Something about normal bases over finite fields

David Thomson

Carleton University
dthomson@math.carleton.ca

WCNT, December 17, 2013

Existence and properties of k-normal elements over finite fields

David Thomson

Carleton University
dthomson@math.carleton.ca

WCNT, December 17, 2013

with S. Huczynska (St. Andrews), G. L. Mullen (PSU) and Daniel Panario (Carleton)

Rough Outline

The beginning

The middle

The end

Basis Representation

This talk will give one sort of duality between the algebraic and geometric descriptions of finite fields.

We can view $\mathbb{F}_{q^n}$ as a vector space of dimension n over $\mathbb{F}_q$. Then, any basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ can be used to represent the elements in $\mathbb{F}_{q^n}$.

An element $\alpha \in \mathbb{F}_{q^n}$ is normal if

$$N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\},$$

is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The basis N is a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

By convention we define $\alpha_i = \alpha^{q^i}$ for $i = 0, 1, \ldots, n-1$.

Normal bases in computation

Let $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ be a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ with $\alpha_i = \alpha^{q^i}$, and $A \in \mathbb{F}_{q^n}$ be

$$A = (a_0, a_1, \ldots, a_{n-1}) = \sum_{i=0}^{n-1} a_i \alpha_i.$$

Then, since $\alpha_i^q = \alpha_{i+1}$ for $i = 0, 1, \ldots, n-2$ and $\alpha_{n-1}^q = \alpha$, we have

$$A^q = \sum_{i=0}^{n-1} a_i \alpha_i^q = \sum_{i=0}^{n-1} a_i \alpha_{i+1} = (a_{n-1}, a_0, \ldots, a_{n-2}).$$

q-th power $\Longleftrightarrow$ cyclic shift of coordinates.

This means taking qth powers has negligible cost!

Normal Bases

The normal basis theorem for finite fields (Eisenstein, Schönemann, Hensel) establishes that for any prime power q and positive integer n, there is a normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

An exact expression for the number of normal elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ was determined by Ore (1934). Explicit (easy to use) lower and upper bounds are known. For example, the probability that an arbitrary element in $\mathbb{F}_{q^n}$ is normal is larger than $1/(16 \log_q n)$.

As a geometric object

Let $f(x) = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{F}_q[x]$ and define an action on the algebraic closure of $\mathbb{F}_q$ by

$$f \circ \alpha = \sum_{i=0}^{n-1} a_i \sigma_q^i(\alpha) = \sum_{i=0}^{n-1} a_i \alpha^{q^i}.$$

This action imbues $\overline{\mathbb{F}_q}$ with the structure of an $\mathbb{F}_q[x]$-module.

Using this action, we have trivially that

$$(x^n - 1) \circ \alpha = \alpha^{q^n} - \alpha = 0$$

if and only if $\alpha \in \mathbb{F}_{q^n}$. Moreover,

$$\mathbb{F}_{q^n} \cong \mathbb{F}_q[x]/(x^n - 1).$$

Additive order

Moreover, for any $\alpha \in \mathbb{F}_{q^n}$ the annihilator of α is an ideal, and is generated by a polynomial of minimum degree.

Definition. If $\mathrm{Ann}(\alpha) = \langle g \rangle \in \mathbb{F}_q[x]$, then g is the $\mathbb{F}_q$-Order of α, which we denote by $\mathrm{Ord}(\alpha)$.

We have seen that $\alpha \in \mathbb{F}_{q^n}$ implies that α is annihilated by $x^n - 1$. Moreover, if α is normal, it cannot be annihilated by a polynomial of smaller degree.

Proposition. An element $\alpha \in \mathbb{F}_{q^n}$ is normal if and only if

$$\mathrm{Ord}(\alpha) = x^n - 1.$$

k-normal elements

Definition. Let $\alpha \in \mathbb{F}_{q^n}$ and let $\mathrm{Ord}(\alpha) = g$. If $\deg(g) = n - k$, then α is k-normal.

k-normal elements

Definition. Let $\alpha \in \mathbb{F}_{q^n}$ and let $\mathrm{Ord}(\alpha) = g$. If $\deg(g) = n - k$, then α is k-normal.

In what follows, we need the natural analogue of the Euler phi function for polynomials.

Definition. Let $f \in \mathbb{F}_q[x]$ be monic, the *Euler Phi function for polynomials* is given by $\Phi_q(f) = |(\mathbb{F}_q[x]/f\mathbb{F}_q[x])^*|$.

Proposition. **(Ore - 1934)** 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 $\Phi_q(f)$.

The number of k-normal elements

Theorem. The number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is given by

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

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

When $k = 0$, that is, when counting the number of normal elements, the above summation reduces to $\Phi_q(x^n - 1)$, as expected.

The number of k-normal elements

Theorem. The number of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is given by

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

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

When $k = 0$, that is, when counting the number of normal elements, the above summation reduces to $\Phi_q(x^n - 1)$, as expected.

Clearly,

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1),$$

so the only values of k for which k-normal elements are guaranteed to exist for every (q, n) are $0, 1$ and $n - 1$.

Some trivia about k-normals

Theorem. Let $\alpha \in \mathbb{F}_{q^n}$. The following are equivalent:

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

(ii) $\deg(\mathrm{Ord}(\alpha)) = n - k$;

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

(iv) $\deg(\gcd(x^n - 1, \alpha x^{n-1} + \alpha^q x^{n-1} + \cdots + \alpha^{q^{n-1}})) = n - k$;

(v) Let $A_\alpha = \begin{pmatrix} \alpha & \alpha^q & \alpha^{q^2} & \ldots & \alpha^{q^{n-1}} \\ \alpha^{q^{n-1}} & \alpha & \alpha^q & \ldots & \alpha^{q^{n-2}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \ldots & \alpha \end{pmatrix}$, then $\mathrm{rank}(A_\alpha) = n - k$.

Primitive and normal

Definition. An element $\alpha \in \mathbb{F}_q$ is primitive if $\langle \alpha \rangle = \mathbb{F}_q^*$.

Primitive elements are therefore generators of the multiplicative (field-theoretic) structure of $\mathbb{F}_q$ and normal elements are, in some sense, generators of an additive (geometric) structure of $\mathbb{F}_q$.

A natural question is whether elements exist which combine these two notions.

Theorem. **(Carlitz - 1952, Davenport - 1968, Lenstra and Schoof - 1987, Cohen and Huczynska - 2003)**
There exists an element $\alpha \in \mathbb{F}_q$ which is simultaneously primitive and normal.

Primitive k-normals

We have used a basic *Sage* program to enumerate every element of small finite fields for k-normal and primitive k-normal elements.

$q = 2$, $n = 6$

k	# k-norm.	# pr. k-norm.
0	24	18
1	12	12
2	18	6
3	3	0
4	5	0
5	1	0

$q = 5$, $n = 6$

k	# k-norm.	# pr. k-norm.
0	9216	2568
1	4608	1320
2	1344	360
3	384	72
4	64	0
5	8	0

$q = 5$, $n = 7$

k	# k-norm.	# pr. k-norm.
0	62496	31248
1	15624	7812
2	0	0
3	0	0
4	0	0
5	0	0
6	4	0

Non-existence of some k-normals

Non-existence result. Let $k = n - 1$. There are no primitive k-normal elements.

Proof. Suppose α is a primitive $(n-1)$-normal element. Then $(x - \beta) \circ \alpha = 0$ for some $\beta \in \mathbb{F}_q$. Hence, $\alpha^q - \beta\alpha = 0$ and $\alpha^{q-1} \in \mathbb{F}_q$.

Therefore, the multiplicative order of α divides $(q-1)^2$, which is a contradiction for $n > 2$.

Similar reasoning shows that there are no primitive $(n-2)$-normals when $q \equiv 1 \pmod 4$. But this is incremental (boring).

The method of Carlitz and Davenport

Let

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

$$\Omega(\alpha) = \sum_{g|x^n-1} \frac{M(g)}{\Phi(g)} \sum_{\lambda \in \hat{\mathbb{F}_{q^n}}, \mathrm{Ord}(\lambda)=g} \lambda(\alpha).$$

The number of elements $\alpha \in \mathbb{F}_{q^n}$ which are primitive and normal is

$$\sum_{\alpha \in \mathbb{F}_{q^n}} \omega(\alpha)\Omega(\alpha).$$

Using standard Gauss sum arguments, it is easy to show that primitive normal bases exist asymptotically (Carlitz, Davenport). Finer counts and refinements are needed for the final result (Lenstra and Schoof, Cohen and Huczynska).

Some issues to deal with

Difficulty 1. It is clear that primitive k-normals do not exist for all k, n.

Difficulty 2. We do not have a characteristic function for k-normality.

We can fix this in some cases by considering the notion of free elements.

(a) For $m|q^n - 1$, $\alpha \in \mathbb{F}_{q^n}^*$ is m-free if $\alpha = \beta^d$, for any divisor d of m, implies $d = 1$.

(b) For $M|x^n - 1$, $\alpha \in \mathbb{F}_{q^n}$ is M-free if $\alpha = H(\beta)$, where H is the q-associate of a divisor h of M, implies $h = 1$.

Using freeness

Proposition. An element is primitive if and only if it is $(q^n - 1)$-free. An element is normal if and only if it is $(x^n - 1)$-free.

Difficulty. If α is g-free for some divisor g of $x^n - 1$, then α is h-free for all $h|g$.

Proposition. Suppose $x^n - 1$ has a non-repeated linear factor $x - \zeta$, $\zeta \in \mathbb{F}_q$. Then

$$\mathrm{Ord}(\alpha) = \frac{x^n - 1}{x - \zeta}$$

if and only if

$$\alpha \text{ is a non-normal } \left(\frac{x^n - 1}{x - \zeta}\right) \text{-free element.}$$

Putting it together

So, instead we prove existence of:

1. $(q^n - 1)$-free,
2. $\left(\frac{x^n-1}{x-1}\right)$-free,
3. Trace-0 (non-normal and with a known characteristic function).

elements when p does not divide n.

Lucky for us: Character sums of this form were studied by Cohen and Hachenberger (1999).

Our result

Theorem. Let $q = p^e$ be a prime power and let n be a positive integer with $p \not| n$. 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 basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Concluding problems

Problem. Obtain a complete existence result for primitive 1-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. We conjecture that such elements always exist.

Problem. Determine the pairs (n, k) such that primitive k-normals elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ exist.