PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 132, Number 1, Pages 15–31
S 0002-9939(03)07040-0
Article electronically published on May 8, 2003

p-ADIC FORMAL SERIES AND PRIMITIVE POLYNOMIALS OVER FINITE FIELDS

SHUQIN FAN AND WENBAO HAN

(Communicated by Wen-Ching Winnie Li)

ABSTRACT. In this paper, we investigate the Hansen-Mullen conjecture with the help of some formal series similar to the Artin-Hasse exponential series over p-adic number fields and the estimates of character sums over Galois rings. Given n we prove, for large enough q, the Hansen-Mullen conjecture that there exists a primitive polynomial $f(x) = x^n - a_1x^{n-1} + \cdots + (-1)^n a_n$ over F_q of degree n with the m-th $(0 < m < n)$ coefficient a_m fixed in advance except when $m = \frac{n+1}{2}$ if n is odd and when $m = \frac{n}{2}, \frac{n}{2} + 1$ if n is even.

1. INTRODUCTION

Let F_q be a finite field with $q = p^k$ elements where p is a prime number, and let k a positive integer. A monic polynomial $f(x) \in F_q[x]$ of degree n is called a primitive polynomial if the least positive integer T such that $f(x)|x^T - 1$ over $F_q[x]$ is $q^n - 1$. Hansen and Mullen [9] conjectured that with the three nontrivial exceptions

$$(q, n, m, a) = (4, 3, 1, 0), (4, 3, 2, 0), (2, 4, 2, 1),$$

there exists a primitive polynomial over F_q of degree n with the m-th $(0 < m < n)$ coefficient $a \in F_q$ fixed in advance. For $m = 1$, the Hansen-Mullen conjecture is true by the work on the existence of primitive element solutions of trace equations over finite fields, which was done by Cohen [1], Davenport [3], Jungnickel and Vanstone [11], Moreno [17], etc. For $m = 2$, Han [5, 6] proved that the Hansen-Mullen conjecture is true if

(1) q is odd and $n \geq 7$; or
(2) q is even and $(n, a) \neq (4, 0), (5, 0), (6, 0)$.

On the other hand, Han [7] discussed Cohen's Problem [2] and proved that for any positive integer $k < p$, there exists a primitive polynomial $f(x) = x^n - a_1x^{n-1} + \cdots + (-1)^n a_n$ over F_q of degree n with the first k coefficients $a_1, a_2, \cdots, a_k$ fixed in advance if $n > 2k$ and q is large enough. As a corollary, the Hansen-Mullen conjecture of the k-th $(1 \leq k < p)$ coefficient is true for q large enough and $n > 2k$. The main idea of the proof is to express the conditions on the coefficients of the primitive polynomial in terms of traces of powers of its roots.

Received by the editors March 13, 2002 and, in revised form, August 24, 2002.
2000 *Mathematics Subject Classification.* Primary 11T55, 11F85, 11L40, 11L07.
Key words and phrases. Finite field, primitive polynomial, character sums over Galois rings, p-adic formal series.
This work was supported by NSF of China with contract No. 19971096 and No. 90104035.

For $k \geq p$, however, we must cope with the inevitable problems relating to the characteristic in handling the trace conditions. In this paper, we will transfer the working to the unramified extensions of the p-adic fields and their completions, as well as the appropriate quotient rings, Galois rings where we can translate the existence of the primitive polynomial into the existence of the primitive element solution of some system of trace equations over Galois rings. To estimate the number of primitive element solutions, we need the estimates of character sums over Galois rings [10, 13] and over the Teichmüller points of p-adic number fields [15].

In this paper, we investigate the Hansen-Mullen conjecture with the help of some p-adic formal series similar to the Artin-Hasse exponential series over K_k (the unique unramified extension of $\mathbb{Q}_p$ of degree k) and the estimates of character sums over Galois rings. The paper is arranged as follows. First we give a short review on character sums over Galois rings. In Section 3, we give a description of the Hansen-Mullen conjecture over O_k (the ring of integers of K_k). Then we define a p-adic formal series $E_{t,e}(x)$ over K_k associated with the traces of powers of Teichmüller points $\xi \in \Gamma_{nk}$, the set of Teichmüller points in K_{nk}. Using Dieudonné's Theorem we prove that $E_{t,e}(x) \in O_k[[x]]$ so that we obtain a congruence connection between the traces of powers of Teichmüller points and the coefficients of the lifting primitive polynomials over O_k. In Section 4, we obtain the estimate of the number of the primitive element solutions in Γ_{nk} of some system of trace equations by using the estimates of character sums over Galois rings. In fact, we get two main results: (a) The Hansen-Mullen conjecture of the m-th $(0 < m < n)$ coefficient over F_q holds if $q^{\frac{n}{2}-(m-\left[\frac{m_1}{p}\right])} > m2^{\omega(q^n-1)}$; (b) The Hansen-Mullen conjecture of the $(n-m)$-th $(0 < m < n)$ coefficient over F_q holds if $q^{\frac{n}{2}-(m-\left[\frac{m_1}{p}\right])-1} > m2^{\omega(q^n-1)}$. In the above, $\omega(q^n-1)$ is the number of the distinct prime factors of q^n-1 and m_1 is the "non-p part" of m, i.e. m_1 is the largest divisor of m prime to p. In fact, (a) and (b) are suitable for those m such that $m \leq \frac{n}{2}$ and $m > \frac{n}{2}$, respectively. As an asymptotic result, we prove that for any given n, there exists a constant $c(n)$ such that the Hansen-Mullen conjecture over F_q of the m-th coefficient is true for $q > c(n)$ except when $m = \frac{n+1}{2}$ if n is odd and when $m = \frac{n}{2}, \frac{n}{2}+1$ if n is even.

2. Estimates of character sums over Galois rings

2.1. **p-adic number fields and Galois rings.** Let p be a prime number. For $r = \frac{a}{b} \in \mathbb{Q}$, $a, b \in \mathbb{Z}\backslash\{0\}$, define the order of $a \in \mathbb{Z}$ at p, denoted by $ord_p a$, to be the largest integer d such $p^d | a$ and $ord_p r = ord_p a - ord_p b$. The non-archimedean valuation $|\ |_p$ on $\mathbb{Q}$ can be defined by

$$\begin{cases} |0|_p = 0, \\ |r|_p = p^{-ord_p r}. \end{cases}$$

It is well known that $|\ |_p$ is a metric on $\mathbb{Q}$.

Let $\mathbb{Q}_p$ be the completion of $\mathbb{Q}$ with respect to the metric $|\ |_p$, let K_k be the unique unramified extension of $\mathbb{Q}_p$ of degree k, let $O_k = \{x \in K_k | |x|_p \leq 1\}$ be the ring of integers of K_k, let $\overline{\mathbb{Q}_p}$ be the algebraic closure of $\mathbb{Q}_p$, and let Ω be the completion of $\overline{\mathbb{Q}_p}$. Denote the set of the Teichmüller points in K_k by

$$\Gamma_k = \{\xi \in K_k |\ \xi^{p^k} = \xi\}$$

and $\Gamma_k^* = \Gamma_k \backslash \{0\}$. Then every element $\alpha \in K_k$ can be written in a unique way as

$$\alpha = \sum_{i=i_0}^{\infty} a_i p^i \quad \text{where } a_i \in \Gamma_k, i_0 \in \mathbb{Z}.$$

If $\alpha \in O_k$, we have

$$\alpha = \sum_{i=0}^{\infty} a_i p^i \quad \text{where } a_i \in \Gamma_k.$$

Define the canonical projective map ϕ from O_k to Γ_k by

$$\phi(\alpha) = a_0.$$

In fact, O_k is a local ring with unique maximal ideal $P_k = pO_k$. For $e \geq 1$, the Galois ring $R_{e,k}$ is defined by O_k/p^eO_k. In particular, when $e = 1$, $R_{e,k} = F_q$ is a finite field with $q = p^k$ elements and $F_q = \{\overline{\xi} | \xi \in \Gamma_k\}$ where $\overline{\xi}$ is the residue class mod p including ξ. It is obvious that any element $\beta \in R_{e,k}$ can be uniquely written as

$$\beta = \sum_{i=0}^{e-1} b_i p^i \quad \text{where } b_i \in \Gamma_k.$$

Let $n > 0$ be an integer and τ_k the Frobenius map of K_{nk} over K_k given by

$$\tau_k(z) = \sum_{i=i_0}^{\infty} a_i^{p^k} p^i$$

for $z = \sum_{i=i_0}^{\infty} a_i p^i \in K_{nk}$, where $a_i \in \Gamma_{nk},\ i_0 \in \mathbb{Z}$. As we know, τ_k is the generator of the Galois group of K_{nk}/K_k which is a cyclic group of order n. The trace map $Tr(\cdot) : K_{nk} \longrightarrow K_k$ is defined via

$$Tr(x) = x + \tau_k(x) + \cdots + \tau_k^{n-1}(x)$$

for $x \in K_{nk}$.

$\tau_k|_{O_{nk}} \mod p^e$ is the Frobenius map of $R_{e,nk}$ over $R_{e,k}$. Later we also use τ_k to denote $\tau_k|_{O_{nk}} \mod p^e$ without confusion. As we know, τ_k is the generator of the Galois group of $R_{e,nk}/R_{e,k}$ which is a cyclic group of order n. More precisely, we have

$$\tau_k(z) = \sum_{i=0}^{e-1} a_i^{p^k} p^i$$

for $z = \sum_{i=0}^{e-1} a_i p^i \in R_{e,nk}$, where $a_i \in \Gamma_{nk}$, $i = 0, 1, \cdots, e-1$.

The map $Tr_{e,nk,k}(\cdot) = Tr(\cdot)|_{O_{nk}} \mod p^e$ is the trace map from $R_{e,nk}$ to $R_{e,k}$. More precisely,

$$Tr_{e,nk,k}(x) = x + \tau_k(x) + \cdots + \tau_k^{n-1}(x)$$

for $x \in R_{e,nk}$.

Similarly, the norm map $Norm(\cdot)$ from K_{nk} to K_k can be defined by

$$Norm(x) = x \cdot \tau_k(x) \cdots \tau_k^{n-1}(x)$$

for $x \in K_{nk}$.

2.2. **Characters over Galois rings.** Let $e, k, n \in \mathbb{Z}_{>0}$. Now we give a few basic facts on the additive characters over Galois rings $R_{e,k}$ and multiplicative characters over Γ_{nk}^*.

2.2.1. *Additive characters over Galois rings.* An additive character of $R_{e,k}$ is a homomorphism from the additive group of $R_{e,k}$ to $\mathbb{C}^*$, the multiplicative group of a complex field. Define $\psi(c) = e^{2\pi i Tr_{e,k,1}(c)/p^e}$ for $c \in R_{e,k}$. It is easily seen that ψ is an additive character of $R_{e,k}$, that is, the so-called canonical additive character. For $a \in R_{e,k}$, define $\psi_a(c) = \psi(ac)$, $c \in R_{e,k}$. Similar to the case of finite fields, we can prove that ψ_a is also an additive character. In fact, we have

Lemma 1. *$\{\psi_a\}_{a \in R_{e,k}}$ consists of all the additive characters of $R_{e,k}$.*

Proof. It is obvious that we only need to prove $a = 0$ if and only if ψ_a is trivial, that is, a principle character. Suppose $a \neq 0$, $a = p^l u$, where $u \in R_{e,k}^*$, $0 \leq l \leq e-1$, such that $Tr_{e,k,1}(ac) = 0$ for all $c \in R_{e,k}$. We have $p^l Tr_{e,k,1}(uc) = 0$ for all $c \in R_{e,k}$, hence $p^l Tr_{e,k,1}(c) = 0$ for all $c \in R_{e,k}$. Since $Tr_{e,k,1}(\cdot) : R_{e,k} \to \mathbb{Z}_{p^e}$ is surjective, there exists $c' \in R_{e,k}$ such that $Tr_{e,k,1}(c') = 1$. This gives $p^l = 0$, a contradiction. □

Lemma 2. *Let $a \in R_{e,k}$, and let ψ be the canonical additive character of $R_{e,k}$. We have*

$$\sum_{c \in R_{e,k}} \psi_c(a) = \begin{cases} q^e & \text{if } a = 0; \\ 0 & \text{if } a \neq 0. \end{cases}$$

Proof. Special case for Theorem 5.4 in [16]. □

We have a more general result than Lemma 2.

Lemma 3. *Let $a \in R_{e,k}$, and let ψ be the canonical additive character of $R_{e,k}$. We have*

$$\sum_{c \in R_{d,k}} \psi_c(p^{e-d}a) = \begin{cases} q^d & \text{if } a = 0 \bmod p^d; \\ 0 & \text{otherwise,} \end{cases}$$

where $1 \leq d \leq e$.

2.2.2. *Multiplicative character over Teichmüller points.* By definition, Γ_{nk} is the set of Teichmüller points in K_{nk} and is independent on e. Γ_{nk}^* forms a multiplicative group with order $q^n - 1$. Let g be a primitive element (i.e. generator) of Γ_{nk}^*; the canonical multiplicative character χ can be defined by $\chi(g^l) = e^{2\pi i l/q^n - 1}$ for $0 \leq l \leq q^n - 2$. For $0 \leq j \leq q^n - 2$, define $\chi_j(g^l) = \chi(g^{lj})$. The χ_j's are all the multiplicative characters of Γ_{nk}^* and form a cyclic group with order $q^n - 1$. It is familiar that the order of each character χ_j is a divisor of $q^n - 1$.

Lemma 4. *Let n be a positive integer, $\xi \in \Gamma_{nk}^*$. Then we have*

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

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

Proof. In the following formula, γ runs through all the distinct prime factors of q^n-1:

$$\sum_{d|q^n-1}\frac{\mu(d)}{\varphi(d)}\sum_{\chi^{(d)}}\chi^{(d)}(\xi)=\prod_{\gamma|q^n-1}\left(1+\frac{\mu(\gamma)}{\varphi(\gamma)}\sum_{\chi^{(\gamma)}}\chi^{(\gamma)}(\xi)\right).$$

If ξ is a primitive element of Γ_{nk}^*, then

$$\prod_{\gamma|q^n-1}\left(1+\frac{\mu(\gamma)}{\varphi(\gamma)}\sum_{\chi^{(\gamma)}}\chi^{(\gamma)}(\xi)\right)=\prod_{\gamma|q^n-1}\left(1+\frac{1}{\varphi(\gamma)}\right)=\frac{q^n-1}{\varphi(q^n-1)}.$$

Otherwise, there exists a prime number $\gamma \mid \frac{q^n-1}{\mathrm{order}(\xi)}$ so that $\sum\limits_{\chi^{(\gamma)}}\chi^{(\gamma)}(\xi)=\varphi(\gamma)$, hence

$$\prod_{\gamma|q^n-1}\left(1+\frac{\mu(\gamma)}{\varphi(\gamma)}\sum_{\chi^{(\gamma)}}\chi^{(\gamma)}(\xi)\right)=0.$$

□

2.3. **Estimates of character sums over Galois rings.** Let $k,n\geq 1$, and let $h(x)$ be a polynomial over $R_{e,nk}$ with $h(0)=0$ and $h(x)$ not identically 0. Let

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

be the p-adic expansion of $h(x)$. Such an expansion can be derived from a p-adic expansion of the coefficients of $h(x)$. Let d_i be the degree of $h_i(x)$ and let

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

$h(x)$ is called *nondegenerate* if the coefficients $h_{i,j}$ of $h_i(x)$ satisfy

$$h_{i,j}=0,\quad if\ j\equiv 0(\mathrm{mod}\,p), 0\leq j\leq d_i, 0\leq i\leq e-1.$$

Define *the weighted e-degree* of $h(x)$ by

$$D_e(h(x))=\max(d_0p^{e-1},d_1p^{e-2},\cdots,d_{e-1}).$$

Various kinds of character sums over Galois rings are investigated; see for example [10], [15], etc. Here we give two theorems from [15] in a little different form for our later use. These results are analogous to Weil estimates on character sums over finite fields.

Theorem 5 ([13], [15])**.** *Let $f(x)\in R_{e,nk}[x]$ be nondegenerate with weighted e-degree $D_e(f(x))$, and let $\psi_{e,n}$ be a nontrivial additive character of $R_{e,nk}$. Then*

$$|\sum_{\xi\in\Gamma_{nk}}\psi_{e,n}(f(\xi))|\leq(D_e(f(x))-1)q^{n/2}.$$

For twisted character sums, we have

Theorem 6 ([15])**.** *Let $f(x)\in R_{e,nk}[x]$ be nondegenerate with weighted e-degree $D_e(f(x)),\psi_{e,n}$ a nontrivial additive character of $R_{e,nk}$ and χ a nontrivial multiplicative character of Γ_{nk}^*. Then*

$$|\sum_{\xi\in\Gamma_{nk}^*}\psi_{e,n}(f(\xi))\chi(\xi)|\leq D_e(f(x))q^{n/2}.$$

3. Hansen-Mullen conjecture over p-adic number fields

Throughout this section, $q = p^k, e \in \mathbb{Z}_{>0}$.

Let $\widetilde{f}(x) \in O_k[x]$ be a monic polynomial of degree n. We call $\widetilde{f}(x)$ a basic irreducible polynomial over O_k if $\widetilde{f}(x) \mod p$ is irreducible over F_q.

Definition 7. Let $\widetilde{f}(x) \in O_k[x]$ be a basic irreducible polynomial of degree n. We call $\widetilde{f}(x)$ a lifting primitive polynomial over O_k if there exists a positive integer T such that $\widetilde{f}(x)|x^T - 1$ and the least positive integer $T = q^n - 1$.

In fact, the set of primitive elements of Γ_{nk}^* (all the generators of Γ_{nk}^* as a cyclic multiplicative group) is the same as the set of roots (in O_{nk}) of lifting primitive polynomials of degree n in $O_k[x]$. So in the rest of the paper, we will identify them without explanation.

If $\widetilde{f}(x)$ is a lifting primitive polynomial of $O_k[x]$, it is easily seen that $f(x) = \widetilde{f}(x) \mod p$ is a primitive polynomial over F_q. On the other hand, if $f(x)$ is a primitive polynomial over F_q, by the Hensel Lemma there is a polynomial $\widetilde{f}(x) \in O_k[x]$ such that $f(x) \equiv \widetilde{f}(x) \mod p$ and $\widetilde{f}(x)$ is a lifting primitive polynomial over O_k.

By the discussions above, the coefficients of primitive polynomials over F_q and the lifting primitive polynomials over O_k are closely related. Now we reformulate the Hansen-Mullen conjecture using O_k.

Hansen-Mullen conjecture over O_k. Let $q = p^k$. For any given $a \in \Gamma_k$, with the three nontrivial exceptions

$$(q, n, m, a) = (4, 3, 1, 0), (4, 3, 2, 0), (2, 4, 2, 1),$$

there exists a lifting primitive polynomial $f(x)$ over O_k of degree n with the m-th $(0 < m < n)$ coefficient a_m fixed in advance such that $\phi(a_m) = a$, where ϕ is the canonical projective map from O_k to $R_{1,k} = F_q$.

So we only need to consider the existence of the lifting primitive polynomials over O_k. As in [5, 6, 7], we want to express the conditions on the coefficients of a primitive polynomial over F_q in terms of traces of the powers of the roots in an extension field of F_q of the primitive polynomial. To cope with the inevitable problems relating to the characteristic in handling the trace conditions, the work is transferred to the unramified extensions of the p-adic field and their completions, as well as the appropriate quotient rings, Galois rings.

For this reason, we investigate the relation between the coefficients of the lifting primitive polynomial over p-adic number field K_k and the traces of the powers of the roots, in the extension field K_{nk}, of the lifting primitive polynomial and reducing the formula associated to the coefficients and the roots modulo suitable p^e.

Lemma 8 ([12])**.** *Let A be an $n \times n$ matrix with entries in Ω. We have the following identity of formal power series in $\Omega[x]$:*

$$\det(1 - Ax) = \exp(-\sum_{s=1}^{\infty} Tr(A^s)x^s/s) \tag{1}$$

where $Tr(A^s)$ is the trace of matrix A^s, $s = 1, 2, \cdots$.

Let $\widetilde{f}(x)$ be a lifting primitive polynomial of degree n over O_k. Now we give the relation between the coefficients of lifting primitive polynomial $\widetilde{f}(x)$ over p-adic number field K_k and the traces of the powers of the roots of $\widetilde{f}(x)$ in the extension

field K_{nk}. It is easy to see that if ξ is a root of $\widetilde{f}(x)$ in Ω, then $\xi, \xi^q, \cdots, \xi^{q^{n-1}}$ are all the roots of $\widetilde{f}(x)$ in Ω.

Lemma 9. *Let $\widetilde{f}(x) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n \in O_k[x]$ be a lifting primitive polynomial of degree n, and let ξ be a root of $\widetilde{f}(x)$ in Ω. We have*

$$x^n \widetilde{f}(\frac{1}{x}) = \exp(-\sum_{s=1}^{\infty} Tr(\xi^s) x^s / s). \tag{2}$$

Proof. Let $A = (a_{ij})_{1 \le i \le n, 1 \le j \le n}$, where

$$a_{ij} = \begin{cases} 0 & \text{if } i \neq j; \\ \xi^{q^{i-1}} & \text{if } i = j. \end{cases}$$

Expanding the left-hand and right-hand sides of (1), respectively, we get (2). □

Now we go back to the Hansen-Mullen conjecture and discuss the relation between the existence of lifting primitive polynomials of degree n over O_k with the m-th coefficient fixed for $1 \le m \le n-1$, $m = p^{e-1} m_1$, $(m_1, p) = 1$ and the existence of primitive element solutions in Γ_{nk}^* of some kind of system of trace equations, that is:

$$\begin{cases} Tr(x^t) = 0 & \mod p^e, \\ \text{if } 1 \le t < m_1,\ (t,p) = 1, & \\ & \\ Tr(x^t) = 0 & \mod p^{e-l}, \\ \text{if } m_1 p^{l-1} < t < m_1 p^l,\ (t,p) = 1, l = 1, \cdots, e-1, & \\ & \\ Tr(x^{m_1}) = p^{e-1} a, & \mod p^e, \end{cases} \tag{3}$$

where $Tr(\cdot)$ is the trace from K_{nk} to K_k, $a \in \Gamma_k$.

Theorem 10. *Let $a \in \Gamma_k, m = p^{e-1} m_1, (m_1, p) = 1$ and $e \ge 1$. Let*

$$\begin{aligned} \widetilde{f}(x) &= (x-\xi)(x-\xi^q)\cdots(x-\xi^{q^{n-1}}) \\ &= x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n \end{aligned}$$

be the minimal polynomial of ξ over O_k where the system of equations (3) is assumed to have a primitive element solution $\xi \in \Gamma_{nk}^*$. For $1 \le m \le n$, we have

$$\sigma_m \equiv (-1)^{m-1} m_1^{-1} a^{p^{e-1}} \mod p.$$

Proposition 11. *If the system of equations (3) has one primitive element solution $\xi \in \Gamma_{nk}^*$ for any given $a \in \Gamma_k$, the Hansen-Mullen conjecture is true for the m-th coefficient.*

Proof. By Theorem 10, $\phi(\sigma_m)$ runs across Γ_k if a runs through Γ_k. □

Since the reciprocal polynomial of a (lifting) primitive polynomial over F_q (or O_k) is also a (lifting) primitive polynomial, then, if there exists a (lifting) primitive polynomial over F_q (or O_k) with the m-th coefficient fixed and the constant term fixed as a primitive element b in Γ_k, there exists a primitive polynomial with $(n-m)$-th coefficient fixed. So we consider another system of equations with the constant

term fixed:

$$
(4)\quad \begin{cases} Tr(x^t)=0 & \mod p^e,\\ \text{if } 1\le t<m_1,\ (t,p)=1,\\ \\ Tr(x^t)=0 & \mod p^{e-l},\\ \text{if } m_1p^{l-1}<t<m_1p^l,\ (t,p)=1,\ l=1,\cdots,e-1,\\ \\ Tr(x^{m_1})=p^{e-1}a, & \mod p^e,\\ \\ Norm(x)=b. \end{cases}
$$

Proposition 12. *Let b be a primitive element of Γ_k. If the system of equations (4) has one primitive element solution $\xi\in\Gamma_{nk}^*$ for any given $a\in\Gamma_k$, the Hansen-Mullen conjecture is true for the $(n-m)$-th coefficient.*

Proof. Let $\xi\in\Gamma_{nk}^*$ be a primitive element solution of (4), $f(x)$ the minimal polynomial of ξ over O_k and σ_m the m-th coefficient of $f(x)$. Then $\frac{1}{b}x^nf(\frac{1}{x})$ is a lifting primitive polynomial over O_k and the $(n-m)$-th coefficient of $\frac{1}{b}x^nf(\frac{1}{x})$ is $\frac{\sigma_m}{b}$. By Theorem 10, $\phi(\frac{\sigma_m}{b})$ runs across Γ_k if a runs through Γ_k. So we finish the proof of the Hansen-Mullen conjecture for the $(n-m)$-th coefficient. □

Before we prove Theorem 10, we give a simple result.

Lemma 13. *Let $(t,p)=1$ and $\hat{\xi}\in\Gamma_{nk}$. We have*

$$Tr(\hat{\xi}^{tp^i})=\tau^i(Tr(\hat{\xi}^t))$$

where τ^i is the Frobenius map of K_k over Q_p for $i=0,1,\cdots$.

To prove Theorem 10, we define, for later use, a formal series over K_k similar to the Artin-Hasse exponential series associated with the trace of power of $\xi\in\Gamma_{nk}^*$, that is,

$$
(5)\qquad E_{t,e}(x)=\exp\left(-\sum_{s=e}^{\infty}\frac{Tr(\xi^{tp^s})x^{tp^s}}{tp^s}\right)
$$

where $t,e\in\mathbb{Z}_{\ge0}$ and $(t,p)=1$. Later we use E_t to denote $E_{t,0}$. We want to discuss the p-adic property of the coefficients of $E_{t,e}(x)$ under some conditions. Now we give Dieudonné's Theorem as a lemma.

Lemma 14 (Dieudonné's Theorem)**.** *Let $f(x)=1+a_1x+a_2x^2+\cdots\in1+xK_k[[x]]$. Then*

$$f(x)\in1+xO_k[[x]]$$

if and only if

$$
(6)\qquad \frac{f(x)^p}{f^\tau(x^p)}\in1+pxO_k[[x]]
$$

where τ is the Frobenius map of K_k over Q_p.

Lemma 15. *Let $t,e\ge1$ be positive integers satisfying $(t,p)=1$, and let ξ be a primitive element of Γ_{nk}^* such that $Tr(\xi^t)\equiv0$ mod p^e. Then we have*

$$E_{t,e}(x)\in1+xO_k[[x]].$$

Proof. Consider

$$\begin{aligned} E_{t,e}(x)^p &= \exp(-p\sum_{s=e}^{\infty}\frac{Tr(\xi^{tp^s})}{tp^s}x^{\ tp^s}) \\ &= \exp(-p\frac{Tr(\xi^{tp^e})}{tp^e}x^{tp^e} - p\sum_{s=e+1}^{\infty}\frac{Tr(\xi^{tp^s})}{tp^s}x^{\ tp^s}) \end{aligned}$$

and

$$\begin{aligned} E^{\tau}_{t,e}(x^p) &= \exp(-\sum_{s=e}^{\infty}\frac{Tr(\xi^{tp^{s+1}})}{tp^s}x^{\ tp^{s+1}}) \\ &= \exp(-p\sum_{s=e+1}^{\infty}\frac{Tr(\xi^{tp^s})}{tp^s}x^{\ tp^s}). \end{aligned}$$

Therefore

$$\frac{E_{t,e}(x)^p}{E^{\tau}_{t,e}(x^p)} = \exp(-p\frac{Tr(\xi^{tp^e})}{tp^e}x^{tp^e}) \in 1 + pxO_k[[x]].$$

By Dieudonné's Theorem, we have

$$E_{t,e}(x) \in 1 + xO_k[[x]].$$

□

Lemma 16. *Let $t, e \geq 1$ be positive integers satisfying $(t,p) = 1$, and let ξ be a primitive element of Γ^*_{nk} such $Tr(\xi^t) \equiv 0$ mod p^e. Let*

$$E_t(x) = 1 + a_1x + \cdots + a_lx^l + \cdots.$$

Then we have

$$a_l \in pO_k \quad \text{if } p^e \nmid l.$$

More precisely

$$E_t(x) \equiv E_{t,e}(x) \mod p.$$

Proof. We rewrite $E_t(x)$ as

$$E_t(x) = \exp(-\sum_{s=e}^{\infty}\frac{Tr(\xi^{tp^s})}{tp^s}x^{tp^s})\prod_{i=0}^{e-1}\exp(-\frac{Tr(\xi^{tp^i})}{tp^i}x^{tp^i}).$$

Since the first term (i.e., $E_{t,e}(x)$) is in $1 + xO_k[[x]]$ and the second product of the right-hand side belongs to $1 + pxO_k[[x]]$, the only possible terms a_l such that $a_l \notin pO_k$ are the terms in the expansion of $E_{t,e}(x)$. So we must have $p^e|l$. □

Now we come back to prove Theorem 10.

Proof of Theorem 10. By Lemma 9, we have

$$\begin{aligned} x^n\ \widetilde{f}(\frac{1}{x}) &= \exp(-\sum_{s=1}^{\infty} Tr(\xi^s)x^s/s) \\ &= \prod_{\substack{(t,p)=1\\ t>0}} E_t(x) = \prod_{\substack{(t,p)=1\\ t\le m}} E_t(x) \prod_{\substack{(t,p)=1\\ t>m}} E_t(x) \\ &= \prod_{\substack{(t,p)=1\\ t\le m_1}} E_t(x) \prod_{l=1}^{e-1} \prod_{\substack{(t,p)=1\\ m_1p^{l-1}<t<m_1p^l}} E_t(x) \prod_{\substack{(t,p)=1\\ t>m}} E_t(x). \end{aligned}$$

Then by Lemma 16

$$\begin{aligned} x^n\widetilde{f}(\frac{1}{x}) = E_{m_1,e-1}(x) \prod_{\substack{(t,p)=1\\ t<m_1}} E_{t,e}(x) \prod_{l=1}^{e-1} \prod_{\substack{(t,p)=1\\ m_1p^{l-1}<t<m_1p^l}} \\ \times E_{t,e-l}(x) \prod_{\substack{(t,p)=1\\ t>m}} E_t(x) \mod p. \end{aligned}$$

It is obvious that the degrees of the nonconstant terms in

$$\prod_{\substack{(t,p)=1\\ m_1p^{l-1}<t<m_1p^l}} E_{t,e-l}(x)$$

for $l = 1, \cdots, e-1$ and in

$$\prod_{\substack{(t,p)=1\\ t>m}} E_t(x)$$

are greater than m, hence the coefficient of x^m in $x^n\widetilde{f}(\frac{1}{x}) \mod p$ is same as the coefficient of x^m in

$$H(x) = E_{m_1,e-1}(x) \prod_{\substack{0<t<m_1\\ (t,p)=1}} E_{t,e}(x) \mod p.$$

Since there exists a formal series $G(x) \in O_k[[x]]$ such that

$$G(x^{p^e}) = \prod_{\substack{0<t<m_1\\ (t,p)=1}} E_{t,e}(x)$$

and $m = m_1p^{e-1}$, the coefficient of x^m in $H(x)$ is the same as the coefficient of x^m in $E_{m_1,e-1}(x)$. By observing that the coefficient of x^m in $E_{m_1,e-1}(x)$ is $-\frac{Tr(\xi^m)}{m}$, we have

$$(-1)^m\sigma_m \equiv -\frac{Tr(\xi^m)}{m} \mod p.$$

As a result, we have

$$\sigma_m \equiv (-1)^{m-1}m_1^{-1}a^{p^{e-1}} \mod p.$$

□

In the next section we will estimate the number of primitive element solutions of Γ_{nk}^* in (3) and (4).

4. Estimates and calculations

Now we estimate the number of primitive element solutions of (3) and (4) in Γ_{nk}^*, respectively. For this reason, we define

$$S_l = \{t | p^{l-1}m_1 < t < p^l m_1 \text{ and } (t,p) = 1\} \tag{7}$$

for $l = 1, 2, \cdots, e-1$ and

$$S_0 = \{t | 1 \le t \le m_1, (t,p) = 1\}, \tag{8}$$

$$\mathbb{S} = \{(c_t)_{(t,p)=1} |\ c_t \in R_{e-l,k} \text{ for } t \in S_l, l = 0, 1, \cdots, e-1\}.$$

Let $W = \#\mathbb{S}$. We have $W = q^{\sum_{l=0}^{e-1}(e-l)\#S_l}$.

Let N be the number of primitive element solutions of (3) in Γ_{nk}^*, ψ the canonical additive character of $R_{e,k}$, $\psi_{e,n} = \psi \cdot Tr_{e,nk,k}$ the canonical additive character of $R_{e,nk}$ and $\chi^{(d)}$ run through all the multiplicative character over Γ_{nk}^* with order d. From Lemmas 2, 3 and 4,

$$\begin{aligned} N &= \delta \sum_{\xi \in \Gamma_{nk}^*} \Big(\prod_{l=0}^{e-1} \prod_{\substack{t \in S_l \\ t \neq m_1}} \sum_{c_t \in R_{e-l,k}} \psi(p^l c_t Tr(\xi^t))\Big) \\ &\quad \times \Big(\sum_{c_{m_1} \in R_{e,k}} \psi(c_{m_1}(Tr(\xi^{m_1}) - p^{e-1}a))\Big) \sum_{d | q^n - 1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \chi^{(d)}(\xi) \\ &= \delta \sum_{d | q^n - 1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \sum_{(c_t)_{(t,p)=1} \in \mathbb{S}} \psi(-p^{e-1} c_{m_1} a) \\ &\quad \times \Lambda((c_t)_{(t,p)=1}, \chi^{(d)}), \end{aligned}$$

where

$$\delta = \frac{\varphi(q^n - 1)}{(q^n - 1)} q^{-\sum_{l=0}^{e-1}(e-l)\#S_l}$$

and

$$\Lambda((c_t)_{(t,p)=1}, \chi^{(d)}) = \sum_{\xi \in \Gamma_{nk}^*} \chi^{(d)}(\xi) \psi_{e,n}\Big(\sum_{l=0}^{e-1} p^l \sum_{t \in S_l} c_t \xi^t\Big)$$

where $(c_t)_{(t,p)=1} \in \mathbb{S}$.

Denote

$$h(x) = \sum_{l=0}^{e-1} p^l \sum_{t \in S_l} c_t x^t.$$

It is easy to check that $h(x)$ is nondegenerate if $h(x) \neq 0$. So

$$\Lambda((c_t)_{(t,p)=1}, \chi^{(d)}) = \sum_{\xi \in \Gamma_{nk}^*} \chi^{(d)}(\xi) \psi_{e,n}(h(x)).$$

Now we estimate N.

(1) Suppose $h(x) = 0$. Then $c_t = 0 \in R_{e-l,k}$ for $t \in S_l$, where $l = 0, 1, \cdots, e-1$. So

$$\psi(p^{e-1} c_{m_1} a) = 1.$$

(a) When $d = 1$, $\frac{\mu(d)}{\varphi(d)} = 1$ and

$$\Lambda((c_t)_{(t,p)=1}, \chi^{(d)}) = q^n - 1.$$

(b) When $d > 1$,

$$\Lambda((c_t)_{(t,p)=1}, \chi^{(d)}) = 0.$$

We have

$$\sum_{d|q^n-1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \sum_{h(x)=0} \psi(p^{e-1}c_{m_1}a) \times \Lambda((c_t)_{(t,p)=1}, \chi^{(d)})) = q^n - 1.$$

(2) Suppose $h(x) \neq 0$. Then $c_t \neq 0$ for some $t \in S_l$ and some l such that $0 \leq l \leq e-1$. In this case $h(x)$ is nondegenerate.

(a) When $d = 1$, by Theorem 5

$$\begin{aligned} |\Lambda((c_t)_{(t,p)=1}, \chi^{(1)})| &\leq (D_e(h(x)) - 1)q^{n/2} + 1 \\ &\leq D_e(h(x))q^{n/2}. \end{aligned}$$

(b) When $d \neq 1$, by Theorem 6

$$|\Lambda((c_t)_{(t,p)=1}, \chi^{(d)})| \leq D_e(h(x))q^{n/2}.$$

In the above $D_e(h(x))$ is the weighted degree of $h(x)$ and $D_e(h(x)) \leq m$.
Since the total number of multiplicative characters $\chi^{(d)}$ is $\varphi(d)$, we get

$$N \geq \delta \Big\{ (q^n - 1) - 2^{\omega(q^n-1)}(W-1)mq^{\frac{n}{2}} \} \tag{9}$$

where $\omega(q^n - 1)$ is the number of the distinct prime factors of $q^n - 1$.

Lemma 17. *Let $m = p^{e-1}m_1, (m_1, p) = 1$. Let*

$$\theta_{m_1,e} = \sum_{l=0}^{e-1} (e-l)\#S_l$$

where S_l are defined by (7) *and* (8). *Then*

$$\theta_{m_1,e} = m - [\frac{m_1}{p}],$$

so $\theta_{m_1,e} = m$ if and only if $m_1 < p$.

Proof. By definition of S_l, we have

$$\begin{aligned} \#S_0 &= m_1 - [\frac{m_1}{p}], \\ \#S_1 &= m_1 p - m_1 - \#S_0 \\ &= m_1 p - 2m_1 + [\frac{m_1}{p}]; \end{aligned}$$

if $1 < l < e$, then

$$\begin{aligned} \#S_l &= m_1 p^l - m_1 p^{l-1} - (m_1 p^{l-1} - m_1 p^{l-2}) \\ &= m_1 p^l - 2m_1 p^{l-1} + m_1 p^{l-2}. \end{aligned}$$

It is easily check that Lemma 17 holds for $e \leq 2$. Let $e > 2$; we use induction on e. Therefore

$$\begin{aligned}
\theta_{m_1,e+1} &= \sum_{l=0}^{e}(e+1-l)\#S_l \\
&= \sum_{l=0}^{e-1}(e-l)\#S_l + \sum_{l=0}^{e}\#S_l \\
&= \theta_{m_1,e} + m_1 - [\frac{m_1}{p}] + m_1 p - 2m_1 + [\frac{m_1}{p}] \\
&\quad + \sum_{l=2}^{e}(m_1 p^l - 2m_1 p^{l-1} + m_1 p^{l-2}) \\
&= \theta_{m_1,e} - m_1 p^{e-1} + m_1 p^e
\end{aligned}$$

and $m_1 p^e - \theta_{m_1,e+1} = m_1 p^{e-1} - \theta_{m_1,e}$. By induction hypothesis on e, that is, $m_1 p^{e-1} - \theta_{m_1,e} = [\frac{m_1}{p}]$, we have $\theta_{m_1,e+1} = m_1 p^e - [\frac{m_1}{p}]$. The second conclusion is obvious. So we finish the proof of Lemma 17. □

Theorem 18. *Let N be the number of primitive element solutions of (3) in Γ^*_{nk}. For $0 < m < n$, let $m = p^{e-1}m_1, (m_1, p) = 1$. If*

$$q^{\frac{n}{2}-(m-[\frac{m_1}{p}])} > m2^{\omega(q^n-1)} \tag{10}$$

where $\omega(q^n-1)$ is the number of the distinct prime factors of q^n-1, then $N > 0$.

Proof. By (9) and Lemma 17, it is easily seen that $N > 0$ if

$$\begin{aligned}
q^{\frac{n}{2}} &> m2^{\omega(q^n-1)}q^{\sum_{l=0}^{e}(e-l)\#S_l} \\
&= m2^{\omega(q^n-1)}q^{m-[\frac{m_1}{p}]}.
\end{aligned}$$

Hence our theorem holds. □

Following the method introduced by Lenstra and Schoof [14], for given positive integer n and prime number p , if $m - \left[\frac{m_1}{p}\right] < \frac{n}{2}$, inequality (10) holds for q large enough, where q is the power of p. Therefore we prove

Proposition 19. *Let n be a positive integer, p a prime number and q a power of p. For $0 < m < n$, let $m = p^{e-1}m_1, (m_1, p) = 1$. If $m - \left[\frac{m_1}{p}\right] < \frac{n}{2}$, there exists a constant $c(n, m, p)$ depending on n, m, p such that there exists a primitive polynomial over F_q of degree n with the m-th coefficient fixed in advance if $q > c(n, m, p)$.*

Similary we have

Proposition 20. *Let n be a positive integer. If $m < \frac{n}{2}$, there exists a constant $c(n, m)$ depending on n, m such that there exists a primitive polynomial over F_q of degree n with the m-th coefficient fixed in advance if $q > c(n, m)$.*

From Proposition 20, for large enough q, the Hansen-Mullen conjecture is true for those terms x^{n-m} such that $m \leq \frac{n}{2}$ except when $m = \frac{n}{2}$ if n is even. But for the terms x^{n-m} such that $m > \frac{n}{2}$, the above estimate (10) gives no information in most cases. However, we can consider the reciprocal polynomial of a primitive polynomial since the reciprocal polynomial of a primitive polynomial is still a primitive polynomial. We hope that we can prove the Hansen-Mullen conjecture of the

m-th coefficient for $m > \frac{n}{2}$ in most cases if q is large enough. In this way we can establish the Hansen-Mullen conjecture of the m-th coefficient with only possibly one or two exceptions, that is, those terms x^{n-m} such that m is around $\frac{n}{2}$. In fact, the $(n-m)$-th coefficient can be fixed if the m-th coefficient and the constant term can be fixed at the same time.

For this reason, we estimate the number of primitive element solution of (4), which we denote by N'.

Let $\psi, \psi_{e,n}, \chi^{(d)}$ be defined as before, and let $\chi_{e,n}$ be the multiplicative character over Γ_{nk} defined by $\chi_{e,n} = \chi \cdot Norm$. We have

$$\begin{aligned} N' &= \delta \sum_{\xi \in \Gamma_{nk}^*} \Big(\prod_{l=0}^{e-1} \prod_{\substack{t \in S_l \\ t \neq m_1}} \sum_{c_t \in R_{e-l,k}} \psi(p^l c_t Tr(\xi^t)) \\ &\quad \times \Big(\sum_{c_{m_1} \in R_{e,k}} \psi(c_{m_1}(Tr(\xi^{m_1}) - p^{e-1}a))\Big) \\ &\quad \times \sum_{\chi} \chi\Big(\frac{Norm(\xi)}{b}\Big) \sum_{d|q^n-1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \chi^{(d)}(\xi) \\ &= \delta \sum_{\chi} \chi\Big(\frac{1}{b}\Big) \sum_{d|q^n-1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \sum_{(c_t)_{(t,p)=1} \in \mathbb{S}} \psi(-p^{e-1} c_{m_1} a) \\ &\quad \times \Lambda((c_t)_{(t,p)=1}, \chi^{(d)}, \chi_{e,n}). \end{aligned}$$

In the above, χ run across all the multiplicative characters over T_k^*,

$$\delta = \frac{1}{(q-1)} \frac{\varphi(q^n-1)}{(q^n-1)} q^{-\sum_{l=0}^{e-1}(e-l)\#S_l}$$

and

$$\Lambda((c_t)_{(t,p)=1}, \chi^{(d)}, \chi_{e,n}) = \sum_{\xi \in \Gamma_{nk}^*} (\chi^{(d)} \cdot \chi_{e,n})(\xi) \psi_{e,n}(h(\xi))$$

where $(c_t)_{(t,p)=1} \in \mathbb{S}$ and $h(x)$ is defined as before.

Now we estimate N'.

(1) Suppose $h(x) \neq 0$. Then $c_t \neq 0$ for some $t \in S_l$ and some l such that $0 \leq l \leq e-1$. From Theorems 5 and 6,

$$\Big|\Lambda((c_t)_{(t,p)=1}, \chi^{(d)}, \chi_{e,n})\Big| \leq D_e(h(x)) \cdot q^{\frac{n}{2}},$$

and since the number of the multiplicative characters with order d is $\varphi(d)$,

$$\begin{aligned} &|\sum_{\chi} \chi\Big(\frac{1}{b}\Big) \sum_{d|q^n-1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \sum_{h(x)\neq 0} \psi(-p^{e-1} c_{m_1} a) \cdot \Lambda((c_t)_{(t,p)=1}, \chi^{(d)}, \chi_{e,n})| \\ &\leq (q-1) \cdot 2^{\omega(q^n-1)} \cdot (q^{m - \lfloor \frac{m_1}{p} \rfloor} - 1) \cdot D_e(h(x)) \cdot q^{\frac{n}{2}}. \end{aligned}$$

(2) Suppose $h(x) = 0$. Then $c_t = 0 \in R_{e-l,k}$ for $t \in S_l$, where $l = 0, 1, \cdots, e-1$.

(a) When $\chi^{(d)} \cdot \chi_{e,n} = \chi_0$,

$$\psi(p^{e-1} c_{m_1} a) = 1$$

and

$$\Lambda((c_t)_{(t,p)=1}, \chi^{(d)}, \chi_{e,n}) = q^n - 1.$$

Let $\chi_{e,n}^{-1}$ be the multiplicative character such that $\chi_{e,n}^{-1} \cdot \chi_{e,n} = \chi_0$; we have $order(\chi) = order(\chi_{e,n}) = order(\chi_{e,n}^{-1})$. Let $\chi_{(d_1)}$ be the multiplicative character χ over Γ_k with order d_1; we have

$$\sum_{\chi} \chi(\frac{1}{b}) \sum_{d|q^n-1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi_{e,n}\cdot\chi^{(d)}=\chi_0} \sum_{h(x)=0} \psi(-p^{e-1}c_{m_1}a) \cdot \Lambda((c_t)_{(t,p)=1}, \chi^{(d)}, \chi_{e,n})$$
$$= \sum_{d_1|q-1} \frac{\mu(d_1)}{\varphi(d_1)} \sum_{\chi_{(d_1)}} \chi_{(d_1)}(\frac{1}{b})(q^n-1) = \frac{q-1}{\varphi(q-1)}(q^n-1)$$

where the last equation holds since $\frac{1}{b}$ is a primitive element.

(b) When $\chi^{(d)} \cdot \chi_{e,n} \neq \chi_0$,

$$\Lambda((c_t)_{(t,p)=1}, \chi^{(d)}, \chi_{e,n}) = 0$$

and

$$\sum_{\chi} \chi(\frac{1}{b}) \sum_{d|q^n-1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi_{e,n}\cdot\chi^{(d)}\neq\chi_0} \sum_{h(x)=0} \psi(-p^{e-1}c_{m_1}a)$$
$$\cdot \Lambda((c_t)_{(t,p)=1}, \chi^{(d)}, \chi_{e,n}) = 0.$$

Therefore

$$N' \geq \delta \cdot (\frac{q-1}{\varphi(q-1)}(q^n-1) - (q-1) \cdot 2^{\omega(q^n-1)} \cdot (q^{m-\lfloor \frac{m_1}{p} \rfloor} - 1) \cdot D_e(h(x)) \cdot q^{\frac{n}{2}}).$$

If

$$q^{\frac{n}{2}-(m-\lfloor \frac{m_1}{p} \rfloor)} > \varphi(q-1) \cdot m \cdot 2^{\omega(q^n-1)},$$

even stronger, if

$$q^{\frac{n}{2}-(m-\lfloor \frac{m_1}{p} \rfloor)-1} > m \cdot 2^{\omega(q^n-1)},$$

we have $N' > 0$. So we have

Theorem 21. *Let N' be the number of primitive element solutions of (4) in Γ_{nk}^*. For $0 < m < n$, let $m = p^{e-1}m_1, (m_1, p) = 1$. If*

$$q^{\frac{n}{2}-\left(m-\left[\frac{m_1}{p}\right]\right)-1} > m \cdot 2^{\omega(q^n-1)} \tag{11}$$

where $\omega(q^n-1)$ is the number of the distinct prime factors of q^n-1, then $N' > 0$.

Again by the method of Lenstra and Schoof, for given n and prime number p, if $m - \left[\frac{m_1}{p}\right] < \frac{n}{2} - 1$, there exists a constant $c(n,m,p)$ depending on n, m, p such that there exists a primitive polynomial over F_q of degree n with the m-th coefficient fixed as any element in F_q and the constant term fixed as any primitive element in F_q in advance for $q > c(n,m,p)$, where q is the power of p. Considering the reciprocal polynomial of primitive polynomial, we can give the following

Proposition 22. *Let n be a positive integer, p a prime number and q power of p. For $0 < m < n$, if $(m - \left\lfloor \frac{m_1}{p} \right\rfloor) < \frac{n}{2} - 1$, there is a constant $c(n,m,p)$ depending on n, m, p such that there exists a primitive polynomial over F_q of degree n with the $(n-m)$-th coefficient fixed in advance if $q > c(n,m,p)$.*

We can also get

Proposition 23. *Let n be a positive integer and $\frac{n}{2} < m < n$. If $\frac{n}{2} + 1 < m$, there exists a constant $c(n, m)$ depending on n, m such that there exists a primitive polynomial over F_q of degree n with the m-th coefficient fixed in advance if $q > c(n, m)$.*

Now we give our two main results of this paper.

Theorem 24. *Let n be a positive integer, p a prime number and q a power of p. Let n_1 be the "non-p part" of $\frac{n}{2}$ if n is even and the "non-p part" of $\frac{n-1}{2}$ if n is odd. There exists a constant $c(n, p)$ depending on n, p such that the Hansen-Mullen conjecture over F_q of the m-th $(0 < m < n)$ coefficient of primitive polynomial with degree n is true for $q > c(n, p)$ except when:*

(1) *$m = \frac{n+1}{2}$ if n is odd, $n_1 < p$;*
(2) *$m = \frac{n}{2}, \frac{n}{2} + 1$ if n is even, $n_1 < p$.*

Proof. We first prove the case of odd n. From Proposition 19 there exists a constant $c(n, m, p)$ such that for every $1 \leq m < \frac{n}{2}$ there exists a primitive polynomial of degree n with the m-th coefficient over F_q if $q > c(n, m, p)$. By Proposition 22, for every pair (n, m, p) such that $\frac{n}{2} < m < n$ when $n_1 \geq p$ and $\frac{n}{2} + 1 < m \leq n - 1$ when $n_1 < p$, there exists a constant $c(n, m, p)$ such that there exists a primitive polynomial over F_q of degree n with the m-th coefficient fixed as any element in F_q if $q > c(n, m, p)$. If $n_1 < p$, let

$$c(n, p) = \max_{\substack{0<m<n \\ m \neq \frac{n+1}{2}}} c(n, m, p)$$

and if $n_1 > p$, let

$$c(n, p) = \max_{0<m<n} c(n, m, p).$$

Then the Hansen-Mullen conjecture over F_q of the m-th $(0 < m < n)$ coefficient of primitive polynomial with degree n is true for $q > c(n, p)$ except when $m = \frac{n+1}{2}$ if n is odd and $n_1 < p$.

The proof of even n is similar. So we have completed the proof. □

We give still another theorem:

Theorem 25. *Let n be a positive integer. There is a constant $c(n)$ depending on n such that there exists a primitive polynomial of degree n over F_q with the m-th $(0 < m < n)$ coefficient fixed in advance for $q > c(n)$ except when $m = \frac{n+1}{2}$ if n is odd and when $m = \frac{n}{2}, \frac{n}{2} + 1$ if n is even.*

Proof. From Propositions 20 and 23 we can easily obtain the proof. □

Acknowledgement

The authors are indebted to the referee for her or his valuable comments which corrected several errors in the original paper and made the paper simpler and more succinct.

References

1. S.D.Cohen, Primitive elements and polynomials with arbitrary traces, Discrete Math, vol. 83, no. 1, pp. 1-7, 1990. MR **91h:**11143
2. S.D.Cohen, Primitive elements and polynomials: existence results, Lect. Notes in Pure and Applied Math, vol. 141, edited by G.L.Mullen and P.J.Shiue, Dekker, New York, pp. 43-55, 1993. MR **93k:**11113
3. H.Davenport, Bases for finite fields, J.London Math. Soc, vol. 43, pp. 21-39, 1968. MR **37:**2729
4. B. Dwork, G.Gerotto and F.J.Sullivan, An Introduction to G-Functions, Annals of Mathematics Studies, Number 133, Princeton University Press, 1994. MR **96c:**12009
5. W-B.Han, The coefficients of primitive polynomials over finite fields, Math. of Comp, vol. 65, no. 213, pp. 331-340, Jan. 1996. MR **96d:**11128
6. W-B.Han, On two exponential sums and their applications, Finite Fields and Their Applications, 3, pp. 115-130, 1997.
7. W-B.Han, On Cohen's Problem, Chinacrypt'96, Academic Press(China), pp. 231-235, 1996 (in Chinese).
8. W-B.Han, The distribution of the coefficients of primitive polynomials over finite fields, Proceeding of CCNT'99, Prog.in Comp. Sci. and Applied. Logic, vol. 20, Birkhäuser Verlag, Basel/Switzerland, pp. 43-57, 2001.
9. T.Hansen and G.L.Mullen, Primitive polynomials over finite fields, Math. of Comp, vol. 59, no. 200, pp. 639-643, Supplement: S47-S50, Oct. 1992. MR **93a:**11101
10. T.Helleseth, P.V.Kumar, O.Moreno and A.G.Shanbhag, Improved estimates via exponential sums for the minimum distance of $\mathbb{Z}_4$ -linear trace codes, IEEE. Trans. Inform. Theory, vol. 42, no.4, pp. 1212-1216, July 1996. MR **97m:**94028
11. D.Jungnickel and S.A.Vanstone, On primitive polynomials over finite fields, J. of Algebra, vol. 124, pp. 337-353, 1989. MR **90k:**11164
12. N. Koblitz, p-adic number, p-adic analysis and zeta functions, GTM58, Springer-Verlag, 1984. MR **86c:**11086
13. P.V.Kumar, T.Helleseth and A.R.Calderbank, An upper bound for Weil exponential sums over Galois rings and applications, IEEE. Trans. Inform. Theory, vol. 41, no.2, pp. 456-468, Mar. 1995. MR **96c:**11140
14. H.W.Lenstra and R.J.Schoof, Primitive normal bases for finite fields, Math. of Comp, vol. 48, no. 177, pp. 217-232, 1987. MR **88c:**11076
15. W.-C.W.Li, Character sums over p-adic fields, J. Number Theory, 74, pp. 181-229, 1999. MR **2000b:**11100
16. R.Lidl, H.Niedereiter, Finite Fields, Addison-Wesley, London, 1983. MR **86c:**11106
17. O.Moreno, On the existence of a primitive quadratic trace over $GF(p^m)$, J. of Combin. Theory Ser. A, vol. 51, pp. 104-110, 1989. MR **90b:**11133

Department of Applied Mathematics, Information Engineering University, Zhengzhou, 450002, People's Republic of China

E-mail address: sq.fan@263.net

Department of Applied Mathematics, Information Engineering University, Zhengzhou, 450002, People's Republic of China

E-mail address: wb.han@netease.com