Journal of Mathematical Research & Exposition
Vol.24, No.2, 219-224, May, 2004

Distribution of Elements in Primitive Sequences over Z_{p^e} *

FAN Shu-qin, HAN Wen-bao
(Dept. of Appl. Math., Information Engineering University, Zhengzhou 450002, China)

Abstract: Using the estimates of character sums over Galois rings and the trace description of primitive sequences over Z_{p^e}, we obtain an estimate for the frequency of the occurrences of any element in Z_{p^e} in one period of a primitive sequence, which is better than Kuzmin's results[1] if $n > 4e$, where n is the degree of the generating polynomial of the primitive sequence.

Key words: primitive sequence over ring; element distribution; character sum.

Classification: AMS(2000) 11T24, 94A60/CLC number: O156, TP309

Document code: A **Article ID:** 1000-341X(2004)02-0219-06

Let Z_{p^e} be the residue ring of integers modulo p^e. For a monic polynomial $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in Z_{p^e}[x]$ with $f(0) \neq 0 \bmod p$, there exists a positive integer T such that $f(x)|x^T - 1$ over Z_{p^e} , and the smallest T is called the period of $f(x)$ over Z_{p^e}, denoted by $per(f(x))_e$. By [2] $\mathrm{per}(f(x))_e \leq p^{e-1}(p^n - 1)$. If $\mathrm{per}(f(x))_e = p^{e-1}(p^n - 1)$, $f(x)$ is called a primitive polynomial over Z_{p^e}. The sequence $\underline{a} = (a_i)_{i=0}^{\infty} \in Z_{p^e}^{\infty}$ satisfying $a_{i+n} = -(c_{n-1}a_{i+n-1} + \cdots + c_0 a_i)$ is called a linear recurring sequence over Z_{p^e} generated by $f(x)$. $\underline{a}$ is called a primitive sequence if $\underline{a}$ is generated by a primitive polynomial $f(x)$ and $\underline{a} \neq 0 \bmod p$. In this paper, we will investigate the distribution of elements in the primitive sequences.

When $p^e = 4$, the distribution of elements in the primitive sequences over Z_{p^e} has been explicitly investigated in [3,4,5]. In [1], Kuzmin investigated the distributions of elements in the primitive sequences for general p^e. Let $\underline{a}$ be a primitive sequence over Z_{p^e}, n the degree of the generating polynomial, $T(\underline{a})$ the period of $\underline{a}$ which is $p^{e-1}(p^n - 1)$ and $\nu(l)$ the number of occurrences of an element $l \in Z_{p^e}$ in one period of $\underline{a}$. Kuzmin obtained the following estimates:

(1) If $p \geq 3$, $\nu(l) \geq \frac{p-1}{p} \cdot \frac{T(\underline{a})}{p^e}$.

(2) If $p = 2$ and $n \geq 3$, $\nu(l) \geq \frac{1}{4} \cdot \frac{T(\underline{a})}{2^e}$.

Galois rings have played very important roles in designing large families of phase-shift-key sequences having low correlations[4,6] which can be potentially used as the candidates

*Received date: 2002-03-04
Foundation item: Supported by NNSF of China (19971096, 90104035)
Biography: FAN Shu-qin (1978-), female, the doctorate candidate.

of CDMA signature sequences. Some famous nonlinear binary codes such as Kerdock, Preparata, Goethals and related codes can be viewed as linear codes over Galois ring Z_4. To analyze the properties of the codes over Galois rings, some kinds of character sums over Galois rings were introduced and investigated[7].

In this paper, with the help of the trace description of primitive sequences and the estimates of character sums over Galois rings, we prove that the frequency of occurrences of any element in Z_{p^e} in one period of a primitive sequence is asymptotic to $1/p^e+O(p^{-n/2})$ for given p^e. More precisely, we will prove

(1) If $l \neq 0$, $|\nu(l) - p^{n-1}| \leq \frac{p-1}{p} \cdot (\frac{p^{2e}-1}{p^2-1} - \frac{p^e-1}{p-1}) \cdot p^{n/2}$.

(2) If $l = 0$, $|\nu(0) - (p^{n-1} - p^{e-1})| \leq \frac{p-1}{p} \cdot (\frac{p^{2e}-1}{p^2-1} - \frac{p^e-1}{p-1}) \cdot p^{n/2}$.

This shows that if p^e is fixed and n is large enough, the distribution of elements in the primitive sequences over Z_{p^e} is balanced. Furthermore if $n > 4e$, our estimate is better than Kuzmin's results.

2. Preliminary

2.1 Galois rings of characteristic p^e

Let $e \geq 1$ be a fixed integer and p a prime number. A monic polynomial $f(x) \in Z_{p^e}[x]$ is said to be a basic irreducible polynomial of degree n if $f(x) \bmod p \in Z_p[x]$ is a monic irreducible polynomial. The Galois ring $R_{e,n} = \mathrm{GR}(p^e, n)$ is the unique extension of degree n over Z_{p^e} and can be written as $Z_{p^e}[x]/(f(x))$, where $f(x)$ is a basic irreducible polynomial of degree n over Z_{p^e}. $R_{e,n}$ is a local ring with the unique maximal ideal $pR_{e,n}$. The set of units $R^*_{e,n} = R_{e,n} \backslash pR_{e,n}$ is a multiplicative group with the following structure:

$$R^*_{e,n} \cong Z_{p^n-1} \times \underbrace{Z_{p^{e-1}} \times \cdots \times Z_{p^{e-1}}}_{n \text{ copies}}$$

when p is odd or $p = 2$ and $e = 2$. When $p = 2$ and $e \geq 3$, the group structure is:

$$R^*_{e,n} \cong Z_{p^n-1} \times Z_p \times Z_{p^{e-2}} \times \underbrace{Z_{p^{e-1}} \times \cdots \times Z_{p^{e-1}}}_{n-1 \text{ copies}}.$$

Let ξ be a generator of the cyclic group of $R^*_{e,n}$ corresponding to Z_{p^n-1}. Define $\Gamma_{e,n} = \{0, 1, \xi, \cdots, \xi^{p^n-2}\}$. It can be shown that every element $z \in R_{e,n}$has a unique p-adic expansion $z = z_0 + pz_1 + \cdots + p^{e-1}z_{e-1}, \quad z_i \in \Gamma_{e,n}$.

Let σ be the Frobenius map from $R_{e,n}$ to $R_{e,n}$ given by

$$\sigma(z) = z_0^p + pz_1^p + \cdots + p^{e-1}z_{e-1}^p.$$

As we know, σ is the generator of the Galois group of $R_{e,n}/Z_{p^e}$ which is a cyclic group of order n. The trace mapping $Tr_{e,n}(.) : R_{e,n} \to Z_{p^e}$ is defined via $Tr_{e,n}(x) = x + \sigma(x) + \cdots + \sigma^{n-1}(x)$ for $x \in R_{e,n}$.

2.2 Estimates of character sums over Galois rings

Let ψ be the canonical additive character over Z_{p^e} defined by $\psi(a) = e^{2\pi ia/p^e}$ for $a \in Z_{p^e}$, $\psi_{e,n}$ the canonical additive character over $R_{e,n}$ defined by $\psi_{e,n}(x) = (\psi \circ Tr_{e,n})(x) = e^{2\pi i Tr_{e,n}(x)/p^e}$ for $x \in R_{e,n}$.

Lemma 1 *Let ψ be the canonical additive character of Z_{p^e} and $a \in Z_{p^e}$. We have*

$$\sum_{c \in Z_{p^e}} \psi(ca) = \begin{cases} p^e, & \text{if } a = 0; \\ 0, & \text{if } a \neq 0. \end{cases}$$

Let $g(x)$ be a polynomial over $R_{e,n}$ with $g(0) = 0$ and $g(x)$ not identically 0. Let $g(x) = g_0(x) + g_1(x)p + \cdots + g_{e-1}(x)p^{e-1}$ be the p-adic expansion of $g(x)$, where $g_i(x)$ is a polynomial of degree d_i with coefficients in $\Gamma_{e,n}$ for $i = 0, 1, \cdots, e-1$. Define the weighted degree of $g(x)$ by $D_{e,g} = \max\{d_0 p^{e-1}, d_1 p^{e-2}, \cdots, d_{e-1}\}$.

Definition 1 *Let $g(x)$ be a polynomial as above and $g_i(x) = \sum_{j=0}^{d_i} G_{i,j} x^j$, $G_{i,j} \in \Gamma_{e,n}$. $g(x)$ is called nondegenerate if $G_{i,j} = 0$, if $j \equiv 0 \bmod p, 0 \leq j \leq d_i, 0 \leq i \leq e-1$.*

Various kinds of character sums over Galois rings have been investigated in [7,8,9]. Here we give a theorem from [7] which is analogous to Weil estimates on character sums over finite fields.

Theorem 1[7] *Let $g(x) \in R_{e,n}[x]$ be a nondegenerate polynomial of weighted degree $D_{e,g}$, and $\psi_{e,n}$ the canonical additive character over $R_{e,n}$. Then*

$$|\sum_{x \in \Gamma_{e,n}} \psi_{e,n}(g(x))| \leq (D_{e,g} - 1) \cdot \sqrt{p^n}.$$

3. The estimate of the frequencies of the elements in primitive sequences over Z_{p^e}

3.1 Trace description of primitive sequences over Z_{p^e}

Let $f(x)$ be a primitive polynomial over Z_{p^e} with degree n. Denote by $\Omega(f(x))_e$ the set of all sequences generated by $f(x)$ over Z_{p^e}. For any sequence $\underline{a} = (a_0, a_1, \cdots) \in \Omega(f(x))_e$, the period of $\underline{a}$ is defined by $\mathrm{per}(\underline{a})_e = \min\{T \in \mathbf{N} | a_{i+T} = a_i, \forall i \in \mathbf{Z}_{\geq 0}\}$. It is obvious that $\mathrm{per}(\underline{a})_e | \mathrm{per}(f(x))_e$. If $\underline{a}$ is a primitive sequence generated by $f(x)$, we have $\mathrm{per}(\underline{a})_e = p^{e-1}(p^n - 1)$. In fact, the set of all primitive sequences generated by $f(x)$ is $\Omega'(f(x))_e = \{\underline{a} \in \Omega(f(x))_e | \ \underline{a} \neq 0 \bmod p\}$. For the primitive sequences, we have the following trace description :

Lemma 2 (Trace Description) *Let $f(x)$ be a primitive polynomial over Z_{p^e} with degree $n, \gamma \in R_{e,n}$ a root of $f(x)$. Then for any primitive sequence $\underline{a} \in \Omega'(f(x))_e$, there exists a unique $\alpha \in R^*_{e,n}$ such that $a_i = Tr_{e,n}(\alpha \gamma^i)$ for $i \in \mathbf{Z}_{\geq 0}$.*

As we know, the order of γ in Lemma 2 is $p^{e-1}(p^n - 1)$. So γ can be written as $\gamma = \xi(1 + p\xi_1)$, where ξ is a generator of the multiplicative group $\Gamma^*_{e,n}$ and $\xi_1 \in R^*_{e,n}$. The set of all primitive sequences generated by $f(x)$ can be written as $\{\{Tr_{e,n}(\alpha(\xi(1 + p\xi_1))^j)\}_{j=0}^{\infty} | \alpha \in R^*_{e,n}\}$.

3.2 Estimate of frequencies

In this subsection, we will discuss the distribution of elements in one period of the primitive sequence $\{Tr_{e,n}(\alpha(\xi(1+p\xi_1))^j)\}_{j=0}^{p^{e-1}(p^n-1)}$, where ξ is a generator of the multiplicative group $\Gamma_{e,n}^*$ and $\xi_1 \in R_{e,n}^*$.

Divide the sequence $\underline{a} = \{Tr_{e,n}(\alpha(\xi(1+p\xi_1))^j)\}_{j=0}^{p^{e-1}(p^n-1)}$ into p^{e-1} subsequences according to $j \bmod p^{e-1}$. For $0 \le k \le p^{e-1}-1$, the p^{e-1} subsequences can be written as $\underline{a}^k = \{Tr_{e,n}(\alpha(\xi(1+p\xi_1))^{p^{e-1}t+k})\}_{t=0}^{p^n-2}$. Denote by $\nu_{k,\alpha}(l)$ the number of l ($l = 0, 1, \cdots, p^e-1$) in the subsequence $\underline{a}^k$, then

$$\begin{aligned}\nu_{k,\alpha}(l) &= \#\{t \in \{0,1,\cdots,p^n-2\} | Tr_{e,n}(\alpha(\xi(1+p\xi_1))^{p^{e-1}t+k}) = l\} \\ &= \#\{t \in \{0,1,\cdots,p^n-2\} | Tr_{e,n}(C_{k,\alpha}(\xi(1+p\xi_1))^{p^{e-1}t}) = l\} \\ &= \#\{t \in \{0,1,\cdots,p^n-2\} | Tr_{e,n}(C_{k,\alpha}\xi^{p^{e-1}t}) = l\}\end{aligned}$$

where $C_{k,\alpha} = \alpha(\xi(1+p\xi_1))^k$. It is obvious that $C_{k,\alpha} \in R_{e,n}^*$.

Since $(p^{e-1}, p^n-1) = 1$, $p^{e-1}t \bmod p^n-1$ covers $\{0,1,\cdots,p^n-2\}$ when t runs across $\{0,1,\cdots,p^n-2\}$. So

$$\begin{aligned}\nu_{k,\alpha}(l) &= \#\{t \in \{0,1,\cdots,p^n-2\} | Tr_{e,n}(C_{k,\alpha}\xi^t) = l\} \\ &= \#\{x \in \Gamma_{e,n}^* | Tr_{e,n}(C_{k,\alpha}x) = l\} \\ &= \begin{cases} \nu_{k,\alpha}(l)' - 1 & \text{if } l = 0; \\ \nu_{k,\alpha}(l)' & \text{if } l \neq 0. \end{cases}\end{aligned}$$

where $\nu_{k,\alpha}(l)' = \#\{x \in \Gamma_{e,n} | Tr_{e,n}(C_{k,\alpha}x) = l\}$.

Let ψ be the canonical additive character over Z_{p^e}, $\psi_{e,n}$ the canonical additive character over $R_{e,n}$. From Lemma 1 we have

$$\begin{aligned}\nu_{k,\alpha}(l)' &= \frac{1}{p^e}\sum_{x\in\Gamma_{e,n}}\sum_{d\in Z_{p^e}}\psi(d(Tr_{e,n}(C_{k,\alpha}x)-l)) \\ &= \frac{1}{p^e}\sum_{d\in Z_{p^e}}\sum_{x\in\Gamma_{e,n}}\psi(d(Tr_{e,n}(C_{k,\alpha}x)-l)) \\ &= \frac{1}{p^e}\sum_{d\in Z_{p^e}}\psi(-dl)\sum_{x\in\Gamma_{e,n}}\psi\circ Tr_{e,n}(dC_{k,\alpha}x) \\ &= \frac{1}{p^e}\sum_{d\in Z_{p^e}}\psi(-dl)\sum_{x\in\Gamma_{e,n}}\psi_{e,n}(dC_{k,\alpha}x).\end{aligned}$$

Now we estimate $\nu_{k,\alpha}(l)'$.

Case 1 If $d = 0$, $\psi(-dl)\sum_{x\in\Gamma_{e,n}}\psi_{e,n}(dC_{k,\alpha}x) = p^n$.

Case 2 If $d \neq 0$, from Theorem 1 we have

$$|\psi(-dl)\sum_{x\in\Gamma_{e,n}}\psi_{e,n}(dC_{k,\alpha}x)| \le (D_{e,g_d}-1)p^{n/2},$$

where D_{e,g_d} is the weighted degree of $g_d(x) = dC_{k,\alpha}x$.

For $d \in Z_{p^e}\backslash\{0\}$, there exist $p^{e-m} - p^{e-1-m}d$'s such that

$$D_{e,g_d} = p^{e-1-m} \cdot \sum_{m=0}^{e-1}(p^{e-m} - p^{e-1-m})p^{e-1-m} = (p-1)\sum_{m=0}^{e-1} p^{2m} = (p-1)\cdot\frac{p^{2e}-1}{p^2-1}$$

So we have

$$|\sum_{d\in Z_{p^e}\backslash\{0\}} \psi(-dl) \sum_{x\in\Gamma_{e,n}} \psi_{e,n}(dC_{k,\alpha}x)| \le (p-1)\cdot(\frac{p^{2e}-1}{p^2-1} - \frac{p^e-1}{p-1})\cdot p^{n/2}.$$

As a result,

$$|\nu_{k,\alpha}(l)' - \frac{1}{p^e}\cdot p^n| \le \frac{p-1}{p^e}\cdot(\frac{p^{2e}-1}{p^2-1} - \frac{p^e-1}{p-1})\cdot p^{n/2}.$$

Denote by $\nu(l)$ the number of occurrences of l in one period of the primitive sequence $\underline{a} = \{Tr_{e,n}(\alpha(\xi(1+p\xi_1))^j)\}_{j=0}^{p^{e-1}(p^n-1)}$. It is easy to see that $\nu(l) = \sum_{k=0}^{p^{e-1}-1} \nu_{k,\alpha}(l)$. We have proved

Theorem 2 *Let p be a prime number, $f(x)$ a primitive polynomial over Z_{p^e} of degree n, and $\underline{a}$ a primitive sequence generated by $f(x)$. For $l = 0, 1, \cdots, p^e - 1$, denote by $\nu(l)$ the number of occurrences of l in one period of $\underline{a}$. We have*

$$|\nu(l) - p^{n-1}| \le \frac{p-1}{p}\cdot(\frac{p^{2e}-1}{p^2-1} - \frac{p^e-1}{p-1})\cdot p^{n/2} \ (l \ne 0),$$

and

$$|\nu(0) - (p^{n-1} - p^{e-1})| \le \frac{p-1}{p}\cdot(\frac{p^{2e}-1}{p^2-1} - \frac{p^e-1}{p-1})\cdot p^{n/2}.$$

Corollary 3 *Let p be a prime number, $f(x)$ a primitive polynomial over Z_{p^e} of degree n, $\underline{a}$ a primitive sequence generated by $f(x)$. For $l = 0, 1, \ldots, p^e - 1$, denote by $\lambda(l)$ the frequency of the occurrences of $l \in Z_{p^e}$ in one period of $\underline{a}$. We have*

$$|\lambda(l) - \frac{1}{p^e}\cdot\frac{p^n}{p^n-1}| \le \frac{p-1}{p^e}\cdot(\frac{p^{2e}-1}{p^2-1} - \frac{p^e-1}{p-1})\cdot\frac{p^{n/2}}{p^n-1} \ (l \ne 0),$$

and

$$|\lambda(0) - \frac{1}{p^e}\cdot\frac{(p^n-p^e)}{p^n-1}| \le \frac{p-1}{p^e}\cdot(\frac{p^{2e}-1}{p^2-1} - \frac{p^e-1}{p-1})\cdot\frac{p^{n/2}}{p^n-1}.$$

From Theorem 2 and Corollary 3, for any given e, the frequency of occurrences of an element $l \in Z_{p^e}$ in the primitive sequences over Z_{p^e} is asymptotically $1/p^e + O(p^{-n/2})$. This means when n is large enough, the distribution of elements in the primitive sequences over Z_{p^e} is balanced. Furthermore if $n > 4e$, our estimate is better than Kuzmin's results[1].

Example 1 Let $e = 1$. From Theorem 2, $\nu(l) = p^{n-1}$ for $l \ne 0$, and $\nu(0) = p^{n-1} - 1$.

which is the distribution of elements in the m-sequences over F_p.

Remark 1 When $p^e = 4$, there is a complete description of all possible values of the distribution of the elements in the primitive sequences [4,5].

References:

[1] KUZMIN A.S. *The distribution of elements on cycles of linear recurrents over rings of residues* [J]. Russian Math. Surveys, 1992, **47**: 219–221.

[2] WARD M. *The arithmetical theory of linear recurring sequences* [J]. Trans. Amer. Math. Soc., 1933, **35**(6): 600–628.

[3] BOZATAS S, HAMMONS A R, KUMAR P V. *4-phase sequences with near-optimum correlation properties* [J]. IEEE. Trans. Inform.Theory, 1992, **38**(3): 1101–1113.

[4] HAMMONS A R, KUMAR P V, CALDERBANK A R, et al. *The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes* [J]. IEEE. Trans. Inform. Theory, 1994, **40**: 301–319.

[5] KUZMIN A S, NECHAV A A. *A construction of noise stable codes using linear recurrents over Galois rings* [J]. Russian Math. Surveys, 1992, **47**: 189–190.

[6] HELLESETH T, KUMAR P V, MORENO O, et al. *Improved estimates via exponential sums for the minimum distance of Z_4-linear trace codes* [J]. IEEE. Trans. Inform. Theory, 1996, **42**(4): 1212–1216.

[7] KUMAR P V, HELLESETH T, CALDERBANK A R. *An upper bound for Weil exponential sums over Galois rings and applications* [J]. IEEE. Trans. Inform. Theory, 1995, **41**(2): 456–468.

[8] HELLESETH T, KUMAR P V, SHANBHAG A G. *Exponential sums over Galois rings and their applications* [C]. In: Finite Fields and Applications, S.D.Cohen and H.Nierreiter edited, London Math. Soc. Lecture Notes Series 233, Cambridge Univ. Press, 1996, 109–128.

[9] SHANBHAG A G, KUMAR P V, HELLESETH T. *Upper bound for a hybrid sum over Galois rings with applications to aperiodic correlation of some q-ary sequences* [J], IEEE. Trans. Inform. Theory, 1996, **42**(1): 250–254.

Z_{p^e} 上本原序列的元素分布

范 淑 琴， 韩 文 报

(解放军信息工程大学信息工程学院应用数学系， 河南 郑州 450002)

摘 要: 文研究了 Z_{p^e} 上本原序列的元素分布. 利用 Galois 环上的指数和估计和本原序列的迹表示，得到了 Z_{p^e} 中各元素在本原序列的一个周期中出现频率的一个估计. 当 $n > 4e$ 时 (n 为本原序列生成多项式的次数). 我们的估计优于 Kuzmin 的结果 [1].

关键词: 环上本原序列；元素分布；指数和.