Primitive Normal Bases with Prescribed Trace

S. D. Cohen[1], D. Hachenberger[2]

[1] Department of Mathematics, University of Glasgow, Glasgow G12 8QW, Scotland
(e-mail: sdc@maths.gla.ac.uk)
[2] Institut für Mathematik, Universität Augsburg, D-86159 Augsburg, Germany
(e-mail: Hachenberger@math.uni-augsburg.de)

Received: June 15, 1998; revised version: December 2, 1998

Abstract. Let E be a finite degree extension over a finite field $F = \mathrm{GF}(q)$, G the Galois group of E over F and let $a \in F$ be nonzero. We prove the existence of an element w in E satisfying the following conditions:

- w is primitive in E, i.e., w generates the multiplicative group of E (as a module over the ring of integers).
- the set $\{w^g \mid g \in G\}$ of conjugates of w under G forms a normal basis of E over F.
- the (E, F)-trace of w is equal to a.

This result is a strengthening of the *primitive normal basis theorem* of Lenstra and Schoof [10] and the theorem of Cohen on *primitive elements with prescribed trace* [3]. It establishes a recent conjecture of Morgan and Mullen [14], who, by means of a computer search, have verified the existence of such elements for the cases in which $q \leq 97$ and $n \leq 6$, n being the degree of E over F. Apart from two pairs (F, E) (or (q, n)) we are able to settle the conjecture purely theoretically.

Keywords: Finite field, Primitive element, Normal basis, Free element, Trace, Character sum

1 Introduction

Let E be a finite field. It is well-known that the multiplicative group $(E^*, \cdot)$ of E is cyclic, i.e., free on one generator as a module over the ring of integers. Every generator of $(E^*, \cdot)$ is called *a primitive element of* E.

If $F = \mathrm{GF}(q)$, the Galois field with cardinality q, is a subfield of E, then E is a Galois extension over F with cyclic Galois group G. A canonical generator of G is the Frobenius automorphism σ which maps each element of E onto its qth power. It was first proved by Hensel [8] that E admits *a normal basis over* F, i.e., there exists an element in E such that its conjugates under G form an F-basis of E. The additive group $(E, +)$ of E carries a module structure over the polynomial ring $F[x]$ with respect to σ: the scalar multiplication is defined by

$$f \circ \alpha := f(\sigma)(\alpha), \quad f \in F[x], \ \alpha \in E. \tag{1.1}$$

The normal basis theorem simply states that $(E, +)$ is free on one generator as $F[x]$-module. Since the normal bases for E over F are precisely the sets of G-conjugates of $F[x]$-generators of $(E, +)$, every such generator is called *a normal element of* E *over* F. (The terminology is not consistent; the term *free in* E *over* F is frequently used in [7]; *primitive of the second kind* is used in [1].)

The combination of *primitivity and normality* was first studied by Carlitz [1]. He proved that there are at most finitely many pairs (F, E) of finite fields (with E an extension of F) for which there does not exist an element in E which is primitive *and* normal over F. Such an element is called *primitive of the third kind* in [1]): we shall use the term *primitive* F*-normal element.* In the case where the cardinality q of F is a prime number, the existence of a primitive F-normal element was proved in Davenport [5]. Lenstra and Schoof [10] affirmatively settled the existence of primitive F-normal elements for all finite fields F and all finite extensions E over F.

Coding Theory [12] motivated the study of *primitive elements with prescribed trace* by several workers [3,9,13,14]. Recall that the (E, F)-trace (or F-trace or simply trace) $\mathrm{Tr}(w)$ of $w \in E$ is the sum of the G-conjugates of w, i.e.,

$$\mathrm{Tr}(w) := \mathrm{Tr}_{E,F}(w) := \sum_{i=0}^{n-1} \sigma^i(w) = \sum_{i=0}^{n-1} w^{q^i}, \tag{1.2}$$

where $n := [E : F]$ denotes the degree of E over $F = \mathrm{GF}(q)$. The complete answer was given by Cohen [3]: if $n \geq 3$ and $(q, n) \neq (4, 3)$, then, for every $a \in F$, there exists a primitive element $w \in E$ such that $\mathrm{Tr}(w) = a$. Moreover, if $n = 2$ or $(q, n) = (4, 3)$, then, for every nonzero $a \in F$, there exists a primitive element $w \in E$ such that $\mathrm{Tr}(w) = a$.

In respect of primitive elements with nonzero trace, parts of the latter result were independently proved by Jungnickel and Vanstone [9]: existence was settled for every nonzero $a \in F$ whenever $n \geq 3$, whereas for $n = 2$ it was shown that there are at most 143 exceptional values for q. The case of nonzero trace and $q = 2$ had been handled already by Moreno [13].

The aim of the present work is the combination of *primitivity, normality* and *prescribed trace*. Our main result is a strengthening of both the *primitive normal basis theorem* of Lenstra and Schoof and the theorem of Cohen on *primitive elements with prescribed trace*. Evidently, the universality of the result makes it of great potential use for constructions dependent on the existence of such bases.

Main Theorem. *Let E be a finite extension over a finite field F and let $a \in F$ be nonzero. Then there exists an element w in E which is primitive and F-normal and has F-trace equal to a.*

Observe (e.g., by (1.2)) that a normal element never has trace equal to zero, whence the assumption on a is necessary.

The existence of primitive F-normal elements with prescribed trace has been conjectured recently by Morgan and Mullen [14, Conjecture 1] (see also Conjecture 8 in [15][1]) and this has been the motivation for our work. In [14] it is mentioned that existence holds whenever $q \leq 97$ and $n \leq 6$: given $F = \mathrm{GF}(q)$ with $q \leq 97$, a nonzero element $a \in F$ and $n \leq 6$, they have determined a monic polynomial $f_{n,a} \in F[x]$ of degree n, irreducible over F, with roots being primitive and F-normal, whose x^{n-1}-coefficient is equal to $-a$ (of course this solves the problem for the triple (q, n, a)).

Apart from two pairs (q, n) we are able to settle the conjecture of Morgan and Mullen purely theoretically, i.e., without searching in the underlying fields. The two exceptional pairs are covered by their computational work, though we include our independent verification in these particular cases.

In Section 2 we prove preliminary existence results, i.e., for some classes of pairs (q, n) the problem is reduced to the existence of primitive elements with prescribed trace (which is covered by [3]), or to the existence of primitive F-normal elements (in which case [10] applies). For example, if $n = 2$, then every primitive element is already normal (e.g., see [6]) whence all pairs $(q, 2)$ are covered by [3]. Or, if $q = 2$, then nonzero trace is the same as trace equal to 1, whence the problem is a particular instance of [10].

The essential ingredients for the main part of the proof are (estimates of) character sums. The use of character sums for the study of primitive elements with additional properties already goes back to the work of Carlitz [1] and Davenport [5]; it is of fundamental importance in [3], [9], [13] and [10], also. Further applications of this method can be found in Cohen's survey [4]. In Section 3 we determine an expression in terms of character sums for the characteristic function of the set of primitive F-normal elements with prescribed trace a. This formula is used in Section 4, where a sufficient number-theoretical condition for this set to be nonempty is derived. For moderate sizes for q and n this condi-

[1] There have been attempts by others to resolve this conjecture. These have not been substantiated.

tion can be checked with the aid of a computer algebra package equipped with algorithms for factorizing integers. For our calculations, we have used Maple (in the version Maple V, Release 4). Whereas our estimate is efficient for $n \geq 6$, the cases $n = 3, 4$ and 5 are handled in Section 5 by applying a basic counting argument in combination with effective estimates for the number of primitive elements with prescribed trace. The outcome of Section 4 and Section 5 is a concrete list of 38 pairs (q, n) containing all for which the conjecture of Morgan and Mullen fails. Apart from the two cases (7, 3) and (13, 4), all entries of this list are ruled out theoretically in Section 6. Fortunately, the remaining two pairs have parameters allowing direct verification in the fields.

2 Preliminary Existence Results

Throughout, let $q > 1$ be a prime power and $n \geq 2$ an integer. By $\mathcal{S}$ we denote the set of all pairs (q, n) for which the following statement is true:

for every nonzero $a \in F = \mathrm{GF}(q)$ there exists a primitive F-normal element $w \in E = \mathrm{GF}(q^n)$ whose (E, F)-trace is equal to a.

When considering E as $F[x]$-module, the notion of F-order is of fundamental importance (see [10] or [6,7]; it is the additive analogue of that of the *multiplicative order* of a nonzero field element): for $w \in E$ the *F-order of w* is the monic polynomial f of least degree in $F[x]$ such that $f(\sigma)(w) = 0$; it is denoted by $\mathrm{Ord}_F(w)$ or $\mathrm{Ord}_q(w)$. Since $w^{q^n} - w = 0$ for all $w \in E$, the F-order of each $w \in E$ is a divisor of $x^n - 1$. In fact, $x^n - 1$ is the minimal polynomial of E as an F-vector space with respect to σ. Then $w \in E$ is normal over F if and only if $\mathrm{Ord}_F(w) = x^n - 1$. Similarly, the multiplicative order of w is denoted by $\mathrm{ord}(w)$; it divides the exponent $q^n - 1$ of $(E^*, \cdot)$; w is primitive if and only if $\mathrm{ord}(w) = q^n - 1$.

Throughout, let p be the characteristic of F and

$$t := t_n := \frac{x^n - 1}{x - 1}. \tag{2.3}$$

Then $t(\sigma)(w) = \mathrm{Tr}(w)$. Moreover, $\mathrm{Tr}(w) = 0$ if and only if $\mathrm{Ord}_F(w)$ divides t. Again, this shows that a normal element necessarily has nonzero trace. The converse of the latter however is not true in general. In fact, it holds precisely when n is a power of the characteristic p. Consequently, in that case, the existence of primitive F-normal elements with prescribed trace already follows from Cohen [3]. Proposition 2.2 is a generalization of the latter argument. We require the following lemma which is proved in [7, Proposition 5.5].

Lemma 2.1 *Let $n = \pi n'$ where $\pi \geq 1$ is a power of p and n' is prime to p. Let K be the intermediate field of degree n' over F. Then $w \in E$ is normal over F if and only if $Tr_{E,K}(w)$ is normal in K over F.* □

Proposition 2.2 *If p divides n, then $(q, n) \in \mathcal{S}$.*

Proof. Let $n = \pi n'$ and K be as in Lemma 2.1. Given a nonzero element a of F, choose $v \in K$, normal over F with (K, F)-trace a. By Cohen's theorem there exists a primitive $w \in E$ with $\mathrm{Tr}_{E,K}(w) = v$. By Lemma 2.1, w is normal over F. The transitivity of the trace mappings shows that $\mathrm{Tr}(w) = a$. □

We continue with a sufficient condition for normality. It follows immediately from our short discussion on F-order and the definition of t.

Lemma 2.3 *Assume that the F-order of $w \in E$ is divisible by t and that $Tr(w)$ is nonzero. Then w is normal over F.* □

We have already mentioned that for $n = 2$ primitivity implies normality. On the other hand, $n = 2$ is the most difficult instance when considering primitive elements with prescribed trace and demands particular attention (see [2], [3] and also [9]). The following reduction to Cohen's theorem incorporates the case $n = 2$.

Proposition 2.4 *If n is a prime different from p and if the multiplicative order of q modulo n is equal to $n - 1$, then $(q, n) \in \mathcal{S}$.*

Proof. The assumption that q is a primitive root modulo n implies that t is irreducible over F. Moreover, since n is prime, $x^n - 1 = (x - 1)t$ is the complete factorization of $x^n - 1$ over F. If w is an element of E but not of F (e.g., a primitive element of E) then $\mathrm{Ord}_F(w)$ does not divide $x - 1$. Thus, t divides $\mathrm{Ord}_F(w)$. If additionally w has nonzero trace, then w is normal over F by Lemma 2.3. In particular, if w is primitive with nonzero trace, then w is normal over F. Hence, $(q, n) \in \mathcal{S}$ by Cohen's theorem. □

So far, we have made considerable use of the existence of primitive elements with prescribed trace. In the following we shall see that some (other) instances of our problem can be reduced to the existence of primitive F-normal elements, i.e., the theorem of Lenstra and Schoof is applicable.

Lemma 2.5 *Let $\mathcal{P}$ be the set of primitive elements of E and $\lambda \in E$ a nonzero element. Then $\lambda\mathcal{P} = \mathcal{P}$ if and only if the square-free part of $(q^n - 1)/\mathrm{ord}(\lambda)$ is equal to the square-free part of $q^n - 1$.*

Proof. Let $\prod_r r^{\alpha_r}$ be the prime power factorization of $q^n - 1$. In accordance with this, let

$$(E^*, \cdot) = \prod_r S_r$$

be the decomposition of the multiplicative group of E into the product of its Sylow subgroups (S_r being the Sylow r-subgroup). For a nonzero γ of E

let $\prod_r \gamma_r$ be the decomposition of γ into its Sylow-components. Since every subgroup of $(E^*, \cdot)$ is cyclic and the function ord is multiplicative, then γ is primitive if and only if each γ_r generates S_r, i.e., if and only if $\mathrm{ord}(\lambda_r) = r^{\alpha_r}$ for each r.

Let $\lambda = \prod_r \lambda_r$ be nonzero. If λ_r generates S_r then so does λ_r^{-1}. If γ is a primitive element with S_r-component λ_r^{-1} then $\lambda\gamma$ is not primitive since its S_r-component is equal to 1 and thus not a generator of S_r. Assume conversely that no S_r-component of λ has (maximal) multiplicative order r^{α_r}. Letting γ again be primitive, we see that for each r, $\lambda_r\gamma_r$ is a generator of the S_r: this is because the subgroups of cyclic groups of prime power order are linearly ordered by inclusion and λ_r lies in the unique maximal subgroup of S_r but γ_r does not.

Summarizing, we have proved that $\lambda\gamma$ is primitive for all $\gamma \in \mathscr{P}$ if and only if all prime divisors of $q^n - 1$ divide $(q^n - 1)/\mathrm{ord}(\lambda)$. □

As an application of Lemma 2.5, we obtain the following result which is Theorem 4 in [14].

Proposition 2.6 *If the square-free part of $q - 1$ divides n, then $(q, n) \in \mathscr{S}$.*

Proof. Let r be a prime divisor of $q - 1$. By assumption, r divides n and therefore the maximal power of r dividing $q^n - 1$ exceeds the maximal power of r dividing $q - 1$ (the latter is covered e.g. by [7, Lemma 19.5]). Consequently, Lemma 2.5 applies to all $\lambda \in F^*$. Now let a be a nonzero element of F. Take any primitive F-normal w in E (which exists by the theorem of Lenstra and Schoof). A suitable choice of $\lambda \in F^*$ gives that $\mathrm{Tr}(\lambda w) = a$. Of course, since $\lambda \in F^*$, λw is normal over F. The crucial fact is that by the assumption on the parameters q and n, λw likewise is primitive. Thus, everything is proved. □

We finally summarize the results of the present section as follows:

Theorem 2.7 *If (q, n) is not contained in $\mathscr{S}$, then, necessarily, all the following conditions hold:*

(1) $n \geq 3$;
(2) $q \geq 3$;
(3) *n and q are relatively prime*;
(4) *the square-free part of $q - 1$ does not divide n*;
(5) *if n is prime, then q is not a primitive root modulo n.* □

3 Character Sums and Characteristic Functions

If S is a set and R a subset of S, the *characteristic function of R (in S)* is the mapping $S \to C$ of S into the field C of complex numbers defined by $x \to 1$ if $x \in R$ and $x \to 0$, otherwise.

Let again $n \geq 2$, $F = \mathrm{GF}(q)$, p be the characteristic of F and $E = \mathrm{GF}(q^n)$. For $a \in F$, let $\mathscr{P}_a$ and $\mathscr{N}_a$ be the sets of primitive elements and F-normal elements, respectively, in E with F-trace a. In the present section we shall give an expression for the characteristic function of $\mathscr{P}_a \cap \mathscr{N}_a$ in terms of character sums. Our considerations include a multiplicative, an additive and a trace part, and indeed combinations of these. The contents of the multiplicative and additive parts and the (remarkable) analogy between them go back to the work of Carlitz [1] and of Davenport [5] (see also Section 2 in [10]). For the basic theory of characters of finite fields, we refer to [11].

The multiplicative part

Let e be a divisor of $q^n - 1$ and let $v \in E^*$. Then v is said to be *not any kind of eth power* (see [4]) if e and $(q^n - 1)/\mathrm{ord}(v)$ are relatively prime. For $w \in E^*$ let

$$M_e(w) := \frac{\varphi(e)}{e} \sum_{d|e} \frac{\mu(d)}{\varphi(d)} \sum_{(\eta,d)} \eta(w), \tag{3.1}$$

where φ denotes the Euler totient function, μ the Möbius function, the first sum runs over all positive divisors of e and the second sum runs over all multiplicative characters of E having order exactly d. The following derives from Carlitz [1] (though the original idea in this context is attributed to I. M. Vinogradov).

Proposition 3.1 *M_e is the characteristic function of the set of all w in E^* which are not any kind of eth power. In particular, $M_{q^n-1}(w) = 1$ if and only if w is primitive. Moreover, with the convention that $M_e(0) := 0$, we have that $\sum_{w \in E} M_{q^n-1}(w) = \varphi(q^n - 1)$ is the total number of primitive elements of E.* □

The additive part

Let f be a monic F-divisor of $x^n - 1$ and let $v \in E$. Then v is said to be *not any kind of fth multiple* if f and $(x^n - 1)/\mathrm{Ord}_F(v)$ are relatively prime. Of course, if n is indivisible by the characteristic p (the situation with which we are principally concerned), then this is equivalent to $\mathrm{Ord}_F(v)$ being divisible by f. For $w \in E$ let

$$A_f(w) := \frac{\phi_q(f)}{q^{\deg(f)}} \sum_{g|f} \frac{\mu_q(g)}{\phi_q(g)} \sum_{(\chi,g)} \chi(w), \tag{3.2}$$

where ϕ_q and μ_q denote the Euler function and the Möbius function, respectively, for the ring $F[x]$, deg the degree of a polynomial; the first sum runs over all monic F-divisors of f and the second sum runs over all additive characters of E having F-order exactly g. The latter makes sense, since (see [10]) the

character group $\hat{E}$ of $(E, +)$ is turned into a module over $F[x]$ with respect to σ by defining

$$(g \circ \chi)(w) := \chi(g \circ w), \quad g \in F[x], \ w \in E, \ \chi \in \hat{E} \tag{3.3}$$

(compare this with (1.1)). With respect to this action, the F-order of an additive character is defined analogously as the F-order of a field element. Also, $\hat{E}$ is annihilated by $x^n - 1$; moreover, it is free on one generator, whence $\hat{E}$ and $(E, +)$ are isomorphic as $F[x]$-modules. As for elements of (the additive group of) E, for every monic F-divisor g of $x^n - 1$, there are precisely $\phi_q(g)$ additive characters having F-order g. The following is the additive analogue of Proposition 3.1. We shall include a proof, since this generalizes the corresponding aspect in [10], where a proof is omitted.

Proposition 3.2 *A_f is the characteristic function of the set of all w in E which are not any kind of fth multiple. In particular, $A_{x^n-1}(w) = 1$ if and only if w is normal over F. Moreover, $\sum_{w \in E} A_{x^n-1}(w) = \phi_q(x^n - 1)$ is the total number of normal elements of E over F.*

Proof. Observe first that

$$\frac{\phi_q(f)}{q^{\deg(f)}} = \frac{\phi_q(\nu(f))}{q^{\deg(\nu(f))}}, \tag{3.4}$$

where $\nu(f)$ denotes the square-free part of f. Since $\mu_q(g) = 0$ if and only if g is not square-free, it follows that $A_f = A_{\nu(f)}$. Using the multiplicativity of the mappings ϕ_q and μ_q as well as that of the function Ord_F (see e.g. [7, Theorem 8.6]), we obtain

$$A_f(w) = \prod_g \frac{q^{\deg(g)} - 1}{q^{\deg(g)}} \prod_g \left(1 - \frac{1}{q^{\deg(g)} - 1} \sum_{(\chi, g)} \chi(w) \right), \tag{3.5}$$

where the products run over all monic irreducible F-divisors of f.

Now, if w is "some kind of fth multiple", i.e., if $w = g(\sigma)(\alpha)$ for some irreducible F-divisor g of f and some $\alpha \in E$, then, by (3.2), $\chi(w) = 1$ for all χ having F-order g. Thus the factor in the second product of $A_f(w)$ in (3.5) corresponding to g is equal to zero, whence $A_f(w) = 0$. Conversely, if w is not any kind of fth multiple, we claim that $\sum_{(\chi, g)} \chi(w) = -1$ for every irreducible F-divisor g of f. Were this true, then $A_f(w) = 1$ would follow readily.

To prove the claim we first introduce some useful terminology: for a monic divisor g of $x^n - 1$ let $C_{F,g}$ be the set of additive characters of E having F-order dividing g. This set is an $F[x]$-submodule of $\hat{E}$. Its dual subgroup

$$C_{F,g}^{\perp} := \{w \in E \mid \chi(w) = 1 \text{ for all } \chi \in C_{F,g}\} \tag{3.6}$$

is exactly the set $U_{F,(x^n-1)/g}$ of all elements of E whose F-orders divide $(x^n - 1)/g$. The latter is an $F[x]$-submodule of E (see [7, Theorem 8.3]). By an elementary result on character sums,

$$\frac{1}{|C_{F,g}|}\sum_{\chi\in C_{F,g}}\chi = \frac{1}{q^{\deg(g)}}\sum_{\chi\in C_{F,g}}\chi \tag{3.7}$$

is the characteristic function of $U_{F,(x^n-1)/g}$.

We now return to our situation above. If w is not any kind of fth multiple, then for every irreducible F-divisor g of f, w is not contained in the dual subgroup of $C_{F,g}$. Consequently, observing that $\chi \in C_{F,g}$ has F-order either equal to 1 or g, we have

$$0 = \sum_{\chi\in C_{F,g}}\chi(w) = \sum_{(\chi,g)}\chi(w) + \chi_0(w) = \sum_{(\chi,g)}\chi(w) + 1,$$

where χ_0 denotes the trivial additive character, i.e., the characteristic function of E. Thus, everything is proved. □

The trace part

If λ is an additive character of F, then λ *lifts* to an additive character $\hat{\lambda}$ of E by setting

$$\hat{\lambda}(w) := \lambda(\mathrm{Tr}(w)). \tag{3.8}$$

Moreover, $\hat{\lambda} \in C_{F,x-1}$ and, in fact, $C_{F,x-1}$ is the submodule of $\hat{E}$ corresponding to the lifted additive characters of F. Furthermore, $C_{F,x-1}^{\perp}$ is equal to $U_{F,t}$ (where t is as in (2.1)) which is the kernel of Tr. For $a \in F$ let

$$T_a(w) := \frac{1}{q}\sum_{\lambda\in\hat{F}}\lambda(\mathrm{Tr}(w) - a) = \frac{1}{q}\sum_{\lambda\in\hat{F}}\hat{\lambda}(w)\lambda(a)^{-1}. \tag{3.9}$$

The following is easy to show.

Proposition 3.3 *T_a is the characteristic function of the set of w in E having F-trace equal to a.* □

Combining the mappings T_a and A_t, where t again is as in (2.1), we obtain the following criterion for normality over F, as a reformulation of Lemma 2.3.

Lemma 3.4 *Let $a \in F$ be nonzero and assume that $T_a(w)A_t(w) \neq 0$. Then w is normal over F.*

Proof. If p divides n then $v(x^n - 1)$ divides t and therefore $A_t(w) \neq 0$ implies that $x^n - 1$ divides $\mathrm{Ord}_F(w)$ whence w is normal over F. If p and n are prime then $A_t(w) \neq 0$ is equivalent to the fact that t divides $\mathrm{Ord}_F(w)$. Since $T_a(w) \neq 0$, w has nonzero F-trace. Thus, $\mathrm{Ord}_F(w) \neq t$ and w is normal over F. □

Of course, pointwise multiplication of the functions M_{q^n-1} and A_{x^n-1} gives the characteristic function of the set of primitive and F-normal elements. We remark that an important tool in [10] is that

$$\sum_{w\in E} M_{q^n-1}(w)A_{x^n-1}(w) \neq 0$$

(equivalent to the existence of a primitive and F-normal element) is implied already by

$$\sum_{w\in E} M_P(w)A_{x^n-1}(w) \neq 0,$$

where

$$P := \frac{q^n-1}{(q-1)\gcd(q-1,n)}.$$

In our problem, wherein the trace is fixed, this device unfortunately cannot be used. We therefore must work with the following description of the number of primitive and F-normal elements with prescribed trace.

Theorem 3.5 *Let a be a nonzero element of $F = \mathrm{GF}(q)$. Consider the n-dimensional extension $E = \mathrm{GF}(q^n)$ over F and let t be as in (2.1). Then the characteristic function of the set of primitive F-normal elements with prescribed F-trace a in E is equal to $M_{q^n-1} \cdot A_t \cdot T_a$. Moreover, the total number $PN_a(q,n)$ of primitive F-normal elements in E with prescribed F-trace a is equal to*

$$PN_a(q,n) = \sum_{w\in E} M_{q^n-1}(w) \cdot A_t(w) \cdot T_a(w). \qquad \square \qquad (3.10)$$

4 The Method of Lenstra and Schoof

Let $\mathscr{S}$ be as at the beginning of Section 2. In the present section we use the characteristic functions and character sum estimates to derive a sufficient existence criterion for a pair (q,n) to belong to $\mathscr{S}$. It turns out to be efficient for the case in which $n \geq 6$ (and indivisible by the characteristic p of F).

We introduce some further number-theoretical notations. For an integer $N \geq 1$ let $\omega(N)$ be the number of distinct prime divisors of N and $\theta(N) := \varphi(N)/N$. Analogously, for a monic polynomial $f \in F[x]$ let $\Omega_q(f)$ be the number of distinct irreducible monic F-divisors of f and $\theta_q(f) := \phi_q(f)/q^{\deg(f)}$.

Proposition 4.1 *Assume that n and q are relatively prime. If (q,n) is not in $\mathscr{S}$, then, necessarily, with t being as in (2.1),*

$$q^{\frac{n}{2}-1} < 2^{\omega(q^n-1)+\Omega_q(t)}. \qquad (*)$$

Proof. By the results of the previous section, we have

$$\frac{PN_a(q,n)}{\theta(q^n-1)\theta_q(t)} = \frac{1}{q}\sum_{d|q^n-1}\sum_{g|t}\frac{\mu(d)}{\varphi(d)}\frac{\mu_q(g)}{\phi_q(g)}\sum_{(\eta,d)}\sum_{(\chi,g)}\sum_{\lambda\in C_{F,x-1}} G(\eta,\chi\lambda), \quad (4.1)$$

where (see [11, Section 5.2]) $G(\eta,\chi\lambda)$ denotes the *Gauss sum*

$$G(\eta,\chi\lambda) = \sum_{w\in E}\eta(w)(\chi\lambda)(w). \quad (4.2)$$

The additive characters χ occuring in (4.1) all have F-order dividing t. Since $C_{F,t} + C_{F,x-1}$ is a direct decomposition of $\hat{E}$, we see that $\chi\lambda$ is trivial if and only if both χ and λ are trivial. If $\eta = \eta_0$ is trivial (i.e., $d = 1$) and $\chi\lambda = \chi_0$ is trivial (i.e., $g = 1$ and $\lambda = \lambda_0$ is trivial) then (with the convention $\eta_0(0) = 1$) the corresponding term in (4.1) is equal to

$$\frac{G(\eta_0,\chi_0\lambda_0)}{q} = q^{n-1}. \quad (4.3)$$

If $\eta = \eta_0$ but $\chi\lambda$ is nontrivial, then $G(\eta_0,\chi\lambda) = 0$. The same holds when η is nontrivial, but $\chi\lambda$ is trivial. If η and $\chi\lambda$ both are nontrivial, then the absolute value of the corresponding Gauss sum is equal to $q^{n/2}$, i.e.,

$$|G(\eta,\chi\lambda)| = q^{\frac{n}{2}}. \quad (4.4)$$

(More details on Gauss sums can be found in [11, Section 5.2].) Subtracting the term q^{n-1} from both sides of (4.1) gives the left side

$$l(q,n) := \frac{PN_a(q,n)}{\theta(q^n-1)\theta_q(t)} - q^{n-1}. \quad (4.5)$$

By the triangle inequality, the above discussion yields an estimate of the following type

$$|l(q,n)| \le c(q,n)\cdot q^{\frac{n}{2}}.$$

This expression is made more precise in the following. By the definition of the Möbius functions, in (4.1), one has only to form the sums over divisors of the square-free parts of q^n-1 and t, respectively. Observing that there are precisely $\varphi(d)$ multiplicative characters of order precisely d (for each d) and precisely $\phi_q(g)$ additive characters of F-order precisely g (for each g), we deduce that $l(q,n)$ does not exceed

$$\frac{1}{q}\sum_{1\neq d|\nu(q^n-1)}\sum_{1\neq g|t}\sum_{\lambda\in C_{F,x-1}} q^{\frac{n}{2}} + \frac{1}{q}\sum_{1\neq d|\nu(q^n-1)}\sum_{1\neq\lambda\in C_{F,x-1}} q^{\frac{n}{2}}.$$

An easy calculation now shows that

$$|l(q,n)| \le (2^\omega - 1)\left(2^\Omega - \frac{1}{q}\right)q^{\frac{n}{2}}, \quad (4.6)$$

where, for simplicity, $\omega = \omega(q^n - 1)$ and $\Omega = \Omega_q(t)$. Consequently, if $PN_a(q, n) = 0$, then

$$q^{\frac{n}{2}-1} \leq (2^\omega - 1)\left(2^\Omega - \frac{1}{q}\right) < 2^{\omega+\Omega}. \tag{4.7}$$

From that, (*) readily follows and the proof is complete. □

From now on, let $\mathscr{F}^*$ be the set of pairs (q, n), relatively prime, for which (*) holds. We remark that (*) does not provide any information when $n = 2$, and a determination of all q such that $(q, 3) \in \mathscr{F}^*$ seems to be hopeless. We are, however, able to determine all $(q, n) \in \mathscr{F}^*$ with $n \geq 6$. To that end we proceed basically as Lenstra and Schoof did in [10]. The next two lemmas give upper bounds for $\omega(q^n - 1)$ and $\Omega_q(t)$, respectively. For proofs we refer to [10].

Lemma 4.2 *Let $N > 1$, $l > 1$ be integers and Λ be a set of primes all less or equal to l. Let $L := \prod_{r\in\Lambda} r$. Assume that every prime divisor $r < l$ of N is contained in Λ. Then*

$$\omega(N) \leq \frac{\log N - \log L}{\log l} + |\Lambda|. \qquad \square$$

Lemma 4.3 *Let n be relatively prime to q and let t be as in (2.1). Then the following hold, where for simplicity $\Omega := \Omega_q(t)$.*

(1) $\Omega \leq \frac{1}{2}(n + \gcd(n, q - 1)) - 1$. *In particular, $\Omega \leq n - 1$ (with equality if and only if $q - 1$ is divisible by n). Moreover, $\Omega \leq \frac{3}{4}n - 1$, if $q - 1$ is not divisible by n.*

(2) $\Omega \leq \frac{1}{3}n + 5$, *if* $q = 5$.

(3) $\Omega \leq \frac{1}{3}n + 1$, *if* $q = 4$ *and* $n \neq 15$.

(4) $\Omega \leq \frac{1}{3}n + \frac{1}{3}$, *if* $q = 3$ *and* $n \neq 4, 8, 16$. □

Note that, generally, the upper bounds for Ω in Lemma 4.3 are of the form $\alpha n + \beta$.

Lemma 4.4 *Let $(q, n) \in \mathscr{F}^*$. Then, for every choice for the values α, β, l, L, Λ, we have*

$$\left(\frac{\log q}{\log 4} - \frac{\log q}{\log l} - \alpha\right) \cdot n < \beta + |\Lambda| + \frac{\log q}{\log 2} - \frac{\log L}{\log l} \tag{4.8}$$

and

$$\left(\frac{n}{\log 4} - \frac{n}{\log l} - \frac{1}{\log 2}\right) \cdot \log q < \alpha n + \beta + |\Lambda| - \frac{\log L}{\log l}. \tag{4.9}$$

Proof. The result follows easily from (*) using the bounds of Lemma 4.2 and Lemma 4.3. □

We continue with an analysis of the bounds given in Lemma 4.4. Throughout, we assume that n and q are relatively prime and that $q \geq 3$. For a given degree n, a suitable choice of Λ and l yields that

$$b(\Lambda, l) := \frac{n}{\log 4} - \frac{n}{\log l} - \frac{1}{\log 2} \tag{4.10}$$

is greater than 0, whence q is bounded. For the remaining values of q, utilizing Maple (in version Maple V, Release 4), we test the condition (*). Similarly, if q is fixed, after choosing a bound for $\Omega_q(t)$, a suitable choice of Λ and l yields that

$$a(\Lambda, l) := \frac{\log q}{\log 4} - \frac{\log q}{\log l} - \alpha \tag{4.11}$$

is greater than 0, whence n is bounded. This analysis results in a concrete list of pairs (q, n) which are members of $\mathscr{F}^*$ and therefore might not lie in $\mathscr{S}$.

Part 1. Assume that $q - 1$ is divisible by n and that $n \geq 6$.
Then $\Omega_q(t) = n - 1$. Let $\alpha = 1$ and $\beta = -1$. Take $l = 54$ and Λ as the set of primes less than l. Then $|\Lambda| = 16$ and $b(\Lambda, l) > 0$. We obtain the following data.

n	$q \leq$	$(q, n) \in \mathscr{F}^*$ for q equal to
6	1151	7, 13, 19, 25, 31, 37, 43, 49, 61, 121
7	329	8
8	156	9
9	95	–
10	67	11
11	51	–
12	42	13
$13 \leq n \leq 19$	35	–
≥ 20	contradiction	–

Part 2. Assume that $q - 1$ is not divisible by n, $n \geq 6$ and $q \geq 11$.
Take $\alpha = \frac{3}{4}$, $\beta = -1$ and Λ, l as in Part 1. This gives the data

n	$11 \leq q \leq$	$(q, n) \in \mathscr{F}^*$ for q equal to
6	388	11, 29
7	128	–
8	66	–
9	42	–
10	31	–
11	24	–
12	20	–
13	17	–
14	15	–
15	14	–
$16 \leq n \leq 19$	13	–
≥ 20	contradiction	–

Part 3. Let $q = 9$ and assume $n \geq 3$.
First, $(9, 4), (9, 8) \in \mathscr{F}^*$. If n does not divide 8, take $\alpha = \frac{3}{4}, \beta = -1, l = 32$ and Λ the set of primes less than l. Then $|\Lambda| = 11$ and $a(\Lambda, l) > 0$. We obtain $n \leq 28$: testing (*) shows that only $(9, 5)$ survives.

Part 4. Let $q = 8$ and assume $n \geq 3$.
We have already seen that $(8, 7)$ satisfies (*). Assume therefore that $n \neq 7$. Take $\alpha = \frac{3}{4}$ and $\beta = -1$ and Λ and l as in Part 3. Then $n \leq 36$ but (*) is satisfied only for $(8, 3)$.

Part 5. Let $q = 7$ and assume $n \geq 3$.
Then $(7, 3), (7, 6) \in \mathscr{F}^*$. Assuming that $q - 1$ is not divisible by n, we take again $\alpha = \frac{3}{4}$ and $\beta = -1$, Λ the set of all primes less than 54 and let $l = 54$. Then $a(\Lambda, l) > 0$ and $n \leq 39$. Test of (*) shows that only $(7, 4), (7, 12) \in \mathscr{F}^*$.

Part 6. Let $q = 5$ and assume $n \geq 3$.
Then $(5, 4) \in \mathscr{F}^*$. Assuming that $q - 1$ is not divisible by n, with $\alpha = \frac{1}{3}$ and $\beta = 4$, Λ and l as in Part 5, gives $n \leq 26$. Test of (*) shows that only $(5, 3), (5, 6), (5, 8), (5, 12) \in \mathscr{F}^*$.

Part 7. Let $q = 4$ and assume that $n \geq 3$.
The pairs $(4, 3)$ and $(4, 15)$ are members of $\mathscr{F}^*$. Assuming that $n \neq 3$ and $n \neq 15$, we may take $\alpha = \frac{1}{3}$ and $\beta = 1$. Let Λ and l be as in Part 5. Then $n \leq 24$ and test of (*) shows that only $(4, 5), (4, 9) \in \mathscr{F}^*$.

Part 8. Let $q = 3$. Assume that $n \geq 4$.
Then $(3, 4), (3, 8) \in \mathscr{F}^*$ but $(3, 16)$ is not in $\mathscr{F}^*$. For all other values of n we may take $\alpha = \frac{1}{3}$ and $\beta = \frac{1}{3}$. With Λ and l as in Part 5 we obtain $n \leq 36$. Test of (*) shows that only $(3, 5) \in \mathscr{F}^*$.

For completeness, we remark that $(2, 3), (2, 5), (2, 7), (2, 9)$ and $(2, 15)$ are the only members of $\mathscr{F}^*$ with $q = 2$ and n odd (this is achieved by taking $\alpha = \frac{1}{4} = \beta$, Λ and l as in Part 5, which shows $n \leq 77$).

Summarizing the results of the present section, we have proved the following.

Theorem 4.5 *Let q and n be relatively prime. Assume that $n \geq 6$ if $q \geq 11$ and that $n \geq 3$ if $3 \leq q \leq 9$. If (q, n) does not belong to $\mathscr{S}$, then, necessarily, (q, n) is one of the following pairs:*

$$(4, 15), (13, 12), (7, 12), (5, 12), (11, 10),$$

$$(4, 9), (9, 8), (5, 8), (3, 8), (8, 7),$$

$$(121, 6), (61, 6), (49, 6), (43, 6), (37, 6), (31, 6),$$

$$(29, 6), (25, 6), (19, 6), (13, 6), (11, 6), (7, 6), (5, 6),$$

$$(9,5),(4,5),(3,5),(9,4),(7,4),(5,4),(3,4),$$
$$(8,3),(7,3),(5,3),(4,3).$$

□

5 Variations of a Counting Argument

In the present section we study primitive normal bases with prescribed trace for extensions of degree 3, 4 and 5. The main ingredient is a basic counting argument that turns out to be very efficient for these (low) degrees. Let $\mathscr{P}_a$ and $\mathscr{N}_a$ be as at the beginning of Section 3 and let P_a and N_a, respectively, denote the cardinalities of these sets. Moreover, let $PN_a(q,n)$ be as in Theorem 3.5.

Lemma 5.1 *Let $a \in F$ be nonzero. Then*

$$PN_a(q,n) \geq N_a + P_a - q^{n-1}. \tag{5.1}$$

Proof. We have

$$PN_a(q,n) = |\mathscr{N}_a \cap \mathscr{P}_a| = N_a + P_a - |\mathscr{N}_a \cup \mathscr{P}_a|.$$

Since $\mathscr{N}_a \cup \mathscr{P}_a$ is a subset of the set $\mathscr{T}_a$ of elements of E with F-trace equal to a and $|\mathscr{T}_a| = q^{n-1}$, the result follows. □

The next result shows that $PN_a(q,n)$ is nonzero provided that $\mathscr{P}_a$ is sufficiently large.

Lemma 5.2 *Let $n \geq 2$. If*

$$P_a \geq (n-1)q^{n-2}, \tag{5.2}$$

then $PN_a(q,n) > 0$.

Proof. Since $\phi_q(x^n - 1) \geq (q-1)^n$ (e.g., a consequence of [7, Theorem 10.5]), then

$$N_a = \frac{\phi_q(x^n-1)}{(q-1)} \geq (q-1)^{n-1}.$$

Now, if P_a satisfies the assumption (5.2), then

$$PN_a \geq (q-1)^{n-1} + (n-1)q^{n-2} - q^{n-1}.$$

Using induction on n, we see easily that the latter number is greater than zero for all $q \geq 2$ whenever $n \geq 3$. For $n = 2$, (5.2) implies $P_a \geq 1$. Indeed, since

conjugates have the same trace and the same orders, it follows that $P_a \geq 2$. Thus, again, $PN_a(q,n) > 0$ and everything is proved. □

To verify the bound (5.2) for P_a, we again consider (estimates of) character sums. From Section 3 we know that

$$P_a = \sum_{w \in E} M_{q^n-1}(w) T_a(w). \tag{5.3}$$

This expression was analysed in [3] and [9]: the outcome is that $P_a = 0$ implies

$$q^{n-1} \leq (2^\omega - 2^{\hat{\omega}}) q^{\frac{n-1}{2}} + (2^{\hat{\omega}} - 1) q^{\frac{n-2}{2}}, \tag{5.4}$$

where, throughout, $\omega = \omega(q^n - 1)$ and $\hat{\omega} = \omega\left(\frac{q^n-1}{q-1}\right)$. The noteworthy feature of (5.4) is the occurence of the exponent $\frac{n-1}{2}$ in the main term in the right side instead of $\frac{n}{2}$ as, for instance, in the right side of (4.6). Indeed, using estimates for the relevant terms in $l(q,n)$ (defined in (4.5)) leads to a marginal improvement of (4.6). More importantly, one can deduce a lower bound for P_a itself. Granted the above, the details are obvious and are left to the reader.

Lemma 5.3 *We have*

$$P_a \geq \theta(q^n - 1) \cdot \left(q^{n-1} - (2^\omega - 2^{\hat{\omega}}) q^{\frac{n-1}{2}} - (2^{\hat{\omega}} - 1) q^{\frac{n-2}{2}} \right). \qquad \square \tag{5.5}$$

We now combine the Lemmas 5.1–5.3 to obtain a further sufficient criterion for (q,n) to be in $\mathscr{S}$.

Proposition 5.4 *Assume that (q,n) is not contained in $\mathscr{S}$. Then, necessarily,*

$$q \leq (2^\omega - 2^{\hat{\omega}}) q^{\frac{3-n}{2}} + (2^{\hat{\omega}} - 1) q^{\frac{2-n}{2}} + \frac{n-1}{\theta(q^n - 1)}. \qquad (**)$$

Proof. If $PN_a(q,n) = 0$ then, by Lemma 5.2, $P_a < (n-1)q^{n-2}$ and therefore, by Lemma 5.3,

$$q^{n-1} - (2^\omega - 2^{\hat{\omega}}) q^{\frac{n-1}{2}} - (2^{\hat{\omega}} - 1) q^{\frac{n-2}{2}} < \frac{(n-1)q^{n-2}}{\theta(q^n - 1)}.$$

An easy calculation shows that (**) is satisfied in that situation. □

Let $\mathscr{F}^{**}$ be the set of all pairs (q,n) for which (**) is satisfied. We shall determine all pairs (q,n) of $\mathscr{F}^{**}$ with $n = 3, 4$, or 5 and where n and q are relatively prime. We require a further auxiliary result, first. For an integer $k \geq 1$ let p_k denote the kth prime.

Lemma 5.5 *Let $(q, n) \in \mathcal{F}^{**}$. Assume that, for some integer $k \geq 1$, $p_k \geq 2^n$ and*

$$2^k q^{\frac{3-n}{2}} + (n-1)\prod_{i=1}^{k}\left(\frac{p_i}{p_i - 1}\right) \leq \left(\prod_{i=1}^{k} p_i\right)^{\frac{1}{n}}. \tag{5.6}$$

Then $\omega < k$.

Proof. If $(q, n) \in \mathcal{F}^{**}$, then, in particular,

$$q < 2^{\omega} q^{\frac{3-n}{2}} + \frac{n-1}{\theta(q^n - 1)}. \tag{5.7}$$

Since generally

$$\frac{1}{\theta(q^n - 1)} = \frac{q^n - 1}{\varphi(q^n - 1)} \leq \prod_{i=1}^{\omega}\left(\frac{p_i}{p_i - 1}\right), \tag{5.8}$$

(5.7) implies that

$$q < 2^{\omega} q^{\frac{3-n}{2}} + (n-1)\prod_{i=1}^{\omega}\left(\frac{p_i}{p_i - 1}\right). \tag{5.9}$$

Assume now that (5.6) holds for some $k_0 \geq 1$. If $p_{k_0} \geq 2^n$, then, by induction, (5.6) holds for all $k \geq k_0$. Now, if $\omega \geq k_0$, then

$$q > (q^n - 1)^{\frac{1}{n}} \geq \left(\prod_{i=1}^{k_0} p_i\right)^{\frac{1}{n}},$$

and combining (5.6) and (5.9) produces a contradiction. Thus, the proof is complete. □

We are now ready to analyse the cases $n = 3$, 4 and 5, respectively. Throughout, we assume that $(q, n) \in \mathcal{F}^{**}$.

Part 1. Assume that $n = 3$.
Inequality (5.7) becomes

$$q < 2^{\omega} + \frac{2}{\theta(q^3 - 1)}. \tag{5.10}$$

The assumptions of Lemma 5.5 are satisfied for $k = 9$ whence $\omega \leq 8$. Since generally

$$\frac{1}{\theta(q^n - 1)} \leq 2^{\omega},$$

(5.10) implies $q < 2^8 + 2^9 = 768$. Checking (**) for all these values of q, we get the following list of members of $\mathcal{F}^{**}$:

$$(2, 3), (4, 3), (5, 3), (7, 3), (11, 3).$$

Part 2. Assume that $n = 4$.
Inequality (5.7) becomes

$$q < \frac{2^\omega}{\sqrt{q}} + \frac{3}{\theta(q^4-1)}. \tag{5.11}$$

Since $1/\sqrt{q} < (q^4-1)^{-\frac{1}{8}} \le 2^{-\frac{\omega}{8}}$, (5.11) implies that

$$q < 2^{\frac{7\omega}{8}} + \frac{3}{\theta(q^4-1)}.$$

If $k = 12$ then $p_k \ge 16$ and

$$2^{\frac{7k}{8}} + 3 \cdot \prod_{i=1}^{k} \left(\frac{p_i}{p_i - 1}\right) \le \left(\prod_{i=1}^{k} p_i\right)^{\frac{1}{4}},$$

whence the condition of Lemma 5.5 is satisfied for $k \ge 12$. This implies $\omega \le 11$. Finally, (5.11) and (5.8) give a concrete upper bound 822 for q. A test of all q in that range shows that the pairs $(q, 4)$ in $\mathscr{F}^{**}$ with q odd are exactly

$$(3,4), (5,4), (7,4), (11,4), (13,4).$$

Part 3. Assume that $n = 5$.
Inequality (5.7) implies

$$q < \frac{2^\omega}{q} + \frac{4}{\theta(q^5-1)}. \tag{5.12}$$

Since $1/q < (q^5-1)^{-\frac{1}{5}} \le 2^{-\frac{\omega}{5}}$, (5.12) implies

$$q < 2^{\frac{4\omega}{5}} + \frac{4}{\theta(q^5-1)}.$$

If $k = 16$ then $p_k \ge 32$ and

$$2^{\frac{4k}{5}} + 4 \cdot \prod_{i=1}^{k} \left(\frac{p_i}{p_i - 1}\right) \le \left(\prod_{i=1}^{k} p_i\right)^{\frac{1}{4}}, \tag{5.13}$$

whence Lemma 5.5 is in particular satisfied for $k \ge 16$. Thus, $\omega \le 15$. Finally, (5.8) and (5.12) imply an upper bound 4129 for q. A test of all q in that range shows that the pairs $(q, 5)$ in $\mathscr{F}^{**}$ with q not divisible by 5 are exactly

$$(2,5), (3,5), (4,5), (7,5), (9,5).$$

Altogether, we have proved the following.

Theorem 5.6 *Let q and n be relatively prime. Assume that $n = 3, 4$ or 5 and that $q \geq 3$. If (q, n) does not belong to $\mathscr{S}$, then, necessarily, (q, n) is one of the following pairs:*

$$(9, 5), (7, 5), (4, 5), (3, 5),$$
$$(13, 4), (11, 4), (7, 4), (5, 4), (3, 4),$$
$$(11, 3), (7, 3), (5, 3), (4, 3).$$

□

6 Summary and Conclusion

So far, we have proved that the assertion of the Main Theorem is valid except for at most 38 pairs (q, n), namely, those listed in Theorem 4.5 and 5.6. In the present section, we shall rule out all these pairs and complete the proof of the Main Theorem.

By the first three parts of Theorem 2.7, we may assume that $q \geq 3$, $n \geq 3$ and that q and n are relatively prime.

Part 1. We consider the lists in Theorem 4.5 and 5.6.
Application of Proposition 2.6 excludes all 10 entries with $n \geq 7$ as well as the pairs

$$(49, 6), (37, 6), (25, 6), (19, 6), (13, 6), (7, 6), (5, 6), (5, 4), (3, 4), (4, 3).$$

Further, application of Proposition 2.4 excludes the pairs (7, 5), (3, 5), (11, 3), (8, 3) and (5, 3).

For the remaining entries of the list of Theorem 4.5 we have tested whether condition (**) of Section 5 is satisfied. This excludes the pairs

$$(121, 6), (61, 6), (43, 6), (31, 6), (29, 6), (11, 6), (9, 4).$$

The remaining entries of the lists of Theorem 4.5 and 5.6 satisfying (*), (**) and all conditions of Theorem 2.7 are

$$(9, 5), (4, 5), (13, 4), (11, 4), (7, 4), (7, 3).$$

Part 2. We reconsider the counting argument of Section 5.

By Lemma 5.1 we have $PN_a(q, n) > 0$, if $P_a > q^{n-1} - N_a$. In the discussion of Section 5, we always used the worst lower bound $(q-1)^{n-1}$ for N_a (see the proof of Lemma 5.2). In fact, with t as in (2.1), $N_a = \phi_q(t)$ and so equality holds in this bound if and only if n divides $q - 1$. This is not so for the pairs

$$(9, 5), (4, 5), (11, 4), (7, 4).$$

Indeed, for each of these four pairs, the right hand side of (5.5) is greater than $q^{n-1} - N_a$. This shows that the assertion of the Main Theorem holds also for these cases.

Part 3. The remaining pairs (13, 4) and (7, 3).
We shall finally complete the proof of the Main Theorem by verifying the existence of primitive normal elements with prescribed trace by direct calculation in these fields.

For given (q, n), let $F = \mathrm{GF}(q)$ and $P_{q,n} \in F[x]$ be the monic polynomial whose roots are exactly the elements in $E = \mathrm{GF}(q^n)$ which are normal over F. (Based on the factorization of $x^n - 1$ over F it is demonstrated in [6] how $P_{q,n}$ can be determined by calculating in $F[x]$.) Furthermore, let $Q_{q,n}$ denote the $(q^n - 1)$th cyclotomic polynomial over F. Then the roots of $Q_{q,n}$ are precisely the primitive elements of E. Let $R_{q,n}$ be the greatest common divisor of $P_{q,n}$ and $Q_{q,n}$. Then the roots of $R_{q,n}$ are precisely the primitive and F-normal elements of E.

Using Maple (in version Maple V, Release 4), we have determined $R_{q,n}$ and its complete factorization over the field $\mathrm{GF}(q)$ for the pairs (7, 3) and (13, 4). An inspection of the irreducible factors shows that indeed every nonzero element of the ground field occurs as a second highest coefficient. This completes the proof of the Main Theorem.

For convenience, we provide the reader with some data from the latter calculation. A polynomial $f = f_n x^n + f_{n-1}x^{n-1} + \cdots + f_1 x + f_0$ is written as $(f_n, f_{n-1}, \ldots, f_1, f_0)$.

$R_{7,3}$ has degree 72 and possesses the irreducible factors

$$(1, 1, 1, 2), (1, 2, 4, 2), (1, 3, 2, 2), (1, 4, 4, 4), (1, 5, 5, 2), (1, 6, 6, 4).$$

$R_{13,4}$ has degree 4342 and possesses the irreducible factors

$$(1, 1, 6, 10, 7), (1, 2, 8, 12, 11), (1, 3, 12, 2, 7), (1, 4, 7, 2, 6),$$

$$(1, 5, 12, 4, 11), (1, 6, 10, 4, 7), (1, 7, 12, 0, 11), (1, 8, 6, 5, 2),$$

$$(1, 9, 11, 5, 7), (1, 10, 4, 7, 6), (1, 11, 12, 7, 6), (1, 12, 12, 10, 7).$$

Acknowledgments. During the time of this research the second author was a visitor of the first author at the University of Glasgow. He thanks the Deutsche Forschungsgemeinschaft for supporting this visit through a Forschungsstipendium and the Department of Mathematics of the University of Glasgow for its kind hospitality.

References

1. Carlitz, L.: Primitive roots in a finite field. Trans. Am. Math. Soc. **73**, 373–382 (1952)
2. Cohen, S. D.: Primitive roots in the quadratic extension of a finite field. J. London Math. Soc. **27**, 221–228 (1983)
3. Cohen, S. D.: Primitive elements and polynomials with arbitrary trace. Discrete Math. **83**, 1–7 (1990)
4. Cohen, S. D.: Primitive elements and polynomials: existence results. In: Mullen, G. L. and Shiue, P. J. -S. (eds.): Proceedings of the First International Conference on Finite Fields and Applications. Lecture Notes in Pure and Applied Mathematics **141**. pp 43–55. Dekker 1993

5. Davenport, H.: Bases for finite fields. J. London Math. Soc. **43**, 21–49 (1968)
6. Hachenberger, D.: On primitive and free roots in a finite field. AAECC **3**, 139–150 (1992)
7. Hachenberger, D.: Finite Fields: Normal Bases and Completely Free Elements. Boston: Kluwer Academic Publishers 1997
8. Hensel, K.: Über die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor. J. Reine Angew. Math. **103**, 230–237 (1888)
9. Jungnickel, D., Vanstone, S. A.: On primitive polynomials over finite fields. J. Algebra **124**, 337–353 (1989)
10. Lenstra, H. W., Jr., Schoof, R. J.: Primitive normal bases for finite fields. Math. Comp. **48**, 217–231 (1987)
11. Lidl, R., Niederreiter, H.: Finite Fields. Reading, Mass: Addison-Wesley 1983
12. MacWilliams, F. J., Sloane, N. J. A.: The Theory of Error Correcting Codes. Amsterdam: North-Holland 1977
13. Moreno, O.: On primitive elements of trace equal to 1 in $GF(2^m)^*$. Discrete Math. **41**, 53–56 (1982)
14. Morgan, I. H., Mullen, G. L.: Primitive normal polynomials over finite fields. Math. Comp. **63**, 759–765 (1994)
15. Mullen, G. L., Shparlinski, I.: Open problems and conjectures in finite fields. In: Cohen, S. D., Niederreiter, H. (eds.): Proceedings of the Third International Conference on Finite Fields and Applications. Lecture Notes **233** pp. 243–268. Cambridge University Press 1996