

Translates of completely normal elements and the Morgan-Mullen conjecture

*3rd Congress of Greek Mathematicians
Athens, 1 July 2026*

Giorgos Kapetanakis



University of Thessaly



kapetanakis@uth.gr



gkapet.users.uth.gr

Basic notation and concepts

- 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 (completely) 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), later established in the more general setting of finite Galois extensions by Noether (1932) and Deuring (1933).

Theorem (Completely Normal Basis Theorem)

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

Established by Blessenohl-Johnsen (1986), Hachenberger (1994) gave a simplified proof.

The primitive normal basis theorem

A natural question is whether there exist elements of $\mathbb{F}_{q^n}$ that combine normality and primitivity. 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-Schoof (1987) and Cohen-Huczynska (2003) gave a computer-free proof.
- Numerous generalizations have been considered:
Cohen-Huczynska (2010), GK (2014), GK (2014), GK-Reis (2019).

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, but still open.

Computational results

The most obvious method is direct verification with the help of computers.

Theorem (Morgan-Mullen, 1996)

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

Theorem (Hachenberger-Hackenberg, 2019)

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

Families with the MM property

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*.

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 .

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

Theorem (Hachenberger, 2001, 2010, 2019)

Regular extensions possess the MM property.

General results

Theorem (Hachenberger, 2016)

Suppose that $q \geq n^{7/2}$ and $n \geq 7$, or, $q \geq n^3$ and $n \geq 37$, then $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property.

Theorem (Garefalakis-GK, 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 $n \leq q$ possess the MM property.

Theorem (Garefalakis-GK, 2018)

If either n is odd and $n < q^{4/3}$, or, n is even, $q - 1 \nmid n$ and $n < q^{5/4}$, then $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property.

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.
- 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

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 $a + c$ is q^n/q -normal if and only if $\text{Tr}_{q^n/q}(a + c) \neq 0$.

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

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 $k \geq 2$. Further, take some $q^{p_i^{n_i}}/q$ -completely normal a_i , for every $i = 1, \dots, k$ and set $a = a_1 \cdots a_k$.

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

This means that instead of one q^n/q -completely normal element (that is *definitely not* primitive), we now have $q - 1$ such elements (with most of them being *possibly* primitive).

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 $n = n_1 n_2$, where $n_1, n_2 > 1$ with $\gcd(n_1, n_2) = 1$ and $\mathbb{F}_{q^{n_2}}/\mathbb{F}_q$ is completely basic. Then we call the extension (n_1, n_2) -*partially completely basic*.

The family of partially completely basic extensions is large.

Conditions

Theorem

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

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

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.

Theorem

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

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

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

An asymptotic result

We employ known estimates

- for $W(q')$ by Apostol (1976) and Cohen-Huczynska (2003) and
- for $W(F'_{n_2})$ by Lenstra-Schoof (1987) and Aguirre-Neumann (2021)

and apply them on our conditions. This gives the following:

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 explicit result

We use the same tools to build an algorithm that takes as input n_1 and returns **SUCCESS** if it manages to establish the MM property for all (n_1, n_2) -partially completely basic extensions and **FAIL** otherwise.

By applying it we obtain the following:

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
 - $q \geq 199211272511189639$ ($\approx 2 \cdot 10^{17}$),
 - $n_2 \geq n_1^{n_1} = 256$ and $q \geq 22271$, or,
 - $n_2 \geq n_1^6 = 4096$.

The translate properties

If for every $a \in \mathbb{F}_{q^n}$ such that $\mathbb{F}_q(a) = \mathbb{F}_{q^n}$, $\mathcal{T}_a$ contains a primitive element, then $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the *translate property*. If $\mathcal{T}_a$ contains two primitive elements, $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the *strong translate property*.

Theorem (Davenport-Carlitz, 1937, 1953)

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

In this work we prove the strong version.

Theorem

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

An interesting connection — Is it pointless?

Our construction implies the following:

Theorem

The extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property if, either $p \mid n$ and $q > \text{TP}(n)$, or, $q > \text{STP}(n)$.

- Little is known about the numbers $\text{TP}(n)$ and only a handful of them are known:
 - $\text{TP}(2) = 1$ (Cohen, 1983)
 - $\text{TP}(3) = 37$ (Cohen, 2009)
 - $43 \leq \text{TP}(4) \leq 102829$ (Bailey-Cohen-Sutherland-Trudgian, 2019)
 - $\text{TP}_2(2) = 41$ (Cohen-GK, 2020)
- These suggest that $\text{TP}(n)$ is significantly larger than n , hence, known results already cover the extensions that are known to possess the (strong) translate property.

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.

This work can be found at



T. Garefalakis and G. Kapetanakis.

Translates of completely normal elements and the
Morgan-Mullen conjecture.

Canad. Math. Bull., to appear, 2026.

DOI: 10.4153/S0008439526102082

Thank you for your attention!