Normal and primitive normal elements with prescribed traces in intermediate extensions of finite fields

ACA 2025 - Finite Fields and Applications Session
Heraklion - July 2025

Giorgos Kapetanakis

University of Thessaly
kapetanakis@uth.gr
http://gkapet.users.uth.gr/

Outline

Primitivity and normality

- Let q be a prime power and $m \in \mathbb{Z}_{>0}$. $\mathbb{F}_q$ is the finite field of order q and $\mathbb{F}_{q^m}$ its extension of degree m.
- The group $\mathbb{F}_{q^m}^*$ is cyclic and its generators are called *primitive*.
- Some $\alpha \in \mathbb{F}_{q^m}$ is *normal* if $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$.
- Some $\alpha \in \mathbb{F}_{q^m}$ is *primitive normal* if it is both primitive and normal.
- The above families play critical roles in theoretical and practical applications.
- It is known that over any finite field extension, the above families are nonempty.

The trace of primitive (normal) elements

Take some $d \mid m$. The *trace* of $\alpha \in \mathbb{F}_{q^m}$ over $\mathbb{F}_{q^d}$ is

$$\mathsf{Tr}_{m/d}(\alpha) = \sum_{i=0}^{m/d-1} \alpha^{q^{id}}.$$

Regarding the trace of primitive (normal) elements, we have:

Theorem (Cohen, 1990)

Take some $a \in \mathbb{F}_q$. There exists a primitive element $\alpha \in \mathbb{F}_{q^m}$ such that $\mathsf{Tr}_{m/1}(\alpha) = a$ unless $a = 0$ and $m = 2$ or $a = 0$, $m = 3$ and $q = 4$.

Theorem (Cohen-Hachenberger, 1999)

Take some $a \in \mathbb{F}_q \setminus \{0\}$. There exists a primitive normal element $\alpha \in \mathbb{F}_{q^m}$ such that $\mathsf{Tr}_{m/1}(\alpha) = a$.

The goal of this work

- We explore the existence of normal and primitive normal elements in $\mathbb{F}_{q^m}$ with prescribed traces in several intermediate extensions.
- We obtain concrete results for the case of normal elements.
- We obtain asymptotic and concrete results (under restrictions) for primitive normal elements.

Linearized polynomials and $\mathbb{F}_q$-order

- A polynomial $L_f \in \mathbb{F}_q[x]$ of the form

$$L_f(x) = \sum_{i=0}^{k} f_i x^{q^i}$$

  is a *linearized* polynomial and is the *q-associate* of $f = \sum_{i=0}^{k} f_i x^i$.
- Linearized polynomials satisfy $L_f(ax + by) = aL_f(x) + bL_f(y)$ and $L_f(L_g(x)) = L_{fg}(x)$ (for $a, b \in \mathbb{F}_q$).
- The $\mathbb{F}_q$-*order* (or *additive* order) of $\beta \in \mathbb{F}_{q^m}$, denoted by $\mathrm{Ord}_q(\beta)$ is the minimum degree monic polynomial over $\mathbb{F}_q$, such that $L_{\mathrm{Ord}_q(\beta)}(\beta) = 0$.

More on the $\mathbb{F}_q$-order

Proposition

Let $\beta \in \mathbb{F}_{q^m}$. The following are true:

1. $\mathrm{Ord}_q(\beta) \mid x^m - 1$.
2. *β is normal over $\mathbb{F}_q$ if and only if* $\mathrm{Ord}_q(\beta) = x^m - 1$.
3. *If $d \mid m$, then $\beta \in \mathbb{F}_{q^d}$ if and only if* $\mathrm{Ord}_q(\beta) \mid x^d - 1$.
4. *If $f \in \mathbb{F}_q[x]$, then* $\mathrm{Ord}_q(L_f(\beta)) = \mathrm{Ord}_q(\beta)/\gcd(f, \mathrm{Ord}_q(\beta))$.

The $\mathbb{F}_q$-*order* of an additive character ψ of $\mathbb{F}_{q^m}$ is denoted by $\mathrm{Ord}_q(\psi)$ and is defined as the minimum degree monic polynomial over $\mathbb{F}_q$, such that $\psi\left(L_{\mathrm{Ord}_q(\psi)}(\beta)\right) = 1$, for all $\beta \in \mathbb{F}_{q^m}$.

Characteristic functions

- It is well-known (Vinogradov's formula) that for any $\beta \in \mathbb{F}_{q^m}$,

$$\rho_m(\beta) = \theta(q) \sum_{t \mid q^m - 1} \left(\frac{\mu(t)}{\phi(t)} \sum_{\eta \in \Gamma(t)} \eta(\beta) \right)$$

  is the characteristic function for primitive elements.

- Likewise, for any $\beta \in \mathbb{F}_{q^m}$ and $d \mid m$,

$$\kappa_m(\beta) = \Theta(x^m - 1) \sum_{f \mid x^m - 1} \left(\frac{\mu'(f)}{\Phi(f)} \sum_{\psi \in \Gamma(f)} \psi(\beta) \right)$$

  is the characteristic function for elements that are normal over $\mathbb{F}_{q^d}$.

The prescribed trace characteristic function

Let $n \mid m$, $\gamma \in \mathbb{F}_{q^m}$ such that $\mathrm{Tr}_{m/n}(\gamma) = a \in \mathbb{F}_{q^n}$. Then, the characteristic function for elements in $\mathbb{F}_{q^m}$ with trace a over $\mathbb{F}_{q^n}$ is

$$\tau_{m,n,a}(\beta) = \frac{1}{q^n} \sum_{c \in \mathbb{F}_{q^n}} \chi_c(\beta - \gamma) = \frac{1}{q^n} \sum_{c \in \mathbb{F}_{q^n}} \chi_c(\beta)\chi_c(\gamma)^{-1},$$

where χ is the canonical character and (for $c \in \mathbb{F}_{q^m}$), $\chi_c(\alpha) = \chi(c\alpha)$.

An existence and enumeration result

Theorem (Reis, 2020)

Let $d_1 < \ldots < d_k$ be divisors of m and choose $a_i \in \mathbb{F}_{q^{d_i}}$, $1 \leqslant i \leqslant k$, then there exists some element $\alpha \in \mathbb{F}_{q^m}$ with $\mathsf{Tr}_{m/d_i}(\alpha) = a_i$ for all $1 \leqslant i \leqslant k$ iff

$$\mathsf{Tr}_{d_i/\gcd(d_i,d_j)}(a_i) = \mathsf{Tr}_{m/\gcd(d_i,d_j)}(\alpha) = \mathsf{Tr}_{d_j/\gcd(d_i,d_j)}(a_j), 1 \leqslant i,j \leqslant k.$$

In this case there are exactly

$$\begin{aligned}\lambda(\mathbf{d}) &= \deg(\mathsf{lcm}(x^{d_1}-1,\ldots,x^{d_k}-1)) \\ &= d_1 + \cdots + d_k + \sum_{i=2}^{k} (-1)^{i+1} \sum_{1 \leqslant l_1 < \ldots < l_i \leqslant k} \gcd(d_{l_1},\ldots,d_{l_i})\end{aligned}$$

choices for α.

Some consequences

- The latter implies that if $d_i \mid d_j$, then $\mathrm{Tr}_{m/d_i}(\alpha) = a_i$ is implied by $\mathrm{Tr}_{m/d_j}(\alpha) = a_j$, thus we assume $d_i \nmid d_j$ for any $1 \leqslant i < j \leqslant k$.
- Set as $\lambda_k(m)$ the set of k-tuples $\mathbf{d} = (d_1, \ldots, d_k)$, where $d_1 < \ldots < d_k < m$ are divisors of m such that $d_i \nmid d_j$ for every $1 \leqslant i < j \leqslant k$.
- For $\mathbf{d} = (d_1, \ldots, d_k) \in \lambda_k(m)$, set $\mathbb{F}_{\mathbf{d}} = \prod_{i=1}^{k} \mathbb{F}_{q^{d_i}}$ and some $\mathbf{a} = (a_1, \ldots, a_k) \in \mathbb{F}_{\mathbf{d}}$, is $\mathbf{d}$-*admissible* if, for any $1 \leqslant i < j \leqslant k$, $\mathrm{Tr}_{d_i/\gcd(d_i,d_j)}(a_i) = \mathrm{Tr}_{d_j/\gcd(d_i,d_j)}(a_j)$.

Normal $\mathbf{d}$-admissible k-tuples

From now on, m is relatively prime to q, $\mathbf{d} = (d_1, \ldots, d_k) \in \lambda_k(m)$ and $\mathbf{a} = (a_1, \ldots, a_k) \in \mathbb{F}_{\mathbf{d}}$ is a $\mathbf{d}$-admissible k-tuple.

Lemma

Suppose $\beta \in \mathbb{F}_{q^m}$ is normal over $\mathbb{F}_q$ and $d \mid m$. Then $\mathrm{Tr}_{m/d}(\beta)$ is normal over $\mathbb{F}_q$ (as an element of $\mathbb{F}_{q^d}$).

The above implies that we cannot arbitrarily prescribe the trace of a normal element over intermediate extensions, but instead we have to confine ourselves to the family below.

Definition

Some $\mathbf{d}$-admissible $\mathbf{a} = (a_1, \ldots, a_k) \in \mathbb{F}_{\mathbf{d}}$ is *normal* if $a_i \in \mathbb{F}_{q^{d_i}}$ is normal over $\mathbb{F}_q$ for every $i = 1, \ldots, k$.

Normality's behavior in intermediate extensions

Theorem

Let m and d be such that $d \mid m$. The mapping

$$\nu : \{\gamma \in \mathbb{F}_{q^m} : \gamma \text{ normal}\} \to \{c \in \mathbb{F}_{q^d} : c \text{ normal}\},\ \gamma \mapsto \mathrm{Tr}_{m/d}(\gamma)$$

is an k-to-one correspondence, where $k = \Phi(x^m - 1)/\Phi(x^d - 1)$.

Corollary

Let $\mathbb{F}_{q^m}/\mathbb{F}_q$ be a finite field extension. For every $b \in \mathbb{F}_q^*$, there exist exactly $\Phi(x^m - 1)/(q - 1)$ normal elements $\beta \in \mathbb{F}_{q^m}$, such that $\mathrm{Tr}(\beta) = b$.

Intermediate traces of normal elements

Using the above, and inspired by the work of Reis (2020), we prove

Theorem

Let m be an integer that is not a prime power and $1 < k < \sigma_0(m)$, where $\sigma_0(m)$ denotes the number of positive divisors of m. Let $\mathbf{d} = (d_1, \ldots, d_k) \in \lambda_k(m)$ and $\mathbf{a} = (a_1, \ldots, a_k) \in \mathbb{F}_{\mathbf{d}}$ be a normal $\mathbf{d}$-admissible k-tuple. Set $g := \mathrm{lcm}(x^{d_1} - 1, \ldots, x^{d_k} - 1)$. Then there exist exactly $\Phi(x^m - 1)/\Phi(g)$ normal elements $\alpha \in \mathbb{F}_{q^m}$ with prescribed traces $\mathrm{Tr}_{m/d_i}(\alpha) = a_i$ for every $1 \leqslant i \leqslant k$.

Counting primitive normal elements

- Take $\mathbf{a} \in \mathbb{F}_{\mathbf{d}}$ a normal $\mathbf{d}$-admissible k-tuple. Let $\mathfrak{N}_{m,\mathbf{d},\mathbf{a}}$ be the number of primitive normal elements $\alpha \in \mathbb{F}_{q^m}$ with $\mathrm{Tr}_{m/d_i}(\alpha) = a_i$ for $i = 1, \ldots, k$.
- We have that $\mathfrak{N}_{m,\mathbf{d},\mathbf{a}} = \sum_{w \in \mathbb{F}_{q^m}} \rho_m(w) \cdot \kappa_m(w) \prod_{i=1}^{k} \tau_{m,d_i,a_i}(w)$.
- Set $D = d_1 + \cdots + d_k$. We compute

$$\frac{q^D \cdot \mathfrak{N}_{m,\mathbf{d},\mathbf{a}}}{\theta(q)\Theta(x^m-1)} = \sum_{\substack{t \mid q^m-1 \\ f \mid x^m-1}} \frac{\mu(t)\mu'(f)}{\phi(t)\Phi(f)} \sum_{\substack{\eta \in \Gamma(t) \\ \psi \in \Gamma(f)}} \sum_{\mathbf{c} \in \mathbb{F}_{\mathbf{d}}} \chi_{s(\mathbf{c})}(-\beta) G_m(\eta, \chi_{u+s(\mathbf{c})}),$$

where $G_m(\eta, \chi_{u+s(\mathbf{c})}) = \sum_{w \in \mathbb{F}_{q^m}} \eta(w) \cdot \chi_{u+s(\mathbf{c})}(w)$.

Divide and conquer

- We separate the last sum in two terms S_1 and S_2.
- The term S_1 is the part of the above sum for $\eta \in \Gamma(1)$.
- Then $\theta(q)\Theta(x^m - 1)S_1$ denotes the number of normal elements with their traces over $\mathbb{F}_{q^{d_i}}$ prescribed to a_i, that is,

$$S_1 = \frac{q^m}{\Phi(g)\theta(q)} > q^{m-\lambda(\mathbf{d})}.$$

- The term S_2 is the part for $\eta \notin \Gamma(1)$.
- Using known bounds, we obtain

$$|S_2| \leqslant q^{m/2+D} \cdot W(q^m - 1) \cdot W(x^m - 1).$$

The main result

Theorem

Let m be an integer and $1 < k < \sigma_0(m)$, where $\sigma_0(m)$ denotes the number of positive divisors of m. Let $\mathbf{d} = (d_1, \ldots, d_k) \in \lambda_k(m)$ and $\mathbf{a} = (a_1, \ldots, a_k) \in \mathbb{F}_{\mathbf{d}}$ be normal $\mathbf{d}$-admissible. Then there exists a primitive normal element $\alpha \in \mathbb{F}_{q^m}$ with prescribed traces $\mathrm{Tr}_{n/d_i}(\alpha) = a_i$ for every $1 \leqslant i \leqslant k$, provided that

$$q^{m/2-\lambda(\mathbf{d})-D} \geqslant W(q^m - 1) \cdot W(x^m - 1).$$

Explicit results

Along with known bounds, the above theorems imply:

Theorem

Let m be an integer and $1 < k < \sigma_0(m)$. Let $\mathbf{d} = (d_1, \ldots, d_k) \in \lambda_k(m)$ and $\mathbf{a} = (a_1, \ldots, a_k) \in \mathbb{F}_{\mathbf{d}}$ be normal $\mathbf{d}$-admissible. Suppose $\gcd(d_i, d_j) = 1$ for $1 \leqslant i < j \leqslant k$. Then there exists a primitive normal element $\alpha \in \mathbb{F}_{q^m}$ with prescribed traces $\mathsf{Tr}_{n/d_i}(\alpha) = a_i$ for every $1 \leqslant i \leqslant k$ provided that:

1. $k \geqslant 4$ *and* $q \geqslant 18015$.
2. $k = 3$, $m \geqslant 60$ *and* $q \geqslant 2.2660 \cdot 10^{24072855}$.
3. $k = 2$ *and*
   - 3.1. $d_1 \geqslant 8$ *and q large enough,*
   - 3.2. $d_1 = 7$ *and q large enough with* $(d_1, d_2) \neq (7, 8)$,
   - 3.3. $d_1 = 6$, $d_2 \geqslant 13$ *and q large enough.*

Complete normality

- Recall that normal elements always exist (Normal Basis Theorem).
- Recall that primitive normal elements always exist (Primitive Normal Basis Theorem).
- From now on, we will call an element of $\mathbb{F}_{q^m}$ that is normal over $\mathbb{F}_{q^d}$ (where $d \mid m$) *q^m/q^d-normal*.
- Some $a \in \mathbb{F}_{q^m}$ is *completely normal* if it is q^m/q^d-normal $\forall\, d \mid m$.

Theorem (Completely Normal Basis Theorem)

There exists some $a \in \mathbb{F}_{q^m}$ that is q^m/q-completely normal.

- Initially established in 1986 by Blessenohl and Johnsen.
- In 1994, Hachenberger gave a simplified proof.

The Morgan-Mullen conjecture

A simple glimpse to the aforementioned results leads to the following conjecture.

Conjecture (Morgan-Mullen, 1996)

There exists some $a \in \mathbb{F}_{q^m}$ that is primitive and q^m/q-completely normal.

- We will call the pair (q, m) *MM pair* if the finite field extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ is known or proven to contain a primitive and q^n/q-completely normal element.
- We know that (q, m) is an MM pair for some families of extensions and directly verified for "small" finite field extensions, while no counterexample are known.
- This evidence suggests the validity of the conjecture, which remains unresolved.

Towards the PCNBT

Direct verification

Theorem (Morgan-Mullen, 1996)

Suppose that $q \leqslant 97$ *and* $q^n < 10^{50}$. *Then* (q, n) *is an MM pair.*

Theorem (Hachenberger-Hackenberg, 2019)

Suppose that

1. $n \leqslant 202$ *or*
2. $q < 10^4$ *and* $q^n < 10^{80}$.

Then, (q, n) *is an MM pair.*

Towards the PCNBT

Completely basic extensions

Definition

Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be such that every q^n/q-normal element is q^n/q-completely normal. Then the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is called *completely basic*.

For the case of completely basic extensions, the Morgan-Mullen conjecture follows directly from the Primitive Normal Basis Theorem.

Theorem (Blessenohl-Johnsen, 1991)

The finite field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is completely basic if and only for every prime divisor r of n, $r \nmid d$, where d stands for the order of q modulo the relatively prime to q part of n/r.

In particular (Hachenberger, 2013), this family includes the cases $n = r$, $n = r^2$ (r prime), $n \mid q - 1$ or $n = p^k$, where $p = \operatorname{char} \mathbb{F}_q$.

Towards the PCNBT

Regular extensions

Definition

If $\gcd(n, d) = 1$, where d is the order of q modulo the product of the prime divisors of n that do not divide q, then $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a *regular extension*.

Theorem (Hachenberger)

Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be a regular extension. Then (q, n) is an MM pair.

- The above was initially partially established by Hachenberger in 2001 and 2010 and fully established by the same author in 2019.
- The proof required deep understanding of the underlying module structure of finite fields and combines algebraic and character sum methods.

Towards the PCNBT

Examples of regular extensions

Hachenberger (2013) observed that $\mathbb{F}_{q^n}/\mathbb{F}_q$ is regular in the following cases:

- $\mathbb{F}_{q^n}/\mathbb{F}_q$ is completely basic.
- The set $D = \{r \mid n : r \text{ prime}\}$ satisfies
  1. $|D| = 1$, or,
  2. for every $r \in D$ we have that $r \mid q - 1$ or $r \mid q$, or,
  3. $D \subseteq \{7, 11, 13, 17, 19, 31, 41, 47, 49, 61, 73, 97, 101, 107, 109, 139, 151, 163, 167, 173, 179, 181, 193\}$.
- n is a power of a Carmichael number.

Towards the PCNBT

Combinatorial results

Simple combinatorial arguments led to the following.

Theorem (Hachenberger, 2016)

Suppose that

1. $q \geqslant n^{7/2}$ *and* $n \geqslant 7$ *or*
2. $q \geqslant n^3$ *and* $n \geqslant 37$,

then (q, n) *is an MM pair.*

A crucial part of the proof of the above is a combinatorics-driven estimate of the number of q^n/q-completely normal elements, that does not depend on the prime decomposition of n.

Towards the PCNBT

Character sum results

Using the character sum method, the following was established:

Theorem (Garefalakis-K., 2019)

If the part of n that is relatively prime to q is smaller than q, then (q, n) is an MM pair. In particular, (q, n) is an MM pair for all $n \leqslant q$.

With more attention given to technical details, the above was further improved soon after.

Theorem (Garefalakis-K., 2019)

If either

1. *n is odd and $n < q^{4/3}$, or*
2. *n is even, $q - 1 \nmid n$ and $n < q^{5/4}$,*

then (q, n) is an MM pair.

Towards the PCNBT

Future results?

We aim to make an additional step towards the proof of the Morgan-Mullen conjecture, with a combination of character sum and algebraic methods. Our goal is to

- mark some additional pairs (q, n) as MM pairs and
- add a new recursive weapon to the arsenal found in the literature for the researcher willing to attack this problem.

This talk was based on joint work with D.K. Basnet and A.C. Mazumder (submitted for publication) and on ongoing joint work with Th. Garefalakis.

Thank you for your attention!