Glasgow Math. J. **46** (2004) 47–61. © 2004 Glasgow Mathematical Journal Trust.
DOI: 10.1017/S0017089503001526. Printed in the United Kingdom

p-ADIC FORMAL SERIES AND COHEN'S PROBLEM*

FAN SHUQIN† and HAN WENBAO‡

Department of Applied Mathematics, Institute of Information Engineering, Information Engineering University, Zhengzhou, 450002, PRC

(Received 28 June, 2002; accepted 2 April, 2003)

Abstract. With the help of some p-adic formal series over p-adic number fields and the estimates of character sums over Galois rings, we prove that there is a constant $C(n)$ such that there exists a primitive polynomial $f(x) = x^n - a_1x^{n-1} + \cdots + (-1)^n a_n$ of degree n over F_q with the first $m = \lfloor \frac{n-1}{2} \rfloor$ coefficients $a_1, \ldots, a_m$ prescribed in advance if $q > C(n)$.

2000 *Mathematics Subject Classification.* 11T55, 11F85, 11L40.

1. Introduction. Let F_q be a finite field with $q = p^k$ elements, where p is a prime number and 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 $f(x)|x^T - 1$ is $q^n - 1$. One of the basic problems in computational number theory is to investigate the distribution of the coefficients of primitive polynomials; that is, whether there exists a primitive polynomial with one coefficient or several coefficients prescribed in advance. Based on various tables, Hansen and Mullen [**10**] proposed the following conjecture about the distribution of primitive polynomials with one coefficient prescribed.

Hansen-Mullen conjecture. For any given element $a \in F_q$, there exists a primitive polynomial $f(x) = x^n - a_1x^{n-1} + \cdots + (-1)^n a_n$ of degree n over F_q with the i-th $(0 < i < n)$ coefficient $a_i = a$ except when

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

For $i = 1$, the Hansen-Mullen conjecture is true by the work of Davenport [**3**], Moreno [**17**], Cohen [**1**], Jungnickel and Vanstone [**11**], etc. For $i = 2$, Han [**6**], [**7**] proved that the Hansen-Mullen conjecture is true if

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

As an asymptotic result, Fan and Han proved in [**5**] that there exists a primitive polynomial of degree n over F_q with the m-th $(0 < m < n)$ coefficient prescribed for q large enough except when $m = \frac{n+1}{2}$ if n is odd and $m = \frac{n}{2}, \frac{n}{2} + 1$ if n is even and p exceeds the "non-p part" of n. It convinces us that the Hansen-Mullen conjecture is actually true.

In an excellent survey paper on primitive elements and polynomials, Cohen [**2**] discussed the distribution of primitive polynomials with multiple coefficients prescribed in more detail and asked the following question.

*This work was supported by NSF of China with contract No. 19971096 and No. 90104035.

† e-mail: sq.fan@263.net
‡ e-mail: wb.han@netease.com

https://doi.org/10.1017/S0017089503001526 Published online by Cambridge University Press

Cohen's Problem. Is there some function $c(n)$ such that there exists a primitive polynomial of degree n with $[c(n)]$ coefficients prescribed, where $[\cdot]$ is the round function?

In fact, Han [**6**] proved that there is a primitive polynomial of degree n over F_q with the first and second coefficients prescribed if q is odd and $n \geq 7$. Furthermore, Han [**8**] also obtained the following result.

THEOREM 1. [**8**]. *For $m < p$, there exists a primitive polynomial over F_q of degree n with the first m coefficients prescribed if q is large enough and $n > 2m$.*

We can reformulate Theorem 1 in another way; that is, there exists a primitive polynomial over F_q of degree n with the first $\lfloor \frac{n-1}{2} \rfloor$ coefficients prescribed if $n < 2p$ and q is large enough. In other words, when the degree of the polynomial is small and the characteristic of the finite field is large, there exists a primitive polynomial over F_q with the first half of its coefficients prescribed for q large enough.

The main idea in the proof of Theorem 1 is that the m-th $(0 < m < p)$ coefficient of the primitive polynomial can be expressed in terms of traces of powers of primitive elements. However, for $m \geq p$ we must cope with the inevitable problems relating to the characteristic in handling the trace conditions. In this paper, we shall transfer the working to the unramified extensions of the p-adic fields and their completions, as well as the appropriate quotient rings, Galois rings so that we can translate the existence of primitive polynomials into the existence of the primitive element solutions of Teichmüller points of some system of trace equations with each equation over a suitable Galois ring. To estimate the number of such primitive element solutions, we need the estimates of characters sums over Galois rings [**13**] and over the Teichmüller points of p-adic number fields [**15**].

In this paper, we investigate a varient of Cohen's Problem with the help of some p-adic formal series over p-adic number fields and the estimates of character sums over Galois rings. We get the following main result.

MAIN RESULT. *There is a constant $C(n)$ such that there exists a primitive polynomial $f(x) = x^n - a_1x^{n-1} + \cdots + (-1)^n a_n$ of degree n over F_q with the first $\lfloor \frac{n-1}{2} \rfloor$ coefficients prescribed in advance if $q > C(n)$.*

The paper is arranged as follows. First we give a short review on p-adic number fields and character sums over Galois rings. In Section 3, we set up a one-to-one correspondence between the primitive polynomials over F_q and the lifting primitive polynomials over O_k. Then we reduce the problem of the existence of the lifting primitive polynomials over O_k to the existence of primitive element solutions of some system of trace equations with each equation modulo suitable p^e. We define several p-adic formal series over K_k associated with the traces of powers of Teichmüller points $\xi \in \Gamma_{nk}$, the set of Teichmüller points in K_{nk}, and discuss the properties of those formal series under certain conditions, so that we get the relations between the coefficients of the lifting primitive polynomial and the trace of powers of its roots, and then obtain the reduction. In Section 4, we obtain the estimate of the number of primitive element solutions in Γ_{nk} of the system of trace equations by using the estimates of character sums over Galois rings. We show that if $q^{\frac{n}{2}-m} > m2^{\omega(q^n-1)}$, there exists a primitive polynomial of degree n with the first m coefficients prescribed, where $\omega(q^n - 1)$ is the number of distinct prime factors of $q^n - 1$. As an asymptotic result, we prove our main result that there exists a primitive polynomial over F_q of degree n with the first $\lfloor \frac{n-1}{2} \rfloor$ coefficients prescribed for q large enough.

https://doi.org/10.1017/S0017089503001526 Published online by Cambridge University Press

2. 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 that $p^d | a$ 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 $| \ |_p$, K_k the unique unramified extension of $\mathbb{Q}_p$ of degree k, $O_k = \{x \in K_k; x|_p \leq 1\}$ the ring of integers of K_k, $\overline{\mathbb{Q}_p}$ the algebraic closure of $\mathbb{Q}_p$ and Ω the completion of $\overline{\mathbb{Q}_p}$. Denote by

$$\Gamma_k = \left\{\xi \in K_k;\ \xi^{p^k} = \xi\right\}$$

the set of the Teichmüller points in K_k 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 to be $O_k/p^e O_k$. 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 expressed in the form

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

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

https://doi.org/10.1017/S0017089503001526 Published online by Cambridge University Press

$Tr(\cdot) : K_{nk} \longrightarrow K_k$ is defined via

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

for $x \in K_{nk}$.

$\tau_k|_{O_{nk}} \bmod p^e$ is the Frobenius map of $R_{e,nk}$ over $R_{e,k}$. Later we also use τ_k to denote $\tau_k|_{O_{nk}} \bmod p^e$. 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 $a_i \in \Gamma_{nk}$, $i = 0, 1, \ldots, e-1$.

The map $Tr_{e,nk,k}(\cdot) = Tr(\cdot)|_{O_{nk}} \bmod p^e$ 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 $x \in R_{e,nk}$.

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 $\mathbb{C}\{0\}$. 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 $R_{e,k}$; indeed it is the so-called canonical additive character. For $a \in R_{e,k}$, define $\psi_a(c) = \psi(ac)$, $c \in R_{e,k}$. As in the case of finite fields, we can prove that ψ_a is also an additive character. In fact, we have the following result.

Lemma 2. *$\{\psi_a\}_{a \in R_{e,k}}$ consists of all the additive characters of $R_{e,k}$.*

Proof. It is obvious that we only need to prove that $a = 0$ if and only if ψ_a is trivial, that is, the principal 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 3. *Let $a \in R_{e,k}$ and 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. This is a special case of Theorem 5.4 in [**16**].

Lemma 4. *Let $a \in R_{e,k}$ and ψ be the canonical additive character of $R_{e,k}$. We have*

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

where $1 \leq d \leq e$.

https://doi.org/10.1017/S0017089503001526 Published online by Cambridge University Press

Proof. This more general result is easily deduced from Lemma 3.

2.2.2. Multiplicative character over Teichmüller points. The set 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 well known that the order of each character χ_j is a divisor of $q^n - 1$.

Lemma 5. *Let n be a positive integer and $\xi \in \Gamma_{nk}^*$. We have*

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

where $\mu(d)$ is the Möbius function, $\varphi(d)$ 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 $\gamma \mid \frac{q^n-1}{\text{order}(\xi)}$ such that $\sum_{\chi^{(\gamma)}} \chi^{(\gamma)}(\xi) = \varphi(\gamma)$. 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 $h(x)$ be a polynomial over $R_{e,nk}$ with $h(0) = 0$ and $h(x)$ not identically 0. Let

$$h(x) = h_0(x) + h_1(x)p + \cdots + h_{e-1}(x)p^{e-1}$$

be the p-adic expansion of $h(x)$, where $h_i(x)$ is a polynomial of degree d_i with coefficients in Γ_{nk} for $i = 0, 1, \ldots, e-1$. Define the weighted e-degree of $h(x)$ by

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

https://doi.org/10.1017/S0017089503001526 Published online by Cambridge University Press

Definition 6. Let $h(x) \in R_{e,nk}[x]$ be a polynomial and $h_i(x) = \sum_{j=0}^{d_i} h_{i,j}x^j$, $h_{i,j} \in \Gamma_{nk}$ as above. $h(x)$ is called *nondegenerate* if

$$h_{i,j} = 0, \quad \text{if} \;\; j \equiv 0 \pmod p), 0 \le j \le d_i, 0 \le i \le e-1.$$

Various kinds of character sums over Galois rings are investigated. See for example [**13**], [**15**], etc. Here we give two theorems from [**15**] in a slightly different form for our later use. These results are analogous to Weil estimates on character sums over finite fields.

Theorem 7. [**13**], [**15**]. *Let $f(x) \in R_{e,nk}[x]$ be nondegenerate with weighted e-degree $D_e(f(x))$ and $\psi_{e,n}$ a nontrivial additive character of $R_{e,nk}$. Then*

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

On the other hand, we have the following result.

Theorem 8. [**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*

$$\left|\sum_{\xi\in\Gamma^*_{nk}} \psi_{e,n}(f(\xi))\chi(\xi)\right| \le D_e(f(x))q^{n/2}.$$

3. Problem reduction. In this section, we shall reduce the existence of primitive polynomials over F_q to the existence of primitive element solutions in Γ^*_{nk} of some system of trace equations with each equation over a suitable Galois ring $R_{e,k}$.

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

Definition 9. Let $\tilde{f}(x) \in O_k[x]$ be a basic irreducible polynomial of degree n. We call $\tilde{f}(x)$ *a lifting primitive polynomial over O_k* if there exists a positive integer T such that $\tilde{f}(x)|x^T - 1$ 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 K_{nk}) of all lifting primitive polynomials of degree n in $O_k[x]$. In the rest of the paper, we shall identify them without explanation.

If $\tilde{f}(x)$ is a lifting primitive polynomial over O_k, it is easily seen that $f(x) = \tilde{f}(x)$ mod p is a primitive polynomial over F_q. On the other hand, if $f(x)$ is a primitive polynomial over F_q, then by Hensel's Lemma there exists a unique polynomial $\tilde{f}(x) \in O_k[x]$ such that $f(x) \equiv \tilde{f}(x)$ mod p and $\tilde{f}(x)$ is a lifting primitive polynomial over O_k. Hence the primitive polynomials over F_q and the lifting primitive polynomials over O_k are in one-to-one correspondence.

By the discussions above, the coefficients of primitive polynomials over F_q and the lifting primitive polynomials over O_k are closely related, so that we only need to

https://doi.org/10.1017/S0017089503001526 Published online by Cambridge University Press

consider the lifting primitive polynomials over O_k. We reformulate Cohen's Problem using p-adic number fields.

Cohen's problem over p-adic number fields. Let $q = p^k$ and ϕ be the canonical projective map from O_k to Γ_k. Is there some function $c(n)$ so that there exists a lifting primitive polynomial $f(x) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n$ over O_k of degree n with $m = \lfloor c(n) \rfloor$ coefficients such that $\phi(\sigma_{i_1}) = a_1, \ldots, \phi(\sigma_{i_m}) = a_m$, for any given $a_1, a_2, \ldots, a_m \in \Gamma_k$?

As in [**6**, **8**], we need to find the relation between the coefficient σ_m $(0 < m < n)$ of the lifting primitive polynomial of degree n and the traces of powers of its roots in K_{nk}, the extension field of K_k of degree n. Then we can reduce the existence of the lifting primitive polynomials over O_k with the images of the first m coefficients under the canonical projective map prescribed to the existence of primitive element solutions of some system of trace equations with each equation modulo suitable p^e.

For this reason, we first consider the relations between the coefficients of lifting primitive polynomial over O_k and the traces of powers of its roots.

Lemma 10. [**12**]. *Let A be an $n \times n$ matrix with entries in Ω. We have the following identity of formal power series in $\Omega[[x]]$:*

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

where $Tr(A^s)$ is the trace of the matrix $A^s (s = 0, 1, \ldots)$.

Let $\tilde{f}(x) \in O_k[x]$ be a lifting primitive polynomial of degree n and $\xi \in K_{nk}$ be a root of $\tilde{f}(x)$. Then $\xi \in \Gamma_{nk}$ and $\xi, \xi^q, \ldots, \xi^{q^{n-1}}$ are all the roots of $\tilde{f}(x)$ in K_{nk}.

Proposition 11. *Let $\tilde{f}(x) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n \in O_k[x]$ be a lifting primitive polynomial of degree n, ξ a root of $\tilde{f}(x)$ in K_{nk}. We have*

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

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

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

By expanding the left hand and right hand sides of equation (1), respectively, we get equation (2). □

Theorem 12. [**4**] (Dieudonné's Theorem). *Let $F(x) = 1 + a_1 x + a_2 x^2 + \cdots \in 1 + xK_k[[x]]$. Then*

$$F(x) \in 1 + xO_k[[x]]$$

https://doi.org/10.1017/S0017089503001526 Published online by Cambridge University Press

if and only if

$$\frac{F(x)^p}{F^\tau(x^p)} \in 1 + pxO_k[[x]],$$

where τ is the Frobenius map of K_k over Q_p.

Corollary 13. *Let $a \in O_k$ and $a \equiv 0 \bmod p^e$, $(t,p) = 1$. Let*

$$F_{t,e}(x) = \exp\left(-\sum_{s=e}^{\infty} \frac{a^{\tau^s} x^{tp^s}}{tp^s}\right).$$

Then

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

Proof. It is easy to check that

$$\frac{F_{t,e}(x)^p}{F_{t,e}^\tau(x^p)} = \exp\left(-p\frac{a^{\tau^e}}{tp^e}x^{tp^e}\right) \in 1 + pxO_k[[x]].$$

By Dieudonné's Theorem, we have

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

□

Now we consider the existence of the lifting primitive polynomials over O_k with the images of the first m coefficients under the canonical projective map prescribed. For $0 < t, l \le m$, $(t,p) = 1$, let $e(t,l)$ be the largest integer such that $tp^{e(t,l)-1} \le l$; that is, $e(t,l) = [\log_p(\frac{l}{t})] + 1$. For brevity, we denote $e(t,m)$ by $e(t)$. Now we consider the following system of trace equations:

$$Tr(x^t) = d_t \bmod p^{e(t)}, \quad \text{for } 1 \le t \le m \text{ and } (t,p) = 1, \tag{3}$$

where

$$d_t = d_{t,0} + pd_{t,1} + \cdots + p^{e(t)-1}d_{t,e(t)-1} \tag{4}$$

and $d_{t,j} \in \Gamma_k$ for $1 \le t \le m$, $(t,p) = 1$, $0 \le j \le e(t) - 1$.

Theorem 14. *Assume that the system of equations* (3) *has one primitive element solution $\xi \in \Gamma_{nk}^*$ for any given $d_{t,0}, d_{t,1}, \ldots, d_{t,e(t)-1} \in \Gamma_k$, where $(t,p) = 1$ and $1 \le t \le m$. Then there exists a lifting primitive polynomial over O_k of degree n with the images of the first m coefficients under the canonical projective map prescribed in advance.*

Before we prove Theorem 14, we observe a simple result.

Lemma 15. *Let $(t,p) = 1$ and $\xi \in \Gamma_{nk}$. We have*

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

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

https://doi.org/10.1017/S0017089503001526 Published online by Cambridge University Press

To illustrate the relations between the existence of the lifting primitive polynomials with the images of the first m coefficients under the canonical projective map prescribed and the existence of primitive element solutions ξ of (3) in Γ^*_{nk}, we define a formal series over K_k similar to the Artin-Hasse exponential series (see [**5**]) associated with the traces of powers of ξ for our later use; that is

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

where $(t,p) = 1$, $e \geq 0$ and

$$c(t,s) = Tr\big(\xi^{p^s t}\big) - d_t^{\tau^s}.$$

By Lemma 15,

$$c(t,s) = c(t,0)^{\tau^s}$$

for $s \geq 0$. Hence $E_{t,0} \in 1 + xO_k[[x]]$. On the other hand, from Corollary 13,

$$E_{t,e(t)}(x) \in 1 + xO_k[[x]]. \tag{5}$$

Later we shall denote $E_{t,0}(x)$ by $E_t(x)$.

LEMMA 16. *Let $E_t(x)$ be defined as above,*

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

Then we have

$$a_l \in pO_k \quad \textit{if } tp^{e(t)} \nmid l$$

Moreover $a_l \in pO_k$, for $1 \leq l \leq m$.

Proof. We rewrite $E_t(x)$ as

$$E_t(x) = \exp\left(-\sum_{s=e(t)}^{\infty} \frac{c(t,s)}{tp^s} x^{tp^s}\right) \prod_{s=0}^{e(t)-1} \exp\left(-\frac{c(t,s)}{tp^s} x^{tp^s}\right).$$

Since the first term (i.e $E_{t,e(t)}[[x]]$) is in $1 + xO_k[[x]]$ and the second term of the right hand side is in $1 + pxO_k[[x]]$, the only possible terms a_l's such that $a_l \notin pO_k$ are the terms in the expansion of $E_{t,e(t)}$. Hence we must have $tp^{e(t)}|l$. Moreover, we have $a_l \in pO_k$ for $1 \leq l \leq m$ since $t \cdot p^{e(t)} > m$ by the definition of $e(t)$. □

Next we define two formal series associated with $E_t(x)$. Let

$$E_{t,+}(x) = \exp\left(-\sum_{s=0}^{\infty} \frac{Tr\big(\xi^{tp^s}\big)x^{tp^s}}{tp^s}\right)$$

and

$$E_{t,-}(x) = \exp\left(-\sum_{s=0}^{\infty} \frac{d_t^{\tau^s} x^{tp^s}}{tp^s}\right).$$

https://doi.org/10.1017/S0017089503001526 Published online by Cambridge University Press

Proposition 17. *Let $a_{t,l}$ and $b_{t,l}$ be the coefficients of x^l in $E_{t,+}(x)$ and $E_{t,-}(x)$, respectively. Then*

$$a_{t,l} \equiv b_{t,l} \mod p$$

for $1 \leq l \leq m$.

Proof. It is easy to see from Dieudonné's Theorem that

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

Furthermore

$$E_t(x) \cdot E_{t,-}(x) = E_{t,+}(x)$$

in $O_k[[x]]$. From Lemma 16, we have

$$a_{t,l} \equiv b_{t,l} \mod p$$

for $1 \leq l \leq m$. □

Now we consider the coefficient of x^l in $E_{t,-}(x)$ for $1 \leq l \leq m$.

Lemma 18. *For any given integers t, l such that $1 \leq l, t \leq m$ and $(t, p) = 1$, let $b_{t,l}$ be the coefficient of x^l in $E_{t,-}(x)$. We have*

$$b_{t,l} \equiv g\big(d_{t,0}, \ldots, d_{t,e(t,l)-1}\big) \mod p.$$

In particular, if $t \cdot p^{e(t,l)-1} = l$, then

$$b_{t,l} \equiv g_1\big(d_{t,0}, \ldots, d_{t,e(t,l)-2}\big) - \frac{1}{t} \cdot d_{t,e(t,l)-1}^{p^{e(t,l)-1}} \mod p,$$

where g is a polynomial of $d_{t,0}, \ldots, d_{t,e(t,l)-1}$ over O_k, g_1 is a polynomial of $d_{t,0}, \ldots, d_{t,e(t,l)-2}$ over O_k.

Proof. We only need to consider the coefficient of x^l in

$$\begin{aligned}
\exp\left(-\sum_{s=0}^{e(t,l)-1} \frac{d_t^{\tau^s} x^{tp^s}}{tp^s}\right) &= \exp\left(-\sum_{s=0}^{e(t,l)-1} \frac{d_{t,0}^{p^s} x^{tp^s}}{tp^s}\right) \exp\left(-p\sum_{s=0}^{e(t,l)-1} \frac{d_{t,1}^{p^s} x^{tp^s}}{tp^s}\right) \\
&\quad \ldots \exp\left(-p^{e(t,l)-1}\sum_{s=0}^{e(t,l)-1} \frac{d_{t,e(t,l)-1}^{p^s} x^{tp^s}}{tp^s}\right) \\
&= \exp\left(-\sum_{s=0}^{e(t,l)-1} \frac{d_{t,0}^{p^s} x^{tp^s}}{tp^s}\right) \exp\left(-p\sum_{s=0}^{e(t,l)-1} \frac{d_{t,1}^{p^s} x^{tp^s}}{tp^s}\right) \\
&\quad \ldots \exp\left(-d_{t,e(t,l)-1}^{p^{e(t,l)-1}} \frac{x^{tp^{e(t,l)-1}}}{t}\right) \mod p.
\end{aligned}$$

https://doi.org/10.1017/S0017089503001526 Published online by Cambridge University Press

For $1 \le i \le l$ and $r = 0, \ldots, e(t, l) - 1$, the coefficient of x^i in

$$\exp\left(-p^r \sum_{s=0}^{e(t,l)-1} \frac{d_{t,r}^{p^s} x^{tp^s}}{tp^s}\right)$$

is the same as the coefficient of x^i in

$$\exp\left(-p^r \sum_{s=0}^{\infty} \frac{d_{t,r}^{p^s} x^{tp^s}}{tp^s}\right),$$

and so it must belong to O_k. Hence

$$b_{t,l} \equiv g\big(d_{t,0}, \ldots, d_{t,e(t,l)-1}\big) \mod p.$$

In particular, if $t \cdot p^{e(t,l)-1} = l$, the least non-constant term in

$$\exp\left(-d_{t,e(t,l)-1}^{p^{e(t,l)-1}} \frac{x^{tp^{e(t,l)-1}}}{t}\right)$$

is x^l and the corresponding coefficient is $-\frac{1}{t} \cdot d_{t,e(t,l)-1}^{p^{e(t,l)-1}}$, so that if $t \cdot p^{e(t,l)-1} = l$, then

$$b_{t,l} \equiv g_1\big(d_{t,0}, \ldots, d_{t,e(t,l)-2}\big) - \frac{1}{t} \cdot d_{t,e(t,l)-1}^{p^{e(t,l)-1}} \mod p.$$

This finishes the proof. □

Proposition 19. *Let $1 \le l \le m$, $l = t_l p^{e(t_l,l)-1}$, $(t_l, p) = 1$ and $e(t_l, l) \ge 1$. Let b_l be the coefficient of x^l in $\prod_{(t,p)=1} E_{t,-}(x)$. We have*

$$b_l \equiv g^*(\{d_{t,i} | (t, p) = 1,\ tp^i < l\}) - \frac{1}{t_l} \cdot d_{t_l,e(t_l,l)-1}^{p^{e(t_l,l)-1}} \mod p,$$

where g^* is a polynomial of $\{d_{t,i} | (t, p) = 1,\ tp^i < l\}$ over O_k.

Proof. This result follows from Lemma 18.

Proof of Theorem 14. Let ξ be a primitive element solution of (3) in Γ_{nk} and

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

be the minimal polynomial of ξ over O_k. By Proposition 11,

$$\begin{aligned} x^n \tilde{f}\left(\frac{1}{x}\right) &= \exp\left(-\sum_{s=1}^{\infty} Tr(\xi^s) x^s / s\right) \\ &= \prod_{\substack{(t,p)=1 \\ t>0}} E_{t,+}(x). \end{aligned}$$

https://doi.org/10.1017/S0017089503001526 Published online by Cambridge University Press

Furthermore, from Proposition 17, we only need to consider the coefficient of x^l $(1 \leq l \leq m)$ in

$$\prod_{(t,p)=1} E_{t,-}(x).$$

Consider $1 \leq l \leq m$, $l = t_l p^{e(t_l,l)-1}$, $(t_l, p) = 1$ and $e(t_l, l) \geq 1$. From Proposition 19 we have

$$(-1)^l \sigma_l \equiv g^*(\{d_{t,i} | t \cdot p^i < l\}) - \frac{1}{t_l} \cdot d_{t_l, e(t_l,l)-1}^{p^{e(t_l,l)-1}} \bmod p.$$

For any given $\{d_{t,i} | (t, p) = 1 \text{ and } t \cdot p^i < l\}$, $\phi(\sigma_l)$ runs across Γ_k if $d_{t_l, e(t_l,l)-1}$ runs across Γ_k. This finishes the proof of Theorem 14.

4. Estimates and calculations. We now estimate the number of primitive element solutions of (3) in Γ_{nk}^*.

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

$$S_l = \{t | (t, p) = 1; \, l \text{ is the largest integer such that } t \cdot p^{l-1} \leq m\}$$

for $l = 1, \ldots, e$ and

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

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

Let N_m be the number of primitive element solutions of (3) in Γ_{nk}^*, ψ the canonical additive character of $R_{e,k}$, $\psi_{e,n} = \psi \circ Tr_{e,nk,k}$ the canonical additive character of $R_{e,nk}$ and let $\chi^{(d)}$ run through all the multiplicative characters over Γ_{nk}^* with order d. From Lemma 3, Lemma 4 and Lemma 5,

$$\begin{aligned} N_m &= \delta \sum_{\xi \in \Gamma_{nk}^*} \prod_{l=1}^{e} \prod_{t \in S_l} \sum_{c_t \in R_{l,k}} \psi(p^{e-l}(c_t(Tr(\xi^t) - d_t))) \cdot \sum_{d | q^n - 1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \chi^{(d)}(\xi) \\ &= \delta \sum_{d | q^n - 1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \sum_{(c_t)_{(t,p)=1} \in \mathbb{S}} \psi\left(-\sum_{l=1}^{e} p^{e-l} \sum_{t \in S_l} c_t d_t\right) \cdot \Lambda\big((c_t)_{(t,p)=1}, \chi^{(d)}\big), \end{aligned}$$

where

$$\delta = \frac{\varphi(q^n - 1)}{(q^n - 1)} q^{-m}$$

and

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

Let

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

https://doi.org/10.1017/S0017089503001526 Published online by Cambridge University Press

It is obvious that $h(x)$ is nondegenerate if $h(x) \neq 0$ with

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

Now we estimate N_m.

1. If $h(x) = 0$, that is, $c_t = 0 \in R_{l,k}$ for $t \in S_l$ and $l = 1, \ldots, e$, then

$$\psi\left(-\sum_{l=1}^{e} p^{e-l} \sum_{t \in S_l} c_t d_t\right) = 1.$$

(a) When $d = 1$,

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

and

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

(b) When $d > 1$,

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

We have

$$\sum_{d \mid q^n-1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \sum_{\substack{(c_t)_{(t,p)=1} \in \mathbb{S} \\ h(x)=0}} \psi\left(\sum_{l=1}^{e} p^{e-l} \sum_{t \in S_l} c_t d_t\right) \cdot \Lambda\big((c_t)_{(t,p)=1}, \chi^{(d)}\big)$$
$$= q^n - 1.$$

2. If $h(x) \neq 0$, that is, $c_t \neq 0 \in R_{l,k}$ for some $t \in S_l$ and some $l = 1, \ldots, e$, then in this case $h(x)$ is nondegenerate.

(a) When $d = 1$, from Theorem 7 we obtain

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

(b) When $d \neq 1$, from Theorem 8 we obtain

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

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 have

$$\left|\sum_{d \mid q^n-1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi^{(d)}} \sum_{\substack{(c_t)_{(t,p)=1} \in \mathbb{S} \\ h(x)\neq 0}} \psi\left(\sum_{l=1}^{e} p^{e-l} \sum_{t \in S_l} c_t d_t\right) \cdot \Lambda\big((c_t)_{(t,p)=1}, \chi^{(d)}\big)\right|$$
$$\leq 2^{w(q^n-1)} \cdot m \cdot (q^m - 1) \cdot q^{n/2},$$

so that

$$N_m \geq \delta\big\{(q^n - 1) - 2^{\omega(q^n-1)} m q^{\frac{n}{2}}(q^m - 1)\big\}, \tag{6}$$

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

Theorem 20. *$N_m > 0$ if*

$$q^{\frac{n}{2}-m} > m2^{\omega(q^n-1)}, \tag{7}$$

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

Proof. By (6), it is easily seen that $N_m > 0$ if

$$q^{\frac{n}{2}} > m2^{\omega(q^n-1)}q^m.$$

□

Following the method introduced by Lenstra and Schoof [**14**], the inequality (7) holds for q large enough if $m < \frac{n}{2}$. Therefore we prove the following result.

Theorem 21. *There is a constant $C(n)$ depending on n such that there exists a primitive polynomial over F_q of degree n with the first $\lfloor\frac{n-1}{2}\rfloor$ coefficients prescribed in advance if $q > C(n)$.*

Proof. From Theorem 20 and the method introduced by Lenstra and Schoof, there exists a constant $C(m, n)$ such that for $1 \leq m < \frac{n}{2}$, $N_m > 0$ when $q > C(m, n)$. Let

$$C(n) = \max_{1\leq m<n/2} C(m, n).$$

The present theorem now follows from Theorem 14. □

Remark 22. In this paper, we have proved that there exists a primitive polynomial over F_q with the first $\lfloor\frac{n-1}{2}\rfloor$ coefficients prescribed for q large enough. It is still unknown whether there is a positive integer $s > \lfloor\frac{n-1}{2}\rfloor$ such that there exists a primitive polynomial over F_q with s coefficients prescribed for q large enough.

Acknowledgement. The authors are indebted to the referee for valuable comments which corrected several errors in the original paper and made the paper much clearer.

REFERENCES

1. S. D. Cohen, Primitive elements and polynomials with arbitrary trace, *Discrete Math.* **83** (1990), 1–7.

2. S. D. Cohen, Primitive elements and polynomials: existence results, in *Finite fields, coding theory and advances in communications and computing* (*Las Vegas, Nevada, 1991*) (G. L. Mullen and P. J. Shine eds.), Lecture Notes in Pure and Appl. Math., Vol. 141 (Dekker, New York, 1992), 43–55.

3. H. Davenport, Bases for finite fields, *J. London Math. Soc.* **43** (1968), 21–39.

4. B. Dwork, G. Gerotto and F. J. Sullivan, *An introduction to* G-*functions*, Annals of Mathematics Studies, No. 133 (Princeton University Press, 1994).

5. S. Q. Fan and W. B. Han, *p*-adic Formal series and primitive polynomials over finite fields, *Proc. Amer. Math. Soc.*, to appear.

https://doi.org/10.1017/S0017089503001526 Published online by Cambridge University Press

6. W. B. Han, The coefficients of primitive polynomials over finite fields, *Math. Comp.* **65** (1996), 331–340.

7. W. B. Han, On two exponential sums and their applications, *Finite Fields Appl.* **3** (1997), 115–130.

8. W. B. Han, On Cohen's Problem, in *Chinacrypt'96* (Academic Press (China) 1996), 231–235.

9. W. B. Han, The distribution of the coefficients of primitive polynomials over finite fields, in *Proceedings of CCNT'99*, Prog. in Comp. Sci and Applied Logic, Vol. 20 (Birkhäuser-Verlag, 2001), 43–57.

10. T. Hansen and G. L. Mullen, Primitive polynomials over finite fields, *Math. Comp.* **59** (1992), 639–643. Supplement: S47-S50.

11. D. Jungnickel and S. A. Vanstone, On primitive polynomials over finite fields, *J. Algebra* **124** (1989), 337–353.

12. N. Koblitz, *p-adic number*, *p-adic analysis and zeta functions* (Springer-Verlag, 1984).

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* **41** (1995), 456–468.

14. H. W. Lenstra and R. J. Schoof, Primitive normal bases for finite fields, *Math. Comp.* **177** (1987), 217–232.

15. W. -C. W. Li, Character sums over p-adic fields, *J. Number Theory* **74** (1999), 181–229.

16. R. Lidl and H. Niedereiter, *Finite fields* (Addison-Wesley, 1983).

17. O. Moreno, On the existence of a primitive quadratic trace over $GF(p^m)$, *J. Combin. Theory Ser. A.* **51** (1989), 104–110.

https://doi.org/10.1017/S0017089503001526 Published online by Cambridge University Press