6	4	0

Table 1: Number of k-normal and primitive k-normal elements over some small finite fields.

Problem 6.3. *Determine the values of k such that there exist primitive k-normal elements over any finite field.*

For example, we can immediately show that there are no primitive $(n-1)$-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Suppose α is a primitive $(n-1)$-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then, α satisfies $(x-\beta)\circ\alpha = 0$ for some $\beta \in \mathbb{F}_q$. Thus $(x-\beta)\circ\alpha = \alpha^q - \beta\alpha = 0$ and $\alpha^{q-1} \in \mathbb{F}_q$. The multiplicative order of α therefore divides $(q-1)^2$, which is a contradiction for $n \geq 2$.

Primitive elements of degree n over $\mathbb{F}_q$ are (q^n-1)-free, and for any divisor N of q^n-1, elements having order not properly dividing N are N-free. If f is a divisor of x^n-1, there is an additive (polynomial) analog; elements which are f-free have $\mathbb{F}_q$-Order which is not a proper divisor of f. Character sum estimates for the number of (N, f)-free elements are given in [3].

Another direction of research is a relaxation of the primitive condition, yielding elements of "high order".

Problem 6.4. *Determine the existence of high-order k-normal elements $\alpha \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where "high order" means $\operatorname{ord}(\alpha) = N$ with N a large positive divisor of $q^n - 1$.*

[1] L. Carlitz, Primitive roots in a finite field, *Transactions of the American Mathematical Society*, **73** (1952), 373-382.

[2] L. Carlitz, Some problems involving primitive roots in a finite field, *Proceedings of the National Academy of Sciences of the USA*, **38** (1952), 314-318.

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

[4] H. Davenport, Bases for finite fields, *Journal of the London Mathematical Society*, **43** (1968), 21-39.

[5] D. E. Daykin, On the rank of the matrix $f(A)$ and the enumeration of certain matrices over a finite field, *Journal of the London Mathematical Society*, **35** (1960), 36-42.

[6] G. S. Fransden, On the density of normal bases in finite fields, *Finite Fields and Their Applications*, **6** (2000), 23-38.

[7] S. Gao and D. Panario, Density of normal elements, *Finite Fields and Their Applications*, **3** (1997), 141-150.

[8] J. von zur Gathen and J. Gerhard, Modern Computer Algebra, Cambridge University Press, (Cambridge) 2003.

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

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

[11] R. Lidl and H. Niederreiter, Finite Fields: Encylopedia of Mathematics and its Applications, Vol. 20 (2nd ed.), Cambridge University Press, (Cambridge) 1997.

[12] C. Negre, Finite field arithmetic using quasi-normal bases, *Finite Fields and Their Applications*, **13** (2007), 635-647.

[13] O. Ore, Contributions to the theory of finite fields, *Transactions of the American Mathematical Society*, **36** (1934), 243-274.