

EXISTENCE OF PRIMITIVE POLYNOMIALS WITH THREE COEFFICIENTS PRESCRIBED

DONALD MILLS

ABSTRACT. Let \mathbf{F}_q denote the finite field of q elements, $q = p^r$ a prime power, and set $f(x) = \sum_{i=0}^n f_i x^{n-i} \in \mathbf{F}_q[x]$, with $f_0 = 1$. The question of whether, given $(f_1, f_2, \dots, f_k) \in \mathbf{F}_q^k$ there exists a coefficient vector $(f_{k+1}, f_{k+2}, \dots, f_n) \in \mathbf{F}_q^{n-k}$ such that $f(x)$ is a primitive polynomial of degree n over \mathbf{F}_q has been the subject of interest in recent years by several authors, including Cohen, Jungnickel, and Vanstone for the case $k = 1$ and arbitrary q , and Cohen, Han, and the author for $k = 2$ and odd q . In this paper, we prove that, for any 3-tuple $(f_1, f_2, f_3) \in \mathbf{F}_q^3$, where the characteristic of \mathbf{F}_q is at least 5, $n = 7$ and $q > 361$, there exists a 4-tuple $(f_4, f_5, f_6, f_7) \in \mathbf{F}_q^4$ such that $f(x)$ is a primitive polynomial of degree 7 over \mathbf{F}_q . The proof is accomplished via a character sum analysis that uses a recursive formula involving the trace function for f_1, f_2 and f_3 , followed by the application of a general combinatorial sieve. Although a recent paper of Fan and Han resolves the issue for $n \geq 8$, their methods do not allow for an examination of the $n = 7$ case, whereas our methods do.

AMS 2000 Subject Classification: Primary - 11T06; Secondary - 11T71

Keywords: finite field, primitive polynomial, coefficient

1. INTRODUCTION

Let \mathbf{F}_q denote the finite field of q elements, $q = p^r$ for prime p and positive integer r . A monic polynomial $f(x) = x^n + \sum_{i=1}^n f_i x^{n-i} \in \mathbf{F}_q[x]$ is called a *primitive polynomial* if it is irreducible over \mathbf{F}_q and any of the roots of f can be used to generate the multiplicative group $\mathbf{F}_{q^n}^*$ of \mathbf{F}_{q^n} . Equivalently, f is primitive if the smallest positive integer w such that $f(x) \mid x^w - 1$ is $w = q^n - 1$. Primitive polynomials and their roots are of interest in various applications of finite fields to coding theory and cryptography, and so it is of interest to know whether for a given q and n there exists a primitive polynomial of degree n over \mathbf{F}_q which may satisfy certain additional conditions. One such question is whether there exists a primitive polynomial of degree n over \mathbf{F}_q with first coefficient f_1 prescribed, where we note that $f_1 = -Tr(\alpha)$, α a root of f and Tr the trace function from \mathbf{F}_{q^n} to \mathbf{F}_q . This question has been answered (see [2], [7]), with answer as given in Theorem 1.1.

Date: June 6, 2003.

The author, at the time he began this project, was a Davies Fellow for the National Research Council. He wishes to thank the NRC, and specifically the U.S. Army Research Laboratory and the U.S. Military Academy, for the use of their facilities.

Theorem 1.1. *Let $n > 1$ be an integer, and let $a \in \mathbf{F}_q$ be given. Then there always exists a primitive polynomial $f(x) = x^n + \sum_{i=1}^n f_i x^{n-i} \in \mathbf{F}_q[x]$ such that $a = f_1$ provided $(a, n) \neq (0, 3)$ for $q = 4$ and $(a, n) \neq (0, 2)$ for arbitrary q .*

Cohen, Han and Mills considered the case in which there exists a primitive polynomial with f_1 and f_2 prescribed. Han [6] gave the following; this result was also addressed in [4].

Theorem 1.2. *Let $n \geq 7$ be an integer, and let $f_1, f_2 \in \mathbf{F}_q$ be given, q an odd prime power. Then there always exists a primitive polynomial $f(x) \in \mathbf{F}_q[x]$ of the form $f(x) = x^n + \sum_{i=1}^n f_i x^{n-i}$.*

Equivalently, $N_{q,n}(a, b) > 0$ for all odd prime powers q and all integers $n \geq 7$, where $N_{q,n}(a, b)$ is the number of primitive polynomials in \mathbf{F}_q of degree n with root α such that $Tr(\alpha) = a$ and $Tr(\alpha^2) = b$, Tr the trace function from \mathbf{F}_{q^n} to \mathbf{F}_q . The case where $q = 2^i$ for some i is more difficult; a discussion of this case is provided in [12].

From Theorem 1.2, we infer that the remaining cases of interest are $n = 4, 5$, and 6. Using sieving techniques, Cohen and Mills [4] proved the following, with q an odd prime power.

Theorem 1.3. *For all pairs $a, b \in \mathbf{F}_q$, q odd, $N_{q,n}(a, b) > 0$ for $n = 5, 6$.*

Using the methods mentioned above, as one increases the number of prescribed coefficients, one is forced to exclude more finite fields whose characteristic is small. As we shall see in this paper, use of such methods when three coefficients are prescribed forces us to exclude finite fields of characteristic either two or three. A recent paper by Fan and Han [5] which uses p -adic methods appears to resolve this problem, as they are able to determine the existence of primitive polynomials with the first three coefficients prescribed, regardless of the field's characteristic. However, they are able to answer this question only for polynomials of degree at least eight; the method used in this paper will address the degree seven case, albeit only for fields of characteristic at least five.

The outline of the paper is as follows. In Section 2, we give a formula, over finite fields of suitably large characteristic, for the k th coefficient of an irreducible polynomial. This formula is a direct consequence of Newton's identities. We then use this formula to address the question of the existence of primitive polynomials with three coefficients prescribed over finite fields of characteristic at least five. The main result of the paper is that, for all finite fields \mathbf{F}_q of characteristic at least five with $q > 361$, for every triplet $(f_1, f_2, f_3) \in \mathbf{F}_q^3$ there exists a primitive polynomial of degree $n = 7$ with x^{n-i} coefficient equal to f_i for $i = 1, 2, 3$.

2. A RECURSIVE FORMULA FOR THE k TH COEFFICIENT OF A POLYNOMIAL

Let the irreducible polynomial $f(x) = x^n + \sum_{i=1}^n (-1)^i f_i x^{n-i} \in \mathbf{F}_q[x]$ be given, and let α denote a root of f . Clearly, $f_1 = Tr(\alpha)$, while for odd-characteristic fields, we have, with $f_0 = 1$ (see [4] and [6])

$$\begin{aligned}
 f_2 &= \frac{1}{2} (f_1 \text{Tr}(\alpha) - f_0 \text{Tr}(\alpha^2)) \\
 (1) \qquad &= \frac{1}{2} (\text{Tr}^2(\alpha) - \text{Tr}(\alpha^2)).
 \end{aligned}$$

Moreover, a straightforward argument shows that, for fields of characteristic at least five, we have

$$(2) \qquad f_3 = \frac{1}{3} (f_2 \text{Tr}(\alpha) - f_1 \text{Tr}(\alpha^2) + f_0 \text{Tr}(\alpha^3)),$$

and using Newton's identities (which are obtained using symmetric polynomials – see also [11]) we have, when the characteristic p does not divide k ,

$$(3) \qquad f_k = \frac{1}{k} (f_{k-1} \text{Tr}(\alpha) - f_{k-2} \text{Tr}(\alpha^2) + \cdots + (-1)^{k-1} \text{Tr}(\alpha^k)).$$

Clearly, in order to consider the case in which f_1 , f_2 , and f_3 are prescribed, we will need $p \geq 5$. The character sum analysis will show that we need to restrict k such that $k \leq \lfloor \frac{n}{2} \rfloor$.

3. CHARACTER SUM ANALYSIS

To guarantee the existence of primitive polynomials over a finite field \mathbf{F}_q with f_1 , f_2 , and f_3 prescribed, we will employ a character sum analysis followed by, for $n = 7$, a combinatorial sieve due to Cohen (see [1]).

We first give a definition. An element $x \in \mathbf{F}_q$ is said to be *e-free* (it has also been referred to as “no kind of e th power”; see for example [3]) if, for any $y \in \mathbf{F}_q$ with $y^d = x$ for $d \mid e$, we must have $d = 1$. Thus the primitive elements of \mathbf{F}_q are those which are $(q-1)$ -free, while (trivially) all elements of the field are 1-free.

Now let e denote a divisor of $q^n - 1$, where q , n , and $a, b, c \in \mathbf{F}_q$ are given, and let $N(e)$ denote the number of elements $x \in \mathbf{F}_{q^n}$ that are e -free, with $\text{Tr}(x) = a$, $\text{Tr}(x^2) = b$, and $\text{Tr}(x^3) = c$. Further let $\omega(z)$ denote the number of prime divisors of z . We have the following basic lemmas (see [9]).

Lemma 3.1. *For $\xi \in \mathbf{F}_{q^n}^*$, we have*

$$(4) \qquad \frac{\varphi(e)}{e} \sum_{d \mid e} \frac{\mu(d)}{\varphi(d)} \sum_{\chi_d} \chi^{(d)}(\xi),$$

which equals 1 if ξ is not any kind of e th power, and equals zero otherwise. Here φ and μ are the Euler-phi and Möbius functions, respectively, and the inner sum runs over all d th-order multiplicative characters of \mathbf{F}_{q^n} .

Lemma 3.2. *For $\xi \in \mathbf{F}_q$ and ψ_t an additive character of \mathbf{F}_q for $t \in \mathbf{F}_q$, we have*

$$(5) \qquad \sum_{t \in \mathbf{F}_q} \psi_t(\xi) = q$$

if $\xi = 0$, where the sum runs over all q additive characters ψ_t of \mathbf{F}_q . The sum equals zero otherwise.

Using these lemmas, we may write $N(e)$ as

$$(6) \quad q^3 N(e) = \theta(e) \sum_{d|e} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \sum_{e_1, e_2, e_3 \in \mathbf{F}_q} S_{d, e_1, e_2, e_3}$$

where

$$(7) \quad S_{d, e_1, e_2, e_3} = \sum_{\xi \in \mathbf{F}_{q^n}^*} \psi(Tr(e_1 \xi + e_2 \xi^2 + e_3 \xi^3) - e_1 a - e_2 b - e_3 c) \chi^{(d)}(\xi).$$

Here $\chi^{(d)}$ runs over all d th-order multiplicative characters of \mathbf{F}_{q^n} , ψ is the canonical \mathbf{F}_q -additive character, $\theta(e) = \varphi(e)/e$, and Tr is the trace map from \mathbf{F}_{q^n} to \mathbf{F}_q .

Observe that when $e = q^n - 1$, $N := N(q^n - 1)$ (or, in keeping with the notation in [4], one can say $N := N_{q,n}(a, b, c)$) is the value whose positivity we wish to determine; note as well that the value of $N(e)$ depends only on the distinct prime factors of e . With these observations in hand, we say that divisors e_1, \dots, e_r , $r \geq 1$, of e are *complementary divisors of e with common divisor d* if the set of distinct prime divisors of $\text{lcm}\{e_1, \dots, e_r\}$ is the same as that of e , and, for any pair (i, j) with $1 \leq i \neq j \leq r$, the set of distinct prime divisors of $\text{gcd}(e_i, e_j)$ is that of d . When $r = 1$, we have $e_1 = d = e$.

With these notions in hand, we arrive at the following sieve inequality (see [1] for a proof).

Theorem 3.3. *Let q be a prime power and $n \geq 1$ an integer. Let e_1, \dots, e_r , $r \geq 1$ be complementary divisors of $e \mid q^n - 1$ with common divisor d . Then, with $N(e)$ defined as above, we have*

$$(8) \quad N(e) \geq \left[\sum_{i=1}^r N(e_i) \right] - (r-1)N(d).$$

Thus it suffices to guarantee

$$(9) \quad \left[\sum_{i=1}^r N(e_i) \right] - (r-1)N(d) > 0.$$

Before using the sieve, we must obtain bounds for N , depending upon the values of a , b , and c . First, we note that the following lemma will prove useful [10].

Lemma 3.4. *Let χ denote a d th order multiplicative character and ψ an additive character of \mathbf{F}_q . Let $f(x), g(x) \in \mathbf{F}_q[x]$ be polynomials of degree m, r respectively. If $\text{gcd}(m, d) = \text{gcd}(r, q) = 1$, then*

$$\left| \sum_{c \in \mathbf{F}_q} \chi(f(c))\psi(g(c)) \right| \leq (m+r-1)\sqrt{q}.$$

Of course, $S_{1,0,0,0} = q^n - 1$. We have the following.

Theorem 3.5. *We have*

$$(10) \quad q^3 N \geq \theta(q^n - 1) \{q^n - 1 + T_1 - \sum_{i=2}^8 |T_i|\},$$

where the T_i , $i = 1, \dots, 8$ are defined below.

Proof. Our work is separated into the following cases, based upon the values of d and the e_j :

- (1) $d = 1$, $e_j = 0$ for all j (addressed above).
- (2) $d = 1$, $e_j \neq 0$ for exactly one i .
- (3) $d = 1$, $e_j \neq 0$ for exactly two i .
- (4) $d = 1$, $e_1 e_2 e_3 \neq 0$.
- (5) $d > 1$, distinguishing as to whether $d \mid Q := \frac{q^n - 1}{q - 1}$.

For Case 2, we have the following subcases.

(2a) $e_1 \neq 0$. The sum to consider is

$$\begin{aligned} T_1 &= \sum_{e_1 \in \mathbf{F}_q^*} \sum_{\xi \in \mathbf{F}_{q^n}^*} \psi(\text{Tr}(e_1 \xi) - e_1 a) \\ &= \sum_{e_1 \in \mathbf{F}_q^*} \psi(-e_1 a) \left[\sum_{\xi \in \mathbf{F}_{q^n}} \psi(\text{Tr}(\xi)) - 1 \right]. \end{aligned}$$

Thus,

$$T_1 = \begin{cases} 1 - q & \text{if } a = 0 \\ 1 & \text{if } a \neq 0. \end{cases}$$

(2b) $e_2 \neq 0$. The sum to consider is

$$T_2 = \sum_{e_2 \in \mathbf{F}_q^*} S_{1,0,e_2,0} = \sum_{e_2 \in \mathbf{F}_q^*} \sum_{\xi \in \mathbf{F}_{q^n}^*} \psi(\text{Tr}(e_2 \xi^2) - e_2 b).$$

From [6], we have

$$|T_2| \leq \begin{cases} (q-1)(\sqrt{q^n}+1) & \text{if } b = 0 \\ (\sqrt{q}+1)(\sqrt{q^n}+1) & \text{if } b \neq 0. \end{cases}$$

(2c) $e_3 \neq 0$. We consider

$$T_3 = \sum_{e_3 \in \mathbf{F}_q^*} \sum_{\xi \in \mathbf{F}_{q^n}^*} \psi(\text{Tr}(e_3 \xi^3) - e_3 c) = \sum_{e_3 \in \mathbf{F}_q^*} \psi(-e_3 c) \sum_{\xi \in \mathbf{F}_{q^n}^*} \lambda(e_3 \xi^3),$$

where $\lambda(X) = \psi(\text{Tr}(X))$ for all $X \in \mathbf{F}_{q^n}$. We divide the work here into two subcases.

(2c1) $q \equiv 2 \pmod{3}$. Thus $\gcd(3, q-1) = 1$, and so we may write T_3 as

$$\begin{aligned} T_3 &= \sum_{e_3 \in \mathbf{F}_q^*} \psi(-e_3 c) \sum_{\xi \in \mathbf{F}_{q^n}^*} \lambda(e_3 \xi^3) \\ &= \sum_{e_3 \in \mathbf{F}_q^*} \psi(-e_3^3 c) \sum_{\xi \in \mathbf{F}_{q^n}^*} \lambda((e_3 \xi)^3) \\ &= \sum_{e_3 \in \mathbf{F}_q^*} \psi(-e_3^3 c) \sum_{\xi \in \mathbf{F}_{q^n}^*} \lambda(\xi^3) \end{aligned}$$

Thus, by the Weil bound [9] we have

$$|T_3| \leq \begin{cases} (q-1)(2\sqrt{q^n}+1) & \text{if } c = 0 \\ (2\sqrt{q}+1)(2\sqrt{q^n}+1) & \text{if } c \neq 0. \end{cases}$$

(2c2) $q \equiv 1 \pmod{3}$. Let α denote a fixed cubic nonresidue in \mathbf{F}_q^* , and let C denote the set of cubic residues in \mathbf{F}_q . Observe that $C \cup C\alpha \cup C\alpha^2 = \mathbf{F}_q^*$. We have

$$\begin{aligned} T_3 &= \frac{1}{3} \left(\sum_{i=0}^2 \sum_{e_3 \in \mathbf{F}_q^*} \sum_{\xi \in \mathbf{F}_{q^n}^*} \psi(\text{Tr}(e_3^3 \alpha^i \xi^3) - e_3^3 \alpha^i c) \right) \\ &= \frac{1}{3} \left(\sum_{i=0}^2 \sum_{e_3 \in \mathbf{F}_q^*} \psi(-e_3^3 \alpha^i c) \sum_{\xi \in \mathbf{F}_{q^n}^*} \lambda(\alpha^i \xi^3) \right). \end{aligned}$$

Thus, we again have

$$|T_3| \leq \begin{cases} (q-1)(2\sqrt{q^n}+1) & \text{if } c = 0 \\ (2\sqrt{q}+1)(2\sqrt{q^n}+1) & \text{if } c \neq 0. \end{cases}$$

For Case 3, we also have three subcases to address.

(3a) $e_1e_2 \neq 0$. The sum in question is

$$T_4 = \sum_{e_1, e_2 \in \mathbf{F}_q^*} \sum_{\xi \in \mathbf{F}_{q^n}^*} \psi(\text{Tr}(e_1\xi + e_2\xi^2) - e_1a - e_2b),$$

whose modulus is bounded from above by (see [6])

$$|T_4| \leq \begin{cases} (q-1)^2(\sqrt{q^n} + 1) & \text{if } a = b = 0 \\ (q-1)(\sqrt{q^n} + 1) & \text{if } a \neq 0, b = 0 \\ (q-1)(\sqrt{q} + 1)(\sqrt{q^n} + 1) & \text{if } b \neq 0. \end{cases}$$

(3b) $e_1e_3 \neq 0$. We consider

$$\begin{aligned} T_5 &= \sum_{e_1, e_3 \in \mathbf{F}_q^*} \sum_{\xi \in \mathbf{F}_{q^n}^*} \psi(\text{Tr}(e_1\xi + e_3\xi^3) - e_1a - e_3c) \\ &= \sum_{e, e_1 \in \mathbf{F}_q^*} \sum_{\xi \in \mathbf{F}_{q^n}^*} \psi(\text{Tr}(e_1\xi + e(e_1\xi)^3) - e_1a - ee_1^3c) \\ &= \sum_{e \in \mathbf{F}_q^*} \sum_{\xi \in \mathbf{F}_{q^n}^*} \lambda(\xi + e\xi^3) \sum_{e_1 \in \mathbf{F}_q^*} \psi(-e_1a - ee_1^3c) \end{aligned}$$

where $ee_1^3 = e_3$ and λ has the same meaning as above. Thus

$$|T_5| \leq \begin{cases} (q-1)^2(2\sqrt{q^n} + 1) & \text{if } a = c = 0 \\ (q-1)(2\sqrt{q^n} + 1) & \text{if } a \neq 0, c = 0 \\ (q-1)(2\sqrt{q} + 1)(2\sqrt{q^n} + 1) & \text{if } c \neq 0. \end{cases}$$

(3c) $e_2e_3 \neq 0$. We consider the sum

$$T_6 = \sum_{e_2, e_3 \in \mathbf{F}_q^*} \sum_{\xi \in \mathbf{F}_{q^n}^*} \psi(\text{Tr}(e_2\xi^2 + e_3\xi^3) - e_2b - e_3c).$$

Using similar arguments to that above (see the expanded version of this paper, available at the Mathematics ArXiv, <http://front.math.ucdavis.edu/>, for more detailed arguments), we have

$$|T_6| \leq \begin{cases} (q-1)^2(2\sqrt{q^n} + 1) & \text{if } b = c = 0 \\ (q-1)(\sqrt{q} + 1)(2\sqrt{q^n} + 1) & \text{if } b \neq 0, c = 0 \\ (q-1)(2\sqrt{q} + 1)(2\sqrt{q^n} + 1) & \text{if } c \neq 0. \end{cases}$$

(4) $e_1e_2e_3 \neq 0$. We have

$$T_7 = \sum_{e_1, e_2, e_3 \in \mathbf{F}_q^*} \sum_{\xi \in \mathbf{F}_{q^n}^*} \psi(\text{Tr}(e_1\xi + e_2\xi^2 + e_3\xi^3) - e_1a - e_2b - e_3c).$$

Again employing similar arguments, we have

$$|T_7| \leq \begin{cases} (q-1)^3(2\sqrt{q^n}+1) & \text{if } a = b = c = 0 \\ (q-1)^2(2\sqrt{q^n}+1) & \text{if } a \neq 0, b = c = 0 \\ (q-1)^2(\sqrt{q}+1)(2\sqrt{q^n}+1) & \text{if } b \neq 0, c = 0 \\ (q-1)^2(2\sqrt{q}+1)(2\sqrt{q^n}+1) & \text{if } c \neq 0. \end{cases}$$

(5) $d > 1$. Here we use the fact that the \mathbf{F}_{q^n} -multiplicative character $\chi^{(d)}$, applied to \mathbf{F}_q , is trivial iff $d \mid Q$. The sum to consider is

$$(11) \quad T_8 = \sum_{1 < d \mid q^n - 1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \sum_{e_1, e_2, e_3 \in \mathbf{F}_q} S_{d, e_1, e_2, e_3}.$$

One considers (11) according to the values of the e_i 's, specifically as to whether a certain $e_i = 0$. We shall separate our results according to whether $d \mid Q$. Note that $S_{d, 0, 0, 0} = 0$. Proceeding in the same manner as above, we have (with α a quadratic nonresidue of \mathbf{F}_q in (13), and $ee_1^2 = e_2$ in (14))

$$(12) \quad \sum_{e_1 \in \mathbf{F}_q^*} S_{d, e_1, 0, 0} = \sum_{e_1 \in \mathbf{F}_q^*} \chi^{(d)}(e_1^{-1}) \psi(-(e_1 - 1)a) S_{d, 1, 0, 0},$$

$$(13) \quad \sum_{e_2 \in \mathbf{F}_q^*} S_{d, 0, e_2, 0} = \frac{1}{2} \left(\sum_{i=0}^1 \sum_{e_2 \in \mathbf{F}_q^*} \chi^{(d)}(e_2^{-1}) \psi(-(e_2^2 - 1)\alpha^i b) S_{d, 0, \alpha^i, 0} \right),$$

and

$$(14) \quad \sum_{e_1, e_2 \in \mathbf{F}_q^*} S_{d, e_1, e_2, 0} = \sum_{e, e_1 \in \mathbf{F}_q^*} \chi^{(d)}(e_1^{-1}) \psi(-(e_1 - 1)a - (e_1^2 - 1)eb) S_{d, 1, e, 0}.$$

Further, we have

$$(15) \quad \sum_{e_3 \in \mathbf{F}_q^*} S_{d, 0, 0, e_3} = \sum_{e_3 \in \mathbf{F}_q^*} \chi^{(d)}(e_3^{-1}) \psi(-(e_3^3 - 1)c) S_{d, 0, 0, 1}$$

for $q \equiv 2 \pmod{3}$, while, with $q \equiv 1 \pmod{3}$ and α a fixed cubic nonresidue in \mathbf{F}_q , we have

$$(16) \quad \sum_{e_3 \in \mathbf{F}_q^*} S_{d,0,0,e_3} = \frac{1}{3} \left(\sum_{i=0}^2 \sum_{e_3 \in \mathbf{F}_q^*} \chi^{(d)}(e_3^{-1}) \psi(-(e_3^3 - 1)\alpha^i c) S_{d,0,0,\alpha^i} \right).$$

With $ee_1^3 = e_3$, we have

$$(17) \quad \sum_{e_1, e_3 \in \mathbf{F}_q^*} S_{d,e_1,0,e_3} = \sum_{e, e_1 \in \mathbf{F}_q^*} \chi^{(d)}(e_1^{-1}) \psi(-(e_1 - 1)a - (e_1^3 - 1)ec) S_{d,1,0,e},$$

while, with α a fixed quadratic nonresidue in \mathbf{F}_q and $ee_2^3 = e_3$, we have

$$(18) \quad \sum_{e_2, e_3 \in \mathbf{F}_q^*} S_{d,0,e_2,e_3} = \frac{1}{2} \left(\sum_{i=0}^1 \sum_{e, e_2 \in \mathbf{F}_q^*} \chi^{(d)}(e_2^{-1}) U(e, e_2, \alpha^i) S_{d,0,\alpha^i,e} \right),$$

where $U(e, e_2, \alpha^i) = \psi(-(e_2^2 - 1)\alpha^i b - (e_2^3 - 1)ec)$. Finally, with $ee_1^2 = e_2$ and $ge_1^3 = e_3$, we have

$$(19) \quad \sum_{e_1, e_2, e_3 \in \mathbf{F}_q^*} S_{d,e_1,e_2,e_3} = \sum_{e_1, e, g \in \mathbf{F}_q^*} \chi^{(d)}(e_1^{-1}) V(e_1, e, g) S_{d,1,e,g},$$

where $V(e_1, e, g) = \psi(-(e_1 - 1)a - (e_1^2 - 1)eb - (e_1^3 - 1)gc)$.

Putting it all together, one can obtain bounds for $|T_8|$, depending upon the values of a , b , and c . For brevity's sake, we shall limit our exposition to the cases $a = b = c = 0$, $a \neq 0$ with $b = c = 0$, and $abc \neq 0$, as the other cases are approached similarly.

For $a = b = c = 0$, we have

$$(20) \quad |T_8| \leq (2^{\omega(Q)} - 1)[(q - 1)(3q^2 + 2q + 1)]\sqrt{q^n}.$$

For $a \neq 0$, $b = c = 0$ we have

$$(21) \quad \begin{aligned} |T_8| &\leq (2^{\omega(Q)} - 1)[1 + 10(q - 1) + 6(q - 1)^2]\sqrt{q^n} \\ &+ (2^{\omega(q^n - 1)} - 2^{\omega(Q)})[1 + 5(q - 1) + 3(q - 1)^2]\sqrt{q^{n+1}}, \end{aligned}$$

while for $abc \neq 0$ we have

$$(22) \quad \begin{aligned} |T_8| &\leq (2^{\omega(Q)} - 1)[8\sqrt{q} + 6 + (14\sqrt{q} + 8)(q - 1) + (6\sqrt{q} + 3)(q - 1)^2]\sqrt{q^n} \\ &+ (2^{\omega(q^n - 1)} - 2^{\omega(Q)})[14 + 22(q - 1) + 9(q - 1)^2]\sqrt{q^{n+1}}. \end{aligned}$$

Putting this all together, we obtain (10). This completes the proof. \square

This completes the main portion of our character sum analysis. Starting with the next section, we use a sieving process to resolve, as best we can, the case $n = 7$.

4. SIEVE INEQUALITIES FOR THE THREE-COEFFICIENT PROBLEM

We will use (9), in conjunction with the bounds given for N , to come close to a resolution of the primitive polynomial problem for $n = 7$ with characteristic at least 5.

We first consider the case $a = b = c = 0$. Note here that, based upon our work in bounding $N_{q,n}(0, 0, 0)$, and in reference to (9), we only need to work with divisors of Q . In particular, note that for a divisor m of Q we have

$$(23) \quad q^3 N(m) \geq \theta(m) \{q^n - P(q, n) - (2^{\omega(m)} - 1)R(q, n)\}$$

where $\theta(m) = \varphi(m)/m$,

$$(24) \quad \begin{aligned} P(q, n) &= q + (q-1)(3\sqrt{q^n} + 2) \\ &+ (q-1)^2(5\sqrt{q^n} + 3) + (q-1)^3(2\sqrt{q^n} + 1), \end{aligned}$$

and

$$(25) \quad R(q, n) = (q-1)(3q^2 + 2q + 1)\sqrt{q^n}.$$

Observe first that

$$(26) \quad \begin{aligned} R(q, n) &= 3q^{\frac{n+6}{2}} - q^{\frac{n+4}{2}} - q^{\frac{n+2}{2}} - q^{\frac{n}{2}} \\ &< 3q^{\frac{n+6}{2}}. \end{aligned}$$

Further, after some arithmetic we find that

$$(27) \quad \begin{aligned} P(q, n) &= 2q^{\frac{n+6}{2}} - q^{\frac{n+4}{2}} - q^{\frac{n+2}{2}} + q^3 \\ &< 2q^{\frac{n+6}{2}} \end{aligned}$$

for all prime powers q with $n \geq 7$. Thus,

$$(28) \quad q^3 N(m) > \theta(m) \{q^n - q^{\frac{n+6}{2}}(3 \times 2^{\omega(m)} - 1)\}.$$

In particular, for a set of complementary divisors e_1, \dots, e_r with common divisor d , we have

$$(29) \quad \frac{q^3 N(d)\theta}{\theta(d)} > \theta \{q^n - q^{\frac{n+6}{2}}(3 \times 2^{\omega(d)} - 1)\}$$

where $\theta := -(r-1)\theta(d) + \sum_{i=1}^r \theta(e_i)$. Here we need $\theta > 0$. Now write (9) as

$$(30) \quad \sum_{i=1}^r \left[N(e_i) - \frac{\theta(e_i)}{\theta(d)} N(d) \right] + \frac{\theta}{\theta(d)} N(d) > 0$$

and apply (29), as well as

$$(31) \quad q^3 \left| N(e_i) - \frac{\theta(e_i)}{\theta(d)} N(d) \right| \leq 3q^{\frac{n+6}{2}} \theta(e_i) (2^{\omega(e_i)} - 2^{\omega(d)})$$

for each i , where (31) follows from the estimates of the character sums given earlier, as applied to those divisors of e_i that are not involved in $N(d)$. Thus, using (29) and (31), we want

$$(32) \quad q^{\frac{n-6}{2}} > \frac{3 \sum_{i=1}^r \theta(e_i) (2^{\omega(e_i)} - 2^{\omega(d)})}{\theta} + 3 \times 2^{\omega(d)} - 1$$

in order to ensure that $N > 0$. If one chooses complementary divisors such that $2^{\omega(e_i)} - 2^{\omega(d)} = 2^{\omega(d)}$ for each i , (32) becomes

$$(33) \quad q^{\frac{n-6}{2}} > \frac{3 \times 2^{\omega(d)} (2\theta + (r-1)\theta(d))}{\theta} - 1.$$

We will use (32) and (33) for the case $n = 7$ and $a = b = c = 0$.

We obtain the sieve inequalities for $(a, b, c) \neq (0, 0, 0)$ in much the same way we obtained (32) and (33). First, we consider the case $a \neq 0, b = c = 0$. For m a divisor of $q^n - 1$, we have

$$(34) \quad q^3 N(m) \geq \theta(m) \{ q^n - P(q, n) - (2^{\omega(m)} - 1) R(q, n) \}$$

where

$$(35) \quad \begin{aligned} P(q, n) &= (6\sqrt{q^n} + 4)(q-1) + (4\sqrt{q^n} + 2)(q-1)^2 \\ &< 4q^{\frac{n+4}{2}}, \end{aligned}$$

$$(36) \quad \begin{aligned} R(q, n) &= [1 + 10(q-1) + 6(q-1)^2 + (1 + 5(q-1) + 3(q-1)^2)\sqrt{q}] \sqrt{q^n} \\ &\leq \frac{21}{4} q^{\frac{n+5}{2}} \end{aligned}$$

for $q \geq 5$, and we use $2^{\omega(m)} - 1$ in place of $2^{\omega(\gcd(m, Q))} - 1$ and $2^{\omega(m)} - 2^{\omega(\gcd(m, Q))}$. Arguing as we did for the all-zeros case, it is a straightforward matter to conclude that we want

$$(37) \quad q^{\frac{n-5}{2}} > \frac{21}{4} \left[\frac{\sum_{i=1}^r \theta(e_i) (2^{\omega(e_i)} - 2^{\omega(d)})}{\theta} + 2^{\omega(d)} - 1 \right] + \frac{4}{\sqrt{q}}$$

or, for a choice of complementary divisors such that $2^{\omega(e_i)} - 2^{\omega(d)} = 2^{\omega(d)}$ for each i ,

$$(38) \quad q^{\frac{n-5}{2}} > \frac{(5.25)2^{\omega(d)}(2\theta + (r-1)\theta(d))}{\theta} + \frac{4}{\sqrt{q}} - \frac{21}{4}.$$

As the inequalities for the other cases are obtained in like manner, we list only the final results below, with the proofs left to the reader. For each of these cases, only the general sieve inequality is given, as the sieve inequality produced for the situation in which $2^{\omega(e_i)} - 2^{\omega(d)} = 2^{\omega(d)}$ for each i is easily obtained from the general expression.

For $b \neq 0$, $a = c = 0$ we want

$$(39) \quad q^{\frac{n-5}{2}} > \left(9 + \frac{6}{\sqrt{q}}\right) \left[\frac{\sum_{i=1}^r \theta(e_i)(2^{\omega(e_i)} - 2^{\omega(d)})}{\theta} + 2^{\omega(d)} - 1 \right] + 2 + \frac{4}{\sqrt{q}}.$$

For $c \neq 0$, $a = b = 0$ we want

$$(40) \quad q^{\frac{n-5}{2}} > \left(15 + \frac{5}{\sqrt{q}}\right) \left[\frac{\sum_{i=1}^r \theta(e_i)(2^{\omega(e_i)} - 2^{\omega(d)})}{\theta} + 2^{\omega(d)} - 1 \right] + 4 + \frac{3}{\sqrt{q}}.$$

For $ab \neq 0$, $c = 0$ we want

$$(41) \quad q^{\frac{n-5}{2}} > \left(9 + \frac{4}{\sqrt{q}}\right) \left[\frac{\sum_{i=1}^r \theta(e_i)(2^{\omega(e_i)} - 2^{\omega(d)})}{\theta} + 2^{\omega(d)} - 1 \right] + 2 + \frac{3}{\sqrt{q}}.$$

For $ac \neq 0$, $b = 0$ we want

$$(42) \quad q^{\frac{n-5}{2}} > \left(15 + \frac{5}{\sqrt{q}}\right) \left[\frac{\sum_{i=1}^r \theta(e_i)(2^{\omega(e_i)} - 2^{\omega(d)})}{\theta} + 2^{\omega(d)} - 1 \right] + 4 + \frac{3}{\sqrt{q}}.$$

For $bc \neq 0$, $a = 0$ (and also for $abc \neq 0$) we want

$$(43) \quad q^{\frac{n-5}{2}} > \left(15 + \frac{19}{3\sqrt{q}}\right) \left[\frac{\sum_{i=1}^r \theta(e_i)(2^{\omega(e_i)} - 2^{\omega(d)})}{\theta} + 2^{\omega(d)} - 1 \right] + 4 + \frac{3}{\sqrt{q}}.$$

Of these inequalities, (43) is the most restrictive, and thus we shall use this inequality in the sections to follow.

5. THE PRIMITIVE POLYNOMIAL PROBLEM FOR SEVENTH-DEGREE POLYNOMIALS

We consider the all-zero case first. Observe first that prime p divides Q if and only if $p = 7$ or $p \equiv 1 \pmod{14}$. Using this, we can use Theorem 3.5 to determine that $N > 0$ for $\omega(Q) \geq 266$, where we note that the 266th such prime is $p = 13469$. Use of (32) dramatically improves this to $N > 0$ for $\omega(Q) \geq 10$, as Table 1 shows. In Table 1, we use $e_1 = d = 7$ for $\omega = 1$, while for $\omega \geq 2$, we use complementary divisors such that $2^{\omega(e_i)} - 2^{\omega(d)} = 2^{\omega(d)}$ for each i , and in particular we use $d = 1$ for these values of ω , as they produce better results than the method used for other values of n . That they produce better results is due to the fact that we are working with primes of a certain form, as opposed to having no restriction on which primes divide Q .

The list of possible exceptions is given in Table 2. The values $q = 67, 125, 131, 139, 223, 359, 389$ are eliminated via the sieve, with $d = 1$, while the primes less than $q = 127$ are eliminated via computer. This leaves us with the possible exceptions $q = 25, 49, 121, 169, 191, 197, 199, 239, 269$, a total of 9 possible exceptions.

$\omega(Q)$	q_0	square of RHS
1	1.00	25.00
2	2.19	74.77
3	4.34	156.39
4	9.06	270.94
5	20.13	418.39
6	45.35	601.04
7	109.63	816.53
8	267.73	1067.72
9	667.22	1354.61
10	1707.85	1676.92

TABLE 1. Sieving Table for Case $n = 7, a = b = c = 0$

5	7	11	13	17	19	23	25	29	37
41	43	47	49	53	59	67	71	79	97
103	107	109	113	121	125	127	131	139	169
191	197	199	223	239	269	359	389		

TABLE 2. Possible Exceptions for Case $n = 7, a = b = c = 0$

For the case $(a, b, c) \neq (0, 0, 0)$, one can use Theorem 3.5 to conclude that $N > 0$ for $\omega(q^7 - 1) \geq 100$. Use of (43) improves this to $N > 0$ for $\omega(q^7 - 1) \geq 21$, as shown in Table 3. In this table, we use $e_1 = d = 2$ for $\omega = \omega(q^7 - 1) = 1$, and $e_1 = d = 2$ and $e_2 = 6$ for $\omega = 2$. Further, for $\omega \geq 3$ we use complementary divisors such that $2^{\omega(e_i)} - 2^{\omega(d)} = 2^{\omega(d)}$. For $\omega = 3, d = 2$; for $4 \leq \omega \leq 12, d = 6$; and for $13 \leq \omega \leq 21, d = 30$. The 95 possible exceptions are listed in Table 4. The 42 values eliminated by the sieve with $d = 2$, with $2^{\omega(e_i)} - 2^{\omega(d)} = 2^{\omega(d)}$ for each i , are given in Table 5. The 38 primes in Table 4 less than or equal to 179 were eliminated via computer check, leaving 15 possible exceptions that range in value from $q = 25$ to $q = 361$.

We summarize with the following theorem and conjecture.

Theorem 5.1. $N_{q,7}(a, b, c) > 0$ for all $q > 361$ with $\text{char}(\mathbf{F}_q) \geq 5$.

Conjecture 5.2. $N_{q,7}(a, b, c) > 0$ for all q with $\text{char}(\mathbf{F}_q) \geq 5$.

Resolution of the remaining values is left to those whose computational resources are sufficient to the task.

$\omega(q^r - 1)$	q_0	RHS
1	1.17	27.63
2	1.32	68.15
3	1.63	151.74
4	2.15	258.90
5	3.02	399.61
6	4.36	573.90
7	6.54	777.08
8	9.96	1024.19
9	15.58	1312.77
10	25.21	1636.69
11	41.17	2027.87
12	68.97	2473.11
13	117.23	2934.03
14	200.63	3380.67
15	347.74	3866.04
16	613.17	4383.96
17	1097.89	4935.80
18	1975.19	5539.77
19	3601.44	6182.56
20	6621.27	6874.56
21	12221.66	7628.84

TABLE 3. Sieving Table for Case $n = 7$, $(a, b, c) \neq (0, 0, 0)$

5	7	11	13	17	19	23	25
29	31	37	41	43	47	49	53
59	61	67	71	73	79	83	89
97	101	103	107	109	113	121	125
127	131	137	139	149	151	157	167
169	173	179	181	191	193	197	199
211	223	227	229	233	239	241	257
263	269	271	277	281	283	293	307
311	313	317	331	337	343	359	361
367	373	379	389	397	401	409	431
439	463	491	499	509	529	547	571
613	625	661	691	727	919	953	

TABLE 4. Possible Exceptions for Case $n = 7$, $(a, b, c) \neq (0, 0, 0)$

6. SUMMARY

Using standard character sum arguments, the Cohen sieve, and computational resources, we have determined that for $q > 361$ with $\text{char}(\mathbf{F}_q) \geq 5$ and for any

197	227	229	233	239	263	269
271	277	281	283	293	307	311
313	317	337	343	359	367	373
379	389	397	401	409	431	439
463	491	499	509	529	547	571
613	625	661	691	727	919	953

TABLE 5. Values for Case $n = 7$, $(a, b, c) \neq (0, 0, 0)$ Eliminated via the Sieve

choice of elements $f_1, f_2, f_3 \in \mathbf{F}_q$, there exist $f_j \in \mathbf{F}_q$, $4 \leq j \leq 7$, such that $x^7 + f_1x^6 + f_2x^5 + f_3x^4 + f_4x^3 + f_5x^2 + f_6x + f_7 \in \mathbf{F}_q[x]$ is primitive. Although our method is characteristic-dependent, the estimates are better than those in [5] by a factor of \sqrt{q} . A combination of methods, one that is independent of the characteristic and which provides satisfactory estimates, would be quite welcome.

7. ACKNOWLEDGEMENTS

The author thanks Stephen Cohen of the University of Glasgow for his helpful comments. Additionally, the author gratefully acknowledges the very helpful advice offered by the anonymous referee.

REFERENCES

- [1] Chou, W.-S. and Cohen, S.D. "Primitive elements with zero traces." Dedicated to Professor Chao Ko on the occasion of his 90th birthday. *Finite Fields Appl.* **7** (2001), 125-141.
- [2] Cohen, S.D. "Primitive elements and polynomials with arbitrary trace." *Disc. Math.* **83** (1990), 1-7.
- [3] Cohen, S.D. "Kloosterman sums and primitive elements in Galois fields." *Acta Arith.* **94** (2000), no. 2, 173-201.
- [4] Cohen, S.D. and Mills, D. "Primitive elements with first and second coefficients prescribed." To appear in *Finite Fields Appl.*
- [5] Fan, S.-Q. and Han, W.-B. "Character sums over Galois rings and primitive polynomials over finite fields." To appear in *Finite Fields Appl.*
- [6] Han, W.-B. "Coefficients of primitive polynomials over finite fields." *Math. Comp.* **65** (1996), 331-340.
- [7] Jungnickel, D. and Vanstone, S.A. "On primitive polynomials over finite fields." *J. Algebra* **124** (1989), 337-353.
- [8] Koblitz, N. *A Course in Number Theory and Cryptography*. Springer-Verlag, New York, NY 1987.
- [9] Lidl, R. and Niederreiter, H. *Finite Fields*. Encyclo. Math and Appls. **20**, Addison-Wesley, Reading, Mass. 1983 (now distributed by Cambridge Univ. Press).
- [10] Moreno, O. "On the existence of a primitive quadratic of trace 1 over \mathbf{F}_{p^m} ." *J. Combin. Theory Ser. A* **51** (1989), no. 1, 104-110.
- [11] Ren, De-bin. "On the coefficients of primitive polynomials over finite fields." *Sichuan Daxue Xuebao* **38** (2001), no. 1, 33-36.
- [12] Sun, Q. and Han, W.B. "The absolute trace function and primitive roots in finite fields" (in Chinese). *Chinese Ann. Math. Ser. A* **11** (1990), 202-205.

DEPARTMENT OF MATHEMATICS, SOUTHERN ILLINOIS UNIVERSITY-CARBONDALE, CARBONDALE, IL 62901-4408

E-mail address: dmills@math.siu.edu