TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 355, Number 8, Pages 3099–3116
S 0002-9947(03)03301-4
Article electronically published on April 25, 2003

PRIMITIVE FREE CUBICS WITH SPECIFIED NORM AND TRACE

SOPHIE HUCZYNSKA AND STEPHEN D. COHEN

ABSTRACT. The existence of a primitive free (normal) cubic $x^3 - ax^2 + cx - b$ over a finite field F with arbitrary specified values of a ($\neq 0$) and b (primitive) is guaranteed. This is the most delicate case of a general existence theorem whose proof is thereby completed.

1. INTRODUCTION

Given q, a power of a prime p, let F denote the finite field GF(q) of order q and, for a given positive integer n, let E denote its extension GF(q^n) of degree n. A *primitive element* of E is a generator of the cyclic group E^*. The extension E is also cyclic when viewed as an FG-module, G being the Galois group of E over F, and a generator is called a *free element* of E over F. The core result linking additive and multiplicative structure — the *primitive normal basis theorem* — is that there exists $\alpha \in E$, simultaneously primitive and free over F. Existence of such an element for every extension was demonstrated by Lenstra and Schoof [LeSc] (completing work by Carlitz ([Ca1], [Ca2]) and Davenport [Da]). A computer-free proof of the primitive normal basis theorem is given in [CoHu1].

It is natural to ask whether the result of the Primitive Normal Basis Theorem can be extended by imposing additional conditions on the primitive free element. In particular, we may wish to prescribe the norm or trace of a primitive free element, equivalent to specifying the constant term or the coefficient of x^{n-1} of the corresponding primitive free polynomial. In [CoHa1], it was shown that, given an arbitrary nonzero element $a \in F$, there exists a primitive element ω of E, free over F, such that ω has (E, F)-trace a in F, i.e., $\mathrm{Tr}_{E/F}(\omega) := \sum_{i=0}^{n-1} \omega^{q^i} = a$. Furthermore, in [CoHa2] it was shown that, given an arbitrary primitive element b of F, there exists a primitive element ω of E, free over F, with (E, F)-norm b in F, i.e., $N_{E/F}(\omega) := \prod_{i=0}^{n-1} \omega^{q^i} = \omega^{\frac{q^n-1}{q-1}} = b$.

In [CoHa2], Cohen and Hachenberger posed the following question, known as the PFNT problem. (A similar description of the above problems would be as PFT, PFN respectively, and later we refer to the analogous PNT problem.)

Problem 1.1. 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 $w \in E$, free over F, whose (E, F)-norm and trace equal b and a respectively? Equivalently, amongst all polynomials $\sum_{i=0}^{n} c_i x^i$ ($c_i \in F$) of degree n over F, does there exist

Received by the editors September 26, 2002 and, in revised form, January 30, 2003.
2000 *Mathematics Subject Classification.* Primary 11T06; Secondary 11A25, 11T24, 11T30.

one that is primitive and free, with $c_{n-1} = -a$ and $c_0 = (-1)^n b$? If so for each pair (a, b), then the pair (q, n) corresponding to E/F is called a PFNT pair.

Observe that the problem is meaningful only for $n \geq 3$. Clearly the strongest results (and correspondingly those most challenging to prove) occur for small n, since the corresponding polynomials have fewest "degrees of freedom". The PFNT problem was resolved for all $n \geq 5$ in [Co] (Theorem 1.1); it was observed that the $n = 4$ case was delicate while the $n = 3$ case might prove entirely intractable. The $n = 4$ case was solved in [CoHu2], using a modified version of the $n \geq 5$ approach.

In what follows, we solve the PFNT problem in the affirmative for $n = 3$. Expressing the result in terms of polynomials, we show that: for any prime power q, given $a, b \in F^*$ (b primitive), at least one of the q cubic polynomials $x^3 - ax^2 + cx - b$ ($c \in F$) is primitive and free. Perhaps surprisingly, there are no exceptions.

We have therefore completed the final stage in solving the general PFNT problem, i.e., we have established the existence of a primitive free element with prescribed norm and trace for every extension. The result is summarized in the following theorem.

Theorem 1.2. *Let q be a prime power and $n \geq 3$ an integer. Then (q, n) is a PFNT pair.*

The basic technique ([CoHa2]) of expressing the number of elements with the desired properties in terms of Gauss sums over E yields, if applied directly, estimates in terms of the numbers of prime factors of $q^n - 1$ and irreducible factors of $x^n - 1$. This establishes the result for large n but is inadequate when n is small. In [Co], use of a sieve on both the additive and multiplicative parts produces an expression in terms of the numbers of prime (respectively, irreducible) factors of divisors of $q^n - 1$ (respectively, $x^n - 1$), which are estimated as previously; this approach is more successful in dealing with small n but remains inappropriate for $n < 5$. In this paper, we exploit the idiosyncrasies of the situation when $n = 3$ (allowing us to reduce the PFNT problem to the simpler PNT problem in some cases) and, crucially, employ "external" results to estimate appropriate quantities (i.e., we no longer depend exclusively on the estimates derived from the initial Gauss sum formulation). The extreme delicacy of the $n = 3$ case means that the reductions and improvements which we apply to the basic technique are not merely conveniences, but are vital in establishing the result. Finally, a number of values of $q \leq 256$ (34 in all) had to be checked computationally.

2. Preliminaries

We begin by making some reductions to the problem and formulating the basic theory. The account will be as self-contained as possible, but to avoid excessive repetition, reference will be made to earlier work where appropriate.

By Proposition 4.1 of [CoHa2], (q, n) is a PFNT pair whenever $q - 1$ divides n (so we may assume that $q \neq 2, 4$, in the case when $n = 3$).

From now on, suppose that a,$b \in F$, with $a \neq 0$ and b a primitive element, are given.

Let $m = m(q, n)$ be the greatest divisor of $q^n - 1$ that is relatively prime to $q - 1$ (so in particular m divides $\frac{q^n-1}{(q-1)(n,q-1)}$). In [Co] it was demonstrated that, if $w \in E$ has (E, F)-norm b, then to guarantee that w is primitive it suffices to show that w is m-free in E (i.e., that $w = v^d$, where $v \in E$ and $d|m$, implies $d = 1$).

Analogously for the additive part, let $M = M(q,n)$ be the monic divisor of $x^n - 1$ (over F) of maximal degree that is prime to $x-1$. So $M = \frac{x^n-1}{x^{p^l}-1}$ where $n = n_0 p^l$, $p = \mathrm{char}F$ and $p \nmid n_0$. It was shown in [Co] that, if $w \in E$ has (nonzero) (E,F)-trace a, then to guarantee that w is free over F it suffices to show that w is M-free in E (i.e., that $w = h^\sigma(v)$, where $v \in E$ and h is an F-divisor of M, implies $h = 1$).

Define $N(t,T)$ to be the number of elements of E that

(i) are t-free ($t \in \mathbb{Z}$, $t|m$),
(ii) are T-free ($T(x) \in F[x]$, $T|x^n - 1$),
(iii) have norm b, and
(iv) have trace a.

Write $\pi(t,T)$ for $q(q-1)N(t,T)$. Assume throughout that $t \,|\, m$ and $T \,|x^n - 1\,$.

Next, we express the characteristic functions of the four subsets of E (or E^*) defined by the conditions (i)-(iv) in terms of characters on E or F.

I. *The set of $w \in E^*$ with $N_{E/F}(w) = b$.* The characteristic function of the subset of E^* comprising elements with norm b is

$$\frac{1}{q-1} \sum_{\nu \in \hat{F^*}} \nu(N(w)b^{-1}),$$

where $\hat{F^*}$ denotes the group of multiplicative characters of F^*, and the norm $N_{E/F}$ is abbreviated to N.

II. *The set of $w \in E^*$ with $Tr_{E/F}(w) = a$.* The characteristic function of the subset of E comprising elements with trace a is

$$\frac{1}{q} \sum_{c \in F} \lambda(c(T(w) - a)),$$

where λ is the canonical additive character of F and the trace $Tr_{E/F}$ is abbreviated to T.

III. *The set of $w \in E^*$ that are t-free.* The characteristic function for the subset of t-free elements ($t|m$) of E^* is

$$\theta(t) \int_{d|t} \eta_d(w), \quad w \in E^*,$$

where $\theta(t) = \frac{\phi(t)}{t}$, η_d denotes a character of order d ($d|m$) in $\hat{E^*}$ and, using the notation introduced in [Co], the integral notation is shorthand for a weighted sum:

$$\int_{d|t} \eta_d := \sum_{d|t} \frac{\mu(d)}{\phi(d)} \sum_{(d)} \eta_d.$$

IV. *The set of $w \in E$ that are T-free over F.* The characteristic function of the set of T-free elements of E takes the form

$$\Theta(T) \int_{D|T} \chi_{\delta_D}(w), \quad w \in E,$$

where $\Theta(T) = \frac{\Phi(T)}{T}$, χ is the canonical additive character on E and, as defined in [Co], $\{\chi_{\delta_D} : \delta_D \in \Delta_D\}$ (where $\chi_\delta(w) := \chi(\delta w)$, $w \in E$) is the set of all additive

characters of E of order D ($D|x^n-1$). Again, the integral notation represents a weighted sum:

$$\int_{D|g} \chi_{\delta_D} := \sum_{D|g} \frac{\mu(D)}{\Phi(D)} \sum_{(\delta_D)} \chi_{\delta_D}.$$

Using these characteristic functions, we derive an expression for $\pi(t,T)$:

$$\pi(t,T) = \theta(t)\Theta(T) \int_{d|t} \int_{D|T} \sum_{\nu \in \hat{F}^*} \sum_{c \in F} \bar{\nu}(b)\bar{\lambda}(ac) \sum_{w \in E} (\eta_d \tilde{\nu}(w)\chi((\delta_D + c)w) \tag{2.1}$$

where $\tilde{\nu}(w) = \nu(N(w))$ and $\chi(cw) = \lambda(cT(w))$ (cf. [Co], equation (2.2)).

We shall now specialise to the case when $n = 3$. Observe that, if $p|n$ (i.e., if $q = 3^k$ for some $k \in \mathbb{N}$), then $M = 1$ and the PFNT problem reduces to the (nonzero) PNT problem. If $q \equiv 2 \pmod 3$, then $M = x^2 + x + 1$ is irreducible over F; by Lemma 3.5 of [Co], $\pi(m, M) > 0$ if and only if $\pi(m, 1) > 0$, and so the PFNT problem reduces to the (nonzero) PNT problem in this case also. Hence only in the case when $q \equiv 1 \pmod 3$ need the full PFNT problem be considered. When $q \equiv 1 \pmod 3$, $M = (x-\gamma)(x-\gamma^2)$ (where $\gamma \in F$ is such that $\gamma^3 = 1$, $\gamma \neq 1$).

With regard to the multiplicative part of the problem, we note that all prime divisors of m must be congruent to 1 modulo 6. For, since $m|(q^2+q+1)$, an odd number, then m is odd. Furthermore, suppose that for some prime l, $l|m$. Then $l|q^3-1$ but $l \nmid q-1$; hence $\mathrm{ord}_l q = 3$. By Fermat's Little Theorem, $q^{l-1} \equiv 1 \pmod l$ since $l \nmid q$. So $3|l-1$, i.e., $l \equiv 1 \pmod 3$. Thus all prime divisors of m lie in the set $\{7, 13, 19, 31, 37, \ldots\}$.

Our strategy for proving the PFNT problem for $n = 3$ is to apply a sieving technique. We shall use the basic sieving inequality introduced in Theorem 3.1 of [Co]. Let $d|m$ and $f|x^n - 1$. Then (d_i, f_i) ($i = 1, \ldots, r$ for $r \in \mathbb{N}$) will be called *complementary divisor pairs* with *common divisor pair* (d_0, f_0) if the primes in $\mathrm{lcm}\{d_1, \ldots, d_r\}$ are precisely those in d, the irreducibles in $\mathrm{lcm}\{f_1, \ldots, f_r\}$ are precisely those in f, and for any distinct pair (i, j), the primes and irreducibles in $\gcd(d_i, d_j)$ and $\gcd(f_i, f_j)$ are precisely those in d_0 and f_0 respectively. Observe that the value of $\pi(d, f)$ will depend only on which "atoms" (primes/irreducibles) are present in d and f, not on the power to which the atoms occur.

Lemma 2.1 (Sieving inequality)**.** *For divisors d of m and f of $x^n - 1$, let $\{(d_1, f_1), \ldots, (d_r, f_r)\}$ be complementary divisor pairs of (d, f) with common divisor (d_0, f_0). Then*

$$\pi(d, f) \geq \left(\sum_{i=1}^{r} \pi(d_i, f_i) \right) - (r-1)\pi(d_0, f_0). \tag{2.2}$$

In the PNT case, where there is no additive component, the sieve will clearly take the following simpler form. For divisors d of m, let $d_1, \ldots, d_r$ be divisors of d (with common divisor d_0) such that the primes in $\mathrm{lcm}\{d_1, \ldots, d_r\}$ are precisely those in d and, for any distinct pair (i, j), the primes in $\gcd(d_i, d_j)$ are precisely those in d_0. Then

$$\pi(d, 1) \geq \left(\sum_{i=1}^{r} \pi(d_i, 1) \right) - (r-1)\pi(d_0, 1). \tag{2.3}$$

In the next section, we establish estimates for $\pi(t, 1)$ $(t|m)$.

3. Estimates for integer factors

In this section we obtain new estimates for the number $N(t,1)$ of t-free elements of E with prescribed norm and trace, where $t \in \mathbb{N}$ is a divisor of m. We improve upon the estimates of [Co] by applying some deep results of Katz arising from the study of Soto-Andrade sums [Ka].

Lemma 3.1 ([Ka], Theorem 4)**.** *Suppose that $n \geq 2$. Then*

$$\left| N(1,1) - \frac{q^n - 1}{q(q-1)} \right| \leq n q^{\frac{n-2}{2}}, \tag{3.1}$$

i.e.,

$$|\pi(1,1) - (q^n - 1)| \leq n \left(1 - \frac{1}{q}\right) q^{\frac{n+2}{2}}. \tag{3.2}$$

In particular, for $n = 3$, Lemma 3.1 has the form

$$|\pi(1,1) - (q^3 - 1)| \leq 3 \left(1 - \frac{1}{q}\right) q^{\frac{5}{2}}.$$

Note that this is an improvement, by a factor of approximately $\frac{q^{\frac{1}{2}}}{3}$, on the estimate

$$|\pi(1,1) - q^3| \leq \left(1 - \frac{(e+1)}{q}\right) q^3$$

($e := \gcd(3, q-1)$), obtainable from Corollary 2.2 of [Co] but useless as a lower bound. It is such increases in accuracy that allow us to solve the $n = 3$ case where the method of [Co] fails.

Next, we estimate $N(t,1)$ where $t|m$, $t > 1$.

Lemma 3.2 ([Ka], Corollary of Theorem 3 bis)**.** *Let η be a character of E of order d, where $d|m$, $d > 1$. Suppose $\eta^{n(q-1)}$ is not trivial. Set*

$$M(\eta) = \sum_{\substack{x \in E \\ N(x)=b \\ T(x)=a}} \eta(x).$$

Then

$$|M(\eta)| \leq n q^{\frac{n-2}{2}}.$$

This lemma is applicable when $n = 3$ to all $\eta_d \in \hat{F^*}$ ($d|m$, $d > 1$). For, consider some $\eta \in \hat{F^*}$ of order d, where $d|m$ and $d > 1$. Clearly η^{q-1} cannot be trivial or have order 3, since $(d, q-1) = 1$ and $(d, 3) = 1$.

Corollary 3.3. *Let $t|m$, $t > 1$, and $t_0|t$, $t_0 \geq 1$. Then*

$$\left| \pi(t,1) - \frac{\theta(t)}{\theta(t_0)} \pi(t_0,1) \right| \leq n\theta(t)(W(t) - W(t_0)) \left(1 - \frac{1}{q}\right) q^{\frac{n+2}{2}}. \tag{3.3}$$

Proof. By definition,

$$N(t,1) = \theta(t) \sum_{\substack{w \in E \\ N(w)=b \\ T(w)=a}} \int_{d|t} \eta_d(w) = \theta(t) \int_{d|t} M(\eta_d),$$

and so

$$N(t,1) - \frac{\theta(t)}{\theta(t_0)} N(t_0,1) = \theta(t) \sum_{\substack{d \mid t \\ d \nmid t_0}} M(\eta_d).$$

By Lemma 3.2,

$$\left| N(t,1) - \frac{\theta(t)}{\theta(t_0)} N(t_0,1) \right| \leq \theta(t)(W(t) - W(t_0)) n q^{\frac{n-2}{2}},$$

and hence

$$\left| \pi(t,1) - \frac{\theta(t)}{\theta(t_0)} \pi(t_0,1) \right| \leq n\theta(t)(W(t) - W(t_0)) \left(1 - \frac{1}{q}\right) q^{\frac{n+2}{2}}.$$

In particular, for $n = 3$,

$$\left| \pi(t,1) - \frac{\theta(t)}{\theta(t_0)} \pi(t_0,1) \right| \leq 3\theta(t)(W(t) - W(t_0)) \left(1 - \frac{1}{q}\right) q^{\frac{5}{2}}. \tag{3.4}$$

□

4. The (nonzero) PNT problem

Recall from Section 2 that, if q is a power of 3 or if $q \equiv 2 \pmod 3$, then the PFNT problem reduces to the (nonzero) PNT problem ("nonzero" refers to the fact that the prescribed trace a is nonzero). Hence, to establish the result in these cases, it suffices to show that $\pi(m,1) > 0$.

In order to simplify notation, from this point onwards we shall adopt the convention that all unmarked summation signs have index i running from $i = 1$ to s (where s is the number of distinct primes dividing m), and that $p[i]$ denotes the ith prime congruent to 1 modulo 6, i.e., the ith element of the set $\{7, 13, 19, 31, 37, \ldots\}$.

The following lemma provides a useful upper bound for $W(t)$.

Lemma 4.1. *For any positive integer t,*

$$W(t) \leq c_t t^{1/6}, \tag{4.1}$$

where $c_t = \frac{2^r}{(p_1 \ldots p_r)^{1/6}}$, and $p_1, \ldots, p_r$ are the distinct primes less than 64 that divide t. In particular, if $p_i \equiv 1 \pmod 6$ for all $i = 1, \ldots, r$, then $c_t < 3.08$.

(The proof is obvious using multiplicativity.)

Proposition 4.2. *Suppose q is a prime power, $q \not\equiv 1 \pmod 3$. Then $(q,3)$ is a PNT pair for all $q \geq 622{,}346$. In particular, $(3^k, 3)$ is a PNT pair for all $k \in \mathbb{N}$, $k > 12$.*

Proof. Apply the bounds of Lemma 3.1 and Corollary 3.3 directly, without sieving. Then

$$\pi(m,1) \geq \theta(m) \left\{ (q^3 - 1) - 3\left(1 - \frac{1}{q}\right) q^{\frac{5}{2}} \right\} - 3\theta(m)(W(m) - 1)\left(1 - \frac{1}{q}\right) q^{\frac{5}{2}},$$

and so $\pi(m,1) > 0$ whenever

$$q^{\frac{1}{2}} > 3W(m)\left(1 - \frac{1}{q}\right) + \frac{1}{q^{\frac{5}{2}}}. \tag{4.2}$$

Using the approximation of Lemma 4.1 for $W(m)$, $(q,3)$ is a PNT pair whenever

$$q > 3c_m(q-1)^{\frac{5}{6}} + \frac{1}{q^2}, \tag{4.3}$$

where $c_m = 3.08$. This inequality holds for integers $q \geq 622{,}346$, and so establishes the result. □

The following simplification applies in the case when $3|q$ and m is prime.

Lemma 4.3. *Let $q = 3^k$, $k \in \mathbb{N}$, so that $m = q^2 + q + 1$. Suppose that m is prime. Then*

$$N(m, 1) = N(1, 1),$$

where $N(t, 1)$ $(t|m)$ is the number of t-free elements of E with trace and norm equal to a and b respectively (a, $b \in F$, $a \neq 0$, b primitive).

Proof. Suppose $\alpha \in E$ (i.e., trivially 1-free) with $\mathrm{Tr}(\alpha) = a$, $N(\alpha) = b$, but $\alpha = \beta^m$. Then $\alpha^{q-1} = 1$, i.e., $\alpha \in \mathrm{GF}(q)$. Hence, $\mathrm{Tr}_{E/F}(\alpha) = 3\alpha$, which equals 0 since $\mathrm{char}F = 3$, a contradiction since $a \neq 0$. □

Proposition 4.4. *Suppose q is a prime power, $q \not\equiv 1 \pmod 3$, and let $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. Then $(q, 3)$ is a PNT pair whenever*

$$\pi(1,1)\left\{1 - \sum \frac{1}{p_i}\right\} - 3\left(1 - \frac{1}{q}\right) q^{\frac{5}{2}} \sum \left(1 - \frac{1}{p_i}\right) > 0, \tag{4.4}$$

and so certainly whenever

$$q^{\frac{1}{2}} > C_s \tag{4.5}$$

where

$$C_s := 3\left(2 + \frac{s-1}{1 - \sum_{i=1}^{s} \frac{1}{p[i]}}\right) + \frac{1}{3^{\frac{5}{2}}},$$

where $p[i]$ is the ith prime congruent to 1 modulo 6.

Proof. Apply the sieve with atomic divisors. Using the results of Corollary 3.3, $\pi(m, 1) > 0$ whenever

$$\pi(1,1)\left\{1 - \sum \frac{1}{p_i}\right\} - 3\left(1 - \frac{1}{q}\right) q^{\frac{5}{2}} \sum \left(1 - \frac{1}{p_i}\right) > 0.$$

By Lemma 3.1, $\pi(m, 1) > 0$ if

$$q^{\frac{1}{2}} > 3\left(1 - \frac{1}{q}\right)\left(1 + \frac{\sum(1 - \frac{1}{p_i})}{1 - \sum \frac{1}{p_i}}\right) + \frac{1}{q^{\frac{5}{2}}}. \tag{4.6}$$

Replacing the right-hand side of (4.6) by a larger quantity depending solely on s, we see that the desired result certainly holds when

$$q^{\frac{1}{2}} > C_s \tag{4.7}$$

where

$$C_s := 3\left(2 + \frac{s-1}{1 - \sum \frac{1}{p[i]}}\right) + \frac{1}{3^{\frac{5}{2}}}.$$

Observe that, since C_s is a constant for fixed s and increases as s increases (for all s such that $\sum_{i=1}^{s} \frac{1}{p[i]} < 1$), $q^{\frac{1}{2}} > C_{s_1}$ for some s_1 implies that $q^{\frac{1}{2}} > C_s$ for all $s \leq s_1$. □

Proposition 4.5. (i) *Suppose* $q = 3^k$ *(*$k \in \mathbb{N}$*,* $k \geq 5$ *or* $k = 3$*). Then* $(q, 3)$ *is a PFNT pair.*

(ii) *Suppose* $q \equiv 2 \pmod 3$ *and* $q \leq 622{,}346$ *but* $q \notin \{5, 8, 11, 17, 23, 29, 32, 47, 53, 107, 137, 149, 191\}$*. Then* $(q, 3)$ *is a PNT pair.*

Proof. (i) Lemma 4.2 has established the result for $k > 12$; so we need consider only $k \leq 12$.

Let $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$. We apply Proposition 4.4. For all $q = 3^k$ with $k \leq 12$ we have $s \leq 5$. Since ${C_5}^2 < 577 < 3^6$, the result holds for $q = 3^k$, $k \geq 6$. The result is established for $k = 5$ ($s = 2$), since $3^5 > 71 > {C_2}^2$. When $k = 3$, m (= 757) is prime; hence by Lemma 4.3, m may be replaced by 1. Inequality (4.2) is then satisfied, since $\sqrt{27} > 2.8892$.

(ii) For $q > 2$, let $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$; since $m \leq q^2 + q + 1$, $s \leq 8$ for $q < 622{,}346$ (merely by size considerations). As in part (i), we apply Proposition 4.4.

Since inequality (4.5) holds for all relevant $q > 1622$, the result is established for prime powers $q \geq 1637$. For $q < 1622$, we find that $s \leq 4$; then the desired result holds for $q > 361$, i.e., for all $q \geq 367$. Since the smallest $q \equiv 2 \pmod 3$ with $s = 4$ is $q = 809$, use of inequality (4.5) with $s = 3$ then establishes the result for $q > 204$, i.e., $q \geq 227$. However, even use of exact values fails for those $q < 204$ with $s = 3$, namely $\{107, 137, 149, 191\}$. Similarly, (4.5) holds with $s = 2$ for $q > 98$, and thus establishes the result for all $q \geq 101$ (apart from the preceding exceptions). Use of exact values in inequality (4.6) yields the result for $q = 83$ ($m = 19 \cdot 367$, $\sqrt{83} > 9.110 > 9.065 >$right side of (4.6)). Values of q with $s = 2$ for which exact values are insufficient are $\{11, 23, 29, 32, 47, 53\}$. Finally, $q^{\frac{1}{2}} > C_1$ for all $q > 36$, i.e., $q \geq 41$, which establishes all remaining cases with the exception of $\{5, 8, 17\}$. □

5. The PFNT problem

In this section, the full PFNT problem will be solved for the case when $q \equiv 1 \pmod 3$.

Denote by L a linear factor of M ($= x^2 + x + 1$); L may take the values $x - \gamma$ or $x - \gamma^2$, where $\gamma \in F$ is such that $\gamma^3 = 1$, $\gamma \neq 1$. We begin by deriving estimates for the number $N(1, L)$ of L-free elements of E with prescribed norm and trace. For economy of calculation, it is in fact desirable to consider the difference between $\pi(1, L)$ and $\theta(L)\pi(1, 1)$ (in some sense the "error term"). We will prove the following lemma.

Lemma 5.1. *Let* $q \equiv 1 \pmod 3$*. Then*

$$\begin{aligned} &\left|\pi(1, x - \gamma) + \pi(1, x - \gamma^2) - 2\left(1 - \frac{1}{q}\right)\pi(1, 1)\right| \\ &\qquad \leq 2q^{\frac{5}{2}}\left(1 - \frac{3}{q} - \frac{2}{q^2}\right) + 2q^2\left(1 - \frac{3}{q}\right). \end{aligned} \tag{5.1}$$

First, we establish some results about δ_L. For a polynomial $f(x)$, let f^σ denote the polynomial obtained from f by replacing x^i by x^{q^i}.

Lemma 5.2. *If* $D | x^{n/k} - 1$ *(where* $k | n$*), then* δ_D *is a root of* $(x^{n/k} - 1)^\sigma$*, i.e.,* $\delta_D \in \mathrm{GF}(q^{n/k})$.

Proof. Set $R = q^{n/k}$. So for the canonical character χ_1 of E, $\chi_1(w) = \lambda(\mathrm{Tr}_{R^k/p}(w))$ ($w \in E$), where $\lambda(x) = e^{\frac{2\pi x}{p}}$. Let $\chi(w) = \chi_\delta(w) = \lambda(\mathrm{Tr}_{R^k/p}(\delta w))$ and suppose $\delta \in$

$\mathrm{GF}(R)$; so $\delta^R = \delta$. Then

$$\begin{aligned}\chi(w^R) &= \lambda(Tr_{R^k/p}(\delta w^R)) \\ &= \lambda(Tr_{R/p}(Tr_{R^k/R}(\delta^R w^R))) \\ &= \lambda(Tr_{R/p}(Tr_{R^k/R}(\delta w))) \\ &= \lambda(Tr_{R^k/p}(\delta w)) \\ &= \chi(w).\end{aligned}$$

Hence $\chi(w^R - w) = 1$ for all $w \in E$. So for any $D|x^{n/k} - 1$, i.e., $D^\sigma|x^R - x$, $\chi_\delta(D^\sigma(w)) = 1$. Thus $\delta = \delta_D$ for some $D|x^{n/k} - 1$. Letting δ vary in $\mathrm{GF}(R)$ accounts for all R characters of order dividing $x^{n/k} - 1$. □

Lemma 5.3. *Suppose $q \equiv 1 \pmod 3$, and let $\gamma \in \mathrm{GF}(q)$ be such that $\gamma^3 = 1$, $\gamma \neq 1$.*

(i) *Let $D = x - \gamma$. Then $(x - \gamma^2)^\sigma(\delta_D) = 0$, i.e., ${\delta_D}^q = \gamma^2\delta_D$.*
(ii) *Let $D = x - \gamma^2$. Then $(x - \gamma)^\sigma(\delta_D) = 0$, i.e., ${\delta_D}^q = \gamma\delta_D$.*

Proof. (i) Suppose $\delta^q = \gamma^2\delta$. Define $\chi(w) = \chi_1(\delta w) = \lambda(\mathrm{Tr}_{q^3/p}(\delta w))$, $w \in E = \mathbb{F}_{q^3}$. Then

$$\begin{aligned}\chi(w^q - \gamma w) &= \lambda(\mathrm{Tr}_{q/p}[\mathrm{Tr}_{q^3/q}(\delta(w^q - \gamma w))]) \\ &= \lambda(\mathrm{Tr}_{q/p}[\mathrm{Tr}_{q^3/q}(\gamma\delta^q w^q - \gamma\delta w)] \\ &= \lambda(\mathrm{Tr}_{q/p}[\gamma\,\mathrm{Tr}_{q^3/q}((\delta w)^q - \delta w)]) \\ &= 1,\end{aligned}$$

since $\mathrm{Tr}_{q^3/q}((\delta w)^q - \delta w) \equiv 0$. So the F-order of χ is $x - \gamma$. This accounts for all characters with F-order $x - \gamma$.

(ii) Replace γ by γ^2 in (i). □

We are now ready to prove Lemma 5.1. Throughout this discussion, $G_n(\eta)$ (where η is a multiplicative character on $\mathbb{F}_{q^n}^*$) will denote a Gauss sum in $\mathbb{F}_{q^n}^*$. We will use the notation $J_a(\nu_1, \ldots, \nu_k)$ (where $a \in F$, $\nu_1, \ldots, \nu_k$ are multiplicative characters of F, $k \in \mathbb{N}$) to denote the Jacobi sum

$$\sum_{c_1+\ldots+c_k=a} \nu_1(c_1)\ldots\nu_k(c_k).$$

For extra background material, the reader may consult texts such as [LiNi].

Proof of Lemma 5.1. By equation (2.1), since $\Theta(L) = (1 - \frac{1}{q})$,

$$\begin{aligned}&\pi(1, L) - \Theta(L)\pi(1, 1) \\ &\quad = \Theta(L)\left(-\frac{1}{q-1}\right)\sum_{\nu\in\hat{F^*}}\sum_{c\in F}\sum_{(\delta_L)}\bar{\nu}(b)\bar{\lambda}(ac)\sum_{w\in E}\tilde{\nu}(w)\chi((\delta_L + c)w),\end{aligned} \tag{5.2}$$

where δ_L runs through all $\Phi(L)$ elements of Δ_L (i.e., χ_{δ_L} runs through all additive characters of E of order L). Separating the term for which $c = 0$, we have

$$\begin{aligned}\pi(1,L) - \Theta(L)\pi(1,1) &= -\frac{1}{q}\left\{\sum_{\nu\in\hat{F^*}}\sum_{(\delta_L)}\bar{\nu}(b)\sum_{w\in E}\tilde{\nu}(w)\chi(\delta_L w)\right. \\ &+ \left.\sum_{\nu\in\hat{F^*}}\sum_{c\in F^*}\sum_{(\delta_L)}\bar{\nu}(b)\bar{\lambda}(ac)\sum_{w\in E}\tilde{\nu}(w)\chi((\delta_L+c)w)\right\}. \qquad (5.3)\end{aligned}$$

For the first term on the right side of (5.3), using the fact that $\delta_L \neq 0$, replace w by $\frac{w}{\delta_L}$ to obtain

$$\sum_{\nu\in\hat{F^*}}\nu\left(\frac{1}{b}\right)G_3(\tilde{\nu})\sum_{(\delta_L)}\bar{\tilde{\nu}}(\delta_L).$$

Since $F^*\Delta_D = \Delta_D$,

$$\sum_{(\delta_L)}\bar{\tilde{\nu}}(\delta_L) = \frac{1}{q-1}\sum_{(\delta_L)}\sum_{c\in F^*}\bar{\tilde{\nu}}(c\delta_L) = \frac{1}{q-1}\sum_{(\delta_L)}\bar{\tilde{\nu}}(\delta_L)\left(\sum_{c\in F^*}\bar{\tilde{\nu}}(c)\right),$$

and the inner sum equals 0 unless ν^* ($:= \tilde{\nu}|_F$) is trivial, when it equals $q-1$.

Note that, for $k \in F$, $\nu^*(k) = \tilde{\nu}(k) = \nu(N(k)) = \nu(k^3)$, i.e., $\nu^* = \nu^3$. So the first term of (5.3) can be simplified to

$$\sum_{\substack{\nu\in\hat{F^*}\\ \nu^3=\nu_1}}\sum_{(\delta_L)}\nu\left(\frac{1}{b}\right)G_3(\tilde{\nu})\bar{\tilde{\nu}}(\delta_L).$$

For the second term on the right side of (5.3) (i.e., the part for which $c \neq 0$), replace δ_L by $c\delta_L$, then w by $\frac{w}{c(\delta_L+1)}$, to get

$$\sum_{\nu\in\hat{F^*}}\nu\left(\frac{1}{b}\right)G_3(\tilde{\nu})\sum_{(\delta_L)}\bar{\tilde{\nu}}(\delta_L+1)\sum_{c\in F^*}\bar{\lambda}(ac)\bar{\tilde{\nu}}(c). \qquad (5.4)$$

Consider the inner sum $\sum_{c\in F^*}\bar{\lambda}(ac)\bar{\tilde{\nu}}(c)$ of (5.4); in the case when $\nu^3 = \nu_1$, this reduces to a sum over additive characters of F, while for $\nu^3 \neq \nu_1$, a Gauss sum over F is obtained. Thus the second term of (5.3) may be expanded as

$$-\sum_{\substack{\nu\in\hat{F^*}\\ \nu^3=\nu_1}}\nu\left(\frac{1}{b}\right)G_3(\tilde{\nu})\sum_{(\delta_L)}\bar{\tilde{\nu}}(\delta_L+1) + \sum_{\substack{\nu\in\hat{F^*}\\ \nu^3\neq\nu_1}}\nu^*(a)\nu\left(\frac{1}{b}\right)G_3(\tilde{\nu})\bar{G_1}(\nu^*)\sum_{(\delta_L)}\bar{\tilde{\nu}}(\delta_L+1).$$

Hence,

$$\begin{aligned}\pi(1,L)-\Theta(L)\pi(1,1) &= -\frac{1}{q}\left(\sum_{\substack{\nu\in\hat{F^*}\\ \nu^3\neq\nu_1}}\nu\left(\frac{a^3}{b}\right)G_3(\tilde{\nu})\bar{G_1}(\nu^*)\sum_{(\delta_L)}\bar{\tilde{\nu}}(\delta_L+1)\right.\\ &\quad\left.+\sum_{\substack{\nu\in\hat{F^*}\\ \nu^3=\nu_1\\ \bar{\nu}\neq\eta_1}}\nu\left(\frac{1}{b}\right)G_3(\tilde{\nu})\sum_{(\delta_L)}(\bar{\tilde{\nu}}(\delta_L)-\bar{\tilde{\nu}}(\delta_L+1))\right)\\ &= \frac{1}{q}\left(\sum_{\substack{\nu\in\hat{F^*}\\ \nu^3=\nu_1\\ \nu\neq\nu_1}}\nu\left(\frac{1}{b}\right){G_1}^3(\nu)\sum_{(\delta_L)}[\bar{\nu}(N(\delta_L+1))-\bar{\nu}(N(\delta_L))]\right.\\ &\quad\left.-\sum_{\substack{\nu\in\hat{F^*}\\ \nu^3\neq\nu_1}}\sum_{(\delta_L)}\nu\left(\frac{a^3}{b}\right)\bar{\nu}(N(\delta_L+1))\bar{G_1}(\nu^3){G_1}^3(\nu)\right),\end{aligned}$$

since $G_3(\tilde{\nu})=G_1^3(\nu)$ by the Davenport-Hasse Theorem (see [LiNi], Chapter 5).

Consider the specific values that may be taken by L, namely $L=x-\gamma$ and $L=x-\gamma^2$. By Lemma 5.2, since these L are divisors of x^3-1, ${\delta_L}^{q^3}=\delta_L$. Using Lemma 5.2 and Lemma 5.3, we find that ${\delta_L}^3\in{\mathbb{F}_q}^*$ but $\delta_L\notin{\mathbb{F}_q}^*$, and so ${\delta_L}^3=c$, where c is a non-cube in F. In fact, $\{\delta_{x-\gamma}\}\cup\{\delta_{x-\gamma^2}\}=\{e\in E\colon\ e^{3(q-1)}=1,\ e^{(q-1)}\neq 1\}=\{\text{cube roots of } c,\ c \text{ a non-cube in } F\}$, a set of cardinality $2(q-1)$.

In the case when $L=x-\gamma$, using Lemma 5.3 we get

$$N(\delta_L)=\delta_L{\delta_L}^q{\delta_L}^{q^2}=\delta_L(\gamma^2\delta_L)(\gamma\delta_L)={\delta_L}^3=c$$

and

$$N(1+\delta_L)=(1+\gamma+\gamma^2)(\delta_L+{\delta_L}^2)=(1+{\delta_L}^3)=1+c.$$

The same values are obtained when $L=x-\gamma^2$.

Denote $x-\gamma$ and $x-\gamma^2$ by L_1 and L_2 respectively. Let $\nu_3\in\hat{F^*}$ be an arbitrary character of degree 3. Then

$$\pi(1,L_1)+\pi(1,L_2)-2\Theta(L)\pi(1,1)=\frac{2}{q}\{S_2-S_1\}$$

where

$$S_1:=\sum_{\substack{\nu\in\hat{F^*}\\ \nu^3\neq\nu_1}}\nu\left(\frac{a^3}{b}\right)\bar{G_1}(\nu^3){G_1}^3(\nu)\sum_{c\in F^*}\left(1-\frac{1}{2}(\nu_3(c)+{\nu_3}^2(c))\right)\bar{\nu}(1+c) \tag{5.5}$$

and

$$S_2 := \sum_{\substack{\nu \in \hat{F^*} \\ \nu^3 = \nu_1 \\ \nu \neq \nu_1}} \nu\left(\frac{1}{b}\right) {G_1}^3(\nu) \sum_{c \in F^*} \left[1 - \frac{1}{2}(\nu_3(c) + {\nu_3}^2(c))\right] (\bar{\nu}(1+c) - \bar{\nu}(c)). \tag{5.6}$$

Consider S_1 (as given by (5.5)). It may be written in the form

$$S_1 = \sum_{\substack{\nu \in \hat{F^*} \\ \nu^3 \neq \nu_1}} \nu\left(\frac{a^3}{b}\right) \bar{G_1}(\nu^3) {G_1}^3(\nu)\sigma_1,$$

say, where $\sigma_1 := \sum_{c \in F^*}(1 - \frac{1}{2}(\nu_3(c) + {\nu_3}^2(c)))\bar{\nu}(1+c)$. Then

$$\begin{aligned} \sigma_1 &= \sum_{c \in F^*} \bar{\nu}(1+c) - \frac{1}{2}\nu_3(-1) \sum_{c \in F^*} \nu_3(c)\bar{\nu}(1-c) - \frac{1}{2}{\nu_3}^2(-1) \sum_{c \in F^*} {\nu_3}^2(c)\bar{\nu}(1-c) \\ &= -1 - \frac{1}{2}(J_1(\nu_3, \bar{\nu}) + J_1({\nu_3}^2, \bar{\nu})). \end{aligned}$$

Since each Jacobi sum has absolute value $\sqrt{q}$,

$$|S_1| \leq (q-4)\sqrt{q}q^{\frac{3}{2}}(1 + \sqrt{q}),$$

i.e.,

$$\frac{2}{q}|S_1| \leq 2q^{\frac{5}{2}}\left(1 - \frac{4}{q}\right)\left(1 + \frac{1}{\sqrt{q}}\right). \tag{5.7}$$

Now consider S_2 (as given by (5.6)). For a given ν with $\nu^3 = \nu_1$, $\nu \neq \nu_1$, the inner sum σ_2 has the form

$$\sigma_2 := \sum_{c \in F^*} \left(1 - \frac{1}{2}(\nu_3(c) + {\nu_3}^2(c))\right) (\bar{\nu}(1+c) - \bar{\nu}(c))$$

where ν_3 is an arbitrary character of order 3. Without loss of generality, we may set $\nu_3 := \nu$ in our expression for σ_2:

$$\begin{aligned} \sigma_2 &= \sum_{c \in F^*} \bar{\nu}(1+c) - \sum_{c \in F^*} \bar{\nu}(c) \\ &\quad -\frac{1}{2}\left(\sum_{c \in F^*} \nu(c)\bar{\nu}(1+c) - \sum_{c \in F^*} \nu(c)\bar{\nu}(c)\right. \\ &\qquad \left. + \sum_{c \in F^*} \nu^2(c)\bar{\nu}(1+c) - \sum_{c \in F^*} \nu^2(c)\bar{\nu}(c)\right) \\ &= (-1) - 0 - \frac{1}{2}(J_1(\nu, \bar{\nu}) - (q-1) + J_1(\nu^2, \bar{\nu}) - 0) \\ &= \frac{1}{2}(q-2) - \frac{1}{2}J_1(\nu^2, \bar{\nu}), \end{aligned}$$

since $\nu\bar{\nu} = \nu_1$ and $\nu^2\bar{\nu} = \nu$.

Thus $|\sigma_2| \leq \frac{1}{2}(q-2) + \frac{1}{2}\sqrt{q}$. Hence,

$$|S_2| \leq 2q^{\frac{3}{2}}\left(\frac{1}{2}(q-2) + \frac{1}{2}\sqrt{q}\right) = q^{\frac{5}{2}}\left(1 - \frac{2}{q}\right) + q^2,$$

i.e.,

$$\frac{2}{q}|S_2| \le 2q^{\frac{3}{2}}\left(1-\frac{2}{q}\right)+2q. \tag{5.8}$$

Combining inequalities (5.7) and (5.8), we get

$$\begin{aligned}&|\pi(1,L_1)+\pi(1,L_2)-2\Theta(L)\pi(1,1)|\\ &\quad\le 2q^{\frac{5}{2}}\left(1-\frac{4}{q}\right)\left(1+\frac{1}{\sqrt{q}}\right)+2q^{\frac{3}{2}}\left(1-\frac{2}{q}\right)+2q\\ &\quad= 2q^{\frac{5}{2}}\left(1-\frac{3}{q}-\frac{2}{q^2}\right)+2q^2\left(1-\frac{3}{q}\right),\end{aligned}$$

which proves the result. □

The following is a sufficient condition for $(q,3)$ to be a PFNT pair.

Lemma 5.4. *Suppose $q\equiv 1 \pmod 3$. Then $(q,3)$ is a PFNT pair whenever*

(5.9)

$$\begin{aligned}&\pi(1,1)\left(\theta(m)-\frac{2}{q}\right)\\ &\quad> 3\theta(m)(W(m)-1)\left(1-\frac{1}{q}\right)q^{\frac{5}{2}}+2q^{\frac{5}{2}}\left(1-\frac{3}{q}-\frac{2}{q^2}\right)+2q^2\left(1-\frac{3}{q}\right).\end{aligned}$$

Proof. Apply the sieve in the following form:

$$\pi(m,M)\ge \pi(m,1)+\pi(1,x-\gamma)+\pi(1,x-\gamma^2)-2\pi(1,1).$$

Using the lower bounds for $\pi(m,1)$ and the $\pi(1,L_i)$ $(i=1,2)$ from inequalities (3.3) and Lemma 5.1, we see that $\pi(m,M)>0$ whenever (5.9) holds. □

Lemma 5.5. *Let $q\equiv 1 \pmod 3$ be a prime power, and let m be the greatest divisor of q^3-1 co-prime to $q-1$. Then*

$$\theta(m)>\frac{1}{q^{\frac{1}{6}}}.$$

Proof. Observe first that, if l is a prime divisor of m, then l is congruent to 1 modulo 6 and hence $l\ge 7$. Since $x-x^{\frac{11}{12}}-1>0$ holds for $x\ge 7$, it follows that $\theta(p^k)=\theta(p)=\frac{p-1}{p}>\frac{1}{p^{\frac{1}{12}}}\ge\frac{1}{(p^k)^{\frac{1}{12}}}$ where $p\ge 7$ is prime and $k\in\mathbb{N}$. Thus by multiplicativity, $\theta(m)>\frac{1}{m^{\frac{1}{12}}}$. Since $3m\le\frac{q^3-1}{q-1}<(q+1)^2$, it follows that $q>3^{1/2}m^{1/2}-1$, and so $q\ge m^{\frac{1}{2}}$ for all q. Hence $\frac{1}{q}\le\frac{1}{m^{\frac{1}{2}}}$, and so $\theta(m)>\frac{1}{m^{\frac{1}{12}}}\ge\frac{1}{q^{\frac{1}{6}}}$. □

Proposition 5.6. *Let $q\equiv 1 \pmod 3$ be a prime power. Then $(q,3)$ is a PFNT pair for all $q\ge 252{,}950$.*

Proof. By Lemma 5.4, $\pi(m,M)>0$ if

$$\begin{aligned}&\pi(1,1)\left(\theta(m)-\frac{2}{q}\right)\\ &\quad> 3\theta(m)(W(m)-1)\left(1-\frac{1}{q}\right)q^{\frac{5}{2}}+2q^{\frac{5}{2}}\left(1-\frac{3}{q}-\frac{2}{q^2}\right)+2q^2\left(1-\frac{3}{q}\right).\end{aligned} \tag{5.10}$$

Then by Lemma 3.1, $\pi(m,M)>0$ if

(5.11)
$$\theta(m)\left(q^3-3W(m)\left(1-\frac{1}{q}\right)q^{\frac{5}{2}}-1\right)>2q^{\frac{5}{2}}\left(1-\frac{6}{q}+\frac{1}{q^2}\right)+2q^2\left(2-\frac{3}{q}\right)-\frac{2}{q}.$$

By Lemma 4.1, $W(m)\leq\frac{c_mq^{\frac{1}{2}}}{3^{\frac{1}{6}}(q-1)^{\frac{1}{6}}}$, where $c_m<3.08$. Set $d:=3^{\frac{5}{6}}c_m$; then $3W(m)\leq\frac{dq^{\frac{1}{2}}}{(q-1)^{\frac{1}{6}}}$, and so $3W(m)(\frac{q-1}{q})q^{\frac{5}{2}}\leq d(q-1)^{\frac{5}{6}}q^2$. Using this result and Lemma 5.5, we see that $\pi(m,M)>0$ certainly if

$$\frac{1}{q^{\frac{1}{6}}}\{q^3-d(q-1)^{\frac{5}{6}}q^2-1\}>2q^{\frac{5}{2}}\left(1-\frac{6}{q}+\frac{1}{q^2}\right)+2q^2\left(2-\frac{3}{q}\right)-\frac{2}{q}, \tag{5.12}$$

i.e., if

$$q>d(q-1)^{\frac{5}{6}}+2q^{\frac{2}{3}}\left(1-\frac{6}{q}+\frac{1}{q^2}\right)+2q^{\frac{1}{6}}\left(2-\frac{3}{q}\right)+\frac{1}{q^2}. \tag{5.13}$$

Take $c_m=3.08$ and set $d=7.70$ in inequality (5.13). Then inequality (5.13) holds for all $q\geq 252{,}950$.

In order to establish the result for smaller prime powers q, we will use the following sufficient condition, which arises from the application of the sieve with atomic divisors.

Once again we shall adopt the convention that all unmarked summation signs have index i running from $i=1$ to s.

Lemma 5.7. *The following is a sufficient condition for $(q,3)$ to be a PFNT pair. When $q\equiv 1\,(\mathrm{mod}\ 3)$,*

$$\sqrt{q}>\frac{(3s+2)-\frac{(3s+6)}{q}-\frac{4}{q^2}-3(1-\frac{1}{q})\sum\frac{1}{p_i}+\frac{2}{\sqrt{q}}(1-\frac{3}{q})}{1-\sum\frac{1}{p_i}-\frac{2}{q}}+3(1-\tfrac{1}{q})+\frac{1}{q^{\frac{5}{2}}} \tag{5.14}$$

(where $m=p_1^{\alpha_1}\dots p_s^{\alpha_s}$).

Proof Let $m=p_1^{\alpha_1}\dots p_s^{\alpha_s}$, where $p_1,\dots,p_s$ are distinct primes and $s\in\mathbb{N}$ (recall that the values of the α_i will be irrelevant here). Apply the sieve in the form

$$\pi(m,M)\geq\pi(p_1,1)+\ldots+\pi(p_s,1)+\pi(1,x-\gamma)+\pi(1,x-\gamma^2)-(s+1)\pi(1,1). \tag{5.15}$$

Using the results of Lemma 5.1 and Corollary 3.3, $\pi(m,M)>0$ if

(5.16)
$$\pi(1,1)\left(1-\sum\frac{1}{p_i}-\frac{2}{q}\right)$$
$$-2q^{\frac{5}{2}}\left(1-\frac{3}{q}-\frac{2}{q^2}\right)-2q^2\left(1-\frac{3}{q}\right)-3q^{\frac{5}{2}}\left(1-\frac{1}{q}\right)\sum\left(1-\frac{1}{p_i}\right)>0,$$

i.e., if

$$\pi(1,1)>\frac{q^{\frac{5}{2}}((3s+2)-\frac{(3s+6)}{q}-\frac{4}{q^2}-3(1-\frac{1}{q})\sum\frac{1}{p_i})+2q^2(1-\frac{3}{q})}{1-\sum\frac{1}{p_i}-\frac{2}{q}}, \tag{5.17}$$

and so, using Lemma 3.1, certainly if

(5.18)
$$q > \frac{\sqrt{q}((3s+2) - \frac{(3s+6)}{q} - \frac{4}{q^2}) - 3\sqrt{q}(1-\frac{1}{q})\sum \frac{1}{p_i} + 2(1-\frac{3}{q})}{1 - \sum \frac{1}{p_i} - \frac{2}{q}} + 3\sqrt{q}(1-\tfrac{1}{q}) + \frac{1}{q^2}.$$

Observe that the inequalities of Lemma 5.7 are of use only when the denominator $1 - \sum \frac{1}{p_i} - \frac{3}{q} > 0$; in particular, it is necessary to have $\sum \frac{1}{p_i} < 1$. However, since all prime powers q that are congruent to 1 modulo 3 and less than 252,950 have $s \leq 7$, and all prime divisors of m are congruent to 1 modulo 6, the denominator is always positive in this case. □

Proposition 5.8. *Suppose* $q \equiv 1 \pmod 3$ *and* $q \leq 252{,}950$*, but* $q \notin \{7, 13, 16, 19, 25, 31, 37, 43, 49, 61, 64, 67, 79, 109, 121, 163, 211, 256\}$*. Then* $(q, 3)$ *is a PFNT pair.*

Proof. For $q > 4$, observe that

$$\sum \frac{1}{p_i} \geq \frac{3}{q^2} - \frac{3}{q^3},$$

since $\sum \frac{1}{p_i} \geq \frac{3}{q^2+q+1} = \frac{3}{q^2}(1 - \frac{1}{q} + \frac{1}{q(q^2+q+1)})$. Using this lower bound in Lemma 5.7, the desired result holds if

$$\sqrt{q} > \frac{(3s+2) - \frac{(3s+6)}{q} - \frac{13}{q^2} + \frac{18}{q^3} + \frac{2}{\sqrt{q}}(1-\frac{3}{q})}{1 - \sum \frac{1}{p_i} - \frac{2}{q}} + 3\left(1 - \frac{1}{q}\right) + \frac{1}{q^{\frac{5}{2}}}. \tag{5.19}$$

An upper bound is required for $\sum \frac{1}{p_i}$, say $\sum \frac{1}{p_i} \leq K(q)$ for some function K. In general, to simplify calculations, the crude estimate

$$\sum_{i=1}^{s} \frac{1}{p_i} \leq \sum_{i=1}^{s} \frac{1}{p[i]} \tag{5.20}$$

will be used, where $p[i]$ is the ith prime congruent to 1 modulo 6, as in Section 4. (More precise values may be taken in specific cases.)

Observe that the desired result certainly holds when

$$\sqrt{q} > \frac{(3s+2) + \frac{2}{\sqrt{q}} + \frac{18}{q^3}}{1 - \sum \frac{1}{p_i} - \frac{2}{q}} + 3 + \frac{1}{q^{\frac{5}{2}}}, \tag{5.21}$$

and, for fixed s, the function of q on the right side of (5.21) clearly decreases as q increases. Hence to prove for a given s that the result is true for $q \geq q_0$ (some $q_0 \in \mathbb{N}$), it is sufficient to show that inequality (5.21) holds for $q = q_0$.

For $q \leq 252{,}950$, we have $s \leq 7$. Using the basic estimate

$$\sum \frac{1}{p_i} \leq \frac{1}{7} + \frac{1}{13} + \frac{1}{19} + \frac{1}{31} + \frac{1}{37} + \frac{1}{43} + \frac{1}{61} < 0.3714, \tag{5.22}$$

inequality (5.21) holds with $s = 7$ for relevant $q > 1580$, hence for all $q \geq 1597$. Now, for prime powers $q \equiv 1 \pmod 3$ less than 1580, it happens that $s \leq 4$; in fact, except for the two values $q = 919$ and $q = 1369$, $s \leq 3$. Using the estimate

$$\sum \frac{1}{p_i} \leq \frac{1}{7} + \frac{1}{13} + \frac{1}{19} + \frac{1}{31} < 0.3047, \tag{5.23}$$

inequality (5.21) holds with $s = 4$ for $q > 546$ and hence for all $q \geq 547$. For $s = 3$, use of inequality (5.20) in (5.21) establishes the result for $q > 339$, i.e., $q \geq 343$. For $q = 277$ ($m = 7 \cdot 19 \cdot 193$) and $q = 289$ ($m = 7 \cdot 13 \cdot 307$), use of exact

values in Lemma 5.7 establishes the result. However, this approach is insufficient for $\{121, 163, 211, 256\}$. In the $s = 2$ case, inequality (5.21) establishes the result for $q > 185$, i.e., $q \geq 193$, when applied with the approximation of (5.20), and for $q = 169$ ($m = 61 \cdot 157$) and $q = 181$ ($m = 79 \cdot 139$) when exact values are used in (5.21) (respectively, $181 > 153.49$ and $169 > 148.80$). Use of Lemma 5.7 suffices for $q = 139$ ($m = 13 \cdot 499$), since $139 > 137.14$. Outstanding exceptions in the $s = 2$ case are $\{16, 25, 37, 49, 61, 64, 67, 79, 109\}$. When $s = 1$, replacing p_1 by 7 in inequality (5.21) establishes the result for $q > 86$, i.e., $q \geq 97$; use of exact p_1 ($= m$) deals with the case $q = 73$ ($m = 1801$). The remaining exceptions with $s = 1$ are $\{7, 13, 19, 31, 43\}$. □

6. Computational strategy for remaining cases

To deal with the 34 cases remaining after Propositions 4.5 and 5.8, we use the computer package MAPLE (version 6) to search the field E for m-free elements with norms and traces equal to the required values. (For reference, the set of exceptional q is as follows: $\{3, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 29, 31, 32, 37, 43, 47, 49, 53, 61, 64, 67, 79, 81, 107, 109, 121, 137, 149, 163, 191, 211, 256\}$.)

The following lemma allows us to simplify our computational strategy in some cases for which the PFNT problem reduces to the PNT.

Lemma 6.1. *Let q be a prime power, $q \not\equiv 1 \pmod 3$. Denote by $Z_{\alpha,\beta}(m)$ the number of elements $w \in E$ that are m-free and have $\mathrm{Tr}_{E/F}(w) = \alpha$, $N_{E/F}(w) = \beta$ ($\alpha, \beta \in F$). Suppose*

$$Z_{1,b}(m) > 0 \quad \forall b \in F^*.$$

Then $(q, 3)$ is a PNT pair.

Proof. To prove that $(q, 3)$ is a PNT pair, we must show that $N(m, 1) > 0$, i.e., that $Z_{a,b}(m) > 0$ for all $a, b \in F$, $a \neq 0$, b primitive. We prove the (stronger) result

$$Z_{a,b}(m) > 0 \quad \forall a, b \in F^*.$$

If $a = 1$, there is nothing to prove. Otherwise, set $b^* := \frac{b}{a^3} \in F^*$. Since $Z_{1,b^*}(m) > 0$, there exists an element $\zeta \in E$ such that ζ is m-free, $\mathrm{Tr}_{E/F}(\zeta) = 1$, and $N_{E/F}(\zeta) = b^*$. Then $\alpha := a\zeta$ is also m-free, and has $\mathrm{Tr}_{E/F}(\alpha) = a$ and $N_{E/F}(\alpha) = b$.

Use of Lemma 6.1 reduces the number of necessary tests from $(q-1)\phi(q-1)$ (testing each pair (a, b), b primitive) to $q - 1$ (testing each pair $(1, b)$, b nonzero). Since the condition involved is stronger than the PNT condition, this simplification is only of practical use in those cases when $q - 1$ is prime, or $\phi(q - 1)$ is not too much smaller than $q - 1$. However, it is successful in dealing with all $q \not\equiv 1 \pmod 3$ up to $q = 32$. For larger values of q, we must search E explicitly.

In the PNT case, the desired result holds without exception for all $q \not\equiv 1 \pmod 3$ remaining from the previous sections.

As an illustration, we display the relevant cubic polynomials for the case when $q = 5$. The following table lists eight cubic polynomials over $F = \mathrm{GF}(5)$ whose roots $\alpha \in E = \mathrm{GF}(5^3)$ are primitive and free with norm and trace equal to b and a respectively.

$(a,\ b)$	Relevant PFNT cubic
(1,2)	x^3+4x^2+3
(1,3)	x^3+4x^2+x+2
(2,2)	x^3+3x^2+2x+3
(2,3)	x^3+3x^2+2
(3,2)	x^3+2x^2+3
(3,3)	x^3+2x^2+2x+2
(4,2)	x^3+x^2+x+3
(4,3)	x^3+x^2+2

The cubic polynomials given in the table for $(a,b)=(1,2)$ and $(4,3)$ are in fact unique. Thus, when $q=5$ and $n=3$, we observe that in some sense the PFNT property "only just" holds.

In the case when $q\equiv 1\,(\mathrm{mod}\ 3)$, we search through E explicitly for elements with the required properties. The following lemma lets us reduce the number of pairs (a,b) that must be tested from $(q-1)\phi(q-1)$ to $\frac{1}{3}(q-1)\phi(q-1)$. □

Lemma 6.2. *Let $q\equiv 1\,(\mathrm{mod}\ 3)$, and set $k:=\frac{q-1}{3}$. Suppose that there exist free, primitive $\alpha\in E$ such that $\mathrm{Tr}_{E/F}(\alpha)=a$ and $N_{E/F}(\alpha)=b$, for all pairs (a,b) where b is a primitive element of F and $a\in\{1,\beta,\beta^2,\cdots,\beta^{k-1}:$ β a fixed primitive element of $F\}$. Then there exist free, primitive $\alpha\in E$ such that $\mathrm{Tr}_{E/F}(\alpha)=a$ and $N_{E/F}(\alpha)=b$, for all pairs (a,b) where a is a nonzero element of F and b is a primitive element of F.*

Proof. Fix a primitive element β of F. Observe that F^* may be partitioned into k cosets of the subgroup $H:=\{1,\beta^k,\beta^{2k}\}$ of cube roots of unity, namely $H,\beta H,\ldots,\beta^2H,\ldots,\beta^{k-1}H$. The result follows since $\mathrm{Tr}_{E/F}(h\gamma)=h\,\mathrm{Tr}_{E/F}(\gamma)$, $N(h\gamma)=h^3N_{E/F}(\gamma)$ for all $\gamma\in E$, $h\in F$.

Without exception, for all $q\equiv 1\,(\mathrm{mod}\ 3)$ remaining from the previous section, $(q,3)$ is found to be a PFNT pair.

In closing we remark that, for each of the larger values of q amongst the set of exceptions, the computations to check all the possibilities took several hours to run. (In the case of $q=256$, the original computation time of several weeks was reduced to a few hours by reprogramming.) This vindicates the efforts we have made to solve the problem theoretically in as many cases as possible. □

References

[Ca1] L. Carlitz, *Primitive roots in a finite field*, Trans. Amer. Math. Soc. **73** (1952), 373-382. MR **14:**539a

[Ca2] L. Carlitz, *Some problems involving primitive roots in a finite field*, Proc. Nat. Acad. Sci. U.S.A. **38** (1952), 314-318, 618. MR **14:**250f

[Co] S. D. Cohen, *Gauss sums and a sieve for generators of Galois fields*, Publ. Math. Debrecen **56** (2000), 293-312. MR **2001e:**11120

[CoHa1] S. D. Cohen and D. Hachenberger, *Primitive normal bases with prescribed trace*, Appl. Algebra Engrg. Comm. Comp. **9** (1999), 383-403. MR **2000c:**11198

[CoHa2] S. D. Cohen and D. Hachenberger, *Primitivity, freeness, norm and trace*, Discrete Math. **214** (2000), 135-144. MR **2000j:**11190

[CoHu1] S. D. Cohen and S. Huczynska, *The primitive normal basis theorem — without a computer*, J. London Math. Soc. **67** (2003), 41-56.

[CoHu2] S. D. Cohen and S. Huczynska, *Primitive free quartics with specified norm and trace*, Acta Arith. (to appear).

[Da] H. Davenport, *Bases for finite fields*, J. London Math. Soc. **43** (1968), 21-49. MR **37:**2729

[Ka] N. M. Katz, *Estimates for Soto-Andrade sums*, J. reine angew. Math. **438** (1993), 143-161. MR **94h:**11109

[LeSc] H. W. Lenstra, Jr. and R. J. Schoof, *Primitive normal bases for finite fields*, Math. Comp. **48** (1987), 217-231. MR **88c:**11076

[LiNi] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, Massachusetts, (1983); *2nd edition*: Cambridge University Press, Cambridge (1997). MR **97i:**11115

Department of Mathematics, University of Glasgow, Glasgow G12 8QW, Scotland

Current address: School of Informatics, University of Edinburgh, Edinburgh EH8 9LE, Scotland

E-mail address: shuczyns@inf.ed.ac.uk

Department of Mathematics, University of Glasgow, Glasgow G12 8QW, Scotland

E-mail address: sdc@maths.gla.ac.uk