Designs, Codes and Cryptography manuscript No.
(will be inserted by the editor)

Variations of the Primitive Normal Basis Theorem

Giorgos Kapetanakis · **Lucas Reis**

August 5, 2018

Abstract The celebrated Primitive Normal Basis Theorem states that for any $n \geq 2$ and any finite field $\mathbb{F}_q$, there exists an element $\alpha \in \mathbb{F}_{q^n}$ that is simultaneously primitive and normal over $\mathbb{F}_q$. In this paper, we prove some variations of this result, completing the proof of a conjecture proposed by Anderson and Mullen (2014).

Keywords primitive elements · normal bases · k-normal elements · high-order elements

Mathematics Subject Classification (2000) 12E20 · 11T30

1 Introduction

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a power of a prime p and let $n \geq 1$ be a positive integer. We recall that the multiplicative group $\mathbb{F}_{q^n}^*$ is cyclic and any generator of this group is called *primitive*. Primitive elements have numerous applications in areas like cryptography; perhaps the most notable such example is the widely used Diffie-Hellman key exchange [4]. Also, $\mathbb{F}_{q^n}$ can be regarded as a $\mathbb{F}_q$-vector space of dimension n: an element $\alpha \in \mathbb{F}_{q^n}$ is *normal* over $\mathbb{F}_q$ if $\mathscr{B} = \{\alpha, \ldots, \alpha^{q^{n-1}}\}$ is a basis of $\mathbb{F}_{q^n}$. In this case, $\mathscr{B}$ is called a *normal basis*. For many practical applications, such as cryptography and computer algebra systems, it is more efficient to work with normal bases. For a comprehensive coverage on normal bases and their importance, both in theory and applications, we refer to [5] and the references therein.

Sometimes it is also desired that such normal bases are composed by primitive elements. The Primitive Normal Basis Theorem states that there exists a normal basis composed by

Giorgos Kapetanakis
Faculty of Engineering and Natural Sciences, Sabancı Üniversitesi. Ortha Mahalle, Tuzla 34956, İstanbul, Turkey
E-mail: gnkapet@gmail.com
Lucas Reis
School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa ON (Canada), K1S 5B6
Permanent address: Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte MG (Brazil), 30123-970.
E-mail: lucasreismat@gmail.com

primitive elements in any finite field extension. The proof of this result was first presented by Lenstra and Schoof [8], who performed some minimal calculations with computers. Their techniques were later enhanced by sieving techniques by Cohen and Huczynska [3] who achieved a completely computer-free proof. Recently, Hachenberger [6], using geometric tools, established sharp estimates for the number of such bases.

A variation of normal elements was recently introduced by Huczynska et al. [7], yielding k-normal elements. There are many equivalent definitions for such elements and here we pick the most natural in the sense of vector spaces.

Definition 1.1 For $\alpha \in \mathbb{F}_{q^n}$, consider the set $S_\alpha = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ comprising the conjugates of α by the action of the Galois group of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The element α is *k-normal over $\mathbb{F}_q$* if the $\mathbb{F}_q$-vector space V_α generated by S_α has dimension $n-k$, i.e., $V_\alpha \subseteq \mathbb{F}_{q^n}$ has co-dimension k.

Following this definition, 0-normal elements are just the usual normal elements and $0 \in \mathbb{F}_{q^n}$ is the only n-normal element. Also, we note that the definition of k-normal depends strongly on the base field that we are working and, unless otherwise stated, $\alpha \in \mathbb{F}_{q^n}$ is k-normal if it is k-normal over $\mathbb{F}_q$.

We recall that the multiplicative group $\mathbb{F}_{q^n}^*$ has q^n-1 elements and, for $\alpha \in \mathbb{F}_{q^n}^*$, the multiplicative order of $\alpha \in \mathbb{F}_{q^n}^*$ is the least positive integer d such that $\alpha^d = 1$. We write $d = \mathrm{ord}(\alpha)$. Since $\alpha^{q^n-1} = 1$, d is always a divisor of q^n-1. For instance, the primitive elements are the ones of order q^n-1. We know that, for each divisor e of q^n-1, there exist $\varphi(e)$ elements in $\mathbb{F}_{q^n}$ with order e, where φ is the *Euler Phi* function. We introduce a variation of primitive elements in finite fields.

Definition 1.2 For $\alpha \in \mathbb{F}_{q^n}^*$ and r a divisor of q^n-1, α is *r-primitive* if $\mathrm{ord}(\alpha) = \frac{q^n-1}{r}$.

From definition, the 1-primitive elements correspond to the primitive elements in the usual sense. Motivated by the Primitive Normal Basis Theorem, in 2014, Anderson and Mullen propose the following problem (see [10], Conjecture 3).

Conjecture 1.3 (Anderson-Mullen) Suppose that $p \geq 5$ is a prime and $n \geq 3$. Then, for $a = 1,2$ and $k = 0,1$, there exists some k-normal element $\alpha \in \mathbb{F}_{p^n}$ with multiplicative order $(p^n-1)/a$.

In other words, if $p \geq 5$ and $n \geq 3$, there exists an element $\alpha \in \mathbb{F}_{p^n}$ that is simultaneously a-primitive and k-normal, for $a = 1,2$ and $k = 0,1$. We notice that the case $(a,k) = (1,0)$ is the Primitive Normal Basis Theorem, which holds for arbitrary finite fields. Also, the case $(a,k) = (1,1)$ was recently proved for arbitrary q and $n \geq 3$ (see [11]), yielding the Primitive 1-normal Theorem.

In this paper, we complete the proof of Conjecture 1.3 above, adding the case $a = 2$. In fact, we prove a stronger version of this conjecture.

Theorem 1.4 *Let q be a power of a prime p and let n be a positive integer.*

1. *If $p \geq 3$ and $n \geq 2$, there exists an element $\alpha \in \mathbb{F}_{q^n}$ that is simultaneously 2-primitive and normal over $\mathbb{F}_q$, with the sole genuine exceptions $(q,n) = (3,2),(3,4)$.*
2. *If $p \geq 3$ and $n \geq 3$, there exists an element $\alpha \in \mathbb{F}_{q^n}$ that is simultaneously 2-primitive and 1-normal over $\mathbb{F}_q$. Such an element exists also in the case $(q,n) = (3,2)$, while there do not exist such elements when $n = 2$ and $q > 3$.*

Moreover, in Theorem 5.4, we prove that in item 2 of the above theorem, we could also assume that the element in question is zero-traced over $\mathbb{F}_q$.

We make a brief comment on the techniques used in this paper. We use standard characteristic functions to describe a special class of 2-primitive, k-normal elements (for $k = 0, 1$) over finite fields: these characteristic functions can be described via *character sums*. This characterization provides inequality-like conditions for the existence of such elements and then we study these inequalities in both theoretical and computational aspects.

2 Preliminaries

In this section, we provide a background material for k-normal elements, as well as some particular artihmetic functions and their polynomial version.

Definition 2.1 (a) Let f be a monic polynomial with coefficients in $\mathbb{F}_q$. The *Euler Phi Function* for polynomials over $\mathbb{F}_q$ is given by

$$\Phi(f) = \left| \left(\frac{\mathbb{F}_q[x]}{\langle f \rangle} \right)^* \right|,$$

where $\langle f \rangle$ is the ideal generated by $f(x)$ in $\mathbb{F}_q[x]$.

(b) If t is a positive integer (or a monic polynomial over $\mathbb{F}_q$), $W(t)$ denotes the number of square-free (monic) divisors of t.

(c) If f is a monic polynomial with coefficients in $\mathbb{F}_q$, the *Polynomial Möbius Function* μ_q is given by $\mu_q(f) = 0$ if f is not square-free and $\mu_q(f) = (-1)^r$ if f writes as a product of r distinct irreducible factors over $\mathbb{F}_q$.

2.1 Additive order of elements and k-normals

If $f \in \mathbb{F}_q[x]$, $f = \sum_{i=0}^{s} a_i x^i$, we define $L_f(x) = \sum_{i=0}^{s} a_i x^{q^i}$ as the q-associate of f. Also, for $\alpha \in \mathbb{F}_{q^n}$, set $f \circ \alpha = L_f(\alpha) = \sum_{i=0}^{s} a_i \alpha^{q^i}$. As follows, the q-associates have a good behavior through basic operations of polynomials.

Lemma 2.2 ([9], Theorem 3.62) *Let $f, g \in \mathbb{F}_q[x]$. The following hold:*

(i) $L_f(L_g(x)) = L_{fg}(x)$,
(ii) $L_f(x) + L_g(x) = L_{f+g}(x)$.

Notice that, for any element α in some extension of $\mathbb{F}_q$, $(x^n - 1) \circ \alpha = \alpha^{q^n} - \alpha = 0$ if and only if $\alpha \in \mathbb{F}_{q^n}$. If we set $\mathscr{I}_\alpha = \{g(x) \in \mathbb{F}_q[x] \mid g(x) \circ \alpha = 0\}$, the previous lemma shows that $\mathscr{I}_\alpha$ is an ideal of $\mathbb{F}_q[x]$. In particular, for $\alpha \in \mathbb{F}_{q^n}$, $x^n - 1 \in \mathscr{I}_\alpha$ and so $\mathscr{I}_\alpha$ is a non zero ideal, hence is generated by a polynomial, say $m_\alpha(x)$. Notice that, if we require $m_\alpha(x)$ to be monic, such $m_\alpha(x)$ is unquely determined by α. We define $m_\alpha(x)$ as the $\mathbb{F}_q$-*order* of α. This concept works as an "additive" analogue of multiplicative order over finite fields.

Clearly, for $\alpha \in \mathbb{F}_{q^n}$, $m_\alpha(x)$ divides $x^n - 1$ and then its degree is at most n. For instance, if $\deg(m_\alpha(x)) = 0$, then $m_\alpha(x) = 1$ and $\alpha = 0$. The following result shows a connection between k-normal elements and their $\mathbb{F}_q$-order.

Proposition 2.3 ([7], Theorem 3.2) *Let $\alpha \in \mathbb{F}_{q^n}$. Then α is k-normal if and only if $m_\alpha(x)$ has degree $n-k$.*

For instance, normal elements $\alpha \in \mathbb{F}_{q^n}$ are the ones such that $m_\alpha(x) = x^n - 1$. The previous proposition shows that the existence of k-normal elements depends on the existence of a polynomial of degree $n-k$ dividing x^n-1 over $\mathbb{F}_q$. In fact, according to Theorem 3.5 of [7], if $g \in \mathbb{F}_q[x]$ is a divisor of x^n-1 degree k, there exist $\Phi(g)$ elements $\alpha \in \mathbb{F}_q$ with $m_\alpha(x) = g$.

Since $x-1$ divides x^n-1 for any $n \geq 1$, we see that 1-normal elements exist in any extension of $\mathbb{F}_q$. Clearly, this also implies the existence of $(n-1)$-normal elements. Recall that $0 \in \mathbb{F}_{q^n}$ is n-normal and that 0-normal elements always exist. These are the only values of k for which the existence of k-normal elements is guaranteed in any finite field extension. In fact, suppose that n is a prime and q is primitive $\pmod n$: the polynomial x^n-1 factors as $(x-1)(x^{n-1}+\cdots+x+1)$ over $\mathbb{F}_q$. In particular, from the previous proposition, there are no k-normal elements in $\mathbb{F}_{q^n}$ for any $1 < k < n-1$. Of course, in this paper, we are only interested in 0 and 1-normal elements.

2.2 Application of the method of Lenstra and Schoof

Here we present a modern adoption of the traditional method of Lenstra and Schoof [8] in the characterization of elements in $\mathbb{F}_{q^n}$ with special properties like normal, primitive and of a given prescribed trace over some subfield $\mathbb{F}_{q^m}$ of $\mathbb{F}_{q^n}$. However, we start with the concept of *freeness* that is absent in the original proof of Lenstra and Schoof.

Definition 2.4 1. If m divides q^n-1, an element $\alpha \in \mathbb{F}_{q^n}^*$ is *m-free* if $\alpha = \beta^d$ for any divisor d of m implies $d = 1$.
2. If $m \in \mathbb{F}_q[x]$ divides x^n-1, an element $\alpha \in \mathbb{F}_{q^n}$ is *m-free* if $\alpha = h \circ \beta$ for any divisor h of m implies $h = 1$.

From definition, the primitive elements correspond to the (q^n-1)-free elements. Also, the (x^n-1)-free elements are just the normal elements. Using the concept of freeness, we characterize special classes of 1-normal elements, via trace functions. First, we have the following lemma.

Lemma 2.5 ([7], Theorem 5.4) *Let α be any element in $\mathbb{F}_{q^n}$ and let $f(x) = m_\alpha(x)$ be its $\mathbb{F}_q$-order. For any divisor $g(x)$ of x^n-1, the following are equivalent:*

(a) α is $g(x)$-free,
(b) $g(x)$ and $\frac{x^n-1}{f(x)}$ are relatively prime.

As follows, we show that we have a characterization of elements $\alpha \in \mathbb{F}_{q^n}$ for which $m_\alpha(x) = \frac{x^n-1}{x-1}$.

Proposition 2.6 *Let q be a power of a prime p and $n = p^k u$, where $k \geq 0$ and $\gcd(u,p) = 1$. Write $T(x) = \frac{x^u-1}{x-1}$. Then $\alpha \in \mathbb{F}_{q^n}$ is such that $m_\alpha(x) = \frac{x^n-1}{x-1}$ if and only if α is $T(x)$-free and $\beta = \mathrm{Tr}_{q^n/q^{p^k}}(\alpha)$ is such that $m_\beta(x) = \frac{x^{p^k}-1}{x-1}$.*

Proof If $m_\alpha(x) = \frac{x^n-1}{x-1}$, since $\beta = \mathrm{Tr}_{q^n/q^{p^k}}(\alpha) = \frac{x^n-1}{x^{p^k}-1} \circ \alpha$, it follows that $m_\beta(x) = \frac{x^{p^t}-1}{x-1}$. Conversely, suppose that $m_\beta(x) = \frac{x^{p^t}-1}{x-1}$ and $\beta = \mathrm{Tr}_{q^n/q^{p^k}}(\alpha)$. Clearly $\frac{x^n-1}{x-1} \circ \alpha = \frac{x^{p^k}-1}{x-1} \circ (\frac{x^n-1}{x^{p^k}-1} \circ \alpha) = \frac{x^{p^k}-1}{x-1} \circ \beta = 0$. Since α is $T(x)$-free, it follows from Lemma 2.5 that $m_\alpha(x) = T(x)^{p^k}(x-1)^d$ for some $d \geq 0$ with $d \leq p^k-1$. Since $m_\beta(x) = \frac{x^{p^k}-1}{x-1}$, from the minimality of m_β we have $d = p^k-1$, i.e. $m_\alpha(x) = \frac{x^n-1}{x-1}$. □

In the case when n is divisible by p^2, as noticed in [11], we have an alternative characterization for such 1-normal elements.

Proposition 2.7 *Suppose that $n = p^2 s$ and let $\alpha \in \mathbb{F}_{q^n}$ such that $\mathrm{Tr}_{q^n/q^{ps}}(\alpha) = \beta$. Then $m_\alpha = \frac{x^n-1}{x-1}$ if and only if $m_\beta = \frac{x^{ps}-1}{x-1}$.*

The proof of this proposition is quite simple and can be found in Lemma 5.2 of [11].

2.3 Some characteristic functions

The concept of *freeness* derives some characteristic functions for primitive and normal elements. We pick the notation of [7].

Multiplicative component. $\int\limits_{d|m} \eta_d$ stands for the sum $\sum_{d|m} \frac{\mu(d)}{\varphi(d)} \sum_{(d)} \eta_d$, where μ and φ are the Möbius and Euler functions for integers, respectively, η_d is a typical multiplicative character of $\mathbb{F}_{q^n}$ of order d, and the sum $\sum_{(d)} \eta_d$ runs over all the multiplicative characters of order d.

Additive component. χ is the canonical additive character on $\mathbb{F}_{q^n}$, i.e.

$$\chi(\omega) = \lambda(\mathrm{Tr}_{q^n/q}(\omega)), \quad \omega \in \mathbb{F}_{q^n},$$

where λ is the canonical additive character of $\mathbb{F}_q$ to $\mathbb{F}_p$. Given $\beta \in \mathbb{F}_{q^n}$, we set $\chi_\beta(\omega) = \chi(\beta\omega)$ for any $\omega \in \mathbb{F}_{q^n}$. Then χ_β is another additive character of $\mathbb{F}_{q^n}$ and, in fact, any additive character of $\mathbb{F}_{q^n}$ is of this form. In this context, for a monic divisor $D \in \mathbb{F}_q[x]$ of $x^n - 1$, χ_β has $\mathbb{F}_q$-order D if $\beta \in \mathbb{F}_{q^n}$ has $\mathbb{F}_q$-order D. Here, Δ_D denotes the set of all $\beta \in \mathbb{F}_{q^n}$ such that χ_β has $\mathbb{F}_q$-order D. For instance, $\Delta_1 = \{0\}$ and $\Delta_{x-1} = \mathbb{F}_q^*$. Furthermore, it is well-known that

$$|\Delta_D| = \Phi(D).$$

Following our notation, $\int\limits_{D|T} \chi_{\delta_D}$ stands for the sum

$$\sum_{D|T} \frac{\mu_q(D)}{\Phi(D)} \sum_{(\delta_D)} \chi_{\delta_D},$$

where μ_q and Φ are the Möbius and Euler functions for polynomials over $\mathbb{F}_q$ respectively, χ_{δ_D} is a typical additive character of $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$-order D and the sum $\sum_{(\delta_D)} \chi_{\delta_D}$ runs over all the additive characters of $\mathbb{F}_q$-order D, i.e. all $\delta_D \in \Delta_D$.

For each divisor t of $q^n - 1$ and each monic divisor D of $x^n - 1$, set $\theta(t) = \frac{\varphi(t)}{t}$ and $\Theta(D) = \frac{\Phi(D)}{q^{\deg D}}$. The sums above yield characteristic functions.

Theorem 2.8 ([7], Section 5.2)

1. *For $w \in \mathbb{F}_{q^n}^*$ and t be a positive divisor of $q^n - 1$,*

$$\omega_t(w) = \theta(t) \int_{d|t} \eta_d(w) = \begin{cases} 1 & \text{if } w \text{ is } t\text{-free,} \\ 0 & \text{otherwise.} \end{cases}$$

2. *For $w \in \mathbb{F}_{q^n}$ and D be a monic divisor of x^n-1,*

$$\Omega_D(w) = \Theta(D)\int_{E|D}\chi_{\delta_E}(w) = \begin{cases} 1 & \text{if } w \text{ is } D\text{-free,} \\ 0 & \text{otherwise.} \end{cases}$$

More specifically, for $t = q^n-1$ and $D = x^n-1$, we obtain characteristic functions for primitive and normal elements, respectively. As usual, we may extend the multiplicative characters to 0 by setting $\eta_1(0) = 1$, where η_1 is the trivial multiplicative character and $\eta(0) = 0$ if η is not trivial. For a more detailed account of the above, we refer the interested reader to [2] and the references therein.

2.3.1 Characteristic function for traces

For any divisor m of n, $\mathbb{F}_{q^m}$ is a subfield of $\mathbb{F}_{q^n}$. Let

$$T_{m,\beta}(w) = \begin{cases} 1 & \text{if } \mathrm{Tr}_{q^n/q^m}(w) = \beta, \\ 0 & \text{otherwise.} \end{cases}$$

We need a character sum formula for $T_{m,\beta}$. Let λ and λ_m be the canonical additive characters of $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$, respectively: the character λ lifts λ_m and χ to $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^n}$, respectively. In other words, $\lambda_m(w) = \lambda(\mathrm{Tr}_{q^m/q}(w))$ and $\chi(w) = \lambda(\mathrm{Tr}_{q^n/q}(w)) = \lambda(\mathrm{Tr}_{q^m/q}(\mathrm{Tr}_{q^n/q^m}(w))) = \lambda_m(\mathrm{Tr}_{q^n/q^m}(w))$, since the trace function is transitive. We observe that $T_{m,\beta}$ can be written as

$$T_{m,\beta}(w) = \frac{1}{q^m}\sum_{d\in\mathbb{F}_{q^m}}\lambda_m(d(\mathrm{Tr}_{q^n/q^m}(w)-\beta)) = \frac{1}{q^m}\sum_{d\in\mathbb{F}_{q^m}}\lambda_m(d\cdot\mathrm{Tr}_{q^n/q^m}(w-\alpha)),$$

for any $\alpha \in \mathbb{F}_{q^n}$ such that $\mathrm{Tr}_{q^n/q^m}(\alpha) = \beta$, since

$$\sum_{d\in\mathbb{F}_{q^m}}\lambda_m(d\cdot\mathrm{Tr}_{q^n/q^m}(w-\alpha)) = q^m$$

if and only if $\mathrm{Tr}_{q^n/q^m}(w) = \mathrm{Tr}_{q^n/q^m}(\alpha) = \beta$ and, otherwise, this sum equals 0. In particular,

$$T_{m,\beta}(w) = \frac{1}{q^m}\sum_{d\in\mathbb{F}_{q^m}}\chi_d(w-\alpha) = \frac{1}{q^m}\sum_{d\in\mathbb{F}_{q^m}}\chi_d(w)\chi_d(\alpha)^{-1}.$$

2.4 Character sums estimates

Here we provide some character sum estimates that are further used.

Lemma 2.9 ([9], Theorem 5.41) *Let χ be an additive character of $\mathbb{F}_{q^n}$ and $f \in \mathbb{F}_{q^n}[x]$ be a monic polynomial of positive degree, not of the form $g(x)^p - g(x) + y$ for any $g \in \mathbb{F}_{q^n}[x]$. Suppose that e is the number of distinct roots of f in its splitting field over $\mathbb{F}_{q^n}$. For every $a \in \mathbb{F}_{q^n}$,*

$$\left|\sum_{c\in\mathbb{F}_{q^n}}\chi(af(c))\right| \leq (e-1)q^{n/2}.$$

Theorem 2.10 ([12], Theorem 2G) *Let η be a multiplicative character of $\mathbb{F}_q$ of order $d \neq 1$ and χ a non-trivial additive character of $\mathbb{F}_q$. If $f, g \in \mathbb{F}_q[x]$ are such that f has exactly m roots and $\deg(g) = n$ with $\gcd(d, \deg(f)) = \gcd(n, q) = 1$, then*

$$\left| \sum_{c \in \mathbb{F}_q} \eta(f(c))\chi(g(c)) \right| \leq (m+n-1)q^{1/2}.$$

3 A character sum formula for special elements in finite fields

The following theorem provides a character sum formula for the number of primitive elements $w \in \mathbb{F}_{q^n}$ such that w^r has various additive freeness and prescribed traces. First, we fix some notation: for any additive character χ and any multiplicative character η of $\mathbb{F}_{q^n}$, $G_r(\eta, \chi)$ stands for the sum $\sum_{w \in \mathbb{F}_{q^n}} \eta(w)\chi(w^r)$.

Theorem 3.1 *Write $n = p^t u$, where $\gcd(u, p) = 1$ and $t \geq 0$. Let r be a divisor of $q^n - 1$, f a divisor of $x^u - 1$ such that f is not divisible by $x - 1$ and let m be a divisor of n. Suppose that $m = 1$ or m is a power of p if $f \neq 1$. For $\beta \in \mathbb{F}_{q^m}$, let $\mathcal{N}(r, f, m, \beta)$ be the number of primitive elements $w \in \mathbb{F}_{q^n}$ such that w^r is f-free and $\mathrm{Tr}_{q^n/q^m}(w^r) = \beta$. Additionally, let $\mathcal{N}(r)$ be the number of primitive elements $w \in \mathbb{F}_{q^n}$ such that w^r is normal (i.e., $(x^n - 1)$-free) over $\mathbb{F}_q$. The following hold.*

1. *If α is any element of $\mathbb{F}_{q^n}$ such that $\mathrm{Tr}_{q^n/q^m}(\alpha) = \beta$ and $a_c = \chi_c(\alpha)^{-1}$, we have the following equality*

$$\frac{\mathcal{N}(r, f, m, \beta)}{\theta(q^n - 1)\Theta(f)} = \frac{1}{q^m} \left[q^n + \sum_{c \in \mathbb{F}_{q^m}} a_c \int_{\substack{d \mid q^n - 1 \\ d \neq 1}} \int_{\substack{D \mid f \\ D \neq 1}} G_r(\eta_d, \chi_{\delta_D + c}) + \sum_{c \in \mathbb{F}_{q^m}^*} a_c \int_{\substack{d \mid q^n - 1 \\ d \neq 1}} G_r(\eta_d, \chi_c) \right].$$

   In particular,

$$\frac{\mathcal{N}(r, f, m, \beta)}{\theta(q^n - 1)\Theta(f)} > q^{n-m} - rq^{n/2} W(q^n - 1) W(f). \tag{1}$$

2. *We have that*

$$\frac{\mathcal{N}(r)}{\theta(q^n - 1)\Theta(x^n - 1)} = q^n + \int_{\substack{d \mid q^n - 1 \\ d \neq 1}} \int_{\substack{D \mid x^n - 1 \\ D \neq 1}} G_r(\eta_d, \chi_{\delta_D}).$$

   In particular,

$$\frac{\mathcal{N}(r)}{\theta(q^n - 1)\Theta(x^n - 1)} > q^n - rq^{n/2} W(x^n - 1) W(q^n - 1). \tag{2}$$

Proof We just prove item 1 since item 2 is quite simpler and follows by similar ideas. Combining the characteristic functions for primitivity, f-free and prescribed trace, we obtain the following equality:

$$\mathcal{N}(r, f, m, \beta) = \sum_{w \in \mathbb{F}_{q^n}} \Omega_f(w^r) T_{m,\beta}(w^r) \omega_{q^n - 1}(w),$$

and so

$$\frac{\mathscr{N}(r,f,m,\beta)}{\theta(q^n-1)\Theta(f)} = \frac{1}{q^m}\sum_{c\in\mathbb{F}_{q^m}} a_c \int\limits_{d|q^n-1} \int\limits_{D|f} G_r(\eta_d, \chi_{\delta_D+c}).$$

We first simplify the sum above by eliminating the trivial sums $G_r(\eta_d,\chi_{\delta_D+c})$. We claim that $\delta_D + c \neq 0$, unless $D = 1$ and $c = 0$. For this, we note that for $f = 1$, we only have $D = 1$ and so $\delta_D = 0$, hence $\delta_D + c \neq 0$ unless $c = 0$. If $f \neq 1$, from hypothesis, $m = 1$ or m is a power of p. Since f is not divisible by $x-1$ and $x^m - 1 = (x-1)^m$, δ_D is never an element of $\mathbb{F}_{q^m}$, unless $\delta_D = 0$, i.e., $D = 1$. In particular, since $c \in \mathbb{F}_{q^m}$, it follows that $\delta_D + c \neq 0$ unless $D = 1$ and $c = 0$.

This shows that $G_r(\eta_1,\chi_{\delta_D+c}) = q^n$ if $D = 1$ and $c = 0$ and, otherwise, the orthogonality relations and Lemma 2.9 imply that $G_r(\eta_1,\chi_{\delta_D+c}) = 0$. Also, for $D = 1$, $c = 0$ and $d \neq 1$,

$$G_r(\eta_d,\chi_{\delta_D+c}) = G_r(\eta_d,\chi_0) = 0.$$

In particular, we obtain the following simplified expression:

$$\frac{\mathscr{N}(r,f,m,\beta)}{\theta(q^n-1)\Theta(f)} = \frac{1}{q^m}\left[q^n + \sum_{c\in\mathbb{F}_{q^m}} a_c \int\limits_{\substack{d|q^n-1\\ d\neq 1}} \int\limits_{\substack{D|f\\ D\neq 1}} G_r(\eta_d,\chi_{\delta_D+c}) + \sum_{c\in\mathbb{F}_{q^m}^*} a_c \int\limits_{\substack{d|q^n-1\\ d\neq 1}} G_r(\eta_d,\chi_c)\right],$$

as desired. In the integral notation previously introduced, each term $G_r(\eta_d,\chi_{\delta_D+c})$ comes with a weight $\mu(d)\mu_q(D)$ and, in particular, only the terms with d and D squarefree are relevant in the sum above. We have a similar observations for the sums $G_r(\eta_d,\chi_c)$. Set

$$M_1 = \max_{\substack{D|f, d|q^n-1, c\in\mathbb{F}_{q^m}\\ d,D\neq 1}} |G_r(\eta_d,\chi_{\delta_D+c})| \quad \text{and} \quad M_2 = \max_{\substack{d|q^n-1, c\in\mathbb{F}_{q^m}^*\\ d\neq 1}} |G_r(\eta_d,\chi_c)|.$$

In particular,

$$\left|\sum_{c\in\mathbb{F}_{q^m}} a_c \int\limits_{\substack{d|q^n-1\\ d\neq 1}} \int\limits_{\substack{D|f\\ D\neq 1}} G_r(\eta_d,\chi_{\delta_D+c})\right| \leq (W(q^n-1)-1)(W(f)-1)q^m M_1.$$

Also,

$$\left|\sum_{c\in\mathbb{F}_{q^m}^*} a_c \int\limits_{\substack{d|q^n-1\\ d\neq 1}} G_r(\eta_d,\chi_c)\right| \leq (W(q^n-1)-1)(q^m-1)M_2.$$

From Lemma 2.10, it follows that $M_1, M_2 \leq rq^{n/2}$. Therefore,

$$\frac{\mathscr{N}(r,f,m,\beta)}{\theta(q^n-1)\Theta(f)} > q^{n-m} - rq^{n/2}W(q^n-1)W(f).$$

□

We observe that we have a simple characterization of 2-primitive elements: $\alpha \in \mathbb{F}_{q^n}$ is 2-primitive if and only if $\alpha = w^2$ for some primitive element $w \in \mathbb{F}_{q^n}$. In particular, we obtain the following corollary.

Corollary 3.2 *Write $n = p^t u$, where $\gcd(u,p) = 1$ and $t \geq 0$. The following hold:*

(a) if

$$q^{p^t(u/2-1)} > W(q^n-1)W(x^u-1), \tag{3}$$

then there exist 2-primitive, 1-normal elements in $\mathbb{F}_{q^n}$,

(b) if

$$q^{n/2} > 2W(q^n-1)W(x^u-1), \tag{4}$$

then there exist 2-primitive, normal elements in $\mathbb{F}_{q^n}$,

(c) if $t \geq 1$ and

$$q^{n/2-n/p} > 2W(q^n-1), \tag{5}$$

then for $\beta \in \mathbb{F}_{q^{n/p}}$, there exists a 2-primitive element $\alpha \in \mathbb{F}_{q^n}$ such that $\mathrm{Tr}_{q^n/q^{n/p}}(\alpha) = \beta$.

Proof (a) Let $\beta \in \mathbb{F}_{q^{p^t}}$ be an element with $\mathbb{F}_q$-order $(x-1)^{p^t-1}$. From Proposition 2.6, if there exists a primitive element $\alpha \in \mathbb{F}_{q^n}$ such that α^2 is $\frac{x^u-1}{x-1}$-free and has trace $\mathrm{Tr}_{q^n/q^{p^t}}(\alpha^2) = \beta$, such an α^2 is 2-primitive and 1-normal over $\mathbb{F}_q$. In fact, the $\mathbb{F}_q$-order of α^2 equals $\frac{x^n-1}{x-1}$. In the notation of Theorem 3.1, such element α exists if $\mathscr{N}(2,f,p^t,\beta) > 0$, where $f = \frac{x^u-1}{x-1}$. Since $2W\left(\frac{x^u-1}{x-1}\right) = W(x^u-1)$, from Eq. (1), we have that $\mathscr{N}(2,f,p^t,\beta) > 0$ whenever Eq. (3) holds.

(b) This follows directly by Eq. (2) and observing that $W(x^n-1) = W(x^u-1)$.

(c) This follows directly by Eq. (1) for $\mathscr{N}(2,1,n/p,\beta)$. □

Remark 3.3 We note that the Cohen-Huczynska [3] sieving techniques are applicable in our setting and yield weaker conditions that those appearing above. This could reduce the number of possible exceptions, appearing in the proceeding chapter, but not completely eliminate them. However, for the sake of simplicity and clarity and since our proofs would still be computer-dependent and the final results identical, we chose not to apply them.

We observe that Eq. (3) is always false for $n = p, 2p$. For these cases, we employ a refinement of our main result, using simple combinatorial arguments.

Proposition 3.4 *Let $n = p, 2p$. Then there exist 2-primitive, 1-normal elements in $\mathbb{F}_{q^n}$ in each of the following cases.*

(a) $n = p$ and

$$\frac{q^{p-2}}{\theta(q^p-1)} \leq \frac{q^{p-1}}{2} - q^{p/2}W(q^p-1), \tag{6}$$

(b) $n = 2p$ and

$$\frac{q^{2p-1}}{(q-1)\theta(q^{2p}-1)} \leq \frac{q^{2p-1}}{2} - 2q^pW(q^{2p}-1). \tag{7}$$

Proof We split the proof into cases.

(a) Let N_0 be the number of 2-primitive elements in $\mathbb{F}_{q^p}$ with trace zero over $\mathbb{F}_q$. Following the notation of Theorem 3.1, $\mathscr{N}(2,1,1,0)$ is the number of primitive elements $w \in \mathbb{F}_{q^n}$ for which w^2 has trace zero over $\mathbb{F}_q$. Since $w^2 = w_0^2$ if and only if $w = \pm w_0$, we have that

$$N_0 \geq 1/2 \cdot \mathscr{N}(2,1,1,0). \tag{8}$$

We observe that any element $\alpha \in \mathbb{F}_{q^p}$ with trace zero over $\mathbb{F}_q$ satisfies $L_T(\alpha) = 0$, where $T = \frac{x^p-1}{x-1} = (x-1)^{p-1}$. In particular, the $\mathbb{F}_q$-order of any element in $\mathbb{F}_{q^p}$ with zero trace over $\mathbb{F}_q$ equals $(x-1)^d$ for some $0 \leq d \leq p-1$. Therefore, if there do not exist 2-primitive, 1-normal elements in $\mathbb{F}_{q^p}$, then any 2-primitive element $\alpha \in \mathbb{F}_{q^p}$ with trace zero over $\mathbb{F}_q$ satisfies $L_{T_0}(\alpha) = 0$, where $T_0 = (x-1)^{p-2}$. The equation $L_{T_0}(x) = 0$ has at most q^{p-2} solutions over $\mathbb{F}_{q^p}$ and then we conclude that $N_0 \leq q^{p-2}$. However, according to Eq. (1) and (8),

$$\frac{N_0}{\theta(q^p-1)} = \frac{N_0}{\theta(q^p-1)\Theta(1)} \geq \frac{\mathscr{N}(2,1,1,0)}{2\theta(q^p-1)\Theta(1)} > \frac{q^{p-1}}{2} - q^{p/2}W(q^p-1).$$

Therefore,

$$\frac{q^{p-2}}{\theta(q^p-1)} > \frac{q^{p-1}}{2} - q^{p/2}W(q^p-1).$$

(b) Let N_1 be the number of 2-primitive, $(x+1)$-free elements in $\mathbb{F}_{q^{2p}}$ with trace zero over $\mathbb{F}_q$. Again, since $w^2 = w_0^2$ if and only if $w = \pm w_0$, we have that

$$N_1 \geq 1/2 \cdot \mathscr{N}(2,x+1,1,0). \tag{9}$$

We observe that any element $\alpha \in \mathbb{F}_{q^{2p}}$ with trace zero over $\mathbb{F}_q$ satisfies $L_S(\alpha) = 0$, where $S = \frac{x^{2p}-1}{x-1} = (x+1)^p(x-1)^{p-1}$. In addition, any $(x+1)$-free element of $\mathbb{F}_{q^{2p}}$ has $\mathbb{F}_q$-order divisible by $(x+1)^p$ (see Lemma 2.5). In particular, the $\mathbb{F}_q$-order of an $(x+1)$-free element $\alpha \in \mathbb{F}_{q^{2p}}$ with trace zero over $\mathbb{F}_q$ equals $(x+1)^p(x-1)^d$ for some $d \leq p-1$. Therefore, if there do not exist 2-primitive, 1-normal elements in $\mathbb{F}_{q^{2p}}$, then any 2-primitive, $(x+1)$-free element $\alpha \in \mathbb{F}_{q^{2p}}$ with trace zero over $\mathbb{F}_q$ satisfies $L_{S_0}(\alpha) = 0$, where $S_0 = (x+1)^p(x-1)^{p-2}$. The equation $L_{S_0}(x) = 0$ has at most q^{2p-2} solutions over $\mathbb{F}_{q^{2p}}$ and so we conclude that $N_1 \leq q^{2p-2}$. However, according to Eq. (1) and (9),

$$\begin{aligned}\frac{qN_1}{(q-1)\theta(q^{2p}-1)} = \frac{N_1}{\theta(q^{2p}-1)\Theta(x+1)} &\geq \frac{\mathscr{N}(2,x+1,1,0)}{2\theta(q^{2p}-1)\Theta(x+1)} \\ &> \frac{q^{2p-1}}{2} - 2q^pW(q^{2p}-1).\end{aligned}$$

Therefore,

$$\frac{q^{2p-1}}{(q-1)\theta(q^{2p}-1)} > \frac{q^{2p-1}}{2} - 2q^pW(q^{2p}-1).$$

□

4 Inequality checking methods

In this section, we study the inequalities that arise from Corollary 3.2 and Proposition 3.4. These inequalities guarantee the existence of 2-primitive elements with various additive freeness and prescribed traces. As we further see, the existence of 2-primitive, 1-normal elements in $\mathbb{F}_{q^n}$ can be easily deduced from the existence of 2-primitive elements with prescribed trace over $\mathbb{F}_{q^{n/p}}$ if n is divisible by p^2. In particular, the inequalities in Corollary 3.2 that concern 1-normal elements are further explored only in the cases $t = 0$ and $t = 1$.

The function $W(t)$ plays an important role in the various inequalities of Corollary 3.2. Here we present some estimates on the function $W(t)$ when t is a positive integer or a monic polynomial over $\mathbb{F}_q$. We first observe that, if $w(t)$ denotes the number of distinct prime (monic irreducible) divisors of t, then $W(t) = 2^{w(t)}$. We have the following bounds.

Lemma 4.1 *Let t,a be positive integers and let $p_1,\dots,p_j$ be the distinct prime divisors of t such that $p_i \le 2^a$. Then $W(t) \le c_{t,a}t^{1/a}$, where*

$$c_{t,a} = \frac{2^j}{(p_1\cdots p_j)^{1/a}}.$$

In particular, for $c_t := c_{t,4}$ and $d_t := c_{t,8}$ we have the bounds $c_t < 4.9$ and $d_t < 4514.7$ for every positive integer t.

Proof The statement is an immediate generalization of Lemma 3.3 of [3] and can be proved using multiplicativity. The bounds for c_t and d_t can be easily computed. □

Remark 4.2 We emphasize that the bounds for $c_{t,a}$ are computed considering the extremal case when all the prime numbers $\le 2^a$ actually divide t. Nonetheless, since this extremal case is quite unlikely, the constants c_t and d_t turn out to be quite smaller in most of the cases and are easily computable if t is given. In fact, even when t is not completely given, we may obtain sharper bounds for c_t or d_t. For instance, if q is a power of 5 and $t = q^n - 1$, 5 does not divide $q^n - 1$ and so $d_{q^n-1} = c_{q^n-1,8} < 2760.4$.

When t is a polynomial, we are mostly interested in computing $W(t)$ in the case $t = x^u - 1$. From Lemma 2.11 of [8], we have the following result.

Lemma 4.3 *For every positive integer n, $W(x^n-1) \le 2^{(\gcd(n,q-1)+n)/2}$. Additionally, the bound $W(x^n-1) \le 2^{s(n)}$ holds in the following cases:*

1. $s(n) = \frac{\min\{n,q-1\}+n}{2}$ *for every q,*
2. $s(n) = \frac{n+4}{3}$ *for $q = 3$ and $u \neq 4, 8, 16$,*
3. $s(n) = \frac{n}{3} + 6$ *for $q = 5$.*

In the following subsections, we explore the pairs (q,n) satisfying the inequalities of Corollary 3.2. Our method is based on two main steps.

- **Step 1.** Use the bounds for $W(q^n-1)$ and $W(x^u-1)$ given in Lemmas 4.1 and 4.3; at this point, only a finite number of pairs (q,n) does not satisfy the inequalities.
- **Step 2.** Check the inequalities by semi-direct computations; in general, after this step, the remaining pairs that do not satisfy the inequalities do not have q and n too large.

Remark 4.4 For all the computations that are further mentioned, we used common modern computers, running the SAGEMATH software. We note that the computations of Section 4 needed a few seconds of computer time, with the sole exception of the $n = 4$ case in Subsubsection 4.3.1, which turned out to be a very expensive computation that required a few hours. The computations of Section 5 consumed a few minutes of computer time.

4.1 Inequality for 2-primitive, normal elements

Here we study Eq. (4), that provides a sufficient condition on the existence of normal elements with multiplicative order $\frac{q^n-1}{2}$. For simplicity, we replace $x^u - 1$ by $x^n - 1$, since $W(x^n-1) = W(x^u-1)$ if $n = p^t u$. In other words, we are interested in the following inequality:

$$q^{n/2} > 2W(q^n-1)W(x^n-1). \tag{10}$$

The case $n = 2$ is settled in Lemma 5.1, thus we confine ourselves to the case $n \geq 3$. We first employ **Step 1** with the bounds $W(q^n-1) \leq 4.9q^{n/4}$ and $W(x^n-1) \leq 2^{s(n)}$, where $s(n) = n$ for $q \geq 23$, $s(n) = \frac{n+q-1}{2}$ for $7 \leq q \leq 19$ and $s(n)$ is given as in Lemma 4.3 for $q = 3,5$. In particular, if

$$q^{n/4} > 9.8 \cdot 2^{s(n)}, \tag{11}$$

then Eq. (10) holds. We directly verify that Eq. (11) holds true for the pairs (q,n) presented in Table 1.

q	≥ 336	≥ 157	≥ 100	≥ 74	≥ 51	≥ 27	≥ 23	$[13,19]$	$=11$	$=9$	$=7$	$=5$	$=3$
n	≥ 3	≥ 4	≥ 5	≥ 6	≥ 8	≥ 18	≥ 26	≥ 22	≥ 23	≥ 25	≥ 32	≥ 38	≥ 74

Table 1 Values for q and n such that Eq. (11) holds.

In particular, for each odd prime power q, there exists a constant N_q such that Eq. (10) holds for the pairs (q,n) with $n \geq N_q$, where N_q is obtained from Table 1 and $N_q = 3$ if $q \geq 336$. A finite number of pairs (q,n) are excluded in Table 1 with respect to the region $q \geq 3$ and $n \geq 3$. We proceed to **Step 2**, checking if Eq. (10) holds for these pairs, where the quantity $W(q^n-1)$ is explicitly computed and the bound $W(x^n-1) \leq 2^{(n+\min\{n,q-1\})/2}$ is employed. The exceptions are compiled in Table 2.

n	q	#
3	3 ,5 ,7 ,9 ,11 ,13 ,19 ,23 ,25 ,29 ,31 ,37 ,61	13
4	3 ,5 ,7 ,9 ,11 ,13 ,17 ,19 ,23 ,27 ,29 ,31 ,43	13
5	3 ,5 ,7 ,9, 11	5
6	3 ,5 ,7 ,9, 11, 13	6
7	3 , 5 ,7	3
8	3 ,5, 7 , 9, 11, 13	6
9	3 , 5, 7, 9	4
10	3, 5	2
11	3	1
12	3, 5, 7, 11	4
13	3	1
14	3	1
15	3	1
16	3	1
17	3	1
18	3	1
20	3	1
22	3	1
24	3	1
30	3	1
36	3	1
	Total:	68

Table 2 Pairs (q,n) that may not satisfy Eq. (10).

In conclusion, we obtain the following result.

Proposition 4.5 *Let q be a power of an odd prime and let $n \geq 3$ be a positive integer. With the possible exception of the pairs (q,n) in Table 2, there exists a normal element $\alpha \in \mathbb{F}_{q^n}$ with multiplicative order $\frac{q^n-1}{2}$.*

4.2 Inequality for 2-primitive elements with prescribed trace

Here we study Eq. (5). This inequality provides a sufficient condition for the existence of 2-primitive elements in $\mathbb{F}_{q^n}$ with prescribed trace over $\mathbb{F}_{q^{n/p}}$. Here we are interested in the case when n is divisible by p^2 and q is odd. We write $n = p^2 n_0$, where $n_0 \geq 1$ and $p \geq 3$. In other words, we want to find the pairs (q, n_0) such that

$$q^{n_0(p^2/2-p)} > 2W(q^{p^2 n_0} - 1). \tag{12}$$

We first consider the case $p \geq 5$. Write $q = p^s$ with $s \geq 1$. Employing **Step 1**, with the bound $W(q^{p^2 n_0} - 1) \leq 4.9 q^{p^2 n_0/4}$, we see that if

$$h(p, s, n_0) = q^{n_0 p^2 (1/4 - 1/p)} > 9.8, \tag{13}$$

then Eq. (12) holds, where $h(p, s, n_0) = p^{s n_0 p^2 (1/4 - 1/p)}$. We observe that $h(p, s, n_0)$ is an increasing function on p, s and n_0. Since $h(5,1,2) = h(5,2,1) > 9.8$ and $h(7,1,1) > 9.8$. In particular, Eq. (13) holds for any triple (p, s, n_0), where $p \geq 5$, with the exception of the case $(5,1,1)$. By direct computations, we verify that Eq. (12) holds true for the triple $(5,1,1)$. In particular, we have covered the case $p \geq 5$.

We now consider the case $p = 3$. Write $q = 3^s$, where $s \geq 1$. Employing **Step 1**, with the bound $W(q^{p^2 n_0} - 1) \leq 4514.7 q^{p^2 n_0/8}$, we see that if

$$H(s n_0) = q^{n_0(27/8 - 3)} > 9029.4, \tag{14}$$

then Eq. (12) holds, where $H(m) = 3^{3m/8}$. We observe that $H(m)$ is an increasing function and $H(23) > 9029.4$. In particular, if $s n_0 \geq 23$, then Eq. (14) holds for the pair (q, n_0), where $q = 3^s$. For the remaining cases $s n_0 \leq 22$, we directly verify that Eq. (12) holds for the pairs (q, n_0) with the exception of the ones such that $q^{n_0} = 3^m$ with $m = 1, 2, 4$. This excludes the pairs $(q, n_0) = (3,1), (9,1), (81,1), (3,2), (9,2), (3,4)$. All in all, we obtain the following result.

Proposition 4.6 *Let q be a power of an odd prime p and let $n = p^2 n_0$ with $n_0 \geq 1$. Let β be an arbitrary element of $\mathbb{F}_{q^{n/p}}$. With the possible exception of the pairs*

$$(q, n) = (3,9);\ (9,9);\ (81,9);\ (3,18);\ (9,18);\ (3,36),$$

there exists an element $\alpha \in \mathbb{F}_{q^n}$ with multiplicative order $\frac{q^n - 1}{2}$ such that $\mathrm{Tr}_{q^n/q^{n/p}}(\alpha) = \beta$.

In particular, we obtain the following result.

Corollary 4.7 *Let q be a power of an odd prime p and let $n = p^2 n_0$ with $n_0 \geq 1$. With the possible exception of the pairs*

$$(q, n) = (3,9);\ (9,9);\ (81,9);\ (3,18);\ (9,18);\ (3,36),$$

there exists an 1-normal element $\alpha \in \mathbb{F}_{q^n}$ with multiplicative order $\frac{q^n - 1}{2}$.

Proof Let $\beta \in \mathbb{F}_{q^{n/p}}$ be an element such that $m_\beta = \frac{x^{n/p} - 1}{x - 1}$. From Proposition 4.6, with the possible exceptions of the pairs (q, n) in our statement, there exists an element $\alpha \in \mathbb{F}_{q^n}$ with multiplicative order $\frac{q^n - 1}{2}$ such that $\mathrm{Tr}_{q^n/q^{n/p}}(\alpha) = \beta$. From Proposition 2.7, such an α satisfies $m_\alpha = \frac{x^n - 1}{x - 1}$ and so α is 1-normal. □

4.3 Inequalities for 2-primitive, 1-normal elements

We we provide a detailed study on Eq. (3), i.e., we are interested in the pairs (q,n) such that q is a power of p, $n = p^t \cdot u$ with $\gcd(p,u) = 1$ and

$$q^{p^t(u/2-1)} > W(q^n-1)W(x^u-1).$$

Following Corollary 4.7, we focus on the cases $t = 0$ and $t = 1$.

4.3.1 The case $\gcd(n,p) = 1$

We start with case case $\gcd(n,p) = 1$, i.e., $t = 0$. In other words, we want to study the following inequality

$$q^{n/2-1} > W(q^n-1)W(x^n-1). \tag{15}$$

Employing **Step 1**, with the bounds $W(q^n-1) < 4514.7q^{n/8}$ and $W(x^n-1) \le 2^n$, we see that if

$$q^{3n/8-1} > 4514.7 \cdot 2^n, \tag{16}$$

then Eq. (15) holds true. We directly verify that Eq. (16) holds true for the pairs (q,n) presented in Table 3.

q	$\ge 5.22\times 10^9$	$\ge 8\times 10^5$	$\ge 23{,}370$	$\ge 3{,}514$	$\ge 1{,}076$	≥ 479	≥ 266	≥ 170	≥ 29	≥ 21
n	4	5	6	7	8	9	10	$[11,20]$	$[21,25]$	≥ 26

Table 3 Values for q and n such that Eq. (16) holds.

In particular, for each positive integer $4 \le n \le 25$, there exists a constant M_n such that the pair (q,n) satisfies Eq. (15) if $q \ge M_n$, where M_n is explicitly given in Table 3. Excluding the case $n = 4$, we proceed to **Step 2** and check if Eq. (15) holds true for the pairs (q,n) with $n \le 25$ and $q < M_n$, where $W(q^n-1)$ is explicitly computed and the bound $W(x^n-1) \le 2^{(\gcd(n,q-1)+n)/2}$ is employed. The exceptions are compiled in Table 4. For the case $n = 4$, we observe that the constant $M_4 = 5.22 \cdot 10^9$ is quite large and so we require a sharper estimate in **Step 1**: we employ the bounds $W(x^4-1) \le 16$ and $W(q^4-1) < d_{q^4-1}q^{1/2}$, where the constant d_{q^4-1} is explicitly computed. With these bounds, we observe that within the range $3 \le q < 5.22 \cdot 10^9$, the largest prime power q that do not satisfy Eq. (15) is $q = 1658623$. So we have reduced M_4 to $M_4' = 1658623$. For $q \le M_4'$, we proceed to **Step 2** and check if Eq. (15) holds true for the pairs $(q,4)$. The exceptions are added to Table 4.

From now, we only need to investigate the pairs (q,n) such that $n \ge 26$ and $q < 21$. We make a detailed study on each case $q = 3,5,7,9,11,13,17$ and 19. Essentially, we provide a refinement of Eq. (16) using a bound that is sharper than $d_{q^n-1} < 4514.7$: if q is a power of a prime $p \le 2^8 = 256$, p does not divide q^n-1 and so $d_{q^n-1} = c_{q^n-1,8}$ attains its maximum when q^n-1 is divisible by every prime $r \le 256$ with the exception of $r = p$. If e_q denotes this maximum, from Lemma 4.1, it follows that $W(q^n-1) < e_q \cdot q^{n/8}$. We have that $W(x^n-1) \le 2^{s(n)}$, where $s(n) = \frac{u+q-1}{2}$ or $s(n)$ is given as in Lemma 4.3 for $q \le 5$. Therefore, if

$$q^{3n/8-1} > e_q \cdot 2^{s(n)}, \tag{17}$$

then Eq. (15) holds true. We directly verify that Eq. (17) holds true for the pairs (q,n) presented in Table 5.

n	q	#
4	3, 5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 79, 81, 83, 89, 97, 101, 103, 107, 109, 113, 121, 125, 127, 131, 137, 139, 149, 151, 157, 163, 167, 169, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 243, 251, 257, 263, 269, 277, 281, 283, 289, 293, 307, 311, 313, 317, 331, 337, 343, 347, 349, 353, 359, 361, 367, 373, 379, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 529, 541, 547, 557, 563, 569, 571, 577, 593, 599, 601, 613, 617, 619, 625, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 727, 729, 733, 743, 757, 761, 769, 773, 787, 797, 809, 811, 821, 827, 829, 839, 841, 853, 857, 859, 863, 877, 881, 883, 887, 911, 919, 929, 937, 941, 947, 953, 961, 967, 977, 983, 997, 1009, 1013, 1019, 1021, 1033, 1049, 1061, 1087, 1093, 1097, 1109, 1117, 1123, 1201, 1217, 1223, 1229, 1231, 1237, 1259, 1277, 1289, 1291, 1297, 1301, 1303, 1321, 1327, 1331, 1369, 1373, 1381, 1409, 1427, 1429, 1433, 1453, 1481, 1483, 1487, 1493, 1549, 1553, 1559, 1567, 1583, 1597, 1607, 1609, 1613, 1627, 1637, 1657, 1669, 1681, 1693, 1697, 1699, 1709, 1721, 1723, 1733, 1741, 1747, 1777, 1787, 1789, 1801, 1823, 1847, 1849, 1861, 1871, 1873, 1877, 1889, 1913, 1931, 1933, 1973, 1979, 1993, 1997, 2003, 2017, 2029, 2053, 2069, 2089, 2129, 2141, 2153, 2197, 2209, 2213, 2221, 2293, 2297, 2309, 2333, 2393, 2417, 2437, 2441, 2477, 2521, 2551, 2617, 2621, 2633, 2707, 2729, 2777, 2801, 2843, 2861, 2917, 2939, 2953, 2969, 3011, 3037, 3121, 3125, 3181, 3221, 3229, 3301, 3319, 3323, 3359, 3361, 3373, 3389, 3433, 3481, 3541, 3557, 3583, 3613, 3617, 3637, 3659, 3671, 3673, 3697, 3739, 3761, 3769, 3793, 3821, 3853, 3863, 3877, 3947, 4003, 4027, 4073, 4093, 4217, 4229, 4421, 4649, 4789, 4817, 4957, 4969, 5153, 5237, 5333, 5413, 5521, 5641, 5657, 5701, 5741, 5813, 6073, 6089, 6133, 6257, 6269, 6277, 6323, 6397, 6469, 6481, 6553, 6577, 6709, 6733, 6833, 6889, 6917, 7177, 7193, 7253, 7297, 7309, 7481, 7549, 7561, 7639, 7669, 7717, 7789, 7853, 7867, 7877, 8093, 8117, 8161, 8273, 8377, 8581, 8741, 8861, 9043, 9281, 9941, 10009, 10613, 10789, 10847, 11131, 11437, 11471, 11717, 12433, 12641, 14029, 14281, 14461, 14629, 14633, 14669, 14897, 15053, 15313, 15619, 15817, 16253, 16301, 17389, 19469, 20747, 21013, 21713, 21757, 23561, 24389, 24509, 25117, 25453, 25943, 26417, 29173, 30103, 30269, 30341, 32117, 32381, 32537, 38917, 53129, 59753, 60397, 102829	439
5	3 , 7 , 9 , 11 , 13 , 19, 31, 37, 59 , 61 , 71 , 81 , 101	13
6	5 ,7 ,11 ,13 ,17 ,19, 25,31 ,37	8
7	3 ,5	2
8	3 ,5 ,7 ,9 ,13 ,17 ,25	7
9	5 ,7	2
10	3 ,11	2
11	3	1
12	5, 7, 13	3
13	3	1
14	3	1
16	3	1
17	3	1
20	3	1
22	3	1
	Total:	483

Table 4 Pairs (q,n) with $\gcd(q,n) = 1$ that may not satisfy Eq. (15).

q	3	5	7	9	11	13	17	19
e_q	2589.6	2760.4	2879	2589.6	3046.3	3110.6	3216.7	3261.7
n	≥ 55	≥ 37	≥ 32	≥ 27	≥ 26	≥ 24	≥ 23	≥ 23

Table 5 Values for q and n such that Eq. (17) holds and the explicit value of e_q.

In particular, for each odd prime power $q < 21$, there exists a constant N_q such that the pair (q,n) satisfies Eq. (15) if $n \geq N_q$, where N_q is explicitly given in Table 5. We proceed again to **Step 2** and check if Eq. (15) holds true for the pairs (q,n) with $q < 21$ and $26 \leq n < N_q$, where $W(q^n-1)$ is explicitly computed, the bound $W(x^n-1) \leq 2^{(\gcd(n,q-1)+n)/2}$ is employed for $q > 3$ and the bound $W(x^n-1) \leq 2^{s(n)}$ is employed for $q = 2,3$ with $s(n)$ as in Lemma 4.3; we remark that this lemma does not contain any restriction for $n \geq 26$. After calculations, we do not find additional exceptions. All in all, we obtain the following result.

Proposition 4.8 *Let q be a power of an odd prime and let $n \geq 4$ be a positive integer such that $\gcd(q,n) = 1$. With the possible exception of the pairs (q,n) in Table 4, Eq.* (3) *holds*

true for the pair (q,n)*. In particular, with the possible exception of these pairs, there exists an* 1*-normal element* $\alpha \in \mathbb{F}_{q^n}$ *with multiplicative order* $\frac{q^n-1}{2}$.

4.3.2 The case $n = pu$ *with* $\gcd(u,p) = 1$

We proceed to the case $t = 1$. In other words, we want to study the following inequality

$$q^{p(u/2-1)} > W(q^{pu}-1)W(x^u-1), \tag{18}$$

where $\gcd(u,p) = 1$. We observe that, for $u = 1,2$, this inequality is trivially false for every prime power q. Therefore, we confine ourselves to the case $u \geq 3$. We employ **Step 1** with the bounds $W(q^{pu}-1) < 4514.7q^{pu/8}$ and $W(x^u-1) \leq 2^u$. Write $q = p^s$ with $s \geq 1$. We see that if

$$p^{ps(3u/8-1)} = q^{p(3u/8-1)} > 4514.7 \cdot 2^u, \tag{19}$$

then Eq. (18) holds true. We start with the critical cases $u \leq 6$. We directly verify that Eq. (19) holds true for the pairs (p,s) presented in Table 6.

$u = 3$:

p	5	7	11	13	≥ 17	≥ 29
s	≥ 11	≥ 7	≥ 4	≥ 3	≥ 2	≥ 1

$u = 4$:

p	3	5	7	≥ 11
s	≥ 7	≥ 3	≥ 2	≥ 1

$u = 5$:

p	3	≥ 7
s	≥ 5	≥ 1

$u = 6$:

p	5	≥ 7
s	≥ 2	≥ 1

Table 6 Values for p and s such that Eq. (19) holds with $3 \leq u \leq 6$ and $\gcd(p,u) = 1$.

As before, we proceed to **Step 2** and check if Eq. (18) holds for the excluded triples (u,p,s) in Table 6 with respect to the region $3 \leq u \leq 6$, $s \geq 1$ with $\gcd(p,u) = 1$. The quantity $W(q^{pu}-1)$ is explicitly computed and we employ the trivial bound $W(x^u-1) \leq 2^u$. The exceptions are presented in Table 7.

(u,p)	s	#
(3, 5)	1, 2	2
(4, 3)	1, 2	2
(4, 5)	1	1
(5, 3)	1	1
(8, 3)	1	1
	Total:	7

Table 7 Triples (u,p,s) that may not satisfy Eq. (18) with $\gcd(p,u) = 1$ and $q = p^s$.

We now proceed to the case $u \geq 7$. Again, we write $q = p^s$ with $s \geq 1$. Employing **Step 1** with the bounds $W(q^{pu}-1) < 4.9q^{pu/4}$ and $W(x^u-1) \leq 2^u$, we see that if

$$p^{ps(u/4-1)} = q^{p(u/4-1)} > 4.9 \cdot 2^u, \tag{20}$$

then Eq. (18) holds true. We can easily check that Eq. (20) holds for $s \geq 1$, $p \geq 7$ and $u \geq 7$. So we just need to consider the cases $p \leq 5$. We directly verify that Eq. (20) holds true for the pairs (u,s) presented in Table 8.

$$p=3\text{:}\ \begin{array}{c||c|c} u & [7,9] & \geq 10 \\ \hline\hline s & \geq 3 & \geq 2 \end{array}$$

$$p=5\text{:}\ \begin{array}{c||c|c} u & 7 & \geq 8 \\ \hline\hline s & \geq 2 & \geq 1 \end{array}$$

Table 8 Values of u and s such that Eq. (20) holds with $p \leq 5$ and $\gcd(p,u) = 1$.

Again, we proceed to **Step 2** and check if Eq. (18) holds for the triples (u,p,s) that are excluded in Table 8 with respect to the regions $p = 3$ and $s \geq 2$ and $p = 5$ and $s \geq 1$. For these cases, the quantity $W(q^{pu}-1)$ is explicitly computed and we employ the trivial bound $W(x^u-1) \leq 2^u$. The exceptions are added in Table 7.

In particular, we have covered the cases $q = p^s$, where $q \neq 3$. We now consider the critical cases $q = 3$. As before, we provide a refinement of Eq. (20) using a bound that is sharper than $c_{q^{pu}-1} < 4.9$: for $q = 3$, 3 does not divide $q^{pu}-1$ and so $c_{3^{pu}-1} = c_{3^{pu}-1,4}$ attains its maximum k_3 when $3^{3u}-1$ is divisible by every prime $r \leq 16$ with the exception of $r = 3$. We obtain $k_3 = 3.2$ and, from Lemma 4.1, we have that $W(3^{pu}-1) < 3.2 \cdot 3^{pu/4}$. From Lemma 4.3, for $q = 3$, $W(x^u-1) \leq 2^{s(u)}$, where $s(u) = (u+4)/3$ if $u \neq 4,8,16$ and $s(u) = (u+q-1)/2 = (u+2)/2$ if $u = 4,8,16$. Additionally, looking at Table 8, one can suppose that $u \geq 10$ if $q = 3$. Therefore, if

$$3^{p(u/4-1)} > 3.2 \cdot 2^{s(u)}, \tag{21}$$

then Eq. (18) holds true for $q = 3$. We directly verify that Eq. (21) holds true for any $u \neq 10$ with the possible exception of $u = 16$; for this case, we directly verify that Eq. (18) holds with all the quantities explicitly computed. Therefore, we do not have additional exceptions. All in all, we obtain the following result.

Proposition 4.9 *Let $q = p^s$ be a power of an odd prime p and let n be a positive integer such that $n = pu$ with $u \geq 3$ and $\gcd(p,u) = 1$. With the possible exception of the triples (u,p,s) in Table 7, Eq. (3) holds true for the pair (q,n) with $q = p^s$. In particular, with the possible exception of these pairs, there exists an 1-normal element $\alpha \in \mathbb{F}_{q^n}$ with multiplicative order $\frac{q^n-1}{2}$.*

4.3.3 The critical cases $n = p, 2p$

Here we study Eqs. (6) and (7), that provide sufficient condition for the existence of r-primitive, 1-normal elements in $\mathbb{F}_{q^{pu}}$, where $u = 1,2$ and $\gcd(p,u) = 1$. We confine ourselves to the cases $p \geq 5$ if $u = 1$ and $p \geq 3$ if $u = 2$. We start with the following useful result.

Lemma 4.10 ([11], Lemma A.4) *Suppose that q is a power of a prime p, where $p \geq 5$ or $p = 3$ and $q \geq 27$. For $s \geq 1$, we have*

$$\theta(q^{ps}-1)^{-1} = \frac{q^{ps}-1}{\varphi(q^{ps}-1)} < 3.6\log q + 1.8\log s. \tag{22}$$

We proceed to Eq. (6), i.e., we are interested in the following inequality:

$$\frac{q^{p-2}}{\theta(q^p-1)} \leq \frac{q^{p-1}}{2} - q^{p/2}W(q^p-1). \tag{23}$$

We employ **Step 1** with the bounds $W(q^p-1) \leq 4.9q^{p/4}$ and $\theta(q^p-1)^{-1} \leq 3.6\log q$ (see Eq. (22)). In particular, if

$$3.6\log q \leq q/2 - 4.9q^{2-p/4}, \tag{24}$$

then Eq. (23) holds. If we write $q = p^s$ with $s \geq 1$, we directly verify that Eq. (24) holds for $p = 5$ and $s \geq 6$, $p = 7$ and $s \geq 3$ and for arbitrary s with $p \geq 11$ and $q \geq 24$. For the remaining cases $q = 5^s$ with $s \leq 5$, $q = 7^s$ with $s = 1,2$ and $q = 11,13,17,19,23$ we proceed to **Step 2** and directly verify Eq. (23), where all the quantities are explicitly computed. We arrive in the only exception $p = 5$ and $s = 1$.

Next, we proceed to Eq. (7), i.e., we are interested in the following inequality:

$$\frac{q^{2p-1}}{(q-1)\theta(q^{2p}-1)} \leq \frac{q^{2p-1}}{2} - 2q^pW(q^{2p}-1). \tag{25}$$

We employ **Step 1** with the bounds $W(q^{2p}-1) \leq 4.9q^p$ and $\theta(q^{2p}-1)^{-1} \leq 3.6\log q + 1.25$ with $q \geq 27$ if q is a power of 3 (see Eq. (22)). In particular, if

$$3.6\log q + 1.25 \leq (q-1)\cdot(0.5 - 4.9q^{(2-p)/2}), \tag{26}$$

then Eq. (25) holds. If we write $q = p^s$ with $s \geq 1$, we directly verify that Eq. (26) holds for $p = 3$ and $s \geq 5$, $p = 5$ and $s \geq 3$ and for arbitrary s with $p \geq 7$ and $q \geq 28$. For the remaining cases $q = 3^s$ with $s \leq 4$, $q = 5^s$ with $s = 1,2$ and $q = 7,11,13,17,19,23$ we proceed to **Step 2** and directly verify Eq. (26), where all the quantities are explicitly computed. We arrive in the exceptions $p = 3$ and $s = 1,2$. All in all, we obtain the following result.

Proposition 4.11 *Let q be a power of an odd prime p and $n = p, 2p$. Suppose that $p \geq 5$ if $n = p$. The following hold:*

1. *With the possible exception of the pair $(q,p) = (5,5)$, there exists an 1-normal element in $\mathbb{F}_{q^p}$ with multiplicative order $\frac{q^p-1}{2}$.*
2. *With the possible exception of the pairs $(q,2p) = (3,6),(9,6)$, there exists an 1-normal element in $\mathbb{F}_{q^{2p}}$ with multiplicative order $\frac{q^p-1}{2}$.*

5 Main existence results

In this section, we complete the proof of our main results. We use many different techniques to treat the cases that are left to consider after all the preliminary results given in the previous section. Some persistent cases are left to consider after we employ all of our methods (most of them are from the tables in Section 4). In these cases, we verify the existence of elements of our interest by direct computer search; the SAGEMATH software is used and the pseudocode can be found in Appendix A. We start with some auxiliary results.

Lemma 5.1 *If $q > 3$ is an odd prime power, then all 2-primitive $c \in \mathbb{F}_{q^2}$ are normal over $\mathbb{F}_q$. In contrast, all 2-primitive elements of $\mathbb{F}_{3^2}$ are 1-normal over $\mathbb{F}_3$.*

Proof Observe that any nonzero element of $\mathbb{F}_{q^2}$ is either normal or 1-normal. If $\alpha \in \mathbb{F}_{q^2}^*$ is 1-normal, then $(x-b) \circ \alpha = 0$ for some $b \in \mathbb{F}_q^*$, hence $\alpha^q = b\alpha$ and so $\alpha^{(q-1)^2} = 1$. In particular, any element in $\mathbb{F}_{q^2}$ with multiplicative order greater than $(q-1)^2$ is normal. For $q > 3$, $(q^2-1)/2 > (q-1)^2$ and this implies the normality over $\mathbb{F}_q$ of all 2-primitive elements. If $c \in \mathbb{F}_{3^2}$ is 2-primitive, then it has multiplicative order 4, and so $c^q = c^3 = \pm c$. In other words, c is 1-normal. □

Lemma 5.2 (see [1]) *Let q be a power of a prime. If $m \geq 3$ and $(q,m) \neq (4,3)$, then for every $a \in \mathbb{F}_q$, there exists a primitive element $\alpha \in \mathbb{F}_{q^m}$ such that $\mathrm{Tr}_{q^m/q}(\alpha) = a$. Moreover, if $m = 2$ or $(q,m) = (4,3)$, for every nonzero element $a \in \mathbb{F}_q$, there exists a primitive element $\alpha \in \mathbb{F}_{q^m}$ such that $\mathrm{Tr}_{q^m/q}(\alpha) = a$.*

Proposition 5.3 *Let q be a power of an odd prime. Then there exists a 2-primitive, 1-normal element in $\mathbb{F}_{q^3}$ over $\mathbb{F}_q$.*

Proof We observe that any element of $\mathbb{F}_{q^3}^*$ with trace zero over $\mathbb{F}_q$ is either 1-normal or 2-normal. Following the proof of Lemma 5.1, the multiplicative order of any 2-normal element of $\mathbb{F}_{q^3}^*$ is at most $(q-1)^2 < \frac{q^3-1}{2}$. In particular, if there exists a 2-primitive element $\alpha \in \mathbb{F}_{q^3}$ with trace zero over $\mathbb{F}_q$, such an α is 1-normal. We prove the existence of an element α having these properties with the help of Lemma 5.2; from this lemma, there exists a primitive element $w \in \mathbb{F}_{q^3}$ such that $\mathrm{Tr}_{q^3/q}(w) = 0$. We observe that, if $q-1 = 2^a \cdot b$ with b odd, then $q^3 - 1 = 2^a \cdot b'$ with b' odd. We set $\delta = w^{b's}$, where $s = 1$ if $b' \equiv 1 \pmod 4$ and $s = 3$ if $b' \equiv 3 \pmod 4$. In any case, $\delta^{2^a} = 1$ and so $\delta^{q-1} = 1$, i.e., $\delta \in \mathbb{F}_q^*$. Therefore, for $\alpha = \delta \cdot w$, $\mathrm{Tr}_{q^3/q}(\alpha) = \delta \cdot \mathrm{Tr}_{q^3/q}(w) = 0$. We claim that $\alpha = \delta \cdot w = w^{b's+1}$ is 2-primitive. For this, we observe that, since w is primitive, the multiplicative order of α equals $\frac{q^n-1}{d}$, where

$$d = \gcd(b's+1, q^3-1) = \gcd(b's+1, b' \cdot 2^a) = \gcd(b's+1, 2^a) = 2,$$

since $a \geq 1$ and $b's+1 \equiv 2 \pmod 4$. □

5.1 Existence of 2-primitive, normal elements

Here we establish item 1 of Theorem 1.4, proving the existence of 2-primitive, normal elements in $\mathbb{F}_{q^n}$, where $n \geq 2$. The case $n = 2$ follows directly from Lemma 5.1. In addition, up to the pairs (q,n) in Table 2, the case $n \geq 3$ is covered. For the pairs (q,n) in Table 2, we directly search for 2-primitive, normal elements. With the sole exception of $(q,n) = (3,4)$, a 2-primitive normal element is explicitly is found.

5.2 Existence of 2-primitive, 1-normal elements

Here we establish item 2 of Theorem 1.4, proving the existence of 2-primitive, 1-normal elements in $\mathbb{F}_{q^n}$, where $n \geq 2$. The statement regarding the case $(q,n) = (3,2)$ follows from Lemma 5.1 and the case $n = 3$ is proved in Proposition 5.3. Up to the pairs (q,n) in Table 4, the case $n \geq 4$ with $\gcd(n,q) = 1$ is covered in Proposition 4.8. Up to the pairs in Table 7, the case $n \neq p, 2p$ with $\gcd(n,q) = p$ is covered in Proposition 4.9, with the possible exceptions of Table 7. The case $n = p, 2p$, with $n \neq 3$, is covered by Proposition 4.11 and some possible exceptions are given there and, finally, the case $p^2 \mid n$ is covered by Corollary 4.7, with a list of possible exceptions given in the statement.

Let S be the set of all the described possible exceptions. For each pair (q,n) in S, a 2-primitive 1-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is explicitly found (see Algorithm 1 for the pseudocode). We comment that our results here also provide the following stronger version of item 2 in Theorem 1.4.

Theorem 5.4 *Let q be a power of an odd prime and let $n \geq 3$ be a positive integer. Then there exists a 2-primitive, 1-normal element $\alpha \in \mathbb{F}_{q^n}$ such that $\mathrm{Tr}_{q^n/q}(\alpha) = 0$.*

We observe that, up to the pairs (q,n) in S that we previously described, we establish item 2 of Theorem 1.4 proving the existence of a 2-primitive, 1-normal element $\alpha \in \mathbb{F}_{q^n}$ with $\mathbb{F}_q$-order equals $\frac{x^n-1}{x-1}$ (see the proofs of Proposition 3.2, Corollary 4.7 and Proposition 5.3). In particular, such an α has trace zero over $\mathbb{F}_q$ and so Theorem 5.4 is established up to the pairs (q,n) in S. For the pairs (q,n) in the set S, by a small variation of Algorithm 1, we explicitly find a 2-primitive, 1-normal element of $\mathbb{F}_{q^n}$ with trace zero over $\mathbb{F}_q$.

Acknowledgements We are grateful to the anonymous referees for their suggestions and comments. The first author was supported by TÜBİTAK Project Number 114F432 and the second author was supported by CAPES-PDSE (process - 88881.134747/2016-01).

References

1. S. D. Cohen. Primitive elements and polynomials with arbitrary trace. *Discrete Math.*, 83(1):1–7, 1990.
2. S. D. Cohen and D. Hachenberger. Primitive normal bases with prescribed trace. *Appl. Algebra Engrg. Comm. Comput.*, 9(5):383–403, 1999.
3. S. D. Cohen and S. Huczynska. The primitive normal basis theorem – without a computer. *J. London Math. Soc.*, 67(1):41–56, 2003.
4. W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, 22(6):644–654, 1976.
5. S. Gao. *Normal Basis over Finite Fields*. PhD thesis, University of Waterloo, 1993.
6. D. Hachenberger. Primitive normal bases for quartic and cubic extensions: a geometric approach. *Des. Codes Cryptogr.*, 77(2–3):335–350, 2015.
7. S. Huczynska, G. L. Mullen, D. Panario, and D. Thomson. Existence and properties of k-normal elements over finite fields. *Finite Fields Appl.*, 24:170–183, 2013.
8. H. W. Lenstra, Jr and R. J. Schoof. Primitive normal bases for finite fields. *Math. Comp.*, 48(177):217–231, 1987.
9. R. Lidl and H. Niederreiter. *Finite Fields*, volume 20 of *Enyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.
10. G. L. Mullen. Some open problems arising from my recent finite field research. In A. Canteaut, G. Effinger, S. Huczynska, D. Panario, and L. Storme, editors, *Contemporary developments in finite fields and applications*, pages 254–269. World Scientific, 2016.
11. L. Reis and D. Thomson. Existence of primitive 1-normal elements in finite fields. *Finite Fields Appl.*, 51:238–269, 2018.
12. W. M. Schmidt. *Equations over Finite Fields, An Elementary Approach*. Springer-Verlag, Berlin Heidelberg, 1976.

A Pseudocodes for search for 2-primitive elements with special properties

Following the approach of [11], Algorithm 1 presents a search routine for 2-primitive, k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. This search is based on the original characterization of k-normal elements from [7].

Theorem A.1 *Let $\alpha \in \mathbb{F}_{q^n}$ and let $g_\alpha(x) = \sum_{i=0}^{n-1} \alpha^{q^i} x^{n-1-i} \in \mathbb{F}_{q^n}[x]$. Then $\gcd(x^n-1, g_\alpha(x))$ has degree k if and only if α is a k-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

Algorithm 1 proceeds as follows. Let $\mathbb{F}_{q^n} \cong \mathbb{F}_q[x]/(f)$ with f a primitive polynomial, and let g be a root of f. Hence, g is a generator of $\mathbb{F}_{q^n}^*$ and g^i is 2-primitive if and only if $\gcd(i, q^n-1) = 2$. For each 2-primitive element, check its k-normality using Theorem A.1. If $k = 1$, the resulting element is 2-primitive, 1-normal and is returned. The algorithm returns "Fail" if no 2-primitive 1-normal is found after $q^n - 2$ iterations; that is, if all of $\mathbb{F}_{q^n}^*$ is traversed.

Algorithm 1 Pseudocode for 2-primitive 1-normal element search algorithm

Input: positive integers q, n
Returns: 2-primitive 1-normal element: elt $\in \mathbb{F}_{q^n}$; otherwise "Fail"
mult_order $\leftarrow q^n - 1$
$g \leftarrow$ generator$(\mathbb{F}_{q^n}^*)$
$cyclo \leftarrow x^n - 1 \in \mathbb{F}_{q^n}[x]$

function check_k_normal(v) ▷ See Theorem A.1
  $g_v(x) \leftarrow vx^{n-1} + v^q x^{n-2} + \cdots + v^{q^{n-1}}$
  $k \leftarrow \deg(\gcd(g_v, cyclo))$
  return k
end function

$i \leftarrow 1$
while True **do**
  if i **is** mult_order **then** ▷ No 2-primitive 1-normals found in $\mathbb{F}_{q^n}$
    return "Fail"
  end if
  if $\gcd(i,$ mult_order$) \neq 2$ **then** ▷ Only check 2-primitive elements
    $i \leftarrow i+1$
    continue
  end if
  elt $\leftarrow g^i$
  $k \leftarrow$ check_k_normal(elt)
  if k **is** 1 **then**
    return elt
  end if
  $i \leftarrow i+1$
end while