Translates of completely normal elements and the Morgan-Mullen conjecture

3rd Greek Number Theory Meeting
Patras - December 2025

Giorgos Kapetanakis
Joint work with T. Garefalakis

University of Thessaly
kapetanakis@uth.gr
gkapet.users.uth.gr

Outline

- Motivation
- Known cases
- Preparation
- A new construction of completely normal elements
- Conditions
- Results
- Future work
- The translate properties and the MM property

Basic notation and concepts

- Let q be a power of the prime p and n a positive integer.
- Set $\mathbb{F}_q$ the finite field of order q, $\mathbb{F}_{q^n}$ for its extension of degree n, and for $d \mid n$, $\mathbb{F}_{q^d}$ the corresponding intermediate extension.
- Some $a \in \mathbb{F}_{q^n}$ is called *primitive* if it generates the multiplicative group $\mathbb{F}_{q^n}^*$. It is known that every finite field contains primitive elements, while primitive elements are important for both theoretical and practical reasons.
- Some $a \in \mathbb{F}_{q^n}$ is called q^n/q*-normal* (or *normal over* $\mathbb{F}_q$ or just *normal*) if its $\mathbb{F}_q$-conjugates form an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$ (when viewed as an $\mathbb{F}_q$-vector space). A basis of this form is called an q^n/q*-normal basis*.
- Some $a \in \mathbb{F}_{q^n}$ is called q^n/q*-completely normal* (or just *completely normal*) if it is q^n/q^d-normal for all $d \mid n$.

The normal basis theorem

Theorem (Normal Basis Theorem)

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

- Initially established by Hensel (1888).
- Also proven in the more generally setting of finite Galois extensions, independently by Noether (1932) and Deuring (1933).

The primitive normal basis theorem

A natural question is whether there exist elements of $\mathbb{F}_{q^n}$ that combine both of the above properties. The answer to that question was given by the following celebrated result.

Theorem (Primitive Normal Basis Theorem)

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

- Initially established by Lenstra Jr. and Schoof (1987).
- Cohen and Huczynska (2003) gave a computer-free proof.

The completely normal basis theorem

Theorem (Completely Normal Basis Theorem)

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

- Initially established by Blessenohl and Johnsen (1986), with general Galois extensions in mind.
- Hachenberger (1994) gave a simplified proof that is specific to finite field extensions.

The Morgan-Mullen conjecture

A simple glimpse to the previous theorems leads to wondering about the existence of elements of $\mathbb{F}_{q^n}$ that are, at the same time, primitive and completely normal.

Conjecture (Morgan-Mullen, 1996)

Every finite field extension possesses the MM property.

- The extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the *MM property* if it contains an element $a \in \mathbb{F}_{q^n}$ that is primitive and completely normal.
- Partially established by various means.
- No known counterexamples.

Computational results

- The most obvious method is direct verification with the help of computers.
- This is in fact the method that Morgan and Mullen used in order to support their conjecture.

Theorem (Morgan-Mullen, 1996)

Suppose that $q \leqslant 97$ *and* $q^n < 10^{50}$. *Then* $\mathbb{F}_{q^n}/\mathbb{F}_q$ *possesses the MM property.*

Theorem (Hachenberger-Hackenberg, 2019)

Suppose that $n \leqslant 202$ *or* $q < 10^4$ *and* $q^n < 10^{80}$. *Then,* $\mathbb{F}_{q^n}/\mathbb{F}_q$ *possesses the MM property.*

Completely basic extensions

- If $\mathbb{F}_{q^n}/\mathbb{F}_q$ is such that every q^n/q-normal element is q^n/q-completely normal, this extension is *completely basic*.
- The MM property is immediate for completely basic extensions.
- We have a complete characterization.

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.

- This family includes cases such as $n = r^2$ (where r is a prime number), $n \mid q - 1$ or $n = p^k$, where k is arbitrary and $p = \operatorname{char} \mathbb{F}_q$.

Regular extensions

- 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 called a *regular extension*.
- Completely basic extensions are regular extensions.
- This family also include extensions $\mathbb{F}_{q^n}/\mathbb{F}_q$, where 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. $D \subseteq \{7, 11, 13, 17, 19, 31, 41, 47, 49, 61, 73, 97, 101, 107, 109, 139, 151, 163, 167, 173, 179, 181, 193\}$.
- $\mathbb{F}_{q^n}/\mathbb{F}_q$ is regular if n is a power of a Carmichael number.

Regular extensions

It has been established that regular extensions possess the MM property.

Theorem (Hachenberger)

Regular extensions possess the MM property.

- Partially established by Hachenberger (2001 and 2010).
- Fully established by the same author in 2019.
- This required deep understanding of the underlying module structure of finite fields and combines algebraic and character sum methods.

A combinatorial effort

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 $\mathbb{F}_{q^n}/\mathbb{F}_q$ *possesses the MM property.*

- Uses elementary combinatorial arguments.
- The proof depends on an estimate of the number of q^n/q-completely normal elements, that derives from combinatorial arguments.
- The number of q^n/q-completely normal elements is unknown and we do not even have useful estimates if n is large compared to q.

Our first addition

Theorem (Garefalakis-K., 2018)

If the part of n that is relatively prime to q is smaller than q, then $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property. In particular, all extensions $\mathbb{F}_{q^n}/\mathbb{F}_q$ with $n \leqslant q$ possess the MM property.

- A tweak of the character sum method was used.

An improvement

Theorem (Garefalakis-K., 2018)

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 $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property.

- Essentially with the same techniques as the previous result, with more emphasis given to technical details.

Characters

We will use the following incomplete character sum estimate.

Theorem

Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be a finite field extension and take χ a multiplicative character of $\mathbb{F}_{q^n}$ and ψ an additive character of $\mathbb{F}_q$, such that not both of them are trivial. Further, let $a \in \mathbb{F}_{q^n}$ be such that $\mathbb{F}_q(a) = \mathbb{F}_{q^n}$. Then

$$\left| \sum_{c \in \mathbb{F}_q} \chi(a+c)\psi(c) \right| \leqslant nq^{1/2}.$$

- Initially shown by Fu and Wan (2014).
- A simplified proof was recently presented by Mazumder, K., Kala, and Basnet (2025).

Characteristic functions

Primitivity

By Vinogradov's formula, the characteristic function for $a \in \mathbb{F}_{q^n}$ being primitive is

$$\omega(a) := \theta(q') \sum_{d \mid q'} \frac{\mu(d)}{\phi(d)} \sum_{\chi \in \widehat{\mathbb{F}_{q^n}^*},\, \mathrm{ord}(\chi) = d} \chi(a),$$

where $q' = q^n - 1$, $\theta(r) = \phi(r)/r$, μ is the Möbius function and ϕ is the Euler function.

Characteristic functions

Normality

The characteristic function for $a \in \mathbb{F}_{q^d}$ being q^d/q-normal is

$$\Omega_d(a) := \theta_q(F'_d) \sum_{f \mid F'_d} \frac{\mu_q(f)}{\phi_q(f)} \sum_{\psi \in \widehat{\mathbb{F}_{q^d}},\, \mathrm{ord}(\psi) = f} \psi(a),$$

where $F'_d = x^d - 1 \in \mathbb{F}_q[x]$, $\theta_q(f) := \phi_q(f)/q^{\deg(f)}$ and μ_q and ϕ_q are the Möbius and Euler functions in $\mathbb{F}_q[x]$, respectively.

Characteristic functions

Non-zero elements

The orthogonality relations yield that the characteristic function for some $a \in \mathbb{F}_q$ to be nonzero is

$$z(a) = \frac{1}{q} \sum_{\eta \in \widehat{\mathbb{F}_q}} (1 - \eta(a)).$$

Translates and trace

- The *set of translates* of $a \in \mathbb{F}_{q^n}$ is defined as

$$\mathcal{T}_a = \{a + c : c \in \mathbb{F}_q\}.$$

- The q^n/q*-trace* is the function

$$\mathrm{Tr}_{q^n/q} : \mathbb{F}_{q^n} \to \mathbb{F}_q,\ a \mapsto \sum_{i=0}^{n-1} a^{q^i} = \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)} \sigma(a).$$

- It is known that if a is q^n/q-normal, then $\mathrm{Tr}_{q^n/q}(a) \neq 0$.

Some background from the proof of the CNBT

In the proof of the CNBT the following plays a vital role.

Proposition (Hachenberger, 1994)

Assume that $n = n_1 n_2$ where n_1, n_2 are relatively prime. If $a_i \in \mathbb{F}_{q^{n_i}}$ is q^{n_i}/q-completely normal for $i = 1, 2$, then $a_1 a_2$ is q^n/q-completely normal.

- Inductively, this leads to the CNBT.
- Here, we are interested in q^n/q-completely normal elements with multiplicative order $q^n - 1$.
- The element $a_1 a_2$ above has order at most $(q^{n_1} - 1)(q^{n_2} - 1)/(q - 1)$, i.e., it is never primitive.
- This is a key factor for the persistence of the Morgan-Mullen Conjecture.

Our generalization

An auxiliary lemma

Lemma

Suppose $a \in \mathbb{F}_{q^n}$ is q^n/q-normal and take some $c \in \mathbb{F}_q$. If $p \mid n$, then $a + c$ is q^n/q-normal. If $p \nmid n$, then the following are equivalent:

1. *$a + c$ is q^n/q-normal.*
2. $\mathrm{Tr}_{q^n/q}(a + c) \neq 0$.
3. *$c \neq -\mathrm{Tr}_{q^n/q}(a) \cdot n^{-1}$, where n is seen as an element of $\mathbb{F}_q$.*

Our generalization

An auxiliary proposition

Proposition

Assume that $n = n_1 n_2$ where n_1 and n_2 are relatively prime. If $a_i \in \mathbb{F}_{q^{n_i}}$ is q^{n_i}/q-completely normal for $i = 1, 2$. If $p \mid n$, then $a_1 a_2 + c$ is q^n/q-completely normal for every $c \in \mathbb{F}_q$. If $p \nmid n$, then, for every $c \in \mathbb{F}_q$, the following are equivalent:

1. *$a_1 a_2 + c$ is q^n/q-completely normal.*
2. *$\mathrm{Tr}_{q^n/q}(a_1 a_2 + c) \neq 0$.*
3. *$c \neq -\mathrm{Tr}_{q^n/q}(a_1 a_2) \cdot n^{-1}$, where n is seen as an element of $\mathbb{F}_q$.*

Our generalization

Sketch of the proof

- $a_1 a_2$ is q^n/q-completely normal.
- Fix some $c \in \mathbb{F}_q$. If $c = -n^{-1} \operatorname{Tr}_{q^n/q}(a_1 a_2)$ (in the case $p \nmid n$), $a_1 a_2 + c$ cannot be q^n/q-completely normal. So, from now on, either $p \mid n$, or $\operatorname{Tr}_{q^n/q}(a_1 a_2 + c) \neq 0$ if $p \nmid n$.
- Take some $d \mid n$. If $p \mid (n/d)$, $a_1 a_2 + c$ is q^n/q^d-normal. So, we focus on the case $p \nmid (n/d)$.
- In this case, $a_1 a_2 + c$ is q^n/q^d-normal if $\operatorname{Tr}_{q^n/q^d}(a_1 a_2 + c) \neq 0$. However, if this is not the case, then

$$\operatorname{Tr}_{q^n/q}(a_1 a_2 + c) = \operatorname{Tr}_{q^d/q}\left(\operatorname{Tr}_{q^n/q^d}(a_1 a_2 + c)\right) = \operatorname{Tr}_{q^d/q}(0) = 0,$$

a contradiction.

Translates of completely normal elements

Theorem

Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be a finite field extension and let $n = p_1^{n_1} \cdots p_k^{n_k}$ be the prime decomposition of n, with $k \geqslant 2$. Further, take some $q^{p_i^{n_i}}$/q-completely normal a_i, for every $i = 1, \ldots, k$ and set $a = a_1 \cdots a_k$.

1. *If $p \mid n$, the set of translates $\mathcal{T}_a$ is comprised of q^n/q-completely normal elements.*
2. *If $p \nmid n$, then the set $\mathcal{T}_a \setminus \{a - Tr_{q^n/q}(a) \cdot n^{-1}\}$ (where n is seen as an element of $\mathbb{F}_q$), is comprised of q^n/q-completely normal elements*

Proof

Inductively, $a_1 \cdots a_{k-1}$ is $q^{p_1^{n_1} \cdots p_{k-1}^{n_{k-1}}}$/$q$-completely normal. Now, apply the last proposition. □

Partially completely basic extensions

We introduce the following notion.

Definition

Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be an extension of finite fields, such that
1. $n = n_1 n_2$, where $n_1, n_2 > 1$ with $\gcd(n_1, n_2) = 1$ and
2. $\mathbb{F}_{q^{n_2}}/\mathbb{F}_q$ is completely basic.

Then we call the extension (n_1, n_2)-*partially completely basic*.

- The family of partially completely basic extensions is large.
- For example, if $n = r_1^{n_1} \cdots r_k^{n_k}$ and $\mathbb{F}_{q^n}/\mathbb{F}_q$ is not completely basic, it is partially completely basic if $n_i = 1$ or 2 for some i, if $r_i = p$ for some i, or, if $r_i^{n_i} \mid q^n - 1$ for some i.
- An extension may be (n_1, n_2)-partially completely basic for multiple parameters n_1 and n_2.

A condition

Theorem

Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be an (n_1, n_2)-partially completely basic extension, such that $p \nmid n$ and

$$\frac{q-2}{q-1} \cdot q^{n_2/2} \geqslant 2n_1 W(q') W(F'_{n_2}),$$

where $W(X)$ is the number of squarefree divisors of X, $q' = q^n - 1$ and $F'_{n_2} = x^{n_2} - 1 \in \mathbb{F}_{q^{n_2}}[x]$. Then $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property.

Sketch of the proof

- Take some $a \in \mathbb{F}_{q^{n_1}}$ that is q^{n_1}/q-completely normal.
- Since $\mathbb{F}_{q^{n_2}}/\mathbb{F}_q$ is completely basic, if we identify some $b \in \mathbb{F}_{q^{n_2}}$ and $c \in \mathbb{F}_q^*$ such that
  1. b is q^{n_2}/q-normal,
  2. $ab + c$ is primitive, and
  3. $\mathrm{Tr}_{q^n/q}(ab + c) \neq 0$,

  then $ab + c$ is primitive and q^n/q-completely normal.
- The number of $(b, c) \in \mathbb{F}_{q^{n_2}} \times \mathbb{F}_q^*$ that combine the desired properties as above is

$$\mathcal{N} = \sum_{b \in \mathbb{F}_{q^{n_2}}} \sum_{c \in \mathbb{F}_q^*} \omega(ab + c)\Omega_{n_2}(b) z\left(\mathrm{Tr}_{q^n/q}(ab + c)\right).$$

Sketch of the proof

- We have that

$$\frac{\mathcal{N}}{\theta(q')} = \sum_{d|q'} \frac{\mu(d)}{\phi(d)} \sum_{\substack{\chi \in \widehat{\mathbb{F}_{q^n}^*} \\ \mathrm{ord}(\chi)=d}} \sum_{\substack{b \in \mathbb{F}_{q^{n_2}} \\ c \in \mathbb{F}_q^*}} \chi(ab+c)\Omega_{n_2}(b) z\left(\mathrm{Tr}_{q^n/q}(ab+c)\right)$$

$$= S_1 + S_2,$$

  where S_1 corresponds to $d = 1$ and S_2 to $d \neq 1$.

- Then, $S_1 = (q-2)\phi_q(F'_{n_2})$ and

$$|S_2| < \frac{\phi_q(F'_{n_2})}{q^{n_2/2}} W(q') W(F'_{n_2})(q-1)2n_1.$$

- The result follows.

The case $p \mid n$

For the case $p \mid n$ we have the following improved version.

Theorem

Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be an (n_1, n_2)-partially completely basic extension, such that $p \mid n$. Then, if

$$q^{n_2/2} \geqslant n_1 W(q') W(F'_{n_2}),$$

$\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property.

A remark on $q = 2$

- The first theorem is ineffective in the case $q = 2$ as its condition can never hold.
- The reason is that, the set where we are looking for primitive completely normal elements is the singleton $\{ab\}$, but ab is never primitive.
- The case $q = 2$ and n even can be treated by the second theorem.

An asymptotic result

Lemma (Apostol, 1976)

For every $\delta > 0$, $W(n) = o(n^{\delta})$, where o signifies the little-o notation.

Lemma (Lenstra-Schoof, 1987)

Let q be a prime power and n a positive integer. Then, we have $W(F'_n) \leqslant 2^{\frac{1}{2}(n+\gcd(n,q-1))}$. In particular, $W(F'_n) \leqslant 2^n$, while the equality holds if and only if $n \mid q-1$. Furthermore, if $n \nmid q-1$, $W(F'_n) \leqslant 2^{3n/4}$.

Lemma (Aguirre-Neumann, 2021)

Let q be a prime power and n a positive integer. Then, $W(F'_n) \leqslant 2^{\frac{n+a}{b}}$ for some $a, b \in \mathbb{Z}$. In particular, for $q \geqslant 29$, we have $(a, b) = (0, 1)$; for $7 \leqslant q \leqslant 27$, we have $(a, b) = (q-1, 2)$ and for $q \leqslant 5$ we have the following values for a, b:

q	a	b	q	a	b	q	a	b	q	a	b
2	14	5	3	20	4	4	12	3	5	18	3

An asymptotic result

Upon combining the previous lemmas with our conditions, we obtain:

Theorem

Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be an (n_1, n_2)-partially completely basic extension, where n_2 is large compared to n_1, then $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property, unless n is odd and $q = 2$.

An algorithm for the MM property

Preparation

Lemma (Cohen-Huczynska, 2003)

For any $\alpha \in \mathbb{N}$ and a positive real number ν, $W(\alpha) \leqslant \mathcal{C}_\nu^{(\alpha)} \cdot \alpha^{1/\nu}$, where $\mathcal{C}_\nu^{(\alpha)} = \prod_{i=1}^{t} 2/(p_i^{1/\nu})$ and $p_1, p_2, \ldots, p_t$ are the primes less than or equal to 2^ν that divide α.

Let $p_1, \ldots, p_s$ be *all* the primes less or equal to 2^ν. In addition to the number $\mathcal{C}_\nu^{(\alpha)}$ defined above we will use the following two numbers:

1. $\mathcal{C}_\nu := \prod_{i=1}^{s} 2/(p_i^{1/\nu})$. Clearly, $\mathcal{C}_\nu^{(\alpha)} \leqslant \mathcal{C}_\nu$ for all $\alpha \in \mathbb{Z}$.
2. For any $1 \leqslant j \leqslant s$, $\mathcal{C}_\nu^{[p_j]} := \mathcal{C}_\nu p_j^{1/\nu}/2$. Clearly, $\mathcal{C}_\nu^{(\alpha)} \leqslant \mathcal{C}_\nu^{[p_j]}$ for all $\alpha \in \mathbb{Z}$ with $p_j \nmid \alpha$.

An algorithm for the MM property

Input: n_1
Output: **SUCCESS** or **FAIL**

Step 1 Set $n_{\min}$ as the minimum value of n_2 that is not covered by the Hachenberger-Hackenberg computations.

Step 2 For $n_2 = n_{\min}$, find $q_{\max}$, the minimum q that satisfies our condition, with estimates for $W(F'_{n_2})$ and $W(q')$ (we use $\mathcal{C}_{4n_1}$).

Step 3 For each $3 \leqslant q < q_{\max}$, find the maximum value of n_2, $n_{\max}^{(q)}$, not satisfying the condition of the previous step (we use $\mathcal{C}_{4n_1}^{[p]}$).

Step 4 For each $3 \leqslant q \leqslant q_{\max}$ we identify which $n_{\min} \leqslant n_2 \leqslant n_{\max}^{(q)}$ are such that

- $\mathbb{F}_{q^{n_2}}/\mathbb{F}_q$ is completely basic,
- $\gcd(n_1, n_2) = 1$, and
- $q^{n_1 n_2} > 10^{80}$.

An algorithm for the MM property

Step 5 For each pair check our condition, with $W(F'_{n_2})$ explicitly computed and $W(q')$ estimated (we use $\mathcal{C}_{4n_1}^{(q^{n_1 n_2}-1)}$). Remove from the list of possible exceptions the pairs that pass this test.

Step 6 For each pair check our condition, with $W(F'_{n_2})$ and $W(q')$ explicitly computed. Remove from the list of possible exceptions the pairs that pass this test.

Step 7 If the list of possible exceptions is nonempty, return **FAIL**.

Step 8 Repeat the previous steps for $q = 2$ with the second condition ($p \mid n$) over the first ($p \nmid n$).

Step 9 If the list of possible exceptions remain nonempty, return **FAIL**. Otherwise, return **SUCCESS**.

An explicit result

We successfully applied the algorithm (on SageMath) for $n_1 = 2$ and 3 and obtained partial results for $n_1 = 4$.

Theorem

Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be an (n_1, n_2)-partially completely basic extension. Then $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property in the following cases:

1. $n_1 = 2$ *or* 3.
2. $n_1 = 4$ *and either*
   - $q \geqslant 19921127251118963 9 \ (\approx 2 \cdot 10^{17})$,
   - $n_2 \geqslant n_1^{n_1} = 256$ *and* $q \geqslant 22271$, *or,*
   - $n_2 \geqslant n_1^6 = 4096$.

Future work

- We believe that (with additional computational efforts) our concrete results can potentially be extended to $n_1 = 4$.
- Increasing n_1 further should be feasible after implementing known methods for relaxing conditions such as ours. These methods should increase n_1 to two-digit numbers.
  - Prime sieve (Cohen-Huczynska, 2003).
  - Modified prime sieve (Bailey-Cohen-Sutherland-Trudgian, 2019).
  - Hybrid bound (Bagger, 2024).
- In the literature, for example see (Aravena, 2020), one can find additional constructions of completely normal elements. These constructions could be exploited into establishing the MM property for additional finite fields extensions.

The translate properties

Definitions

Definition

Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be a finite field extension such that, for every $a \in \mathbb{F}_{q^n}$ such that $\mathbb{F}_q(a) = \mathbb{F}_{q^n}$, some primitive element lies within the set of translates $\mathcal{T}_a$. Then the extension possesses the *translate property*. If, every such set of translates $\mathcal{T}_a$ contains two distinct primitive elements, then the extension possesses the *strong translate property*.

The translate properties

The theorems

Theorem (Translate Property)

Let n be a positive integer. There exists some $\mathrm{TP}(n)$ such that for every prime power $q > \mathrm{TP}(n)$, the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the translate property.

- Initially established by Davenport (1937) for prime q.
- Extended to its stated form by Carlitz (1953).
- In this work we prove the strong version.

Theorem (Strong Translate Property)

Let n be a positive integer. There exists some $\mathrm{STP}(n) \geqslant \mathrm{TP}(n)$ such that for every prime power $q > \mathrm{STP}(n)$, the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the strong translate property.

A connection

Our construction implies the following:

Theorem

Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be a finite field extension. If, either

1. $p \mid n$ *and* $q > \mathrm{TP}(n)$, *or,*
2. $q > \mathrm{STP}(n)$,

then the extension possesses the MM property.

A connection

Is it useless?

- The above seems like a meaningful way to attack the Morgan-Mullen conjecture, but this is not the case.
- Little is known about the numbers $\mathrm{TP}(n)$ and only a handful of them are known.
- We know that $\mathrm{TP}(2) = 1$, $\mathrm{TP}(3) = 37$, and $43 \leqslant \mathrm{TP}(4) \leqslant 102829$ (Bailey-Cohen-Sutherland-Trudgian, 2019).
- These suggest that $\mathrm{TP}(\mathrm{n})$ is significantly larger than n.
- Hence, known results already cover the extensions that are known to possess the (strong) translate property.

References I


J. J. Aguirre and V. G. Neumann. Existence of primitive 2-normal elements in finite fields. *Finite Fields Appl.*, 73(101864):26 pages, 2021.


T. Apostol. *Introduction to Analytic Number Theory*. Springer-Verlag, New York Heidelberg Berlin, 1976.


A. Aravena. Iterated constructions of completely normal polynomials. *Finite Fields Appl.*, 68(101755):12 pages, 2020.


G. K. Bagger. Hybrid bounds for prime divisors. arXiv:2412.00010 [math.NT], 2024.


G. Bailey, S. D. Cohen, N. Sutherland, and T. Trudgian. Existence results for primitive elements in cubic and quartic extensions of a finite field. *Math. Comp.*, 88(316):931–947, 2019.


D. Blessenohl and K. Johnsen. Eine verschärfung des satzes von der normalbasis. *J. Algebra*, 103(1):141–159, 1986.


D. Blessenohl and K. Johnsen. Stabile teilkörper galoisscher erweiterungen und ein problem von C. Faith. *Arch. Math.*, 56:245–253, 1991.


L. Carlitz. Distribution of primitive roots in a finite field. *Quart. J. Math. Oxford Ser. (2)*, 4(1):4–10, 1953.


S. D. Cohen and S. Huczynska. The primitive normal basis theorem – without a computer. *J. London Math. Soc.*, 67(1):41–56, 2003.


H. Davenport. On primitive roots in finite fields. *Quart. J. Math. Oxford*, 8(1):308–312, 1937.

References II


L. Fu and D. Wan. A class of incomplete character sums. *Q. J. Math.*, 65(4):1195–1211, 2014.


T. Garefalakis and G. Kapetanakis. Further results on the Morgan-Mullen conjecture. *Des. Codes Cryptogr.*, 87(11):2639–2654, 2019.


T. Garefalakis and G. Kapetanakis. On the existence of primitive completely normal bases of finite fields. *J. Pure Appl. Algebra*, 223(3):909–921, 2019.


D. Hachenberger. On completely free elements in finite fields. *Des. Codes Cryptogr.*, 4:129–143, 1994.


D. Hachenberger. *Finite Fields: Normal Bases and Completely Free Elements*, volume 390 of *Kluwer Internat. Ser. Engrg. Comput. Sci.* Kluwer Academic Publishers, Boston, MA, 1997.


D. Hachenberger. Primitive complete normal bases for regular extensions. *Glasgow Math. J.*, 43(3):383–398, 2001.


D. Hachenberger. Primitive complete normal bases: Existence in certain 2-power extensions and lower bounds. *Discrete Math.*, 310(22):3246–3250, 2010.


D. Hachenberger. Completely normal bases. In G. L. Mullen and D. Panario, editors, *Handbook of Finite Fields*, pages 128–138. CRC Press, Boca Raton, 2013.


D. Hachenberger. Asymptotic existence results for primitive completely normal elements in extensions of Galois fields. *Des. Codes Cryptogr.*, 80(3):577–586, 2016.


D. Hachenberger. Primitive complete normal bases for regular extensions: Exceptional cyclotomic modules. arXiv:1912.04886 [math.NT], 2019.

References III


D. Hachenberger and S. Hackenberg. Computational results on the existence of primitive complete normal basis generators. arXiv:1912.07541 [math.NT], 2019.


D. Hachenberger and D. Jungnickel. *Topics in Galois fields*, volume 29 of *Algorithms Comp. Math.* Springer Nature Switzerland, Cham, 2020.


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


R. Lidl and H. Niederreiter. *Finite Fields*, volume 20 of *Encycl. Math. Appl.* Cambridge University Press, Cambridge, 2nd ed. edition, 1997.


A. C. Mazumder, G. Kapetanakis, and D. K. Basnet. Normal and primitive normal elements with prescribed traces in intermediate extensions of finite fields. *Finite Fields Appl.*, 110(102745):14 pages, 2026.


A. C. Mazumder, G. Kapetanakis, S. Kala, and D. K. Basnet. An estimate for incomplete mixed character sums and applications. Submitted for publication, 2025.


I. H. Morgan and G. L. Mullen. Completely normal primitive basis generators of finite fields. *Util. Math.*, 49:21–43, 1996.

This work can be found at
arXiv:2509.23245

Thank you for your attention!