AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **64(2)** (2016), Pages 289–326

Primitive generators for cyclic vector spaces over a Galois field

Dirk Hachenberger

Institut für Mathematik
Universität Augsburg
86135 Augsburg
Germany
hachenberger@math.uni-augsburg.de

Abstract

For a prime power $q > 1$ and an integer $n \geq 2$ we consider the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ of Galois fields together with a cyclic $\mathbb{F}_q$-vector space endomorphism τ. An element of $\mathbb{F}_{q^n}$ is called a **primitive τ-generator** over $\mathbb{F}_q$ provided it generates the multiplicative group of $\mathbb{F}_{q^n}$, as well as the additive group of $\mathbb{F}_{q^n}$ regarded as an $\mathbb{F}_q[x]$-module with respect to τ. The notion of a primitive τ-generator generalizes the well known concept of a primitive normal basis generator; the latter is just a primitive σ-generator, where σ is the Frobenius automorphism of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

The pair (q, n) as well as the corresponding extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ are called **extensive** provided that for *every* cyclic $\mathbb{F}_q$-vector space endomorphism τ of $\mathbb{F}_{q^n}$ there exists a primitive τ-generator for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Our main result can be summarized as follows. We determine two distinguished (disjoint) sets, $\mathcal{C}$ with 5 pairs (q, n), and $\mathcal{U}$ with 19 pairs, such that no member of $\mathcal{C}$ is extensive, while every pair (q, n) which is *not* contained in the union $\mathcal{C} \cup \mathcal{U}$ is an extensive one. The status whether a pair from $\mathcal{U}$ is extensive or not remains undecided.

The proof is based on various combinatorial techniques: character theory of finite fields, a sieving method, as well as variations of a counting argument which culminate in a promising geometric argument.

1 The main result

Consider a finitely generated vector space E over a field F, say with dimension n, and let τ be an F-endomorphism of E. With respect to τ, the vector space E is turned into a module over the polynomial algebra $F[x]$ by defining

$$f(x) \cdot v := f(\tau)(v) \quad \text{for all } v \in E \text{ and all } f(x) \in F[x].$$

We denote by m_τ and c_τ the minimal and the characteristic polynomial of τ, respectively. The **τ-order** of a vector $v \in E$ is the monic polynomial $g(x) \in F[x]$ of least degree such that $g(x) \cdot v = 0$; it is denoted by $\mathrm{Ord}_\tau(v)$. By definition, m_τ is the least common multiple of all τ-orders $\mathrm{Ord}_\tau(v)$, where $v \in E$. From basic linear algebra (e.g. Lüneburg [16]) it is well known that there always exists a $v \in E$ such that $\mathrm{Ord}_\tau(v) = m_\tau$.

Recall from the Cayley-Hamilton theorem that m_τ is a divisor of c_τ. Equality, $m_\tau = c_\tau$, holds if and only if E is a **cyclic vector space** with respect to τ, which means that there is a $w \in E$ such that $F[x] \cdot w = E$, where $F[x] \cdot w$ is the $F[x]$-submodule of E which is generated by w. In this case, we say that τ is a **cyclic F-endomorphism** of E, and we call every w satisfying $F[x] \cdot w = E$ a **τ-generator** of E. The τ-generators of a cyclic F-endomorphism τ are exactly the elements $w \in E$ which have τ-order equal to m_τ.

In the present work we are interested in the case where the underlying field F is finite. (For the basics on finite fields see Lidl and Niederreiter [15], and Jungnickel [13].) We therefore let $F := \mathbb{F}_q$ be the Galois field with q elements (where $q > 1$ is some prime power). As a vector space of dimension n over F we take the n-dimensional Galois field extension $E := \mathbb{F}_{q^n}$. Assuming that τ is a cyclic F-endomorphism of E we are then interested to establish the existence of a τ-generator of E that is likewise a **primitive** element of E, i.e. a generator of the (cyclic) multiplicative group of E.

Definition 1.1 *Given a cyclic endomorphism τ of $\mathbb{F}_{q^n}/\mathbb{F}_q$, a primitive element of $\mathbb{F}_{q^n}$ that generates $\mathbb{F}_{q^n}$ as $\mathbb{F}_q[x]$-module with respect to τ is called a **primitive τ-generator** of $\mathbb{F}_{q^n}$.* □

For the particular case, where τ is the Frobenius automorphism of E/F (often denoted by σ), a primitive σ-generator is just a **primitive normal bases generator** of E/F; the existence of such an element (for *any* extension E/F) has been established by Lenstra and Schoof (1987) [14].

Already in 1952, Carlitz [1] could prove the existence of a primitive normal basis generator for all but finitely many pairs (q, n), and Davenport [5] settled the existence for all pairs (q, n) with q being a prime number. The basic approach in [1, 5, 14] is to describe the characteristic function of the set of all primitive normal elements in terms of multiplicative and additive characters of finite fields. A complete theoretical solution (for *all* extensions) would not be achieveable without additional skillful ideas together with the 'art' of arranging a proof, where a lot of different situations have to be coped with. In this respect, a main ingredient responsible for the successful attempt of Lenstra and Schoof can be described as the reduction from the order $q^n - 1$ of a primitive element to elements of order at least $(q^n - 1)/(q - 1)\gcd(n, q - 1)$ in combination with normality [14, (1.11–1.15)]; a further important tool is a flexible upper bound for the number of distinct prime divisors of an integer [14, Lemma 2.6].

The key strategy in Cohen and Huczynska's proof of the primitive normal basis theorem [3] is a sieving method, developed by Cohen [2], which leads to improved

estimates involving Gauss sums and which in the meantime has been applied successfully to prove stronger versions of the primitive normal basis theorem, see for instance Cohen and Huczynska [4], and, for a recent survey, Huczynska [12].

Although (as a generator of the Galois group of E/F) the Frobenius automorphism is a very special F-endomorphism, it is apparent that the basic character theoretical approach as well as the sieving method in principle apply to general cyclic vector spaces as well (Sections 3, 4, 9). Next, having no particular cyclic endomorphism τ in mind any more, one is inevitably led to the following definition.

Definition 1.2 *For a prime power $q > 1$ and an integer $n \geq 2$ the field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ as well as the pair (q, n) are **extensive**, provided that for every cyclic endomorphism τ of $\mathbb{F}_{q^n}/\mathbb{F}_q$ there exists a primitive τ-generator of $\mathbb{F}_{q^n}$.* □

In order to formulate our main result (Theorem 1.3), we let $\mathcal{C}$ be the set consisting of the following five pairs:

$$(2,2),\ (3,2),\ (5,2),\ (2,4),\ (2,6).$$

Furthermore, let $\mathcal{U}$ be the set consisting of the following 19 pairs:

$$\begin{array}{l}(2,8),\ (2,10),\ (2,12),\ (2,14),\ (2,15),\ (2,16),\ (2,18),\ (2,20),\ (2,24),\\ (3,8),\ (3,10),\ (3,12),\ (4,6),\ (4,9),\ (4,10),\ (4,12),\ (5,4),\ (7,6),\ (8,8).\end{array}$$

Theorem 1.3 *Let $q > 1$ be a prime power and $n \geq 2$ an integer.*

1. *If $(q, n) \in \mathcal{C}$, then (q, n) **is not** extensive.*
2. *If $(q, n) \notin \mathcal{C} \cup \mathcal{U}$, then (q, n) **is** extensive.*

For the 19 pairs (q, n) from $\mathcal{U}$ the status of being extensive or not could not be decided. We conjecture that from these remaing 19 pairs only the pair $(5, 4)$ is *not* extensive.

At this place we have to mention a recent work of Hsu and Nan [11], which have studied the existence of primitive elements which additionally generate a so-called *finite Carlitz module*. It turns out that their results are covered by our more general notion of extensiveness: taking an element z of the extension field $\mathbb{F}_{q^n}$, the $\mathbb{F}_q$-linear mapping $\gamma_z : v \mapsto zv + v^q$ is a cyclic one, whose minimal polynomial is equal to $f(x)^{n/k} - 1$, where k is the degree of z over $\mathbb{F}_q$ and $f(x)$ is the minimal polynomial of z over $\mathbb{F}_q$. For every extension $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ (i.e. for every pair (q, n)), Hsu and Nan then consider *all* linear mappings of the form γ_z; taking $z = 0$ leads to the Frobenius automorphism and a primitive normal basis.

Observe that for a fixed pair (q, n) there are q^n endomorphisms of type γ_z, whereas, in general, the number of all cyclic $\mathbb{F}_q$-endomorphisms τ of $\mathbb{F}_{q^n}$ is certainly larger since there are already q^n possible distinct minimal polynomials of degree n, and since conjugate endomorphisms have the same minimal polynomial. Moreover,

we achieve stronger results than Hsu and Nan. For the case where $(q, n) = (2, 2)$, Hsu and Nan have extracted a counterexample, and they leave open a list $\mathcal{L}$ of 63 undecided pairs (q, n) (see [11, Remark 3.5]). Apart from the instance $(q, n) = (3, 12)$ any pair of our list $\mathcal{U}$ is contained in $\mathcal{L}$, and apart from the pair $(2, 2)$ any member of $\mathcal{C}$ is contained in $\mathcal{L}$ as well. So, our work resolves 41 instances of $\mathcal{L}$ — these are definitely extensive, and therefore primitive generators in particular do exist for the corresponding Carlitz modules as well. We shall briefly return to this discussion in our final Section 11.

We finally like to comment that, although a lot of computations are involved, our arguments certainly provide a theoretical justification of Theorem 1.3. They do not rely on (exhaustive) searches for primitive τ-generators in specific extensions E/F; the computations rather test sufficient existence criteria, obtained from bounds involving number theoretical properties of a pair (q, n). For the convenience of the reader we have summarized most of the relevant computational details (such as the number of distinct prime divisors of $q^n - 1$, or the very essential number of distinct monic divisors of m_τ which are irreducible over the ground field) in various tables. Only in our final Section 11 we are briefly going to report on attempts to resolve some of the remaining instances by an exhaustive computer search.

2 Outline

In Section 3 we give a sufficient criterion for extensiveness, which is obtained from the theory of finite field characters (Theorem 3.4), and which generalizes a corresponding basic approach on primitive normal bases from [1, 5, 14]. Based on this criterion we show in Section 4 that there are at most 84 pairs (q, n) that are *not* extensive; these pairs are listed in Table 1. After that, these open instances are investigated further with

- a simple counting argument (**sca**), Section 5,
- an improved counting argument (**ica**), Section 7,
- a sieving method (**sm**), Section 9 (adopted from [3]),
- and by geometric considerations (**ga**), Section 10.

We shall establish that 60 of the remaining 84 pairs are in fact extensive. We are also able to determine that the five pairs of the set $\mathcal{C}$ (see Theorem 1.3) are not extensive ones, i.e.

- counterexamples (**ce**), Sections 6 and 8.

This altogether reduces the previous list of 84 pairs to the set $\mathcal{U}$ of 19 pairs, whose status of being extensive or not could not be decided (**?**).

Table 1: The remaining pairs not covered by Theorem 3.4.

$(2,2)$	ce	$(2,3)$	sca	$(2,4)$	ce	$(2,5)$	sca	$(2,6)$	ce	$(2,7)$	sca
$(2,8)$	?	$(2,9)$	ica	$(2,10)$	?	$(2,11)$	ica	$(2,12)$	?	$(2,14)$	?
$(2,15)$	?	$(2,16)$	?	$(2,18)$	?	$(2,20)$	?	$(2,22)$	sm	$(2,24)$	?
$(2,28)$	sm	$(3,2)$	ce	$(3,3)$	ica	$(3,4)$	ga	$(3,5)$	ica	$(3,6)$	ga
$(3,7)$	ica	$(3,8)$	?	$(3,9)$	ica	$(3,10)$	?	$(3,11)$	ica	$(3,12)$	?
$(3,15)$	ica	$(3,16)$	sm	$(3,18)$	sm	$(4,2)$	sca	$(4,3)$	ga	$(4,4)$	ica
$(4,5)$	ica	$(4,6)$	?	$(4,7)$	ica	$(4,8)$	ica	$(4,9)$	?	$(4,10)$	?
$(4,12)$	?	$(4,14)$	sm	$(5,2)$	ce	$(5,3)$	ica	$(5,4)$	?	$(5,5)$	ica
$(5,6)$	ga	$(5,8)$	sm	$(5,9)$	ica	$(5,10)$	sm	$(5,12)$	sm	$(7,2)$	sca
$(7,3)$	ica	$(7,4)$	ga	$(7,5)$	ica	$(7,6)$	?	$(7,7)$	ica	$(7,9)$	sm
$(8,2)$	sca	$(8,4)$	ica	$(8,5)$	ica	$(8,6)$	ica	$(8,8)$	?	$(9,2)$	sca
$(9,3)$	sca	$(9,4)$	ica	$(9,6)$	sm	$(9,8)$	sm	$(9,9)$	ica	$(11,2)$	sca
$(11,3)$	sca	$(11,4)$	ica	$(11,6)$	sm	$(13,2)$	sca	$(13,3)$	sca	$(13,4)$	ica
$(16,2)$	sca	$(16,3)$	sca	$(19,2)$	sca	$(29,2)$	sca	$(41,2)$	sca	$(43,2)$	sca

3 A sufficient criterion based on character theory

Throughout, we fix a pair (q,n) and let $F = \mathbb{F}_q$ and $E = \mathbb{F}_{q^n}$, and τ be a cyclic F-endomorphism of E. Furthermore, let $(\mathbb{C}^*,\cdot)$ be the multiplicative group of the field $\mathbb{C}$ of complex numbers. The $\mathbb{C}$-algebra $\mathbb{C}^E$ of all mappings from E to $\mathbb{C}$ contains the characteristic function P of the set of all primitive elements of E (Subsection 3.1), as well as the characteristic function Γ_τ of the set of all τ-generators of E/F (Subsection 3.2). The pointwise product $P \cdot \Gamma_\tau$, which is the characteristic function of the set of all primitive τ-generators for E/F, can be described with the help of finite field characters, which is the basis of an efficient existence criterion (Subsection 3.3).

3.1 Multiplicative characters and the primitivity condition

A multiplicative character of E is a group homomorphism $\psi : (E^*,\cdot) \to (\mathbb{C}^*,\cdot)$, where $(E^*,\cdot)$ is multiplicative group of E. The set $\hat{E^*}$ of all multiplicative characters is turned into a group by defining $\psi \cdot \eta(v) := \psi(v)\eta(v)$ for all $v \in E^*$. The neutral element ψ_0 that maps every $v \in E^*$ to 1 is called the trivial multiplicative character. The groups $(\hat{E^*},\cdot)$ and $(E^*,\cdot)$ are isomorphic, i.e. both cyclic of order $q^n - 1$. For $v \in E^*$ the **(multiplicative) order** is the least integer $\ell \geq 1$ such that $v^\ell = 1$; it is denoted by $\mathrm{ord}(v)$. The same notation is used for multiplicative characters as well. It is convenient to extend any multiplicative character ψ by $\psi(0) := 1$, if $\psi = \psi_0$, and by $\psi(0) := 0$, if $\psi \neq \psi_0$.

For the ring $\mathbb{Z}$ of integers, let φ and μ denote the Euler- and the Möbius function,

respectively. Then ([1, 5, 14])

$$P := \frac{\varphi(q^n-1)}{q^n-1} \cdot \sum_{\psi \in \hat{E}^*} \frac{\mu(\mathrm{ord}(\psi))}{\varphi(\mathrm{ord}(\psi))} \cdot \psi \tag{3.1}$$

is the characteristic function of the set of all primitive elements of E, i.e. $P(w) = 1$ whenever w is a primitive element, and $P(w) = 0$, otherwise.

3.2 Additive characters and the τ-generator condition

Let us now turn to $(E, +)$, the additive group of E. An additive character of E is a group homomorphism $\chi : (E, +) \to (\mathbb{C}^*, \cdot)$. The set $\hat{E}$ of all additive characters carries the structure of a group by defining $\chi \cdot \lambda(v) := \chi(v)\lambda(v)$ for all $v \in E$ (observe that $\hat{E}$ is written multiplicatively). The neutral element χ_0 that maps every $v \in E$ to 1 is the trivial additive character. The groups $(E, +)$ and $(\hat{E}, \cdot)$ are isomorphic, i.e. both elementary abelian.

Next, consider some F-endomorphism τ of E, and let m_τ be its minimal polynomial. By defining

$$[f(x) \cdot \chi](v) := \chi(f(x) \cdot v) = \chi(f(\tau)v)$$

(for all $\chi \in \hat{E}$, all $v \in E$ and all $f(x) \in F[x]$), the additive character group $(\hat{E}, +)$ is turned into an $F[x]$-module with respect to τ. In fact, $(E, +)$ and $(\hat{E}, \cdot)$ are even isomorphic as $F[x]$-modules with respect to τ (which can essentially be shown by making use of Lemma 3.1 below). One therefore may apply the notion of τ-order to additive characters as well: $\mathrm{Ord}_\tau(\chi)$, the **τ-order of** χ, is the monic polynomial $g(x) \in F[x]$ of least degree such that $g(x) \cdot \chi = \chi_0$.

For a monic divisor $g(x)$ of $m_\tau(x)$ let

$$V_g := \{w \in E : g(x) \cdot w = 0\} \quad \text{and} \quad I_g := \{g(x) \cdot w : w \in E\}. \tag{3.2}$$

Similar, on the side of additive characters, let

$$C_g := \{\chi \in \hat{E} : g(x) \cdot \chi = \chi_0\} \tag{3.3}$$

be the kernel of $g(\tau)$ on $\hat{E}$. For a subgroup V of $(E, +)$ its dual group is

$$V^\perp := \{\chi \in \hat{E} : \chi(u) = 1 \text{ for all } u \in V\}.$$

Lemma 3.1 *Let τ be some F-endomorphism of E and assume that $g(x) \in F[x]$ is a monic divisor of $m_\tau(x)$. Then $C_g = I_g^\perp$.*

Proof: Let first $\chi \in C_g$. If $v \in I_g$ then there is a $w \in E$ such that $v = g(x) \cdot w$. Therefore, $\chi(v) = \chi(g(x) \cdot w) = [g(x) \cdot \chi](w) = \chi_0(w) = 1$ gives $I_g \subseteq \ker(\chi)$ for every $\chi \in C_g$. Consequently, $C_g \subseteq I_g^\perp$.

If, on the other hand, $\lambda \in I_g^\perp$, then $\lambda(g(x) \cdot w) = 1$ for all $w \in E$. But this implies $[g(x) \cdot \lambda](w) = \lambda(g(x) \cdot w) = 1 = \chi_0(w)$ for all $w \in E$, hence $g(x) \cdot \lambda = \chi_0$ and therefore $\lambda \in C_g$. □

In the case where τ is a cyclic F-endomorphism (which we are going to assume from now on), any V_g is a cyclic $F[x]$-module with respect to τ. Moreover, $\dim_F(V_g) = \deg(g)$ and $\dim_F(I_g) = n - \deg(g)$ in that case.

Next, we let ϕ_q and μ_q denote the Euler-, respectively Möbius function for the polynomial ring $F[x]$. Then the number of elements of E (and $\hat{E}$ as well) having τ-order g is equal to $\phi_q(g)$ (for any monic $g(x) \in F[x]$ dividing m_τ). For any such g, let

$$\Gamma_g := \frac{\phi_q(g)}{|V_g|} \cdot \sum_{\chi \in C_g} \frac{\mu_q(\mathrm{Ord}_\tau(\chi))}{\phi_q(\mathrm{Ord}_\tau(\chi))} \cdot \chi. \tag{3.4}$$

When $g = m_\tau$ we however use the simpler notation Γ_τ instead of Γ_{m_τ}, throughout. Because of the multiplicativity of the number theoretical functions involved, it holds that $\Gamma_g\Gamma_h = \Gamma_{gh}$ whenever g and h are relatively prime. Moreover, letting $\nu(g)$ be the square-free part of g, we have $\Gamma_g = \Gamma_{\nu(g)}$. Using elementary properties of additive characters (see Jungnickel [13, Section 7.1]), one can show that Γ_r is the characteristic function of the set $E \setminus I_r$ whenever $r(x) \in F[x]$ is a monic irreducible divisor of $m_\tau(x)$, i.e.

$$\Gamma_r(w) = \begin{cases} 1 & \text{if } w \text{ is } \textit{not} \text{ a member of } I_r, \\ 0 & \text{if } w \in I_r. \end{cases} \tag{3.5}$$

Now, if $r_1, \ldots, r_t \in F[x]$ are the distinct monic irreducible divisors of m_τ, then $\Gamma_\tau = \prod_{i=1}^t \Gamma_{r_i}$ is the characteristic function of the complement of the set $\bigcup_{i=1}^t I_{r_i}$ in E. On the other hand, since τ is assumed to be cyclic, $I_g = V_h$ where $h = m_\tau/g$, and therefore $\Gamma_\tau(w) = 1$ if and only if w is not a member of any of the maximal τ-invariant F-subspaces of E (and $\Gamma_\tau(w) = 0$, else). This altogether gives the following proposition.

Proposition 3.2 *Assume that τ is a cyclic F-endomorphism of E. Then Γ_τ is the characteristic function of the set of all τ-generators of E.* □

3.3 Primitive τ-generators and extensiveness

From the above, letting τ again be a cyclic F-endomorphism of E, we obtain that

$$\sum_{w \in E} P(w)\Gamma_\tau(w) \tag{3.6}$$

is the number of all primitive τ-generators of E/F. Using (3.1) and (3.4) (with $g = m_\tau$) gives that this number is equal to

$$\frac{\varphi(q^n-1)}{q^n-1}\frac{\phi_q(m_\tau)}{q^n} \cdot \sum_{\psi \in \hat{E}^*} \sum_{\chi \in \hat{E}} \frac{\mu(\mathrm{ord}(\psi))\mu_q(\mathrm{Ord}_\tau(\chi))}{\varphi(\mathrm{ord}(\psi))\phi_q(\mathrm{Ord}_\tau(\chi))} \cdot G(\psi, \chi), \tag{3.7}$$

where $G(\psi, \chi)$ is the Gauss sum $\sum_{w \in E} \psi(w)\chi(w)$. It is well known that $G(\psi_0, \chi_0) = q^n$, and $|G(\psi, \chi)| = \sqrt{q^n}$ when ψ and χ both are non-trival characters; moreover, if

either ψ or χ is trivial, then $G(\psi, \chi) = 0$ (see Lidl and Niederreiter [15, Section 5.2] or Jungnickel [13, Section 7.2]).

Next, assuming that there is no primitive τ-generator, using properties of the Möbius functions involved, one derives from (3.7) the inequality

$$q^n \leq \sum_{\substack{\nu(q^n-1)\\ d\neq 1}} \sum_{\substack{g|\nu(m_\tau)\\ g\neq 1}} \frac{\sqrt{q^n}}{\varphi(d)\cdot\phi_q(g)},$$

where ν yields the square-free part of its argument. The right hand side is equal to $(2^\omega - 1)(2^{\Omega_\tau} - 1)\sqrt{q^n}$, where ω denotes the number of distinct prime divisors of $q^n - 1$, while Ω_τ is the number of distinct monic divisors of m_τ from $F[x]$ which are irreducible. This altogether proves the following result.

Proposition 3.3 *Consider the field extension E/F where $E = \mathbb{F}_{q^n}$ and $F = \mathbb{F}_q$. Let $\omega = \omega(q, n)$ be the number of distinct prime divisors of $q^n - 1$. Let τ be a cyclic F-endomorphism of E and let $\Omega_\tau = \Omega_\tau(q, n)$ be the number of distinct monic irreducible divisors of m_τ in $F[x]$. Suppose that*

$$\sqrt{q^n} > (2^\omega - 1)(2^{\Omega_\tau} - 1).$$

Then there exists a primitive τ-generator for E/F. □

An immediate consequence of Proposition 3.3 is a sufficent criterion for a pair to be extensive:

Theorem 3.4 *Consider the field extension $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Let*

$$\Omega' = \Omega'(q, n) := \max\{\Omega_\tau : \tau \text{ a cyclic } \mathbb{F}_q\text{-endomorphism of } \mathbb{F}_{q^n}\} \tag{3.8}$$

and let $\omega = \omega(q, n)$ be as in Proposition 3.3. Assume that $\sqrt{q^n} > (2^\omega - 1)(2^{\Omega'} - 1)$. Then the pair (q, n) is extensive. □

4 Evaluation of the character theoretical criterion

Throughout, we denote the sufficient condition in Theorem 3.4 by (**ctc**). We are going to evaluate this criterion in the present section and shall achieve the following result.

Theorem 4.1 *Let $q > 1$ be a prime power and $n \geq 2$ an integer, and let $\omega = \omega(q, n)$ and $\Omega' = \Omega'(q, n)$ be as in Theorem 3.4. Then $\sqrt{q^n} > (2^\omega - 1)(2^{\Omega'} - 1)$ is satisfied if and only if (q, n) does not belong to the list of 84 pairs given in Table 1.*

The strategy for proving Theorem 4.1 is as follows: Obviously, $(2^\omega - 1)\cdot(2^{\Omega'} - 1) \leq 2^{\omega+\Omega'}$; we then use upper bounds u and U for ω and Ω', respectively, and show that

even $u + U \leq \log_2(\sqrt{q^n})$ for pairs (q, n) from a particular range. For the remaining not yet covered pairs, we definitely test (ctc) by determining the exact values of ω (by factorizing $q^n - 1$, for instance with the help of some Computer algebra system[1]) and of Ω' (by considering all monic irreducible polynomials of small degree over $\mathbb{F}_q$ as possible divisors of m_τ). Most of the computational results are summarized in the Tables 3–5. There, we have used the symbols • and ∘ to indicate whether

- $\sqrt{q^n} > (2^\omega - 1)(2^{\Omega'} - 1)$ (showing that (q, n) is extensive), or
- ∘ $\sqrt{q^n} \leq (2^\omega - 1)(2^{\Omega'} - 1)$ (leaving open whether (q, n) is extensive or not).

4.1 Upper bounds for ω and Ω'

In order to derive upper bounds for ω, we use Lemma 2.6 of [14] (already mentioned in Section 1). For $M \in \mathbb{N}^*$ let $\pi(M)$ be the set of distinct prime divisors of M. Furthermore, for an $\ell \in \mathbb{N}^*$ let π_ℓ be the set of all primes r such that $r < \ell$. If Λ is a set of primes such that $\pi(M) \cap \pi_\ell \subseteq \Lambda \subseteq \pi_\ell$, and if $L := \prod_{r \in \Lambda} r$, then

$$|\pi(M)| \;\leq\; \frac{\log(M) - \log(L)}{\log(\ell)} + |\Lambda|. \tag{4.1}$$

Proposition 4.2 *Consider the finite field $\mathbb{F}_{q^n}$. Then*

$$\omega = |\pi(q^n - 1)| \;<\; \frac{n}{6}\log_2(q) + \frac{21}{4}.$$

Proof: Taking $\ell := 64$ and $\Lambda := \pi_\ell$ gives $|\Lambda| = 18$ and $\log_2(L)/\log_2(\ell) \geq 12.75$. Thus, (4.1) implies

$$\omega \;\leq\; \frac{\log_2(q^n - 1) - \log_2(L)}{\log_2(\ell)} + |\Lambda| \;<\; \frac{n}{6}\log_2(q) - 12.75 + 18,$$

which is the desired upper bound. □

In order to obtain good upper bounds, or even the exact value for Ω' when q is small, we denote by $i_q(k)$ the number of distinct monic irreducible polynomials of degree k over $\mathbb{F}_q$. It is well known that $i_q(k) = \frac{1}{k}\sum_{d|k} \mu(\frac{k}{d}) q^d$. Furthermore, for an $m \in \mathbb{N}$ let

$$I_q(m) := \sum_{k=1}^{m} k i_q(k). \tag{4.2}$$

Lemma 4.3 *If $n \geq I_q(m)$, then*

$$\Omega' \;\leq\; \sum_{k=1}^{m} i_q(k) \;+\; \left\lfloor \frac{n - I_q(m)}{m+1} \right\rfloor.$$

[1]We have made use of `Maple`.

Table 2: Some values for $I_m(q)$ with q small.

	m	$i_q(m)$	$\sum_{k=1}^{m} i_q(k)$	$I_q(m)$
$q=5$	1	5	5	5
$q=5$	2	10	15	25
$q=5$	3	40	55	85
$q=4$	1	4	4	4
$q=4$	2	6	10	16
$q=4$	3	20	30	76
$q=3$	1	3	3	3
$q=3$	2	3	6	9
$q=3$	3	8	14	33
$q=3$	4	18	32	105
$q=2$	1	2	2	2
$q=2$	2	1	3	4
$q=2$	3	2	5	10
$q=2$	4	3	8	22
$q=2$	5	6	14	52
$q=2$	6	9	23	106

PROOF: If $n \geq I_q(m)$, then the minimal polynomial m_τ, which may be any polynomial of degree n, can potentially have every irreducible polynomial $r(x) \in F[x]$ with degree $\leq m$ as a factor. If this is the case, then dividing m_τ by all these irreducible divisors $r(x)$ leaves a polynomial of degree $n - I_q(m)$. But this can have at most $\lfloor \frac{n-I_q(m)}{m+1} \rfloor$ further distinct irreducible factors that are different from those of degree at most m, and therefore have degree at least $m+1$, each. □

Table 2 shows some relevant values of $I_q(m)$ when q is small.

4.2 The range $n \geq 16$ and $q \geq 16$

Assume that $\min(q, n) \geq 16$. We take $\Omega' \leq n$ as a trivial upper bound for Ω'. Then Proposition 4.2 implies $\omega + \Omega' \leq \frac{n}{6}\log_2(q) + \frac{21}{4} + n$, and this is less than or equal to $\frac{n}{2}\log_2(q)$ if and only if

$$\log_2(q) \;\geq\; \frac{63}{4n} + 3. \tag{4.3}$$

Since $q \geq 16$, one has $\log_2(q) \geq 4$ and as $n \geq 16$, one has $\frac{63}{4n} + 3 \leq \frac{63}{64} + 3 < 4$. This shows that (q, n) is an extensive pair whenever $\min(q, n) \geq 16$.

4.3 The range $n \leq 15$ and $q \geq 16$

For every fixed n with $2 \leq n \leq 15$, the number of all $q \geq 16$ such that $\log_2(q) < \frac{63}{4n}+3$ (see (4.3)) is finite. Letting

$$Q(n) := \lfloor 2^{3+63/(4n)} \rfloor,$$

we obtain the following data.

n	15	14	13	12	11	10	9	8	7	6	5	4	3	2
$Q(n)$	16	17	18	19	21	23	26	31	38	49	71	122	304	1878

For all pairs (q, n) such that $2 \leq n \leq 15$ and $16 \leq q \leq Q(n)$ a prime power, we have tested whether $\sqrt{q^n} > (2^\omega - 1)(2^n - 1)$ is satisfied. Observe that this is the bound from Theorem 3.4, because $\Omega' = n$ in that case, since $n \leq q-1$ in the present range. It turned out that (ctc) is satisfied by all these pairs (q, n) except when

$$(q, n) \in \{(16, 2), (19, 2), (29, 2), (41, 2), (43, 2), (16, 3)\}.$$

4.4 The range $q \in \{7, 8, 9, 11, 13\}$

An improvement of the ω-bound in Proposition 4.2 is available by setting $\Lambda := \pi_{64} \setminus \{p\}$, where p is the characteristic of $\mathbb{F}_q$.[2] If $n \geq q+2$, then we have taken the bound

$$\Omega' \leq q + \frac{n-q}{2} = \frac{1}{2}q + \frac{1}{2}n,$$

as the number of monic (irreducible) polynomials of degree 1 in $\mathbb{F}_q[x]$ is q. Then, $\frac{n}{6}\log_2(q) + \frac{21}{4} + \frac{1}{2}q + \frac{1}{2}n \leq \frac{n}{2}\log_2(q)$ if and only if

$$n \;\geq\; \frac{\frac{21}{4} + \frac{q}{2}}{\frac{1}{3}\log_2(q) - \frac{1}{2}}.$$

For $q = 13$ or $q = 11$ the latter is satisfied when $n \geq 17$. For $q = 9$ it is satisfied when $n \geq 18$. For $q = 8$ it holds when $n \geq 19$, and for $q = 7$ it is satisfied when $n \geq 21$.

Next, we have checked (ctc) for the remaining range (i.e. $n \leq 21$) and obtained that it is satisfied if and only if (q, n) does not belong to one of the following 25 pairs:

q	n							
7	2	3	4	5	6	7		9
8	2		4	5	6		8	
9	2	3	4		6		8	9
11	2	3	4		6			
13	2	3	4					

The computational results rely on the data in Table 3.

[2] However, we did not make use of this.

Table 3: Character theoretical criterion (ctc) for $q \in \{7, 8, 9, 11, 13\}$.

$q = 13$	n	ω	Ω'	$q = 13$	n	ω	Ω'	$q = 13$	n	ω	Ω'
•	16	7	14	•	15	6	14	•	14	6	13
•	13	5	13	•	12	8	12	•	11	6	11
•	10	6	10	•	9	4	9	•	8	6	8
•	7	3	7	•	6	5	6	•	5	3	5
○	4	5	4	○	3	3	3	○	2	3	2

$q = 11$	n	ω	Ω'	$q = 11$	n	ω	Ω'	$q = 11$	n	ω	Ω'
•	16	7	13	•	15	6	13	•	14	6	12
•	13	4	12	•	12	9	11	•	11	4	11
•	10	5	10	•	9	5	9	•	8	5	8
•	7	4	7	○	6	6	6	•	5	3	5
○	4	4	4	○	3	4	3	○	2	3	2

$q = 9$	n	ω	Ω'	$q = 9$	n	ω	Ω'	$q = 9$	n	ω	Ω'
•	17	6	13	•	16	6	12	•	15	8	12
•	14	6	11	•	13	3	11	•	12	7	10
•	11	5	10	•	10	5	9	○	9	6	9
○	8	5	8	•	7	3	7	○	6	5	6
•	5	3	5	○	4	3	4	○	3	3	3
○	2	2	2								

$q = 8$	n	ω	Ω'	$q = 8$	n	ω	Ω'	$q = 8$	n	ω	Ω'
•	18	6	13	•	17	5	12	•	16	9	12
•	15	6	11	•	14	6	11	•	13	4	10
•	12	8	10	•	11	4	9	•	10	6	9
•	9	3	8	○	8	6	8	•	7	3	7
○	6	4	6	○	5	3	5	○	4	4	4
•	3	2	3	○	2	2	2				

$q = 7$	n	ω	Ω'	$q = 7$	n	ω	Ω'	$q = 7$	n	ω	Ω'
•	20	8	13	•	19	4	13	•	18	7	12
•	17	4	12	•	16	6	11	•	15	6	11
•	14	6	10	•	13	3	10	•	12	7	9
•	11	4	9	•	10	5	8	○	9	5	8
•	8	4	7	○	7	4	7	○	6	4	6
○	5	3	5	○	4	3	4	○	3	3	3
○	2	2	2								

4.5 The range $q \in \{2,3,4,5\}$

The proofs of the subsequent statements are based on the computational results summarized in Table 4 and Table 5.

Let us first consider $q = 5$. Then (ctc) is satisfied for all n except when n is one of the nine members from $\{2,3,4,5,6,8,9,10,12\}$.

Proof: Assume first that $n \geq 28$. Then $n \geq 25 = I_5(2)$ and therefore

$$\Omega' \leq i_5(1) + i_5(2) + \frac{n - I_5(2)}{3} = \frac{1}{3}n + \frac{20}{3} \quad \text{for these } n.$$

Hence, $\omega + \Omega' \leq \frac{n}{6}\log_2(5) + \frac{21}{4} + \frac{1}{3}n + \frac{20}{3}$. The latter is less than or equal to $\frac{n}{2}\log_2(5)$ if and only if

$$n \geq \frac{\frac{21}{4} + \frac{20}{3}}{\frac{1}{3}\log_2(5) - \frac{1}{3}},$$

and this holds for all $n \geq 28$.

- If $n \in \{25,26,27\}$, then the maximal m such that $I_5(m) \leq n$ is $m = 2$. This gives $\Omega' = i_5(1) + i_5(2) + \lfloor \frac{n - I_5(2)}{3} \rfloor = 15 + \lfloor \frac{n-25}{3} \rfloor$ for these n.
- If $5 \leq n \leq 24$, then the maximal m such that $I_5(m) \leq n$ is $m = 1$. Hence, $\Omega' = i_5(1) + \lfloor \frac{n - I_5(1)}{2} \rfloor = 5 + \lfloor \frac{n-5}{2} \rfloor$ for these n.
- If $n \in \{2,3,4\}$, then $\Omega' = n$. □

Let us consider next $q = 4$. Then (ctc) is satisfied for all n except when n is one of the eleven members of $\{2,3,4,5,6,7,8,9,10,12,14\}$.

Proof: Assume that $n \geq 30$. Then $n \geq 33 = I_4(2)$ and therefore

$$\Omega' \;\leq\; i_4(1) + i_4(2) + \frac{n - I_4(2)}{3} \;=\; \frac{1}{3}n + \frac{14}{3} \quad \text{for these } n.$$

Consequently, $\omega + \Omega' \leq \frac{n}{6}\log_2(4) + \frac{21}{4} + \frac{1}{3} \cdot n + \frac{14}{3} = \frac{2}{3}n + \frac{21}{4} + \frac{20}{3}$, and the latter is less than or equal to $\frac{n}{2}\log_2(4) = n$ if and only if $n \geq 3 \cdot \left(\frac{21}{4} + \frac{14}{3}\right) = \frac{119}{4}$.

- If $16 \leq n \leq 29$, then the maximal m such that $I_4(m) \leq n$ is $m = 2$. Therefore $\Omega' = i_4(1) + i_4(2) + \lfloor \frac{n - I_4(2)}{3} \rfloor = 10 + \lfloor \frac{n-16}{3} \rfloor$ for these n.
- If $4 \leq n \leq 15$, then the maximal m such that $I_4(m) \leq n$ is $m = 1$. Therefore $\Omega' = i_4(1) + \lfloor \frac{n - I_4(1)}{2} \rfloor = 4 + \lfloor \frac{n-4}{2} \rfloor$ for these n.
- If $n \in \{2,3\}$, then $\Omega' = n$. □

Assume now that $q = 3$. Then (ctc) is satisfied for all n except when n is equal to one of the 14 values from $\{2,3,4,5,6,7,8,9,10,11,12,15,16,18\}$.

PROOF: We use Table 2. Assume that $n \geq 40$. Then $n \geq 33 = I_3(3)$ and therefore

$$\Omega' \;\leq\; i_3(1) + i_3(2) + i_3(3) + \frac{n - I_3(3)}{4} \;=\; \frac{1}{4}n + \frac{23}{4}.$$

Moreover, $\omega + \Omega' \leq \frac{n}{6}\log_2(3) + \frac{21}{4} + \frac{1}{4}n + \frac{23}{4}$. The latter is less than or equal to $\frac{n}{2}\log_2(3)$ if and only if

$$n \;\geq\; \frac{11}{\frac{1}{3}\log_2(3) - \frac{1}{4}},$$

and this holds for all $n \geq 40$.

- If $33 \leq n \leq 39$, then the maximal m such that $I_3(m) \leq n$ is $m = 3$. Therefore $\Omega' = i_3(1) + i_3(2) + i_3(3) + \lfloor \frac{n - I_3(3)}{4} \rfloor = 14 + \lfloor \frac{n-33}{4} \rfloor$ for these n.
- If $10 \leq n \leq 32$, then the maximal m such that $I_3(m) \leq n$ is $m = 2$. Hence, $\Omega' = i_3(1) + i_3(2) + \lfloor \frac{n - I_3(2)}{3} \rfloor = 6 + \lfloor \frac{n-9}{3} \rfloor$ for these n.
- If $4 \leq n \leq 9$, then the maximal m such that $I_3(m) \leq n$ is $m = 1$, and therefore $\Omega' = i_3(1) + \lfloor \frac{n - I_3(1)}{2} \rfloor = 3 + \lfloor \frac{n-3}{2} \rfloor$ for these n.
- If $n \in \{2, 3\}$, then $\Omega' = n$. □

Finally let $q = 2$. Then (ctc) is satisfied for all n except when n is equal to one of the 19 values in $\{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 16, 18, 20, 22, 24, 28\}$.

PROOF: We again use Table 2. Assume that $n \geq 64$. Then $n \geq 52 = I_2(5)$ and therefore

$$\Omega' \;\leq\; i_2(1) + i_2(2) + i_2(3) + i_2(4) + i_2(5) + \frac{n - I_2(5)}{6} \;=\; \frac{1}{6}n + \frac{16}{3}.$$

This gives $\omega + \Omega' \leq \frac{n}{6}\log_2(2) + \frac{21}{4} + \frac{1}{6}n + \frac{16}{3} = \frac{1}{3}n + \frac{21}{4} + \frac{16}{3}$. The latter is less than or equal to $\frac{n}{2}\log_2(2) = \frac{n}{2}$ if and only if $n \geq 6 \cdot \left(\frac{21}{4} + \frac{16}{3}\right) = \frac{127}{2}$.

- If $52 \leq n \leq 63$, then the maximal m such that $I_2(m) \leq n$ is $m = 5$. Therefore $\Omega' = i_2(1) + i_2(2) + i_2(3) + i_2(4) + i_2(5) + \lfloor \frac{n - I_2(5)}{6} \rfloor = 14 + \lfloor \frac{n-52}{6} \rfloor$ for these n.
- If $22 \leq n \leq 51$, then the maximal m such that $I_2(m) \leq n$ is $m = 4$. Hence, for these n, one has $\Omega' = i_2(1) + i_2(2) + i_2(3) + i_2(4) + \lfloor \frac{n - I_2(4)}{5} \rfloor = 8 + \lfloor \frac{n-22}{5} \rfloor$.
- If $10 \leq n \leq 21$, then the maximal m such that $I_2(m) \leq n$ is $m = 3$. Therefore $\Omega' = i_2(1) + i_2(2) + i_2(3) + \lfloor \frac{n - I_2(3)}{4} \rfloor = 5 + \lfloor \frac{n-10}{4} \rfloor$ for these n.
- If $4 \leq n \leq 9$, then the maximal m such that $I_2(m) \leq n$ is $m = 2$. Therefore $\Omega' = i_2(1) + i_2(2) + \lfloor \frac{n - I_2(2)}{3} \rfloor = 3 + \lfloor \frac{n-4}{3} \rfloor$ for this range of n.
- Finally, if $n \in \{2, 3\}$, then $\Omega' = n$. □

Table 4: Character theoretical criterion (ctc) for $q \in \{3, 4, 5\}$.

$q=5$	n	ω	Ω'	$q=5$	n	ω	Ω'	$q=5$	n	ω	Ω'
•	27	8	15	•	26	5	15	•	25	7	15
•	24	8	14	•	23	3	14	•	22	6	13
•	21	5	13	•	20	8	12	•	19	4	12
•	18	7	11	•	17	3	11	•	16	6	10
•	15	6	10	•	14	5	9	•	13	2	9
○	12	6	8	•	11	2	8	○	10	5	7
○	9	4	7	○	8	4	6	•	7	2	6
○	6	4	5	○	5	3	5	○	4	3	4
○	3	2	3	○	2	2	2				

$q=4$	n	ω	Ω'	$q=4$	n	ω	Ω'	$q=4$	n	ω	Ω'
•	29	6	14	•	28	8	14	•	27	6	13
•	26	7	13	•	25	7	13	•	24	9	12
•	23	4	12	•	22	7	12	•	21	6	11
•	20	7	11	•	19	3	11	•	18	8	10
•	17	3	10	•	16	5	10	•	15	6	9
○	14	6	9	•	13	3	8	○	12	6	8
•	11	4	7	○	10	5	7	○	9	4	6
○	8	4	6	○	7	3	5	○	6	5	5
○	5	3	4	○	4	3	4	○	3	2	3
○	2	2	2								

$q=3$	n	ω	Ω'	$q=3$	n	ω	Ω'	$q=3$	n	ω	Ω'
•	39	6	15	•	38	5	15	•	37	3	15
•	36	9	14	•	35	5	14	•	34	6	14
•	33	5	14	•	32	6	13	•	31	4	13
•	30	8	13	•	29	4	12	•	28	6	12
•	27	6	12	•	26	3	11	•	25	4	11
•	24	7	11	•	23	3	10	•	22	5	10
•	21	4	10	•	20	5	9	•	19	3	9
○	18	6	9	•	17	3	8	○	16	5	8
○	15	4	8	•	14	3	7	•	13	2	7
○	12	5	7	○	11	3	6	○	10	3	6
○	9	3	6	○	8	3	5	○	7	2	5
○	6	3	4	○	5	2	4	○	4	2	3
○	3	2	3	○	2	1	2				

Table 5: Character theoretical criterion (ctc) for $q = 2$.

$q=2$	n	ω	Ω'	$q=2$	n	ω	Ω'	$q=2$	n	ω	Ω'
•	63	6	15	•	62	3	15	•	61	1	15
•	60	11	15	•	59	2	15	•	58	6	15
•	57	4	14	•	56	8	14	•	55	6	14
•	54	6	14	•	53	3	14	•	52	7	14
•	51	5	13	•	50	7	13	•	49	2	13
•	48	9	13	•	47	3	13	•	46	4	12
•	45	6	12	•	44	7	12	•	43	3	12
•	42	6	12	•	41	2	11	•	40	7	11
•	39	4	11	•	38	3	11	•	37	2	11
•	36	8	10	•	35	4	10	•	34	3	10
•	33	4	10	•	32	5	10	•	31	1	9
•	30	6	9	•	29	3	9	○	28	6	9
•	27	3	9	•	26	3	8	•	25	3	8
○	24	6	8	•	23	2	8	○	22	4	8
•	21	3	7	○	20	5	7	•	19	1	7
○	18	4	7	•	17	1	6	○	16	4	6
○	15	3	6	○	14	3	6	•	13	1	5
○	12	4	5	○	11	2	5	○	10	3	5
○	9	2	4	○	8	3	4	○	7	1	4
○	6	2	3	○	5	1	3	○	4	2	3
○	3	1	2	○	2	1	2				

5 The simple counting argument

From Theorem 4.1 there are 84 open cases for which, at this stage, we do not know whether the corresponding pair is extensive or not. In the present section we are going to show that the 18 pairs (q, n) with

$$n = 2\text{: } q \in \{4, 7, 8, 9, 11, 13, 16, 19, 29, 41, 43\}$$

$$n = 3\text{: } q \in \{9, 11, 13, 16\}$$

$$q = 2\text{: } n \in \{3, 5, 7\}$$

are in fact extensive ones. In order to do so, we let

$$\phi'_q(n) := \min\{\phi_q(f) : f \in \mathbb{F}_q[x] \text{ monic of degree } n\}. \tag{5.1}$$

The following criterion is called the **simple counting argument**, (**sca**).

Theorem 5.1 *Assume that $\varphi(q^n - 1) > q^n - 1 - \phi'_q(n)$. Then (q, n) is extensive.*

Proof: Let τ be any cyclic endomorphism. Then m_τ has degree n. Let $\mathcal{P}$ be the set of primitive elements of $\mathbb{F}_{q^n}$ and $\mathcal{G}_\tau$ the set of τ-generators of $\mathbb{F}_{q^n}/\mathbb{F}_q$. Then

$$\begin{aligned} |\mathcal{P} \cap \mathcal{G}_\tau| &= |\mathcal{P}| + |\mathcal{G}_\tau| - |\mathcal{P} \cup \mathcal{G}_\tau| \\ &\geq |\mathcal{P}| + |\mathcal{G}_\tau| - (q^n - 1) \\ &= \varphi(q^n - 1) + \phi_q(m_\tau) - (q^n - 1) \\ &\geq \varphi(q^n - 1) + \phi'_q(n) - (q^n - 1). \end{aligned}$$

So, if $\varphi(q^n - 1) - \big(q^n - 1 - \phi'_q(n)\big)$ is positive, then $\mathcal{P} \cap \mathcal{G}_\tau$ is nonempty for every τ. □

It turns out that (sca) works well for $n = 2$ and it is rather good when $n = 3$. In order to apply it, we need information on the functions ϕ_q and ϕ'_q. Let therefore

$$m_\tau(x) = \prod_{j=1}^{s} g_j(x)^{a_j} \tag{5.2}$$

be the decomposition of m_τ into monic irreducible polynomials (over $\mathbb{F}_q$) and write $d_j := \deg(g_j)$ for $j = 1, \ldots, s$. Then $\sum_{j=1}^{s} a_j d_j = n$ and

$$\phi_q(m_\tau) = \prod_{j=1}^{s} q^{(a_j-1)d_j} \cdot (q^{d_j} - 1). \tag{5.3}$$

In this situation we call

$$\Delta_\tau := [d_1^{a_1}, d_2^{a_2}, \ldots, d_m^{a_m}] \tag{5.4}$$

Table 6: Simple counting argument (sca) for $n \in \{2, 3\}$.

$n=2$	q	$\varphi(q^2-1)$	$q^2-1-\phi'_q(2)$
○	2	2	2
○	3	4	4
•	4	8	6
○	5	8	8
•	7	16	12
•	8	36	14
•	9	32	16
•	11	32	20
•	13	48	24
•	16	128	30
•	19	96	36
•	29	192	56
•	41	384	80
•	43	480	84

$n=3$	q	$\varphi(q^3-1)$	$q^3-1-\phi'_q(3)$
○	3	12	18
○	4	36	36
○	5	60	60
○	7	108	126
•	9	288	216
•	11	432	330
•	13	720	468
•	16	1728	720

the **factor pattern** of m_τ, a terminology which we also frequently use in the forthcomming sections. We shall later however omit a superscript a_i when $a_i = 1$. Equation (5.3) shows that $\phi_q(m_\tau)$ only depends on the factor pattern of m_τ and we therefore may also write

$$\phi_q(\Delta_\tau) \text{ for } \phi_q(m_\tau).$$

If Δ' is a factor pattern such that $\phi_q(\Delta') = \phi'_q(n)$, then Δ' is called a *worst case factor pattern*. When $n \leq q$, hence $\Omega' = n$, one has $\phi'_q(n) = \phi([1, \ldots, 1]) = (q-1)^n$. So, for $n = 2$ we have $\phi'_q(2) = \phi_q([1, 1]) = (q-1)^2$, which yields $q^2 - 1 - \phi'_q(2) = 2q - 2$. And for $n = 3$ and $q \geq 3$ we have $\phi'_q(3) = \phi([1, 1, 1]) = (q-1)^3$, which gives $q^3 - 1 - \phi'_q(3) = 3q^2 - 3q$ for $q \geq 3$. The relevant computational results are summarized in Table 6.

For the cases $q = 2$ and $n \in \{3, 5, 7\}$ the numbers $2^3 - 1 = 7$ and $2^5 - 1 = 31$ and $2^7 - 1 = 127$ are primes. Hence every nonzero element of $\mathbb{F}_{q^n}$ is primitive, and the corresponding pairs are trivially extensive.

6 Three counterexamples

In the present section we consider the values $q = 2, 3, 5$ with $n = 2$. It is interesting to see that the simple counting argument here just fails with equality (Table 6), and we will show indeed that these pairs are *not* extensive.

6.1 The pair $(q, n) = (2, 2)$

Write $E = \mathbb{F}_4 = \{0, 1, \zeta, \zeta + 1\}$, where ζ is a primitive third root of unity, i.e. $\zeta^2 = \zeta + 1$. Observe that ζ, ζ^2 is a primitive normal basis for $\mathbb{F}_4$ over $\mathbb{F}_2$.

The requirement is that m_τ has factor pattern $[1, 1]$. This implies $m_\tau = x(x-1)$. Defining τ by $\tau(\zeta) = 0$ and $\tau(\zeta^2) = \zeta^2$ gives the desired minimal polynomial, and the only τ-generator is 1. Consequently, the pair $(q, n) = (2, 2)$ is not extensive.

6.2 The pair $(q, n) = (3, 2)$

The polynomial $y^2 + y + 2$ is irreducible over $\mathbb{F}_3$. Let ζ be a root of that polynomial (in the field $\mathbb{F}_9$). Then ζ is a primitive element of $\mathbb{F}_9$, and therefore the $\varphi(3^2 - 1) = 4$ primitive elements of $\mathbb{F}_9$ are ζ, $\zeta^3 = 2\zeta + 2$, $\zeta^5 = 2\zeta$ and $\zeta^7 = \zeta + 1$. The non-zero elements which are not primitive are $\zeta^2 = 2\zeta + 1$, $\zeta^4 = 2$, $\zeta^6 = \zeta + 2$ and $\zeta^8 = 1$.

Now, take 1 together with ζ as a canonical basis of $\mathbb{F}_9$ over $\mathbb{F}_3$ and define the $\mathbb{F}_3$-endomorphism τ on $\mathbb{F}_9$ by $\tau(1) := 2\zeta$ and $\tau(\zeta) := \zeta$. Then $m_\tau = x(x - 1)$. The eigenspace for the eigenvalue $\lambda = 0$ is $E_0 = \{0, 2\zeta + 2, 2\zeta\}$ and the eigenspace for the eigenvalue $\lambda = 1$ is $E_1 = \{0, \zeta, \zeta + 1\}$. Therefore, no primitive element is a τ-generator. This shows that the pair $(q, n) = (3, 2)$ is not extensive.

6.3 The pair $(q, n) = (5, 2)$

The polynomial $y^2 + y + 2$ is irreducible over $\mathbb{F}_5$. Let ζ be a root of that polynomial (in the field $\mathbb{F}_{25}$). Then ζ is a primitive element of $\mathbb{F}_{25}$, all other primitive elements are marked with an $*$ in Table 7, where the powers of ζ are expressed in the canonical basis $1, \zeta$ for $\mathbb{F}_{25}$ over $\mathbb{F}_5$.

The $\mathbb{F}_5$-subspace spanned by ζ is equal to $\{0, \zeta, 2\zeta, 3\zeta, 4\zeta\}$, while the $\mathbb{F}_5$-subspace spanned by ζ^5 is equal to $\{0, \zeta + 1, 2\zeta + 2, 3\zeta + 3, 4\zeta + 4\}$. Remarkably, the nonzero elements of these two spaces are exactly the primitive elements of $\mathbb{F}_{25}$. These can be made into the eigenspaces of an endomorphism τ with minimal polynomial $m_\tau(x) = (x - a)(x - b)$ for distinct $a, b \in \mathbb{F}_5$. In all these situations there is no primitive element which is a τ-generator, and therefore the pair $(q, n) = (5, 2)$ is not extensive.

For instance, choosing $a = 1$ and $b = -1$ gives $m_\tau = x^2 - 1$, which is the same minimal polynomial as that of the Frobenius automorphism of $\mathbb{F}_{25}$ over $\mathbb{F}_5$. But for the Frobenius automorphism a primitive generator does exist by the primitive normal basis theorem!

Table 7: The quadratic extension of $\mathbb{F}_5$.

ℓ	ζ^ℓ	ℓ	ζ^ℓ
2	$4\zeta+3$	13^*	4ζ
3	$4\zeta+2$	14	$\zeta+2$
4	$3\zeta+2$	15	$\zeta+3$
5^*	$4\zeta+4$	16	$2\zeta+3$
6	2	17^*	$\zeta+1$
7^*	2ζ	18	3
8	$3\zeta+1$	19^*	3ζ
9	$3\zeta+4$	20	$2\zeta+4$
10	$\zeta+4$	21	$2\zeta+1$
11^*	$3\zeta+3$	22	$4\zeta+1$
12	4	23^*	$2\zeta+2$

7 The improved counting argument

The simple counting argument from Section 5 is rather limited when $n \geq 4$. In the present section we therefore establish an improvement of Theorem 5.1 (see Theorem 7.3). This criterion is in fact a forerunner of the geometric approach we are going to consider in Section 10. Here, we prove that the following 25 pairs are extensive:

$q = 2$: $n \in \{9, 11\}$

$q = 3$: $n \in \{3, 5, 7, 9, 11, 15\}$

$q = 4$: $n \in \{4, 5, 7, 8\}$

$q = 5$: $n \in \{3, 5, 9\}$

$q = 7$: $n \in \{3, 5, 7\}$

$q = 8$: $n \in \{4, 5, 6\}$

$q = 9$: $n \in \{4, 9\}$

$(q, n) = (11, 4)$ and $(q, n) = (13, 4)$

The idea is to study the problem from a *projective point of view*. This means that we are now going to consider $E = \mathbb{F}_{q^n}$ as an $(n-1)$-dimensional projective space over the ground field $F = \mathbb{F}_q$, i.e. as $\Pi := PG_{n-1}(q)$. (For the basics on projective geometry see Hirschfeld [10].) The *points* of Π are the one-dimensional subspaces of E. For a nonzero $v \in E$, we let

$$F^*v = \{\lambda v : \lambda \in F,\ \lambda \neq 0\}$$

be the set of nonzero elements of the point Fv. A point Fv is called **primitive**, if there is a primitive element in F^*v. In order to determine the number of primitive elements contained in a primitive point, we let

$$q-1=\prod_{i=1}^{k} r_i^{a_i}\cdot\prod_{j=1}^{\ell} s_j^{b_j} \quad \text{and} \quad q^n-1=\prod_{i=1}^{k} r_i^{a_i}\cdot\prod_{j=1}^{\ell} s_j^{b'_j}\cdot\prod_{k=1}^{m} t_k^{c_k} \tag{7.1}$$

be the prime power factorizations of $q-1$ and q^n-1, respectively, where the r_i and the s_j are the common primes of these two numbers, and where $b_j < b'_j$ for all $j=1,\ldots,\ell$. Let further

$$R:=\prod_{i=1}^{k} r_i^{a_i} \quad \text{and} \quad S:=\prod_{j=1}^{\ell} s_j^{b_j}. \tag{7.2}$$

The following is a consequence from basic group theory. For a proof we refer to [8, Section 5].

Proposition 7.1 *Assume that v is a primitive element. Then the primitive point Fv contains exactly $\varphi(R)\cdot S$ primitive elements.* □

Later, we will often refer to $\varphi(R)\cdot S$ as a *multiplier*. Moreover, in Section 10, the extension field E will sometimes also be considered as a projective space over some intermediate field K of E/F, and then the K-points have the form Kv, and a corresponding multiplier for E/K then counts the number of primitive elements in some primitive K-point.

Consider next the decomposition of m_τ as in (5.2) of Section 5. For every monic irreducible divisor $g_i \in F[x]$ of m_τ, let $M_i := m_\tau/g_i$ and $V_i := V_{M_i}$. Then V_i, the subspace of E that is annihilated by M_i, is a maximal τ-invariant subspace of E. Furthermore, let

$$C_\tau := \bigcup_{i=1}^{s} V_i. \tag{7.3}$$

Then C_τ consists of all elements of E that are *not* τ-generators of E, and therefore $|C_\tau| = q^n - \phi_q(m_\tau)$. Since C_τ is closed under the multiplication with field elements $\lambda \in F$, we may consider C_τ as a **configuration of points** from the underlying projective space Π; when doing so, we use the calligraphic notation $\mathcal{C}_\tau$. The number of points of $\mathcal{C}_\tau$ is therefore equal to

$$|\mathcal{C}_\tau| = \frac{|C_\tau|-1}{q-1}. \tag{7.4}$$

Proposition 7.2 *Let (q,n) and a cyclic $\mathbb{F}_q$-endomorphism τ of $\mathbb{F}_{q^n}$ be given. Assume that*

$$|\mathcal{C}_\tau|\cdot\varphi(R)\cdot S \;<\; \varphi(q^n-1).$$

Then there exists a primitive τ-generator in $\mathbb{F}_{q^n}$.

PROOF: The total set $\mathcal{P}$ of primitive elements of E gives

$$\frac{\varphi(q^n-1)}{\varphi(R)\cdot S}$$

primitive points in the projective geometry Π. If this number is larger than $|\mathcal{C}_\tau|$, then there exists a primitive point outside the configuration $\mathcal{C}_\tau$. Consequently, any primitive element of such a point is a τ-generator of E. □

The consideration of a worst case leads to the following sufficient criterion for extensiveness. We call it the **improved counting argument** (**ica**), and therefore let

$$c' = c'(q,n) := \frac{q^n - 1 - \phi'_q(n)}{q-1}, \tag{7.5}$$

where $\phi'_q(n)$ is defined in (5.1).

Theorem 7.3 *Let (q,n) be given. Assume that*

$$c' \cdot \varphi(R)\cdot S \;<\; \varphi(q^n-1).$$

Then (q,n) is extensive. □

As mentioned at the end of Section 5, for $q \geq n$ the worst case arises always when m_τ splits into distinct linear factors. This gives

$$c' = \frac{q^n - 1 - (q-1)^n}{q-1}.$$

When however $q < n$, then c' is derived from a worst case factor pattern Δ' giving $\phi_q(\Delta') = \phi'_q(n)$. Some relevant data is summarized in Table 8.

The positive results obtained by an application of Theorem 7.3 are summarized in Table 9. The improved counting argument failed for all other open pairs.

8 Two further counterexamples

In the present section we consider the two pairs $(2,4)$ and $(2,6)$. We will see that these pairs are not extensive.

8.1 The pair $(q,n) = (2,4)$

As a model for $E = \mathbb{F}_{2^4}$ we choose the irreducible polynomial

$$z^4 + z + 1$$

Table 8: Worst case factor patterns for certain pairs (q, n).

q	n	worst case pattern Δ'
3	5	$[1, 1, 1, 2]$
4	5	$[1, 1, 1, 1^2]$
3	7	$[1, 1, 1, 2, 2]$
4	7	$[1, 1, 1, 1^2, 2]$
4	8	$[1, 1, 1, 1, 2, 2]$
2	9	$[1, 1^3, 2, 3]$
3	9	$[1, 1, 1, 2, 2, 2]$
5	9	$[1, 1, 1, 1, 1, 2, 2]$
2	11	$[1, 1^2, 2, 3, 3]$
3	11	$[1, 1, 1^3, 2, 2, 2]$
3	15	$[1, 1, 1, 2, 2, 2, 3, 3]$

from $\mathbb{F}_2[z]$, whose roots are in fact primitive elements of E, here primitive 15th roots of unity. So, we take $1, z, z^2, z^3$ as an F-basis of E. Now, let τ be the F-endomorphism of E, which, with respect to this basis is represented by the matrix

$$\begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Then $\tau(1) = z$ and $\tau(z) = z^2$ and $\tau(z^2) = z^3+1$ and $\tau(z^3) = z^3+z+1$ show that the τ-order of 1 is equal to $x^4 + x^3 = x^3(x + 1)$. Hence, τ is a cyclic $\mathbb{F}_2$-endomorphism and $m_\tau = x^3(x + 1)$. This implies that there are exactly

$$\phi_q(m_\tau) = (2^3 - 2^2) \cdot (2 - 1) = 4$$

τ-generators of E. Apart from 1, these are the elements

$$\begin{array}{lllllll} (x^2 + x + 1) \cdot 1 & = & \tau^2(1) + \tau(1) + 1 & = & z^2 + z + 1 & = & z^{10}, \\ (x^3 + x + 1) \cdot 1 & = & \tau^3(1) + \tau(1) + 1 & = & z^3 + z & = & z^9, \\ (x^3 + x^2 + 1) \cdot 1 & = & \tau^3(1) + \tau^2(1) + 1 & = & z^3 + z^2 & = & z^6. \end{array}$$

Since none of the z-exponents of these elements is relatively prime to $2^4 - 1 = 15$, i.e. either divisible by 3 or by 5, none of these elements is primitive. This shows that there is no primitive τ-generator and therefore the pair $(2, 4)$ is not extensive.

8.2 The pair $(q, n) = (2, 6)$

As a model for $E = \mathbb{F}_{2^6}$ we choose the irreducible polynomial

$$\Phi_9(y) = y^6 + y^3 + 1$$

Table 9: Application of Theorem 7.3 (ica).

q	n	c'	R	S	$c' \cdot \varphi(R) \cdot S$	$\varphi(q^n - 1)$
3	3	9	2	1	9	12
5	3	15	4	1	30	60
7	3	21	2	3	63	108
4	4	58	3	1	116	128
8	4	242	7	1	1 452	1 728
9	4	308	1	8	2 464	2 560
11	4	464	5	2	3 712	3 840
13	4	6 532	3	4	5 216	6 144
3	5	89	2	1	89	110
4	5	233	3	1	466	600
5	5	525	4	1	1 050	1 400
7	5	1 505	6	1	3 010	5 600
8	5	2 280	7	1	13 680	27 000
8	6	20 642	7	1	123 852	139 968
3	7	837	2	1	837	1 092
4	7	3 841	3	1	7 682	10 584
7	7	90 601	6	1	181 202	264 992
4	8	15 770	3	1	31 540	32 768
2	9	427	1	1	427	432
3	9	7 793	12	1	7 793	9 072
5	9	340 825	4	1	681 650	894 240
9	9	31 650 345	8	1	126 601 380	141 087 744
2	11	1 753	1	1	1 753	1 936
3	11	70 141	2	1	70 141	84 700
3	15	5 790 005	2	1	5 790 005	6 019 200

from $\mathbb{F}_2[y]$, whose roots are the primitive 9th roots of unity. So, we take 1, y, y^2, y^3, y^4, y^5 as an F-basis of E. Now let τ be the F-endomorphism of E that is represented by the matrix

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

with respect to this basis.

1. Let $X := y + 1$. Then $\tau(X) = \tau(y + 1) = y^4 + 1$ and $\tau(y^4 + 1) = y^4 + y$ and therefore
$$(\tau^2 + \tau + 1)(X) = y^4 + y + y^4 + 1 + y + 1 = 0$$
shows that $X = y + 1$ has τ-order $x^2 + x + 1$. The τ-orders of $Y := y^4 + 1$ and $X + Y = y^4 + y$ are equal to $x^2 + x + 1$ as well.

2. Let $A := y^3$. Then $\tau(A) = y^4 + y^2 + y$ and $\tau(y^4 + y^2 + y) = 0$, which shows that A has τ-order x^2. Also, $B := y^4 + y^3 + y^2 + y$ has τ-order x^2 while $A + B$ has τ-order x.

3. Let $C := y^3 + y^2 + 1$. Then $\tau(C) = y^5 + y^3 + y + 1$ and $\tau(y^5 + y^3 + y + 1) = C$, which shows that C has τ-order $x^2 + 1 = (x + 1)^2$. Also, $D := y^5 + y^3 + y + 1$ has τ-order $(x + 1)^2$ while $C + D = y^5 + y^2 + y$ has τ-order $x + 1$.

This altogether implies that the minimal polynomial of τ is equal to

$$m_\tau = (x^2 + x + 1)x^2(x + 1)^2,$$

and that τ is a cyclic $\mathbb{F}_2$-endomorphism. Next, let $z := y + 1$. Then z is a primitive element of E. All the τ-generators are as follows, expressed as powers of z:

$$\begin{aligned} X + A + C &= z^{57}, & X + A + D &= z^{28}, \\ X + B + C &= z^{35}, & X + B + D &= z^{15}, \\ Y + A + C &= z^{51}, & Y + A + D &= z^{30}, \\ Y + B + C &= z^{56}, & Y + B + D &= z^{7}, \\ X + Y + A + C &= z^{54}, & X + Y + A + D &= z^{45}, \\ X + Y + B + C &= z^{63}, & X + Y + B + D &= z^{27}. \end{aligned}$$

Since none of the z-exponents of these elements is relatively prime to $2^6 - 1 = 63$, i.e. either divisible by 3 or by 7, none of these elements is primitive. This shows that there is no primitive τ-generator and therefore the pair $(2, 6)$ is not extensive.

9 The sieving method

As mentioned in the introduction, Cohen and Huczynska's proof of the primitive normal basis theorem [3] is based on a sieving method. We adopt this approach (culminating in Theorem 9.2 below) for the present problem as well, and argue that the following 12 pairs are extensive:

$q = 2$: $n \in \{22, 28\}$

$q = 3$: $n \in \{16, 18\}$

$(q, n) = (4, 14)$

$q = 5$: $n \in \{8, 10, 12\}$

$(q, n) = (7, 9)$

$q = 9$: $n \in \{6, 8\}$

$(q, n) = (11, 6)$

Recall the definitions of the functions P and Γ_g from Section 3, see (3.1) and (3.4), where $g \in F[x]$ is a monic divisor of m_τ. We define

$$\#(g) := \sum_{w \in E} P(w)\Gamma_g(w). \tag{9.1}$$

Then $\#(1) = \varphi(q^n - 1)$ is just the number of primitive elements, and for $g \neq 1$ the function $\#(g)$ counts the number of primitive elements $w \in E$ with the property that w is not of the form $r(\tau)(v)$ for every irreducible divisor r of g. On the lines of the argumentation of the proof of Proposition 3.3, one may derive the following result which corresponds to [3, Corollary 3.2] (again, ω is the number of distinct prime divisors of $q^n - 1$).

Proposition 9.1 *With $g(x) \in F[x]$ being a monic divisor of m_τ, it holds that*

$$\frac{q^n - 1}{\varphi(q^n - 1)} \cdot \#(g) \;\leq\; \frac{\phi_q(g)}{q^{\deg(g)}} \cdot \left(q^n - \varepsilon_g + (2^\omega - 1)(2^{\Omega(g)} - 1)\sqrt{q^n}\right)$$

and

$$\frac{q^n - 1}{\varphi(q^n - 1)} \cdot \#(g) \;\geq\; \frac{\phi_q(g)}{q^{\deg(g)}} \cdot \left(q^n - \varepsilon_g - (2^\omega - 1)(2^{\Omega(g)} - 1)\sqrt{q^n}\right),$$

where $\varepsilon_g = 1$, if $g = 1$, and $\varepsilon_g = 0$, otherwise. Furthermore, $\Omega(g)$ denotes the number of distinct monic irreducible F-divisors of g. □

This generalized counting function is necessary in order to formulate the **basic sieving inequality** (9.2); compare with [3, Proposition 4.1]: Assume that $g_1, \ldots, g_s$ are monic divisors of g (all polynomials from $F[x]$) such that $\mathrm{lcm}(g_1, \ldots, g_s) = g$ and $\gcd(g_i, g_j) = g_0$ for all $i \neq j$. Then $g_1, \ldots, g_s$ is called a *list of complementary divisors of g with common factor g_0*. In that case, one has

$$\#(g) \;\geq\; \left(\sum_{i=1}^{s} \#(g_i)\right) - (s-1) \cdot \#(g_0). \tag{9.2}$$

Proposition 9.1 and (9.2) imply the announced sufficient criterion for the existence of a primitive τ-generator.

Theorem 9.2 *Let $g_1, \ldots, g_s$ be a list of complementary divisors of m_τ with common factor g_0. Let*

$$lhs := \sum_{i=1}^{s} \frac{\phi_q(g_i)}{q^{\deg(g_i)}} \cdot \left(q^n - (2^\omega - 1)(2^{\Omega(g_i)} - 1)\sqrt{q^n}\right)$$

and

$$rhs := (s-1) \cdot \frac{\phi_q(g_0)}{q^{\deg(g_0)}} \cdot \left(q^n - \varepsilon_{g_0} + (2^\omega - 1)(2^{\Omega(g_0)} - 1)\sqrt{q^n}\right).$$

Assume that lhs is greater than rhs. Then there exists a primitive τ-generator for $E = \mathbb{F}_{q^n}$ over $F = \mathbb{F}_q$. □

Observe that this argument only depends on the factorization pattern of the list of complementary divisors. When $g_0 = 1$, then $rhs = (s-1) \cdot (q^n - 1)$. We are able to successfully apply this argument in the subsequent situations; in the Subsections 9.1-9.7 (i.e. for the seven pairs $(11, 6)$, $(9, 8)$, $(9, 6)$, $(7, 9)$, $(5, 12)$, $(5, 10)$, $(5, 8)$) we could always choose $g_0 = 1$.

As in Proposition 3.3, we let Ω_τ be the number of distinct monic irreducible divisors of m_τ in $\mathbb{F}_q[x]$.

9.1 The pair $(q, n) = (11, 6)$

Here, $\omega = 6$. If $\Omega_\tau \leq 4$, then Proposition 3.3 gives the existence of a primitive τ-generator. It therefore remains to consider the cases where $\Omega_\tau = 5$ or $\Omega_\tau = 6$. In all these cases we shall take $s = 3$, and the polynomials g_i are quadratic for $i = 1, 2, 3$. The right hand side (rhs) in Theorem 9.2 always attains the value 3 543 120.

1. Assume first that $\Omega_\tau = 6$. Then m_τ splits into distinct linear factors. Then the left hand side (lhs) in Theorem 9.2 is equal to 3 768 600.

2. Assume next that $\Omega_\tau = 5$. There are two possible factor patterns of m_τ to be considered, namely $[1, 1, 1, 1, 1^2]$ or $[1, 1, 1, 1, 2]$. In the first case, let g_1 and

g_2 have factor pattern $[1,1]$, while the pattern of g_3 is $[1^2]$; then the left hand side of Theorem 9.2 gives 4 046 680. In the second case, we let g_1 and g_2 have type $[1,1]$, while g_3 has type $[2]$; then the left hand side of Theorem 9.2 gives 4 186 160.

Altogether, this shows that $(11,6)$ is extensive.

9.2 The pair $(q,n) = (9,8)$

Here, $\omega = 5$. If $\Omega_\tau \leq 7$, then Proposition 3.3 gives the existence of a primitive τ-generator. Therefore, it remains to consider the case where $\Omega_\tau = 8$, and this means that m_τ splits into eight distinct linear factors. Let now $s = 4$, and let each g_i (for $i = 1,2,3,4$) have factor pattern $[1,1]$. Then, in Theorem 9.2 the left hand side is equal to 134 120 448 while the right hand side is equal to 129 140 160. This shows that $(9,8)$ is extensive.

9.3 The pair $(q,n) = (9,6)$

Here, again $\omega = 5$. If $\Omega_\tau \leq 4$, then Proposition 3.3 implies the existence of a primitive τ-generator. It remains to consider the cases $\Omega_\tau = 5$ or $\Omega_\tau = 6$. In both cases we take $s = 3$; furthermore, the g_i are quadratic polynomials and g_1 and g_2 have factor pattern $[1,1]$, each. The right hand side gives 1 062 880 in both cases.

1. Assume first that $\Omega_\tau = 6$. Then m_τ splits into distinct linear factors. In Theorem 9.2 the left hand side is then equal to 1 099 008.

2. Assume next that $\Omega_\tau = 5$. There are two possible factor patterns, namely $[1,1,1,1,1^2]$ or $[1,1,1,1,2]$. In the first case, with g_3 having pattern $[1^2]$, the left hand side of Theorem 9.2 gives 1 184 976. In the second case, with g_3 having pattern $[2]$, the left hand side of Theorem 9.2 is 1 235 232.

Altogether, this shows that $(9,6)$ is extensive.

9.4 The pair $(q,n) = (7,9)$

Here, we have $\omega = 5$. If $\Omega_\tau \leq 7$, Proposition 3.3 gives the existence of a primitive τ-generator. It therefore remains to consider the cases where $\Omega_\tau \geq 8$. But then $\Omega_\tau = 8$, and m_τ splits as $[1,1,1,1,1,1,1,2]$. We try again $s = 3$ and build g_1 and g_2 with pattern $[1,1,1]$, while g_3 has pattern $[1,2]$. Then in Theorem 9.2 the left hand side attains the value $49\,088\,204 + 33\,386\,865 = 82\,475\,069$, while the right hand side is equal to 80 707 212. This shows that $(7,9)$ is extensive.

9.5 The pair $(q, n) = (5, 12)$

Here, $\omega = 6$. If $\Omega_\tau \leq 7$, then Proposition 3.3 implies the existence of a primitive τ-generator. Hence, it remains to consider the cases where $\Omega_\tau \geq 8$. But then $\Omega_\tau = 8$, and m_τ splits as $[1, 1, 1, 1, 1^2, 2, 2, 2]$ or as $[1, 1, 1, 1, 2, 2, 2, 2]$.

In the first case, we take $s = 4$ and build four patterns of type $[1, 2]$ for the g_i. Then in Theorem 9.2 the left hand side is equal to 740 928 000 while the right hand side is equal to 732 421 872.

For the second case, we take $s = 3$ and build groups of the form $[1^2]$ and $[1, 1, 1, 1]$ and $[2, 2, 2]$. Then in Theorem 9.2 the left hand side is equal to the sum of the three values 194 525 000, 93 952 000 and 209 903 616 which altogether is 498 380 616, and which is greater than 488 281 248, the evaluation of the right hand side of Theorem 9.2.

Consequently, $(5, 12)$ is extensive.

9.6 The pair $(q, n) = (5, 10)$

Here, $\omega = 5$. If $\Omega_\tau \leq 6$, then Proposition 3.3 gives the existence of a primitive τ-generator. It therefore remains to consider the cases where $\Omega_\tau \geq 7$. But then $\Omega_\tau = 7$, and m_τ splits as $[1, 1, 1, 1, 1^2, 2, 2]$ or as $[1, 1, 1, 1, 2, 2, 2]$. We always take $s = 2$ and therefore obtain $5^{10} - 1 = 9\,765\,624$ in the right hand side.

Consider first the case $[1, 1, 1, 1, 2, 2, 2]$. Build the two groups $[1, 1, 1, 1]$ and $[2, 2, 2]$. Then in Theorem 9.2 the left hand side is equal to the sum of 3 404 800 and 8 040 038.4, which is 11 444 838.4. Let m_τ next have pattern $[1, 1, 1, 1, 1^2, 2, 2]$. Build the groups $[1, 1, 1, 1, 1^2]$ and $[2, 2]$. Then in Theorem 9.2 the left hand side is equal to the sum of the two values 2 215 936 and 8 732 160, which is 10 948 096.

Consequently, $(5, 10)$ is extensive.

9.7 The pair $(q, n) = (5, 8)$

Here, $\omega = 4$. If $\Omega_\tau \leq 5$, then Proposition 3.3 gives the existence of a primitive τ-generator. It therefore remains to consider the cases where $\Omega_\tau \geq 6$. But then $\Omega_\tau = 6$ and m_τ splits as $[1, 1, 1, 1, 1^2, 2]$, or as $[1, 1, 1, 1, 2, 2]$, or as $[1, 1, 1, 1, 1, 3]$. We always take $s = 2$, whence the right hand side of Theorem 9.2 is $5^8 - 1 = 390\,624$.

Consider first $[1, 1, 1, 1, 1^2, 2]$ grouped as $[1, 1, 1, 1, 1^2]$ and $[2]$; then the left hand side of Theorem 9.2 gives 398 768. If m_τ has pattern $[1, 1, 1, 1, 2, 2]$, take the blocks $[1, 1, 1, 1]$ and $[2, 2]$; the left hand side of Theorem 9.2 then attains the value 436 480. Assume finally that m_τ has pattern $[1, 1, 1, 1, 1, 3]$; take the blocks $[1, 1, 1, 1, 1]$ and $[3]$; then the left hand side of Theorem 9.2 gives 410 968.

This altogether shows that $(5, 8)$ is extensive.

9.8 The pair $(q, n) = (4, 14)$

Here, $\omega = 4$. If $\Omega_\tau \leq 8$, then Proposition 3.3 shows the existence of a primitive τ-generator. Hence, it remains to consider the cases where $\Omega_\tau \geq 9$. But then $\Omega_\tau = 9$, and m_τ definitely splits as $[1, 1, 1, 1, 2, 2, 2, 2, 2]$. We are going to take g_0 of type $[1, 1, 1, 1]$ (so for the first time $g_0 \neq 1$) and $s = 2$ with g_1 of type $[1, 1, 1, 1, 2, 2, 2]$ and g_2 of type $[1, 1, 1, 1, 2, 2]$. The left hand side of Theorem 9.2 gives a value which is greater than 92 373 696. The right hand side is equal to 89 833 536.

This shows that $(4, 14)$ is extensive.

9.9 The pair $(q, n) = (3, 18)$

Here, $\omega = 6$. If $\Omega_\tau \leq 8$, then Proposition 3.3 gives the existence of a primitive τ-generator. It therefore remains to consider the cases where $\Omega_\tau \geq 9$. But then $\Omega_\tau = 9$, and m_τ definitely splits as $[1, 1, 1, 2, 2, 2, 3, 3, 3]$. We are going to take g_0 of type $[1, 1, 1]$ and $s = 2$ with g_1 of type $[1, 1, 1, 2, 2, 2]$ and g_2 of type $[1, 1, 1, 3, 3, 3]$. The left hand side of Theorem 9.2 then gives the sum of 64 364 544 and 81 833 856, which is 146 198 400, while the right hand side is equal to 117 363 168.

This shows that $(3, 18)$ is extensive.

9.10 The pair $(q, n) = (3, 16)$

Here, $\omega = 5$. If $\Omega_\tau \leq 7$, then Proposition 3.3 gives the existence of a primitive τ-generator. Therefore, it remains to consider the cases where $\Omega_\tau \geq 8$. But then $\Omega_\tau = 8$, and there are three possible factor patterns for m_τ. In any case, we take $s = 2$. In the first two cases we take g_0 of type $[1, 1, 1]$, and let g_0 have type $[1, 1, 1^2]$ in the last case.

1. Assume first the pattern is $[1, 1, 1, 2, 2, 2, 3, 4]$. Take g_1 of type $[2, 2, 2, 1, 1, 1]$ and g_2 of type $[3, 4, 1, 1, 1]$. We divide both sides of the inequality in Theorem 9.2 by the common term $(3 - 1)^3 \cdot 3^{8-3}$ and then obtain on the left a sum which is greater than $3\,236 + 5\,326 = 8\,562$, while the right hand side gives $3^8 + 31 \cdot 7 = 6\,778$.

2. Consider next the pattern $[1, 1, 1, 2, 2, 3, 3, 3]$. Take now g_1 of type $[2, 2, 1, 1, 1]$ and g_2 of type $[3, 3, 3, 1, 1, 1]$. Again, we divide both sides of the inequality in Theorem 9.2 by the common term $(3 - 1)^3 \cdot 3^{8-3}$ and then obtain on the left a sum which is greater than $4\,424 + 4\,114 = 8\,538$, while the right hand side gives again 6 778.

3. Consider finally the pattern $[1, 1, 1^2, 2, 2, 2, 3, 3]$. We are going to take g_1 of type $[1, 1, 1^2, 2, 2, 2]$ and g_2 of type $[1, 1, 1^2, 3, 3]$. Dividing both sides of the inequality in Theorem 9.2 by the common term $(3 - 1)^2 \cdot (3^2 - 3) \cdot 3^{8-2-2}$ gives on the left a sum greater than $3\,236 + 5\,192 = 8\,428$, while the right hand side yields once more 6 778.

Table 10: Factor patterns for the pair $(2, 28)$.

m_τ	g_0	$\overline{g}_1$	$\overline{g}_2$
$[1, 1, 2, 3, 3, 4, 4, 4, 6]$	$[1, 1]$	$[3, 3, 6]$	$[2, 4, 4, 4]$
$[1, 1^2, 2, 3, 3, 4, 4, 4, 5]$	$[1, 1^2]$	$[3, 3, 5]$	$[2, 4, 4, 4]$
$[1, 1^3, 2, 3, 3, 4, 4, 4, 4]$	$[1, 1^3]$	$[3, 3, 4]$	$[2, 4, 4, 4]$
$[1^2, 1^2, 2, 3, 3, 4, 4, 4, 4]$	$[1^2, 1^2]$	$[3, 3, 4]$	$[2, 4, 4, 4]$
$[1, 1, 2^2, 3, 3, 4, 4, 4, 4]$	$[1, 1]$	$[2^2, 3, 3]$	$[4, 4, 4, 4]$

This altogether shows that $(3, 16)$ is extensive.

9.11 The pair $(q, n) = (2, 22)$

Here, $\omega = 4$. If $\Omega_\tau \leq 7$, then the character sum criterion gives the existence of a primitive τ-generator. Therefore, it remains to consider the cases where $\Omega_\tau \geq 8$. But then $\Omega_\tau = 8$ and there is only one possible factor pattern for m_τ, namely $[1, 1, 2, 3, 3, 4, 4, 4]$. We are going to take g_0 of type $[1, 1]$ and $s = 2$ with g_1 of type $[1, 1, 2, 3, 3]$ and g_2 of type $[1, 1, 4, 4, 4]$. We divide both sides of the inequality in Theorem 9.2 by the common term 2^{11-2} and then obtain on the left a sum which is greater than $795 + 1\,304 = 2\,099$, while the right hand side gives $2^{11} + 15 \cdot 3 = 2\,078$.

This shows that $(2, 22)$ is extensive.

9.12 The pair $(q, n) = (2, 28)$

Here, $\omega = 6$. If $\Omega_\tau \leq 8$, then the character sum argument gives the existence of a primitive τ-generator. Therefore, it remains to consider the cases where $\Omega_\tau \geq 9$. But then $\Omega_\tau = 9$. Nevertheless, there are five possible factor patterns for m_τ. For every pattern, the strategy is the same. We let $s = 2$ and g_0 have a pattern of the form $[1^a, 1^b]$. Furthermore, let $\overline{g}_1 := g_1/g_0$ and $\overline{g}_2 := g_2/g_0$; the factor patterns of $\overline{g}_1$ have the form $[3, 3, 4]$ or $[3, 3, 5]$ or $[3, 3, 6]$ or $[2^2, 3, 3]$, while that of $\overline{g}_2$ have the form $[2, 4, 4, 4]$ or $[4, 4, 4, 4]$. Table 10 shows all possibilities.

We may always divide out the common term $\sqrt{2^{28}} \cdot \phi_2(g_0)/q^{\deg(g_0)}$; after that the relevant summands are as follows:

- $[2^2, 3, 3]$ gives a value greater than 8 286,
- $[3, 3, 4]$ gives a value greater than 10 358,
- $[3, 3, 5]$ gives a value greater than 10 703,
- $[3, 3, 6]$ gives a value greater than 10 876,
- $[2, 4, 4, 4]$ gives a value greater than 7 672,

- $[4, 4, 4, 4]$ gives a value greater than 9 590.

The right hand sides are always equal to $2^{14} + 63 \cdot 3 = 16\,573$. Now, for the left hand side,

- pattern $[1, 1, 2, 3, 3, 4, 4, 4, 6]$ gives $10\,876 + 7\,672 = 18\,548$,
- pattern $[1, 1^2, 2, 3, 3, 4, 4, 4, 5]$ gives $10\,703 + 7\,672 = 18\,375$,
- pattern $[1, 1^3, 2, 3, 3, 4, 4, 4, 4]$ and pattern $[1^2, 1^2, 2, 3, 3, 4, 4, 4, 4]$ both give $10\,358 + 7\,672 = 18\,030$,
- pattern $[1, 1, 2^2, 3, 3, 4, 4, 4, 4]$ also gives $8\,286 + 9\,590 = 17\,876$.

This altogether shows that the pair $(2, 28)$ is extensive.

We have not been able to successfully apply the sieving method to the remaining pairs.

10 The geometric approach

The geometric approach (ga) is a development of the improved counting argument from Section 7. It works well at least for small values of n (say $n \leq 6$), and has been successfully applied in order to determine good lower bounds for the number of *primitive normal* elements in cubic and quartic extensions of Galois fields in [8] (see also [9]). Similar to the spirit of the handling of the pairs $(5, 6)$ and $(3, 6)$ below, we currently explore the number of *primitive completely normal* elements in six-dimensional extensions of Galois fields. (An element $w \in \mathbb{F}_{q^n}$ is completely normal over $\mathbb{F}_q$, if it is normal over every intermediate field $\mathbb{F}_{q^d}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, see [7].) Basically, as in Section 7, we consider the extension E as $PG_{n-1}(F)$, and for an F-endomorphism τ, we let $\mathcal{C}_\tau$ be the configuration of points which are covered by the maximal τ-invariant subspaces of E (see (7.3) and the remark afterwards). We now have a closer look at the subspace arrangement $\mathcal{C}_\tau$. Instead of a systematic treatment, we have looked individually at the remaining pairs and could succesfully apply (ga) to prove the extensiveness of five further pairs, namely

$$(q, n) \in \{(4, 3), (3, 4), (7, 4), (3, 6), (5, 6)\}.$$

We use the terminology as introduced in Section 7.

10.1 The pair $(4, 3)$

The number of primitive elements is equal to $\varphi(4^3 - 1) = 36$. Consider E as a projective plane $\Pi = PG_2(F)$ of order 4. The number of points of that plane is $4^2 + 4 + 1 = 21$. Since a primitive point contains exactly 3 primitive elements (see Proposition 7.1), we conclude that there are altogether $36/3 = 12$ primitive points.

If m_τ has pattern [3] or [2, 1] or [1^3] or [1^2, 1], then the number of points covered by the configuration $\mathcal{C}_\tau$ is equal to 0 or 6 or 5 or 9, respectively. This is less than 12. It therefore remains to consider those τ where m_τ has pattern [1, 1, 1], leading to exactly 12 points in the configuration $\mathcal{C}_\tau$ (which coincides with the 36 elements that are not τ-generators, then). We want to prove that there is a primitive point outside $\mathcal{C}_\tau$.

Assume that this is not the case. Let $m_\tau = abc$. Then the three lines V_{ab}, V_{ac} and V_{bc} cover exactly $3 \cdot (4 + 1) - 3 = 12$ points, and these must all be primitive by assumption. Next, consider E also as a module with respect to the Frobenius automorphism σ over F. We have $m_\sigma = x^3 - 1 = (x-1)(x-\lambda)(x-\lambda^2)$, where $\lambda \in F$ is a primitive 3rd root of unity. Let u have σ-order[3] $x-\lambda$ and let v have σ-order $x-\lambda^2$. Then u and v are primitive 9th roots of unity, whence the corresponding points are not primitive. Consequently, the line G through u and v, which in fact is the kernel of the (E, F)-trace-mapping, intersects the configuration $\mathcal{C}_\tau$ in three distinct points; these are the points on G that are different from Fu and Fv, hence represented by $u + \lambda v$ and $u + \lambda^2 v$ and $u + v$, all primitive by assumption. Since every element of a primitive point is primitive as well, this gives rise to $3 \cdot 3 = 9$ primitive elements in E that have (E, F)-trace equal to 0 (in fact with σ-order $x^2 + x + 1$). These together with the six primitive 9th roots of unity and the zero-element determine then all of the 4^2 elements of the (E, F)-trace kernel. However, the 7th cyclotomic polynomial splits over F as $\Phi_7(x) = (x^3 + x^2 + 1)(x^3 + x + 1)$; the trace coefficient of the second factor is equal to 0, and we therefore obtain a contradiction, because there are also three primitive 7th roots of unity in the kernel of the (E, F)-trace mapping. The pair $(4, 3)$ is therefore extensive.

10.2 The pair $(3, 4)$

Here, we have $\omega = 2$ and $\varphi(3^4 - 1) = 32$. Unfortunately, the criterion from Proposition 3.3 fails whenever $\Omega_\tau \geq 2$. The multiplier $\varphi(R) \cdot S$ (see Proposition 7.1 and the remark afterwards) only gives 1, i.e. a reduction to the simple counting argument. Anyway, for a given τ, with pattern Δ_τ and with configuration $\mathcal{C}_\tau$, we let $\delta := \varphi(3^4 - 1) - |\mathcal{C}_\tau|$ be the *discrepancy* (compare with Proposition 7.2). If positive, the existence of a τ-generator is guaranteed. The relevant data is summarized in Table 11.

In order to cope with the remaining cases, our geometric reasoning is as follows. Consider E first as a projective space $\Pi = PG_3(F)$. Every primitive F-point has two primitive elements. Hence Π contains $32/2 = 16$ primitive F-points.

Next, let $K = \mathbb{F}_9$ be the intermediate field of E/F, and consider E now as a projective line $\Gamma = PG_1(K)$ over K. Since $|K^*| = 3^2 - 1 = 8$, every primitive K-point has exactly 8 primitive elements. This shows that there are $32/8 = 4$ primitive K-points. Any point in Γ gives rise to a projective line $PG_1(F)$ (with exactly $q + 1 = 4$ points of type F). In the present situation, any primitive K-

[3]Instead of σ-order often the notion **q-order** is used.

Table 11: The pair $(3,4)$.

Δ_τ	$\phi_3(\Delta_\tau)$	$\lvert\mathcal{C}_\tau\rvert = 3^4 - 1 - \phi_3(\Delta_\tau)$	δ
$[2,2]$	$(3^2-1)^2 = 64$	16	$32 - 16 = 16$
$[1,3]$	$2 \cdot (3^3-1) = 52$	28	$32 - 28 = 4 = 84$
$[1^2,2]$	$(3^2-3) \cdot (3^2-1) = 48$	32	$32 - 32 = 0$
$[1^2,1^2]$	$(3^2-3)^2 = 36$	44	$32 - 44 = -12$
$[1,1,1^2]$	$2^2 \cdot (3^2-3) = 24$	56	$32 - 56 = -24$
$[1,1,2]$	$2^2 \cdot (3^2-1) = 32$	48	$32 - 48 = -16$

point considered as an F-line consists entirely of primitive F-points. The important feature is that pairwise distinct K-points lead to pairwise *skew* F-lines, i.e. they have pairwise empty intersection.

So, consider the factor patterns from above with nonpositive discrepancy δ. There are at most three different irreducible factors in m_τ, and the corresponding maximal τ-invariant subspaces may therefore be imbedded into at most three F-hyperplanes in Π. Because of the skewness of the K-points, any such hyperplane can contain at most one primitive F-line. Consequently, there is at least one (from the four) primitive F-lines which is not contained in some of these hyperplanes. Take one of these lines. It intersects any hyperplane in exactly one point (by reasons of dimension). Since there are four points on the line, but at most three hyperplanes, there is a point of that line which is outside the union of the hyperplanes. This point is primitive, and since the configuration $\mathcal{C}_\tau$ is covered by the hyperplanes, this gives a primitive τ-generator.

The pair $(q,n) = (3,4)$ is therefore extensive.

10.3 The pair $(7,4)$

First of all, $7^4 - 1 = 2^5 \cdot 3 \cdot 5^2$ gives $\omega = 3$ and $\varphi(7^4-1) = 16 \cdot 2 \cdot 20 = 640$. The criterion from Proposition 3.3 fails whenever $\Omega_\tau \geq 3$.

But, when $\Omega_\tau = 3$, then Proposition 7.2 shows the existence of a primitive τ-generator: Here, $7 - 1 = 2 \cdot 3$ and therefore the relevant multiplier is equal to $\varphi(R) \cdot S = \varphi(3) \cdot 2 = 4$. If the pattern is $[1,1,2]$ then $\lvert\mathcal{C}_\tau\rvert = (q^4-1) - (q^2-1)(q-1)^2 = 2400 - 48 \cdot 36 = 672$; if the pattern is $[1,1,1^2]$, then $\lvert\mathcal{C}_\tau\rvert = (q^4-1) - (q^2-q)(q-1)^2 = 2400 - 42 \cdot 36 = 888$. Since already $\frac{888}{7-1} \cdot 4 = 592 < 640$, τ-generators always exist, when $\Omega_\tau = 3$.

It remains to consider the case where $\Omega_\tau = 4$, in which case $\Delta_\tau = [1,1,1,1]$, and therefore $\lvert\mathcal{C}_\tau\rvert = (q^4-1) - (q-1)^4 = 2\,400 - 1\,296 = 1\,104$. Here, Proposition 7.2 fails, because $\frac{1\,104}{6} \cdot 4 = 736 > 640$. So, consider $E = \mathbb{F}_{7^4}$ first as a projective line $\Gamma = PG_1(K)$ over $K = \mathbb{F}_{7^2}$. Since $7^2 - 1 = 48 = 2^4 \cdot 3$, the K-multiplier (see Proposition 7.1) is here equal to $\varphi(R) \cdot S = \varphi(3) \cdot 2^4 = 2^5 = 32$. And this means that every primitive K-point contains exactly 32 elements, and Γ therefore contains

exactly $640/32 = 20$ primitive K-points (and a total number of $7^2 + 1 = 50$ points of type K). When considering E as a projective space $\Pi = PG_3(F)$ over $F = \mathbb{F}_7$, every K-point is an F-line consisting of $7 + 1 = 8$ points of type F. Since the F-multiplier is equal to 4 (see above), the 20 primitive elements of a primitive K-point are distributed into $20/4 = 5$ primitive F-points. I.e., every primitive K-point as an F-line contains exactly 5 primitive F-points.

Now, the configuration $\mathcal{C}_\tau$ corresponding to τ is a union of four hyperplanes of Π (since $\Delta_\tau = [1, 1, 1, 1]$). Because of the skewness of the K-points (compare with the case $(q, n) = (3, 4)$), any hyperplane contains at most one (possibly primitive) K-point. So there are plenty of primitive K-points which are not contained in one of the hyperplanes. Let G be such a point, considered as an F-line. Then G intersects each of the four hyperplanes in one F-point. Consequently, G carries at least $8 - 4 = 4$ points that are outside the configuration $\mathcal{C}_\tau$. But as G has five primitive F-points, at least one of these is a primitive one, and this shows that $(7, 4)$ is extensive.

Observe that the argument even shows that there are at least $(20 - 3) \cdot 4 = 68$ primitive τ-generators.

10.4 The pair $(5, 6)$

We have $5^6 - 1 = 15\,624 = 2^3 \cdot 3^2 \cdot 7 \cdot 31$ and therefore $\varphi(5^6 - 1) = 4 \cdot 6 \cdot 6 \cdot 30 = 4\,320$ and $\omega = 4$. The character sum criterion of Proposition 3.3 therefore fails when $\Omega_\tau \geq 4$. On the other hand, for this pair, Ω_τ is at most 5.

The factor patterns with $\Omega_\tau = 4$ are

$$[1, 1, 1, 1^3],\ [1, 1, 1^2, 1^2],\ [1, 1, 1^2, 2],\ [1, 1, 1, 3],\ [1, 1, 2, 2],\ [1, 1, 1, 3],$$

and the only pattern with $\Omega_\tau = 5$ is $[1, 1, 1, 1, 2]$. The geometric argument will be applicable to all these cases.

Let $E = \mathbb{F}_{5^6}$ and $K = \mathbb{F}_{5^3}$ and $F = \mathbb{F}_5$. Consider E first as a projective line $\Gamma = PG_1(K)$ over K. Since $|K^*| = 124 = 2^2 \cdot 31$, the K-multiplier (see once more Proposition 7.1) is equal to $\varphi(R) \cdot S = \varphi(31) \cdot 2^2 = 120$, and therefore every primitive K-point of Γ contains exactly 120 primitive elements (and four elements with a smaller order). When however considering E as a projective space $\Pi = PG_5(F)$, then every primitive F-point has exactly 4 primitive elements (because the F-multiplier is $\varphi(R) \cdot S = \varphi(1) \cdot 2^2 = 4$). Since K has dimension three over F, each K-point Q gives rise to a projective F-plane of order 5, i.e. with $5^2 + 5 + 1 = 31$ points. If Q is primitive, then, as an F-plane, Q has exactly 30 primitive F-points, i.e. all except one.

Now, in any of the above cases, the configuration $\mathcal{C}_\tau$ can be covered by a configuration $\mathcal{H}_\tau$ of at most five F-hyperplanes of Π. Since the F-planes corresponding to the K-points of Γ are pairwise skew, each such $\mathcal{H}_\tau$-hyperplane can contain at most one K-point. So, from the $4320/120 = 36$ primitive K-points there are at least $36 - 5 = 31$ which are not part of one of these hyperplanes. Any of these primitive K-points Q, considered as an F-plane, intersects each hyperplane of $\mathcal{H}_\tau$

in an F-line. So, the maximal number of F-points from Q that are contained in $\mathcal{C}_\tau$ is $5 \cdot (6-1)+1 = 26$; this corresponds to the worst case of five lines meeting in a point (which in fact cannot occur, since all hyperplanes together have only trivial intersection). Anyway, there are at least five F-points of Q which are outside the configuration $\mathcal{C}_\tau$, and at least four of them are primitive.

Thus, $(5, 6)$ is extensive.

10.5 The pair $(3, 6)$

The geometric situation in this case is comparable with that from the pair $(5, 6)$. Let us start with the fact that $3^6 - 1 = 728 = 2^3 \cdot 7 \cdot 13$, and therefore $\varphi(3^6-1) = 288$ and $\omega = 3$. Hence Proposition 3.3 fails when $\Omega_\tau \geq 3$. On the other hand, $\Omega_\tau \leq 4$, since $q = 3$. When $\Omega_\tau = 4$, the possible factor patterns are

$$[1, 1, 1^2, 2] \quad \text{and} \quad [1, 1, 1, 3] \quad \text{and} \quad [1, 1, 2, 2].$$

There are however plenty of factor patterns when $\Omega_\tau = 3$ (namely 12), but we do not have to look at them individually.

Let $E = \mathbb{F}_{3^6}$ and $K = \mathbb{F}_{3^3}$ and $F = \mathbb{F}_3$. Consider E first as a projective line $\Gamma = PG_1(K)$ over K. Since $|K^*| = 26 = 2 \cdot 13$, the K-multiplier is equal to $\varphi(R) \cdot S = \varphi(13) \cdot 2 = 24$, and therefore every primitive K-point of Γ contains exactly 24 primitive elements (and two elements with a smaller order). The total number of primitive K-points of Γ is $288/24 = 12$. When considering E as a projective space $\Pi = PG_5(F)$, every primitive F-point has 2 primitive elements (because here the F-multiplier is $\varphi(R) \cdot S = \varphi(1) \cdot 2 = 2$). Since K has dimension three over F, each K-point Q gives rise to a projective F-plane of order 3, i.e. with $3^2 + 3 + 1 = 13$ points. If Q is primitive, then, as an F-plane, Q has exactly $24/2 = 12$ primitive F-points, i.e. all its F-points are primitive, except one.

Assume now, that $\Omega_\tau = 3$. In any of these cases, the configuration $\mathcal{C}_\tau$ is contained in the union of three hyperplanes (corresponding to the maximal divisors of m_τ). So, from the 12 primitive K-points there are at least 9 which are not contained in one of these hyperplanes. Every other K-point Q, when considered as an F-plane, intersects each hyperplane in a line. Now, the three intersection lines of Q with the arrangement $\mathcal{H}_\tau$ of hyperplanes are either three lines through a point or a triangle. In the first case, $3 \cdot (4-1)+1 = 10$ of the F-points of Q are covered by $\mathcal{H}_\tau$; in the second case, there are covered only $3 \cdot (3+1) - 3 = 9$ of the F-points of Q. So, there are at least three F-points of Q that are outside $\mathcal{C}_\tau$. At least two of these F-points are primitive ones, and therefore primitive τ-generators exist for all these patterns, i.e. when $\Omega_\tau = 3$.

Consider finally the case where $\Omega_\tau = 4$. Each of the patterns now gives rise to a configuration that can be covered by an arrangement $\mathcal{H}_\tau$ of four hyperplanes. Again, there are plenty of primitive K-points that are not contained in one of the covering hyperplanes $(12 - 4 = 8)$. Take such a primitive K-point Q.

1. If the pattern is $[1,1,1,3]$, let H_1, H_2, H_3 and A be the corresponding maximal subspaces of $\mathcal{C}_\tau$. Since the dimension of A is 3 (giving rise to a projective plane), at most one of the possible eight points Q has a line together with A (skewness). So, the typical intersection of Q (considered as an F-plane) with $\mathcal{C}_\tau$ are three lines and a point. Hence, the number of F-points of Q that are outside $\mathcal{C}_\tau$ is at least $13-(10+1)=2$, at least one of which is primitive.

2. If the pattern is $[1,1,2,2]$, let H_1, H_2 and L_1, L_2 be the corresponding maximal subspaces of $\mathcal{C}_\tau$. The worst case arising here is that a primitive K-point Q intersects each of these maximal spaces in a line. But since $H_1 \cap H_2 \cap L_1 \cap L_2$ is the zero-space, the four lines cannot meet in a point, and therefore there are at most $4\cdot 4-3-2=11$ F-points of Q that are inside $\mathcal{C}_\tau$. From the remaining two F-points at least one is primitive.

3. The same argument as in (2) applies to the pattern $[1,1,1^2,2]$ as well.

Hence, $(3,6)$ is extensive.

11 Concluding remarks

Let us finally return to the discussion about the work of Hsu and Nan [11] from the end of Section 1. After all, it makes sense to call a pair (q,n) **Carlitz-extensive**, provided that for every $z \in \mathbb{F}_{q^n}$ there exists a primitive element which generates $\mathbb{F}_{q^n}$ as a cyclic $\mathbb{F}_q$-vector space with respect to the $\mathbb{F}_q$-linear mapping $\gamma_z : v \mapsto zv + v^q$. As explained in Section 1, every extensive pair is Carlitz-extensive as well. As a part of his master thesis [6], Thomas Gruber, a former student of mine, found out by a complete enumeration that from the 23-element set

$$(\mathcal{C} \setminus \{(2,2)\}) \cup \mathcal{U}$$

(see Section 1) the 16 pairs

$$(2,4),(2,6),(2,8),(2,10),(2,12),(2,14),(2,15),(2,16),$$
$$(3,2),(3,8),(3,10),(4,6),(4,9),(5,2),(5,4),(7,6)$$

are in fact Carlitz-extensive. Thomas Gruber used an implementation within the computer algebra system `Sage` (which is a free open-source mathematics software system, see http://www.sagemath.org/). Given that the pair $(3,12)$ is not contained in Hsu and Nan's list of possible exceptions, there altogether just remain six pairs for which the status of Carlitz-extensiveness is not decided:

$$(2,18),(2,20),(2,24),(4,10),(4,12),(8,8).$$

References

[1] L. Carlitz, Primitive roots in a finite field, *Trans. Amer. Math. Soc.* **73** (1952), 373–382.

[2] S. D. Cohen, Gauss sums and a sieve for generators of Galois fields, *Publ. Math. Debrecen* **56** (2000), 293–312.

[3] S. D. Cohen and S. Huczynska, The primitive normal basis theorem—without a computer, *J. London Math. Soc.* (2) **67** (2003), 41–56.

[4] S. D. Cohen and S. Huczynska, The strong primitive normal basis theorem, *Acta Arith.* **143** (2010), 299–332.

[5] H. Davenport, Bases for finite fields, *J. London Math. Soc.* **43** (1968), 21–39.

[6] T. Gruber, *Eine Programmierumgebung zur Unterstützung der Grundlagenforschung im Bereich der endlichen Körper*, Masterarbeit, Institut für Mathematik der Universität Augsburg, Augsburg, 2013.

[7] D. Hachenberger, *Finite fields: Normal bases and completely free elements*, Kluwer Academic Publishers, Boston, 1997.

[8] D. Hachenberger, Primitive normal bases for quartic and cubic extensions: A geometric approach, *Designs, Codes and Cryptography* **77** (2015), 335–350.

[9] D. Hachenberger, Ovoids and primitive normal bases for quartic extensions of Galois fields, *submitted* (2015).

[10] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields.* Clarendon Press, Oxford (1998), 2nd ed.

[11] C. N. Hsu and T. T. Nan, A generalization of the primitive normal basis theorem, *J. Number Theory* **131** (2011), 146–157.

[12] S. Huczynska, Existence results for finite field polynomials with specified properties, In "Finite Fields and Their Applications: Character Sums and Polynomials", Eds: Charpin, P., Pott, A. and Winterhof, A., De Gruyter, Berlin (2013), 65–87.

[13] D. Jungnickel, *Finite fields: Structure and arithmetics*, Bibliographisches Institut, Mannheim, 1993.

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

[15] R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, MA, 1983.

[16] H. Lüneburg, *Vorlesungen über Lineare Algebra*, Bibl. Institut, Mannheim, 1993.

(Received 2 Dec 2014; revised 17 Nov 2015)