TRANSLATES OF COMPLETELY NORMAL ELEMENTS AND THE MORGAN-MULLEN CONJECTURE

THEODOULOS GAREFALAKIS AND GIORGOS KAPETANAKIS

ABSTRACT. Denote by $\mathbb{F}_q$ the finite field of order q and by $\mathbb{F}_{q^n}$ its extension of degree n. Some $a \in \mathbb{F}_{q^n}$ is called *primitive* if it generates the multiplicative group $\mathbb{F}_{q^n}^*$ and it is called q^n/q-*normal* if its $\mathbb{F}_q$-conjugates form an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$ if the latter is viewed as an $\mathbb{F}_q$-vector space. Furthermore, some $a \in \mathbb{F}_{q^n}$ is called q^n/q-*completely normal* if it is q^n/q^d-normal for all $d \mid n$. In this work we prove a new construction of sets of completely normal elements and we establish, under conditions, the existence of elements that are simultaneously primitive and q^n/q-completely normal, covering some yet unresolved cases of a 30-year-old conjecture by Morgan and Mullen.

1. INTRODUCTION

Throughout this text q will denote a power of the prime p and n a positive integer. Further, $\mathbb{F}_q$ will stand for the finite field of order q and $\mathbb{F}_{q^n}$ for its extension of degree n, while for any $d \mid n$, $\mathbb{F}_{q^d}$ will stand for 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 well-known that every finite field contains primitive elements, see [24, Theorem 2.8], while primitive elements of finite fields are important for both theoretical and practical reasons, with their most notable applications found in areas such as cryptography and coding theory.

On the other hand, 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, that is the set

$$\{\sigma(a) : \sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)\} = \{a, a^q, \ldots, a^{q^{n-1}}\},$$

forms an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$ when the latter is viewed as an $\mathbb{F}_q$-vector space. A basis of this form is called an q^n/q-*normal basis*. The existence of these elements is known.

Theorem 1.1 (Normal Basis Theorem)**.** *There exists some $a \in \mathbb{F}_{q^n}$ that is q^n/q-normal.*

For a proof of the above, we refer the reader to [24, Theorem 2.35]. Although primitive elements are more commonly employed for practical purposes than normal elements, the latter category is important for both theoretical and practical reasons on its own right, with their most notable applications found in areas where efficient finite field arithmetic is important, such as coding theory or radar technology.

Date: November 21, 2025.

2020 *Mathematics Subject Classification.* 11T30; 11T23; 12E20.

Key words and phrases. finite fields; primitive elements; normal basis; completely normal basis; Morgan-Mullen conjecture; character sums.

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 1.2 (Primitive Normal Basis Theorem)**.** *There exists some $a \in \mathbb{F}_{q^n}$ that is simultaneously primitive and q^n/q-normal.*

The above was initially established in 1987 by Lenstra Jr. and Schoof [23], but Cohen and Huczynska [9] gave a computer-free proof in 2003. Both of these works employ the *character sum method*, which we will also employ in this work. Roughly speaking, this method is used in existence questions. In its typical application, the number of elements of interest is expressed as a sum that involves characters. Then, the sum is split in two terms: the *main term* and the *error term*. The main term corresponds to all the characters being trivial and the error term is the remaining sum. The existence assertion follows, should the difference of the two terms be nonzero.

A natural question that arises from Theorem 1.1 is whether some $a \in \mathbb{F}_{q^n}$ can be normal over the intermediate extensions of $\mathbb{F}_{q^n}/\mathbb{F}_q$. In particular, $a \in \mathbb{F}_{q^n}$ is called *q^n/q-completely normal* (or just *completely normal*) if it is q^n/q^d-normal for all $d \mid n$ and the existence of such elements has also been established.

Theorem 1.3 (Completely Normal Basis Theorem)**.** *There exists some $a \in \mathbb{F}_{q^n}$ that is q^n/q-completely normal.*

The above was initially established in 1986 by Blessenohl and Johnsen [6], but with general Galois extensions in mind. Later on, in 1994, Hachenberger [14] gave a simplified proof that is specific to finite field extensions.

A simple glimpse to Theorems 1.1, 1.2 and 1.3 immediately leads to wondering about the existence of elements of $\mathbb{F}_{q^n}$ that are, at the same time, primitive and completely normal. Thus, we say that 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. In fact, in 1996 by Morgan and Mullen [27] stated the following.

Conjecture 1.4 (Morgan-Mullen)**.** *Every finite field extension possesses the MM property.*

The above, as we will see in some detail in Section 2, has been partially established. In particular, we know that certain families possess the MM property and the conjecture has been directly verified by computational means, for numerous *small* finite field extensions, while no counterexample has been found. This evidence strongly suggests the validity of this conjecture, which is, however, not yet fully resolved.

The aim of this work is to make an additional step towards the proof of Conjecture 1.4, by establishing that new families of finite field possess the MM property, by adding a new weapon to the arsenal found in the literature, for the researcher willing to attack this problem, and by demonstrating that new algebraic constructions of completely normal elements can be used to attack Conjecture 1.4.

Towards this end, we introduce the family of partially completely basic finite fields extensions and establish that, under conditions, these extensions possess the MM property.

This paper is organized as follows. In Sect. 2 we present the known conditions under which Conjecture 1.4 is known to hold. In Sect. 3 we present some background

material that we will use along the way. In Sect. 4 we establish a novel construction of sets of completely normal elements, see Proposition 4.8 and Theorem 4.11. In Sect. 5 we introduce the family of (n_1, n_2)-*partially completely basic* extensions of finite fields and prove novel conditions that ensures the existence of elements that are primitive and q^n/q-completely normal for such extensions, see Theorems 5.4 and 5.5. In Sect. 6 we establish an asymptotic result for (n_1, n_2)-partially completely basic extensions to possess the MM property (see Theorem 6.4). In Sect. 7 we explore the computational aspects of our work. In particular, we describe an algorithm that takes advantage of our theoretical arguments to establish the MM property for (n_1, n_2)-partially completely basic extensions, for fixed n_1, see Subsect. 7.1. Then, in Subsect. 7.2 we use the algorithm to settle the $n_1 = 2$ and $n_1 = 3$ cases, see Theorem 7.2, and comment on the $n_1 = 4$ case. We conclude this work with a small discussion about future additions or improvements to this line of research in Sect. 8.

2. Towards the Primitive Completely Normal Basis Theorem

We will split our exhibition of previous results depending on the means that workers that attacked Conjecture 1.4 have adopted in the past, rather than a strictly chronological order. The first and most obvious method is direct verification with the help of computers. This is in fact the method that Morgan and Mullen [27] used in order to support Conjecture 1.4.

Theorem 2.1 (Morgan-Mullen)**.** *Suppose that $q \leq 97$ and $q^n < 10^{50}$. Then $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property.*

Later still, with the help of more modern equipment, advanced computational methods and theoretical arguments, Hachenberger and Hackenberg [21] extended the original Morgan-Mullen verifications as follows.

Theorem 2.2 (Hachenberger-Hackenberg)**.** *Suppose that*

(1) $n \leq 202$ or
(2) $q < 10^4$ and $q^n < 10^{80}$.

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

However, most of the advances towards establishing Conjecture 1.4 have been achieved with theoretical means. A first observation is that all completely normal elements are, by definition, normal, but the inverse is true only for certain finite field extensions. So, the following definition is essential.

Definition 2.3. 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, Conjecture 1.4 is directly implied by Theorem 1.2, thus, if $\mathbb{F}_{q^n}/\mathbb{F}_q$ is completely basic, it possesses the MM property. Clearly, if r is prime, $\mathbb{F}_{q^r}/\mathbb{F}_q$ is completely basic, but this is not the only family of completely basic extensions. In fact, we have the following complete characterization of this family by Blessenohl and Johnsen [7].

Theorem 2.4 (Blessenohl-Johnsen)**.** *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, see [18, Example 5.4.19], 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 $p = \operatorname{char} \mathbb{F}_q$.

Another family that is of interest for us is the following.

Definition 2.5. 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 clearly regular extensions. But, see [18, Example 5.4.47], 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) $D \subseteq \{7, 11, 13, 17, 19, 31, 41, 47, 49, 61, 73, 97, 101, 107, 109, 139, 151, 163, 167, 173, 179, 181, 193\}$.

Also, $\mathbb{F}_{q^n}/\mathbb{F}_q$ is regular if n is a power of a Carmichael number. It has been established that regular extensions possess the MM property.

Theorem 2.6 (Hachenberger)**.** *Regular extensions possess the MM property.*

The above was initially partially established by Hachenberger [16, 17] and, subsequently, fully established by the same author [20]. Furthermore, we note that, the establishment of Theorem 2.6 required deep understanding of the underlying module structure of finite fields and combines algebraic and character sum methods.

Last but not least, some efforts have been made with the adoption of combinatorial and character sum methods. Namely, in 2016, Hachenberger [19] used elementary combinatorial arguments in order to obtain the following.

Theorem 2.7 (Hachenberger)**.** *Suppose that*

(1) $q \geq n^{7/2}$ *and* $n \geq 7$*, or,*
(2) $q \geq n^3$ *and* $n \geq 37$*,*

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

It is worth mentioning that the results of [19] depend on an estimate of the number of q^n/q-completely normal elements, that derives from combinatorial arguments and does not depend on the prime decomposition of n and its relation with q.

Inspired by this work, the authors adjusted the character sum method accordingly for this setting. More precisely, in [12, 13], the main term of the authors' application of the method was manipulated in a way that it equaled the number of q^n/q-completely normal elements. This lead to the following improvement of Theorem 2.7 in [13].

Theorem 2.8 (Garefalakis-Kapetanakis)**.** *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.*

Soon after, with more attention given to technical details, the above was further improved in [12] by the same authors.

Theorem 2.9 (Garefalakis-Kapetanakis)**.** *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.

Here, we remark that, in this section, emphasis was given to the end results regarding the existence of primitive and q^n/q-completely normal elements, which is also the object of this work. However, in addition to this question, there are many interesting related questions, such as the distribution of these elements. We refer the interested reader to the references of this work and in particular to related textbooks [15, 18, 22] and the references therein.

3. Preliminaries

As we mentioned in Sect. 1, in this work we will take advantage of the character sum method. In this method, characters and their sums play a crucial role in characterizing elements of finite fields with the desired properties and in estimating the number of elements that combine all the desired properties.

Definition 3.1. Let $\mathfrak{G}$ be a finite abelian group. A *character* of $\mathfrak{G}$ is a group homomorphism $\mathfrak{G} \to \mathbb{C}^*$. The characters of $\mathfrak{G}$ form a group under multiplication, which is isomorphic to $\mathfrak{G}$. This group is called the *dual* of $\mathfrak{G}$ and denoted by $\widehat{\mathfrak{G}}$. Furthermore, the character $\chi_0 : \mathfrak{G} \to \mathbb{C}^*$, where $\chi_0(g) = 1$ for all $g \in \mathfrak{G}$, is called the *trivial character* of $\mathfrak{G}$. Finally, by $\bar{\chi}$ we denote the inverse of χ and observe that, for every $g \in \mathfrak{G}$ and $\chi \in \widehat{\mathfrak{G}}$, $|\chi(g)| = 1$.

The finite field $\mathbb{F}_{q^n}$ is associated with its multiplicative and its additive group. From now on, we will call the characters of $\mathbb{F}_{q^n}^*$ *multiplicative characters* and the characters of $\mathbb{F}_{q^n}$ *additive characters*. Furthermore, we will denote by χ_0 and ψ_0 the trivial multiplicative and additive character respectively and we will extend the multiplicative characters to zero with the rule

$$\chi(0) := \begin{cases} 0, & \text{if } \chi \in \widehat{\mathbb{F}_{q^n}^*} \setminus \{\chi_0\}, \\ 1, & \text{if } \chi = \chi_0. \end{cases}$$

A *character sum* is a sum that involves characters. In this work we will use the following incomplete character sum estimate.

Theorem 3.2. *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*

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

The above follows from the main result of [11]. However, an alternative simplified proof was established recently, see [26].

The additive and the multiplicative groups of $\mathbb{F}_{q^n}$ can also be seen as modules. In particular $\mathbb{F}_{q^n}^*$ (the multiplicative group) can be seen as a $\mathbb{Z}$-module under the rule $r \circ a = a^r$, where $r \in \mathbb{Z}$ and $a \in \mathbb{F}_{q^n}$. The fact that $\mathbb{F}_{q^n}$ contains primitive elements implies that this module is cyclic.

By using Vinogradov's formula for generators of cyclic modules over Euclidean domains, it follows that the characteristic function for $a \in \mathbb{F}_{q^n}$ being primitive is

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

where $q' = q^n - 1$, $\theta(r) = \phi(r)/r$, μ is the Möbius function, ϕ is the Euler function and the *order* of a multiplicative character is defined as its multiplicative order in $\widehat{\mathbb{F}^*_{q^n}}$. Also, we stress that $\mathbb{F}^*_{q^n}$ contains $\phi(q')$ primitive elements.

Regarding the additive group, for any $d \mid n$, $\mathbb{F}_{q^d}$ can be seen as an $\mathbb{F}_q[x]$-module under the rule $f \circ a = \mathfrak{f}(a)$, where $\mathfrak{f}$ stands for the *q-associate* of $f \in \mathbb{F}_q[x]$, that is, for $f = \sum_{i=0}^k f_i x^i$, then $\mathfrak{f} = \sum_{i=0}^k f_i x^{q^i}$.

Theorem 1.1 implies that for all $d \mid n$, the corresponding module is cyclic. Similarly, the characteristic function for $a \in \mathbb{F}_{q^d}$ being q^d/q-normal is

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

where $F'_d = x^d - 1 \in \mathbb{F}_q[x]$, $\theta_q(f) := \phi_q(f)/q^{\deg(f)}$, μ_q and ϕ_q are the Möbius and Euler functions in $\mathbb{F}_q[x]$, respectively, the first sum extends over the monic divisors of F'_d in $\mathbb{F}_q[x]$ and the second sum runs through the additive characters of $\mathbb{F}_q$ of q-order f. The *q-order* of some $\psi \in \widehat{\mathbb{F}_{q^d}}$, denoted by $\mathrm{ord}(\psi)$, is defined as the lowest degree monic polynomial $g \in \mathbb{F}_q[x]$ such that $\psi(g \circ a) = 1$ for all $a \in \mathbb{F}_{q^d}$. We note that the q-order of an additive character of $\mathbb{F}_{q^d}$ divides F'_d and that $\mathbb{F}_{q^d}$ contains $\phi_q(F'_d)$ elements that are q^d/q-normal.

Last but not least, it follows immediately from the orthogonality relations that the characteristic function for some $a \in \mathbb{F}_q$ to be nonzero is

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

4. A construction of completely normal elements

Before we proceed, we start with the following definition.

Definition 4.1. Take some finite field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ and some $a \in \mathbb{F}_{q^n}$. The *set of translates* of a is defined as

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

In this section we will modify the following proposition, that plays an important role in the original proof of Theorem 1.3.

Proposition 4.2 ([14, Claim (3.1.4)])**.** *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.*

Towards this end, we will need the following auxiliary lemmas and the notion of the trace function. The *q^n/q-trace* is the function

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

Lemma 4.3 ([14, Claim (3.1.2)]). *Let n_1, n_2 be relatively prime and assume that some $a \in \mathbb{F}_{q^{n_1}}$ is q^{n_1}/q-normal. Then a is $q^{n_1 n_2}/q^{n_2}$-normal (as an element of $\mathbb{F}_{q^{n_1 n_2}}$).*

Lemma 4.4 ([14, Claim (3.1.3)]). *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 $\mathbb{F}_{q^{n_i}}/\mathbb{F}_q$-normal for $i = 1, 2$, then $a_1 a_2$ is q^n/q-normal.*

Lemma 4.5 ([25, Lemma 3.1]). *Suppose $a \in \mathbb{F}_{q^n}$ is q^n/q-normal and $d \mid n$. Then $\mathrm{Tr}_{q^n/q^d}(a)$ is q^d/q-normal. In particular, $\mathrm{Tr}_{q^n/q^d}(a) \neq 0$.*

Lemma 4.6. *Suppose $a \in \mathbb{F}_{q^n}$ is q^n/q-normal. Choose some $\lambda_i \in \mathbb{F}_q$ for $i = 0, \ldots, n-1$. Then $\sum_{i=0}^{n-1} \lambda_i a^{q^i} \in \mathbb{F}_q$ if and only if all of the λ_i's are equal.*

Proof. Since a is q^n/q-normal, the map

$$\mathbb{F}_q^n \to \mathbb{F}_{q^n},\ (\lambda_0, \ldots, \lambda_{n-1}) \mapsto \sum_{i=0}^{n-1} \lambda_i a^{q^i}$$

is a bijection. Thus, it suffices to prove the inverse claim. For the inverse, observe that, if $\lambda_i = \lambda$ for all $i = 0, \ldots, n-1$, then

$$\sum_{i=0}^{n-1} \lambda_i a^{q^i} = \lambda \,\mathrm{Tr}_{q^n/q}(a) \in \mathbb{F}_q,$$

while Lemma 4.5 yields that $\mathrm{Tr}_{q^n/q}(a) \neq 0$. □

We prove the following lemma.

Lemma 4.7. *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 $\mathbb{F}_q$.

Proof. Take

$$\sum_{i=0}^{n-1} \lambda_i (a + c)^{q^i} = 0,$$

for some $\lambda_i \in \mathbb{F}_q$, for $i = 0, \ldots, n-1$. Recall that $a + c$ is q^n/q-normal if and only if the above holds only for $\lambda_i = 0$ for all $i = 0, \ldots, n-1$. Now, the latter is equivalent to

$$\sum_{i=0}^{n-1} \lambda_i a^{q^i} = -c \sum_{i=0}^{n-1} \lambda_i.$$

Further, Lemma 4.6 entails that $\lambda_i = \lambda$ for every $i = 0, \ldots, n-1$, for some $\lambda \in \mathbb{F}_q$. Finally, the last equation becomes

$$\lambda \left(\mathrm{Tr}_{q^n/q}(a) + cn \right) = 0,$$

which implies the desired result, with Lemma 4.5 in mind. □

Proposition 4.8. *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) $\mathrm{Tr}_{q^n/q}(a_1a_2 + c) \neq 0$.
(3) $c \neq -\mathrm{Tr}_{q^n/q}(a_1a_2) \cdot n^{-1}$, *where* n *is seen as an element of* $\mathbb{F}_q$.

Proof. Recall that a_1a_2 is q^n/q-completely normal by Proposition 4.2. Next, fix some $c \in \mathbb{F}_q$. Clearly, if $c = -n\,\mathrm{Tr}_{q^n/q}(a_1a_2)$ (in the case $p \nmid n$), then, by Lemma 4.7, a_1a_2+c cannot be q^n/q-completely normal. So, from now on, we assume that either $p \mid n$, or $\mathrm{Tr}_{q^n/q}(a_1a_2 + c) \neq 0$ if $p \nmid n$.

Now, take some $d \mid n$. If $p \mid (n/d)$, Lemma 4.7 yields that $a_1a_2 + c$ is q^n/q^d-normal. So, we may focus on the case $p \nmid (n/d)$.

In this case, Lemma 4.7 implies that $a_1a_2 + c$ is q^n/q^d-normal if $\mathrm{Tr}_{q^n/q^d}(a_1a_2 + c) \neq 0$. However, if this is not the case, then

$$\mathrm{Tr}_{q^n/q}(a_1a_2 + c) = \mathrm{Tr}_{q^d/q}\left(\mathrm{Tr}_{q^n/q^d}(a_1a_2 + c)\right) = \mathrm{Tr}_{q^d/q}(0) = 0,$$

a contradiction. □

Remark 4.9. The proof of Proposition 4.8 uses essentially the same arguments with that of Proposition 4.2, only with Lemma 4.7 in mind, instead of Lemma 4.4.

Remark 4.10. For the purposes of this work, we are interested in finding q^n/q-completely normal elements, that have multiplicative order $q^n - 1$. However, the element a_1a_2 that is obtained from Lemma 4.4 has order at most $(q^{n_1} - 1)(q^{n_2} - 1)/(q - 1)$. In other words the construction of completely normal elements in the original proof of Theorem 1.3 never yields primitive elements. In our opinion this is a key factor for the persistence of Conjecture 1.4.

As a corollary of Proposition 4.8, we obtain the main result of this section.

Theorem 4.11. *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* $i = 1, \ldots, k$ *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. Proposition 4.2, used inductively, ensures that $a_1 \cdots a_{k-1}$ is $q^{p_1^{n_1} \cdots p_{k-1}^{n_{k-1}}}/q$-completely normal. Now, apply Proposition 4.8. □

Remark 4.12. Another way to attack Conjecture 1.4 emerges from Theorem 4.11. Namely, Theorem 4.11 links the MM property with the translate property (and its strong version). The corresponding definitions and the details of this interesting connection are explained briefly in Appendix A. However, as explained in more detail in Appendix A, this connection is of small practical interest for the purposes of this work.

5. Main condition

Before we proceed further, we introduce the following family of finite field extensions that will be of interest for us.

Definition 5.1. Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be an extension of finite fields, such that

(1) $n = n_1n_2$, 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*.

Remark 5.2. With the discussion on completely basic extensions in mind, see Sect. 2, we observe that the family of partially completely basic extensions is rather large. In particular, if $n = r_1^{n_1} \cdots r_k^{n_k}$ is the prime factorization of n, if the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ 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, while it is clear a fixed extension may be (n_1, n_2)-partially completely basic for multiple parameters n_1 and n_2.

We will also need the following technical definition.

Definition 5.3. Let X be a positive integer or a polynomial in $\mathbb{F}_q[x]$. Then $W(X)$ denotes the number of squarefree divisors or the number of squarefree monic divisors of X, respectively.

We are now in position to prove the main results of this section.

Theorem 5.4. *Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be an (n_1, n_2)-partially completely basic extension, such that $p \nmid n$ and*

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

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

Proof. Theorem 1.3 ensures the existence of some $a \in \mathbb{F}_{q^{n_1}}$ that is q^{n_1}/q-completely normal. The fact that $\mathbb{F}_{q^{n_2}}/\mathbb{F}_q$ is completely basic and Proposition 4.8 imply that, 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. In particular, $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the MM property.

From the characteristic functions of the corresponding properties, as presented in Sect. 3, it follows that the number of $b \in \mathbb{F}_{q^{n_2}}$ that combine the desired properties as above is

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

So, for our purposes, it suffices to show that $\mathcal{N} \neq 0$. We replace ω and Ω_{n_2} with their expressions from Sect. 3 and obtain:

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

$$= S_1 + S_2, \tag{1}$$

where S_1 is the part that corresponds to $d = 1$ and S_2 the one that corresponds to $d \neq 1$.

First we focus on S_1. We have that

$$S_1 = \sum_{b \in \mathbb{F}_{q^{n_2}}} \Omega_{n_2}(b) \sum_{c \in \mathbb{F}_q^*} z\left(\mathrm{Tr}_{q^n/q}(ab + c)\right) = (q-2)\phi_q(F'_{n_2}). \tag{2}$$

Then, we turn our attention to S_2. We have that

$$S_2 = \frac{\theta_q(F'_{n_2})}{q} \sum_{\substack{d|q' \\ d\neq 1}} \sum_{f|F'_{n_2}} \frac{\mu(d)\mu_q(f)}{\phi(d)\phi_q(f)} \sum_{\substack{\chi\in\widehat{\mathbb{F}^*_{q^n}} \\ \mathrm{ord}(\chi)=d}} \sum_{\substack{\psi\in\widehat{\mathbb{F}_{q^{n_2}}} \\ \mathrm{ord}(\psi)=f}} \sum_{\eta\in\widehat{\mathbb{F}_q}} \sum_{c\in\mathbb{F}^*_q} \mathcal{C}(\chi,\psi,\eta,c),$$

where

$$\mathcal{C}(\chi,\psi,\eta,c) := \sum_{b\in\mathbb{F}_{q^{n_2}}} \chi(ab+c)\psi(b)\left(1-\eta(\mathrm{Tr}_{q^n/q}(ab+c))\right).$$

It follows that

$$|\mathcal{C}(\chi,\psi,\eta,c)| \leq$$

$$|\chi(a)| \cdot \left|\sum_{b\in\mathbb{F}_{q^{n_2}}} \chi(a^{-1}c+b)\psi(b)\right| + \left|\chi(a)\eta\left(\mathrm{Tr}_{q^n/q}(c)\right)\right| \cdot \left|\sum_{b\in\mathbb{F}_{q^{n_2}}} \chi(a^{-1}c+b)\rho(b)\right|,$$

where $\rho(b) = \psi(b)\eta(\mathrm{Tr}_{q^n/n}(ab))$ is an additive character of $\mathbb{F}_{q^{n_2}}$. Further, observe that, since a is q^{n_1}/q-normal, Lemma 4.3 entails that it is also q^n/q^{n_2}-normal, thus $\mathbb{F}_{q^{n_2}}(a) = \mathbb{F}_{q^n}$, i.e., $\mathbb{F}_{q^{n_2}}(a^{-1}c) = \mathbb{F}_{q^n}$. It follows from Theorem 3.2 (applied on the extension $\mathbb{F}_{q^n}/\mathbb{F}_{q^{n_2}}$) that, since χ is not trivial, $|\mathcal{C}(\chi,\psi,\eta,c)| \leq 2n_1 q^{n_2/2}$. Furthermore, recall that there are exactly $\phi(d)$ (resp. $\phi_q(f)$) multiplicative (resp. additive) characters of order d (resp. q-order f). It follows that

$$\begin{aligned} |S_2| &\leq \frac{\theta_q(F'_{n_2})}{q}(W(q')-1)W(F'_{n_2})q(q-1)2n_1 q^{n_2/2} \\ &< \frac{\phi_q(F'_{n_2})}{q^{n_2/2}} W(q')W(F'_{n_2})(q-1)2n_1 \end{aligned} \tag{3}$$

We combine Eqs. (1), (2) and (3) and obtain that $\mathcal{N} \neq 0$ if

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

from where the result follows. □

For the case $p \mid n$ we have the following improved version of Theorem 5.4.

Theorem 5.5. *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*

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

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

Proof. If $p \mid n$, the requirement $\mathrm{Tr}_{q^n/q}(ab+c) \neq 0$ is satisfied for all $c \in \mathbb{F}^*_q$. This means that the term $q-2$ that appears in Eq. (2) can be replaced by $q-1$ and that the function z can be skipped altogether. All the other arguments remain identical as the ones in the proof of Theorem 5.4 □

Remark 5.6. Note that Theorem 5.4 is ineffective in the case $q = 2$ as its condition can never hold. In fact, our method fails in the case $q = 2$ and n odd. The underlying reason is that, under the assumptions of Theorem 4.11, the set where we are looking for primitive completely normal elements is the singleton $\{ab\}$, but ab, as already mentioned in Remark 4.10, is never primitive. The case $q = 2$ and n even can be, however, treated by Theorem 5.5.

Remark 5.7. In the literature one can find several powerful strategies to weaken the conditions of Theorems 5.4 and 5.5, such as the prime sieve [9], the modified prime sieve [5] or the hybrid bound [4]. However, in this work, we choose to not use any of these in an attempt to keep the text as simple as possible focus on the novel aspects of this work.

6. An asymptotic result

In this section, we will use Theorems 5.4 and 5.5, in order to obtain an asymptotic condition for an (n_1, n_2)-partially completely basic extension to possess the MM property. We will need the following classic result.

Lemma 6.1 ([2, p. 296])**.** *For every $\delta > 0$, $W(n) = o(n^\delta)$, where o signifies the little-o notation.*

We will also need the following lemmas.

Lemma 6.2 ([23, Lemma 2.9])**.** *Let q be a prime power and n a positive integer. Then, we have $W(F'_n) \leq 2^{\frac{1}{2}(n+\gcd(n,q-1))}$. In particular, $W(F'_n) \leq 2^n$, while the equality holds if and only if $n \mid q-1$. Furthermore, if $n \nmid q-1$, $W(F'_n) \leq 2^{3n/4}$.*

For small values of q, we will use the following.

Lemma 6.3 ([1, Lemma 3.7])**.** *Let q be a prime power and n a positive integer. Then, $W(F'_n) \leq 2^{\frac{n+a}{b}}$ for some $a, b \in \mathbb{Z}$. In particular, for $q \geq 29$, we have $(a, b) = (0, 1)$; for $7 \leq q \leq 27$, we have $(a, b) = (q-1, 2)$ and for $q \leq 5$ we have the following values for a, b:*

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

We are now in position to prove the main result of this section.

Theorem 6.4. *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 $q = 2$.*

Proof. First we assume $q > 2$. Fix some $n_1 \geq 2$. Theorem 5.4, along with Lemmas 6.1 and 6.2, implies that an (n_1, n_2)-partially completely basic extension possesses the MM property, given that

$$\left(\frac{\sqrt{q}}{2}\right)^{n_2} > 4n_1 \cdot o(q^{n_2/4}).$$

This implies the result for $q > 4$. For $q = 3$ and 4, Lemma 6.3 yields $W(F'_{n_2}) \leq 2^{\frac{n_2+20}{3}}$ and the above condition is replaced by

$$\left(\frac{\sqrt{q}}{\sqrt[3]{2}}\right)^{n_2} > 2^{26/3} n_1 \cdot o(q^{n_2/4}),$$

which settles the cases $q = 3$ and 4. Finally, for $q = 2$, we are confined to n even, thus we may use Theorem 5.5 instead. Now, Lemma 6.3 entails $W(F'_{n_2}) \leq 2^{\frac{n_2+14}{5}}$ and the above condition is replaced by

$$2^{3n_2/10} > 2^{14/5} n_1 \cdot o(2^{n_2/5}),$$

which completes our proof. □

7. Computational aspects

In this section we explore the computational aspects of Theorem 5.4. First, with the condition of Theorem 5.4 in mind, we see that a concrete expression of Lemma 6.1 is needed.

Lemma 7.1 ([9, Lemma 3.7]). *For any $\alpha \in \mathbb{N}$ and a positive real number ν, $W(\alpha) \leq \mathcal{C}_\nu^{(\alpha)} \cdot \alpha^{1/\nu}$, 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. We note that, in this section, 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, $\mathcal{C}_\nu^{(\alpha)} \leq \mathcal{C}_\nu$ for all $\alpha \in \mathbb{Z}$.
(2) For any $1 \leq j \leq s$, $\mathcal{C}_\nu^{[p_j]} := \mathcal{C}_\nu p_j^{1/\nu}/2$. Clearly, $\mathcal{C}_\nu^{(\alpha)} \leq \mathcal{C}_\nu^{[p_j]}$ for all $\alpha \in \mathbb{Z}$ with $p_j \nmid \alpha$.

Furthermore, the number $\mathcal{C}_\nu^{(\alpha)}$ in the statement of Lemma 7.1 can be freely replaced by either $\mathcal{C}_\nu$, or, if the prime $r \leq 2^\nu$ does not divide α, by $\mathcal{C}_\nu^{[r]}$.

7.1. **An algorithm for the MM property.** Now, we present an algorithm, that takes n_1 as its input and aims to establish that all (n_1, n_2)-partially completely basic extensions possess the MM property is given. The algorithm is comprised by the following steps:

Step 1 Set $n_{\min}$ as the minimum value of n_2 that is not covered by Theorem 2.2 for the given n_1.

Step 2 For $n_2 = n_{\min}$, find $q_{\max}$, the minimum prime power q that satisfies the condition of Theorem 5.4, where the numbers $W(F'_{n_2})$ and $W(q')$ are estimated by Lemmas 6.2 and 7.1, respectively. We note that, with the notation of Lemma 7.1, we take $\nu = 4n_1$ and we bound the constant $\mathcal{C}_{4n_1}^{(q^{n_1 n_2}-1)}$ by the generic bound $\mathcal{C}_{4n_1}$. At this point we are left with a finite number of prime powers q that are not covered.

Step 3 For each prime power $3 \leq q < q_{\max}$, find the maximum value of n_2, $n_{\max}^{(q)}$, not satisfying the condition of the previous step. Note that in this step, every q is treated as fixed, the sharper estimate $\mathcal{C}_{4n_1}^{[p]}$ (where p stands for the unique prime divisor of q) is employed over the generic $\mathcal{C}_{4n_1}$ and n_2 is treated as a variable. Upon completion, for each prime power $3 \leq q < q_{\max}$, we are left with a range $n_{\min} \leq n_2 \leq n_{\max}^{(q)}$ of yet unsettled cases.[1]

Step 4 For each prime power $3 \leq q \leq q_{\max}$ and integers $n_{\min} \leq n_2 \leq n_{\max}^{(q)}$, we explicitly identify which values of n_2 are such that

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

The first two conditions ensure that the extension $\mathbb{F}_{q^{n_1 n_2}}\mathbb{F}_q$ is (n_1, n_2)-partially completely basic and the third one that the extension is not already covered by Theorem 2.2. At this point, we are left with a finite list of pairs (q, n_2) that correspond to the (n_1, n_2)-partially completely basic extensions not already covered.

[1]Here, observe that since the sharper $\mathcal{C}_{4n_1}^{[p]}$ is favored over the generic $\mathcal{C}_{4n_1}$ of the previous step, it is possible that $n_{\max}^{(q)} < n_{\min}$; this means that the corresponding prime power q is settled.

Step 5 For each of these pairs we check the condition of Theorem 5.4, where $W(F'_{n_2})$ is explicitly computed and $W(q')$ is estimated by Lemma 7.1, where, under the notation Lemma 7.1, $\nu = 4n_1$ and the constant $\mathcal{C}_{4n_1}^{(q^{n_1 n_2}-1)}$ is explicitly computed. Remove from the list of possible exceptions the pairs that pass this test.

Step 6 For the remaining pairs we check the condition of Theorem 5.4, where $W(F'_{n_2})$ and $W(q')$ are both explicitly computed. Remove from the list of possible exceptions the pairs that pass this test.

Step 7 If the list of possible exceptions remain nonempty at this point, return **FAIL**.

Step 8 Now, we move on to the case $q = 2$. We repeat Steps 3–6 with the difference that Theorem 5.5 is used over Theorem 5.4 and that, in Step 4, we additionally demand n_2 to be even.

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

The rest of this section is dedicated into applying this algorithm in an attempt to establish the MM property for (n_1, n_2)-partially completely basic extensions for small values of n_1.

7.2. **Concrete results.** We successfully applied the algorithm of Subsect. 7.1 for $n_1 = 2$ and $n_1 = 3$, while we obtained partial results for $n_1 = 4$. Namely, we establish the following theorem.

Theorem 7.2. *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,*
- *$n_2 \geq n_1^6 = 4096$.*

For our calculations we used the SageMath system, running on a modern laptop. In the following subsections we present the most important details of our calculations.

7.2.1. *The cases $n_1 = 2$ and $n_1 = 3$.* The most essential information of our implementation for the cases $n_1 = 2$ and $n_1 = 3$ is summarized in Table 1.

				# of pairs after Step						
n_1	$n_{\min}$	$\mathcal{C}_{4n_1}$	$q_{\max}$	4	5	6	8.4	8.5	8.6	time
2	102	4514.6265	11	15	0	0	0	0	0	∼1 sec.
3	67	$1.057 \cdot 10^{24}$	487	3011	0	0	111	0	0	∼30 sec.

Table 1. Summary of the implementation of the algorithm of Subsect. 7.1 for $n_1 = 2$ and $n_1 = 3$.

We note that the zeros appearing in the columns under Steps 6, and 8.6 show that the application was successful. The zeros in the columns under Steps 5, and 8.5 show that we never had to resort to computing $W(q')$, which is an expensive computation, as the computer should first factor $q^{n_1 n_2} - 1$ into primes. Furthermore,

the zero in the entry that corresponds to $n_1 = 2$ and Step 8.4 is the result of the fact that, in this case, we expect n_2 to be both odd (as it has to be relatively prime to $n_1 = 2$) and even (as it has to be divided by $p = 2$).

Next, in Table 2, we present the numbers appearing in Step 3 for $n_1 = 2$ and, in Table 3, we present the numbers appearing in Step 3 for $n_1 = 3$. We note that in Table 2, the case $q = 2$ is missing, as, we already explained, this case is irrelevant and, in Table 3, the entries that correspond to $q = 2$ derive from Step 8.3.

q	$n_{\max}^{(q)}$	$\mathcal{C}_{4n_1}^{[p]}$	q	$n_{\max}^{(q)}$	$\mathcal{C}_{4n_1}^{[p]}$	q	$n_{\max}^{(q)}$	$\mathcal{C}_{4n_1}^{[p]}$
3	133	2589.5959	4	108	2461.6176	5	81	2760.3433
7	84	2878.9167	8	68	2461.6176	9	60	2589.5959

TABLE 2. Prime powers $3 \leq q < q_{\max}$, the corresponding $n_{\max}^{(q)}$ and the corresponding value of $\mathcal{C}_{4n_1}^{[p]}$ for $n_1 = 2$.

q	$n_{\max}^{(q)}$	$\mathcal{C}_{4n_1}^{[p]}$	q	$n_{\max}^{(q)}$	$\mathcal{C}_{4n_1}^{[p]}$	q	$n_{\max}^{(q)}$	$\mathcal{C}_{4n_1}^{[p]}$
2	1666	$5.6008 \cdot 10^{23}$	3	599	$5.7933 \cdot 10^{23}$	4	517	$5.6008 \cdot 10^{23}$
5	357	$6.0453 \cdot 10^{23}$	7	421	$6.2172 \cdot 10^{23}$	8	341	$5.6008 \cdot 10^{23}$
9	294	$5.7933 \cdot 10^{23}$	11	238	$6.4558 \cdot 10^{23}$	13	207	$6.5463 \cdot 10^{23}$
16	179	$5.6008 \cdot 10^{23}$	17	173	$6.6943 \cdot 10^{23}$	19	162	$6.7566 \cdot 10^{23}$
23	148	$6.8651 \cdot 10^{23}$	25	142	$6.0453 \cdot 10^{23}$	27	138	$5.7933 \cdot 10^{23}$
29	382	$6.9990 \cdot 10^{23}$	31	344	$7.0380 \cdot 10^{23}$	32	327	$5.6008 \cdot 10^{23}$
37	271	$7.1425 \cdot 10^{23}$	41	242	$7.2039 \cdot 10^{23}$	43	230	$7.2325 \cdot 10^{23}$
47	211	$7.2863 \cdot 10^{23}$	49	203	$6.2172 \cdot 10^{23}$	53	190	$7.3597 \cdot 10^{23}$
59	175	$7.4257 \cdot 10^{23}$	61	170	$7.4464 \cdot 10^{23}$	64	163	$5.6008 \cdot 10^{23}$
67	159	$7.5048 \cdot 10^{23}$	71	153	$7.5412 \cdot 10^{23}$	73	150	$7.5587 \cdot 10^{23}$
79	143	$7.6086 \cdot 10^{23}$	81	140	$5.7933 \cdot 10^{23}$	83	139	$7.6400 \cdot 10^{23}$
89	133	$7.6845 \cdot 10^{23}$	97	127	$7.7399 \cdot 10^{23}$	101	124	$7.7660 \cdot 10^{23}$
103	123	$7.7787 \cdot 10^{23}$	107	120	$7.8034 \cdot 10^{23}$	109	119	$7.8155 \cdot 10^{23}$
113	117	$7.8390 \cdot 10^{23}$	121	112	$6.4558 \cdot 10^{23}$	125	111	$6.0453 \cdot 10^{23}$
127	110	$7.9156 \cdot 10^{23}$	128	109	$5.6008 \cdot 10^{23}$	131	109	$7.9361 \cdot 10^{23}$
137	106	$7.9658 \cdot 10^{23}$	139	106	$7.9754 \cdot 10^{23}$	149	102	$8.0217 \cdot 10^{23}$
151	102	$8.0306 \cdot 10^{23}$	157	100	$8.0568 \cdot 10^{23}$	163	98	$8.0820 \cdot 10^{23}$
167	97	$8.0983 \cdot 10^{23}$	169	97	$6.5463 \cdot 10^{23}$	173	96	$8.1222 \cdot 10^{23}$
179	95	$8.1453 \cdot 10^{23}$	181	94	$8.1528 \cdot 10^{23}$	191	92	$8.1894 \cdot 10^{23}$
193	92	$8.1966 \cdot 10^{23}$	197	91	$8.2106 \cdot 10^{23}$	199	91	$8.2175 \cdot 10^{23}$
211	89	$8.2577 \cdot 10^{23}$	223	87	$8.2958 \cdot 10^{23}$	227	86	$8.3081 \cdot 10^{23}$
229	86	$8.3142 \cdot 10^{23}$	233	85	$8.3262 \cdot 10^{23}$	239	85	$8.3439 \cdot 10^{23}$
241	84	$8.3497 \cdot 10^{23}$	243	84	$5.7933 \cdot 10^{23}$	251	83	$8.3780 \cdot 10^{23}$
256	82	$5.6008 \cdot 10^{23}$	257	82	$8.3945 \cdot 10^{23}$	263	82	$8.4107 \cdot 10^{23}$
269	81	$8.4265 \cdot 10^{23}$	271	81	$8.4317 \cdot 10^{23}$	277	80	$8.4471 \cdot 10^{23}$
281	80	$8.4572 \cdot 10^{23}$	283	80	$8.4622 \cdot 10^{23}$	289	79	$6.6943 \cdot 10^{23}$
293	79	$8.4867 \cdot 10^{23}$	307	78	$8.5198 \cdot 10^{23}$	311	77	$8.5290 \cdot 10^{23}$
313	77	$8.5336 \cdot 10^{23}$	317	77	$8.5426 \cdot 10^{23}$	331	76	$8.5734 \cdot 10^{23}$
337	75	$8.5863 \cdot 10^{23}$	343	74	$6.2172 \cdot 10^{23}$	347	74	$8.6072 \cdot 10^{23}$

Continued on next page.

Continued from previous page.

q	$n_{\max}^{(q)}$	$\mathcal{C}_{4n_1}^{[p]}$	q	$n_{\max}^{(q)}$	$\mathcal{C}_{4n_1}^{[p]}$	q	$n_{\max}^{(q)}$	$\mathcal{C}_{4n_1}^{[p]}$
349	74	$8.6113 \cdot 10^{23}$	353	74	$8.6195 \cdot 10^{23}$	359	74	$8.6316 \cdot 10^{23}$
361	73	$6.7566 \cdot 10^{23}$	367	73	$8.6475 \cdot 10^{23}$	373	73	$8.6592 \cdot 10^{23}$
379	72	$8.6707 \cdot 10^{23}$	383	72	$8.6783 \cdot 10^{23}$	389	72	$8.6896 \cdot 10^{23}$
397	71	$8.7043 \cdot 10^{23}$	401	71	$8.7116 \cdot 10^{23}$	409	71	$8.7259 \cdot 10^{23}$
419	70	$8.7435 \cdot 10^{23}$	421	70	$8.7470 \cdot 10^{23}$	431	70	$8.7641 \cdot 10^{23}$
433	70	$8.7675 \cdot 10^{23}$	439	69	$8.7776 \cdot 10^{23}$	443	69	$8.7842 \cdot 10^{23}$
449	69	$8.7941 \cdot 10^{23}$	457	68	$8.8070 \cdot 10^{23}$	461	68	$8.8134 \cdot 10^{23}$
463	68	$8.8166 \cdot 10^{23}$	467	68	$8.8229 \cdot 10^{23}$	479	67	$8.8416 \cdot 10^{23}$

TABLE 3. Prime powers $2 \leq q < q_{\max}$, the corresponding $n_{\max}^{(q)}$ and the corresponding value of $\mathcal{C}_{4n_1}^{[p]}$ for $n_1 = 3$.

7.2.2. *The case* $n_1 = 4$. Finally, we comment on our attempt in implementing the algorithm of Subsect. 7.1 on the $n_1 = 4$ case. The main information of our attempt on the $n_1 = 4$ case is summarized in Table 4.

First, we attempted to run algorithm of Subsect. 7.1 as it is. So, we computed $n_{\min} = 50$, $\mathcal{C}_{4n_1} = 1.9356 \cdot 10^{200}$ and $q_{\max} = 199211272511189639 \approx 2 \cdot 10^{17}$. However, the vast size of $q_{\max}$ makes it clear that even storing the numbers $n_{\max}^{(q)}$ for each $3 \leq q \leq q_{\max}$ is not straightforward and, in fact, our computer crashed during the computation of these numbers.

Then, we confined ourselves (arbitrarily) to $n_{\min} = n_1^{n_1} = 256$. In this case, we computed $q_{\max} = 22271$. This made the completion of Step 3 feasible with a total number of 82148 possible exceptional pairs. However, due to the large size of these numbers, our computer failed to complete Step 4 after having examined about 2200 pairs, with no exceptional pair found until this point.

Our attempt on the $n_{\min} = n_1^5 = 1024$ case faced similar difficulties, although, in this case, we got a significantly smaller $q_{\max} = 27$ and after Step 3 we had 5936 possible exceptional pairs. This time, only around 1650 of them were in fact checked during Step 4, before our computer's crash, without any exceptions up to this point.

Finally, we successfully run the algorithm with the twist that we chose $n_{\min} = n_1^6 = 4096$, where we obtained $q_{\max} = 4$. Also, we note that in this case, we got $n_{\max}^{(2)} = 13385$, $\mathcal{C}_{4n_1}^{(2)} = 1.0106 \cdot 10^{200}$, $n_{\max}^{(3)} = 4605$, and $\mathcal{C}_{4n_1}^{(3)} = 1.0366 \cdot 10^{200}$, respectively. This completes the proof of Theorem 7.2.

8. Discussion

We conclude this work with a short discussion about possible future research directions regarding Conjecture 1.4.

The first one is hinted in Remark 5.7. In particular, we believe that, with considerably additional computational efforts and resources, Theorem 7.2 can potentially be extended to $n_1 = 4$. However, increasing n_1 further should be feasible only after implementing the methods described in Remark 5.7. Our impression is that these methods should be able to increase n_1 even to two-digit numbers.

		# of pairs after Step						
$n_{\min}$	$q_{\max}$	4	5	6	8.4	8.5	8.6	time
50	$\approx 2 \cdot 10^{17}$	-	-	-	-	-	-	-
256	22271	82148	-	-	-	-	-	-
1024	27	5936	-	-	-	-	-	-
4096	4	188	0	0	3317	0	0	$\sim$8 min.

TABLE 4. Summary of the implementation of the algorithm of Subsect. 7.1 for $n_1 = 4$, with various choices of $n_{\min}$.

Also, we stress that in the literature, for example see [3], one can find additional constructions of completely normal elements. Possibly, these constructions can be exploited into establishing the MM property for additional finite fields extensions, or even into completely resolving Conjecture 1.4.

ACKNOWLEDGMENT

We are grateful to D. Hachenberger for pointing out a serious mistake in our original manuscript and his useful comments.

REFERENCES

[1] J. J. R. Aguirre and V. G. L. Neumann, *Existence of primitive 2-normal elements in finite fields*, Finite Fields Appl. **73** (2021), no. 101864, 26 pages.
[2] T. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York Heidelberg Berlin, 1976.
[3] A. Aravena, *Iterated constructions of completely normal polynomials*, Finite Fields Appl. **68** (2020), no. 101755, 12 pages.
[4] G. K. Bagger, *Hybrid bounds for prime divisors*, 2024. arXiv:2412.00010 [math.NT].
[5] 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** (2019), no. 316, 931–947.
[6] D. Blessenohl and K. Johnsen, *Eine verschärfung des satzes von der normalbasis*, J. Algebra **103** (1986), no. 1, 141–159.
[7] ———, *Stabile teilkörper galoisscher erweiterungen und ein problem von C. Faith*, Arch. Math. **56** (1991), 245–253.
[8] L. Carlitz, *Distribution of primitive roots in a finite field*, Quart. J. Math. Oxford Ser. (2) **4** (1953), no. 1, 4–10.
[9] S. D. Cohen and S. Huczynska, *The primitive normal basis theorem – without a computer*, J. London Math. Soc. **67** (2003), no. 1, 41–56.
[10] H. Davenport, *On primitive roots in finite fields*, Quart. J. Math. Oxford **8** (1937), no. 1, 308–312.
[11] L. Fu and D. Wan, *A class of incomplete character sums*, Q. J. Math. **65** (2014), no. 4, 1195–1211.
[12] T. Garefalakis and G. Kapetanakis, *Further results on the Morgan-Mullen conjecture*, Des. Codes Cryptogr. **87** (2019), no. 11, 2639–2654.
[13] ———, *On the existence of primitive completely normal bases of finite fields*, J. Pure Appl. Algebra **223** (2019), no. 3, 909–921.
[14] D. Hachenberger, *On completely free elements in finite fields*, Des. Codes Cryptogr. **4** (1994), 129–143.
[15] ———, *Finite fields: Normal bases and completely free elements*, Kluwer Internat. Ser. Engrg. Comput. Sci., vol. 390, Kluwer Academic Publishers, Boston, MA, 1997.
[16] ———, *Primitive complete normal bases for regular extensions*, Glasgow Math. J. **43** (2001), no. 3, 383–398.

[17] ———, *Primitive complete normal bases: Existence in certain 2-power extensions and lower bounds*, Discrete Math. **310** (2010), no. 22, 3246–3250.
[18] ———, *Completely normal bases*, Handbook of finite fields, 2013, pp. 128–138.
[19] ———, *Asymptotic existence results for primitive completely normal elements in extensions of Galois fields*, Des. Codes Cryptogr. **80** (2016), no. 3, 577–586.
[20] ———, *Primitive complete normal bases for regular extensions: Exceptional cyclotomic modules*, 2019. arXiv:1912.04886 [math.NT].
[21] D. Hachenberger and S. Hackenberg, *Computational results on the existence of primitive complete normal basis generators*, 2019. arXiv:1912.07541 [math.NT].
[22] D. Hachenberger and D. Jungnickel, *Topics in Galois fields*, Algorithms Comp. Math., vol. 29, Springer Nature Switzerland, Cham, 2020.
[23] H. W. Lenstra Jr and R. J. Schoof, *Primitive normal bases for finite fields*, Math. Comp. **48** (1987), no. 177, 217–231.
[24] R. Lidl and H. Niederreiter, *Finite fields*, 2nd ed., Enycl. Math. Appl., vol. 20, Cambridge University Press, Cambridge, 1997.
[25] 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** (2026), no. 102745, 14 pages.
[26] A. C. Mazumder, G. Kapetanakis, S. Kala, and D. K. Basnet, *An estimate for incomplete mixed character sums and applications*, 2025. Submitted for publication.
[27] I. H. Morgan and G. L. Mullen, *Completely normal primitive basis generators of finite fields*, Util. Math. **49** (1996), 21–43.

Appendix A. The translate properties and their connection with the MM property

In this appendix, we dive deeper in the perspective raised in Remark 4.12. We start with defining the properties that are of interest for us.

Definition A.1. 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*.

Furthermore, it is known that, for fixed n, if q is large enough, then the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the translate property.

Theorem A.2 (The 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.*

The above was initially established by Davenport [10] for prime q and extended to its stated form by Carlitz [8]. In a similar fashion, in this work, we prove the strong version as follows.

Theorem A.3 (The Strong Translate Property)**.** *Let n be a positive integer. There exists some $\mathrm{STP}(n) \geq \mathrm{TP}(n)$ such that for every prime power $q > \mathrm{STP}(n)$, the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the strong translate property.*

Proof. We assume that $q > \mathrm{TP}(n)$ and fix some $b \in \mathbb{F}_{q^n}$, such that $\mathbb{F}_q(b) = \mathbb{F}_{q^n}$. We will show that, if q is large enough, $\mathcal{T}_b$ contains two primitive elements. Theorem A.2 implies that, for some $c \in \mathbb{F}_q$, the element $a = b + c$ is primitive, while clearly $\mathcal{T}_b = \mathcal{T}_a$, that is, if the set $\mathcal{T}_a \setminus \{a\}$ contains a primitive element, our proof is complete.

The number of primitive elements within the set $\mathcal{T}_a \setminus \{a\}$ is

$$\begin{aligned}\mathcal{N}_{\mathrm{STP}} &= \sum_{c\in\mathbb{F}_q^*} \omega(a+c)\\ &= \theta(q')\sum_{d\mid q'}\frac{\mu(d)}{\phi(d)} \sum_{\substack{\chi\in\widehat{\mathbb{F}_{q^n}^*}\\ \mathrm{ord}(\chi)=d}} \sum_{c\in\mathbb{F}_q^*}\chi(a+c)\\ &= \theta(q')(S_1+S_2), \qquad (4)\end{aligned}$$

where $q' = q^n - 1$, S_1 is the part of the sum that corresponds to $d = 1$ and S_2 is the remaining sum.

Clearly, $S_1 = q-1$. Further, the fact that, for $d \mid q'$, there are $\phi(d)$ multiplicative characters of order d and Theorem 3.2 yield $|S_2| \le W(q')(nq^{1/2}+1)$, hence, $|S_2| < 2nW(q')\sqrt{q}$.

Now, Lemma 6.1 yields that, for q large enough, $S_1 = q-1 > |S_2|$, which, combined with Eq. (4) implies $\mathcal{N}_{\mathrm{STP}} \neq 0$. The result follows. □

Now, observe that Theorem 4.11 yields that, if $p \mid n$, the translate property implies the MM property, while, in any case, the strong translate property implies the MM property. In other words, we have the following.

Theorem A.4. *Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be a finite field extension, such that, either*

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

(2) $q > \mathrm{STP}(n)$,

then this extension possesses the MM property.

Remark A.5. Despite the fact that Theorem A.4 might appear like a meaningful way to attack Conjecture 1.4, this is, unfortunately, not the case. This is due to the fact that, although little is known about the numbers $\mathrm{TP}(n)$ and only a handful of them are known, these numbers suggest that, in principle, they tend to be significantly larger than n. In particular, see [5] and the references therein, we know that $\mathrm{TP}(2) = 1$, $\mathrm{TP}(3) = 37$, and $43 \le \mathrm{TP}(4) \le 102829$. In other words, Theorems 2.7, 2.8, and 2.9 probably already cover the extensions that are known to possess the (strong) translate property.

Department of Mathematics & Applied Mathematics, University of Crete, Voutes Campus, 70013 Heraklion, Greece

Email address: tgaref@uoc.gr

Department of Mathematics, University of Thessaly, 3rd km Old National Road Lamia-Athens, 35100 Lamia, Greece

Email address: kapetanakis@uth.gr