MATHEMATICS OF COMPUTATION
Volume 65, Number 213
January 1996, Pages 331–340

THE COEFFICIENTS OF PRIMITIVE POLYNOMIALS OVER FINITE FIELDS

WEN BAO HAN

ABSTRACT. For $n \geq 7$, we prove that there always exists a primitive polynomial of degree n over a finite field F_q (q odd) with the first and second coefficients prescribed in advance.

1. INTRODUCTION

Let F_q be a finite field with q elements, $q = p^l, l$ a positive integer and p a prime number. A monic polynomial $f(x) \in F_q[x]$ of degree n is called a primitive polynomial if the least positive integer e such that $f(x)|x^e - 1$ is $q^n - 1$. It is well known that $f(x)$ is irreducible over $F_q[x]$. If ξ is a root of $f(x)$ in F_{q^n}, then ξ is a primitive element of F_{q^n}, namely the generator of the multiplicative group $F_{q^n}^*$ of F_{q^n}. Davenport and Carlitz have studied the properties of primitive elements. Recently, because of the applications of finite fields in cryptography, coding theory, designing Costas arrays etc., various properties of primitive elements have been investigated again. Let $T(x) = x + x^q + \cdots + x^{q^{n-1}}$ be the trace from F_{q^n} to F_q. We have the following result.

Theorem A. *Let $n > 1$ be an integer, $a \in F_q$. Then there always exists a primitive element $\xi \in F_{q^n}$ such that $T(\xi) = a$ if $(a, n) \neq (0, 3)$ for $q = 4$ and $(a, n) \neq (0, 2)$ for q arbitrary.*

The theorem above was proved by Davenport [3] for $q = 2$ as a consequence of his existence theorem of normal bases, by Moreno [9] for $n = 2$, Sun and Han [11] for $q = p$, Jungnickel and Vanstone [6], Cohen [1] for general cases. In fact, Theorem A is equivalent to the following result.

Theorem B. *Let $a \in F_q$ and $n > 1$ be an integer. Then there always exists a primitive polynomial $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ over F_q such that $a_1 = a$ if $(a, n) \neq (0, 3)$ for $q = 4$ and $(a, n) \neq (0, 2)$ for q arbitrary.*

Later we always assume that the polynomial we consider is monic. Let $g(x) = x^m + b_1 x^{m-1} + \cdots + b_m \in F_q[x]$. We call b_i the ith coefficient of $f(x)$. Theorem B gives the distribution of the first coefficient of primitive polynomials. It is natural to consider the other coefficients of primitive polynomials. In [5], Hansen and Mullen conjectured that with the three nontrivial exceptions $(q, n, i, a) = (4, 3, 1, 0)$, $(4, 3, 2, 0)$, $(2, 4, 2, 1)$, there is a primitive polynomial of degree n with the ith coefficient prescribed $(0 < i < n)$. Further, in an excellent survey paper on primitive

Received by the editor January 12, 1994 and, in revised form, June 2, 1994 and December 5, 1994.

1991 *Mathematics Subject Classification.* Primary 11T06.

Key words and phrases. Finite field, primitive polynomial.

elements, Cohen [2] asked whether there is some function $c(n)$ so that there is one with $[c(n)]$ (the integer part of $c(n)$) coefficients prescribed. In this paper, we prove that if $n \geq 7$ and q is odd, there exists a primitive polynomial of degree n with the first and second coefficients prescribed; consequently Hansen and Mullen's conjecture holds for $i = 2$ and $n \geq 7$. By our method, it seems plausible that we can take $c(n)$ to be the least integer $< \frac{n}{2}$ although it is not easy to prove. The case of small characteristic is more difficult; see [11] for a discussion of the case $p = 2$.

2. Lemmas and estimates

First of all, we give a lemma from which the second coefficient of an irreducible polynomial can be represented by the traces of a root and the square of a root. Then Hansen and Mullen's conjecture reduces to the existence of primitive element solutions of some equation associated with the trace from F_{q^n} to F_q.

Lemma 1. *Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ be an irreducible polynomial over F_q, ξ be a root of $f(x)$ in F_{q^n}, q odd. Then $a_2 = \frac{1}{2}(T(\xi)^2 - T(\xi^2))$, where $T(x)$ is the trace from F_{q^n} to F_q.*

Proof. Since $f(x)$ is irreducible, $\xi, \xi^q, \ldots, \xi^{q^{n-1}}$ are all roots of $f(x)$ in F_{q^n}. Therefore,

$$f(x) = (x - \xi)(x - \xi^q) \cdots (x - \xi^{q^{n-1}})$$

and

$$\begin{aligned} a_2 &= \sum_{0 \leq i < j < n} \xi^{q^i} \xi^{q^j} \\ &= \tfrac{1}{2} \sum_{\substack{0 \leq i,j < n \\ i \neq j}} \xi^{q^i} \xi^{q^j} \\ &= \tfrac{1}{2} T(\xi^{1+q} + \xi^{1+q^2} + \cdots + \xi^{1+q^{n-1}}) \\ &= \tfrac{1}{2} T(\xi T(\xi) - \xi^2) \\ &= \tfrac{1}{2}(T(\xi)^2 - T(\xi^2)). \end{aligned}$$

By Lemma 1, the existence of primitive element solutions of the equation $T(x)^2 - T(x^2) = c$ for $c \in F_q$ yields the conjecture of Hansen and Mullen in the case of the second coefficient. But we prefer to consider the following system of equations to obtain a strong conclusion:

$$\begin{cases} T(x) = a, \\ T(x^2) = b, \end{cases} \tag{2.1}$$

where $a, b \in F_q$. If (2.1) has a primitive element solution ξ in F_{q^n}, let $f(x)$ be the minimal polynomial of ξ over F_q. Then the first and second coefficients of $f(x)$ are a and $\frac{1}{2}(a^2 - b)$. Furthermore, $f(x)$ is a primitive polynomial of degree n. Hence, there exists a primitive polynomial with the first coefficient a and second coefficient $\frac{1}{2}(a^2 - b)$. So we need to discuss the existence of the primitive element solutions of (2.1). For this reason, we review a few basic facts about the characters over finite fields. □

Lemma 2. *Let $\xi \in F_{q^n}^*$; then*

$$\sum_{d|q^n-1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \chi^{(d)}(\xi) = \begin{cases} \frac{q^n-1}{\varphi(q^n-1)} & \text{if } \xi \text{ is a primitive element of } F_{q^n}, \\ 0 & \text{otherwise,} \end{cases}$$

where $\mu(d)$ is a Möbius function, $\varphi(d)$ is Euler's function and $\chi^{(d)}$ runs through all dth order multiplicative characters of F_{q^n}.

Let Tr be the absolute trace from F_q to F_p. Then the mapping $\psi : x \to e^{2\pi i \operatorname{Tr}(x)/p}$ $(x \in F_q)$ is an additive character of F_q, called the canonical additive character. We define $\psi_a(x) = \psi(ax), a$ (fixed), $x \in F_q$. Then the ψ_a's $(a \in F_q)$ are all additive characters of F_q. We also observe that $\Psi_a(x) = \psi(aT(x))$ is an additive character of F_{q^n}.

Lemma 3. *Let $\xi \in F_q$. Then*

$$\sum_{a \in F_q} \psi_a(\xi) = \begin{cases} q & \text{if } \xi = 0, \\ 0 & \text{if } \xi \neq 0. \end{cases}$$

We still need an estimate on twisted exponential sums. Thanks to Weil, we have the following result.

Lemma 4 ([9])**.** *Let χ be a dth order multiplicative character and λ an additive character of F_q. Let $g(x), h(x) \in F_q[x], m = \deg g(x)$, $r = \deg h(x)$. If $(m, d) = (r, q) = 1$, then*

$$\left| \sum_{x \in F_q} \chi(g(x))\lambda(h(x)) \right| \leq (m + r - 1)\sqrt{q}.$$

Let $N_{q,n}(a, b)$ denote the number of the primitive element solutions of (2.1) in F_{q^n} and $Q = \frac{q^n-1}{q-1}$. Now we can prove our main result.

Theorem 1. (i) *There holds*

$$N_{q,n}(0,0) \geq \frac{\varphi(q^n-1)}{q^2(q^n-1)}\{q^n - q - (q-1)q(\sqrt{q^n}+1) - (2^{\omega(Q)}-1)(q-1)(2q+1)\sqrt{q^n}\};$$

(ii) *if $a \neq 0$, then*

$$N_{q,n}(a,0) \geq \frac{\varphi(q^n-1)}{q^2(q^n-1)}\{q^n - 2(q-1) + (2q-1)\sqrt{q^n} - 2^{\omega(Q)}(4q-3)\sqrt{q^n} - (2^{\omega(q^n-1)} - 2^{\omega(Q)})(2q-1)\sqrt{q^{n+1}}\};$$

(iii) *if $b \neq 0$, then*

$$N_{q,n}(a,b) \geq \frac{\varphi(q^n-1)}{q^2(q^n-1)}\{q^n - \delta q + q(\sqrt{q}+1)(\sqrt{q^n}+1) - (2^{\omega(Q)}-1)(2(\sqrt{q}+1)q + \delta q - 2\delta + 1)\sqrt{q^n} - (2^{\omega(q^n-1)} - 2^{\omega(Q)})(4q + 1 - \delta)\sqrt{q^{n+1}}\},$$

where $\omega(m)$ is the number of the distinct prime factors of m and

$$\delta = \begin{cases} 0 & \text{if } a \neq 0, \\ 1 & \text{if } a = 0. \end{cases}$$

Proof. By Lemmas 2, 3, we have

$$\begin{aligned} N_{q,n}(a,b) &= \frac{q^n-1}{q^2(q^n-1)} \sum_{\xi \in F_{q^n}^*} \sum_{c_1 \in F_q} \psi_{c_1}(T(\xi)-a) \sum_{c_2 \in F_q} \psi_{c_2}(T(\xi^2)-b) \\ &\quad \times \sum_{d \mid q^n-1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \chi^{(d)}(\xi) \\ &= \frac{\varphi(q^n-1)}{q^2(q^n-1)} \sum_{d \mid q^n-1} \frac{\mu(d)}{\varphi(d)} \\ &\quad \times \sum_{\chi^{(d)}} \sum_{c_1,c_2 \in F_q} \sum_{\xi \in F_{q^n}^*} \psi(T(c_1\xi + c_2\xi^2) - c_1a - c_2b)\chi^{(d)}(\xi). \end{aligned} \tag{2.2}$$

Here, $\chi^{(d)}$ runs through all dth order multiplicative characters of F_{q^n}. Let S_{d,c_1,c_2} denote the term

$$\sum_{\xi \in F_{q^n}^*} \psi(T(c_1\xi + c_2\xi^2) - c_1a - c_2b)\chi^{(d)}(\xi).$$

Now we discuss separately the inner terms of (2.2):
(1) $S_{1,0,0} = q^n - 1$;
(2) If $d = 1, c_1 \neq 0$, then

$$\begin{aligned} \Delta_1 = \sum_{c_1 \in F_q^*} S_{1,c_1,0} &= \sum_{c_1 \in F_q^*} \sum_{\xi \in F_{q^n}^*} \psi(T(c_1\xi) - c_1a) \\ &= \sum_{c_1 \in F_q^*} \psi(-c_1a) \left(\sum_{\xi \in F_{q^n}} \psi(T(c_1\xi)) - 1 \right) \\ &= \begin{cases} 1-q & \text{if } a = 0, \\ 1 & \text{if } a \neq 0. \end{cases} \end{aligned}$$

(3) If $d = 1, c_2 \neq 0$, and α is a fixed nonquadratic residue in F_q, then

$$\begin{aligned} \Delta_2 &= \sum_{c_2 \in F_q^*} S_{1,0,c_2} = \sum_{c_2 \in F_q^*} \sum_{\xi \in F_{q^n}^*} \psi(T(c_2\xi^2) - c_2b) \\ &= \frac{1}{2} \left(\sum_{c_2 \in F_q^*} \sum_{\xi \in F_{q^n}^*} \psi(T(c_2^2\xi^2) - c_2^2b) + \sum_{c_2 \in F_q^*} \sum_{\xi \in F_{q^n}^*} \psi(T(c_2^2\alpha\xi^2) - c_2^2\alpha b) \right) \\ &= \frac{1}{2} \left(\sum_{c_2 \in F_q^*} \psi(-c_2^2b) \sum_{\xi \in F_{q^n}^*} \psi(T(\xi^2)) \right. \\ &\qquad \left. + \sum_{c_2 \in F_q^*} \psi(-c_2^2\alpha b) \sum_{\xi \in F_{q^n}^*} \psi(T(\alpha\xi^2)) \right). \end{aligned}$$

From Gauss, we know that

$$|\Delta_2| \le \begin{cases} (q-1)(\sqrt{q^n}+1) & \text{if } b=0, \\ (\sqrt{q}+1)(\sqrt{q^n}+1) & \text{if } b \ne 0. \end{cases}$$

(4) If $d=1, c_1 \ne 0, c_2 \ne 0$, then

$$\begin{aligned} |\Delta_3| &= \sum_{c_1,c_2 \in F_q^*} S_{1,c_1,c_2} \\ &= \sum_{c_1,c_2 \in F_q^*} \sum_{\xi \in F_{q^n}} \psi(T(c_1\xi + c_2\xi^2) - c_1 a - c_2 b) \\ &= \sum_{c \in F_q^*} \sum_{c_1 \in F_q^*} \sum_{\xi \in F_{q^n}^*} \psi(T(\xi + c\xi^2) - c_1 a - c c_1^2 b), \quad \text{where } c c_1^2 = c_2, \\ &= \sum_{c \in F_q^*} \sum_{c_1 \in F_q^*} \psi(-c_1 a - c c_1^2 b) \sum_{\xi \in F_{q^n}^*} \psi(T(\xi + c\xi^2)). \end{aligned}$$

It is obvious that

$$\sum_{c_1 \in F_q^*} \psi(-c_1 a - c c_1^2 b) = \begin{cases} (q-1) & \text{if } a=b=0, \\ -1 & \text{if } a \ne 0, b=0. \end{cases}$$

If $b \ne 0, c \ne 0$, then

$$\left| \sum_{c_1 \in F_q^*} \psi(-c_1 a - c c_1^2 b) \right| \le \sqrt{q} + 1,$$

$$\left| \sum_{\xi \in F_{q^n}^*} \psi(\xi + c\xi^2) \right| \le \sqrt{q^n} + 1.$$

Hence, we have

$$|\Delta_3| \le \begin{cases} (q-1)^2(\sqrt{q^n}+1) & \text{if } a=b=0, \\ (q-1)(\sqrt{q^n}+1) & \text{if } a \ne 0, b=0, \\ (q-1)(\sqrt{q}+1)(\sqrt{q^n}+1) & \text{if } b \ne 0. \end{cases}$$

(5) If $d>1$, and α is a fixed nonquadratic residue in F_q, then

$$\begin{aligned} \Delta_4 &= \sum_{1<d|q^n-1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \sum_{c_1,c_2 \in F_q} S_{d,c_1,c_2} \\ &= \sum_{1<d|q^n-1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \Bigg(S_{d,0,0} + \sum_{c_2 \in F_q^*} S_{d,0,c_2} \\ &\qquad + \sum_{c_1 \in F_q^*} S_{d,c_1,0} + \sum_{c_1,c_2 \in F_q^*} S_{d,c_1,c_2} \Bigg) \end{aligned}$$

$$= \sum_{1<d|q^n-1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \Bigg(S_{d,0,0} + \frac{1}{2} \Bigg(\sum_{c_2 \in F_q^*} \chi^{(d)}(c_2^{-1}) \psi(-c_2^2 b) S_{d,0,1} + \sum_{c_2 \in F_q^*} \chi^{(d)}(c_2^{-1}) \psi(-c_2^2 \alpha b) S_{d,0,\alpha} \Bigg) + \sum_{c_1 \in F_q^*} \chi^{(d)}(c_1^{-1}) \psi(-c_1 a) S_{d,1,0} + \sum_{c \in F_q^*} \sum_{c_1 \in F_q^*} \chi^{(d)}(c_1^{-1}) \psi(-c_1 a - c c_1^2 b) S_{d,1,c} \Bigg).$$

Since $S_{d,0,0} = 0$ and the induced character of $\chi^{(d)}$ over F_q is trivial if and only if $d|Q$, we have

$$\Delta_4 = \sum_{1<d|Q} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \Bigg(\frac{1}{2} \Bigg(\sum_{c_2 \in F_q^*} \psi(-c_2^2 b) S_{d,0,1} + \sum_{c_2 \in F_q^*} \psi(-c_2^2 \alpha b) S_{d,0,\alpha} \Bigg) + \sum_{c_1 \in F_q^*} \psi(-c_1 a) S_{d,1,0} + \sum_{c_2 \in F_q^*} \sum_{c_1 \in F_q^*} \psi(-c_1 a - c c_1^2 b) S_{d,1,c} \Bigg)$$
$$+ \sum_{\substack{1<d|q^n-1 \\ d \nmid Q}} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \Bigg(\frac{1}{2} \Bigg(\sum_{c_2 \in F_q^*} \chi^{(d)}(c_2^{-1}) \psi(-c_2^2 b) S_{d,0,1} + \sum_{c_2 \in F_q^*} \chi^{(d)}(c_2^{-1}) \psi(-c_2^2 \alpha b) S_{d,0,\alpha} \Bigg) + \sum_{c_1 \in F_q^*} \chi^{(d)}(c_1^{-1}) \psi(-c_1 a) S_{d,1,0} + \sum_{c \in F_q^*} \sum_{c_1 \in F_q^*} \chi^{(d)}(c_1^{-1}) \psi(-c_1 a - c c_1^2 b) S_{d,1,c} \Bigg).$$

Now by Lemma 4 we obtain

$$|\Delta_4| \le \begin{cases} (2^{\omega(Q)} - 1)(q-1)(2q+1)\sqrt{q^n} & \text{if } a = b = 0, \\ (2^{\omega(Q)} - 1)(4q-3)\sqrt{q^n} + (2^{\omega(q^n-1)} - 2^{\omega(Q)})(2q-1)\sqrt{q^{n+1}} & \text{if } a \neq 0,\ b = 0, \\ (2^{\omega(Q)} - 1)(2(\sqrt{q}+1)q + \delta q - 2\delta + 1)\sqrt{q^n} + (2^{\omega(q^n-1)} - 2^{\omega(Q)})(4q + 1 - \delta)\sqrt{q^{n+1}} & \text{if } b \neq 0. \end{cases}$$

We observe that

$$N_{q,n}(a,b) \geq \frac{\varphi(q^n-1)}{q^2(q^n-1)}\{q^n - 1 + \Delta_1 - |\Delta_2| - |\Delta_3| - |\Delta_4|\}.$$

Using the estimate above, we prove the theorem. □

Now we give a simple proposition to show when $N_{q,n}(a,b) > 0$. It is useful in the next section.

Proposition 1. (i) *If* $q^{\frac{n}{2}-2} \geq 2^{\omega(Q)}$, *then* $N_{q,n}(0,0) > 0$.
(ii) *Let* $(a,b) \neq (0,0)$. *If* $q^{\frac{n}{2}-\frac{3}{2}} \geq (\frac{13}{3})2^{\omega(q^n-1)}$, *then* $N_{q,n}(a,b) > 0$.

Proof. This is an easy consequence of Theorem 1. □

Proposition 2. (i) *Let* $n \geq 5$. *Then* $N_{q,n}(0,0) > 0$ *for* q^n *large enough.*
(ii) *Let* $n \geq 4, (a,b) \neq (0,0)$. *Then* $N_{q,n}(a,b) > 0$ *for* q^n *large enough.*

Proof. This is an easy consequence of Proposition 1. □

We see that Hansen and Mullen's conjecture for $i = 2$ holds if $n \geq 4$ and q^n is large enough. In the next section, we will prove that $N_{q,n}(a,b) > 0$ for $n \geq 7$.

3. Computations

First of all, we write $u_0 = (\frac{1}{2} - \frac{2}{n})^{-1}, u_1 = (\frac{1}{2} - \frac{3}{2n})^{-1}$. Then the conditions in Proposition 1 can be translated into the following:

Condition (A). $q^n \geq 2^{u_0\omega(Q)}$.

Condition (B). $q^n \geq (\frac{13}{3})^{u_1}2^{u_1\omega(q^n-1)}$.

It is obvious that Conditions (A) and (B) hold when q^n is large enough. Now we give lower bounds for $n \geq 7$.

Proposition 3. (i) *If* $q^n \geq A_n$, *then Condition* (A) *holds.*
(ii) *If* $q^n \geq B_n$, *then Condition* (B) *holds.*
Here, A_n, B_n *are given in Table* 3.1.

Table 3.1

n	u	u_1	A_n	B_n
7	$\frac{14}{3}$	$\frac{7}{2}$	2^{14}	2^{42}
8	4	$\frac{16}{5}$	2^{49}	2^{39}
9	$\frac{18}{5}$	3	1	2^{26}
≥ 10	$\leq \frac{10}{3}$	$\leq \frac{20}{7}$	2^{34}	2^{35}

Proof. The proof is computational. For example, take $n = 7$; we have $u_0 = \frac{14}{3}, u_1 = \frac{7}{2}$. We observe that the possible prime factors of $\frac{q^7-1}{q-1}$ are 7 or the prime numbers of type $(14k + 1)$. Let $\omega_0 = \omega(\frac{q^7-1}{q-1})$. We get

$$\begin{aligned}\frac{q^7-1}{q-1} &\geq 7 \times 29 \times 43 \times 71 \times 2^{6.82(\omega_0-4)} \\ &> 2^{u_0\omega_0+(6.82-u_0)\omega_0-8.04}.\end{aligned}$$

If $\omega_0 \geq 4$, we get $\frac{q^7-1}{q-1} > 2^{u_0\omega_0}$ and $q^7 > \frac{q^7-1}{q-1}$. If $\omega_0 \leq 3$ and $q^7 > 2^{14}$, then Condition (A) holds. So we can take $A_7 = 2^{14}$.

On the other hand,

$$\begin{aligned}q^7 - 1 &= \left(\frac{q^7-1}{q-1}\right)(q-1) \\ &\geq 2 \times 3 \times 5 \times 7 \times 11 \times 2^{u_1(\omega(q-1)-5)} \times \left(\frac{q^7-1}{q-1}\right) \\ &> 2^{11.17} \times \left(\frac{q^7-1}{q-1}\right) \times 2^{u_1(\omega(q-1)-5)}.\end{aligned}$$

Hence, if

$$\frac{q^7-1}{q-1} \geq \left(\frac{13}{3}\right)^{u_1} \times 2^{5u_1} \times 2^{-11.17} \times 2^{u_1\omega_0}, \tag{3.1}$$

Condition (B) holds. But

$$\begin{aligned}\frac{q^7-1}{q-1} &\geq 7 \times 29 \times 43 \times 71 \times 113 \times 127 \times 197 \times 2^{7.72(\omega_0-7)} \\ &> 2^{7.72\omega_0-13.37}.\end{aligned}$$

If $\omega_0 \geq 7$, we have that (3.1) holds. If $\omega_0 \leq 6$ and

$$q^6 \geq \left(\frac{13}{3}\right)^{u_1} \times 2^{5u_1} \times 2^{-11.17} \times 2^{6u_1},$$

namely $q \leq 61$, then again (3.1) holds. So we can take $B_7 = 2^{24}$.

For $n = 8, 9$, using the fact that the possible prime factors of q^4+1 resp. q^6+q^3+1 are 2 resp. 3 or a prime number of type $(8k + 1)$, resp. $(18k + 1)$, we can give a similar discussion and obtain the lower bounds indicated in Table 3.1.

For $n \geq 10$, we have $u_0 \leq \frac{10}{3}$ and $u_1 \leq \frac{20}{7}$. If $\omega(\frac{q^n-1}{q-1}) \geq 11$, then

$$\begin{aligned}\frac{q^n-1}{q-1} &\geq 2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17 \times 19 \times 23 \times 29 \times 31 \\ &\quad \times 2^{5(\omega(Q)-11)} > 2^{u_0\omega(Q)}.\end{aligned}$$

If $\omega(Q) \leq 10$ and $q^n \geq 2^{100/3}$, Condition (A) holds. So we can take $A_n = 2^{34}$ for $n \geq 10$. Similarly, we can take $B_n = 2^{35}$ for $n \geq 10$. □

Theorem 2. *If $n \geq 7$, $N_{q,n}(a, b) > 0$ for any $a, b \in F_q$.*

TABLE 3.2

n	$q^n < A_n$	$q^n < B_n$
7	3^7	p^7 $(3 \le p \le 61)$ 3^{14}; 3^{21}; 5^{14}; 7^{14};
8	p^8 $(3 \le p \le 67)$; 3^{16}; 3^{24}; 5^{16}; 7^{16};	p^8 $(3 \le p \le 29)$; 3^{16}; 3^{24}; 5^{16};
9	no	3^9; 5^9; 7^9;
≥ 10	3^k $(10 \le k \le 21)$; 5^k $(10 \le k \le 14)$; 7^k $(10 \le k \le 12)$;	3^k $(10 \le k \le 22)$; 5^k $(10 \le k \le 15)$; 7^k $(10 \le k \le 12)$; 11^{10}

Proof. If $q^n \ge A_n$ resp. B_n, then $N_{q,n}(a,b) > 0$ by Proposition 3. If $q^n < A_n$ resp. B_n, then q^n must appear in Table 3.2.

Factoring $q^n - 1$ for q^n listed in Table 3.2, we find that Condition (A) holds for $n \ge 7$ and Condition (B) holds for $(n,q) \ne (7,7)$, (7,3), (8,5), (8,3), (9,3). But for $(n,q) = (8,5)$, (8,3), (9,3), we can prove $N_{q,n}(a,b) > 0$ by direct use of Theorem 1 rather than Condition (A) or (B).

Following the suggestions of a referee, we use the Cohen Sieve [2] for $(a,b) \ne (0,0)$, $(n,q) = (7,3), (7,7)$. Let $e | q^n - 1$; define

$$\begin{aligned} T(e) = \{\xi \in F_{q^n} \mid \xi \text{ is a solution of (2.1)} \\ \text{and } \xi \text{ is not any kind of } e\text{th power in } F_{q^n}, \\ \text{that is, } \xi = \rho^d,\ \rho \in F_{q^n},\ d \mid e \text{ only if } d = 1\}. \end{aligned}$$

It is obvious that $|T(q-1)| = N_{q,n}(a,b)$. We have

$$\begin{aligned} T(e_1) \cap T(e_2) &= T([e_1, e_2]), \\ T(e_1) \cup T(e_2) &= T((e_1, e_2)). \end{aligned}$$

Here, $e_1 | q^n - 1, e_2 | q^n - 1$, $[e_1, e_2]$ and (e_1, e_2) denote separately the least common multiple and the greatest common factor of e_1 and e_2.

If $[e_1, e_2] = q - 1$, then

$$\begin{aligned} N_{q,n}(a,b) &= |T(q-1)| \\ &= |T(e_1)| + |T(e_2)| - |T((e_1,e_2))|. \end{aligned} \tag{3.2}$$

To estimate $T(e)$, we need the following fact.

Lemma 2* ([2]). *Let $\xi \in F_{q^n}^*$; then*

$$\sum_{d|e} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \chi^{(d)}(\xi) = \begin{cases} \frac{e}{\varphi(e)} & \text{if } \xi \text{ is not any kind of } e\text{th power,} \\ 0 & \text{otherwise,} \end{cases}$$

where $\chi^{(d)}$ runs through all dth order multiplicative characters of F_{q^n}.

Suppose $(a,b) \ne (0,0)$, we consider the case $(n,q) = (7,7)$. Let $e_1 = 174, e_2 = 9466$; then $[e_1, e_2] = q^n - 1, (e_1, e_2) = 2$. Using Lemma 2* instead of Lemma 2 in

the proof of Theorem 1, we obtain

$$|T(174)| \geq 3367,$$
$$|T(9466)| \geq 6895,$$
$$|T(2)| \leq 9079.$$

By (3.2), we obtain $N_{q,n}(a,b) > 0$. For $(n,q) = (7,3)$, we take $e_1 = 2, e_2 = 1093$. A similar computation gives $N_{q,n}(a,b) > 0$. Hence we finish the proof of Theorem 2. □

By Lemma 1 and Theorem 2, we can easily give the following corollaries.

Corollary 1. *Suppose $n \geq 7$. Then there exists a primitive polynomial in $F_q[x]$ of degree n with the first and second coefficients prescribed in advance.*

Corollary 2. *Suppose $n \geq 7$. There are at least q primitive polynomials in $F_q[x]$ of degree n with the first or second coefficient prescribed in advance.*

Corollary 2 shows that Hansen and Mullen's conjecture holds for $i = 2$ if $n \geq 7$.

In the cases $n = 4, 5, 6$, the lower bounds A_n's in Proposition 3 are too large since $q^n - 1$ may have more small prime factors. To give a complete list of the exceptions for which our conclusion in Theorem 2 does not hold, we suggest the Cohen Sieve [2] as a means of attack. The analysis of these cases is contemplated in future work.

Acknowledgment

The author is indebted to Professor Q. Sun for his encouragement and to the referees for their suggestions.

References

1. S. D. Cohen, *Primitive elements and polynomials with arbitrary traces*, Discrete Math. (2) **83** (1990), 1–7.
2. ———, *Primitive elements and polynomials: existence results*, Lecture Notes in Pure and Appl. Math., vol. 141, edited by G. L. Mullen and P. J. Shiue, Marcel Dekker, New York, 1992, pp. 43–55.
3. H. Davenport, *Bases for finite fields*, J. London Math. Soc. **43** (1968), 21–39.
4. W.-B. Han, *Primitive roots and linearized polynomials*, Adv. in Math. (China) **22** (1994), 460–462.
5. T. Hansen and G. L. Mullen, *Primitive polynomials over finite fields* Math. Comp. **59** (1992), 639–643.
6. D. Jungnickel and S. A. Vanstone, *On primitive polynomials over finite fields*, J. Algebra **124** (1989), 337–353.
7. R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, MA, 1983.
8. H. W. Lenstra and R. J. Schoof, *Primitive normal bases for finite fields*, Math. Comp. **48** (1987), 217–232.
9. O. Moreno, *On the existence of a primitive quadratic trace* 1 *over* GF(p^m), J. Combin. Theory Ser. A **51** (1989), 104–110.
10. W. M. Schmidt, *Equations over finite fields; an elementary approach*, Lecture Notes in Math., vol. 536, Springer-Verlag, Berlin and New York, 1976.
11. Q. Sun and W.-B. Han, *The absolute trace function and primitive roots in finite fields* (*in Chinese*), Chinese Ann. Math. Ser. A **11** (1990), 202–205.
12. ———, *Improvement of Weil exponential sums and its application*, preprint.

Department of Mathematics, University of Science and Technology of China, Hefei, Anhui 230026, The People's Republic of China