Primitive normal polynomials with the last half coefficients prescribed

Shuqin Fan

Department of Applied Mathematics, Information Engineering University, Zhengzhou 450002, PR China

Abstract

In this paper, we prove that for any given $n \geq 2$, there exists a constant $C(n)$ such that for any prime power $q > C(n)$, there exists a primitive normal polynomial of degree $n$ over $F_q$ with the last $\left\lfloor \frac{n}{2} \right\rfloor$ coefficients prescribed, where the last coefficient is a primitive element. Furthermore, the number of prescribed coefficients increases from $\left\lfloor \frac{n}{2} \right\rfloor$ to $\left\lfloor \frac{n+1}{2} \right\rfloor$ when the coefficients are specified as $(0, \ldots, 0, b)$ with $b$ any primitive element. This result is a complement to the existence of a primitive normal polynomial with the first $\left\lfloor \frac{n}{2} \right\rfloor$ coefficients prescribed which was proved in [S.Q. Fan, W.B. Han, K.Q. Feng, Primitive normal polynomials with multiple coefficients prescribed: An asymptotic result, Finite Fields Appl. 13 (2007) 1029–1044]. The outline of this paper is similar to the above reference with the following two different treatments. On one hand, we use $1/x$ instead of $x$ in the problem reduction step and as a consequence use the hybrid Kloostermann sums instead of hybrid Weil sums over Galois rings. On the other hand, the estimates are slightly more complicated and the results in some special cases are better than those in [S.Q. Fan, W.B. Han, K.Q. Feng, Primitive normal polynomials with multiple coefficients prescribed: An asymptotic result, Finite Fields Appl. 13 (2007) 1029–1044].

© 2009 Elsevier Inc. All rights reserved.

Keywords:
Finite field
Primitive polynomial
Character sums over Galois rings
Normal basis
$p$-Adic method

Article history:
Received 22 October 2008
Revised 22 April 2009
Available online 21 May 2009
Communicated by Stephen D. Cohen

© 2009 Elsevier Inc. All rights reserved.
1. Introduction

Let $F_{q^n}$ be a finite degree extension over finite field $F_q$ with $q = p^k$ elements where $p$ is a prime number and $k$ a positive integer. It is known that every generator of $F_{q^n}^* = F_{q^n} \setminus \{0\}$, which is a multiplicative cyclic group, is called a primitive element. On the other hand, $F_{q^n}$ can also be viewed as a vector space of dimension $n$ over $F_q$. An element $\alpha \in F_{q^n}$ is called normal if $[\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}]$ forms a set of $F_q$-basis of $F_{q^n}$. $\alpha$ is called a primitive normal element if it is both primitive and normal. Let $f(x)$ be a monic polynomial over $F_q$. $f(x)$ is called a primitive normal (primitive, normal) polynomial if it is the minimal polynomial of a primitive normal (primitive, normal) element.

Let $f(x) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n$. For $1 \leq i \leq n$, we call $\sigma_i$ the $i$th coefficient of $f(x)$. Especially, $\sigma_1$ and $\sigma_n$ are called the trace and norm of $f(x)$ respectively.

Because of the many applications such as fast Fourier transformation, coding theory and cryptography for doing computations efficiently in finite fields, primitive normal elements and primitive normal polynomials over finite fields were widely discussed [1–3,7–9,12]. In 1987, Lenstra and Schoof [9] proved that there exists a primitive normal basis of $F_{q^n}$ over $F_q$ for every prime power $q$ and every positive integer $n$, which we call primitive normal basis theorem.

Several papers discussed the existence of a primitive normal polynomial with specified trace and norm [1–3]. By using the $p$-adic method, Fan et al. [8] in 2007 proved the existence of a primitive normal polynomial of degree $n$ with the first two coefficients $\sigma_1, \sigma_2$ prescribed for $n \geq 7$. In another paper [7], they got a general result:

**Known result 1.** For any given positive integer $n \geq 2$, there exists a constant $C(n)$ such that for any prime power $q > C(n)$, there exists a primitive normal polynomial over $F_q$ of degree $n$ with the first $\lfloor \frac{n}{2} \rfloor$ coefficients $\sigma_1, \ldots, \sigma_{\lfloor \frac{n}{2} \rfloor}$ prescribed, where the first coefficient $\sigma_1 \neq 0$.

It is natural to ask the following question:

**Question 1.** For any given positive integer $n \geq 2$, whether there exists a primitive normal polynomial over $F_q$ of degree $n$ with the last $\lfloor \frac{n}{2} \rfloor$ coefficients prescribed?

As for the case of primitive polynomial, the existence of a primitive polynomial with the last $\lfloor \frac{n}{2} \rfloor$ coefficients prescribed can be deduced from the existence of a primitive polynomial with the first $\lfloor \frac{n}{2} \rfloor - 1$ coefficients and the norm prescribed since the reciprocal polynomial of a primitive polynomial is also a primitive polynomial. But this method cannot be used to the case of primitive normal polynomial since the reciprocal polynomial of a primitive normal polynomial may be not a primitive normal polynomial.

In this paper, we investigate Question 1 and get the following asymptotic main result.

**Main result.** For any given $n \geq 2$, there exists a constant $C(n)$ such that for any prime power $q > C(n)$, there exists a primitive normal polynomial of degree $n$ over $F_q$ with the last $\lfloor \frac{n}{2} \rfloor$ coefficients prescribed, where the last coefficient is a primitive element. Furthermore, the number of prescribed coefficients increases from $\lfloor \frac{n}{2} \rfloor$ to $\lfloor \frac{n+1}{2} \rfloor$ when the coefficients are specified as $(0, \ldots, 0, b)$ with $b$ any primitive element.

The outline of this paper is similar to reference [7] with the following two different treatments. First, we use the $p$-adic method as in [7] to translate the existence of a primitive normal polynomial with the last $m$ coefficients prescribed to the existence of a primitive normal element solution of some system of equations consisting of some trace equations with variable $x^{-1}$, while the corresponding system of equations in [7] consists of some trace equations with variable $x$. Then with the help of the estimates of character sums over Galois rings and some delicate and effective computing techniques we finally get the above main result. We use the hybrid extended Kloostermann sums in this paper instead of the hybrid weil sums in [7]. Furthermore, the estimates are slightly more complicated than those in [7] and the results are better than those in [7] in some special cases.
Since the outline of this paper is similar to [7], we will focus on the different parts. The more details can be referenced to [7].

2. Problem reduction: The $p$-adic method and the use of variable $x^{-1}$

We first assume the readers are familiar with the $p$-adic number fields and Galois rings. Let $e, k, n \geq 1$ be positive integers, Galois rings $R_{e,k}$ be the unramified extension of $\mathbb{Z}_p^e$ of degree $k$ and $\Gamma_k$ be the set of the Teichmüller points of $R_{e,k}$, $\Gamma_k^\ast = \Gamma_k \setminus \{0\}$. Denote $\text{Tr}(\cdot)$ the trace map from $R_{e,nk}$ to $R_{e,k}$ and $\text{Norm}(\cdot)$ the norm map from $\Gamma_{nk}$ to $\Gamma_k$. Denote $\phi$ the canonical projective map from $R_{e,k}$ to $\Gamma_k$. For more details see [7] or [11].

In this section, we will translate the existence of a primitive normal polynomial of degree $n$ over $F_q$ with the last $m$ coefficients prescribed to the existence of a primitive normal element solution of some system of equations, which consists of some trace equations with variable $x^{-1}$ and one norm equation with variable $x$ over suitable Galois rings.

For the primitive polynomial case, since the reciprocal polynomial of a primitive polynomial is also a primitive polynomial, the existence of a primitive polynomial with the last $m$ coefficients prescribed can be deduced by the existence of a primitive polynomial with the first $m - 1$ coefficients and the norm prescribed. But as we know, the reciprocal polynomial of a primitive normal polynomial may not be a primitive normal polynomial, for example, the first coefficient of a primitive normal polynomial $\sigma_1 \neq 0$, but the first coefficient of its reciprocal polynomial can be zero, i.e., $\sigma_{n-1}$ can be zero. So we cannot handle the primitive normal polynomial case the same as what we did in the primitive polynomial case.

We next give the idea of our solution by a lemma.

**Lemma 1.** Suppose that for any given $a_1, \ldots, a_m \in F_q$, and any given primitive element $b \in F_q^\ast$, there exists a primitive normal polynomial of degree $n$ over $F_q$ with the last $m + 1$ coefficients prescribed.

1. its first $m$ coefficients $\sigma_1, \ldots, \sigma_m$ are prescribed as $a_1, \ldots, a_m$;
2. its norm $\sigma_n$ is prescribed as $b$;
3. its reciprocal polynomial is a primitive normal polynomial.

Then there exists a primitive normal polynomial of degree $n$ over $F_q$ with the last $m + 1$ coefficients prescribed.

**Proof.** Let $f(x) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^{n-1} \sigma_{n-1} x + (-1)^n b$ be a primitive polynomial satisfying the above conditions. Consider its reciprocal polynomial

$$f^*(x) = (-1)^n b^{-1} x^n f\left(\frac{1}{x}\right) = x^n - \frac{\sigma_{n-1}}{b} x^{n-1} + \cdots + (-1)^n b^{-1} x + (-1)^n \frac{1}{b}.$$

$f^*(x)$ is a primitive normal polynomial by condition 3. Furthermore, $\frac{\sigma_m}{b}, \ldots, \frac{\sigma_1}{b}$ run across $F_q^m$ when $\sigma_1, \ldots, \sigma_m$ run across $F_q^m$. On the other hand, $\frac{1}{b}$ runs across the set of primitive elements when $b$ runs across the set of primitive elements of $F_q^\ast$. This finishes the proof. $\square$

We will next reformulate Lemma 1 by the existence of a primitive normal element solution of some system of equations, which consist of some trace equations of $x^{-1}$ and one norm equation of $x$ over suitable Galois rings. Similar to [7], we use the $p$-adic method introduced by the author and Professor Han [6] to finish the reduction step.

As we know, for any irreducible (primitive, primitive normal) polynomial $f(x)$ of degree $n$ over $F_q$, $f(x)$ can be uniquely hensel lifted to a polynomial $\tilde{f}$, which we call lifted irreducible (primitive, primitive normal) polynomial over $R_{e,k}$. For more details see [6] or [7]. Since the lifted primitive normal polynomials of degree $n$ over $R_{e,k}$ are one-to-one correspondence to the primitive normal polynomials of degree $n$ over $F_q$, we only need to investigate the existence of a lifted primitive normal polynomial of degree $n$ over $R_{e,k}$ with the canonical projective map of the last $m$ coefficients prescribed.
We first give a lemma.
For \(1 \leq t, l \leq m\), \((t, p) = 1\), let \(e(t, l)\) be the largest integer such that \(tp^{e(t,l)-1} \leq l\).

**Lemma 2.** (See [6].) Let \(f(x) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n\) be an irreducible polynomial over \(R_{e,k}\). \(\xi\) be a root of \(f(x)\). For \(1 \leq l \leq m\), let \(l = t_i p^{s(t_i,l)-1}\), where \((t_i, p) = 1\) and \(e(t_i, l) \geq 1\). Suppose that for each \(1 \leq t \leq l\), \((t, p) = 1\),

\[
\text{Tr}(\xi) = d_{t,0} + pd_{t,1} + \cdots + p^{e(t,l)-1}d_{t,e(t,l)-1} \mod p^{e(t,l)}.
\]

Then we have

\[
(-1)^l \sigma_l \equiv g\left(\left\{d_{t,i} \mid (t, p) = 1, \, tp^i < l\right\}\right) = \frac{1}{\sigma_l} \cdot d_{t,e(t,l)-1} \mod p,
\]

where \(g(x)\) is a polynomial of \(\{d_{t,i} \mid (t, p) = 1, \, tp^i < l\}\) over \(R_{e,k}\).

From Lemmas 1 and 2 we have

**Theorem 3.** Let \(e(t)\) be the largest integer such that \(tp^{e(t)-1} \leq m\). Suppose that for any given \(d_{t,i} \in \Gamma_k\), where \((t, p) = 1\) and \(1 \leq t \leq m\), \(0 \leq i \leq e(t) - 1\), and any primitive element \(b \in \Gamma_k^*\), there exists a primitive normal element solution of the following system of equations

\[
\begin{align*}
\text{Tr}(x^{-i}) = & \; d_{t,i} + pd_{t,1} + \cdots + p^{e(t)-1}d_{t,e(t)-1} \mod p^{e(t)}, \quad \text{for } 1 \leq t \leq m, \quad (t, p) = 1; \\
\text{Norm}(x) = & \; b.
\end{align*}
\]

Then there exists a primitive normal polynomial over \(F_q\) of degree \(n\) with the last \(m + 1\) coefficients prescribed, where the last coefficient \(\sigma_n\) is a primitive element.

**Proof.** Let \(\xi\) be a primitive normal element solution of Eqs. (1), \(f(x)\) be its minimum polynomial and \(f^*(x)\) be the reciprocal polynomial of \(f(x)\). Then \(f(x)\) is a lifted primitive normal polynomial and \(f^*(x)\) is a lifted primitive polynomial, \(\xi^{-1}\) is a root of \(f^*(x)\). From Lemma 2, the canonical projective map of the first \(m\) coefficients \(\sigma_1^*, \ldots, \sigma_m^*\) of \(f^*(x)\) runs across \(\Gamma_k^m\) when \(d_{t,i}, \,(t, p) = 1\), \(tp^i \leq m\) run across \(\Gamma_k^m\). On the other hand, the norm \(\sigma_n^* = b^{-1}\). So \(f^*(x) \mod p\) is a primitive polynomial over \(F_q\) satisfying the three conditions in Lemma 1, and thus there exists a primitive normal polynomial of degree \(n\) over \(F_q\) with the last \(m + 1\) coefficients prescribed. \(\square\)

### 3. Estimates

In this section, we will estimate the number of primitive normal element solutions of Eqs. (1), which we denote by \(N_m(d_t,b)\). Unlike the estimates in [7], we use the hybrid extended Kloosterman sums in this paper instead of the hybrid weil sums over Galois rings. Furthermore, the estimates are slightly more complicated than those in [7] and the results are better than those in [7] in some special cases.

Let \(\psi_{e,k}, \psi_{e,nk}\) be the canonical additive character of \(R_{e,k}\) and \(R_{e,nk}\). \(\chi, \chi_n\) be a multiplicative character of \(\Gamma_k\) and \(\Gamma_{nk}\) respectively. Denote \(\hat{R}_{e,k}\) the set of all the additive characters of \(R_{e,k}\) and \(\hat{\Gamma}_k^*\) the set of all the multiplicative characters of \(\Gamma_k^*\).

#### 3.1. Estimates of character sums over Galois rings

We first give some estimates of character sums over Galois rings for our later use. When \(e = 1\), it is just the estimates of character sums over finite fields. We first give a definition.
Let \( h(x) \) be a polynomial over \( R_{e,nk} \) with \( h(0) = 0 \) and \( h(x) \) not identically 0. Let

\[
h(x) = h_0(x) + h_1(x)p + \cdots + h_{e-1}(x)p^{e-1}, \quad h_1(x) \in \Gamma_{nk}[x],
\]

be the \( p \)-adic expansion of \( h(x) \) and

\[
h_i(x) = \sum_{j=0}^{d_i} h_{i,j}x^j, \quad h_{i,j} \in \Gamma_{nk},
\]

where \( d_i \) is the degree of \( h_i(x) \). \( h(x) \) is called nondegenerate if for all \( 0 \leq i \leq e - 1, \ 0 \leq j \leq d_i \), the coefficients \( h_{i,j} \) of \( h_i(x) \) satisfy \( h_{i,j} = 0 \) if \( j \equiv 0 \) (mod \( p \)). Define the weighted \( e \)-degree of \( h(x) \) by

\[
D_{e,h} = \max(d_0p^{e-1}, d_1p^{e-2}, \ldots, d_{e-1}).
\]

**Lemma 4.** (See [10].) Let \( f(x), g(x) \in R_{e,nk}[x] \) be nondegenerate polynomials with weighted \( e \)-degree \( D_{e,f} \) and \( D_{e,g} \) respectively and \( \chi_n \) be a nontrivial multiplicative character of \( \Gamma_{nk} \). Then

1. \[
\left| \sum_{x \in \Gamma_{nk}} \psi_{e,nk}(f(x)) \right| \leq (D_{e,f} - 1)q^{n/2}.
\]
2. \[
\left| \sum_{x \in \Gamma_{nk}^*} \psi_{e,nk}(f(x)) \chi_n(x) \right| \leq D_{e,f}q^{n/2}.
\]
3. \[
\left| \sum_{x \in \Gamma_{nk}^*} \psi_{e,nk}(f(x) + g(x^{-1})) \right| \leq (D_{e,f} + D_{e,g})q^{n/2}.
\]
4. \[
\left| \sum_{x \in \Gamma_{nk}^*} \psi_{e,nk}(f(x) + g(x^{-1})) \chi_n(x) \right| \leq (D_{e,f} + D_{e,g})q^{n/2}.
\]

### 3.2. Characteristic functions

In fact, Theorem 3 cares about the existence of \( \omega \in \Gamma_{nk} \) satisfying the following four conditions.

1. \( \text{Tr}(\omega^{-t}) = d_t = dt,0 + pdt,1 + \cdots + p^{e(t)-1}dt,e(t)-1 \mod p^{e(t)} \), for \( 1 \leq t \leq m \), \( (t, p) = 1 \);
2. \( \text{Norm}(\omega) = b \);
3. \( \omega \) is a primitive element;
4. \( \omega \) is a normal element.

We next give the characteristic functions of the above four conditions respectively. It is similar to those in [7] so we will omit the details and only present the results for later use.

Let \( e \) be the largest integer such that \( p^{e-1} \leq m \). Denote

\[
S_l = \{ t \mid (t, p) = 1, \ t \text{ is the largest integer such that } tp^{l-1} \leq m \}
\]

for \( l = 1, 2, \ldots, e \) and

\[
S = \{ (c_t)_{(t,p)=1} \mid c_t \in R_{t,k} \text{ for } t \in S_l, \ l = 1, 2, \ldots, e \}.
\]
Let $W = \#S$. We have $W = q^m$. Denote

$$h(x) = \sum_{l=1}^{e} p^{e-l} \sum_{t \in S_l} c_t x^t.$$  

Lemma 5. Let $\psi_{e,k}, \psi_{e,nk} = \psi_{e,k} \circ \text{Tr}$ be the canonical additive characters of $R_{e,k}$ and $R_{e,nk}$ respectively, $h(x)$ be defined as above and $\omega \in \Gamma_{nk}^*$. Then

$$T_{(d_1)}(\omega) = \frac{1}{q^m} \sum_{(c_t) \in S} \psi_{e,k} \left( -\sum_{l=1}^{e} p^{e-l} \sum_{t \in S_l} c_t d_t \right) \psi_{e,nk}(h(\omega^{-1})) = \begin{cases} 1 & \text{if } \omega \text{ satisfies condition } 1; \\ 0 & \text{otherwise}. \end{cases}$$

Lemma 6. Let $\omega \in \Gamma_{nk}^*$. Then

$$N_b(\omega) = \frac{1}{q-1} \sum_{\chi \in \Gamma_k^*} \chi \left( \frac{\text{Norm}(\omega)}{b} \right) = \begin{cases} 1 & \text{if } \text{Norm}(\omega) = b; \\ 0 & \text{otherwise}. \end{cases}$$

Let $\omega \in \Gamma_{nk}^*$. The order of $\omega$, denoted by $\text{ord}(\omega)$, is defined to be the smallest integer such that $\omega^{\text{ord}(\omega)} = 1$. Let $e|q^n - 1$ and $\nu \in \Gamma_{nk}^*$. Then $\nu$ is said to be $e$-free (or not any kind of $e$th power) if $e$ and $(q^n - 1)/\text{ord}(\nu)$ are relatively prime. It is easy to see that $\omega$ is a primitive element if and only if $\omega$ is $(q^n - 1)$-free. The following lemma gives a characteristic function of an element of e-free.

Lemma 7. (See [5].) Let $e|q^n - 1$ and $\omega \in \Gamma_{nk}^*$. Then we have

$$P_e(\omega) = \frac{\varphi(e)}{e} \sum_{d|e} \frac{\mu(d)}{\varphi(d)} \sum_{\chi \in \Gamma_k^*} \chi^{(d)}(\omega) = \begin{cases} 1 & \text{if } \omega \text{ is e-free}; \\ 0 & \text{otherwise}, \end{cases}$$

where $\mu(d)$ is the Möbius function and $\varphi(d)$ is the Euler function, $\chi^{(d)}$ runs through all the $\varphi(d)$ multiplicative characters over $\Gamma_{nk}^*$ with order $d$.

The following lemma from [7] gives a characteristic function of a normal element. For any $\alpha \in R_{e,nk}$, define $\psi_{e,nk}^\alpha(x) = \psi_{e,nk}(\alpha x)$, $x \in R_{e,nk}$.

Lemma 8. (See [7].) Let $\psi_{e,nk}$ be the canonical additive character of $R_{e,nk}$ and $\omega \in \Gamma_{nk}^*$. Then we have

$$N(\omega) = \frac{\varphi(q^n - 1)}{q^n} \sum_{D|\varphi(q^n)} \frac{\mu_q(D)}{\varphi_q(D)} \sum_{\alpha_D \in \Gamma_k^*} \psi_{e,nk}(p^{e-1} \alpha_D \omega) = \begin{cases} 1 & \text{if } \omega \text{ is normal}; \\ 0 & \text{otherwise}, \end{cases}$$

where $\mu_q(\cdot)$, $\varphi_q(\cdot)$ denote the Möbius function and the Euler function respectively, for the polynomial ring $F_q[x]$, $\alpha_D$ runs across all the $\varphi_q(D)$ number of elements such that $\psi_{e,nk}^{p^{e-1} \alpha_D}$ has $R_{e,k}$-order $D$. For more details see [7].

3.3. Number of primitive normal element solutions

In this subsection we will estimate the number of primitive normal element solutions of Eqs. (1). The techniques used in this paper are slightly more complicated than those in [7] and the results are better than those in [7] in some special cases.
Let \( Q \) be the largest integer such that \( Q \mid q^n - 1 \) and \(\gcd(Q, q - 1) = 1\). We call \( Q \) the \((q - 1)\)-free part of \( q^n - 1 \). The following two lemmas have been proved in [4]. The proof is quite simple and the readers can refer to [4] or prove by themselves.

**Lemma 9.** (See [4].) Let \(\chi_n\) be a multiplicative character of \(\Gamma_{nk}\), and \(\chi_n|\Gamma_k\) be its restriction to \(\Gamma_k\). Suppose that \(\text{ord}(\chi_n)|\frac{q^n - 1}{q - 1}\). Then \(\chi_n|\Gamma_k\) is a trivial multiplicative character of \(\Gamma_k\).

**Lemma 10.** (See [4].) Suppose \( Q \) be the \((q - 1)\)-free part of \( q^n - 1 \) and \(d\mid Q\). Let \(\chi\) be a multiplicative character of \(\Gamma^*_k\) and \(\chi_n = \chi \circ \text{Norm}\) be the lifted multiplicative character, \(\chi(d)\) be a multiplicative character of \(\Gamma^*_nk\) with order \(d\). Then \(\chi(d) \cdot \chi_n\) is a trivial character of \(\Gamma^*_nk\) if and only if \(d = 1\) and \(\chi = \chi_0\).

**Lemma 11.** (See [5].) Let \( Q \) be the \((q - 1)\)-free part of \( q^n - 1 \). An element \(\omega \in \Gamma^*_nk\) is primitive if and only if \(\text{Norm}(\omega)\) is a primitive element of \( I_k \) and \(\omega\) is \(Q\)-free, i.e., \(Q \mid \text{ord}(\omega)\).

Since \( b \) is a primitive element of \(\Gamma^*_k\), from Lemma 11, \(\omega\) is primitive if \(\omega\) is \(Q\)-free and \(\text{Norm}(\omega) = b\). From Lemmas 5, 6, 7 and 8 we have

\[
N_m((d_1), b) = \sum_{\omega \in I^*_nk} T_{(d_1)}(\omega)N_b(\omega)P_Q(\omega)N(\omega)
\]

\[
= \delta \sum_{d \mid (Q, D)^{\mu-1}} \frac{\mu(d)}{\varphi(d)} \sum_{\alpha_D \in I^*_k} \sum_{\chi \in I^*_nk} \chi(b^{-1}) \sum_{(c_e) \in S} \psi_e \left(-\sum_{l=1}^{\mu} \sum_{t \in S_l} c_t d_l \right) \chi(d) \cdot \chi_n(\omega),
\]

where

\[
\delta = \frac{1}{q^m} \cdot \frac{1}{q - 1} \cdot \frac{\varphi(Q)}{Q} \cdot \frac{\varphi(Q^{n-1})}{q^n}
\]

and \(\chi_n = \chi \circ \text{Norm}\) be the lifted multiplicative character of \(\Gamma^*_nk\). Denote

\[
A((c_1), \chi, \chi(d), \alpha_D) = \sum_{\omega \in I^*_nk} \psi_e \left(h(\omega^{-1}) + p^{e-1} \alpha_D \omega \right) \chi(d) \cdot \chi_n(\omega),
\]

\[
\Theta_{d,D}((c_1), \chi) = \frac{\mu(d)}{\varphi(d)} \sum_{\chi \in I^*_nk} \chi(b^{-1}) \psi_e \left(-\sum_{l=1}^{\mu} \sum_{t \in S_l} c_t d_l \right) \sum_{\alpha_D \in I^*_k} A((c_1), \chi, \chi(d), \alpha_D),
\]

and

\[
\Theta_{d,D} = \sum_{(c_1) \in S} \sum_{\chi \in I^*_nk} \Theta_{d,D}((c_1), \chi).
\]

Then

\[
N_m((d_1), b) = \delta \sum_{d \mid (Q, D)^{\mu-1}} \Theta_{d,D}.
\]
Since the estimate of the case $0 = d_t \in R_{l,k}$ for all $t \in S_l$ and all $l = 1, \ldots, e$ is better than the estimate of the case $0 \neq d_t \in R_{l,k}$ for some $t \in S_l$ and some $l = 1, \ldots, e$, we will rewrite $\Theta_{d,D}$ as $\Theta_{d,D}((0), b)$ and $\Theta_{d,D}((d_t)_{i \neq 0}, b)$ for the two cases respectively.

**Proposition 12.** Let $\Theta_{d,D}((0), b)$ and $\Theta_{d,D}((d_t)_{i \neq 0}, b)$ be defined as above.

1. Suppose that $(d, D) = (1, 1)$. Then

$$\Theta_{1,1}((0), b) \geq q^n + 2(m + 1)(q - 1)q^{\frac{n}{2} + m - 1} \quad (3)$$

and

$$\Theta_{1,1}((d_t)_{i \neq 0}, b) \geq q^n - (m + 1)\left(m + \frac{1}{\sqrt{q}}\right)(q - 1)q^{\frac{n-1}{2} + m} \quad (4)$$

2. Suppose that $(d, D) \neq (1, 1)$. Then

$$|\Theta_{d,D}((0), b)| \leq 2(m + 1)(q - 1)q^{\frac{n}{2} + m - 1} \quad (5)$$

and

$$|\Theta_{d,D}((d_t)_{i \neq 0}, b)| \leq (m + 1)\left(m + \frac{1}{\sqrt{q}}\right)(q - 1)q^{\frac{n-1}{2} + m} \quad (6)$$

**Proof.** From Lemma 10, $\Lambda((c_t), \chi, \chi^{(d)}, \alpha_D) = q^n - 1$ if and only if $(d, D, h(x), \chi) = (1, 1, 0, \chi_0)$.

1. Suppose $h(x) = 0$, i.e., $0 = c_t \in R_{l,k}$ for all $t \in S_l$ and $l = 1, 2, \ldots, e$. Then similarly as the estimates in [7] we can easily check

$$\Theta_{1,1}((0), \chi_0) = q^n - 1. \quad (7)$$

And if $\chi \neq \chi_0$,

$$\Theta_{1,1}((0), \chi) = 0. \quad (8)$$

And if $(d, D) \neq (1, 1)$,

$$\left|\sum_{\chi \in \mathfrak{F}_k} \Theta_{d,D}((0), \chi)\right| \leq (q - 1)q^{n/2}. \quad (9)$$

2. Suppose $h(x) \neq 0$. Let

$$T = \begin{cases} 1 & \text{if } (d_t) = (0); \\ \text{the smallest integer such that } 0 \neq d_T & \text{otherwise.} \end{cases}$$

Let $J$ be the largest integer such that $Tp^{j-1} \leq m$. We write $c_T = c_{T,0} + \ldots + c_{T,j-1}p^{j-1}$ and rewrite $\Lambda((c_t), \chi, \chi^{(d)}, \alpha_D)$ and $\Theta_{d,D}((c_t), \chi)$ by $\Lambda(c_{T,0}, \ldots, c_{T,j-1}, (c_t)_{i \neq T}, \chi, \chi^{(d)}, \alpha_D)$ and $\Theta_{d,D}(c_{T,0}, \ldots, c_{T,j-1}, (c_t)_{i \neq T}, \chi)$ respectively for our convenience of later use.
(a) Suppose that $c_{T,0} \neq 0$. Denote
\[
\mathcal{S}^l = \{(c_t)_{t \neq T} \mid c_t \in R_{l,k} \text{ for } t \in S_l, \ l = 1, 2, \ldots, e\}.
\]

Let $g$ be a generator of $\Gamma^*_k$. Suppose $T' = gcd(T, q - 1)$. Then $\bigcup_{l=0}^{T-1} \{g^i v^{T'} \mid v \in \Gamma^*_k\} = \bigcup_{l=0}^{T-1} \{g^i v^{T'} \mid v \in \Gamma^*_k\}$ runs across $\Gamma^*_k$ $T'$ times. Define
\[
\mathcal{A}_s(\chi) = \sum_{c_t, t \in \Gamma^*_k} \sum_{c_t, t \in \Gamma^*_k} \sum_{(c_t)_{t \neq T} \in \mathcal{S}^l} \Theta_d, D(c_{T,0}, \ldots, c_{T, J-1}, (c_t)_{t \neq T}, \chi)
\]
\[
= \frac{1}{T'} \sum_{l=0}^{T-1} \sum_{v \in \Gamma^*_k} \sum_{c_t, t \in \Gamma^*_k} \sum_{(c_t)_{t \neq T} \in \mathcal{S}^l} \Theta_d, D(g^i v^{T'}, c_{T,1}, \ldots, c_{T, J-1}, (c_t)_{t \neq T}, \chi).
\]

Let $\tilde{\omega} = v^{-1} \omega$, $c_{T,i} = v^{-T} c_{T,i}$ for $1 \leq i \leq J - 1$, $c_t = v^{-T} c_t$ for all $t \in S_l$, $t \neq T$ and $\alpha_D^* = \nu_D$. Given $v \neq 0$, it is easy to see that $\tilde{\omega}, c_{T, i}, c^*_t (t \neq T), \alpha_D^*$ runs through $\Gamma^*_{nk}, \Gamma_k, R_{l,k}$ (when $t \in S_l$) and $\Gamma_D$ when $\omega, c_{T, i}, c_t, \alpha_D$ runs through $\Gamma^*_{nk}, \Gamma_k, R_{l,k}$ and $\Gamma_D$ respectively. For $0 \leq i \leq T' - 1$, denote
\[
h_i(x) = p^{e-J}(g^i + c_{T,1}^* p + \cdots + c_{T, J-1}^* p^{J-1})x^T + \sum_{l=1}^{e} p^{e-l} \sum_{t \in S_l, t \neq T} c_t^* x^T,
\]
and
\[
l_i(x) = \begin{cases} 0 & \text{if } (d_t) = (0); \\
p^{e-J}(g^i + c_{T,1}^* p + \cdots + c_{T, J-1}^* p^{J-1})d_T x^T + \sum_{l=1}^{e} p^{e-l} \sum_{t \in S_l, t \neq T} c_t^* d_T x^T & \text{otherwise.}
\end{cases}
\]

From Lemma 9, $\chi^{(d)}|\Gamma_k$ is a trivial character when $d|Q$, so
\[
\mathcal{A}_s(\chi) = \frac{1}{T'} \mu(d) \mu_q(D) \varphi(d) \varphi_q(D) \chi(\mu^{-1}) \sum_{\chi^{(d)} \alpha_D^* \in \Gamma_k} \sum_{l=0}^{T-1} \sum_{(c_t)_{t \neq T} \in \mathcal{S}^l} \sum_{v \in \Gamma^*_k} \psi_{e,k}(\chi_l(v)) \psi_l(\chi_l(v))
\]
\[
\cdot \sum_{\tilde{\omega} \in \Gamma^*_{nk}} \psi_{e,nk}(h_i(\tilde{\omega}^{-1}) + p^{e-1} \alpha_D^* \tilde{\omega}) \chi^{(d)}(\chi_l(\tilde{\omega})).
\]

Since $h_i(x) (0 \leq i \leq T' - 1)$ is nondegenerate with $D_{e,h_i} \leq m$. From Lemma 4,
\[
\left| \sum_{\tilde{\omega} \in \Gamma^*_{nk}} \psi_{e,nk}(h_i(\tilde{\omega}^{-1}) + p^{e-1} \alpha_D^* \tilde{\omega}) \chi^{(d)}(\chi_l(\tilde{\omega})) \right| \leq (m + 1)q^{n/2}.
\]

On the other hand, $l_i(x)$ is nondegenerate with $D_{e,l_i} \leq m$ if $(d_t) \neq (0)$, then we have
\[
\left| \sum_{v \in \Gamma^*_k} \psi_{e,k}(\chi_l(v)) \right| \leq mq^{1/2} \text{ if } (d_t) \neq (0);
\]
\[
= 0 \text{ if } (d_t) = (0), \ \chi \neq \chi_0;
\]
\[
= q - 1 \text{ if } (d_t) = (0), \ \chi = \chi_0.
\]
Since the number of multiplicative characters of $\Gamma^s_{nk}$ with order $d$ is $\psi(d)$ and the number of additive characters of $p^{e-1} \tilde{\mathbb{F}}_{e,nk}$ with $R_{e,k}$-order $D$ is $\varphi_q(D)$, so we have

$$\left| \sum_{\chi \in \Gamma^s_{nk}} \sum_{(c_t) \in S} \Theta_{d,D}(c_{T,0}, \ldots, c_{T,J-1}, (c_t)_{t \neq T}, \chi) \right| \leq \begin{cases} m(m + 1)(q - 1)q^{\frac{n-1}{2}+m} & \text{if } (d_t) \neq (0); \\ (m + 1)(q - 1)q^{\frac{n}{2}+m-1} & \text{if } (d_t) = (0). \end{cases}$$

(10)

(b) Suppose that $c_{T,0} = 0$, $h(x) \neq 0$,

$$\left| \sum_{\chi \in \Gamma^s_{nk}} \sum_{(c_t) \in S} \Theta_{d,D}(0, c_{T,1}, \ldots, c_{T,J-1}, (c_t)_{t \neq T}, \chi) \right| \leq (m + 1)(q - 1)(q^m - 1)q^{n/2}. \quad (11)$$

Combining inequalities (7), (8), (9), (10) and (11), we can get inequalities (3), (4), (5), (6). This finishes the proof. □

4. Main result

Combining Eq. (2) and Proposition 12 we have

$$N_m((0), b) \geq \delta \left\{ q^n - 2^{\omega(Q) + \omega(x^n - 1)}(2m + 2)(q - 1)q^{\frac{n}{2}+m+1} \right\}$$

(12)

and when $0 \neq d_t \in R_{1,k}$ for some $t \in S_i$ and some $l = 1, 2, \ldots, e$,

$$N_m((d_t), b) \geq \delta \left\{ q^n - 2^{\omega(Q) + \omega(x^n - 1)}(m + 1)\left( m + \frac{1}{\sqrt{q}} \right)(q - 1)q^{\frac{n-1}{2}+m} \right\}.$$

(13)

where $\omega(Q)$ and $\omega(x^n - 1)$ denote the number of distinct prime factors of $Q$ and the number of distinct monic irreducible factors of $x^n - 1$ respectively.

From inequalities (12), (13) we have the following theorem.

**Theorem 13.** Let $b$ be any given primitive element of $F_q$.

1. There exists a primitive normal polynomial $f(x) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^{n-1} \sigma_{n-1} x + (-1)^n \sigma_n$ over $F_q$ with $\sigma_{n-m} = \cdots = \sigma_{n-1} = 0$ and $\sigma_n = b$ if

$$q^{\frac{n}{2}-m} > 2^{\omega(Q) + \omega(x^n - 1)} \cdot (2m + 2).$$

(14)

2. For any given $a_1, a_2, \ldots, a_m \in F_q$, $a_1, \ldots, a_m$ not all zero, there exists a primitive normal polynomial $f(x) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^{n-1} \sigma_{n-1} x + (-1)^n \sigma_n$ over $F_q$ with $\sigma_{n-m} = a_m, \ldots, \sigma_{n-1} = a_1$ and $\sigma_n = b$ if

$$q^{\frac{n-1}{2}-m} > 2^{\omega(Q) + \omega(x^n - 1)} \cdot (m + 1) \cdot \left( m + \frac{1}{\sqrt{q}} \right).$$

(15)

Following the method of Lenstra and Schoof [9] or the proof of Lemma 4.3 and Theorem 4.4 of [7], we can get
**Theorem 14.** For any given $n \geq 2$, there exists a constant $C(n)$ such that for any prime power $q > C(n)$, there exists a primitive normal polynomial of degree $n$ over $F_q$ with the last $\lfloor \frac{n}{2} \rfloor$ coefficients prescribed, where the last coefficient is a primitive element. Furthermore, the number of prescribed coefficients increases from $\lfloor \frac{n}{2} \rfloor$ to $\lfloor \frac{n+1}{2} \rfloor$ when the coefficients are specified as $(0, \ldots, 0, b)$ with $b$ any primitive element.

**References**


