

On k -normal elements over finite fields

21 de Outubro de 2021

Lucas Reis – Universidade Federal de Minas Gerais

Introduction

k-normal elements

Character sum method

Results

Introduction

1. For $q = p^s$ a prime power, \mathbb{F}_q denotes the finite field with q elements.
2. For each positive integer n , \mathbb{F}_{q^n} is the unique n -degree extension of \mathbb{F}_q .
3. For any finite field \mathbb{F} , the multiplicative group \mathbb{F}^* is cyclic.
4. Any generator of \mathbb{F}^* is a **primitive element** of \mathbb{F} . (if $q = p$ is a prime, primitive elements are just primitive roots mod p).
5. Primitive elements are remarkable elements in the multiplicative structure of finite fields, and are widely used in applications (e.g. the Discrete Logarithm Problem).

But finite fields have another important structure...

We observe that \mathbb{F}_{q^n} can be regarded as an \mathbb{F}_q -vector space (of dimension n).

For each $\beta \in \mathbb{F}_{q^n}$, let V_β be the \mathbb{F}_q -vector space generated by the \mathbb{F}_q -Galois conjugates of β :

$$\beta, \beta^q, \dots, \beta^{q^{n-1}}.$$

Definition

*An element $\alpha \in \mathbb{F}_{q^n}$ is **normal** over \mathbb{F}_q if $V_\alpha = \mathbb{F}_{q^n}$, that is, the \mathbb{F}_q -Galois conjugates of α comprise an \mathbb{F}_q -basis for \mathbb{F}_{q^n} .*

Normal elements are quite useful in the arithmetic of finite fields. This is mainly due to the fact that some exponentiations are easy to compute:

$$\beta = \sum_{i=0}^{n-1} c_i \alpha^{q^i} \sim (c_0, \dots, c_{n-1}) \Rightarrow$$

$$\beta^q = \sum_{i=0}^{n-1} c_i \alpha^{q^{i+1}} \sim (c_1, \dots, c_{n-1}, c_0).$$

We can combine primitivity and normality...

Theorem (Primitive Normal Basis Theorem)

For any prime power q and any $n \geq 2$, there exists an element $\alpha \in \mathbb{F}_{q^n}$ that is simultaneously primitive and normal (over \mathbb{F}_q).

1. First proof by Lenstra and Schoof (Math. Comp. - 86') with the help of computers.
2. Computer-free proof by Cohen and Huczynska (Proc. LMS - 03').
3. Main tool: character sum formula for the indicator function of primitive and normal elements (additive and multiplicative characters of finite fields), and bounds on character sums.

k-normal elements

Motivated by the concept of normal elements of finite fields, in 2013 Huczynska, Mullen, Panario and Thomson introduced the notion of k -normal elements:

Definition

An element $\alpha \in \mathbb{F}_{q^n}$ is k -normal over \mathbb{F}_q , if the \mathbb{F}_q -vector space V_α generated by the elements

$$\alpha, \alpha^q, \dots, \alpha^{q^{n-1}},$$

is of dimension $n - k$.

1. we always have $0 \leq k \leq n$;
2. $k = 0$ recovers the normal elements, that is, 0-normal elements are just the usual normal elements;
3. $k = n$ implies $\alpha = 0$.

Motivated by the Primitive Normal Basis Theorem, in the same paper the authors proposed the following problem:

Problem

*For what pairs (k, n) can we guarantee the existence of an element $\alpha \in \mathbb{F}_{q^n}$ that is **primitive** and **k -normal** over \mathbb{F}_q ?*

1. case $k = 0$ is the Primitive Normal Basis Theorem;
2. (R. and Thomson, FFA - 18') positive answer if $k = 1$ for arbitrary q and $n \geq 3$ (the case $n = 2$ is a genuine exception for arbitrary q);
3. (J. Aguirre and V. Neumann, FFA 21') positive answer for $k = 2$ iff $n \geq 5$ and $\gcd(q^3 - q, n) > 1$, or $n = 4$ and $q \equiv 1 \pmod{4}$.
4. **negative answer** for $k = n$ and $k = n - 1$ (this is mentioned in the 2013 paper).

In this talk we discuss the previous problem, providing some asymptotic results.

An important related problem is the description of the triples (q, n, k) for which there exist elements of \mathbb{F}_{q^n} that are k -normal (over \mathbb{F}_q).

We start noticing that k -normality depends on the base field:

1. Let $\mathbb{F}_{16} = \mathbb{F}_2(\beta)$ with $\beta^4 + \beta + 1 = 0$.
2. β is 1-normal over \mathbb{F}_2 :

$$\langle \beta, \beta^2, \beta^4, \beta^8 \rangle_{\mathbb{F}_2} = \langle 1, \beta, \beta^2 \rangle_{\mathbb{F}_2}.$$

3. β is 0-normal over \mathbb{F}_4 .

Observe that if we want to compute the dimension of $V_\alpha = \{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$, it is interesting to consider the \mathbb{F}_q -linear combinations of such elements that vanish.

The \mathbb{F}_q -order of an element

The latter can be nicely explored through the $\mathbb{F}_q[x]$ -module structure of finite fields:

Definition

For a polynomial $f(x) = \sum a_i x^i \in \mathbb{F}_q[x]$ and $\alpha \in \mathbb{F}_{q^n}$, set

$$f \circ \alpha = \sum a_i \alpha^{q^i}.$$

Some properties:

1. $(f + g) \circ \alpha = (f \circ \alpha) + (g \circ \alpha)$;
2. $(f \cdot g) \circ \alpha = f \circ (g \circ \alpha)$
3. $f \circ 0 = 0$.

In particular, the set $\mathcal{I}_\alpha = \{g \in \mathbb{F}_q[x] \mid g \circ \alpha = 0\}$ is an ideal of $\mathbb{F}_q[x]$.

For $\alpha \in \mathbb{F}_{q^n}$, we have that $\alpha^{q^n} = \alpha$, hence $x^n - 1 \in \mathcal{I}_\alpha$. Since, $\mathbb{F}_q[x]$ is a PID, we obtain the following result:

Theorem

For each $\alpha \in \mathbb{F}_{q^n}$ there exists a monic polynomial $m_\alpha \in \mathbb{F}_q[x]$ (the \mathbb{F}_q -order of α) generating the ideal I_α . Moreover, $m_\alpha(x)$ is a divisor of $x^n - 1$.

Example

Let $\mathbb{F}_{16} = \mathbb{F}_2(\beta)$ with $\beta^4 = \beta + 1$. Then β has \mathbb{F}_2 -order $x^3 + x^2 + x + 1 = \frac{x^4-1}{x-1}$, and \mathbb{F}_4 -order $x^2 - 1$.

The converse is also true:

Theorem

For a monic divisor $f \in \mathbb{F}_q[x]$ of $x^n - 1$, there exist $\Phi_q(f)$ elements $\alpha \in \mathbb{F}_{q^n}$ such that $m_\alpha = f$, where $\Phi_q(f)$ is the **Euler Totient function** for polynomials.

Proof: Inclusion-exclusion argument, noticing that the equation

$$f \circ \alpha = 0,$$

has $q^{\deg(f)}$ solutions in \mathbb{F}_{q^n} , and such solutions are elements of \mathbb{F}_q -order F (monic) with $F|f$.

$$\phi(n) = n \prod_{P|n} \left(1 - \frac{1}{P}\right) \quad \longrightarrow \quad \Phi_q(f) = q^{\deg(f)} \prod_{\substack{g|f \\ g \text{ irreducible}}} \left(1 - \frac{1}{q^{\deg(g)}}\right).$$

The \mathbb{F}_q -order determines the normality:

Theorem

An element $\alpha \in \mathbb{F}_{q^n}$ is k -normal over \mathbb{F}_q iff the \mathbb{F}_q -order of α is a polynomial of degree $n - k$.

Proof: The Rank-Nullity Theorem applied to the (surjective) map

$$\varphi_\alpha : \frac{\mathbb{F}_q[x]}{(x^n - 1)\mathbb{F}_q[x]} \rightarrow V_\alpha = \langle \alpha, \alpha^q, \dots, \alpha^{q^{n-1}} \rangle_{\mathbb{F}_q},$$

with $\varphi_\alpha(g) = g \circ \alpha$, noticing that

$$\ker \varphi_\alpha = \{m_\alpha \cdot H \mid \deg(H) < n - \deg(m_\alpha)\} \Rightarrow \dim_{\mathbb{F}_q} \ker \varphi_\alpha = n - \deg(m_\alpha).$$

In particular, an element $\beta \in \mathbb{F}_{q^n}$ is normal over \mathbb{F}_q if and only if its \mathbb{F}_q -order equals $x^n - 1$.

Corollary

The number of k -normal elements in \mathbb{F}_{q^n} (over \mathbb{F}_q) equals

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

where the sum is over the monic divisors of $x^n - 1$ of degree $n - k$.

In particular, k -normal elements exist if and only if $x^n - 1$ has a divisor of degree k over \mathbb{F}_q !

Observe that $1, x - 1, \frac{x^n - 1}{x - 1}$ and $x^n - 1$ are divisors of $x^n - 1$, hence we always have k -normal elements for $k = 0, 1, n - 1, n$.

Example

1. *if n is a prime and q is a primitive root (mod n), we only have k -normal elements for $k = 0, 1, n - 1, n$.*
2. *if n is a power of $p = \text{Char}(\mathbb{F}_q)$, we have k -normal elements every $0 \leq k \leq n$.*

The second case deserves special attention...

A natural number N is φ -practical if every integer $1 \leq k \leq N$ can be written as a sum of terms $\varphi(d)$ with $d|N$ (no repetitions allowed). In other words, the polynomial $x^N - 1$ has divisors (over \mathbb{Q}) of every possible degree!

Motivated by the latter, a natural number N is \mathbb{F}_q -practical if the polynomial $x^n - 1$ has divisors (over \mathbb{F}_q) of every possible degree.

Distribution of practical numbers (up to $T \gg 1$):

1. φ -practical numbers: $\frac{CT}{\log T}$ (C. Pomerance, L.Thompson and A. Weingartner, Acta Arith. 16')
2. \mathbb{F}_p -practical numbers (p is prime), **under GRH**:
 $O\left(T \sqrt{\frac{\log \log T}{\log T}}\right)$ (L. Thompson, IJNT 13').

Describing the \mathbb{F}_q -practical numbers seems to be a very difficult problem...

But we can still find large classes of them:

Theorem (R. 19')

Let n be a positive integer with $\text{rad}(n) \mid p(q-1)$. Then n is \mathbb{F}_q -practical.

Proof: induction on the number of prime factors of n , using a classical result on the factorization of cyclotomic polynomials over finite fields (the inductive step is constructive).

Example

1. $n = 2^s$ is always \mathbb{F}_q -practical;
2. $n = 3^s$ is \mathbb{F}_q -practical if $q \equiv 0, 1 \pmod{3}$.

Character sum method

A recurrent problem in the theory of finite fields is the existence of elements in finite fields with special properties. In general, we have two (structured) subsets $A, B \subset \mathbb{F}$ (encoding these properties) and we want to prove that

$$A \cap B \neq \emptyset.$$

In other words, if 1_X stands for the indicator function of a set $X \subseteq \mathbb{F}$ (1 at elements of X and 0 elsewhere), we want to verify that (one of the equivalent expressions)

$$\sum_{x \in \mathbb{F}_{q^n}} 1_A(x) \cdot 1_B(x), \quad \sum_{x \in A} 1_B(x),$$

is **positive**.

Most of the works consider the sets of primitive elements, squares (or perfect powers), normal elements, trace zero, etc.

In the case of primitive elements, the indicator function can be expressed by means of multiplicative characters of finite fields (Vinogradov):

$$1_{\mathcal{P}}(w) = \frac{\phi(q^n - 1)}{q^n - 1} \sum_{t|q^n-1} \frac{\mu(t)}{\phi(t)} \sum_{\text{ord}(\eta)=t} \eta(w).$$

In particular, the number of primitive elements in a set S depends heavily on the sums

$$\sum_{w \in S} \eta(w),$$

where η is a multiplicative character. Any nontrivial bound on the previous sum ($= o(\#S)$) provides estimates on the number of primitive elements in S ...

In particular, we may prove the following result:

Theorem

Let $S \subseteq \mathbb{F}_{q^n}$ and suppose that there exists $M > 0$ such that

$$\left| \sum_{w \in S} \eta(w) \right| \leq M,$$

for every nontrivial multiplicative character η of \mathbb{F}_{q^n} . Then the number P_S of primitive elements in S satisfies

$$P_S = \frac{\phi(q^n - 1)}{q^n - 1} (\#S + R),$$

where $|R| \leq W(q^n - 1) \cdot M$ and $W(q^n - 1)$ is the number of squarefree divisors of $q^n - 1$.

1. Robin's bound provides $W(q^n - 1) \leq q^{\frac{0.96n}{\log \log(q^n - 1)}}$, and it is the main bound employed in asymptotic results.
2. In general, we consider S a "structured" set, where we have nontrivial bounds on character sums (Weil's Bound, Mixed character sums, Gauss sums and bounds on affine spaces).
3. For complete results, computational calculations may be required (but still very limiting, since the factorization of large numbers can be hard). We also have a "sieve" version of the previous result, introduced by Cohen and Huczynska in 2003 (it replaces the function W by a (typically) smaller one).

Lemma

Let η be a multiplicative character of \mathbb{F}_{q^s} of order $r > 1$ and $F \in \mathbb{F}_{q^s}[x]$ be a monic polynomial of positive degree such that F is not of the form $g(x)^r$ for some $g \in \mathbb{F}_{q^s}[x]$. Suppose that e is the number of distinct roots of F in its splitting field over \mathbb{F}_{q^s} . For every $a \in \mathbb{F}_{q^s}$,

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

Lemma

Let η be a multiplicative character of \mathbb{F}_{q^s} of order $d \neq 1$ and χ a non-trivial additive character of \mathbb{F}_{q^s} . If $F, G \in \mathbb{F}_{q^s}[x]$ are such that F has exactly m roots and $\deg(G) = n$ with $\gcd(d, \deg(F)) = \gcd(n, q) = 1$, then

Results

We now discuss the existence of primitive k -normal elements, following two approaches:

1. produce k -normal elements from normal elements, and employ Weil's bound;
2. consider \mathbb{F}_q -vector spaces with a large proportion of k -normal elements, and employ a special bound on character sums over vector spaces (that imply a large proportion of primitive elements there).

For the first approach, we need the following result:

Lemma

Let $\beta \in \mathbb{F}_{q^n}$ be a normal element over \mathbb{F}_q . If $f \in \mathbb{F}_q[x]$ is a k -degree divisor of $x^n - 1$, then the element

$$\alpha = f \circ \beta,$$

has \mathbb{F}_q -order $\frac{x^n-1}{f}$, hence it is k -normal over \mathbb{F}_q .

In particular, if \mathcal{N} and \mathcal{P} denote the sets of normal and primitive elements in \mathbb{F}_{q^n} , respectively, there exists a primitive k -normal element if

$$\sum_{y \in \mathbb{F}_{q^n}} 1_{\mathcal{N}}(y) \cdot 1_{\mathcal{P}}(f \circ y) > 0.$$

It turns out that we have a similar character sum formula for the indicator function $1_{\mathcal{N}}$ of normal elements (now using additive characters):

$$1_{\mathcal{N}}(w) = \frac{\Phi_q(x^n - 1)}{q^n} \sum_{E|x^n-1} \frac{\mu_q(E)}{\Phi_q(E)} \sum_{\text{Ord}(\chi)=F} \chi(w).$$

In particular, we obtain a mixed sum (additive and multiplicative characters multiplied, with polynomial arguments). The term $f \circ y$ is a polynomial expression of degree q^k in y .

We directly verify that we are under the conditions to use Weil's bound, and we obtain that, for each pair of characters (η, χ) (not both trivial), the following inequality holds:

$$\left| \sum_{y \in \mathbb{F}_{q^n}} \chi(y) \cdot \eta(f \circ y) \right| \leq q^{k+n/2}.$$

In particular, we obtain the following result:

Theorem (R., Rev. Mat. Iberoamericana 19')

Suppose that there exist elements in \mathbb{F}_{q^n} that are k -normal over \mathbb{F}_q . Let $W(q^n - 1)$ and $W(x^n - 1)$ be the number of squarefree divisors of $q^n - 1$ and $x^n - 1$ (over \mathbb{F}_q), respectively. If

$$q^{n/2-k} > W(q^n - 1)W(x^n - 1),$$

then at least one of these k -normal elements of \mathbb{F}_{q^n} is also primitive.

The previous theorem generalizes the ideas employed in the complete result for $k = 1$ (R. and Thomson 18'), and it is also used in the complete result for $k = 2$ (J. Aguirre and V. Neumann 21').

We observe that the theorem only gives a sufficient condition...

The proof that no $(n - 1)$ -normal element can be primitive only uses the fact that the \mathbb{F}_q -order of any such element is a binomial $x - \delta$. This can be extended as follows:

Lemma

Let $\alpha \in \mathbb{F}_{q^n}^$ be an element whose \mathbb{F}_q -order divides a binomial $x^d - \delta \in \mathbb{F}_q[x]$ with $d < n$. Then α is not primitive.*

Proof. We have that $0 = (x^d - \delta) \circ \alpha = \alpha^{q^d} - \delta\alpha$. In particular, $\alpha^{q^d-1} = \delta \in \mathbb{F}_q^*$ and so

$$\alpha^{(q^d-1)(q-1)} = 1.$$

But $(q^d - 1)(q - 1) < q^n - 1$ for $d < n$, hence α cannot be primitive.

Necessary condition: $x^n - 1$ has a divisor of degree $n - k$ that does not divide any binomial $x^d - \delta \in \mathbb{F}_q[x]$ with $d < n$.

The other approach goes as follows: suppose that F is a divisor of $x^n - 1$ of degree $n - k$. The equation

$$F \circ y = 0,$$

determines an \mathbb{F}_q -vector space $\mathcal{V}_F \subseteq \mathbb{F}_{q^n}$ of dimension $n - k$ (so it has q^{n-k} elements).

1. In this vector space, $\Phi_q(F) \geq (q - 1)^{n-k}$ of such elements have \mathbb{F}_q -order F (hence are k -normal over \mathbb{F}_q).
2. Recall that F cannot divide a binomial $x^d - \delta$ (otherwise, \mathcal{V}_F would not have any primitive element).
3. The latter implies that \mathcal{V}_F satisfies a special property: for any $\alpha \in \mathcal{V}_F$ with \mathbb{F}_q -order F , we have that $\mathbb{F}_q(\alpha^{q-1}) = \mathbb{F}_{q^n}$.

We observe that $\alpha^{q-1} = \alpha^q \cdot \alpha^{-1}$ and $\alpha, \alpha^q \in \mathcal{V}_F$.

In particular, \mathcal{V}_F contains elements y, z such that $\mathbb{F}_q(yz^{-1}) = \mathbb{F}_{q^n}$ (*n-good*). We have a nontrivial bound for vector spaces satisfying the latter...

Theorem (R. 20')

Let $\mathcal{V} \subseteq \mathbb{F}_{q^n}$ be an \mathbb{F}_q -vector space of dimension t and suppose that there exist $y, z \in \mathcal{V}$ with $\mathbb{F}_q(yz^{-1}) = \mathbb{F}_{q^n}$. Then for every nontrivial multiplicative character η of \mathbb{F}_{q^n} we have that

$$\left| \sum_{y \in \mathcal{V}} \eta(y) \right| \leq nq^{t-1/2}.$$

If $q \rightarrow \infty$, the bound is nontrivial for $n = o(\sqrt{q})$.

We may derive the following result:

Lemma

Let n be a positive integer and $\varepsilon > 0$. Then there exists a constant $c = c(\varepsilon, n)$ such that, for any prime power $q > c$ and any n -good \mathbb{F}_q -vector space $\mathcal{V} \subseteq \mathbb{F}_{q^n}$ of dimension t , the number of primitive elements in \mathcal{V} is at least $q^{t-\varepsilon}$.

In particular, if n is fixed, q is large enough and $F \in \mathbb{F}_q[x]$ is a divisor of $x^n - 1$ of degree $n - k$ not dividing any binomial (of degree $< n$), then:

1. we have at least $q^{n-k-1/2}$ primitive elements in \mathcal{V}_F ;
2. we have at least $(q - 1)^{n-k}$ elements in \mathcal{V}_F that are k -normal.
3. we are done if

$$q^{n-k-1/2} + (q - 1)^{n-k} > q^{n-k} = \#\mathcal{V}_F.$$

We obtain the following criterion:

Theorem

Fix $n > 1$ an integer and let $k < n$. There exists a constant $c = c_n$ such that, for any prime power $q > c$, the following are equivalent:

1. \mathbb{F}_{q^n} contains a primitive k -normal element;
2. *there exists a divisor $F \in \mathbb{F}_q[x]$ of $x^n - 1$ of degree $n - k$ not dividing any binomial (of degree $< n$).*

In particular, there exist primitive $(p - 2)$ -normal elements in \mathbb{F}_{q^p} if q is large enough (**not expected**).


The last result tells us that if n fixed and q is large, the existence of primitive k -normal elements reduces to study the factorization of $x^n - 1$ over \mathbb{F}_q (degree distribution, divisors dividing binomials, etc).

The latter is being explored in collaboration with F. Brochero (UFMG, Brazil) and Sávio Ribas (UFOP, Brazil).

 J.J.R. Aguirre and V.G.L. Neumann.

Existence of primitive 2-normal elements in finite fields.

Finite Fields Appl. 73, 2021.

 S. D. Cohen and S. Huczynska.

The primitive normal basis theorem – without a computer.

J. London Math. Soc., 67(1):41–56, 2003.

 S. Huczynska, G. L. Mullen, D. Panario, D. Thomson.

Existence and properties of k -normal elements over finite fields.

Finite Fields Appl. 24:170–183, 2013.

 H. W. Lenstra Jr. and R. J. Schoof.

Primitive normal bases for finite fields.

Math. Comp., 48(177): 217–231, 1987.

 C. Pomerance, L. Thompson, A. Weingartner.

On integers n for which $x^n - 1$ has a divisor of every degree.

Acta Arith. 175: 225–243, 2016



L. Reis, D. Thomson.

Existence of primitive 1-normal elements in finite fields

Finite Fields Appl. 51: 238–269, 2018.



L. Reis.

Existence results on k -normal elements over finite fields.

Rev. Mat. Iberoam. 35: 805–822, 2019.



L. Reis.

Some applications of character sums bounds over affine spaces.

Submitted, 2020.



L. Thompson.

On the divisors of $x^n - 1$ in $\mathbb{F}_p[x]$.

Int. J. Number Theory 9: 421–430, 2013.

Obrigado!

Lucas Reis - UFMG - lucasreismat@gmail.com