MATHEMATICS OF COMPUTATION
Volume 77, Number 263, July 2008, Pages 1623–1637
S 0025-5718(08)02075-9
Article electronically published on January 31, 2008

ON THE DISTINCTNESS OF MODULAR REDUCTIONS OF MAXIMAL LENGTH SEQUENCES MODULO ODD PRIME POWERS

XUAN-YONG ZHU AND WEN-FENG QI

Abstract. We discuss the distinctness problem of the reductions modulo M of maximal length sequences modulo powers of an odd prime p, where the integer M has a prime factor different from p. For any two different maximal length sequences generated by the same polynomial, we prove that their reductions modulo M are distinct. In other words, the reduction modulo M of a maximal length sequence is proved to contain all the information of the original sequence.

1. Introduction

Pseudo-random sequences are important in many areas of communications and computing, such as cryptography, spread spectrum communications, error correcting codes, and Monte Carlo Integration. Linear recurring sequences and their varieties are important subjects in the research of pseudo-random sequences.

For an integer $N \geq 2$, let $\mathbb{Z}/(N)$ be the integer residue ring modulo N, which can also be represented as $\{0, 1, \cdots, N-1\}$. In this paper, given a positive integer $m \geq 2$, we always consider $a(\mathrm{mod}\, m)$ to be an element in $\{0, 1, \cdots, m-1\}$.

A sequence $\underline{a} = (a(t))_{t\geq 0}$ over $\mathbb{Z}/(N)$ satisfying the recursion

$$a(i+n) = -[c_0 a(i) + c_1 a(i+1) + \cdots + c_{n-1} a(i+n-1)](\mathrm{mod}\, N), i = 0, 1, 2, \cdots,$$

is called *a linear recurring sequence* of degree n over $\mathbb{Z}/(N)$, generated by $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in \mathbb{Z}/(N)[x]$. For convenience, denote $G(f(x), N)$ as the set of all linear recurring sequences over $\mathbb{Z}/(N)$ generated by $f(x)$. Linear recurring sequences have been studied for a hundred years, and their behavior is closely linked to the properties of the polynomial $f(x)$, although in the case that N is not a prime the elements of the sequence come from a finite ring, rather than a finite field (as is the usual case). For more considerations on linear recurring sequences over a finite field, please see [11]. Reference [9] is a good introduction on linear recurring sequences over an integer residue ring.

Let M be an integer with $2 \leq M < N$. By reducing each element in the sequence $\underline{a} \in G(f(x), N)$ modulo M, we can naturally obtain a pseudo-random

Received by the editor August 9, 2004 and, in revised form, May 24, 2007.
2000 *Mathematics Subject Classification.* Primary 11B50, 94A55.
Key words and phrases. Integer residue ring, linear recurring sequence, primitive polynomial, primitive sequence, modular reduction.
This work was supported by the National 863 Plan of China (Grant 2006AA01Z417) and the National Natural Science Foundation of China (Grant 60673081).
This paper is in final form and no version of it will be submitted for publication elsewhere.

sequence over $\mathbb{Z}/(M)$ of which the successive terms are quite difficult to predict, since the operation of $\bmod M$ destroys the linear structure of the original sequence $\underline{a} \in G(f(x), N)$. Sequences of this kind have applications in a variety of situations, such as cryptography and parallel calculations. Typically one needs to have a large class of distinct sequences to work with. Since $M < N$ there is an obvious risk that the reductions modulo M of several different sequences might be the same. If this were to happen, then any application involving several such sequences would need to have a built-in test to verify that duplicate sequences were not being used. Moreover, there would be a risk that some simple predictive algorithm might be used to discover the parameters that were used to define the sequence.

The distinctness problem of reductions modulo M of the sequences in $G(f(x), N)$ gradually become an important topic. In this paper, we discuss this problem for the case of $N = p^e$, powers of an odd prime p. We obtain the following result. Let M be a positive integer which has a prime factor other than p. If $f(x)$ is a polynomial with maximal period over $\mathbb{Z}/(p^e)$, then the reductions modulo M of any two different sequences in $G(f(x), p^e)$ are also different. That is, $\underline{a} = \underline{b}$ if and only if $\underline{a} \equiv \underline{b} (\bmod M)$ for $\underline{a}, \underline{b} \in G(f(x), p^e)$. Furthermore, we also prove that the period of the reduction sequence is equal to that of the original sequence. (Note that, during the reviewing process of this paper, we have obtained similar results for the case of $N = 2^e$.)

In a large literature, such modular reduction of sequences is considered as a kind of compression map. If the reductions of any two different sequences are distinct, then the compression map is said to be injective. An injective compression map implies that the compression sequence contains all the information of its original sequence, which means, once the compression sequence is known, we can uniquely determine its original sequence. That is to say, the original sequence can be recovered from its compression sequence in theory.

During the last ten years there have been a number of people discussing other forms of reductions of maximal length sequences modulo powers of a prime p. In [5], Huang and Dai have proven that the significant p-adic level sequences of any two different maximal length sequences are different. (Please see Theorem 3.1 in this paper.) Many other general injective compression maps are extensively studied. (See [5], [7], [10], [14], [15], [16], [21] and [22].)

Feedback with carry shift register sequences (FCSR sequences), especially l-sequences (or maximal length FCSR sequences), are attracting more and more attention in the area of pseudorandom sequences. They are thought to be a source of ideal pseudorandom sequences (see [3], [4], [8], [17] and [18]). Through the exponential representation of FCSR sequences (see [8]), it can be found that, in fact, an FCSR sequence is the reduction modulo 2 of a linear recurring sequence of degree 1 over $\mathbb{Z}/(m)$ with odd positive integer $m \geq 3$. From this point of view, an l-sequence is simply the reduction modulo 2 of a maximal length sequence of degree 1 over $\mathbb{Z}/(p^e)$, where p is an odd prime and 2 is a primitive root modulo p^e. Suppose $\underline{a}$ is a maximal length sequence of degree n over $\mathbb{Z}/(p^e)$. Then $\underline{a}$ can be considered as a natural extension of l-sequences. In this paper, for any two different maximal length sequences over $\mathbb{Z}/(p^e)$, generated by the same polynomial, we show that their reductions modulo 2 are distinct (just the case of $q = 2$ in Theorem 4.1).

The rest of this paper is arranged as follows. In Section 2, some results are presented on the sequences and polynomials modulo prime powers. In Section 3,

we discuss the uniqueness of the distribution of zeroes of the level sequence, which is the basis of dealing with our main problem. In Section 4, we discuss the distinctness of modular reductions of sequences modulo odd prime powers and obtain the main result of this paper.

2. Sequences and polynomials modulo prime powers

Let p be a prime number, integer $e \geq 1$, and $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ be a monic polynomial of degree n over $\mathbb{Z}/(p^e)$. If $f(0) \not\equiv 0 (\mathrm{mod}\, p)$, then there always exists a positive integer P such that $f(x)$ divides $x^P - 1$ over $\mathbb{Z}/(p^e)$. The least such P is called the period of $f(x)$ over $\mathbb{Z}/(p^e)$ and denoted by $\mathrm{per}(f(x), p^e)$. Denote $T = \mathrm{per}(f(x), p)$, and we have $x^T \equiv 1 + ph_1(x) (\mathrm{mod}\, f(x))$ and

$$x^{p^{i-1}T} \equiv 1 + p^i h_i(x) (\mathrm{mod}\, f(x)), i = 1, 2, \ldots, e-1, \tag{2.1}$$

where $h_i(x)$ is a polynomial over $\mathbb{Z}/(p^e)$ of degree less than n. Thus $\mathrm{per}(f(x), p^e) \leq p^{e-1}T$. On the other hand, $T = \mathrm{per}(f(x), p) \leq p^n - 1$, where $n = \deg f(x)$, so that we have $\mathrm{per}(f(x), p^e) \leq p^{e-1}(p^n - 1)$.

Definition 2.1. Let $f(x)$ be a monic polynomial of degree n over $\mathbb{Z}/(p^e)$ with prime p and positive integer e. Then $f(x)$ is called a **primitive polynomial** over $\mathbb{Z}/(p^e)$ if

$$\mathrm{per}(f(x), p^e) = p^{e-1}(p^n - 1).$$

In some literature, e.g. [1], [14] and [19], a primitive polynomial is also called a **maximal period polynomial**. Ward in [19] proved that $f(x)$ is a primitive polynomial over $\mathbb{Z}/(p^e)$ if and only if $f(x) (\mathrm{mod}\, p)$ is a primitive polynomial over $\mathbb{Z}/(p)$ and $h_{e-1}(x) \not\equiv 0 (\mathrm{mod}\, p)$, where $h_{e-1}(x)$ is defined by (2.1). Furthermore, Huang and Dai in [2] and [6] presented the coefficient criteria to judge whether a polynomial over $\mathbb{Z}/(p^e)$ is primitive or not. For more considerations on primitive polynomials over $\mathbb{Z}/(p^e)$, please see [2], [6], [10], [13] and [19].

Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$. Then it is clear that $f(x) (\mathrm{mod}\, p^i)$ is also a primitive polynomial over $\mathbb{Z}/(p^i)$, whose period is

$$\mathrm{per}(f(x), p^i) = p^{i-1}(p^n - 1)$$

for $i = 1, 2, \ldots, e-1$. In particular, $f(x) (\mathrm{mod}\, p)$ is a primitive polynomial over the prime field $\mathrm{GF}(p)$; see [11]. Thus, we have

$$x^{p^{i-1}T} \equiv 1 + p^i h_i(x) (\mathrm{mod}\, f(x)), i = 1, 2, \ldots, e-1,$$

where $T = \mathrm{per}(f(x), p) = p^n - 1$ and $h_i(x)$ is a polynomial over $\mathbb{Z}/(p^e)$ of degree less than n satisfying $h_i(x) \not\equiv 0 (\mathrm{mod}\, p)$. Clearly, $h_i(x)$ is coprime with $f(x) (\mathrm{mod}\, p)$ over $\mathbb{Z}/(p)$. Furthermore, we have (see [1, 7])

(1) if $p = 2$, then $h_2(x) \equiv h_3(x) \equiv \cdots \equiv h_{e-1}(x) \not\equiv 0 (\mathrm{mod}\, 2)$ and $h_2(x) = h_1(x)^2 + h_1(x) (\mathrm{mod}\, f(x))$.
(2) if $p \geq 3$, then $h_1(x) \equiv h_2(x) \equiv \cdots \equiv h_{e-1}(x) \not\equiv 0 (\mathrm{mod}\, p)$.

From the above results, we can easily deduce the following proposition.

Proposition 1. *Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ with odd prime p and positive integer e. Then there exists a unique polynomial $h(x)$ over $\{0, 1, \ldots, p-1\}$ with $\deg h(x) < n$, such that*

$$x^{p^{i-1} \cdot T} \equiv 1 + p^i \cdot h(x) (\mathrm{mod}\, f(x), p^{i+1}), i = 1, 2, \ldots, e-1, \tag{2.2}$$

where $T = p^n - 1$.

Any element a in $\mathbb{Z}/(p^e)$ has a unique p-adic expansion as

$$a = a_0 + a_1 \cdot p + \cdots + a_{e-1} \cdot p^{e-1},$$

where $a_i \in \{0, 1, \ldots, p-1\}$ for $0 \leq i \leq e-1$. Similarly, a sequence $\underline{a}$ over $\mathbb{Z}/(p^e)$ also has a unique p-adic expansion as

$$\underline{a} = \underline{a}_0 + \underline{a}_1 \cdot p + \cdots + \underline{a}_{e-1} \cdot p^{e-1},$$

where each $\underline{a}_i$ is a sequence over $\{0, 1, \ldots, p-1\}$, and is called the i-th level component (or sequence) of $\underline{a}$, for $0 \leq i \leq e-1$. $\underline{a}_{e-1}$ is also called the highest-level component (or sequence) of $\underline{a}$. They can be naturally considered as the sequences over the finite field $\mathrm{GF}(p)$.

Let $\underline{a} = (a(t))_{t\geq 0}$ and $\underline{b} = (b(t))_{t\geq 0}$ be sequences over $\mathbb{Z}/(p^e)$ and $c \in \mathbb{Z}/(p^e)$. Define $\underline{a} + \underline{b} = (a(t) + b(t) (\mathrm{mod}\, p^e))_{t\geq 0}$, $c\underline{a} = (c \cdot a(t) (\mathrm{mod}\, p^e))_{t\geq 0}$ and the shift operator x^k as $x^k \underline{a} = (a(t+k))_{t\geq 0}$ for $k = 0, 1, 2, \ldots$. Then we have

$$G(f(x), p^e) = \{\underline{a} \in (\mathbb{Z}/(p^e))^\infty \mid f(x)\underline{a} = \underline{0}\}$$

and we set

$$G'(f(x), p^e) = \{\underline{a} \in G(f(x), p^e) \mid \underline{a} \not\equiv \underline{0} (\mathrm{mod}\, p)\}.$$

Definition 2.2. Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ with prime p and positive integer e. Any sequence $\underline{a}$ in $G'(f(x), p^e)$ is called *a* **primitive sequence** over $\mathbb{Z}/(p^e)$, generated by $f(x)$.

In some literature, e.g. [1], [14] and [19], primitive sequences are also called **maximal length sequences**. Primitive sequences over $\mathbb{Z}/(p)$ are so-called m-sequences; see [11]. For more discussions on primitive sequences over $\mathbb{Z}/(p^e)$ and their highest-level sequences, see [1], [5], [9], [10], [13], [15] and [19].

We can easily deduce that the number of primitive sequences in $G'(f(x), p^e)$ is $p^{en} - p^{(e-1)n}$, and the number of distinct cycles of primitive sequences in $G'(f(x), p^e)$ is $p^{(e-1)(n-1)}$. These two numbers grow rapidly as e and n increase, so that primitive sequences over $\mathbb{Z}/(p^e)$ are very abundant.

For a periodic sequence $\underline{\alpha} = (\alpha(t))_{t\geq 0}$, let $\mathrm{per}(\underline{\alpha})$ denote the period of $\underline{\alpha}$, which is the least positive integer P such that $\alpha(t+P) = \alpha(t)$ for all $t = 0, 1, \ldots$. As in [1], we have

Proposition 2. *Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ with prime p and integer $e \geq 2$, $\underline{a} \in G(f(x), p^e)$ and $T = p^n - 1$. Then*

1. $\mathrm{per}(\underline{a}_{e-1}) = \mathrm{per}(\underline{a})$, *that is to say, sequences $\underline{a}$ and $\underline{a}_{e-1}$ have the same period;*
2. *if $\underline{a}_0 = \underline{a}_1 = \cdots = \underline{a}_{i-1} = \underline{0}$ and $\underline{a}_i \neq \underline{0}$ with $1 \leq i \leq e-1$, then*
$$\mathrm{per}(\underline{a}) = p^{-i} \cdot \mathrm{per}(f(x), p^e) = p^{e-1-i} \cdot T;$$
3. *if $\underline{a}_0 \neq \underline{0}$, then $\mathrm{per}(\underline{a}) = \mathrm{per}(f(x), p^e) = p^{e-1} \cdot T$ and $\mathrm{per}(\underline{a} \bmod p^i) = p^{i-1} \cdot T$ for $i = 1, 2, \ldots, e$.*

Proposition 3. *Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ with odd prime p and integer $e \geq 2$. For $\underline{a} \in G'(f(x), p^e)$, set $\underline{\alpha} = h(x)\underline{a}_0 (\mathrm{mod}\, p)$, where $h(x)$ is defined by (2.2). Then*

$$a(t + p^{e-1}T/2) \equiv -a(t) (\mathrm{mod}\, p^e), t \geq 0, \tag{2.3}$$

$$a_{e-1}(t + j \cdot p^{e-2}T) \equiv a_{e-1}(t) + j \cdot \alpha(t) (\mathrm{mod}\, p), t \geq 0, \tag{2.4}$$

for $j = 0, 1, \ldots, p-1$, *where* $T = p^n - 1$. *Furthermore, if* $\alpha(t) \neq 0$, *then*

$$\{a_{e-1}(t + j \cdot p^{e-2}T) \mid j = 0, 1, \ldots, p-1\} = \{0, 1, \ldots, p-1\}. \tag{2.5}$$

Proof. Since $f(x)$ is a primitive polynomial over $\mathbb{Z}/(p^e)$, which implies that

$$\mathrm{per}(f(x), p^e) = p^{e-1} \cdot T,$$

we have that $f(x)$ divides $x^{p^{e-1}T} - 1$, but not $x^{p^{e-1}T/2} - 1$, over $\mathbb{Z}/(p^e)$. However, since

$$x^{p^{e-1}T} - 1 = (x^{p^{e-1}T/2} - 1) \cdot (x^{p^{e-1}T/2} + 1)$$

and

$$\gcd(x^{p^{e-1}T/2} - 1 (\mathrm{mod}\, p), x^{p^{e-1}T/2} + 1 (\mathrm{mod}\, p)) = 1,$$

we know that $f(x)$ divides $x^{p^{e-1}T/2} + 1$ over $\mathbb{Z}/(p^e)$ by the Hensel Lemma [12], that is, $x^{p^{e-1}T/2} = -1 (\mathrm{mod}\, f(x), p^e)$. Thus, (2.3) follows.

Let j be an integer with $1 \leq j \leq p-1$. On one hand, by (2.2), we can get

$$(x^{j \cdot p^{i-1}T} - 1)\underline{a} \equiv j \cdot p^i h(x)\underline{a} \equiv j \cdot p^i h(x)\underline{a}_0 (\mathrm{mod}\, p^{i+1}), \tag{2.6}$$

for $i = 1, 2, \ldots, e-1$. On the other hand, we have

$$(x^{j \cdot p^{i-1}T} - 1)\underline{a} \equiv (x^{j \cdot p^{i-1}T} - 1)(\textstyle\sum_{k \geq i} \underline{a}_k \cdot p^k) \equiv p^i \cdot (x^{j \cdot p^{i-1}T} - 1)\underline{a}_i (\mathrm{mod}\, p^{i+1}) \tag{2.7}$$

since $\mathrm{per}(\underline{a} \bmod p^i) = \mathrm{per}(f(x), p^i) = p^{i-1}T$, for $i = 1, 2, \ldots, e-1$. It follows from (2.6) and (2.7) that

$$(x^{j \cdot p^{i-1}T} - 1)\underline{a}_i \equiv j \cdot h(x)\underline{a}_0 (\mathrm{mod}\, p), j = 1, 2, ..., p-1,$$

for $i = 1, 2, \ldots, e-1$, implying that equation (2.4) holds. Finally, (2.5) follows from (2.4). □

3. Uniqueness of the distribution of zeroes in the highest-level sequences

Huang and Dai in [5] and Kuzmin and Nechaev in [10] independently proposed the following theorem which has important cryptographic significance.

Theorem 3.1. *Let* $f(x)$ *be a primitive polynomial over* $\mathbb{Z}/(p^e)$ *with prime* p *and positive integer* e. *Then* $\underline{a} = \underline{b}$ *if and only if* $\underline{a}_{e-1} = \underline{b}_{e-1}$ *for* $\underline{a}, \underline{b} \in G(f(x), p^e)$.

Theorem 3.1 implies that $\underline{a}_{e-1}$ contains all the information of the original sequence $\underline{a}$, which also means $\underline{a}_{e-1}$ uniquely determines the original sequence $\underline{a}$ in theory.

In this section, we discuss the uniqueness of the distribution of zeroes in the highest-level sequence $\underline{a}_{e-1}$.

Definition 3.2. Let $\underline{\alpha} = (\alpha(t))_{t \geq 0}$, $\underline{\beta} = (\beta(t))_{t \geq 0}$ and $\underline{\gamma} = (\gamma(t))_{t \geq 0}$ be sequences over a ring R. If $\alpha(t) = 0$ if and only if $\beta(t) = 0$ for all $t \geq 0$, we say that $\underline{\alpha}$ and $\underline{\beta}$ have the distribution uniformity of element 0, or $\underline{\alpha}$ and $\underline{\beta}$ are of 0-uniformity for short. If $\alpha(t) = 0$ if and only if $\beta(t) = 0$ for all t with $\gamma(t) \neq 0$, we say that $\underline{\alpha}$ and $\underline{\beta}$ are of 0-uniformity with $\gamma(t) \neq 0$.

Lemma 3.3. *Let* $f(x)$ *be a primitive polynomial of degree* n *over the finite field* $\mathrm{GF}(p)$ *and* $\underline{\alpha}, \underline{\beta} \in G'(f(x), p)$. *Then*

1. *for a polynomial* $g(x)$ *over* $\mathrm{GF}(p)$ *coprime with* $f(x)$, $g(x)\underline{\alpha}$ *and* $g(x)\underline{\beta}$ *are of* 0*-uniformity if and only if* $\underline{\alpha}$ *and* $\underline{\beta}$ *are of* 0*-uniformity;*

(2) *sequences* $\underline{\alpha}$ *and* $\underline{\beta}$ *are of* 0*-uniformity if and only if there exists a nonzero* λ *in* GF(p) *such that* $\underline{\alpha} = \lambda\underline{\beta}$.

Proof. The results are trivial for the case of $n = 1$. In the following we suppose $n \geq 2$.

Because $f(x)$ is a primitive polynomial over GF(p) and coprime with $g(x)$, there exists an integer k such that $x^k \equiv g(x) (\mathrm{mod}\, f(x))$. It follows that $\underline{\alpha}$ and $\underline{\beta}$ are of 0-uniformity if and only if $x^k\underline{\alpha}$ and $x^k\underline{\beta}$ are of 0-uniformity. The first statement is proved.

It is straightforward to see that $\underline{\alpha} = \lambda\underline{\beta}$ implies $\underline{\alpha}$ and $\underline{\beta}$ are of 0-uniformity. Note that both $\underline{\alpha}$ and $\underline{\beta}$ are m-sequences generated by $f(x)$ over GF(p). If $\underline{\alpha}$ and $\underline{\beta}$ are of 0-uniformity, then there exists an integer k with $0 \leq k < p^n - 1$ such that $x^k\underline{\alpha} = (\underbrace{0, \ldots, 0}_{n-1}, \delta_1, \ldots)$ and $x^k\underline{\beta} = (\underbrace{0, \ldots, 0}_{n-1}, \delta_2, \ldots)$, where δ_1 and δ_2 are nonzero elements in GF(p). Let $\lambda = \delta_1 \cdot \delta_2^{-1}$. That is $\delta_1 = \lambda \cdot \delta_2$. Since any sequence in $G(f(x), p)$ is uniquely determined by its initial state (the first n elements of the sequence), it follows that $x^k\underline{\alpha} = \lambda \cdot x^k\underline{\beta}$. Thus, $\underline{\alpha} = \lambda \cdot \underline{\beta}$, the necessary condition of the second statement is proved. □

Lemma 3.4. *Let* $f(x)$ *be a primitive polynomial of degree* n *over* $\mathbb{Z}/(p^e)$ *with odd prime* p *and integer* $e \geq 2$. *For* $\underline{b} \in G'(f(x), p^e)$, *set* $\underline{\beta} = h(x)\underline{b}_0 (\mathrm{mod}\, p)$, *where* $h(x)$ *is defined by* (2.2). *Then there exists an integer* s *with* $0 \leq s < p^{e-1}(p^n - 1)$ *such that* $b_{e-1}(s) = 0$, $\beta(s) \neq 0$, *and* $b(s) \not\equiv 0 (\mathrm{mod}\, p^{e-1})$.

Proof. Let $T = p^n - 1$. Both $\underline{\beta} = h(x)\underline{b}_0 (\mathrm{mod}\, p)$ and $\underline{b}_0$ are m-sequences in $G(f(x), p)$, so there is an integer s_0 with $0 \leq s_0 < T$ such that $\beta(s_0) \neq 0$ and $b_0(s_0) \neq 0$. It shows $b(s_0) (\mathrm{mod}\, p^{e-1})$ is also nonzero.

Since $\beta(s_0) \neq 0$, it follows from (2.5) in Proposition 3 that

$$\{b_{e-1}(s_0 + j \cdot p^{e-2}T) \mid j = 0, 1, \ldots, p-1\} = \{0, 1, \ldots, p-1\},$$

which implies that there exists an integer j_0 with $0 \leq j_0 \leq p - 1$ such that

$$b_{e-1}(s_0 + j_0 \cdot p^{e-2}T) = 0.$$

Let $s = s_0 + j_0 \cdot p^{e-2}T$. Then we have $\beta(s) = \beta(s_0) \neq 0$ and $b(s) (\mathrm{mod}\, p^{e-1}) = b(s_0) (\mathrm{mod}\, p^{e-1}) \neq 0$ since $p^{e-2}T$ is divisible by the periods of both $\underline{\beta}$ and $\underline{b} (\mathrm{mod}\, p^{e-1})$. Thus s is the integer we need. □

Theorem 3.5. *Let* $f(x)$ *be a primitive polynomial of degree* n *over* $\mathbb{Z}/(p^e)$ *with odd prime* p *and integer* $e \geq 2$. *Let* $\underline{a}, \underline{b} \in G'(f(x), p^e)$ *and* $\underline{\alpha} = h(x)\underline{a}_0 (\mathrm{mod}\, p)$, *where* $h(x)$ *is defined by* (2.2). *If* $\underline{a}_{e-1}$ *and* $\underline{b}_{e-1}$ *are of* 0*-uniformity with* $\alpha(t) \neq 0$, *then* $\underline{a} = \underline{b}$.

Proof. We first prove $\underline{a}_0$ and $\underline{b}_0$ are of 0-uniformity. If $\underline{a}_0$ and $\underline{b}_0$ are not of 0-uniformity, then since $h(x)$ is coprime with $f(x) (\mathrm{mod}\, p)$, $\underline{\alpha} = h(x)\underline{a}_0 (\mathrm{mod}\, p)$ and $\underline{\beta} = h(x)\underline{b}_0 (\mathrm{mod}\, p)$ are also not of 0-uniformity by Lemma 3.3. It implies that m-sequences $\underline{\alpha}$ and $\underline{\beta}$ are linearly independent, so there exists an integer t_0 such that $\alpha(t_0) = \delta \neq 0$ and $\beta(t_0) = 0$.

Let $T = p^n - 1$. By (2.4) in Proposition 3, we have

$$\begin{aligned} a_{e-1}(t_0 + jp^{e-2}T) &\equiv a_{e-1}(t_0) + j \cdot \alpha(t_0) \equiv a_{e-1}(t_0) + j\delta (\mathrm{mod}\, p), \\ b_{e-1}(t_0 + jp^{e-2}T) &\equiv b_{e-1}(t_0) + j \cdot \beta(t_0) \equiv b_{e-1}(t_0) (\mathrm{mod}\, p) \end{aligned}$$

for $j = 0, 1, \ldots, p-1$. Since $\alpha(t_0) = \delta \neq 0$ and $\beta(t_0) = 0$, there exists j_0 with $0 \leq j_0 \leq p-1$ such that one of the two numbers $a_{e-1}(t_0 + j_0 \cdot p^{e-2}T)$ and $b_{e-1}(t_0 + j_0 \cdot p^{e-2}T)$ is zero while the other one is nonzero. Since $\alpha(t_0 + j_0 \cdot p^{e-2}T) = \alpha(t_0) \neq 0$, this contradicts the fact that $\underline{a}_{e-1}$ and $\underline{b}_{e-1}$ are of 0 -uniformity with $\alpha(t) \neq 0$. Thus $\underline{a}_0$ and $\underline{b}_0$ are of 0-uniformity.

Next we prove $\underline{a}_0 = \underline{b}_0$. Since $\underline{a}_0$ and $\underline{b}_0$ are m-sequences over $\mathrm{GF}(p)$ and of 0-uniformity, we have, by Lemma 3.3, $\underline{a}_0 \equiv \lambda \cdot \underline{b}_0 (\mathrm{mod}\, p)$ and $h(x)\underline{a}_0 \equiv \lambda \cdot h(x)\underline{b}_0 (\mathrm{mod}\, p)$, where $\lambda \in \{1, 2, \ldots, p-1\}$. That is, $\underline{\alpha} \equiv \lambda \cdot \underline{\beta} (\mathrm{mod}\, p)$.

For any index t, we claim that

$$\alpha(t) \neq 0 \Longrightarrow a_{e-1}(t) \equiv \lambda \cdot b_{e-1}(t) (\mathrm{mod}\, p). \tag{3.1}$$

If $\alpha(t) \neq 0$, then, by (2.5) in Proposition 3, we have

$$\{a_{e-1}(t + j \cdot p^{e-2}T) \mid j = 0, 1, \ldots, p-1\} = \{0, 1, \ldots, p-1\}.$$

It implies that there exists j with $0 \leq j \leq p-1$ such that $a_{e-1}(t + jp^{e-2}T) = 0$. Since $\underline{a}_{e-1}$ and $\underline{b}_{e-1}$ are of 0-uniformity with $\alpha(t) \neq 0$, it follows that $b_{e-1}(t + jp^{e-2}T) = 0$. Thus, by (2.4) in Proposition 3, we have $a_{e-1}(t) = -j \cdot \alpha(t) (\mathrm{mod}\, p)$ and $b_{e-1}(t) = -j \cdot \beta(t) (\mathrm{mod}\, p)$, which implies that $a_{e-1}(t) \equiv \lambda \cdot b_{e-1}(t) (\mathrm{mod}\, p)$. The claim is proved.

By Lemma 3.4, there exists an integer s_0 with $0 \leq s_0 < p^{e-1}T$ such that

$$\beta(s_0) \neq 0,\ b_{e-1}(s_0) = 0, \text{ and } b(s_0) \not\equiv 0 (\mathrm{mod}\, p^{e-1}).$$

Since $\underline{\alpha} \equiv \lambda \cdot \underline{\beta} (\mathrm{mod}\, p)$, we have $\alpha(s_0) \equiv \lambda \cdot \beta(s_0) \not\equiv 0 (\mathrm{mod}\, p)$. Thus we have $a_{e-1}(s_0) = \lambda \cdot b_{e-1}(s_0) = 0$ by (3.1).

Since $b(s_0 + p^{e-1}T/2) = p^e - b(s_0) (\mathrm{mod}\, p^e)$ by (2.3) in Proposition 3, $b(s_0) \not\equiv 0 (\mathrm{mod}\, p^{e-1})$ and $b_{e-1}(s_0) = 0$, we get

$$b_{e-1}(s_0 + p^{e-1}T/2) = p - 1 - b_{e-1}(s_0) = p - 1. \tag{3.2}$$

By the same argument, if $a(s_0) \not\equiv 0 (\mathrm{mod}\, p^{e-1})$, then $a_{e-1}(s_0 + p^{e-1}T/2) = p-1$. It shows that

$$a_{e-1}(s_0 + p^{e-1}T/2) = b_{e-1}(s_0 + p^{e-1}T/2) \neq 0.$$

Since $a_{e-1}(t) = \lambda \cdot b_{e-1}(t) (\mathrm{mod}\, p)$ for $t = s_0 + p^{e-1}T/2$, we have $\lambda = 1$.

If $a(s_0) = 0 (\mathrm{mod}\, p^{e-1})$, then $a(s_0) = 0$ follows from $a(s_0) = a(s_0) (\mathrm{mod}\, p^{e-1}) + a_{e-1}(s_0)$ and $a_{e-1}(s_0) = 0$. By (2.3) in Proposition 3, we have $a(s_0 + p^{e-1}T/2) = -a(s_0) = 0 (\mathrm{mod}\, p^e)$, implying that $a_{e-1}(s_0 + p^{e-1}T/2) = 0$. On the other hand, $b_{e-1}(s_0 + p^{e-1}T/2) = p - 1$ by (3.2). Note that $\alpha(s_0 + p^{e-1}T/2) = -\alpha(s_0) \neq 0 (\mathrm{mod}\, p)$, so that we get a contradiction to the fact that $\underline{a}_{e-1}$ and $\underline{b}_{e-1}$ are of 0-uniformity with $\alpha(t) \neq 0$.

Finally we prove $\underline{a} = \underline{b}$. Since we have already shown that $\lambda = 1$ in (3.1), it follows from (3.1) that $a_{e-1}(t) = b_{e-1}(t)$ for any t with $\alpha(t) \neq 0$.

Let $\underline{c} = \underline{a} - \underline{b} (\mathrm{mod}\, p^e)$. Then $\underline{c} \in G(f(x), p^e)$ and $\underline{c}_{e-1} = \underline{a}_{e-1} - \underline{b}_{e-1} + \underline{\delta} (\mathrm{mod}\, p)$, where $\underline{\delta} = (\delta(t))_{t \geq 0}$ is defined by

$$\delta(t) = \begin{cases} 0, & \text{if } a(t) (\mathrm{mod}\, p^{e-1}) \geq b(t) (\mathrm{mod}\, p^{e-1}), \\ -1, & \text{if } a(t) (\mathrm{mod}\, p^{e-1}) < b(t) (\mathrm{mod}\, p^{e-1}). \end{cases}$$

Thus, it can be shown that $c_{e-1}(t) \in \{0, p-1\}$ for any integer t with $\alpha(t) \neq 0$.

If $\underline{a} \neq \underline{b}$, then $\underline{c} \neq \underline{0}$. Let $\underline{c} = p^r \cdot \underline{u}$, where $0 \leq r \leq e-1$ and $\underline{u} \in G'(f(x), p^{e-r})$. If $r = e-1$, then there exists an integer t such that $\alpha(t) \neq 0$ and $c_{e-1}(t) = 1$ since both $\underline{c}_{e-1}$ and $\underline{\alpha}$ are m-sequences in $G(f(x), p)$. Note that p is an odd prime, so

that it is a contradiction to $c_{e-1}(t) \in \{0, p-1\}$. If $0 \leq r < e-1$, then $e-r \geq 2$. We have that $\underline{\alpha}$, $\underline{u}_0$ and $\underline{\gamma} = h(x)\underline{u}_0 (\mathrm{mod}\, p)$ are m-sequences in $G(f(x), p)$. Then there exists an integer t, such that $\alpha(t) \neq 0$ and $\gamma(t) \neq 0$. From (2.5) in Proposition 3, we know that

$$\{u_{e-1-r}(t + j \cdot p^{e-2-r}T) \mid j = 0, 1, \ldots, p-1\} = \{0, 1, \ldots, p-1\}. \tag{3.3}$$

Because p is an odd prime and $\underline{u}_{e-1-r} = \underline{c}_{e-1}$, (3.3) is a contradiction to the fact that $c_{e-1}(t) \in \{0, p-1\}$ for t with $\alpha(t) \neq 0$. Thus $\underline{a} = \underline{b}$. □

Remark 3.6. Partial result of Theorem 3.5 can be found in [20].

4. The distinctness of modular reductions of primitive sequences

This section are mainly devoted to the proof of Theorem 4.1.

Theorem 4.1. *Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ with odd prime p and positive integer e. For any prime q different from p, $\underline{a} = \underline{b}$ if and only if $\underline{a} \equiv \underline{b} (\mathrm{mod}\, q)$ for $\underline{a}$, $\underline{b} \in G(f(x), p^e)$. Furthermore,* $\mathrm{per}(\underline{a} \bmod q) = \mathrm{per}(\underline{a})$ *for $\underline{a} \in G(f(x), p^e)$.*

Corollary 1. *Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ with odd prime p and positive integer e. For any prime q different from p and positive integer k, $\underline{a} = \underline{b}$ if and only if $\underline{a} \equiv \underline{b} (\mathrm{mod}\, q^k)$ for $\underline{a}$, $\underline{b} \in G(f(x), p^e)$.*

Theorem 4.2 immediately follows from Corollary 1 and the Chinese Reminder Theorem, which is the main result of the paper.

Theorem 4.2. *Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ with odd prime p and positive integer e. For any positive integer M which has a prime factor different from p, $\underline{a} = \underline{b}$ if and only if $\underline{a} \equiv \underline{b} (\mathrm{mod}\, M)$ for $\underline{a}, \underline{b} \in G(f(x), p^e)$. Furthermore,* $\mathrm{per}(\underline{a} \bmod M) = \mathrm{per}(\underline{a})$ *for $\underline{a} \in G(f(x), p^e)$.*

Before proceeding to prove Theorem 4.1, we first present several lemmas.

Lemma 4.3. *Let p and q be two different primes and $p \geq 3$. Let $\lambda, \delta, \alpha, \beta \in \{1, 2, \ldots, p-1\}$ with $\delta \equiv 0 (\mathrm{mod}\, q)$ and $\alpha \equiv \lambda\beta (\mathrm{mod}\, p)$. If $1 \leq \lambda < p-1$, then there exists an integer j with $1 \leq j \leq p-1$ such that $j \cdot \alpha (\mathrm{mod}\, p) (\mathrm{mod}\, q) \neq j \cdot \beta + \delta (\mathrm{mod}\, p) (\mathrm{mod}\, q)$.*

Proof. It suffices to consider the case of $2 \leq q < p$. Since $\alpha \equiv \lambda\beta (\mathrm{mod}\, p)$, we have

$$\begin{aligned} & \{(j \cdot \alpha (\mathrm{mod}\, p), j \cdot \beta + \delta (\mathrm{mod}\, p)) \mid j = 0, 1, \ldots, p-1\} \\ = \; & \{(j \cdot \lambda (\mathrm{mod}\, p), j + \delta (\mathrm{mod}\, p)) \mid j = 0, 1, \ldots, p-1\}. \end{aligned}$$

Without loss of generality, we assume that $\alpha = \lambda$ and $\beta = 1$. In the following, we prove that there exists an integer j with $1 \leq j \leq p-1$ such that

$$j \cdot \lambda (\mathrm{mod}\, p) (\mathrm{mod}\, q) \neq j + \delta (\mathrm{mod}\, p) (\mathrm{mod}\, q). \tag{4.1}$$

(1) $\lambda = 1$.

Here $(p-\delta) + \delta (\mathrm{mod}\, p) (\mathrm{mod}\, q) = 0$. Since $\gcd(p, q) = 1$ and $\delta \equiv 0 (\mathrm{mod}\, q)$, we have $(p-\delta) \cdot \lambda (\mathrm{mod}\, p) (\mathrm{mod}\, q) = (p-\delta) (\mathrm{mod}\, q) \neq 0$. Thus (4.1) holds for $j = p - \delta$.

(2) $2 \le \lambda \le p-2$ and $2 \le \delta < p-1$.

If $\lambda(\mathrm{mod}\, q) = 0$, then $1 \cdot \lambda(\mathrm{mod}\, p)(\mathrm{mod}\, q) = 0$. On the other hand, since $2 \le \delta < p-1$ and $\delta \equiv 0(\mathrm{mod}\, q)$, we have $1 + \delta(\mathrm{mod}\, p)(\mathrm{mod}\, q) = 1$. Thus (4.1) holds for $j = 1$.

If $\lambda(\mathrm{mod}\, q) \neq 0$, let k_1 be the integer such that $(k_1 - 1)\lambda < p < k_1\lambda$. It is clear that $k_1 \ge 2$.

(a) Suppose $k_1 > p - \delta$.
Here $(p-\delta)\lambda < p$, and we can get $(p-\delta)\lambda(\mathrm{mod}\, q) \neq 0$ from $\lambda(\mathrm{mod}\, q) \neq 0$ and $\gcd(p, q) = 1$. On the other hand, $(p - \delta) + \delta(\mathrm{mod}\, p) = 0$. Thus (4.1) holds for $j = p - \delta$.

(b) Suppose $k_1 < p - \delta$ and $\lambda(\mathrm{mod}\, q) \neq 1$.
Here $\lambda(\mathrm{mod}\, p)(\mathrm{mod}\, q) \neq 1$ and $1 + \delta(\mathrm{mod}\, p)(\mathrm{mod}\, q) = 1$. Thus (4.1) holds for $j = 1$.

(c) Suppose $k_1 < p - \delta$ and $\lambda(\mathrm{mod}\, q) = 1$.
Here we have $k_1\lambda(\mathrm{mod}\, p)(\mathrm{mod}\, q) = (k_1\lambda - p)(\mathrm{mod}\, q) = k_1 - p(\mathrm{mod}\, q)$. On the other hand, since $k_1 < p - \delta$ and $\delta \equiv 0(\mathrm{mod}\, q)$, we have $k_1 + \delta(\mathrm{mod}\, p)(\mathrm{mod}\, q) = k_1 + \delta(\mathrm{mod}\, q) = k_1(\mathrm{mod}\, q)$. Since $\gcd(p, q) = 1$, we have $k_1 - p(\mathrm{mod}\, q) \neq k_1(\mathrm{mod}\, q)$. Thus (4.1) holds for $j = k_1$.

(d) Suppose $k_1 = p - \delta$ and $\lambda = 2$.
Here $\lambda(\mathrm{mod}\, p)(\mathrm{mod}\, q) = 2$ and $1 + \delta(\mathrm{mod}\, p)(\mathrm{mod}\, q) = 1$. Thus (4.1) holds for $j = 1$.

(e) Suppose $k_1 = p - \delta$ and $3 \le \lambda \le p - 2$.
Case 1. $\lambda(\mathrm{mod}\, q) \neq 1$.
Clearly $(p-\delta) + \delta(\mathrm{mod}\, p) = 0$. On the other hand, from the definition of k_1 and $k_1 = p - \delta$, we can get $(p - \delta)\lambda(\mathrm{mod}\, p)(\mathrm{mod}\, q) = (p - \delta)\lambda - p(\mathrm{mod}\, q) = p(\lambda - 1)(\mathrm{mod}\, q)$. Because $\gcd(p, q) = 1$ and $\lambda(\mathrm{mod}\, q) \neq 1$, we have $p(\lambda - 1)(\mathrm{mod}\, q) \neq 0$. Thus (4.1) holds for $j = p - \delta$.
Case 2. $\lambda(\mathrm{mod}\, q) = 1$.
Since $3 \le \lambda \le p - 2$, we have $p \ge 5$ and $(p - 1)\lambda > 2p$. Let k_2 be the integer such that $(k_2 - 1)\lambda < 2p < k_2\lambda$. Then $p - \delta = k_1 < k_2 \le p - 1$, so that $k_2\lambda(\mathrm{mod}\, p)(\mathrm{mod}\, q) = k_2\lambda - 2p(\mathrm{mod}\, q) \equiv k_2 - 2p(\mathrm{mod}\, q)$. On the other hand, because $p - \delta = k_1 < k_2 \le p - 1$, we have $k_2 + \delta(\mathrm{mod}\, p)(\mathrm{mod}\, q) = k_2 + \delta - p(\mathrm{mod}\, q) \equiv k_2 - p(\mathrm{mod}\, q)$. Furthermore, since $\gcd(p, q) = 1$, we have $k_2 - 2p(\mathrm{mod}\, q) \not\equiv k_2 - p(\mathrm{mod}\, q)$. Thus (4.1) holds for $j = k_2$.

(3) $2 \le \lambda \le p - 2$ and $\delta = p - 1$.

If $\lambda(\mathrm{mod}\, q) \neq 0$, then $\lambda(\mathrm{mod}\, p)(\mathrm{mod}\, q) \neq 0$ and $1 + \delta(\mathrm{mod}\, p)(\mathrm{mod}\, q) = 0$. Thus (4.1) holds for $j = 1$.

If $\lambda(\mathrm{mod}\, q) = 0$, we can get $2 \le \lambda \le p - 1 - q$ from $2 \le \lambda \le p - 2$ and $\delta = p - 1 \equiv 0(\mathrm{mod}\, q)$. So $p - \lambda \ge q + 1$. Assume k to be the least positive integer such that $k\lambda(\mathrm{mod}\, p) < p - \lambda$. Clearly $1 \le k \le p - q$. Thus

$$\begin{aligned} k\lambda(\mathrm{mod}\, p)(\mathrm{mod}\, q) &= (k+1)\lambda(\mathrm{mod}\, p)(\mathrm{mod}\, q), \\ k + (p-1)(\mathrm{mod}\, p)(\mathrm{mod}\, q) &\neq (k+1) + (p-1)(\mathrm{mod}\, p)(\mathrm{mod}\, q) \end{aligned}$$

which implies that $(k+1)\lambda(\mathrm{mod}\, p)(\mathrm{mod}\, q) \neq (k+1) + (p-1)(\mathrm{mod}\, p)(\mathrm{mod}\, q)$ or $k\lambda(\mathrm{mod}\, p)(\mathrm{mod}\, q) \neq k + (p-1)(\mathrm{mod}\, p)(\mathrm{mod}\, q)$. Thus (4.1) holds for $j = k$ or $k + 1$. □

Lemma 4.4. *Let p and q be two different primes and $p \geq 3$. Let $f(x)$ be a primitive polynomial over $\mathbb{Z}/(p^e)$ with integer $e \geq 2$. For $\underline{a}, \underline{b} \in G'(f(x), p^e)$, set $\underline{\alpha} = h(x)\underline{a}_0(\mathrm{mod}\, p)$ and $\underline{\beta} = h(x)\underline{b}_0(\mathrm{mod}\, p)$, where $h(x)$ is defined by (2.2). If $\underline{a} \not\equiv -\underline{b}(\mathrm{mod}\, p^e)$ and $\underline{\alpha} \equiv (p-1)\underline{\beta}(\mathrm{mod}\, p)$, then there exists an integer $t_0 \geq 0$ such that $\alpha(t_0) \neq 0$ and $a_{e-1}(t_0) \not\equiv b_{e-1}(t_0)(\mathrm{mod}\, q)$.*

Proof. It suffices to consider the case of $2 \leq q < p$. Let ζ be the least positive integer such that $p - \zeta \equiv 0(\mathrm{mod}\, q)$. Thus $p - \zeta + j(\mathrm{mod}\, q) \neq 0$ for $1 \leq j \leq \zeta - 1$.

Assume that $a_{e-1}(t) \equiv b_{e-1}(t)(\mathrm{mod}\, q)$ for any integer t with $\alpha(t) \neq 0$. Then we claim that

$$\alpha(t) \neq 0 \Longrightarrow a_{e-1}(t) + b_{e-1}(t) = p - \zeta, t \geq 0. \tag{4.2}$$

Let t be an integer such that $\alpha(t) \neq 0$. Suppose $a_{e-1}(t) + b_{e-1}(t)(\mathrm{mod}\, p) = \tau$ with $0 \leq \tau < p$. By (2.4), we have

$$\begin{aligned} &a_{e-1}(t + j \cdot p^{e-2}T) \equiv a_{e-1}(t) + j \cdot \alpha(t)(\mathrm{mod}\, p), j = 0, 1, \ldots, p-1; \\ &b_{e-1}(t + j \cdot p^{e-2}T) \equiv b_{e-1}(t) + j \cdot \beta(t)(\mathrm{mod}\, p), j = 0, 1, \ldots, p-1, \end{aligned} \tag{4.3}$$

where $n = \deg f(x)$ and $T = p^n - 1$. Since $\underline{\alpha} \equiv (p-1)\underline{\beta}(\mathrm{mod}\, p)$, (4.3) shows that

$$a_{e-1}(t + j \cdot p^{e-2}T) + b_{e-1}(t + j \cdot p^{e-2}T) \equiv a_{e-1}(t) + b_{e-1}(t) \equiv \tau(\mathrm{mod}\, p).$$

Since $\alpha(t) \neq 0(\mathrm{mod}\, p)$, we have

$$\{a_{e-1}(t + j \cdot p^{e-2}T) \mid j = 0, 1, \ldots, p-1\} = \{0, 1, \ldots, p-1\}$$

by (4.3). If $\tau(\mathrm{mod}\, q) \neq 0$, let j_0 be the integer such that $a_{e-1}(t + j_0 \cdot p^{e-2}T) = 0$. Thus $b_{e-1}(t+j_0 \cdot p^{e-2}T) = \tau$ and $a_{e-1}(t+j_0 \cdot p^{e-2}T) \not\equiv b_{e-1}(t+j_0 \cdot p^{e-2}T)(\mathrm{mod}\, q)$. If $\tau(\mathrm{mod}\, q) = 0$ and $\tau < p-\zeta$, let j_0 be the integer such that $a_{e-1}(t+j_0 \cdot p^{e-2}T) = p-\zeta$. Thus $b_{e-1}(t+j_0 \cdot p^{e-2}T) = \tau+\zeta$ and $a_{e-1}(t+j_0 \cdot p^{e-2}T) \not\equiv b_{e-1}(t+j_0 \cdot p^{e-2}T)(\mathrm{mod}\, q)$. Two cases are in contradiction with the assumption, so we get $\tau(\mathrm{mod}\, q) = 0$ and $\tau \geq p-\zeta$. It follows from the definition of ζ that $\tau = p-\zeta$, that is, $a_{e-1}(t)+b_{e-1}(t) = p - \zeta$. Thus the claim is proved.

Now, we can proceed to prove Lemma 4.4. Let $\underline{c} = \underline{a} + \underline{b}(\mathrm{mod}\, p^e)$. Then $\underline{c} \in G(f(x), p^e)$ and $\underline{c}_{e-1} = \underline{a}_{e-1} + \underline{b}_{e-1} + \underline{\delta}$, where $\underline{\delta} = (\delta(t))_{t \geq 0}$ is defined by

$$\delta(t) = \begin{cases} 0, \text{ if } a(t)(\mathrm{mod}\, p^{e-1}) + b(t)(\mathrm{mod}\, p^{e-1}) < p^{e-1}, \\ 1, \text{ if } a(t)(\mathrm{mod}\, p^{e-1}) + b(t)(\mathrm{mod}\, p^{e-1}) \geq p^{e-1}. \end{cases}$$

For the integer t with $\alpha(t) \neq 0$, by (4.2), we have $a_{e-1}(t) + b_{e-1}(t) = p - \zeta$, which implies that $c_{e-1}(t) \in \{p - \zeta, p - \zeta + 1(\mathrm{mod}\, p)\}$.

Since $\underline{a} \not\equiv -\underline{b}(\mathrm{mod}\, p^e)$, we know that $\underline{c} \neq \underline{0}$. Assume $\underline{c} = p^r \cdot \underline{u}$, where $0 \leq r \leq e-1$ and $\underline{u} \in G'(f(x), p^{e-r})$.

If $r = e - 1$, then $\underline{c}_{e-1}$ is an m-sequence in $G(f(x), p)$. Note that $\underline{\alpha}$ is also an m-sequence in $G(f(x), p)$. If $p = 3$, then $q = 2$, $\zeta = 1$ and $c_{e-1}(t) \in \{0, 2\}$. We can choose an integer t such that $\alpha(t) \neq 0$ and $c_{e-1}(t) = 1$. If $p \geq 5$, we can choose an integer t such that $\alpha(t) \neq 0$ and $c_{e-1}(t) = \omega$ with $\omega \in \{1, 2, \ldots, p-1\}$ but $\omega \notin \{p - \zeta, p - \zeta + 1(\mathrm{mod}\, p)\}$. Hence, for any odd prime p, we find an integer t with $\alpha(t) \neq 0$ and $c_{e-1}(t) \notin \{p - \zeta, p - \zeta + 1(\mathrm{mod}\, p)\}$, a contradiction to the fact that $c_{e-1}(t) \in \{p - \zeta, p - \zeta + 1(\mathrm{mod}\, p)\}$. Thus, $r \neq e - 1$.

If $0 \leq r < e-1$, then $e-r \geq 2$. Since $\underline{\alpha}$ and $\underline{\gamma} = h(x)\underline{u}_0(\mathrm{mod}\, p)$ are m-sequences in $G(f(x), p)$, there exists an integer t such that $\alpha(t) \neq 0$ and $\gamma(t) \neq 0$. Then it

follows from (2.5) in Proposition 3 that

$$\{u_{e-1-r}(t + j \cdot p^{e-2-r}T) \mid j = 0, 1, \ldots, p-1\} = \{0, 1, \ldots, p-1\}. \tag{4.4}$$

Since $\mathrm{per}(\underline{\alpha}) = T$, we have $\alpha(t + j \cdot p^{e-2-r}T) = \alpha(t) \neq 0$ for $j = 0, 1, \ldots, p-1$. Note that p is odd and $\underline{u}_{e-1-r} = \underline{c}_{e-1}$. Hence, (4.4) is a contradiction to the fact that $c_{e-1}(t) \in \{p - \zeta, p - \zeta + 1 (\mathrm{mod}\, p)\}$ for t with $\alpha(t) \neq 0$.

Thus the assumption of $a_{e-1}(t) \equiv b_{e-1}(t) (\mathrm{mod}\, q)$ for all integers t with $\alpha(t) \neq 0$ does not hold, and the lemma is proved. □

Lemma 4.5. *Let p and q be two different primes and $p \geq 3$. Let $f(x)$ be a primitive polynomial over $\mathbb{Z}/(p^e)$ with odd prime p and integer $e \geq 2$. For $\underline{a}, \underline{b} \in G'(f(x), p^e)$, set $\underline{\alpha} = h(x)\underline{a}_0 (\mathrm{mod}\, p)$, where $h(x)$ is defined by (2.2). If $\underline{a} \neq \pm\underline{b} (\mathrm{mod}\, p^e)$, then there exists an integer $t_0 \geq 0$ such that $\alpha(t_0) \neq 0$ and $a_{e-1}(t_0) \not\equiv b_{e-1}(t_0) (\mathrm{mod}\, q)$.*

Proof. It suffices to consider the case of $2 \leq q < p$. Let $\underline{\beta} = h(x)\underline{b}_0 (\mathrm{mod}\, p)$. Because $\underline{a}, \underline{b} \in G^{'}(f(x), p^e)$ and $h(x)$ is a polynomial coprime with $f(x) (\mathrm{mod}\, p)$ over $\mathbb{Z}/(p)$, we know that both $\underline{\alpha}$ and $\underline{\beta}$ are m-sequences in $G(f(x), p)$.

If $\underline{\alpha}$ and $\underline{\beta}$ are not of 0-uniformity, then there exists an integer t with $0 \leq t < p^n - 1$ such that $\alpha(t) \neq 0$ and $\beta(t) = 0$. It follows from (2.4) that

$$\begin{aligned} &\{a_{e-1}(t + j \cdot p^{e-2}T) \mid j = 0, 1, \ldots, p-1\} = \{0, 1, \ldots, p-1\}; \\ &b_{e-1}(t + j \cdot p^{e-2}T) = b_{e-1}(t), j = 0, 1, \ldots, p-1. \end{aligned}$$

Thus there exists an integer j_0 with $0 \leq j_0 < p$ such that

$$a_{e-1}(t + j_0 \cdot p^{e-2}T) \not\equiv b_{e-1}(t + j_0 \cdot p^{e-2}T) (\mathrm{mod}\, q).$$

If $\underline{\alpha}$ and $\underline{\beta}$ are of 0-uniformity, then there exists a $\lambda \in \mathbb{Z}/(p)\backslash\{0\}$ such that $\underline{\alpha} \equiv \lambda\underline{\beta} (\mathrm{mod}\, p)$ by Lemma 3.3. Since $\underline{a} \neq \underline{b} \in G^{'}(f(x), p^e)$ and $e \geq 2$, we know that $\underline{a}_{e-1}$ and $\underline{b}_{e-1}$ are not of 0-uniformity with $\alpha(t) \neq 0$ by Theorem 3.5. Hence, there exists an integer t such that $\alpha(t) \neq 0$ and $\{a_{e-1}(t), b_{e-1}(t)\} = \{0, \delta \neq 0\}$.

Since $\underline{\alpha} \equiv \lambda\underline{\beta} (\mathrm{mod}\, p)$ and $\alpha(t), \lambda \in \mathbb{Z}/(p)\backslash\{0\}$, we have $\alpha(t) \not\equiv 0 (\mathrm{mod}\, p)$ and $\beta(t) \equiv \lambda^{-1} \cdot \alpha(t) \not\equiv 0 (\mathrm{mod}\, p)$. By (2.5), we can get

$$\begin{aligned} &\{a_{e-1}(t + j \cdot p^{e-2}T) \mid j = 0, 1, \ldots, p-1\} = \{0, 1, \ldots, p-1\}, \\ &\{b_{e-1}(t + j \cdot p^{e-2}T) \mid j = 0, 1, \ldots, p-1\} = \{0, 1, \ldots, p-1\}. \end{aligned}$$

If $a_{e-1}(t) \neq 0$ and $b_{e-1}(t) = 0$, then there exists an integer j_0 such that

$$a_{e-1}(t + j_0 \cdot p^{e-2}T) = 0,$$

but $b_{e-1}(t + j_0 \cdot p^{e-2}T) \neq 0$. Without loss of generality, we suppose $a_{e-1}(t) = 0$ and $b_{e-1}(t) = \delta$.

If $\delta (\mathrm{mod}\, q) \neq 0$, then $a_{e-1}(t) \not\equiv b_{e-1}(t) (\mathrm{mod}\, q)$ and $\alpha(t) \neq 0$. In the following, we suppose $\delta (\mathrm{mod}\, q) = 0$.

By (2.4), we know that

$$\begin{aligned} a_{e-1}(t + j \cdot p^{e-2}T) &\equiv a_{e-1}(t) + j \cdot \alpha(t) \equiv j \cdot \alpha(t) (\mathrm{mod}\, p), \\ b_{e-1}(t + j \cdot p^{e-2}T) &\equiv b_{e-1}(t) + j \cdot \beta(t) \equiv \delta + j \cdot \beta(t) (\mathrm{mod}\, p), \end{aligned}$$

for $j = 0, 1, \ldots, p-1$. By Lemma 4.3, we know that if $1 \leq \lambda < p-1$, then there exists an integer j_0, such that $j_0 \cdot \alpha(t) (\mathrm{mod}\, p) (\mathrm{mod}\, q) \neq \delta + j_0 \cdot \beta(t) (\mathrm{mod}\, p) (\mathrm{mod}\, q)$, implying that $a_{e-1}(t + j_0 \cdot p^{e-2}T) \not\equiv b_{e-1}(t + j_0 \cdot p^{e-2}T) (\mathrm{mod}\, q)$. Since $\alpha(t_0) = \alpha(t) \neq 0$, the integer $t_0 = t + j_0 \cdot p^{e-2}T$ is what we need. Since $\underline{a} \not\equiv -\underline{b} (\mathrm{mod}\, p^e)$, by Lemma 4.4, we know that the statement also holds for $\lambda = p - 1$. □

Lemma 4.6. *Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p)$ with odd prime p. For any prime q different from p, we have $\underline{a} = \underline{b}$ if and only if $\underline{a} \equiv \underline{b} (\mathrm{mod}\, q)$ for $\underline{a}, \underline{b} \in G(f(x), p)$. Furthermore* $\mathrm{per}(\underline{a} \,\mathrm{mod}\, q) = \mathrm{per}(\underline{a})$ *for* $\underline{a} \in G(f(x), p)$.

Proof. It suffices to consider the case of $2 \leq q < p$. Suppose $\underline{a} \equiv \underline{b} (\mathrm{mod}\, q)$ and we are going to prove that $\underline{a} = \underline{b}$. If $\underline{a} \neq \underline{0}$, then there exists an integer t such that $a(t) = 1$ since $\underline{a}$ is an m-sequence in $G(f(x), p)$. Then it follows from $\underline{a} \equiv \underline{b} (\mathrm{mod}\, q)$ that $b(t) \equiv 1 (\mathrm{mod}\, q)$, so $\underline{b} \neq \underline{0}$. The argument shows that $\underline{a} \neq \underline{0}$ if and only if $\underline{b} \neq \underline{0}$. In the following, we suppose that $\underline{a} \neq \underline{0}$ and $\underline{b} \neq \underline{0}$.

If $\underline{a}$ and $\underline{b}$ are linearly independent over $\mathbb{Z}/(p)$, then there exists an integer t such that $a(t) = 0$ and $b(t) = 1$ since $\underline{a}$ and $\underline{b}$ are m-sequences in $G(f(x), p)$. It implies that $a(t) \not\equiv b(t) (\mathrm{mod}\, q)$, a contradiction to $\underline{a} \equiv \underline{b} (\mathrm{mod}\, q)$.

If $\underline{a}$ and $\underline{b}$ are linearly dependent over $\mathbb{Z}/(p)$, then there exists an integer $\lambda \in \{1, 2, \ldots, p-1\}$ such that $\underline{b} \equiv \lambda \cdot \underline{a} (\mathrm{mod}\, p)$. If $\lambda (\mathrm{mod}\, q) \neq 1$, let t be an integer such that $a(t) = 1$. Then $b(t) (\mathrm{mod}\, p) (\mathrm{mod}\, q) = \lambda (\mathrm{mod}\, q)$, so that $a(t) \not\equiv b(t) (\mathrm{mod}\, q)$. If $\lambda (\mathrm{mod}\, q) = 1$ and $1 < \lambda \leq p - 1$, let k be the integer such that $(k-1)\lambda < p < k\lambda$ and t be an integer such that $a(t) = k$. It follows that $b(t) = k\lambda (\mathrm{mod}\, p) = k\lambda - p$, so $a(t) \not\equiv b(t) (\mathrm{mod}\, q)$. Both of the cases are in contradiction with $\underline{a} \equiv \underline{b} (\mathrm{mod}\, q)$. Thus $\lambda = 1$ and $\underline{a} = \underline{b}$.

Thus the sufficient condition is proved, while the necessary condition is straightforward to check.

In the following, we discuss the period of $\underline{a} (\mathrm{mod}\, q)$. If $\underline{a} = \underline{0}$, then it is clear that $\mathrm{per}(\underline{a} \,\mathrm{mod}\, q) = \mathrm{per}(\underline{a})$. For $\underline{a} \in G^{'}(f(x), p)$ and any integer t with $2 \leq t < \mathrm{per}(\underline{a})$, we know $x^t \underline{a} \in G^{'}(f(x), p)$ and $x^t \underline{a} \neq \underline{a}$. Note that we have proved that $\underline{a} = \underline{b}$ if and only if $\underline{a} \equiv \underline{b} (\mathrm{mod}\, q)$ for $\underline{a}, \underline{b} \in G(f(x), p)$, so $x^t \underline{a} (\mathrm{mod}\, q) \neq \underline{a} (\mathrm{mod}\, q)$. Thus $\mathrm{per}(\underline{a} \,\mathrm{mod}\, q) = \mathrm{per}(\underline{a})$. □

Lemma 4.7. *Let p and q be two positive integers such that $p (\mathrm{mod}\, q) \neq 0$ and $p \geq 3$. If $\{u_j \mid j = 0, 1, \ldots, p-1\} = \{v_j \mid j = 0, 1, \ldots, p-1\} = \{0, 1, \ldots, p-1\}$ and $u_0 \not\equiv v_0 (\mathrm{mod}\, q)$, then there exists an integer j with $1 \leq j \leq p-1$ such that $u_j - v_j \not\equiv u_0 - v_0 (\mathrm{mod}\, q)$.*

Proof. First, it is observed that

$$\sum_{j=0}^{p-1} (u_j - v_j) = 0.$$

Suppose $u_j - v_j (\mathrm{mod}\, q) = \delta \neq 0$ for all $j = 0, 1, \ldots, p-1$. Then

$$\sum_{j=0}^{p-1} (u_j - v_j) \equiv p\delta \not\equiv 0 (\mathrm{mod}\, q),$$

a contradiction. The lemma is proved. □

The Proof of Theorem 4.1. It is straightforward to verify the necessary condition. Suppose that $\underline{a} \neq \underline{b}$ and we are going to prove that $\underline{a} \not\equiv \underline{b} (\mathrm{mod}\, q)$. For $e = 1$, the statement follows from Lemma 4.6. In the following, let $e \geq 2$.

Suppose that $\underline{a} = p^u \cdot \underline{a}'$ and $\underline{b} = p^v \cdot \underline{b}'$, where $0 \leq u, v \leq e-1$, $\underline{a}' \not\equiv \underline{0} (\mathrm{mod}\, p)$ and $\underline{b}' \not\equiv \underline{0} (\mathrm{mod}\, p)$. If $u \leq v$, then it is clear that $\underline{a} \equiv \underline{b} (\mathrm{mod}\, q)$ if and only if $\underline{a}' \equiv p^{v-u} \cdot \underline{b}' (\mathrm{mod}\, q)$; otherwise, $\underline{a} \equiv \underline{b} (\mathrm{mod}\, q)$ if and only if $p^{u-v} \cdot \underline{a}' \equiv \underline{b}' (\mathrm{mod}\, q)$. Thus, without loss of generality, let us suppose that $\underline{a} \not\equiv \underline{0} (\mathrm{mod}\, p)$, that is, $\underline{a}$ is a primitive sequence over $\mathbb{Z}/(p^e)$ generated by $f(x)$.

Let $\underline{\alpha} = h(x)\underline{a}_0(\mathrm{mod}\, p)$ and $\underline{\beta} = h(x)\underline{b}_0(\mathrm{mod}\, p)$, where $h(x)$ is defined by (2.2). Since we have supposed that $\underline{a} \not\equiv \underline{0}(\mathrm{mod}\, p)$, sequence $\underline{\alpha}$ is an m-sequence in $G(f(x), p)$. If $\underline{b}_0 \neq \underline{0}$, then $\underline{\beta}$ is also an m-sequence in $G(f(x), p)$; otherwise, $\underline{\beta} = \underline{0}$.

If $\underline{\alpha}$ and $\underline{\beta}$ are not of 0-uniformity, then there exists an integer $t_0 \geq 0$ such that $\alpha(t_0) \neq 0$ and $\beta(t_0) = 0$. It follows from (2.4) that

$$\begin{array}{l} \{a_{e-1}(t + j \cdot p^{e-2}T) \mid j = 0, 1, \ldots, p-1\} = \{0, 1, \ldots, p-1\}; \\ b_{e-1}(t + j \cdot p^{e-2}T) = b_{e-1}(t), j = 0, 1, \ldots, p-1. \end{array} \tag{4.5}$$

On the other hand, for $\underline{a}, \underline{b} \in G(f(x), p^e)$, by Proposition 2, we have $p^{e-2} \cdot T$ is divisible by $\mathrm{per}(\underline{a} \bmod p^{e-1})$ and $\mathrm{per}(\underline{b} \bmod p^{e-1})$, so that

$$\begin{array}{l} a(t + j \cdot p^{e-2}T)(\mathrm{mod}\, p^{e-1}) = a(t)(\mathrm{mod}\, p^{e-1}), j = 0, 1, \ldots, p-1; \\ b(t + j \cdot p^{e-2}T)(\mathrm{mod}\, p^{e-1}) = b(t)(\mathrm{mod}\, p^{e-1}), j = 0, 1, \ldots, p-1. \end{array} \tag{4.6}$$

Combining it with (4.5), we know that there exists an $j_0 \in \{0, 1, \ldots, p-1\}$ such that $a(t + j_0 \cdot p^{e-2}T) \not\equiv b(t + j_0 \cdot p^{e-2}T)(\mathrm{mod}\, q)$, which implies that $\underline{a} \not\equiv \underline{b}(\mathrm{mod}\, q)$.

Suppose $\underline{\alpha}$ and $\underline{\beta}$ are of 0-uniformity. Because $\underline{a}_0 \neq \underline{0}$ and $\underline{b}_0 \neq \underline{0}$, both $\underline{\alpha}$ and $\underline{\beta}$ are m-sequences in $G(f(x), p)$. Then there exists a $\lambda \in \mathbb{Z}/(p)\backslash\{0\}$ such that $\underline{\alpha} \equiv \lambda\underline{\beta}(\mathrm{mod}\, p)$ by Lemma 3.3. Since $\underline{a}, \underline{b} \in G'(f(x), p^e)$ and $e \geq 2$, it follows from Lemma 4.5 that if $\underline{a} \not\equiv \pm\underline{b}(\mathrm{mod}\, p^e)$, then there exists an integer $t \geq 0$ such that $\alpha(t) \neq 0$ and $a_{e-1}(t) \not\equiv b_{e-1}(t)(\mathrm{mod}\, q)$. Since $\underline{\alpha} \equiv \lambda\underline{\beta}(\mathrm{mod}\, p)$, we have $\beta(t) = \lambda^{-1}\alpha(t)(\mathrm{mod}\, p) \neq 0$. By (2.5), we know that

$$\begin{array}{lll} \{a_{e-1}(t + j \cdot p^{e-2}T) & \mid & j = 0, 1, \ldots, p-1\} = \{0, 1, \ldots, p-1\}, \\ \{b_{e-1}(t + j \cdot p^{e-2}T) & \mid & j = 0, 1, \ldots, p-1\} = \{0, 1, \ldots, p-1\}. \end{array}$$

Since $a_{e-1}(t) \not\equiv b_{e-1}(t)(\mathrm{mod}\, q)$ and $p(\mathrm{mod}\, q) \neq 0$, then there exists a positive integer j with $1 \leq j \leq p-1$ such that $a_{e-1}(t + j \cdot p^{e-2}T) - b_{e-1}(t + j \cdot p^{e-2}T) \not\equiv a_{e-1}(t) - b_{e-1}(t)(\mathrm{mod}\, q)$ by Lemma 4.7. Combining it with (4.6), we can deduce that either $a(t) \not\equiv b(t)(\mathrm{mod}\, q)$ or $a(t + j \cdot p^{e-2}T) \not\equiv b(t + j \cdot p^{e-2}T)(\mathrm{mod}\, q)$. Thus $\underline{a} \not\equiv \underline{b}(\mathrm{mod}\, q)$.

If $\underline{a} \equiv -\underline{b}(\mathrm{mod}\, p^e)$, then $\underline{a} + \underline{b} = \underline{0}(\mathrm{mod}\, p^e)$. Let $d = p^e(\mathrm{mod}\, q)$. Since $\gcd(p, q) = 1$, we have $1 \leq d \leq q-1$. It follows from $\underline{a} \not\equiv \underline{0}(\mathrm{mod}\, p)$ that any element in $\{1, 2, \ldots, p-1\}$ appears in the sequence $\underline{a}$, so that any element in $\{0, 1, \ldots, q-1\}$ appears in the sequence $\underline{a}(\mathrm{mod}\, q)$. Then there exists an integer t with $t \geq 0$ such that $a(t)(\mathrm{mod}\, q) = 0$. Since $\underline{a} + \underline{b} = \underline{0}(\mathrm{mod}\, p^e)$, we have $b(t)(\mathrm{mod}\, q) = p^e - a(t)(\mathrm{mod}\, q) = p^e(\mathrm{mod}\, q) = d \neq 0$. Thus $\underline{a} \not\equiv \underline{b}(\mathrm{mod}\, q)$.

In the following, we discuss the period of $\underline{a}(\mathrm{mod}\, q)$. If $\underline{a} = \underline{0}$, then it is clear that $\mathrm{per}(\underline{a} \bmod q) = \mathrm{per}(\underline{a})$. For $\underline{a} \in G(f(x), p^e)\backslash\{\underline{0}\}$ and any integer t with $2 \leq t < \mathrm{per}(\underline{a})$, we know $x^t\underline{a} \in G(f(x), p^e)\backslash\{\underline{0}\}$ and $x^t\underline{a} \neq \underline{a}$. Since $\underline{a} = \underline{b}$ if and only if $\underline{a} \equiv \underline{b}(\mathrm{mod}\, q)$ for $\underline{a}, \underline{b} \in G(f(x), p^e)$, it follows that $x^t\underline{a}(\mathrm{mod}\, q) \neq \underline{a}(\mathrm{mod}\, q)$. Thus $\mathrm{per}(\underline{a} \bmod q) = \mathrm{per}(\underline{a})$. □

Acknowledgement

The authors would like to thank the anonymous referees for their helpful comments and suggestions that considerably improved the presentation of this paper.

References

[1] Z.D. Dai, "Binary sequences derived from ML-sequences over rings I: periods and minimal polynomials," *J. Cryptology*, vol. 5, no. 4, pp. 193-207, 1992. MR1193387 (93g:68030)

[2] Z.D. Dai and M.Q. Huang, "A criterion for primitiveness of polynomial over $\mathbb{Z}/(2^d)$," *Chinese Sci. Bull.*, vol. 36, pp. 892-895, 1991. MR1138295 (93d:11126)

[3] M. Goresky and A. Klapper, "Arithmetic crosscorrelation of feedback with carry shift register sequences," *IEEE Trans. Inform. Theory*, vol. 43, no. 4, pp. 1342-1345, 1997. MR1454969 (98j:94010)

[4] M. Goresky and A. Klapper, "Fourier transforms and the 2-adic span of periodic binary sequences," *IEEE Trans. Inform. Theory*, vol. 46, no. 2, pp. 687-691, 2000. MR1748998 (2001k:94041)

[5] M.Q. Huang and Z.D. Dai, "Projective maps of linear recurring sequences with maximal p-adic periods," *Fibonacci Quart.*, vol. 30, no. 2, pp. 139-143, 1992. MR1162415 (93b:11012)

[6] M.Q. Huang, "Maximal period polynomials over $\mathbb{Z}/(p^d)$," *Sci. in China, Ser. A*, vol. 35, pp. 271-275, 1992. MR1183712 (93e:11148)

[7] M.Q. Huang, "Analysis and cryptologic evaluation of primitive sequences over an integer residue ring," Ph.D. dissertation, Graduate School of USTC, Academia Sinica, Beijing, China, 1988.

[8] A. Klapper and M. Goresky, "Feedback shift registers, 2-adic span, and combiners with memory," *J. Cryptology*, vol. 10, pp. 111-147, 1997. MR1447843 (98f:94012)

[9] V.L. Kurakin, A.S. Kuzmin, A.V. Mikhalev, and A.A. Nechaev, "Linear recurring sequences over rings and modules," *J. Math. Sci.*, vol. 76, no. 6, pp. 2793-2915, 1995. MR1365809 (97a:11201)

[10] A.S. Kuzmin and A.A. Nechaev, "Linear recurring sequences over Galois rings," *Algebra and Logic*, vol. 34, no. 2, pp. 87–100, 1995; translation from *Algebra Logika*, vol. 34, no. 2, pp. 169-189, 1995.

[11] R. Lidl and H. Niederreiter, *Finite fields*, in *Encyclopedia of Mathematics and its Applications.* Cambridge, U.K.: Cambridge Univ. Press, 1983. vol. 20. MR746963 (86c:11106)

[12] B.R. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York, 1974. MR0354768 (50:7245)

[13] A.A. Nechaev, "Linear recurring sequences over commutative rings," *Diskr. Math.*, vol. 3, no. 4, pp. 105–127, 1991. (English translation: *Diskrete Math. and Appl.*, vol. 2, no. 6, pp. 659–683, 1992.)

[14] W.F. Qi, J.H. Yang, and J.J. Zhou, "ML-sequences over rings $\mathbb{Z}/(2^e)$," in *Advances in Cryptology—ASIACRYPT'98 (Lecture Notes in Computer Science).* Berlin/Heidelberg, Germany: Springer-Verlag, 1998, vol. 1514, pp. 315–325.

[15] W.F. Qi, "Compressing maps of primitive sequences over $\mathbb{Z}/(2^e)$ and analysis of their derivative sequences," Ph.D. Dissertation, Zhengzhou Inform. Eng. Univ., Zhengzhou, China, 1997. Higher Education Press, Beijing, December 2001. (In Chinese.)

[16] W.F. Qi and X.Y. Zhu, "Compressing mappings on primitive sequences over $\mathbb{Z}/(2^e)$ and its Galois extension," *Finite Fields Appl.*, vol. 8, no. 4, pp. 570-588, Oct. 2002. MR1933627 (2004f:11015)

[17] W.F. Qi and H. Xu, "Partial period distribution of FCSR sequences," *IEEE Trans. Inform. Theory*, vol. 49, no. 3, pp. 761-765, 2003. MR1967204 (2004c:94079)

[18] C. Seo, S. LEE, Y. Sung, K. Han, and S. Kim, "A lower bound on the linear span of an FCSR," *IEEE Trans. Inform. Theory*, vol. 46, no. 2, pp. 691-693, 2000. MR1748999 (2000m:94017)

[19] M. Ward, "The arithmetical theory of linear recurring series," *Trans. Amer. Math. Soc.*, vol. 35, pp. 600-628, July 1933. MR1501705

[20] X.Y. Zhu and W.F. Qi, "Uniqueness of the distribution of zeroes of primitive level sequences over $\mathbb{Z}/(p^e)$," *Finite Fields Appl.*, vol. 11, no. 1, pp. 30-44, Jan. 2005. MR2111896 (2005i:11023)

[21] X.Y. Zhu and W.F. Qi, "Compression mappings on primitive sequences over $\mathbb{Z}/(p^e)$," *IEEE Trans. Inform. Theory*, vol. 50, no. 10, pp. 2442-2448, Oct. 2004. MR2097062

[22] X.Y. Zhu, "Some results on injective mappings of primitive sequences modulo prime powers," Ph.D. Dissertation, Zhengzhou Inform. Eng. Univ., Zhengzhou, China, December 2004. (In Chinese.)

China National Digital Switching System Engineering and Technological R&D Center (NDSC), P.O. Box 1001-783, Zhengzhou, 450002, People's Republic of China

E-mail address: xuanyong.zhu@263.net or zxy@mail.ndsc.com.cn

Department of Applied Mathematics, Zhengzhou Information Engineering University, P.O. Box 1001-745, Zhengzhou, 450002, People's Republic of China

E-mail address: wenfeng.qi@263.net