An introduction to k-normal elements over finite fields

Simran Tinani

Graduate Students Seminar, IISER Mohali.
10 March 2021

Overview

Introduction

Let $m \geq 1$ and q be a power of a prime p. Denote by $\mathbb{F}_q$ the finite field of order q. The extension field $\mathbb{F}_{q^m}$ then forms a vector space of dimension m over $\mathbb{F}_q$, and $\mathbb{F}_{q^m}^*$ is a cyclic group, whose generators are called primitive elements.

Definition (Normal Element)

An element $\alpha \in \mathbb{F}_{q^m}$ is called a normal element over $\mathbb{F}_q$ if all its Galois conjugates, i.e. the m elements $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$, form a basis of $\mathbb{F}_{q^m}$ as a vector space over $\mathbb{F}_q$. A basis of this form is called a normal basis.

Theorem 1 (Primitive Normal Basis Theorem ([Lenstra and Schoof, 1987]))

Every finite field extension possesses an element which is simultaneously normal and primitive.

Introduction

Definition (k-normal element)

An element $\alpha \in \mathbb{F}_{q^m}$ is called k-normal if

$$\dim_{\mathbb{F}_q}\left(\mathrm{span}_{\mathbb{F}_q}\left\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\right\}\right) = m - k.$$

An element α is 0-normal if and only if it is normal. The only m-normal element in $\mathbb{F}_{q^m}$ is 0.

Definition (Polynomial Euler-Phi)

Let $f \in \mathbb{F}_q[x]$, $\deg f = m > 0$. Then $\Phi_q(f)$ is defined as the order of the group $\left(\frac{\mathbb{F}_q[x]}{\langle f \rangle}\right)^{\times}$. In other words, $\Phi_q(f)$ gives the number of polynomials with degree $< m$ that are co-prime to f.

Introduction

- For arbitrary m, and k, $0 < k < m-1$, no general rule for the existence of k-normal elements or for their number n_k, when they exist, is known. Many special cases have been dealt with.
- Relation to multiplicative structure of the field: given $d \mid q^m - 1$, how many k-normal elements with order d are in $\mathbb{F}_{q^m}$? One is interested in establishing analogous results to the Primitive Normal Basis theorem [Lenstra and Schoof, 1987].
- Existence of 1-normal primitive elements was posed with a partial solution in [Huczynska et al., 2013] and was fully answered in [Reis and Thomson, 2018].

Background Definitions and Results

Consider the structure of $\mathbb{F}_{q^m}$ as an $\mathbb{F}_q[x]$-module under the action

$$\left(\sum_{i=0}^{n} a_i x^i\right) \cdot \alpha = \sum_{i=0}^{n} a_i \alpha^{q^i}, \ \alpha \in \mathbb{F}_{q^m}.$$

For any $\alpha \in \mathbb{F}_{q^m}$ let $\mathrm{Ann}(\alpha)$ denote the annihilator ideal with respect to this action. Note that we always have $(x^m - 1) \cdot \alpha = x^{q^m} - x = 0$, so $x^m - 1 \in \mathrm{Ann}(\alpha)$

Definition (Ord function)

Define the function $\mathrm{Ord} : \mathbb{F}_{q^m} \to \mathbb{F}_q[x]$ *as follows. For any* $\alpha \in \mathbb{F}_{q^m}$, $\mathrm{Ord}(\alpha)$ *is the unique monic polynomial such that*

$$\mathrm{Ann}(\alpha) = \langle \mathrm{Ord}(\alpha) \rangle \text{ in } \mathbb{F}_q[x].$$

Background Definitions and Results

Theorem 2 ([Huczynska et al., 2013, Theorem 3.2])

Let $\alpha \in \mathbb{F}_{q^m}$ *and* $g_\alpha(x) := \sum_{i=0}^{m-1} \alpha^{q^i} \cdot x^{m-1-i} \in \mathbb{F}_{q^m}[x]$. *Then the following conditions are equivalent:*

- α *is* k*-normal.*
- $\gcd(x^m - 1, g_\alpha(x))$ *over* $\mathbb{F}_{q^m}$ *has degree* k.
- $\deg(\mathrm{Ord}(\alpha)) = m - k$.
- *The matrix*

$$A_\alpha := \begin{bmatrix} \alpha & \alpha^q & \alpha^{q^2} & \cdots & \alpha^{q^{m-1}} \\ \alpha^{q^{m-1}} & \alpha & \alpha^q & \cdots & \alpha^{q^{m-2}} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \cdots & \alpha \end{bmatrix}$$

has rank $m - k$.

Number of k-Normal Elements

Theorem 3 ([Huczynska et al., 2013, Theorem 3.5])

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

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

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

- $x^m - 1$ factorizes over $\mathbb{F}_q$ into the product of cyclotomic polynomials $Q_d(x)$ with degrees dividing m. For $p \nmid d$ each irreducible factor of $Q_d(x)$ has degree $\frac{\phi(d)}{r}$, where r is the multiplicative order of $d \mod q$ [Lidl and Niederreiter, 1997].
- No known closed formula for r, so there is no closed-form complete factorization of $x^m - 1$ over $\mathbb{F}_q$.

- For $k = 0$, the formula in Theorem 3 yields the well-known value $\Phi_q(m)$ for the number of normal elements over in $\mathbb{F}_{q^m}$ [Lidl and Niederreiter, 1997].
- Since $x^m - 1$ always has the divisor $x - 1$ of degree 1 and hence also a divisor of degree $m - 1$ (and since $\Phi_q(f(x)) \neq 0$ for any nonzero polynomial $f(x)$), we always have 1-normal and $(m-1)$-normal elements in $\mathbb{F}_{q^m}$.
- The only values of k for which k-normal elements are guaranteed to exist for every pair $(q,\ m)$ are 0, 1 and $m - 1$ [Huczynska et al., 2013].
- If q is a primitive root modulo m, $\frac{x^m-1}{x-1}$ is irreducible and so for $1 < k < m - 1$, k-normal elements do not exist [Reis and Thomson, 2018].

Main Theorem on Cardinality

Theorem 4

[Tinani and Rosenthal, 2021] Let n_k denote the number of k-normal elements in $\mathbb{F}_{q^m}$. If $n_k > 0$, then

$$n_k \geq \frac{\Phi_q(x^m - 1)}{q^k}.$$

Proof (Sketch).

One may prove that there is a group action of $\left(\frac{\mathbb{K}[x]}{(x^m-1)}\right)^\times$ on the set S_k of all k-normal elements. An upper bound on $|\mathrm{Stab}(\alpha)|$ can be found using Theorem 2. The rest is an application of Orbit-Stabilizer Theorem.

- The proof follows the approach in [Hyde, 2018], which handles the case $k = 0$ and obtains the exact number of normal elements using the freeness and transitivity of the group action.

- For $k > 0$ it is clear that for every k-normal α, there exists $u \in \mathbb{K}[G]$ such that $u \cdot \alpha = \alpha$. However, it is unclear whether such a u always lies in $\mathbb{K}[G]^\times$ and if the action is transitive.

- If a k-normal element α exists, then the lower bound is, in fact, for the number of k-normal elements lying in a single orbit, and therefore in $\text{span}_{\mathbb{F}_q}\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}\}$.

Existence of k-Normal Elements

- There exist values of q, m and k such that no k-normal element over $\mathbb{F}_q$ exists in $\mathbb{F}_{q^m}$. E.g. $q = 2$, $m = 10$, $k = 3$, 7.
- Some results on the number of k-normal elements automatically imply their existence, E.g. [Saygı et al., 2019] for m a power of the characteristic.
- Some other results on the numbers are in implicit form, asymptotic (E.g. [Huczynska et al., 2013]), or assume the existence of at least one k-normal element (E.g. this paper).

Existence of k-Normal Elements

Theorem 5 ([Reis, 2019])

Let q be a power of a prime p and let $m \geq 2$ be a positive integer such that every prime divisor of m divides $p \cdot (q-1)$. Then k-normal elements exist for all $k = 0, 1, 2, \ldots, m$.

- Concrete, significant extension of the case $m = p^r$, but prime factorization of m is still restricted to a particular form.
- Our theorem shows that under weaker constraints on m (m must have a "sufficiently large" common divisor with $q^m - 1$), k-normal elements exist for k above a minimum lower bound.
- When $p \nmid m$, our theorem is a generalization of this result.

A Number Theoretic Prerequisite

Proposition 1

[Tinani and Rosenthal, 2021] Let a and m be arbitrary natural numbers and suppose that $m \nmid a^m - 1$. Then m has a prime factor that does not divide $a^m - 1$.

- The proof proceeds by induction on the largest exponent b of a prime p dividing m.
- The proof was inspired by the proof of a similar result in [Lüneburg, 2012, Theorem 6.3].

Main Theorem on Existence

Theorem 6 (Sufficient Conditions for Existence)

[Tinani and Rosenthal, 2021]

- *If* $m \mid (q^m - 1)$, *then* k*-normal elements exist in* $\mathbb{F}_{q^m}$ *for every integer* k *in the interval* $0 \leq k \leq m - 1$.
- *If* $m \nmid q^m - 1$, *let* $d = \gcd(q^m - 1,\ m)$. *Assume that* $\sqrt{m} < d$. *Let* b *denote the largest prime divisor of* m *that is a non-divisor of* $q^m - 1$. *Then, for* $k \geq m - d - b + 1$, k*-normal elements exist in* $\mathbb{F}_{q^m}$. *In particular, if* m *is prime and* $m \leq d + b - 1$, *then* k*-normal elements exist for every* k *in the interval* $0 \leq k \leq m - 1$.

Note that if $p \nmid m$ and the hypothesis of Theorem 5 holds, i.e. every prime factor of m divides $p \cdot (q - 1)$ then Proposition 1 says that we are in the case $m \mid q^m - 1$.

Proof (Sketch).

- $\mathbb{F}_{q^m}$ contains k-normal elements $\iff$ $x^m - 1$ has a divisor of degree $m - k$.
- If $m \mid q^m - 1$, $x^m - 1$ splits into linear factors over $\mathbb{F}_q$, and $m - k$ linear factors combine to give a factor of degree $m - k$.
- If $m \nmid q^m - 1$, write

$$x^m - 1 = (x - \alpha_1) \cdot (x - \alpha_2) \cdot \ldots \cdot (x - \alpha_d) \cdot \prod_{\substack{t \mid m \\ t \nmid q^m - 1}} Q_t(x),$$

- Proposition 1 says that we have a prime b such that $Q_b(x)$ figures in the latter product. A combinatoric argument then shows that if no k-normal element exists, then

$$k < m - d - \phi(b) = m - d - b + 1.$$

Examples

Example

For $q = 5$, $m = 6$, we have

$$q^m - 1 = 15624 = 0 \mod 6$$

So, Theorem 6 shows that k-normal elements exist in $\mathbb{F}_{q^m}$ for every $k \in \{0, 1, \ldots, m\}$.
Here, Theorem 5 is not applicable because the prime 3 divides m but not $p \cdot (q - 1) = 20$.

Example

For $q = 8,\ m = 6$, we have

$$q^m - 1 = 262143,$$

and so

$$d = \gcd(q^m - 1,\ m) = 3 > \sqrt{6}.$$

The largest prime b that divides 6 and not 262143 is clearly 2.
So, Theorem 6 shows that k-normal elements exist in $\mathbb{F}_{q^m}$ for every $k \geq m - d - b + 1$, i.e. for every $k \geq 2$.
Since we know that 0- and 1-normal elements always exist in $\mathbb{F}_{q^m}$, we conclude that in this case k-normal elements exist for every $k \in \{0, 1, \ldots, m\}$.
Here as well, Theorem 5 is not applicable because the prime 3 divides m but not $p \cdot (q - 1) = 14$.

Normal Elements with Large Multiplicative Order

- So far, we have looked at the "additive" structure of $\mathbb{F}_{q^m}$ as an $\mathbb{F}_q$-vector space and as an $\mathbb{F}_q[x]$-module.
- It is also of interest to study the relation between these additive structures and the multiplicative structure of $\mathbb{F}_{q^m}^*$.

Theorem 7 (Primitive Normal Basis Theorem, [Lenstra and Schoof, 1987])

For every prime power $q > 1$ and every positive integer m there exists an element $a \in \mathbb{F}_{q^m}^*$, with $\mathrm{Ord}(\mathrm{a}) = x^m - 1$ and $\mathrm{ord}(a) = q^m - 1$.

- One may wish to extend this and ask what pairs of multiplicative and additive orders occur together in elements of $\mathbb{F}_{q^m}$.

Normal Elements with Large Multiplicative Order

Theorem 8

Suppose that $(m, q-1) = 1$. Then $\mathbb{F}_{q^m}$ has a normal element with multiplicative order $\frac{q^m-1}{q-1}$.

Idea of Proof.

We showed that the techniques in the proof of the Primitive Normal Basis Theorem in [Lenstra and Schoof, 1987] can be adapted and extended to this case.

Further Research Problems

Given a k-normal element α, does there exist another k-normal element outside $\text{span}_{\mathbb{F}_q}\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}\}$?

Given a k-normal element α, which of the subsets of $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}\}$ with size $m-k$ or smaller, apart from $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-k-1}}\}$ are linearly independent?

Under what circumstances is the group action of $\mathbb{K}[G]^\times$ on S_k free? Under what circumstances is it transitive?

Determine the existence of high-order k-normal elements $\alpha \in \mathbb{F}_{q^m}$ over $\mathbb{F}_q$, where high order means $ord(\alpha) = N$, with N a large positive divisor of $q^m - 1$. [Huczynska et al., 2013, Problem 6.4]

Thank you!

References I

Huczynska, S., Mullen, G. L., Panario, D., and Thomson, D. (2013).
Existence and properties of k-normal elements over finite fields.
Finite Fields Appl., 24:170–183.

Hyde, T. (2018).
Normal elements in finite fields.
arXiv preprint arXiv:1809.02155.

Lenstra, Jr., H. W. and Schoof, R. J. (1987).
Primitive normal bases for finite fields.
Math. Comp., 48(177):217–231.

References II

Lidl, R. and Niederreiter, H. (1997).
Finite fields, volume 20 of *Encyclopedia of Mathematics and its Applications*.
Cambridge University Press, Cambridge, second edition.
With a foreword by P. M. Cohn.

Lüneburg, H. (2012).
Translation Planes.
Springer Berlin Heidelberg.

Reis, L. (2019).
Existence results on k-normal elements over finite fields.
Rev. Mat. Iberoam., 35(3):805–822.

References III

Reis, L. and Thomson, D. (2018).
Existence of primitive 1-normal elements in finite fields.
Finite Fields Appl., 51:238–269.

Saygı , Z., Tilenbaev, E., and Ürtiș, c. (2019).
On the number of k-normal elements over finite fields.
Turkish J. Math., 43(2):795–812.

Tinani, S. and Rosenthal, J. (2021).
Existence and Cardinality of k-normal Elements in Finite Fields.
Theoretical Computer Science and General Issues. Springer International Publishing.