

The Trace of Primitive and 2-Primitive Elements, Revisited

Stephen D. Cohen*

6 Bracken Road, Portlethen, Aberdeen AB12 4TA, Scotland, UK

Email: Stephen.Cohen@glasgow.ac.uk

Giorgos Kapetanakis

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

Email: gnkapet@gmail.com

Received 17 May 2021

Accepted 15 December 2021

Communicated by Nguyen Van Sanh

AMS Mathematics Subject Classification(2020): 11T30, 11T06

Abstract. By definition primitive and 2-primitive elements of a finite field extension \mathbb{F}_{q^n} have order $q^n - 1$ and $(q^n - 1)/2$, respectively. We have already shown that, with minor reservations, there exists a primitive element and a 2-primitive element $\xi \in \mathbb{F}_{q^n}$ with prescribed trace in the ground field \mathbb{F}_q . Here we amend our previous proofs of these results, firstly, by a reduction of these problems to extensions of prime degree n and, secondly, by deriving an exact expression for the number of squares in \mathbb{F}_{q^n} whose trace has prescribed value in \mathbb{F}_q . The latter corrects an error in the proof in the case of 2-primitive elements. We also streamline the necessary computations.

Keywords: Primitive elements; Trace function.

1. Introduction

Let q be the power of a prime p and $n \geq 2$ be an integer. Denote by \mathbb{F}_q the finite field of order q and by \mathbb{F}_{q^n} its extension of degree n . A primitive element

*The first author is Emeritus Professor of Number Theory, University of Glasgow

of \mathbb{F}_{q^n} is a generator of its (cyclic) multiplicative group. More generally, for a divisor r of $q^n - 1$, an r -primitive element has been defined as an element of order $(q^n - 1)/r$. In this sense, a 1-primitive element has the same meaning as a primitive element. We shall be concerned solely with primitive and 2-primitive elements here.

We denote by Tr the trace function $\mathbb{F}_{q^n} \rightarrow \mathbb{F}_q$, that is

$$\text{Tr}(\xi) := \sum_{i=0}^{n-1} \xi^{q^i}, \quad \xi \in \mathbb{F}_{q^n}.$$

By the trace problem for r -primitive elements will be meant a study of whether or not, given $\beta \in \mathbb{F}_q$, there exists an r -primitive $\xi \in \mathbb{F}_{q^n}$ such that $\text{Tr}(\xi) = \beta$. The resolution of the trace problem for primitive elements in [1] is a fundamental result. Indeed, in a recent monograph [6], Hachenberger and Jungnickel devote their final chapter to it (see Result 14.1.1).

Theorem 1.1. *Let q be a prime power, n an integer and $\beta \in \mathbb{F}_q$. Unless $(n, \beta) = (2, 0)$ or $(n, q) = (3, 4)$, there exists a primitive $\xi \in \mathbb{F}_{q^n}$ with $\text{Tr}(\xi) = \beta$.*

The original proof of Theorem 1.1 was obtained by assembling components from different sources and implicitly involved some direct verification by a computer. For this reason another proof was given in [5] which could be checked theoretically with the aid of a basic calculator. The solution in [6] contains additional algebraic ideas. It too reduces the level of computation required to a minimum.

More recently, the authors resolved the basic trace problem for 2-primitive elements in \mathbb{F}_{q^n} (necessarily for odd prime powers q) (see [4, Theorem 1.3]).

Theorem 1.2. *Let q be an odd prime power. Then the following statements hold:*

- (i) *Let $\beta \in \mathbb{F}_q$. Suppose $n \geq 3$. Then there exists a 2-primitive element ξ of \mathbb{F}_{q^n} such that $\text{Tr}(\xi) = \beta$.*
- (ii) *Suppose $n = 2$. Let $\beta \in \mathbb{F}_q^*$. There exists some 2-primitive element ξ of \mathbb{F}_{q^2} such that $\text{Tr}(\xi) = \beta$, unless $q = 3, 5, 7, 9, 11, 13$ or 31 . Further, in the exceptional case when $q = 9$ and $b \in \{\pm 1, \pm i\}$ (where $i^2 = -1$), there exists a 2-primitive element ξ in \mathbb{F}_{81} with $\text{Tr}(\xi) = \beta$.*

Remark 1.3. When $n = 2$, if $\xi \in \mathbb{F}_{q^2}$ has trace 0, then its order must be at most $2(q - 1)$ and so ξ cannot be 2-primitive unless $q = 3$ in which case $\mathbb{F}_{q^2}^* = \mathbb{F}_9^* = \{\pm 1, \pm i, \pm 1 \pm i\}$. Here the primitive elements $\pm 1 \pm i$ have trace ± 1 and the 2-primitive elements $\pm i$ do have trace 0. From now on, if $n = 2$, assume $\beta \neq 0$.

At this point we need to admit that that the argument in the proof of Theorem 1.3 in [4] relating to the terms in the expression (4.1) involving the principal

character χ_1 contain an error which exaggerates the influence of these terms and is pervasive. In particular, the remark at the end of Section 4.1 raises a problem that does not actually arise. Because it is not easy to provide a brief corrigendum to rectify this flaw, one aim of the present article is to purify the exposition.

Another important contribution to the analysis of the trace problem is its reduction to the study of extensions of prime degree n . This forms the substance of Section 2. A subsidiary result which, given $\beta \in \mathbb{F}_q$, yields an exact expression for the number of squares $\xi \in \mathbb{F}_{q^n}$ for which $\text{Tr}(\xi) = \beta$ is provided in Section 3. This eliminates the flaw in the original proof. A further feature of this exposition is more efficient working in the calculations necessary to apply the theory.

2. Reduction to Extensions of Prime Degree

Here we show how the proofs of Theorems 1.1 and 1.2 can be deduced from the case in which n is a prime. In this section, given $d|n$ we denote by $\text{Tr}_{n/d}$ the trace function from \mathbb{F}_{q^n} to \mathbb{F}_{q^d} . The following lemma is also related to [6, Proposition 14.2.2].

Lemma 2.1. *Suppose that Theorem 1.1 has been established for all prime values of n and all prime powers q . Then Theorem 1.1 holds for arbitrary values of n and q .*

Similarly, suppose Theorem 1.2 has been established for all prime values of n and odd prime powers q . Then Theorem 1.2 holds for arbitrary values of n and q .

Proof. Let t denote the total number of primes (including their multiplicity) in the prime decomposition of n . The proof is by induction on t with the case of $t = 1$ corresponding to the stated assumption.

For the induction step write $n = \ell m$, where ℓ is any prime dividing n and $1 < m < n$. Given $\beta \in \mathbb{F}_q$, by elementary linear algebra, it is evident that there are $q^{\ell-1}$ elements in \mathbb{F}_{q^ℓ} whose trace in \mathbb{F}_q is β . Hence, in every case, even if $\beta = 0$, we can choose a *non-zero* $\alpha \in \mathbb{F}_{q^\ell}$ such that $\text{Tr}_{\ell/1}(\alpha) = \beta$. Next, for this non-zero element α apply the induction hypothesis to the extension $\mathbb{F}_{q^n} = \mathbb{F}_{q^{\ell m}}$ over \mathbb{F}_{q^ℓ} . Now, the exceptional cases in the theorems can only be relevant if q^ℓ is a prime (which it is not) or, in Theorem 1.2, when $q^\ell = 9$ and $m = 2$. Moreover, this latter situation can occur only if $q = 3, \ell = 2$ and $n = 4$ (so that $t = 2$). We deduce that, with $r = 1$ or 2 respectively, there exists an r -primitive element $\xi \in \mathbb{F}_{q^n}$ such that $\text{Tr}_{n/\ell}(\xi) = \alpha$, with the possible exception of the case when $r = 2, t = 2, q = 3, n = 4, \ell = 2$ and $\alpha = \pm 1$. In this last situation, the only possible non-zero values for $\beta \in \mathbb{F}_q = \mathbb{F}_3$ are ± 1 and we choose $\alpha = \mp 1$, respectively (since $\text{Tr}_{2/1}(\mp 1) = \pm 1$, respectively). But, from the final assertion of Theorem 1.2, there exist 2-primitive elements $\xi_1, \xi_{-1} \in \mathbb{F}_{81}$ with $\text{Tr}_{4/2}(\xi_1) = 1$ and $\text{Tr}_{4/2}(\xi_{-1}) = -1$. Finally, more generally $\text{Tr}(\xi) = \text{Tr}_{\ell/1}(\text{Tr}_{n/\ell}(\xi)) = \text{Tr}_{\ell/1}(\alpha) = \beta$ in every case and the lemma follows by

induction. ■

Lemma 2.1 significantly reduces the calculations in the previous proof. In particular, in the trace problem for primitive elements, it eliminates the discussion in [5] of the case where $n = 4$ in Section 4.1 and with respect to the case $n = 4, 6$ in Section 5. Similarly, in [6], although the authors choose to perform calculations related to degrees $n = 4, 6$ in Sections 14.5 and 14.6, there would be no need for these to establish simple existence. This completes our discussion of the trace property for primitive elements. We now focus on the property for 2-primitive elements and, in particular, assume that q is odd.

By Lemma 2.1 the material (including the calculations) in Section 5.2 of [4] is now redundant. Further, we assume that n is prime and thus consider only pairs (q, n) where q is an odd prime power and n is prime. Indeed, we shall additionally sift out pairs (q, n) which are *odd* in the sense that $(q^n - 1)/2$ is odd, which means that n is an odd prime and $q \equiv 3 \pmod{4}$.

Lemma 2.2. *Suppose (q, n) is odd. Then $\xi \in \mathbb{F}_{q^n}$ is 2-primitive if and only if $-\xi$ is primitive.*

Proof. Checking the notion of freeness formally defined on Section 4, we have that $\frac{q^n-1}{2}$ is odd, so ξ is 2-primitive if and only if ξ is both $\frac{q^n-1}{2}$ -free and a square in \mathbb{F}_{q^n} . Now $(-1)^{(q^n-1)/2} = -1$, thus -1 is a nonsquare in \mathbb{F}_{q^n} . Hence $\xi \in \mathbb{F}_{q^n}$ is a nonsquare if and only if $-\xi$ is a square. Moreover, ξ is $\frac{q^n-1}{2}$ -free if and only if $-\xi$ is $\frac{q^n-1}{2}$ -free. The result follows. ■

It follows from Lemma 2.2 that when (q, n) is odd, the number of 2-primitive elements in \mathbb{F}_{q^n} is the same as the number of primitive elements (namely $\phi(q^n - 1)$, where ϕ is Euler's function). In the situation of Lemma 2.2 we can deduce the existence theorem for 2-primitive elements from Theorem 1.1.

Theorem 2.3. *Suppose (q, n) is odd. Then, given arbitrary $\beta \in \mathbb{F}_q$, there exists a 2-primitive element of \mathbb{F}_{q^n} with trace β . (We can describe this in other words by saying that (q, n) has the trace property for 2-primitive elements.)*

Proof. From Theorem 1.1, there exists a primitive element ξ of \mathbb{F}_{q^n} with trace $-\beta$. By Lemma 2.2, $-\xi$ is 2-primitive and $\text{Tr}(-\xi) = -\text{Tr}(\xi) = \beta$. ■

Remark 2.4. Since Theorem 1.1 was established in [5], without recourse to direct verification for any pair (q, n) , the same can be said for Theorem 2.3.

From now on we assume that (q, n) is *even*, i.e., that $(q^n - 1)/2$ is even, in which case $(-1)^{(q^n-1)/2} = 1$ and so -1 is a square in \mathbb{F}_{q^n} . This implies that, either $n = 2$ or n is odd and the prime $q \equiv 1 \pmod{4}$. Further, $\xi \in \mathbb{F}_{q^n}$ is 2-primitive if and only if $-\xi$ is 2-primitive. In this situation, a 2-primitive element

can be viewed simply as the square ξ^2 of a primitive element ξ . Hence, our problem is to confirm that there exists a primitive element $\xi \in \mathbb{F}_{q^n}$ for which $\text{Tr}(\xi^2) = \beta$. Observe that, if ξ is primitive, then both $(\pm\xi)^2$ yield the same 2-primitive element ξ^2 . In particular, it is clear that the total number of 2-primitive elements in \mathbb{F}_{q^n} is $\frac{\phi(q^n-1)}{2}$.

3. The Number of Squares with Prescribed Trace

At this point it is convenient to derive, using additive characters, an explicit expression for the number of non-zero squares $\xi \in \mathbb{F}_{q^n}$ for which $\text{Tr}(\xi) = \beta$ for any given $\beta \in \mathbb{F}_q$. We continue to assume n is prime and (q, n) is even (although these restrictions could be lifted).

We employ additive characters of both \mathbb{F}_{q^n} and \mathbb{F}_q . Let ψ be the canonical additive character of \mathbb{F}_q , that is $\psi(g) = \exp(2\pi i \text{Tr}_0(g)/p)$, where Tr_0 stands for the *absolute trace* of $g \in \mathbb{F}_q$, i.e., its trace over \mathbb{F}_p , the prime subfield of \mathbb{F}_q . Then an arbitrary additive character of \mathbb{F}_q has the action which takes $g \in \mathbb{F}_q$ onto $\psi(ug)$ and thereby, as u varies, we obtain all the q additive characters of \mathbb{F}_q , whose set we will denote by $\widehat{\mathbb{F}_q}$. For the trivial character, take $u = 0$. Then the characteristic function for elements of \mathbb{F}_{q^n} , with trace β , can be expressed as

$$t_\beta(\xi) := \frac{1}{q} \sum_{u \in \mathbb{F}_q} \bar{\psi}(u\beta) \tilde{\psi}(u\xi), \quad (1)$$

where, $\bar{\psi}$ stands for the inverse of ψ and $\tilde{\psi}$ stands for the *lift* of ψ to an additive character of \mathbb{F}_{q^n} , i.e., for every $\xi \in \mathbb{F}_{q^n}$, we have that $\tilde{\psi}(\xi) = \psi(\text{Tr}(\xi))$. In particular, $\tilde{\psi}$ is the canonical character of \mathbb{F}_{q^n} .

The next two lemmas recall standard facts about the quadratic Gauss sum over \mathbb{F}_{q^n} (see [7, Section 7.5, Theorem 5.4] and [10, Section 5.2]).

Lemma 3.1. *Let $u \in \mathbb{F}_{q^n}$ and set*

$$g_n(u) = \sum_{\xi \in \mathbb{F}_{q^n}} \psi(u\xi^2) = \sum_{\xi \in \mathbb{F}_{q^n}} \chi_2(\xi) \psi(u\xi),$$

where χ_2 denotes the quadratic character and ψ the canonical additive character on \mathbb{F}_{q^n} . Then

$$g_n(u) = \chi_2(u)g_n(1).$$

Lemma 3.2. *Let q be a power of the prime p and $u \in \mathbb{F}_{q^n}$.*

If $n = 2$, then $g_2(u) = \chi_2(u)\varepsilon_1 q$, where

$$\varepsilon_1 = \begin{cases} 1 & \text{if } q \equiv 3 \pmod{4}, \\ -1 & \text{if } q \equiv 1 \pmod{4}. \end{cases}$$

On the other hand, if n is an odd prime, then $g_n(u) = \chi_2(u)\varepsilon_2 q^{n/2}$, where

$$\varepsilon_2 = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \text{ and } q \text{ is a nonsquare,} \\ & \text{or } p \equiv 3 \pmod{4} \text{ and } q \text{ is a square but not a 4th power,} \\ -1 & \text{if } p \equiv 1 \pmod{4} \text{ and } q \text{ is a square,} \\ & \text{or } p \equiv 3 \pmod{4} \text{ and } q \text{ is a 4th power.} \end{cases} \quad (2)$$

Proposition 3.3. Assume (q, n) is even and n is a prime. Given $\beta \in \mathbb{F}_q$, let \mathcal{M}_β be the number non-zero squares $\xi \in \mathbb{F}_{q^n}$ with $\text{Tr}(\xi) = \beta$.

If $n = 2$ then, for $\beta \in \mathbb{F}_q^*$,

$$\mathcal{M}_\beta = \frac{1}{2}(q - \varepsilon_1), \quad (3)$$

where

$$\varepsilon_1 = \begin{cases} 1 & \text{if } q \equiv 3 \pmod{4} \\ -1 & \text{if } q \equiv 1 \pmod{4} \end{cases}$$

On the other hand, if n is an odd prime, then

$$\mathcal{M}_\beta = \begin{cases} \frac{1}{2}(q^{n-1} - 1) & \text{if } \beta = 0, \\ \frac{1}{2}(q^{n-1} + \chi_2(\beta)q^{\frac{n-1}{2}}) & \text{if } \beta \neq 0, \end{cases} \quad (4)$$

where χ_2 denotes the quadratic character in \mathbb{F}_q .

Proof. Observe that, by (1),

$$2\mathcal{M}_\beta = \frac{1}{q} \sum_{u \in \mathbb{F}_q} \bar{\psi}(u\beta)\mathcal{X}_u =: \frac{1}{q} \sum_{u \in \mathbb{F}_q} \bar{\psi}(u\beta) \sum_{\xi \in \mathbb{F}_{q^n}^*} \tilde{\psi}(u\xi^2),$$

because each of $\pm\xi \in \mathbb{F}_{q^n}^*$ yields the same square $\xi^2 \in \mathbb{F}_{q^n}^*$. Hence

$$2q\mathcal{M}_\beta = \sum_{u \in \mathbb{F}_q} \mathcal{X}_u = q^n - 1 + \sum_{u \in \mathbb{F}_q^*} \bar{\psi}(u\beta)\mathcal{X}_u,$$

where $\mathcal{X}_u = \sum_{\xi \in \mathbb{F}_{q^n}^*} \tilde{\psi}(u\xi^2)$.

Suppose $n = 2$ and $\beta \neq 0 \in \mathbb{F}_q$. Then every $u \in \mathbb{F}_q^*$ is a square in \mathbb{F}_{q^2} so that, by Lemma 3.2, $\mathcal{X}_u = g_2(u) - 1 = \varepsilon_1 q - 1$. Hence,

$$2q\mathcal{M}_\beta = q^2 - 1 + (\varepsilon_1 q - 1) \sum_{u \in \mathbb{F}_q^*} \bar{\psi}(u\beta) = q^2 - 1 - (\varepsilon_1 q - 1),$$

since $\sum_{u \in \mathbb{F}_q} \bar{\psi}(u\beta) = 0$. Consequently, (3) holds.

Now, suppose, n is an odd prime so that nonsquares in \mathbb{F}_q remain nonsquares in \mathbb{F}_{q^n} . Thus, given a fixed nonsquare $c \in \mathbb{F}_q$, the elements of \mathbb{F}_q^* can be written

as a disjoint union $\{u^2 : u \in \mathbb{F}_q^*\} \cup \{cu^2 : u \in \mathbb{F}_q^*\}$, where each member of \mathbb{F}_q^* appears twice.

This time, by Lemma 3.1, if $\beta = 0$, then

$$2q\mathcal{M}_0 = q^n - 1 + \frac{1}{2} \sum_{u \in \mathbb{F}_q} (\mathcal{X}_{u^2}(\chi_1) + \mathcal{X}_{cu^2}(\chi_1)) = q^n - 1 - (q - 1) = q^n - q$$

and this case of (4) follows. Finally suppose $\beta \neq 0$. We have

$$\begin{aligned} 2q\mathcal{M}_\beta - (q^n - 1) &= \frac{1}{2} \left(\sum_{u \in \mathbb{F}_q^*} \bar{\psi}(\beta u^2) \mathcal{X}_{u^2} + \bar{\psi}(c\beta u^2) \mathcal{X}_{cu^2} \right) \\ &= \frac{1}{2} \left(\sum_{u \in \mathbb{F}_q^*} \bar{\psi}(\beta u^2) \mathcal{X}_1 + \bar{\psi}(c\beta u^2) \mathcal{X}_c \right) \quad (5) \\ &= \frac{1}{2} \{ (\chi_2(\beta) \varepsilon_2 q^{1/2} - 1) (\varepsilon_2 q^{n/2} - 1) + \\ &\quad (\chi_2(c\beta) \varepsilon_2 q^{1/2} - 1) (\chi_2(c) \varepsilon_2 q^{n/2} - 1) \} \\ &= \chi_2(\beta) q^{(n+1)/2} + 1, \end{aligned}$$

where, at (5), Lemma 3.2 with $n = 1$ and ε_2 given by (2) is applied to the sums over $u \in \mathbb{F}_q^*$ in addition to the sums over $\xi \in \mathbb{F}_{q^n}^*$ and we note that $\varepsilon_2^2 = 1$. This yields (4) more generally. \blacksquare

4. Mixed Character Sums

Assume throughout that q is an odd prime and n is prime with (q, n) even (although this is not essential for much of the discussion). We begin by introducing the notion of freeness. Let $m \mid q^n - 1$. An element $\xi \in \mathbb{F}_{q^n}^*$ is *m-free* if $\xi = \zeta^d$ for some $d \mid m$ and $\zeta \in \mathbb{F}_{q^n}^*$ implies $d = 1$. It is clear that primitive elements are exactly those that are q_0 -free, where q_0 is the square-free part of $q^n - 1$. It is also evident that there is some relation between m -freeness and multiplicative order.

Lemma 4.1. [8, Proposition 5.3] *If $m \mid q^n - 1$ then $\xi \in \mathbb{F}_{q^n}^*$ is m -free if and only if $\gcd\left(m, \frac{q^n - 1}{\text{ord}(\xi)}\right) = 1$.*

We introduced the quadratic character of \mathbb{F}_{q^n} in Lemma 3.1. More generally, the multiplicative characters of $\mathbb{F}_{q^n}^*$ form a group isomorphic to $\mathbb{F}_{q^n}^*$. Each character χ has order of degree d , a divisor of $q^n - 1$, and $\chi(0) = 0$, by definition. In particular, we denote by χ_1 the trivial multiplicative character and by χ_2 the quadratic character.

Vinogradov's formula yield an expression of the characteristic function of m -free elements in terms of multiplicative characters, namely:

$$\omega_m(\xi) := \theta(m) \sum_{d|m} \frac{\mu(d)}{\phi(d)} \sum_{\text{ord}(\chi_d)=d} \chi_d(\xi),$$

where μ stands for the Möbius function and $\theta(m) := \phi(m)/m$. Also, here the inner sum runs through multiplicative characters χ_d of order d .

Proposition 4.2. *Let q be an odd prime and χ_d be a multiplicative character of order d , $u \in \mathbb{F}_q$. Set*

$$A := \sum_{\xi \in \mathbb{F}_{q^n}} \chi_d(\xi) \tilde{\psi}(u\xi^2).$$

Then the following statements hold:

- (i) If $d = 1$ and $u = 0$, then $A = q^n - 1$.
- (ii) If $d = 1$ and $u \neq 0$, then $|A| \leq q^{n/2} + 1$.
- (iii) If $d \neq 1$ and $u = 0$, then $A = 0$.
- (iv) If $d \neq 1$ and $u \neq 0$, then $|A| \leq 2q^{n/2}$.

Proof. When $d = 1$, since $\chi_1(0) = 0$, we have that $A = g_n(u) - 1$. From this, we immediately obtain the first and second items. The third item is a consequence of the orthogonality relations and the last item is implied by [11, Theorem 2G]. ■

Finally, the following is an improvement of the main result of [9], in the case $n = 2$, see [2, Lemma 3.3].

Lemma 4.3. *Let $\theta \in \mathbb{F}_{q^2}$ be such that $\mathbb{F}_{q^2} = \mathbb{F}_q(\theta)$ and χ a non-trivial character. Set*

$$B := \sum_{\alpha \in \mathbb{F}_q} \chi(\theta + \alpha).$$

Then the following statements hold:

- (i) If $\text{ord}(\chi) \nmid q + 1$, then $|B| = \sqrt{q}$.
- (ii) If $\text{ord}(\chi) \mid q + 1$, then $B = -1$.

5. Conditions for Even Pairs

Recall that 2-primitive elements are exactly the squares of primitive elements. In other words, we are looking for a primitive element the trace of whose square is fixed to some $\beta \in \mathbb{F}_q$. With that in mind, following the analysis of Section 4, we define the following

$$\mathcal{N}_\beta(m) := \sum_{\xi \in \mathbb{F}_{q^n}} \omega_m(\xi) t_\beta(\xi^2),$$

where $m \mid q^n - 1$. In particular, our aim is to prove that $\mathcal{N}_\beta(q_0) \neq 0$ (where we recall that q_0 stands for the square-free part of $q^n - 1$) and note that, in fact, since (q, n) is even, $\mathcal{N}_\beta(q_0)$ counts twice the number of 2-primitive elements with trace β . Next, we compute:

$$\begin{aligned} \frac{\mathcal{N}_\beta(m)}{\theta(m)} &= \frac{1}{q} \sum_{\xi \in \mathbb{F}_{q^n}} \sum_{d \mid m} \frac{\mu(d)}{\phi(d)} \sum_{\text{ord}(\chi_d)=d} \chi_d(\xi) \sum_{u \in \mathbb{F}_q} \bar{\psi}(u\beta) \tilde{\psi}(u\xi^2) \\ &= \frac{1}{q} \sum_{d \mid m} \frac{\mu(d)}{\phi(d)} \sum_{\text{ord}(\chi)=d} \sum_{u \in \mathbb{F}_q} \bar{\psi}(u\beta) \mathcal{X}_u(\chi_d), \end{aligned} \quad (6)$$

where

$$\mathcal{X}_u(\chi_d) := \sum_{\xi \in \mathbb{F}_{q^n}} \chi_d(\xi) \tilde{\psi}(u\xi^2).$$

Now observe that the terms on the right side of (6) corresponding to $d = 1$ are given precisely by $2\mathcal{M}_\beta$ as evaluated in Proposition 3.3 and note that this is where the discrepancy occurs in [4, Eq. (4.5)].

We proceed to consider the contribution of the terms on the right side of (6) with $d > 1$: call this quantity $R_\beta(m)$. The argument echoes that of the proof of Proposition 3.3 without the precision of the latter.

By Proposition 4.2 (3) we can suppose $u \neq 0$. Observe that

$$\begin{aligned} \sum_{u \in \mathbb{F}_q^*} \bar{\psi}(u\beta) \mathcal{X}_u(\chi_d) &= \frac{1}{2} \left(\sum_{u \in \mathbb{F}_q^*} \bar{\psi}(u^2\beta) \mathcal{X}_{u^2}(\chi_d) + \sum_{u \in \mathbb{F}_q^*} \bar{\psi}(cu^2\beta) \mathcal{X}_{cu^2}(\chi_d) \right) \\ &= \frac{1}{2} \left(\sum_{u \in \mathbb{F}_q^*} \bar{\chi}_d(u) \bar{\psi}(\beta u^2) \mathcal{X}_1(\chi_d) + \sum_{u \in \mathbb{F}_q^*} \bar{\chi}_d(u) \bar{\psi}(c\beta u^2) \mathcal{X}_c(\chi_d) \right) \end{aligned}$$

Thus, again writing \mathbb{F}_q^* as a disjoint union of squares and nonsquares (each counted twice), we have

$$R_\beta(m) = \frac{1}{2q} \sum_{\substack{d \mid m \\ d > 1}} \frac{\mu(d)}{\phi(d)} \sum_{\text{ord}(\chi_d)=d} \sum_{u \in \mathbb{F}_q^*} (\bar{\psi}(u^2\beta) \bar{\chi}_d(u) \mathcal{X}_1(\chi_d) + \bar{\psi}(u^2c\beta) \bar{\chi}_d(u) \mathcal{X}_c(\chi_d)), \quad (7)$$

To proceed we distinguish between the cases $\beta \neq 0$ and $\beta = 0$.

5.1. The Case $\beta \neq 0$ and n Prime

In this situation (7) can be rewritten as follows.

Lemma 5.1. *Assume (q, n) is even and $\beta(\neq 0) \in \mathbb{F}_q$. Then*

$$R_\beta(m) = \frac{1}{2q} \sum_{\substack{d|m \\ d>1}} \frac{\mu(d)}{\phi(d)} \sum_{\text{ord}(\chi_d)=d} (\overline{X_\beta(\chi_d)} \mathcal{X}_1(\chi_d) + \overline{X_{c\beta}(\chi_d)} \mathcal{X}_c(\chi_d)),$$

where $X_\beta(\chi_d)$ (with χ_d restricted to \mathbb{F}_q) is the sum $\sum_{u \in \mathbb{F}_q} \chi_d(u) \psi(u^2 \beta)$ (i.e., the sum $\mathcal{X}_\beta(\chi_d)$ over \mathbb{F}_q rather than \mathbb{F}_{q^n}).

Next, we present a lower bound for $\mathcal{N}_\beta(m)$ which yields a condition for it to be positive. A key point is that in sums over divisors d of an integer m with a factor $\mu(d)$ effectively involve only *squarefree* divisors d and we designate the number of such divisors by $W(m) = 2^{\nu(m)}$, where $\nu(m)$ is the number of distinct prime disisors of m ,

Theorem 5.2. *Assume (q, n) is even, where q is an odd prime power and n is a prime. Let $\beta \in \mathbb{F}_q^*$ and m be an even divisor of $q^n - 1$ with m_Q be the product of those primes in m which divide $Q = \frac{q^n - 1}{q - 1}$. Then*

$$\mathcal{N}_\beta(m) \geq \theta(m) q^{\frac{n-1}{2}} \left\{ q^{\frac{n-1}{2}} - 4W(m) + 2W(m_Q) + 1 \right\}. \quad (8)$$

Hence $\mathcal{N}_\beta(q^n - 1)$ is positive whenever

$$q^{\frac{n-1}{2}} > 4W(q^n - 1) - 2W(Q) - 1. \quad (9)$$

Proof. From (6) we have

$$\frac{\mathcal{N}_\beta(m)}{\theta(m)} = 2M_\beta + R_\beta(m).$$

Moreover, by Prop. 3.3, $|2M_\beta - q^{n-1}| \leq q^{\frac{n-1}{2}}$. From Prop. 4.2, for any $\beta \in \mathbb{F}_q^*$ and multiplicative character χ , $|\mathcal{X}_\beta(\chi)| \leq 2q^{\frac{n}{2}}$ and $|X_\beta(\chi)| \leq 2q^{\frac{1}{2}}$. Indeed when $d \mid m_Q$, then χ_d restricted to \mathbb{F}_q is the trivial character and $|X_\beta(\chi_d)| \leq q^{\frac{1}{2}} + 1$. In fact, we can be more precise about the latter bound (i.e., when $d \mid m_Q$). For, whether n is even or odd, by (2), $X_\beta(\chi_1)$ and $X_{c\beta}(\chi_1)$ take the two real values $\pm q^{1/2} - 1$ in either order. Thus, one of $|\overline{X_\beta(\chi_d)} \mathcal{X}_1(\chi_d)|$ and $|\overline{X_{c\beta}(\chi_d)} \mathcal{X}_c(\chi_d)|$ is bounded by $2(q^{1/2} - 1)q^{n/2}$ and the other by $2(q^{1/2} + 1)q^{n/2}$. So their sum is bounded absolutely by $4q^{(n+1)/2}$. Thus, by Lemma 5.1,

$$\frac{\mathcal{N}_\beta(m)}{\theta(m) q^{\frac{n-1}{2}}} \geq q^{\frac{n-1}{2}} - 1 - 4(W(m) - W(m_Q)) - 2(W(m_Q) - 1).$$

and the result follows. ■

5.2. The Case $\beta = 0$ and n an Odd Prime

Next we suppose that n is an odd prime and $\beta = 0$. Now (7) does not have a Gauss sum factor. We show that, to ensure that $\mathcal{N}_0(q^n - 1)$ is positive, it suffices to show that $\mathcal{N}_0(Q)$ is positive.

Lemma 5.3. *Suppose $\xi \in \mathbb{F}_{q^n}$ is Q -free. Then there exists $c \in \mathbb{F}_q$ with $c\xi \in \mathbb{F}_{q^n}$ primitive. Further, if $\text{Tr}(\xi^2) = 0$, then $\text{Tr}((c\xi)^2) = 0$.*

Proof. It is possible that $q - 1$ and Q have a common prime factor (or factors), namely prime factors of n . Express $q - 1$ as a product LM , where L and M are coprime, such that ξ is QL -free and ξ is an m -th power in \mathbb{F}_{q^n} for each prime m dividing M (so $m \nmid QL$). Hence, if γ is a primitive element of \mathbb{F}_{q^n} , then $\xi = \gamma^{M_0 t}$, where t and Q are coprime and M_0 is such that its square-free part is identical with the square-free part of M . Define $g = \gamma^Q$, a primitive element of \mathbb{F}_q , and set $c = g^L = \gamma^{QL}$. Thus $c\xi = \gamma^{QLt + M_0 t}$ is QLM -free, i.e., $(q^n - 1)$ -free.

If actually $\text{Tr}(\xi^2) = 0$, then $\text{Tr}((c\xi)^2) = \text{Tr}(c^2\xi^2) = 0$ since $c^2 \in \mathbb{F}_q$. \blacksquare

After Lemma 5.3, to show there exists a 2-primitive element with trace 0, it suffices to show there exists a Q -free element ξ such that $T(\xi^2) = 0$.

Lemma 5.4. *Assume (q, n) is even with n an odd prime, and that $m \mid Q$.*

$$R_0(m) = \frac{q-1}{2q} \sum_{\substack{d|m \\ d>1}} \frac{\mu(d)}{\phi(d)} \sum_{\text{ord}(\chi_d)=d} (\mathcal{X}_1(\chi_d) + \mathcal{X}_c(\chi_d)). \quad (10)$$

Proof. The above is an immediate consequence of (7), after considering the fact that χ_d is trivial on \mathbb{F}_q for every $d \mid Q$. \blacksquare

Theorem 5.5. *Assume (q, n) is even with n an odd prime. Suppose that $m \mid Q$. Then, with $\beta = 0$,*

$$\mathcal{N}_0(m) \geq \theta(m)q^{\frac{n}{2}-1} \{q^{\frac{n}{2}} - 2W(m)(q-1)\}. \quad (11)$$

Consequently, if

$$q^{\frac{n}{2}} > 2W(Q)(q-1), \quad (12)$$

then $\mathcal{N}_0(q^n - 1) > 0$.

Proof. Lemma 5.4, combined with Propositions 4.2 and 3.3, yields

$$\mathcal{N}_0(m) \geq \theta(m)q^{\frac{n}{2}-1} \left\{ q^{\frac{n}{2}} - q^{1-n/2} - 2(W(m) - 1)(q-1) \right\}$$

and (11) easily follows.

Now, assume that (12) holds. By (11), there exists some Q -free $\zeta \in \mathbb{F}_{q^n}$ with $\text{Tr}(\zeta^2) = 0$ and from Lemma 5.3, this implies the existence of a primitive $\xi \in \mathbb{F}_{q^n}$ such that $\text{Tr}(\xi^2) = 0$. ■

6. Sieving Conditions

Our next aim is to modify the conditions in Section 5 by adopting a well-established prime sieving technique (see [3]). For any divisor m of $q^n - 1$ in expressions such as $\mathcal{N}_\beta(m)$ we freely interchange m and its radical, i.e., the product of distinct primes dividing m .

Proposition 6.1. (Sieving inequality) *Assume (q, n) is even. Let $m \mid q_0$ (the squarefree part of $q^n - 1$) and $\beta \in \mathbb{F}_q$. Write $m = kp_1 \dots p_s$, where p_1, \dots, p_s are distinct prime divisors of m . Then*

$$\mathcal{N}_\beta(m) \geq \sum_{i=1}^s \mathcal{N}_\beta(kp_i) - (s - 1)\mathcal{N}_\beta(k).$$

First suppose $\beta \neq 0$ and n is a prime. Let the radical of $q^n - 1$ be expressed as $kp_1 \dots p_s$, where p_1, \dots, p_s are distinct primes and $s \geq 0$ and define $\delta = 1 - \sum_{i=1}^s \frac{1}{p_i}$, with $\delta = 1$, if $s = 0$. Suppose further that $p_i \mid Q$ for $i = 1, \dots, r$ and $p_i \nmid Q$ for $i = r + 1, \dots, s$. Set $\delta_Q = 1 - \sum_{i=1}^r \frac{1}{p_i}$.

Theorem 6.2. *Assume (q, n) is even with n a prime. Suppose $\beta \neq 0$. Define δ, δ_Q as above and assume that δ is positive. Then*

$$\begin{aligned} \mathcal{N}_\beta(q^n - 1) &\geq \delta \theta(k) q^{\frac{n-1}{2}} \left\{ q^{\frac{n-1}{2}} - 4 \left(\frac{s-1}{\delta} + 2 \right) W(k) \right. \\ &\quad \left. + 2 \left(\frac{r-1+\delta_Q}{\delta} + 1 \right) W(k_Q) \right\}. \end{aligned} \tag{13}$$

Hence, if

$$q^{\frac{n-1}{2}} > 4 \left(\frac{s-1}{\delta} + 2 \right) W(k) - 2 \left(\frac{r-1+\delta_Q}{\delta} + 1 \right) W(k_Q),$$

then $\mathcal{N}_\beta(q^n - 1) > 0$.

Proof. Proposition 6.1 implies that, for any $\beta \in \mathbb{F}_q$,

$$\begin{aligned} \mathcal{N}_\beta(q^n - 1) &\geq \sum_{i=1}^s \mathcal{N}_\beta(kp_i) - (s - 1)\mathcal{N}_\beta(k) \\ &\geq \delta \mathcal{N}_\beta(k) - \sum_{i=1}^s \left| \mathcal{N}_\beta(kp_i) - \left(1 - \frac{1}{p_i} \right) \mathcal{N}_\beta(k) \right| \end{aligned} \tag{14}$$

In (14) use (8) with $m = k$ as a lower bound. For the absolute value of the difference expressions we distinguish between values two cases according as $p_i \mid Q$ or not. Suppose $p_i \nmid Q$. Then

$$\left| \mathcal{N}_\beta(kp_i) - \left(1 - \frac{1}{p_i}\right) \mathcal{N}_\beta(k) \right| \leq 4\theta(k) \left(1 - \frac{1}{p_i}\right) q^{\frac{n-1}{2}} W(k), \quad (15)$$

since $W(kp_i) - W(k) = W(k)$. On the other hand, if $p_i \mid Q$, we have the improved bound

$$\left| \mathcal{N}_\beta(kp_i) - \left(1 - \frac{1}{p_i}\right) \mathcal{N}_\beta(k) \right| \leq \theta(k) \left(1 - \frac{1}{p_i}\right) q^{\frac{n-1}{2}} \{4W(k) - 2W(k_Q)\}, \quad (16)$$

using also the fact that $W(k_Q p_i) - W(k_Q) = W(k_Q)$. By combining (8), (14), (15) and (16) we deduce that (13) holds. ■

Finally, suppose $\beta = 0$ and n is an odd prime. We use the sieve version of the criterion (12) to obtain a result that depends on writing Q (rather than $q^n - 1$) as $Q = kp_1 \dots p_s$.

Theorem 6.3. *Assume (q, n) is even with $n \geq 3$. With the notation $Q = kp_1 \dots p_s$, with p_1, \dots, p_s distinct primes dividing Q , set $\delta = 1 - \sum_{i=1}^s \frac{1}{p_i}$. Assume that δ is positive. Then*

$$\mathcal{N}_0(Q) > \delta \theta(k) q^{\frac{n}{2}} \left\{ q^{\frac{n}{2}-1} - 2 \left(\frac{s-1}{\delta} + 2 \right) W(k) \right\}.$$

Hence, if

$$q^{\frac{n}{2}-1} > 2 \left(\frac{s-1}{\delta} + 2 \right) W(k),$$

then $\mathcal{N}_0(q^n - 1) > 0$.

Proof. The proof follows the same pattern as that of Theorem 6.2, this time with the difference being that (11) substitutes for (8). ■

For a multiplicative character χ of \mathbb{F}_{q^n} denote by $G_n(\chi)$ the Gauss sum $G_n(\chi) = \sum_{\xi \in \mathbb{F}_{q^n}} \chi(\xi) \psi(\xi)$, where ψ is the canonical additive character. In particular, $G_n(\chi_2) = g_n(1)$ as used in Lemma 3.1. Indeed, by Lemma 3.1 we have

$$\sum_{\xi \in \mathbb{F}_{q^n}} \psi(b\xi^2) = \chi_2(b) G_n(\chi_2).$$

In the case in which q is prime and $n = 1$, the following lemma is established in [12, Lemma 4]. Here, we prove it more generally.

Lemma 6.4. *Assume (q, n) is even. Let χ be any non-trivial multiplicative character of \mathbb{F}_{q^n} . Then, for any $b \in \mathbb{F}_{q^n}$,*

$$|\mathcal{X}_b(\chi)|^2 = (1 + \chi(-1))q^n + \chi_2(b)G_n(\chi_2)C(\chi), \quad (17)$$

where $C(\chi) := \sum_{\xi \in \mathbb{F}_{q^n}} \chi(\xi) \chi_2(\xi^2 - 1)$. Thus $|C(\chi)| \leq 2q^{\frac{n}{2}}$.

Proof. Let ψ be the canonical additive character of \mathbb{F}_{q^n} . We have that

$$\begin{aligned}
|\mathcal{X}_b(\chi)|^2 &= \sum_{\xi \in \mathbb{F}_{q^n}^*} \chi(\xi) \psi(b\xi^2) \overline{\sum_{\zeta \in \mathbb{F}_{q^n}^*} \chi(\zeta) \psi(b\zeta^2)} \\
&= \sum_{\xi \in \mathbb{F}_{q^n}^*} \sum_{\zeta \in \mathbb{F}_{q^n}^*} \chi\left(\frac{\xi}{\zeta}\right) \psi(b(\xi^2 - \zeta^2)) \\
&= \sum_{\xi \in \mathbb{F}_{q^n}^*} \sum_{\zeta \in \mathbb{F}_{q^n}^*} \chi(\xi) \psi(b\zeta^2(\xi^2 - 1)) \\
&= \sum_{\xi \in \mathbb{F}_{q^n}^*} \chi(\xi) \left[\sum_{\zeta \in \mathbb{F}_{q^n}} \psi(b\zeta^2(\xi^2 - 1)) - 1 \right] \\
&= (1 + \chi(-1))q^n + \sum_{\substack{\xi \in \mathbb{F}_{q^n}^* \\ \xi \neq \pm 1}} \chi(\xi) \sum_{\zeta \in \mathbb{F}_{q^n}} \psi(b\zeta^2(\xi^2 - 1)) - \sum_{\xi \in \mathbb{F}_{q^n}^*} \chi(\xi).
\end{aligned}$$

The result now follows from Lemma 3.1. ■

As we know from Lemma 3.2, when (q, n) is even, we have $G_n(\chi_2) = \pm q^{\frac{n}{2}}$. We proceed with the implications of Lemma 6.4 when n is odd; in particular it applies in the key case when $n = 3$. In this situation, since (q, n) is even, necessarily $q \equiv 1 \pmod{4}$.

Lemma 6.5. *Assume $q \equiv 1 \pmod{4}$ and n is an odd prime. Let χ be a non-trivial multiplicative character of \mathbb{F}_{q^n} and c a nonsquare in \mathbb{F}_q . Then*

$$|\mathcal{X}_1(\chi)| + |\mathcal{X}_c(\chi)| \leq 2\sqrt{2}q^{\frac{n}{2}}.$$

Proof. Since in this context Q is odd, c remains a nonsquare in \mathbb{F}_{q^n} . Thus $\chi_2(c) = -1 = -\chi_2(1)$. Hence, from (17),

$$(|\mathcal{X}_1(\chi)| + |\mathcal{X}_c(\chi)|)^2 = 2(1 + \chi(-1))q^n + 2|\mathcal{X}_1(\chi)||\mathcal{X}_c(\chi)|. \quad (18)$$

Additionally, in a similar manner as in the proof of Lemma 6.4, we have that

$$\begin{aligned}
\mathcal{X}_1(\chi) \overline{\mathcal{X}_c(\chi)} &= \sum_{\xi \in \mathbb{F}_{q^n}^*} \sum_{\zeta \in \mathbb{F}_{q^n}^*} \chi\left(\frac{\xi}{\zeta}\right) \psi(\xi^2 - c\zeta^2) \\
&= \sum_{\xi \in \mathbb{F}_{q^n}^*} \sum_{\zeta \in \mathbb{F}_{q^n}^*} \chi(\xi) \psi(\zeta^2(\xi^2 - c)) \\
&= \sum_{\xi \in \mathbb{F}_{q^n}^*} \chi(\xi) \left[\sum_{\zeta \in \mathbb{F}_{q^n}} \psi(\zeta^2(\xi^2 - c)) - 1 \right]
\end{aligned}$$

$$= \sum_{\xi \in \mathbb{F}_{q^n}^*} \chi(\xi) \sum_{\zeta \in \mathbb{F}_{q^n}} \psi(\zeta^2(\xi^2 - c)).$$

Now Lemma 3.1 yields that

$$\mathcal{X}_1(\chi) \overline{\mathcal{X}_c(\chi)} = G_n(\chi_2) \sum_{\xi \in \mathbb{F}_{q^n}^*} \chi(\xi) \chi_2(\xi^2 - c).$$

From the fact that $G_n(\chi_2) = \pm q^{n/2}$ and that the (absolute value of the) inner sum is bounded by $2q^{n/2}$, it follows that

$$|\mathcal{X}_1(\chi)| |\mathcal{X}_c(\chi)| = |\mathcal{X}_1(\chi) \overline{\mathcal{X}_c(\chi)}| \leq 2q^n$$

and the result follows once we insert the above in (18). \blacksquare

By applying Lemma 6.5 to (10) (instead of $|\mathcal{X}_b(\chi)| \leq 2q^{\frac{3}{2}}$) and extending this to the sieve result we obtain the following improvements to Theorems 6.2 and 6.3.

Theorem 6.6. *Assume $q \equiv 1 \pmod{4}$ and n is an odd prime. With the notation of Theorem 6.2, assume $\beta \neq 0$ and $\delta > 0$. Suppose*

$$q^{\frac{n-1}{2}} > 2\sqrt{2} \left(\frac{s-1}{\delta} + 2 \right) W(k) - \sqrt{2} \left(\frac{r-1+\delta_Q}{\delta} + 1 \right) W(k_Q).$$

Then $\mathcal{N}_\beta(q^n - 1) > 0$.

Theorem 6.7. *Assume $q \equiv 1 \pmod{4}$ and n is an odd prime. In the situation insofar of Theorem 6.3, assume $\beta = 0$ and $\delta > 0$. Suppose that*

$$q^{\frac{n}{2}-1} > \sqrt{2} \left(\frac{s-1}{\delta} + 2 \right) W(k).$$

Then $\mathcal{N}_0(q^n - 1) > 0$.

7. Extensions of Odd Prime Degree

In this section we complete the proof of Theorem 1.2 for n an odd prime, insofar as it can be accomplished theoretically. By Lemma 2.1 we can assume n is prime. If q is odd, then $q \equiv 1 \pmod{4}$. We distinguish the cases, n a prime exceeding 4 and $n = 3$, while the case $n = 2$ is studied in Section 8. Recall $W(t) = 2^{\nu(t)}$ is the number of the square-free divisors of t . The following provides a bound for this number.

Lemma 7.1. *Let t, ℓ be positive integers and let p_1, \dots, p_j be the distinct prime divisors of t such that $p_i \leq 2^\ell$. Then $W(t) \leq c_\ell(t) t^{1/\ell}$, where*

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

In particular, $c_4(t) < 4.87$ for every t . Indeed, if t is odd, then $c_4(t) < 2.9$.

Further, for any t , $c_6(t) < 46.103$.

Proof. The statement is an immediate generalization of [3, Lemma 3.3] and can be proved using multiplicativity. ■

Other specific applications of Lemma 7.1 will be given where they are used. We comment that, in [4], less successfully, we used a bound for $c_8(t)$.

7.1. The Case $n > 4$, Prime

We suppose $n \geq 5$ is prime and that $4|q-1$ (so that $q \geq 5$). Take any $\beta \in \mathbb{F}_q^*$. We begin by employing the simplest condition for $\mathcal{N}_\beta(q_0) \neq 0$ to check, that is

$$q^{\frac{n}{4}-\frac{1}{2}} > 4 \cdot 4.87/2^{\frac{1}{4}} = 16.38\dots, \quad (19)$$

which is a consequence of (9) and Lemma 7.1. Now, (19) is satisfied for $n \geq 17$ and $q \geq 3$, which means that the case $n > 13$ is settled. It also holds if $q > 3$ when $n = 11$, if $q > 7$ when $n = 7$ and if $q > 41$ when $n = 5$. The remaining cases can be checked using the simple sufficient condition $q^{\frac{n-1}{2}} > 4W(q^5 - 1)$ except when $(q, n) = (5, 5)$. In this last case $5^5 - 1 = 2^2 \cdot 11 \cdot 71$ so that $Q = 11 \cdot 71$. With $m = 5^5 - 1$ in Theorem 5.2, $\mathcal{N}_\beta(5^5 - 1)$ is positive since $q^2 = 25 > 4W(q^n - 1) - 2W(Q) - 1 = 32 - 8 - 1 = 23$.

Now, take $\beta = 0$. Since Q is odd, after Theorem 5.5 with Lemmas 5.3 and 7.1, it suffices to show that

$$\frac{q^{\frac{n}{2}}}{q-1} > 2 \cdot 2.9 \cdot \left(\frac{q^n - 1}{q-1}\right)^{\frac{1}{4}}, \quad (20)$$

which can be written

$$\frac{x^2}{x-1} > 5.8^4(q-1)^3,$$

where $x = q^n$. Now the function $x^2/(x-1)$ is increasing for $x > 2$ and so, if (20) holds for the pair (q, n) it holds, then it holds for (q, n_1) where $n_1 > n$. Moreover, (20) holds when $n = 7$ and $q \geq 5$. Hence it holds for larger primes than 7. It also holds for $n = 5$ provided $q > 32$. Further, if $n = 5$ and $q < 32$, we can suppose Q is such that its prime divisors less than 16 are (at most) 5 and 11. Hence, with $t = Q$ in Lemma 7.1, $c_4(Q) < 1.469$ and we can replace 2.9 by 1.469 on the right side of (19) with $n = 5$ and this satisfied whenever $n > 6$. Finally, when $(q, n) = (5, 5)$ we have $c_4(Q) < 1.099$ and (20) is satisfied with 2.9 replaced by 1.099.

Summarising we have established the following.

Proposition 7.2. *Let q be an odd prime power and $n > 4$ a prime with $q \equiv 1 \pmod{4}$. Then, for any $\beta \in \mathbb{F}_q$, there exists a 2-primitive $\xi \in \mathbb{F}_{q^n}$ with $\text{Tr}(x) = \beta$.*

7.2. The Case $n = 3$

Here we assume that $n = 3$ and $\beta \in \mathbb{F}_q$, where $q \equiv 1 \pmod{4}$ is prime (so that $4|q^3 - 1$ and $q \geq 5$).

First suppose $\beta \neq 0$. Then, with $n = 3$, using (19) and Theorem 6.6 we obtain the sufficient condition

$$q^{\frac{1}{4}} > 2\sqrt{2} \cdot 4.87/2^{\frac{1}{4}} = 11.5828\dots$$

This is satisfied if $q > 18000$. So assume $q < 18000$ so that $q^3 - 1 < 5.5833 \cdot 10^{12}$. This implies that $\nu(q_0) \leq 11$. Assuming for the moment that also $\nu(q_0) \geq 9$, apply the sieving condition, see Theorem 6.6, with $\nu(k) = 2$ (relating to the two smallest primes dividing $q^3 - 1$) and $s \leq 9$. The largest δ would occur if the set of sieving primes comprise those from 5 to 31. Thus $\delta > 0.26763$ and the condition is satisfied if $q \geq 361$. So we can assume $q < 361$ and $q^3 - 1 < 4.7046 \cdot 10^7$. This implies $\nu(q_0) \leq 8$. Another round of the sieve yields a condition that is satisfied if $q > 173$. So we can assume $q \leq 1169$. A final general round of sieving produces a condition that is satisfied if $q > 128$ so we can assume $q \leq 125$.

The next stage is to apply the full condition of Theorem 6.6 to the remaining prime powers ≤ 125 using the precise decomposition. Even without sieving (i.e., with $k = q_0$) this yields a condition that is satisfied unless $q = 5, 9, 13, 25, 29, 61$ and 121 . We successfully apply sieving for $q = 29, 61$ and 121 , with $\{67, 13, 7\}$, $\{97, 13, 5\}$ and $\{37, 19, 7\}$ as our set of sieving primes respectively. This concludes the case $\beta \neq 0$.

Now suppose $\beta = 0$. From Theorem 6.7 with $k = Q$, the basic condition to be satisfied is

$$q^{\frac{1}{2}} > \sqrt{2}W(Q).$$

Now the primes dividing $Q = q^2 + q + 1$ can only be 3 or primes $\equiv 1 \pmod{6}$. Thus, by Lemma 7.1 with $\ell = 6$ and $t = Q$ (so the possible primes less than 64 dividing t lie in the set $\{3, 7, 13, 19, 31, 37, 43, 61\}$) we have $c_6(Q) < 5.1211$ and a sufficient condition is

$$q^{\frac{1}{2}} > \sqrt{2} \cdot 5.1211 \cdot (q^2 + q + 1)^{\frac{1}{6}}$$

and this is satisfied when $q \geq 144303$. So assume $q < 144303$ which means that $Q < 2.08236 \cdot 10^{10}$. Taking into account the nature of the possible primes dividing Q , this implies $\nu(Q) \leq 8$. Temporarily assuming additionally that $\nu(Q) \geq 6$, apply Theorem 6.7 with $\nu(k) = 1$ and $s \leq 7$ so that $\delta \geq 1 - \frac{1}{7} - \frac{1}{13} - \dots - \frac{1}{61} > 0.62865$. Then the condition is satisfied if $q > 1067$. So, assume $q < 1067$ and apply another round of sieving. We have $\nu(Q) \leq 5$ and take $k = 3$ and $\delta > 0.69633$. The condition then holds if $q > 319$. A final round of general sieving leads to a condition that is satisfied if $q > 185$. Hence we may assume $q \leq 181$. By applying Theorem 6.7 without sieving using exact prime decompositions yields a condition that is satisfied except when $q = 5, 9, 13, 25, 29, 37, 49, 61, 81, 109, 121$ (11 values). Four of these, however,

succumb to the sieving process as follows: $q = 29$ with sieving primes $\{13, 67\}$; $61, \{3, 13, 97\}$; $81, \{13, 73\}$; $109, \{7, 571\}$.

Summing up, we have proved the following proposition.

Proposition 7.3. *Let q be a prime power such that $q \equiv 1 \pmod{4}$. For any $\beta \in \mathbb{F}_q$, there exists a 2-primitive $\xi \in \mathbb{F}_{q^3}$ with $\text{Tr}(\xi) = \beta$, unless $q = 5, 9, 13$ or 25 and $\beta \in \mathbb{F}_q$ or $q = 37, 49$ or 121 and $\beta = 0$.*

8. Quadratic Extensions

For $n = 2$ we recall that we may assume that $\beta \neq 0$. From Theorem 5.2, we have the sufficient criterion that $\mathcal{N}_\beta(q^2 - 1)$ is positive whenever

$$q^{1/2} > 4W(q^2 - 1) - 2W(q + 1) - 1.$$

Similarly, there is a corresponding sieving criterion derivable from Theorem 6.2. The adoption, however, of a strategy found in [1] yields stronger results, so we repeat this approach here.

Lemma 8.1. *For every $\beta \in \mathbb{F}_q^*$, there exist $\theta_1, \theta_2 \in \mathbb{F}_{q^2}$, such that $\{\theta_1, \theta_2\}$ is an \mathbb{F}_q -basis of \mathbb{F}_{q^2} , $\text{Tr}(\theta_1) = \beta$ and $\text{Tr}(\theta_2) = 0$.*

Proof. The trace function is onto, hence there exists some $\theta_1 \in \mathbb{F}_{q^2}$ such that $\text{Tr}(\theta_1) = \beta$. Next, extend $\{\theta_1\}$ to an \mathbb{F}_q -basis of \mathbb{F}_{q^2} , say $\{\theta_1, \theta'_2\}$ and set $\theta_2 := \theta'_2 - \frac{\text{Tr}(\theta'_2)}{\text{Tr}(\theta_1)} \cdot \theta_1$. It is clear that $\{\theta_1, \theta_2\}$ satisfies the desired conditions. ■

Corollary 8.2. *Let $\beta, \theta_1, \theta_2$ be as in Lemma 8.1. For every $\alpha \in \mathbb{F}_q$, we have that $\text{Tr}(\theta_1 + \alpha\theta_2) = \beta$.*

Fix $\beta \in \mathbb{F}_q^*$ and let θ_1, θ_2 be as in Lemma 8.1. Since $\{\theta_1, \theta_2\}$ are \mathbb{F}_q -linearly independent, we have that $\theta_1/\theta_2 \notin \mathbb{F}_q$, that is $\mathbb{F}_{q^2} = \mathbb{F}_q(\theta_1/\theta_2)$. In addition, Corollary 8.2 implies that for every $\alpha \in \mathbb{F}_q$, $\text{Tr}(\theta_1 + \alpha\theta_2) = \beta$.

Write $q^2 - 1 = 2^\ell q_2$, where q_2 is odd, and notice that, since q is odd, $8 \mid q^2 - 1$, that is $\ell \geq 3$, while the fact that $\gcd(q - 1, q + 1) = 2$ implies that $q_2 = r_2 s_2$ where r_2 and s_2 are the 2-free parts of $q + 1$ and $q - 1$ respectively and they are co-prime. Also, set q'_2, r'_2 and s'_2 as the square-free parts of q_2, r_2 and s_2 respectively.

Next, take $r \mid q'_2$ and set \mathcal{Q}_r to be the number of r -free elements of the form $\theta_1 + \alpha\theta_2$ for some $\alpha \in \mathbb{F}_q$, that are squares but not 4th powers. Following the analysis of Section 4, we get that

$$\mathcal{Q}_r = \sum_{x \in \mathbb{F}_q} \omega_r(\theta_1 + x\theta_2) w_2(\theta_1 + x\theta_2) (1 - w_4(\theta_1 + x\theta_2))$$

$$= \sum_{x \in \mathbb{F}_q} \omega_r(\theta_1 + x\theta_2)(w_2(\theta_1 + x\theta_2) - w_4(\theta_1 + x\theta_2)), \quad (21)$$

given that, by definition, for all $\xi \in \mathbb{F}_{q^2}^*$, $w_2(\xi)w_4(\xi) = w_4(\xi)$. In addition, notice that, for all $\xi \in \mathbb{F}_{q^2}^*$, we have that

$$\begin{aligned} w_2(\xi) - w_4(\xi) &= \frac{1}{2} \sum_{\delta|2} \sum_{\text{ord}(\chi_\delta)=\delta} \chi_\delta(\xi) - \frac{1}{4} \sum_{\delta|4} \sum_{\text{ord}(\chi_\delta)=\delta} \chi_\delta(\xi) \\ &= \frac{1}{2} \sum_{\delta|4} \sum_{\text{ord}(\chi_\delta)=\delta} \ell_\delta \chi_\delta(\xi), \end{aligned} \quad (22)$$

where,

$$\ell_\delta := \begin{cases} 1/2 & \text{if } \delta = 1 \text{ or } 2, \\ -1/2 & \text{if } \delta = 4. \end{cases}$$

Furthermore, Lemma 4.1 implies that an element is q'_2 -free if and only if it is 2^i -primitive for some $0 \leq i \leq \ell$. It follows that 2-primitive elements of \mathbb{F}_{q^2} are the q'_2 -free elements that are squares, but not 4th powers. In other words, it suffices to show that $\mathcal{Q}_{q'_2} \neq 0$, while it is clear that

$$\mathcal{Q}_{q'_2} \neq 0 \Rightarrow \mathcal{N}_\beta(q^2 - 1) \neq 0.$$

In (21), we replace ω_r by its expression and $w_2 - w_4$ by its expression in (22) and we get that

$$\begin{aligned} \frac{4\mathcal{Q}_r}{\theta(r)} &= \left(\sum_{\substack{d|r \\ \delta|4}} \frac{\mu(d)}{\phi(d)} 2\ell_\delta \sum_{\substack{\text{ord}(\chi_d)=d \\ \text{ord}(\chi_\delta)=\delta}} \mathcal{Y}(\chi_d, \chi_\delta) \right) \\ &= \left(\sum_{d|r} \frac{\mu(d)}{\phi(d)} \sum_{\text{ord}(\chi_d)=d} \mathcal{Z}(\chi_d) \right), \end{aligned} \quad (23)$$

where

$$\mathcal{Y}(\chi_d, \chi_\delta) := \sum_{\alpha \in \mathbb{F}_q} \psi_{d,\delta}(\theta_1 + \alpha\theta_2) = \psi_{d,\delta}(\theta_2) \sum_{\alpha \in \mathbb{F}_q} \psi_{d,\delta} \left(\frac{\theta_1}{\theta_2} + \alpha \right)$$

and

$$\mathcal{Z}(\chi_d) := \mathcal{Y}(\chi_d, \chi_1) + \mathcal{Y}(\chi_d, \chi_2) - \mathcal{Y}(\chi_d, \eta_1) - \mathcal{Y}(\chi_d, \eta_2),$$

where $\psi_{d,\delta} := (\chi_d \chi_\delta)$ is the product of the corresponding characters, χ_2 is the quadratic character and η_1, η_2 are the two multiplicative characters of order exactly 4. Furthermore, since d is odd and $\delta \mid 4$, it is clear that $\psi_{d,\delta}$ is trivial if and only if $d = \delta = 1$.

Recall that $\mathbb{F}_{q^2} = \mathbb{F}_q(\theta_1/\theta_2)$. First, assume $q \equiv 1 \pmod{4}$. Then $4 \nmid q + 1$. Hence Lemma 4.3 implies that

- (i) for χ_1 , $|\mathcal{Z}(\chi_1)| \geq q - 1 - 2\sqrt{q}$,
- (ii) for $1 \neq \text{ord}(\chi_d) \mid q + 1$, $|\mathcal{Z}(\chi_d)| \leq 2 + 2\sqrt{q}$,
- (iii) for $\text{ord}(\chi_d) \nmid q + 1$, $|\mathcal{Z}(\chi_d)| \leq 4\sqrt{q}$.

Next, assume that $q \equiv 3 \pmod{4}$. Then $4 \mid q + 1$ and Lemma 4.3 implies that

- (i) for χ_1 , $|\mathcal{Z}(\chi_1)| \geq q - 3$,
- (ii) for $1 \neq \text{ord}(\chi_d) \mid q + 1$, $|\mathcal{Z}(\chi_d)| \leq 4$,
- (iii) for $\text{ord}(\chi_d) \nmid q + 1$, $|\mathcal{Z}(\chi_d)| \leq 4\sqrt{q}$.

We substitute the above in (21) and arrive at the following conclusions.

Proposition 8.3. *Let q , and r be as above and let r_1 be the product of the prime divisors of r that divide $q + 1$.*

- (i) *If $q \equiv 1 \pmod{4}$, then*

$$\frac{4\mathcal{Q}_r}{\theta(r)} \geq q + 1 - 4W(r)\sqrt{q} + 2W(r_1)(\sqrt{q} - 1); \quad (24)$$

that is, if

$$q + 1 > 4 \left(W(r)\sqrt{q} - W(r_1) \left(\frac{\sqrt{q} - 1}{2} \right) \right),$$

then $\mathcal{Q}_r \neq 0$.

- (ii) *If $q \equiv 3 \pmod{4}$, then*

$$\frac{4\mathcal{Q}_r}{\theta(r)} \geq q + 1 - 4W(r)\sqrt{q} + 4W(r_1)(\sqrt{q} - 1); \quad (25)$$

that is, if

$$q + 1 > 4(W(r)\sqrt{q} - W(r_1)(\sqrt{q} - 1)),$$

then $\mathcal{Q}_r \neq 0$.

Again, as in previous sections, we employ a sieving inequality as follows.

Proposition 8.4. (Sieving inequality) *Let $r \mid q'_2$. Write $r = kp_1 \cdots p_s$, where p_1, \dots, p_s are distinct prime divisors of r . Then*

$$\mathcal{Q}_r \geq \sum_{i=1}^s \mathcal{Q}_{r_i} - (s - 1)\mathcal{Q}_{r_0}.$$

Write $q'_2 = kp_1 \cdots p_s$, where p_1, \dots, p_s are distinct primes and $\varepsilon := 1 - \sum_{i=1}^s 1/p_i$, with $\varepsilon = 1$ when $s = 0$. Further, suppose that $p_i \mid q + 1$ for $i = 1, \dots, r$ and $p_i \nmid q + 1$ for $i = r + 1, \dots, s$. Finally, set $\varepsilon' := 1 - \sum_{i=1}^r 1/p_i$ and let k_1 be the part of k , that divides $q + 1$.

Theorem 8.5. *Let q and q'_2 be as above. Additionally, let ε and ε' be as above and assume that $\varepsilon > 0$. Then the following statements hold:*

(i) If $q \equiv 1 \pmod{4}$ and

$$q + 1 > 4 \left[W(k) \left(\frac{s-1}{\varepsilon} + 2 \right) \sqrt{q} - W(k_1) \left(\frac{r-1+\varepsilon'}{\varepsilon} + 1 \right) \left(\frac{\sqrt{q}-1}{2} \right) \right],$$

then $\mathcal{Q}_{q_2'} \neq 0$.

(ii) If $q \equiv 3 \pmod{4}$ and

$$q + 1 > 4 \left[W(k) \left(\frac{s-1}{\varepsilon} + 2 \right) \sqrt{q} - W(k_1) \left(\frac{r-1+\varepsilon'}{\varepsilon} + 1 \right) (\sqrt{q}-1) \right],$$

then $\mathcal{Q}_{q_2'} \neq 0$.

In particular, it is the case that $\mathcal{Q}_{q_2'} > 0$ whenever

$$q \geq 4W(k) \left(\frac{s-1}{\varepsilon} + 2 \right). \quad (26)$$

Proof. Proposition 8.4 implies that

$$\mathcal{Q}_{q_2'} \geq \sum_{i=1}^s \mathcal{Q}_{kp_i} - (s-1)\mathcal{Q}_k \geq \varepsilon\mathcal{Q}_k - \sum_{i=1}^s \left| \mathcal{Q}_{kp_i} - \left(1 - \frac{1}{p_i}\right) \mathcal{Q}_k \right|. \quad (27)$$

Notice that $\theta(kp_i) = \theta(k)(1 - 1/p_i)$. It follows from (23) that

$$\mathcal{Q}_{kp_i} - \left(1 - \frac{1}{p_i}\right) \mathcal{Q}_k = \frac{\theta(k)(p_i-1)}{4p_i} \sum_{d|k} \frac{\mu(dp_i)}{\phi(dp_i)} \sum_{\text{ord}(\chi_{dp_i})=dp_i} \mathcal{Z}(\chi_{dp_i}). \quad (28)$$

First assume that $q \equiv 1 \pmod{4}$. We repeat the arguments that led us to (24) for (28). If $i = 1, \dots, r$, i.e., $p_i \mid q+1$, then

$$\begin{aligned} & \left| \mathcal{Q}_{kp_i} - \left(1 - \frac{1}{p_i}\right) \mathcal{Q}_k \right| \\ & \leq \theta(k) \left(1 - \frac{1}{p_i}\right) \left[2\sqrt{q}(W(k) - W(k_1)) + (1 + \sqrt{q})W(k_1) \right], \end{aligned}$$

since $W(kp_i) = 2W(k)$ and $W(k_1p_i) = 2W(k_1)$. Similarly, if $i = r+1, \dots, s$, i.e., $p_i \nmid q+1$, then

$$\left| \mathcal{Q}_{kp_i} - \left(1 - \frac{1}{p_i}\right) \mathcal{Q}_k(\theta, \alpha) \right| \leq \theta(k) \left(1 - \frac{1}{p_i}\right) 2\sqrt{q}W(k).$$

The combination of (24), (27), (28) and the above bounds yields the desired result.

The $q \equiv 3 \pmod{4}$ case follows similarly, but with (25) in mind. \blacksquare

We are now ready to proceed with our existence results. We start with the simplest condition to check, which follows from (26) and the fact that $W(q_2) = W(q^2 - 1)/2$, namely

$$\sqrt{q} \geq 2W(q^2 - 1).$$

Now, recalling that $8|(q^2 - 1)$ and apply the bound of for $c_6(t)$ in Lemma 7.1, with $t = (q^2 - 1)/4$ to $W(q_0) = W((q^2 - 1)/4)$ we deduce that a sufficient condition is

$$q > (2 \cdot 46.103)^6/4 \simeq 1.536 \cdot 10^{11}.$$

So assume $q < 1.537 \cdot 10^{11}$ and so $q^2 - 1 < 2.363 \cdot 10^{22}$. It follows that $\nu(q^2 - 1) \leq 17$ and so $\nu(q_2) \leq 16$. For the moment suppose also $\nu(q^2 - 1) \geq 11$. We proceed to employ the criterion (26) with $\nu(k) = 2$ and $s \leq 14$ so that $\varepsilon \geq 1 - \frac{1}{7} - \frac{1}{11} - \dots - \frac{1}{59} \geq 0.335869$, the sum relating to the 14 primes between 7 and 59. Then (26) holds whenever $q > 488500$. Now assume $q < 488500$ which implies that $q^2 - 1 < 2.3863 \cdot 10^{11}$. Hence $q^2 - 116893 \cdot 10^9$ and $\nu(q^2 - 1) \leq 10$. Suppose $\nu(q^2 - 1) = 10$ and apply the sieve with $\nu(k) = 1, s = 8$. The condition holds if $q > 41101$. So assume $q < 41101$ so that $q^2 - 1 \leq 1.6893 \times 10^9$. This yields $\nu(q^2 - 1) \leq 9$. Again apply the sieve with $\nu(k) = 1, s \leq 7$. The condition then holds if $q > 25457$. A final round of sieving with $q < 25457, q^2 - 1 < 6.4803 \cdot 10^8$ yields success if $q > 14850$. So we can suppose $q < 14850, q^2 - 1 < 2.2053 \cdot 10^8$. In the interval $3 \leq q \leq 14850$, there are exactly 1784 odd prime powers and we first attempt to use Proposition 8.3. A quick computation reveals that, in the interval in question, there are exactly 744 odd prime powers, where (24) or (25), accordingly, do not hold, with all the mentioned quantities explicitly computed, with $q = 14821$ being the largest among them.

Then, we move on to the sieving part, i.e., Theorem 8.5. Namely, we attempt to satisfy the conditions of Theorem 8.5 as follows. Until we run out of prime divisors of k , or until $\varepsilon \leq 0$, we always add to the set of sieving primes, that is, the primes p_1, \dots, p_s in Theorem 8.5, the largest prime divisor not already contained in the set. If, for one such set of sieving primes, the condition of Theorem 8.5 is valid, then the desired result holds for the prime power in question.

This procedure was successful, for most of the aforementioned 744 prime powers. The 101 exceptional prime powers, for which this procedure failed are listed in the $n = 2$ line of Table 1.

So, to sum up our results so far, we have proved the following theorem.

Theorem 8.6. *For every odd prime power q not listed in Table 1 and $\beta \in \mathbb{F}_q^*$, there exists some 2-primitive $\xi \in \mathbb{F}_{q^2}$ such that $\text{Tr}(\xi) = \beta$.*

9. Completion of the Proof of Theorem 1.2

Then we move on to an explicit verification for the remaining possible exceptions, that is the pairs of Table 1. For this purpose, for all the corresponding pairs (q, n) , we check whether the set of the traces of the 2-primitive elements of \mathbb{F}_{q^n}

coincides with \mathbb{F}_q^* , when $n = 2$, and with \mathbb{F}_q , when $n = 3$. This test required about 3-4 minutes of computer time in a modern mid-range laptop.

n	q	#
2	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, 109, 113, 121, 125, 127, 131, 137, 139, 149, 151, 157, 169, 173, 181, 191, 197, 199, 211, 229, 239, 241, 269, 281, 307, 311, 331, 337, 349, 361, 373, 379, 389, 409, 419, 421, 461, 463, 509, 521, 529, 569, 571, 601, 617, 631, 659, 661, 701, 761, 769, 841, 859, 881, 911, 1009, 1021, 1231, 1289, 1301, 1331, 1429, 1609, 1741, 1849, 1861, 2029, 2281, 2311, 2729, 3541	101
3	5, 9, 13, 25, 37, 49, 121	7
Total:		108

Table 1: Pairs (q, n) for which the existence of 2-primitive elements with prescribed trace was not dealt with theoretically.

The computations validated all the existence claims in Theorem 1.2 for all the pairs (q, n) of Table 1 with the exception, when $n = 2$, of $q = 3, 5, 7, 9, 11, 13$ and 31, these being genuine exceptions. In particular, they were successful for all pairs (q, n) with $n = 3$. Finally, for the exceptions we present the possible traces of 2-primitive elements in Table 2. This completes the proof of Theorem 1.2.

q	Traces	#
3	0	1
5	2, 3	2
7	1, 2, 5, 6	4
9*	$\pm 1, \pm i$	4
11	1, 2, 3, 4, 7, 8, 9, 10	8
13	1, 3, 4, 5, 6, 7, 8, 9, 10, 12	10
31	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 18, 19, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30	28

* For $q = 9$, i is a root of $X^2 + 1 \in \mathbb{F}_3[X]$

Table 2: Traces of 2-primitive elements of \mathbb{F}_{q^2} for $q = 3, 5, 7, 9, 11, 13$ and 31.

References

- [1] S.D. Cohen, Primitive elements and polynomials with arbitrary trace, *Discrete Math.* **83** (1) (1990) 1–7.
- [2] S.D. Cohen, Primitive elements on lines in extensions of finite fields, In: *Finite Fields: Theory and Applications* (Eds: G. McGuire, G.L. Mullen, D. Panario, I.E. Shparlinski), Providence, RI, American Mathematical Society, 2010.
- [3] S.D. Cohen and S. Huczynska, The primitive normal basis theorem – without a computer, *J. London Math. Soc.* **67** (1) (2003) 41–56.
- [4] S.D. Cohen and G. Kapetanakis, The trace of 2-primitive elements of finite fields, *Acta Arith.* **192** (4) (2020) 397–416.

- [5] S.D. Cohen and M. Prešern, Primitive finite field elements with prescribed trace, *Southeast Asian Bull. Math.* **29** (2) (2005) 283–300.
- [6] D. Hachenberger and D. Jungnickel, *Topics in Galois Fields*, Switerland, Springer Nature, 2020.
- [7] L.K. Hua, *Introduction to Number Theory* (translated by P. Shiu), Berlin-Heidelberg, Springer-Verlag, 1982.
- [8] S. Huczynska, G.L. Mullen, D. Panario, D. Thomson, Existence and properties of k -normal elements over finite fields, *Finite Fields Appl.* **24** (2013) 170–183.
- [9] N.M. Katz, An estimate for character sums, *J. Amer. Math. Soc.* **2** (2) (1989) 197–200.
- [10] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge, Cambridge University Press, 1997.
- [11] W.M. Schmidt, *Equations over Finite Fields, An Elementary Approach*, Berlin-Heidelberg, Springer-Verlag, 1976.
- [12] W. Zhang, Moments of generalized quadratic Gauss sums weighted by L -functions, *J. Number Theory* **92** (2) (2002) 304–314.