Primitivity, freeness, norm and trace

Stephen D. Cohen[a], Dirk Hachenberger[b,*]

[a] *Department of Mathematics, University of Glasgow, Glasgow G12 8QW, Scotland, UK*
[b] *Institut für Mathematik der Universität Augsburg, 86159 Augsburg, Germany*

Received 18 November 1998; revised 7 April 1999; accepted 12 April 1999

Abstract

Given the extension E/F of Galois fields, where $F = \mathrm{GF}(q)$ and $E = \mathrm{GF}(q^n)$, we prove that, for any primitive $b \in F^*$, there exists a primitive element in E which is free over F and whose (E,F)-norm is equal to b. Furthermore, if $(q,n) \neq (3,2)$, we prove that, for any nonzero $b \in F$, there exists an element in E which is free over F and whose (E,F)-norm is equal to b. A preliminary investigation of the question of determining whether, in searching for a primitive element in E that is free over F, both the (E,F)-norm and the (E,F)-trace can be prescribed is also made: this is so whenever $n \geqslant 9$.

MSC: 11T30; 12E20; 11T24

Keywords: Finite field; Primitive element; Free element; Normal basis; Trace; Norm

1. The problems PFN, FN and PFNT

To any pair (q,n), where $q>1$ is a prime power and $n \geqslant 1$ is an integer, there corresponds the extension E/F of the Galois fields $F = \mathrm{GF}(q)$ and $E = \mathrm{GF}(q^n)$. It is well known that the multiplicative group E^* of E is cyclic; each generator is called a *primitive element of* E. It is also a classical result that there exists an F-basis of E of the form $\{w, w^q, \ldots, w^{q^{n-1}}\}$ (for some $w \in E$). Such a basis is called a *normal basis of E over F*; w is called *free in E over F*. [1] In completion of previous work of Carlitz [1] and Davenport [5] it was proved only in 1987, by Lenstra and Schoof [10] that there always exists a primitive element w in E which is also free over F, i.e., a *primitive normal basis for E over F* always exists. Equivalently, for every pair (q,n), there exists a monic polynomial $\mu = x^n + \mu_{n-1}x^{n-1} + \cdots + \mu_1 x + \mu_0$ of degree n

* Corresponding author.
E-mail address: hachenberger@math.uni-augsburg.de (D. Hachenberger)

[1] In [4] and several other papers w is called *normal over F*, but we here prefer the term *free*.

in $GF(q)[x]$ which is irreducible over $GF(q)$ and whose roots are primitive in $GF(q^n)$ and linearly independent over $GF(q)$. μ is therefore called *a primitive free polynomial for* $GF(q^n)$ *over* $GF(q)$.

In [4] the authors proved a conjecture of Morgan and Mullen [12] which states that, for every pair (q,n) and for every nonzero $a \in F = GF(q)$, there exists a primitive element w in $E = GF(q^n)$ which is free over F and whose (E,F)-trace $\mathrm{Tr}_{E,F}(w) := \sum_{i=0}^{n-1} w^{q^i}$ is equal to a. As $\mu_{n-1} = -\mathrm{Tr}_{E,F}(w)$ if w is a root of μ, this is equivalent to the fact that the coefficient μ_{n-1} of a primitive-free polynomial for E over F can be prescribed as long as it is nonzero (of course, the trace of a free element is always nonzero). (This solved what might be described as the PFT-problem.) It is natural to ask whether certain other coefficients of a primitive-free polynomial can also be prescribed. An obvious choice is μ_0, since $\mu_0 = (-1)^n N_{E,F}(w)$ where $N_{E,F}(w) = \prod_{i=0}^{n-1} w^{q^i}$ denotes the (E,F)-norm of w. As the (E,F)-norm of a primitive element of E is always primitive in F, we are therefore led to the following problem.

Problem PFN. *Given a finite extension E/F of Galois fields and a primitive element b in F, does there exist a primitive element w in E which is free over F and whose (E,F)-norm is equal to b?*

If the answer is 'yes' for each primitive b, then the pair (q,n) corresponding to E/F is called a PFN-*pair.*

One of the main results of the present paper is the solution of the PFN-problem.

Theorem 1.1. *Let $q > 1$ be a prime power and $n \geqslant 1$ be an integer. Then (q,n) is a* PFN-*pair.*

The proof of Theorem 1.1 comprises two parts. In Section 2 (see Theorem 2.1), we first characterize those pairs (q,n) for which the existence of a primitive free element is already sufficient for the pair to be a PFN-pair, i.e., when the PFN-problem can be reduced to the *Primitive Normal Basis Theorem* of Lenstra and Schoof [10] (for simplicity, we denote the latter as Problem PF). The reduction applies to all cases where n is *small*, e.g., for all pairs (q,n) where $n \leqslant 15$ and $n \neq 9$. This is an important step, since possible exceptions are expected for extensions of small degrees rather than large degrees. In Section 3, we complete the proof of Theorem 1.1 by solving Problem PFN for all pairs (q,n), where $n = 9$ or $n \geqslant 16$. We shall achieve the latter through consideration of the following stronger problem.

Problem PFNT. *Given a finite extension E/F of Galois fields, a primitive element b in F and a nonzero element a in F, does there exist a primitive element w in E which is free over F, whose (E,F)-norm is equal to b and whose (E,F)-trace is equal to a?*

If the answer is 'yes' for each pair (a,b), then the pair (q,n) corresponding to E/F is called a PFNT-*pair.*

In Section 4, we will characterize those instances (q,n) for which Problem PFNT can be reduced to Problem PFN. Together with the results obtained in Section 3, this yields the second main result of the present paper.

Theorem 1.2. *Let $q>1$ be a prime power and $n\geqslant 7$ be an integer. Assume that (q,n) does not belong to the following list of pairs*:

$$(89,8),(41,8),(25,8),(17,8),(13,8),(7,8),(64,7),(4,7).$$

Then (q,n) is a PFNT-*pair.*

In a further paper [3], sieve-methods are employed in order to handle Problem PFNT for the possible exceptions occurring in Theorem 1.2 as well as for the cases $n=6$ and 5. In particular, it is proved that $(64,7)$ and $(4,7)$ are PFNT-pairs, whence, by Theorem 1.2, (q,r) is a PFNT-pair for each prime power $q>1$ and each prime $r\geqslant 7$. The latter result is important for [7], where, in order to demonstrate the existence of trace- and norm-compatible sequences of primitive (completely) free elements for prime power extensions, a generalization of the PFNT-problem, is considered.

Finally, in Section 5, we study Problem FN, which is not merely a relaxation of Problem PFN, since b is assumed to be any nonzero element of F, not necessarily primitive.

Problem FN. *Given a finite extension E/F of Galois fields and a nonzero element b in F, does there exist a free element w in E whose (E,F)-norm is equal to b?*

If the answer is 'yes' for all b, then the pair (q,n) corresponding to E/F is called an FN-*pair.*

The third main result is the following.

Theorem 1.3. *Let $q>1$ be a prime power and $n\geqslant 1$ be an integer. Assume that (q,n) is not equal to $(3,2)$. Then (q,n) is an* FN-*pair. With regard to the case $(q,n)=(3,2)$, if $w\in$ GF(9) is free over* GF(3), *then the* (GF(9), GF(3))-*norm of w is -1.*

We remark that the existence of primitive elements with arbitrary trace (which would be Problem PT in our notation) was completely solved in Cohen [2]: *if $n\geqslant 3$ and $(q,n)\neq(4,3)$, then, for every $a\in F$, there exists a primitive element $w\in E$ such that $\mathrm{Tr}_{E,F}(w)=a$. 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 $\mathrm{Tr}_{E,F}(w)=a$.* (Concerning primitive elements with nonzero trace, for $n\geqslant 3$ the latter result was independently proved by Jungnickel and Vanstone [9] (see also Section 7.5 in [8]).)

Finally, on the philosophy of tackling problems in this series, we comment that, although in every case, the number of relevant objects can be expressed in terms of character sums of various kinds (thereby yielding a solution for all but finitely many values of q and n), it is by exploiting non-counting theoretical arguments (such as links between the problems) that we can obtain complete solutions without excessive computation or direct verification.

2. Reducing Problem PFN to Problem PF

In the present section we consider those pairs (q,n) for which Problem PFN can be reduced to Problem PF.

Theorem 2.1. *Let $q>1$ be a prime power and $n \geqslant 1$ an integer. Let $q-1=2^{\alpha}A$ and $n=2^{\beta}B$ where AB is odd. Assume that $\alpha \geqslant \beta - 1$ if $\alpha \geqslant 2$ and that* $\gcd(A, B/\gcd(A,B))=1$. *Then (q,n) is a* PFN-*pair.*

Corollary 2.2. *Assume that $n=2^{e}n_0$, where n_0 is odd and square-free and where $e \leqslant 3$. Then (q,n) is a* PFN-*pair for all prime powers $q>1$.*

Example 2.3. Let $q>1$ be a prime power and

$$n \in \{1,2,3,\ldots,31\} \setminus \{9,16,18,25,27\}.$$

Then (q,n) is a PFN-pair.

For the proof of Theorem 2.1, we quote a result from [10]. Given the pair (q,n), let again $E=\mathrm{GF}(q^n)$ and $F=\mathrm{GF}(q)$. For a divisor d of q^n-1, let C_d be the unique subgroup of order d of E^*; furthermore, let Γ_d be the set of generators of C_d, i.e., the set of all $x \in E^*$ having multiplicative order $\mathrm{ord}(x)$ equal to d. There are exactly $\varphi(d)$ such elements, where φ denotes Euler's totient function. The following result, drawn from [10] (see (1.12)), characterizes the largest subgroup of E^* which leaves the set of free elements over F invariant under multiplication. Throughout, given (q,n), we let $\delta := (q-1)\cdot \gcd(q-1,n)$: observe that δ divides q^n-1.

Proposition 2.4. *For a given pair (q,n) let E, F, δ be as above. Assume that $\lambda \in C_\delta$ and that $y \in E$ is free over F. Then λy likewise is free in E over F.*

Proof of Theorem 2.1. Consider a prime divisor r of $q-1$, and denote by r^a and r^b, respectively, the largest power of r dividing $q-1$ and n, respectively. We assume first that either r is odd, or that $r=2$ and $q-1$ is divisible by 4. Then (see e.g., Lemmas 19.4 and 19.5 in [6]), $R := r^{a-b}$ is the largest power of r dividing q^n-1, i.e., C_R is the Sylow-r-subgroup of E^*. Assume further that $b \leqslant a$. Then R divides δ and thus, if $y \in E$ is any primitive element which is free over F, Proposition 2.4 implies that yC_R entirely consists of elements which are free in E over F. We write y in the form y_1y_2, where $y_1 \in \Gamma_R$ and where $\mathrm{ord}(y_2)=(q^n-1)/R$ is relatively prime to R. If $\zeta \in C_R$, then ζy is primitive in E if and only if $\zeta y_1 \in \Gamma_R$. Since $\Gamma_R = C_R \setminus C_{R/r}$ the latter holds if and only if ζ is not contained in the coset $y_1^{-1}C_{R/r}$ of $C_{R/r}$ in C_R. This allows exactly $R - R/r = \varphi(R)$ choices for ζ in C_R such that ζy remains primitive. We next consider properties of the (E,F)-norm (which for simplicity is denoted by N throughout). Let $\lambda := N(\zeta)$ and $x := N(y) = y^{(q^n-1)/(q-1)}$. Similar to the above, we write $x = x_1x_2$ with $x_1 \in \Gamma_{r^a}$ being equal to $N(y_1)$ and with $\mathrm{ord}(x_2) = (q-1)/r^a$ being indivisible by r.

Then λx is primitive in F^* if and only if λ does not belong to the coset of $x_2^{-1}C_{r^{a-1}}$ of $C_{r^{a-1}}$ in C_{r^a}, which gives $r^a - r^{a-1} = \varphi(r^a)$ suitable choices for λ. Since r^b is the largest power of r dividing $(q^n-1)/(q-1)$ (see Lemmas 19.4 and 19.5 in [6] and their proofs), the restriction of N to C_R gives an epimorphism onto C_{r^a} with kernel C_{r^b}, and the preimage of λ in C_R under N is thus equal to ζC_{r^b} which has cardinality r^b. Similarly, the restriction of N to $C_{R/r}$ gives an epimorphism onto $C_{r^{a-1}}$ with kernel C_{r^b}. We therefore conclude that

$$\{N(\zeta y_1)\colon \zeta \in C_R \backslash y_1^{-1}C_R\} = \{\lambda x_1\colon \lambda \in C_{r^a} \backslash x_1^{-1}C_{r^{a-1}}\} = \Gamma_{r^a},$$

which means that each element of Γ_{r^a} occurs as the C_{r^a}-part of the norm of some primitive element in E which is free over F.

Assume next that $b > a$. (By our assumptions, this case is needed only if $r = 2$.) Then r^{2a} is the largest power of r dividing δ, whence the Sylow-r-subgroup $C_{r^{2a}}$ of C_δ is a proper subgroup of C_R. As $N(C_{r^{2a}}) = C_{r^{2a-b}}$, the Primitive Normal Basis Theorem of Lenstra and Schoof even guarantees the existence of $r^{2a-b} \leqslant r^{a-1} \leqslant \varphi(r^a)$ elements occurring as the C_{r^a}-part of a primitive element of E which is free over F. Thus, if $b = a+1$ and $r = 2$, then $r^{2a-b} = \varphi(r^a)$ and therefore, as above,

$$N(y_1 C_{2^{2a}}) = x_1 C_{2^{a-1}} = \Gamma_{2^a}.$$

We finally consider the case where $r = 2$ and where $q \equiv 3 \pmod 4$ (i.e., $a = 1$). But here, the C_2-part of the norm of each primitive element in E is always equal to -1 (no matter how large b is). This completes the study of the Sylow subgroups of E^* belonging to prime divisors of $q-1$.

Observe now that F^* is equal to the direct product of its Sylow-r-subgroups $C_{r^{a(r)}}$ (where now for r dividing $q-1$, $r^{a(r)}$ denotes the largest power of r dividing $q-1$). Observe also that Γ_{q-1}, i.e., the set of primitive elements in F, is equal to the product of the sets $\Gamma_{r^{a(r)}}$. We are therefore able to combine the above results to deduce that each element of Γ_{q-1} occurs as the norm of some primitive element in E which is free over F provided the following conditions hold, where now $r^{b(r)}$ denotes the largest power of r dividing n:

(a) $b(r) \leqslant a(r)$, if r is an odd prime divisor of $q-1$, and
(b) $b(2) \leqslant a(2)+1$, if $q-1$ is divisible by 4.

Since this is a reformulation of the contents of Theorem 2.1, everything is proved. □

3. PFNT-pairs and the solution of Problem PFN

In the present section we shall complete the proof of Theorem 1.1. For this purpose, we consider the stronger Problem PFNT.

Throughout, for a given pair (q,n), let $P = P(q,n)$ be the largest divisor of $q^n - 1$ which is relatively prime to $q-1$, and let $\omega = \omega(P)$ be the number of distinct prime divisors of P. Furthermore, let $t = t(q,n)$ be the largest divisor of $x^n - 1$ which is relatively prime to $x-1$, and let $\Omega = \Omega(t)$ be the number of distinct monic divisors $d \neq 1$ of t which are irreducible over $F = \mathrm{GF}(q)$. The following result provides a sufficient criterion for (q,n) to be a PFNT-pair; it is a special case of Proposition 3.1 in [7] (which is proved by examining the characteristic functions of primitive and free elements with prescribed norm and trace which are given in terms of Gauss sums and other character sums). For the basic theory of such characters and sums over finite fields, we refer to [11, Chapter 5; 8, Chapter 7].

Proposition 3.1. *For a given pair (q,n) let P, ω, t, Ω be defined as above. Assume that*

$$\frac{q^{n/2}}{q(q-1)} > \left(2^{\Omega} - \frac{1}{q}\right)\left(2^{\omega} - \frac{1}{q-1}\right). \tag{3.1}$$

Then (q,n) is a PFNT-*pair.*

Using Proposition 3.1, we shall show that for $n \geqslant 7$ there are at most 18 pairs (q,n) which fail to be a PFNT-pair. (In Section 4, this list of possible exceptions is eventually reduced to the 8 members listed in Theorem 1.2.)

In order to apply Proposition 3.1, it is useful to have upper bounds for the parameters ω and Ω. First, an application of Lemma 2.6 in [10] gives the following: if $l > 1$ is an integer and Λ a set of primes $s < l$ such that each prime divisor $r < l$ of P is contained in Λ, then, with $L = L(\Lambda) := \prod_{s \in \Lambda} s$ and $|\Lambda|$ being the cardinality of Λ it holds that

$$\omega \leqslant \frac{\log P - \log L}{\log l} + |\Lambda|. \tag{3.2}$$

Since P is odd, we may always take Λ to be a set of odd primes. Secondly, we use upper bounds for Ω which are given in the form

$$\Omega \leqslant \alpha n + \beta, \tag{3.3}$$

where, depending on the situation, $\alpha > 0$ and β are suitable rational numbers (see e.g., Lemma 4.3 in [4]). Proposition 3.1 in combination with (3.2) and (3.3) yield the following equivalent sufficient criteria for (q,n) to be a PFNT-pair. We leave the simple calculations to the reader.

Lemma 3.2. *If for some choice of l, Λ, α and β either* (3.4) *or* (3.5) *is true, then (q,n) is a* PFNT-*pair.*

$$\left(\frac{n-4}{\log 4} - \frac{n-1}{\log l}\right)\log q \geqslant \alpha n + \beta + |\Lambda| - \frac{\log L}{\log l}, \tag{3.4}$$

$$\left(\frac{\log q}{\log 4} - \frac{\log q}{\log l} - \alpha\right) n \geqslant \frac{2\log q}{\log 2} - \frac{\log q}{\log l} + \beta + |\Lambda| - \frac{\log L}{\log l}. \tag{3.5}$$

We are now going to analyse these conditions for $n \geqslant 7$. The necessary calculations can be done with a computer algebra system (Maple for instance).

Case 1: Assume first that $n \geqslant 10$ and that $q \geqslant 11$. We choose $l = 72$ and, observing that P is always odd, let Λ be the set of all odd primes less than 72.

Case 1a: Assume further that q is congruent to 1 mod n. Then $\Omega = n-1$, whence, assuming that (q,n) is not a PFNT-pair, (3.4) implies $n \leqslant 22$. For each $n \in \{10, 11, \ldots, 22\}$ we use (3.5) to obtain a concrete upper bound for q, i.e., $q \leqslant 407$ if $n = 10$, or $q \leqslant 231$ if $n = 11$, etc. For each pair in this range we either use (3.4) (yet with Λ being the set of all primes r less than 72 which are prime to q and for which n is divisible by the multiplicative order of q modulo r) or Proposition 3.1. The assumption that (q,n) is not a PFNT-pair thus leaves the following pairs for which (3.1) fails:

$$(16,15), (13,12), (11,10). \tag{3.6}$$

Case 1b: We assume next that $q-1$ is not divisible by n. If the characteristic p of F does not divide n, we may take $\alpha = 3/4$ and $\beta = -1$ (see Lemma 4.3 in [4]) and obtain $n \leqslant 24$ by (3.4). An analysis analogous to Case 1 shows that all pairs under consideration are in fact PFNT-pairs. If p divides n, we may choose $\alpha = 1/2$ and $\beta = -1$ to satisfy (3.3) and to obtain $n \leqslant 13$ from (3.4). Again, all pairs under consideration turn out to be PFNT-pairs.

Case 2: We now consider all cases where $n \geqslant 10$ and where $q \in \{9, 8, 7, 5, 4\}$. For $q = 9, 8$ we again choose $l = 72$, while for $q = 7, 5, 4$ we choose $l = 200$. Furthermore, for $q = 9, 8, 7$ we may take $\alpha = 3/4$ and $\beta = -1$, while for $q = 5$, $\alpha = 1/3$ and $\beta = 5$ are suitable (see again Lemma 4.3 in [4]). If $q = 4$ and $n \neq 15$, let $\alpha = 1/3$ and $\beta = 1$. If $q = 9$ we may assume that $3 \notin \Lambda$. An application of (3.5) shows that the failing of (q,n) to be a PFNT-pair implies $n \leqslant 125$. As in the foregoing cases, we test all remaining pairs to determine whether condition (3.4) (using a modified choice of Λ) or (3.1) is satisfied. It turns out that all pairs under consideration are PFNT-pairs. For $q \in \{8, 7, 5, 4\}$ we proceed similarly: we may assume that $7 \notin \Lambda$ if $q = 8, 7$; $3 \notin \Lambda$ if $q = 7, 4$; and $5 \notin \Lambda$ if $q = 5$. The only pairs (q,n) which do not satisfy (3.1) are the following three pairs:

$$(4,15), (7,12), (5,12). \tag{3.7}$$

Case 3: We finally consider all cases where $n \in \{9, 8, 7\}$ and where $q \geqslant 4$. Again, for a given n, we use (3.4) to get an upper bound for q, where, depending on q modulo n, we have various bounds for Ω. We omit the routine details here, and simply report that the pairs (q,n) under consideration which do not satisfy (3.1) are precisely the following:

$$\begin{aligned} &(4,9), \\ &(89,8), (41,8), (25,8), (17,8), (13,8), (9,8), (7,8), (5,8), \\ &(64,7), (8,7), (4,7). \end{aligned} \tag{3.8}$$

We are now able to complete the proof of Theorem 1.1.

Since every PFNT-pair obviously is a PFN-pair, by Theorem 2.1 and the results of the present section, it suffices to show that $(2,n)$ and $(3,n)$ are PFN-pairs for each $n \geqslant 1$ and that $(4,9)$ is a PFN-pair.

Firstly, it is clear that $(2,n)$ is also a PFNT-pair for each $n \geqslant 1$: trivially, this follows already from [10] since trace and norm have to be equal to 1. Secondly, it follows from [4] that $(3,n)$ is also a PFNT-pair for all $n \geqslant 1$, since each primitive element has fixed norm equal to -1 in this case. It finally remains to show that $(4,9)$ is a PFN-pair. We will see in the next section that $(4,9)$ is also a PFNT-pair. Here, we shall prove directly that each pair $(4,n)$ is a PFN-pair: if w is primitive and free in GF(4^n) over GF(4), then w^2 is likewise primitive and free in GF(4^n) over GF(4), but w^2 has a different norm from w. Since there are only two primitive elements in GF(4), everything is proved. □

4. Reducing Problem PFNT to Problem PFN

By Theorem 1.1, the following 10 pairs (q,n) (which are among the 18 pairs in (3.6), (3.7) and (3.8)) are all PFN-pairs.

$$(16,15),(4,15),(13,12),(7,12),(5,12),(11,10),(4,9),(9,8),(5,8),(8,7).$$

Since they fail (3.1) in Section 3, we were not able to show there that these are PFNT-pairs. In the present section we will see that all these pairs are in fact PFNT-pairs: this is a consequence of Proposition 4.1, which, under the assumption that $q-1$ divides n, characterizes instances of Problem PFNT which can be reduced to Problem PFN. Together with the analysis of Problem PFNT in Section 3, this completes the proof of Theorem 1.2.

Proposition 4.1. *Let $q > 1$ be a prime power and let $n \geqslant 1$ be an integer. Assume that $q-1$ divides n. Then (q,n) is a* PFNT-*pair if and only if (q,n) is a* PFN-*pair.*

Proof. Let $F = \mathrm{GF}(q)$ and $E = \mathrm{GF}(q^n)$, let $b \in F^*$ be primitive and $a \in F$ be nonzero. Since (q,n) is a PFN-pair (by Theorem 1.1), there exists a primitive element y of E which is free over F and whose (E,F)-norm is equal to b. Let $x := \mathrm{Tr}_{E,F}(y)^{-1}ay$. Then x is free in E over F and $\mathrm{Tr}_{E,F}(x) = a$. Furthermore, [by Lemma 2.5 and Proposition 2.6 in 4], x is primitive (it is here used that the square-free part of $q-1$ divides n). Moreover, since $q-1$ divides n by assumption, we have that $q-1$ divides $(q^n-1)/(q-1)$ (see e.g., Lemmas 19.4 and 19.5 in [6]). Therefore,

$$N_{E,F}(x) = (\mathrm{Tr}_{E,F}(y)^{-1}a)^{(q^n-1)/(q-1)} \cdot b = b$$

and everything is proved. □

5. The solution of Problem FN

In this last section we consider Problem FN and prove Theorem 1.3. Given (q,n), let δ be as in Proposition 2.4, let P be as in Proposition 3.1 and let $D{:=}(q^n-1)/P$ (whence δ divides D). Proposition 5.1 can be seen as an analogue of Theorem 2.1.

Proposition 5.1. *Assume that for a given pair (q,n) it is the case that $\delta = D$. Then (q,n) is an* FN-*pair.*

Proof. We use the same notation as in the proof of Theorem 2.1. The restriction of N onto C_D gives an epimorphism onto F^* with kernel $C_{D/(q-1)}$. If y is free in E over F, then, under the assumption that $D=\delta$, by Proposition 2.4, yC_D consists entirely of elements which are free in E over F. As $N(C_D y) = F^* y$, the norm of a free element can be prescribed. □

Corollary 5.2. *If n is a square-free odd number, then (q,n) is an* FN-*pair for each q. Further, if (q,n) is an* FN-*pair, where n is odd and $q \equiv 1 \pmod 4$, then $(q,2n)$ and $(q,4n)$ are* FN-*pairs.*

Proposition 5.3 below provides a sufficient criterion for (q,n) to be an FN-pair. It can be seen as an analogue of Proposition 3.1 and is likewise proved by examining the characteristic functions of free elements with prescribed norm given in terms of Gauss sums character sums. We omit the proof and refer to Proposition 4.1 in [4] and Proposition 3.1 in [7] for similar reasoning.

Proposition 5.3. *For a given pair (q,n), let Γ be the number of distinct monic divisors $d \neq 1$ of $x^n - 1$ that are irreducible over $F = \mathrm{GF}(q)$. Assume that*

$$q^{n/2} > (2^\Gamma - 1)(q-2). \tag{5.1}$$

Then (q,n) is an FN-*pair.*

It is easy to see that each pair satisfying (3.1) likewise satisfies (5.1). Thus, for $n \geqslant 7$, in order to show that (q,n) is an FN-pair, it is sufficient to test (5.1) for the 18 pairs listed in (3.6), (3.7) and (3.8), which fail (3.1). Moreover, since 12 of these pairs fall within the scope of Proposition 5.1 and Corollary 5.2, for $n \geqslant 7$, it remains to check the following pairs:

$$(11,10),(7,12),(4,9),(13,8),(7,8),(5,8).$$

It is easy to see that (5.1) is satisfied in all six cases, whence Theorem 1.3 holds whenever $n \geqslant 7$.

In order to complete the proof of Theorem 1.3, using again Proposition 5.1 and Corollary 5.2, it remains to check the cases $n = 6,4,2$ for $q \not\equiv 1 \pmod 4$. Trivially, we may assume that $q \neq 2$. First let $n = 6$. Then $q^3 > 63(q-2)$ is satisfied for all $q \geqslant 7$, implying (5.1) for all $q \geqslant 7$. The pairs (4,6) and (3,6) likewise satisfy (5.1). Next let $n=4$. Then $q^2 > 15(q-2)$ is satisfied whenever $q \geqslant 13$, and (5.1) is likewise satisfied for the pairs $q = 11, 8, 7, 4, 3$. This establishes Theorem 1.3 for $n=6$ and $n=4$.

Finally let $n=2$. Since $q > q-2$, (5.1) is satisfied if q is even. Assume therefore that q is odd, indeed, by Corollary 5.2 that $q \equiv 3 \pmod 4$. Evidently, an element w of E that is free over F and has (E,F)-norm equal to $b \in F^*$, is the root of an irreducible quadratic x^2+ax+b $(a \in F^*)$ over F. If χ is the quadratic character of F, the number of such irreducible quadratics is

$$\frac{1}{2} \sum_{a \in F^*, a^2 \neq 4b} (1 - \chi(a^2-4b)) = \frac{q-1}{2} - \chi(b),$$

because $\sum_{a \in F} \chi(a^2-4b) = -1$ (see [11, Theorem 5.48]) and $\chi(4b) = -\chi(-4b)$, since $q \equiv 3 \pmod 4$. The result follows and the proof of Theorem 1.3 complete. □

References

[1] L. Carlitz, Primitive roots in a finite field, Trans. Amer. Math. Soc. 73 (1952) 373–382.
[2] S.D. Cohen, Primitive elements and polynomials with arbitrary trace, Discrete Math. 83 (1990) 1–7.
[3] S.D. Cohen, Gauss sums and a sieve for generators of Galois fields, submitted for publication.
[4] S.D. Cohen, D. Hachenberger, Primitive normal bases with prescribed trace, Appl. Algebra Eng. Comm. Comput. 9 (1999) 383–403.
[5] H. Davenport, Bases for finite fields, J. London Math. Soc. 43 (1968) 21–49.
[6] D. Hachenberger, Finite Fields: Normal Bases and Completely Free Elements, Kluwer Academic Publishers, Boston, 1997.
[7] D. Hachenberger, Universal generators for primary closures of Galois fields (1999), submitted for publication.
[8] D. Jungnickel, Finite Fields. Structure and Arithmetics, BI-Wissenschaftsverlag, Mannheim, 1993.
[9] D. Jungnickel, S.A. Vanstone, On primitive polynomials over finite fields, J. Algebra 124 (1989) 337–353.
[10] H.W. Lenstra Jr., R.J. Schoof, Primitive normal bases for finite fields, Math. Comput. 48 (1987) 217–231.
[11] R. Lidl, H. Niederreiter, Finite Fields, Addison-Wesley, Reading, MA, 1983; 2nd Edition, Cambridge University Press, Cambridge, 1997.
[12] I.H. Morgan, G.L. Mullen, Primitive normal polynomials over finite fields, Math. Comp. 63 (1994) 759–765.

Scope of the Journal

The aim of this journal is to bring together research papers in different areas of discrete mathematics. Contributions presented to the journal can be research papers, short notes, surveys, and possibly research problems. The 'Communications' section will be devoted to the fastest possible publication of the brief outlines of recent research results, the detailed presentation of which might be submitted for possible publication in DISC or elsewhere. The journal will also publish a limited number of book announcements, as well as proceedings of conferences. The journal will publish papers in combinatorial mathematics and related areas. In particular, graph and hypergraph theory, network theory, coding theory, block designs, lattice theory, the theory of partially ordered sets, combinatorial geometries, matroid theory, extremal set theory, logic and automata, matrices, polyhedra, discrete probability theory, etc. shall be among the fields covered by the journal.

Instructions to contributors

All contributions should be written in English or French, should have an abstract in English (as well as one in French if the paper is written in French), and—with the exception of Communications—should be sent in triplicate to Nelly Segal, Editorial Manager, RUTCOR, Rutgers, the State University of New Jersey, 640 Bartholomew Road, Piscataway, NJ 08854-8003, USA. The authors are requested to put their mailing address on the manuscript.

Upon acceptance of an article, the author(s) will be asked to transfer copyright of the article to the Publisher. This transfer will ensure the widest possible dissemination of information.

Manuscripts submitted for the Communications section, having at most 5 typewritten pages, should be sent to a member of the editorial board in triplicate. Detailed proofs do not have to be included, but results must be accompanied at least by rough outlines of their proofs. Subsequent publication in this journal or elsewhere of the full text of a research report, the outline of which has been published in the Communications section of our journal, is not excluded. Every effort shall be made for the fastest possible publication of Communications.

Please make sure that the paper is submitted in its final form. Corrections in the proofstage, other than of printer's errors, should be avoided; costs arising from such extra corrections will be charged to the authors.

The manuscript should be prepared for publication in accordance with instructions given in the 'Instructions to Authors' (available from the Publisher) details of which are condensed below:

- The manuscript must be typed on one side of the paper in double spacing with wide margins. A duplicate copy should be retained by the author.
- Special care should be given to the preparation of the drawings for figures and diagrams. Except for a reduction in size, they will appear in the final printing in exactly the same form as they were submitted by the author; normally they will not be redrawn by the printer. In order to make a photographic reproduction possible, all drawings should be on separate sheets, with wide margins, drawn large size, in Indian ink, and carefully lettered. Exceptions are diagrams only containing formulae and a small number of single straight lines (or arrows); these can be typeset by the printer.
- References should be listed alphabetically, in the same way as the following examples:
  For a book: W.K. Chen, Applied Graph Theory (North-Holland, Amsterdam, 1971).
  For a paper in a journal: P. Erdős, Some recent problems and results in graph theory, Discrete Math. 164 (1997) 81–85.
  For a paper in a contributed volume: M.O. Rabin, Weakly definable relations and special automata, in: Y. Bar-Hillel, ed., Mathematical Logic and Foundations of Set Theory (North-Holland, Amsterdam, 1970) 1–23.
  For an unpublished paper: R. Schrauwen, Series of singularities and their topology, Ph.D. Thesis, Utrecht University, Utrecht, 1991.
- LaTeX: If your manuscript has been prepared with (La)TeX, then your files may be of use to us for producing galley proofs and for printing. We only wish to receive the files once a paper has been accepted. Kindly send an MSDOS-formatted floppy disc with the final version. The contents of the files on the floppy should be exactly the same as the hard copy that we receive from you. If the file is suitable, proofs will be produced without rekeying the text. The article should be encoded in Elsevier-LaTeX, standard LaTeX, or AMS-LaTeX (in document style 'article'). *No changes from the accepted version are permissble, without the explicit approval by the Editor. The Publisher reserves the right to decide whether to use the author's file or not.* If the file is sent by e-mail, the name of the journal *Discrete Mathematics*, should be mentioned in the "subject field" of the message to identify the paper. Authors should include an ASCII table (available from the Publisher) in their files to enable the detection of transmission errors. The files should be mailed to: Michael D. Griffin, Elsevier Science B.V., P.O. Box 103, 1000 AC Amsterdam, Netherlands, Fax: (31-20) 4852616. E-mail: m.griffin@elsevier.nl.

The Elsevier LaTeX package (including detailed instructions for LaTeX preparation) can be obtained from the Comprehensive TeX Archive Network (CTAN). Search for Elsevier on the CTAN Search page (http://www.ucc.ie/cgi-bin/ctan), or the CTAN-Web page (http://tug2.cs.umb.edu/ctan/), or use direct access via FTP at ftp.dante.de (Germany), ftp.tex.ac.uk (UK), or tug2.cs.umb.edu (Massachusetts, USA) and go to the directory /tex-archive/macros/latex/contrib/supported/elsevier. The Elsevier package consists of the files: ascii.tab (ASCII table), elsart.cls (use this file if you are using LaTeX2e, the current version of LaTeX), elsart.sty and elsart12.sty (use these two files if you are using LaTeX2.09, the previous version of LaTeX), instraut.dvi and/or instraut.ps (instruction booklet), readme. CTAN is a mirrored network of ftp.tex.ac.uk, ftp.dante.de and tug2.cs.umb.edu, which are widely mirrored (see http://tug2.cs.umb.edu/ctan/ctansite.txt) and hold up-to-date copies of all the public-domain versions of TeX, LaTeX, Metafont and ancillary programs.

Author's benefits

1. 30% discount on all book publications of North-Holland.
2. 50 reprints are provided free of charge to the principal author of each paper published.

USA mailing notice: Discrete Mathematics (ISSN 0012-365X is published (total 16 issues) by Elsevier Science B.V. (P.O. Box 211, 1000 AE Amsterdam, The Netherlands). Annual subscription price in the USA US$3709.00 (valid in North, Central and South America), including air speed delivery. Periodical postage rate paid at Jamaica, NY 11431.

USA POSTMASTER: Send address changes to Discrete Mathematics. Publications Expediting Inc., 200 Meacham Ave, Elmont, NY 11003.

AIRFREIGHT AND MAILING in the USA by Publications Expediting Inc., 200 Meacham Avenue, Elmont, NY 11003.