Further results on the distinctness of binary sequences derived from primitive sequences modulo square-free odd integers

Qun-Xiong Zheng and Wen-Feng Qi

Abstract

This paper studies the distinctness of primitive sequences over $\mathbf{Z}/(M)$ modulo 2, where M is an odd integer that is composite and square-free, and $\mathbf{Z}/(M)$ is the integer residue ring modulo M. A new sufficient condition is given for ensuring that primitive sequences generated by a primitive polynomial $f(x)$ over $\mathbf{Z}/(M)$ are pairwise distinct modulo 2. Such result improves a recent result obtained in our previous paper [27] and consequently the set of primitive sequences over $\mathbf{Z}/(M)$ that can be proven to be distinct modulo 2 is greatly enlarged.

Index Terms

Stream ciphers, linear recurring sequences, primitive polynomials, primitive sequences, modular reductions.

I. Introduction

Throughout the paper, for an integer $m \geq 2$, let $\mathbf{Z}/(m)$ denote the integer residue ring modulo m. We choose $\{0, 1, \ldots, m-1\}$ as the complete set of representatives for the elements of the ring $\mathbf{Z}/(m)$. Thus a sequence $\underline{a}$ over $\mathbf{Z}/(m)$ is usually seen as an integer sequence over $\{0, 1, \ldots, m-1\}$. Moreover, for an integer a and a positive integer $b \geq 2$, we denote the least nonnegative residue of a modulo b by $[a]_{\bmod b}$, and similarly for a sequence $\underline{a} = (a(t))_{t\geq 0}$ over $\mathbf{Z}/(m)$, denote $[\underline{a}]_{\bmod b} = ([a(t)]_{\bmod b})_{t\geq 0}$.

Let p be a prime number and e a positive integer. During the past two decades, the maximal period linear recurring sequences over $\mathbf{Z}/(p^e)$, called primitive sequences over $\mathbf{Z}/(p^e)$, have been paid much attention. An enormous amount of effort is directed toward the study of finding useful mappings to derive good pseudorandom sequences from primitive sequences over $\mathbf{Z}/(p^e)$, which are called compression mappings in literature, and proving that they are injective. Generally there are two kinds of compression mappings: one is based on e-variable functions over $\mathbf{Z}/(p)$ [1], [9], [10], [15], [16], [18], [19], [21], [30], [31]; the other is based on the modular arithmetic [11], [34]. Besides, the pseudorandom properties of these compression sequences are also extensively studied, such as periodicity [5], [12], [13], linear complexity [2], [4], [14], [17] and distribution properties [7], [8], [20], [24], [25], [32], [33].

Recently research interests on primitive sequences over $\mathbf{Z}/(p^e)$ are further extended to primitive sequences over $\mathbf{Z}/(M)$ [3], [26]-[29], where M is a square-free odd integer. One of important reasons for this is that the period of a primitive sequence $\underline{a}$ of order n over $\mathbf{Z}/(p^e)$ is undesirable if $e \geq 2$. Recall that the period $per(\underline{a})$ of a primitive sequence $\underline{a}$ of order n over $\mathbf{Z}/(p^e)$ is equal to $p^{e-1} \cdot (p^n - 1) \approx p^{e+n-1}$ [23]. It can be seen that for a fixed p^e with $e \geq 2$, the period $per(\underline{a})$ increases slowly and far less than $p^{e\cdot n}$ as n increases. Therefore, to meet the requirement of long period in practical applications (such as $\geq 2^{64}$), n should be chosen large enough, which will be high resource consumption in hardware and software implementation. For example, to generate a sequence with period not less than 2^{64} over $\mathbf{Z}/(2^8)$, $\mathbf{Z}/(2^{16})$ and $\mathbf{Z}/(2^{32})$, the number of bit-registers required must be larger than 456, 784 and 1056, respectively. However for many choices of M, primitive sequences over $\mathbf{Z}/(M)$ have no such periodic weakness. For cryptographic applications, the moduli of the form $2^e - 1$ have attracted much attention since the

This work was supported by NSF of China under Grant No. (61272042, 61100202, 61070178).

Q.-X. Zheng and W.-F. Qi are with the Department of Applied Mathematics, Zhengzhou Information Science and Technology Institute, Zhengzhou 450002, China. (e-mails: qunxiong_zheng@163.com and wenfeng.qi@263.net)

operation "$\bmod 2^e - 1$" can be efficiently implemented both in hardware and software, and this offers new possibilities for advancement in the solution of applying linear recurring sequences over integer residue rings. For instance, primitive sequences over $\mathbf{Z}/(2^{31}-1)$ are used to design the ZUC algorithm, a stream cipher that is the core of the standardized 3GPP confidentiality algorithm 128-EEA3 and the 3GPP integrity algorithm 128-EIA3, see [6].

By applying the operation $\bmod 2$ to primitive sequences over $\mathbf{Z}/(M)$, one can easily obtain a class of binary sequences, called modulo 2 reductions of primitive sequences over $\mathbf{Z}/(M)$. It is thought that the operation $\bmod 2$ destroys the original linear recurrence relation of primitive sequences over $\mathbf{Z}/(M)$ and the obtained binary sequences should have many desirable cryptographic properties if the modulus M and the order n are carefully chosen. As for cryptographic interests, one of the most concerned problems is whether these modulo 2 reductions are pairwise distinct, that is, whether $\underline{a} = \underline{b}$ iff $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$, where $\underline{a}$ and $\underline{b}$ are two primitive sequences generated by a primitive polynomial $f(x)$ over $\mathbf{Z}/(M)$. If the distinctness holds, then there is a one-to-one correspondence between primitive sequences and their modulo 2 reductions, which implies that every modulo 2 reduction preserves all the information of its original primitive sequence. Moreover, the distinctness also guarantees that the period of these modulo 2 reductions attains the maximum possible value.

For a special case where M is an odd prime number, the problem presented above has been completely solved in [34]. However, if M has at least two different prime divisors, there indeed exist many primitive sequences of order 1 over $\mathbf{Z}/(M)$ such that their modulo 2 reductions are the same [3]. It is long unclear whether primitive sequences of order $n \geq 2$ over $\mathbf{Z}/(M)$ are pairwise distinct modulo 2. In [3], for the case $M = pq$, a product of two different odd prime numbers, a sufficient condition was given for (n, p, q) such that primitive sequences generated by a primitive polynomial of degree n over $\mathbf{Z}/(pq)$ are distinct modulo 2. Then in [26] based on a new result on the element distribution property of primitive sequences over $\mathbf{Z}/(pq)$, the set of primitive sequences that can be proved to be distinct modulo 2 is further enlarged. In [28], for a special modulus $M = 2^{32}-1$, a relatively complete result was obtained by taking full use of the arithmetic properties of primitive sequences over $\mathbf{Z}/(2^{32}-1)$. However, for the case of a general modulus M that is odd, composite, and square-free, the distinctness of primitive sequences over $\mathbf{Z}/(M)$ modulo 2 has been quite resistant to proof. Until now only a class of primitive sequences of order $2n'+1$ ($n' \geq 1$) over $\mathbf{Z}/(M)$ are proved to be distinct modulo 2 in [27]. Besides there are several papers [28], [29], [32] study the distinctness of primitive sequences over $\mathbf{Z}/(M)$ modulo H, where $H > 2$ has a prime divisor coprime with M, and in particular in [29] a relatively complete result had been obtained for a general modulus M that is odd, composite and square-free.

In this paper, we further study the modulo 2 distinctness of primitive sequences of order $n \geq 2$ over $\mathbf{Z}/(M)$, where M is an odd integer that is composite and square-free. A new sufficient condition (see Theorem 2) is given for ensuring that primitive sequences generated by a primitive polynomial $f(x)$ over $\mathbf{Z}/(M)$ are pairwise distinct modulo 2. Compared with [27, Theorem 19], it can be seen that the condition that (M, n) is a distinguishable pair (the definition of a distinguishable pair see [27, Definition 3]) is deleted in the new result, and so the generating polynomial can be a primitive polynomial of degree $n \geq 2$, rather than a typical primitive polynomial of degree $2n'+1$ (see [27, Remark 5]). As a result, the set of primitive sequences over $\mathbf{Z}/(M)$ that can be proven to be distinct modulo 2 is greatly enlarged. In particular, two relatively complete results (see Theorem 7 and Theorem 10) are obtained for two special cases: one is that $v_2(p_1^n - 1) = v_2(p_2^n - 1) = \cdots = v_2(p_r^n - 1)$, where $M = p_1 p_2 \cdots p_r$ is the canonical factorization of M and $v_2(m)$ denotes the greatest nonnegative integer k such that 2^k divides m; the other is that the generating polynomial is a typical primitive polynomial over $\mathbf{Z}/(M)$.

The rest of the paper is organized as follows. Section II presents some necessary preliminaries. Section III gives the main results of this paper. Finally, conclusions are drawn in Section IV.

II. Preliminaries

Let m be an integer greater than 1. If a sequence $\underline{a} = (a(t))_{t \geq 0}$ over $\mathbf{Z}/(m)$ satisfies

$$a(i+n) = [c_{n-1}a(i+n-1) + \cdots + c_1 a(i+1) + c_0 a(i)]_{\bmod m}$$

for all integer $i \geq 0$, where n is a positive integer and $c_0, c_1, \ldots, c_{n-1} \in \mathbf{Z}/(m)$ are constant coefficients, then $\underline{a}$ is called a **linear recurring sequence** of order n over $\mathbf{Z}/(m)$ generated by $f(x) = x^n - c_{n-1}x^{n-1} - \cdots - c_0$ (or $\underline{a}$ is a sequence of order n over $\mathbf{Z}/(m)$ in short). For convenience, the set of sequences generated by $f(x)$ over $\mathbf{Z}/(m)$ is generally denoted by $G(f(x), m)$. Particular interests for cryptography are the maximal period linear recurring sequences also called primitive sequences over $\mathbf{Z}/(m)$, which are generated by primitive polynomials over $\mathbf{Z}/(m)$. Next we introduce the definitions of primitive polynomials and primitive sequences over $\mathbf{Z}/(m)$.

Let $f(x)$ be a monic polynomial of degree n over $\mathbf{Z}/(m)$. If $f(0)$ is an invertible element in $\mathbf{Z}/(m)$, then there exists a positive integer T such that $x^T - 1$ is divisible by $f(x)$ in $\mathbf{Z}/(m)[x]$. The minimum of such T is called the period of $f(x)$ over $\mathbf{Z}/(m)$ and denoted by $per(f(x), m)$. For the case that m is a prime power, say $m = p^e$, it is known that $per(f(x), p^e) \leq p^{e-1}(p^n - 1)$, see [23]. If $per(f(x), p^e) = p^{e-1}(p^n - 1)$, then $f(x)$ is called a **primitive polynomial** of degree n over $\mathbf{Z}/(p^e)$. A sequence $\underline{a}$ over $\mathbf{Z}/(p^e)$ is called a **primitive sequence** of order n if $\underline{a}$ is generated by a primitive polynomial of degree n over $\mathbf{Z}/(p^e)$ and $[\underline{a}]_{\bmod p}$ is not an all-zero sequence. A primitive sequence $\underline{a}$ of order n over $\mathbf{Z}/(p^e)$ is (strictly) periodic and the period $per(\underline{a})$ is equal to $p^{e-1}(p^n - 1)$, see [23]. For the case of a general integer m, assume $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ is the canonical factorization of m. A monic polynomial $f(x)$ of degree n over $\mathbf{Z}/(m)$ is called a **primitive polynomial** if for every $i \in \{1, 2, \ldots, r\}$, $f(x) \pmod{p_i^{e_i}}$ is a primitive polynomial of degree n over $\mathbf{Z}/(p_i^{e_i})$. A sequence $\underline{a}$ over $\mathbf{Z}/(m)$ is called a **primitive sequence** of order n if $\underline{a}$ is generated by a primitive polynomial of degree n over $\mathbf{Z}/(m)$ and $[\underline{a}]_{\bmod p_i}$ is not an all-zero sequence for every $i \in \{1, 2, \ldots, r\}$, that is, $[\underline{a}]_{\bmod p_i^{e_i}}$ is a primitive sequence of order n over $\mathbf{Z}/(p_i^{e_i})$. It can be seen that the period of a primitive polynomial of degree n over $\mathbf{Z}/(m)$ and that of a primitive sequence of order n over $\mathbf{Z}/(m)$ are both equal to

$$\operatorname{lcm}\left(p_1^{e_1-1}(p_1^n - 1), p_2^{e_2-1}(p_2^n - 1), \ldots, p_r^{e_r-1}(p_r^n - 1)\right).$$

For convenience, the set of primitive sequences generated by a primitive polynomial $f(x)$ over $\mathbf{Z}/(m)$ is generally denoted by $G'(f(x), m)$.

Finally we introduce a special class of primitive polynomials called typical primitive polynomials, which were first proposed and studied in [22].

Let M be a square-free odd integer with the canonical factorization as $M = p_1 p_2 \cdots p_r$. An element $\xi \in \mathbf{Z}/(M)$ is called a **primitive element** in $\mathbf{Z}/(M)$ if $[\xi]_{\bmod p_i}$ is a primitive element in $\mathbf{Z}/(p_i)$ for every $i \in \{1, 2, \ldots, r\}$, i.e., the multiplicative order of $[\xi]_{\bmod p_i}$ in $\mathbf{Z}/(p_i)$ is equal to $p_i - 1$. It is clear that if ξ is a primitive element in $\mathbf{Z}/(M)$, then for any divisor $R > 1$ of M, $[\xi]_{\bmod R}$ is a primitive element in $\mathbf{Z}/(R)$. Let $f(x)$ be a primitive polynomial of degree n over $\mathbf{Z}/(M)$. In the theory of finite fields, it is easy to see that there is a unique element $\xi_f \in \mathbf{Z}/(M)$ such that $x^\theta \equiv \xi_f \bmod f(x)$ holds over $\mathbf{Z}/(M)$, where $\theta = \operatorname{lcm}\left(\frac{p_1^n - 1}{p_1 - 1}, \frac{p_2^n - 1}{p_2 - 1}, \ldots, \frac{p_r^n - 1}{p_r - 1}\right)$. We say that ξ_f is the **associated element** of $f(x)$ over $\mathbf{Z}/(M)$.

Definition 1: ([22]) A primitive polynomial $f(x)$ of degree n over $\mathbf{Z}/(M)$ is called a **typical primitive polynomial** if ξ_f is a primitive element in $\mathbf{Z}/(M)$, where ξ_f is the associated element of $f(x)$ over $\mathbf{Z}/(M)$.

We note that a primitive polynomial is not always a typical primitive polynomial, see for example [22, Example 6]. In [22], some necessary and sufficient conditions for the existence of typical primitive polynomials of degree n over $\mathbf{Z}/(M)$ were presented. Here we emphasize that the existence of typical primitive polynomials of degree n over $\mathbf{Z}/(M)$ only depends on the arithmetic properties of M and n, see [22, Lemma 7]. If the modulus is not square-free, say $m = p^e m'$ for some prime power p^e with $e \geq 2$ and some integer $m' \geq 1$, indeed one can define a typical primitive polynomial over $\mathbf{Z}/(m)$ analogously. However, unlike the case of $\mathbf{Z}/(M)$, the existence of typical primitive polynomials of degree n over $\mathbf{Z}/(m)$ depends on individual primitive polynomials besides n and m, for more details see [22, Section 4].

III. Main results

Let $m \geq 2$ be an integer and $\underline{a}$ a periodic sequence over $\mathbf{Z}/(m)$ with period $T = per(\underline{a})$. Given an element $s \in \mathbf{Z}/(m)$, we say that the element s occurs in the sequence $\underline{a}$ if there exists an integer

$t \in \{0, 1, \ldots, T-1\}$ such that $a(t) = s$.

Then we can make our main result explicit in the following statement.

Theorem 2: Let M be a positive odd integer that is composite and square-free, and let $f(x)$ be a primitive polynomial of degree $n \geq 2$ over $\mathbf{Z}/(M)$, and let ξ_f be the associated element of $f(x)$ over $\mathbf{Z}/(M)$. If

(1) for any sequence $\underline{z} \in G'(f(x), M)$, every element in $\mathbf{Z}/(M)$ occurs in the sequence $\underline{z}$; and

(2) for any divisor $R > 1$ of M, there is an integer $k_R > 0$ such that $\left[\xi_f^{k_R}\right]_{\bmod R}$ is a positive even number,

then for $\underline{a}, \underline{b} \in G'(f(x), M)$, $\underline{a} = \underline{b}$ iff $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$.

Remark 3: If the conditions of Theorem 2 are satisfied, then for any sequence $\underline{a} \in G'(f(x), M)$, theoretically there is an algorithm to recover $\underline{a}$ from $[\underline{a}]_{\bmod 2}$. Therefore in this sense we say that $[\underline{a}]_{\bmod 2}$ contains all the information of the original primitive sequence $\underline{a}$. Moreover, the period of $[\underline{a}]_{\bmod 2}$ attains the maximum possible value, that is $per([\underline{a}]_{\bmod 2}) = per(\underline{a})$ (the prove is similar with that of [28, Theorem 2-(ii)]).

The rest of this section is divided into two subsections. In Subsection III-A we discuss the validity of the conditions of Theorem 2 by combining theoretical analysis and computer experiment, and then in Subsection III-B we give the proof of Theorem 2.

A. Discussions on the conditions of Theorem 2

First we focus on Condition (1) of Theorem 2. Based on some estimates of exponential sums over integer residue rings, a sufficient condition was given in [27, Theorem 9] such that Condition (1) of Theorem 2 is valid for all primitive polynomials of degree n over $\mathbf{Z}/(M)$.

Lemma 4: ([27, Theorem 9]) Let M, n and $f(x)$ be described as in Theorem 2. Suppose $M = p_1 p_2 \cdots p_r$ is the canonical factorization of M. Then Condition (1) of Theorem 2 is valid if

$$\sum_{k=2}^{r} \sum_{1 \leq i_1 < \cdots < i_k \leq r} \frac{\prod_{j=1}^{k} (p_{i_j} - 1) p_{i_j}^{n/2}}{\operatorname{lcm}\left(p_{i_1}^n - 1, \ldots, p_{i_k}^n - 1\right)} < 1 - \sum_{i=1}^{r} \frac{p_i - 1}{p_i^n - 1}. \tag{1}$$

In theory it was proved that for any given square-free odd integer M, inequality (1) is satisfied if n is sufficiently large, see [27, Theorem 11]. Furthermore, experimental data show that inequality (1) is satisfied for most of M if $n > 6$, see [27, Table 1] for more details.

Next we focus on Condition (2) of Theorem 2. For a given primitive polynomial $f(x)$ of degree n over $\mathbf{Z}/(M)$, one can easily calculate the value of ξ_f, and so the validity of Condition (2) of Theorem 2 can be directly checked. It is clear that the validity of Condition (2) of Theorem 2 depends on individual primitive polynomials. If Condition (2) of Theorem 2 is valid for all primitive polynomials of degree n over $\mathbf{Z}/(M)$, then we say that it is valid for (M, n).

Let $M = p_1 p_2 \cdots p_r$ be the canonical factorization of M and Ω_i the set of all primitive elements in $\mathbf{Z}/(p_i)$ for $i \in \{1, \ldots, r\}$. Since $f(x) \pmod{p_i}$ is also a primitive polynomial over $\mathbf{Z}/(p_i)$, in the theory of finite fields there exists a primitive element $\xi_i \in \Omega_i$ such that

$$x^{\frac{p_i^n - 1}{p_i - 1}} \equiv \xi_i \bmod (f(x), p_i) \text{ for } i \in \{1, \ldots, r\},$$

where the notation "$A \equiv B \bmod (f(x), p)$" means that $A \equiv B \bmod f(x)$ holds over $\mathbf{Z}/(p)$. Denote

$$\theta = \operatorname{lcm}\left(\frac{p_1^n - 1}{p_1 - 1}, \ldots, \frac{p_r^n - 1}{p_r - 1}\right) \text{ and } \tau_i = \frac{[\theta]_{\bmod p_i^n - 1}}{\frac{p_i^n - 1}{p_i - 1}} \text{ for } i \in \{1, \ldots, r\}.$$

Then we have that

$$x^{\theta} \equiv \xi_i^{\tau_i} \bmod (f(x), p_i) \text{ for } i \in \{1, \ldots, r\},$$

and so by the Chinese Remainder Theorem together with the fact that $x^{\theta} \equiv \xi_f \bmod (f(x), M)$, we get that

$$\xi_f \equiv x^{\theta} \equiv \text{Lift}(\xi_1^{\tau_1}, \ldots, \xi_r^{\tau_r}) \bmod (f(x), M),$$

where $\text{Lift}(\xi_1^{\tau_1}, \ldots, \xi_r^{\tau_r})$ denotes the unique integer L between 0 and $M-1$ such that

$$L \equiv \xi_i^{\tau_i} \bmod p_i \text{ for } i \in \{1, \ldots, r\}.$$

Observing that Condition (2) of Theorem 2 is necessarily valid for (M, n) if it is valid for every $\xi_f \in \{\text{Lift}(\xi_1^{\tau_1}, \ldots, \xi_r^{\tau_r}) \mid (\xi_1, \ldots, \xi_r) \in \Omega_1 \times \ldots \times \Omega_r\}$. Therefore, based on this observation, the proportions of (M, n)'s such that Condition (2) of Theorem 2 is valid for (M, n)'s are tested under some ranges of M and n, and the results are listed in Table 1. For example, the proportion is at least 98.348090% for $n = 2$ and all odd integers $M < 50000$ that are composite and square-free. It can be see from Table 1 that Condition (2) of Theorem 2 is in fact highly valid and can be valid for the great majority of (M, n)'s.

Table 1 Proportions of (M,n)'s such that Condition (2) is valid for (M,n)'s

n	$M < 50000$	n	$M < 50000$
2	$\geq 98.348090\%$	11	100%
3	$\geq 99.980177\%$	12	$\geq 95.579490\%$
4	$\geq 96.993525\%$	13	100%
5	100%	14	$\geq 97.938417\%$
6	$\geq 97.634465\%$	15	$\geq 99.940531\%$
7	100%	16	$\geq 96.491344\%$
8	$\geq 96.907625\%$	17	$\geq 99.993392\%$
9	$\geq 99.973569\%$	18	$\geq 97.383375\%$
10	$\geq 96.755650\%$	19	100%

Remark 5: There do exist primitive polynomials $f(x)$ such that Condition (2) of Theorem 2 is invalid. For example, it can be verified that $f(x) = x^2 + x + 80$ is a primitive polynomial over $\mathbf{Z}/(7 \times 13)$ and

$$\xi_f \equiv x^{\text{lcm}\left(\frac{7^2-1}{7-1}, \frac{13^2-1}{13-1}\right)} \equiv 3 \bmod (f(x), 7 \times 13).$$

Then

$$\left(\left[\xi_f^t\right]_{\bmod 7 \times 13}\right)_{t \geq 0} = (1, 3, 9, 27, 81, 61, \ldots)$$

is a sequence over $\mathbf{Z}/(7 \times 13)$ with period 6. It can be seen that Condition (2) of Theorem 2 is invalid for $f(x)$.

Finally we present some further results for the following two cases:

Case 1: $v_2(p_1^n - 1) = v_2(p_2^n - 1) = \cdots = v_2(p_r^n - 1)$, where $M = p_1 p_2 \cdots p_r$ is the canonical factorization of M and $v_2(m)$ denotes the greatest nonnegative integer k such that 2^k divides m;

Case 2: $f(x)$ is a typical primitive polynomial over $\mathbf{Z}/(M)$.

First we deal with Case 1. In this case, we will show that Condition (2) of Theorem 2 is always valid.

Lemma 6: Let M, n, $f(x)$ and ξ_f be described as in Theorem 2. Suppose $M = p_1 p_2 \cdots p_r$ is the canonical factorization of M. Then Condition (2) of Theorem 2 is valid if $v_2(p_1^n - 1) = v_2(p_2^n - 1) = \cdots = v_2(p_r^n - 1)$.

Proof: Set $T = \text{lcm}(p_1^n - 1, \ldots, p_r^n - 1)$ and $\theta = \text{lcm}\left(\frac{p_1^n-1}{p_1-1}, \ldots, \frac{p_r^n-1}{p_r-1}\right)$. To prove the lemma, it suffices to show that

$$\xi_f^{T/2\theta} \equiv M - 1 \bmod M, \tag{2}$$

since (2) implies that the congruence

$$\xi_f^{T/2\theta} \equiv R - 1 \bmod R$$

holds for any divisor $R > 1$ of M, where $R - 1$ is a positive even number.

Since $v_2(p_1^n-1)=v_2(p_2^n-1)=\cdots=v_2(p_r^n-1)$ by assumption, we get that $v_2(T)=v_2(p_i^n-1)$ for $i\in\{1,\ldots,r\}$, and so

$$\frac{T}{2}\equiv\frac{p_i^n-1}{2}\bmod p_i^n-1 \text{ for } i\in\{1,\ldots,r\}. \tag{3}$$

Note that $f(x)\pmod{p_i}$ is a primitive polynomial of degree n over the finite field $\mathbf{Z}/(p_i)$. In the theory of finite fields, it is clear that

$$x^{p_i^n-1}\equiv 1\bmod(f(x),p_i) \text{ and } x^{(p_i^n-1)/2}\equiv -1\bmod(f(x),p_i) \text{ for } i\in\{1,\ldots,r\}. \tag{4}$$

Then (3) and (4) together with the fact that $x^\theta\equiv\xi_f\bmod(f(x),M)$ yield

$$\xi_f^{T/2\theta}\equiv x^{T/2}\equiv x^{(p_i^n-1)/2}\equiv -1\bmod(f(x),p_i) \text{ for } i\in\{1,\ldots,r\},$$

which implies that

$$\xi_f^{T/2\theta}\equiv -1\bmod p_i \text{ for } i\in\{1,\ldots,r\}. \tag{5}$$

Therefore (2) follows from (5). This completes the proof. ■

The following Theorem 7 immediately follows from Theorem 2, Lemma 4 and Lemma 6.

Theorem 7: Let M, n and $f(x)$ be described as in Theorem 2. Suppose $M=p_1p_2\cdots p_r$ is the canonical factorization of M. If

(1) $\sum_{k=2}^{r}\sum_{1\le i_1<\cdots<i_k\le r}\frac{\prod_{j=1}^{k}(p_{i_j}-1)p_{i_j}^{n/2}}{\operatorname{lcm}\left(p_{i_1}^n-1,\ldots,p_{i_k}^n-1\right)}<1-\sum_{i=1}^{r}\frac{p_i-1}{p_i^n-1}$; and

(2) $v_2(p_1^n-1)=v_2(p_2^n-1)=\cdots=v_2(p_r^n-1)$,

then for $\underline{a},\underline{b}\in G'(f(x),M)$, $\underline{a}=\underline{b}$ iff $[\underline{a}]_{\bmod 2}=[\underline{b}]_{\bmod 2}$.

Next we deal with Case 2. In this case ξ_f is a primitive element in $\mathbf{Z}/(M)$, and so for any divisor $R>1$ of M, $\left(\left[\xi_f^t\right]_{\bmod R}\right)_{t\ge 0}$ is a primitive sequence of order 1 generated by $x-\left[\xi_f\right]_{\bmod R}$ over $\mathbf{Z}/(R)$. Then we shall use the following Conjecture 8 on primitive sequences of order 1, which was made in [27, Conjecture 15].

Conjecture 8: (**Even Conjecture**) Let m be a square-free odd integer. For every primitive sequence $\underline{a}$ of order 1 over $\mathbf{Z}/(m)$, there exists an even element occurring in $\underline{a}$.

Remark 9: The correctness of Conjecture 8 has been verified for all square-free odd integers less than $300,000$. Moreover, although Conjecture 8 is not completely proven by now, a asymptotic result was obtained in [27, Theorem 18] which implies that Conjecture 8 is true for almost all square-free odd integers.

Therefore, in the case of Case 2, Theorem 2 can be represented as the following Theorem 10, which is an improvement of [27, Theorem 19] since the strongest condition of [27, Theorem 19], that is (M,n) is a typical primitive pair, is deleted in Theorem 10.

Theorem 10: Let M and n be described as in Theorem 2, and let $f(x)$ be a typical primitive polynomial of degree n over $\mathbf{Z}/(M)$. If

(1) for any sequence $\underline{z}\in G'(f(x),M)$, every element in $\mathbf{Z}/(M)$ occurs in the sequence $\underline{z}$; and

(2) Conjecture 8 is true for $m\in D_M$, where D_M is the set of all divisors of M that are greater than 1,

then for $\underline{a},\underline{b}\in G'(f(x),M)$, $\underline{a}=\underline{b}$ iff $[\underline{a}]_{\bmod 2}=[\underline{b}]_{\bmod 2}$.

In [27, Theorem 14], based on some estimates of exponential sums over integer residue rings, a sufficient condition was given for m such that Conjecture 8 is true for m.

Lemma 11: ([27, Theorem 14]) Given a square-free odd integer m, Conjecture 8 is true for m if

$$\frac{m+1}{4}\ge\sum_{\substack{d\mid m\\ d>1}}\frac{d^{3/2}}{\lambda(d)}\cdot\left(\frac{\ln d}{\pi}+\frac{1}{5}\right),$$

where $\lambda(d)=\operatorname{lcm}(d_1-1,\ldots,d_k-1)$ provided that $d=d_1\cdots d_k$ is the canonical factorization of d.

Note that Conjecture 8 naturally holds for the case where m is a prime number, and so we can immediately get the following Corollary 12 by replacing Condition (1) and (2) of Theorem 10 with the estimate of Lemma 4 and Lemma 11, respectively.

Corollary 12: Let M and n be described as in Theorem 2, and let $f(x)$ be a typical primitive polynomial of degree n over $\mathbf{Z}/(M)$. Suppose $M = p_1 p_2 \cdots p_r$ is the canonical factorization of M. If

(1) $\sum_{k=2}^{r} \sum_{1 \le i_1 < \cdots < i_k \le r} \frac{\prod_{j=1}^{k} (p_{i_j} - 1) p_{i_j}^{n/2}}{\operatorname{lcm}\left(p_{i_1}^n - 1, \ldots, p_{i_k}^n - 1\right)} < 1 - \sum_{i=1}^{r} \frac{p_i - 1}{p_i^n - 1}$; and

(2) $\frac{m+1}{4} \ge \sum_{\substack{d \mid m \\ d > 1}} \frac{d^{3/2}}{\lambda(d)} \cdot \left(\frac{\ln d}{\pi} + \frac{1}{5}\right)$ for every nonprime divisor m of M,

then for $\underline{a}, \underline{b} \in G'(f(x), M)$, $\underline{a} = \underline{b}$ iff $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$.

B. Proof of Theorem 2

This subsection is devoted to the proof of Theorem 2. We first give a necessary lemma.

Lemma 13: Let M, n, $f(x)$ and ξ_f be described as in Theorem 2. If

(1) for any sequence $\underline{z} \in G'(f(x), M)$, every element in $\mathbf{Z}/(M)$ occurs in the sequence $\underline{z}$; and

(2) there exists an integer $k_M > 0$ such that $\left[\xi_f^{k_M}\right]_{\bmod M}$ is a positive even number,

then for $\underline{a}, \underline{b} \in G'(f(x), M)$ with $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$, there is a prime divisor p of M such that $[\underline{a}]_{\bmod p} = [\underline{b}]_{\bmod p}$.

Proof: Suppose, on the contrary, that $[\underline{a}]_{\bmod p} \ne [\underline{b}]_{\bmod p}$ for any prime divisor p of M. Then it is clear that $\underline{c} = [\underline{a} - \underline{b}]_{\bmod M}$ is a primitive sequence generated by $f(x)$ over $\mathbf{Z}/(M)$, i.e. $\underline{c} \in G'(f(x), M)$. By Condition (1) there is an integer $t^* \ge 0$ such that $c(t^*) = 1$, i.e. $[a(t^*) - b(t^*)]_{\bmod M} = 1$. Then $[a(t^*)]_{\bmod 2} = [b(t^*)]_{\bmod 2}$ implies that

$$a(t^*) = 0 \text{ and } b(t^*) = M - 1.$$

Since $x^\theta \equiv \xi_f \bmod f(x)$ holds over $\mathbf{Z}/(M)$ for some positive integer θ and by Condition (2) there is an integer $k_M \ge 0$ such that $C := \left[\xi_f^{k_M}\right]_{\bmod M}$ is a positive even number, we get that

$$x^{\theta \cdot k_M} \equiv \xi_f^{k_M} \equiv C \bmod f(x) \tag{6}$$

holds over $\mathbf{Z}/(M)$. Then by applying (6) to $\underline{a}$ and $\underline{b}$, respectively, we get that

$$a(t^* + \theta \cdot k_M) = [C \cdot 0]_{\bmod M} = 0 \text{ and } b(t^* + \theta \cdot k_M) = [C \cdot (M-1)]_{\bmod M} = M - C,$$

which yield

$$[a(t^* + \theta \cdot k_M)]_{\bmod 2} = 0 \ne 1 = [b(t^* + \theta \cdot k_M)]_{\bmod 2},$$

a contradiction to the assumption that $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$. Therefore, there at least exists a prime divisor p of M such that $[\underline{a}]_{\bmod p} = [\underline{b}]_{\bmod p}$. This completes the proof. ■

Now we start to prove Theorem 2.

Proof: [Proof of Theorem 2] Since the necessary condition is trivial, in the following, we only prove the sufficient condition.

If $\underline{a}, \underline{b} \in G'(f(x), M)$ satisfying $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$, then by Lemma 13 there is a prime divisor p of M such that $[\underline{a}]_{\bmod p} = [\underline{b}]_{\bmod p}$. Denote by R the greatest divisor of M satisfying $[\underline{a}]_{\bmod R} = [\underline{b}]_{\bmod R}$. Then it is clear that R is divisible by p. In the following it suffices to show that $R = M$.

Suppose, on the contrary, that $R < M$.

Let us denote $Q = M/R$. Then we have that $Q > 1$ and $[\underline{a}]_{\bmod q} \ne [\underline{b}]_{\bmod q}$ for any prime divisor q of Q. Since M is square-free, it is clear that $\gcd(R, Q) = 1$. By the Chinese Remainder Theorem, there exist unique sequences $\underline{u}_1$ over $\mathbf{Z}/(R)$ and $\underline{u}_2$ over $\mathbf{Z}/(Q)$ such that

$$\underline{a} = [Q \cdot \underline{u}_1 + R \cdot \underline{v}_1]_{\bmod M}, \tag{7}$$

where $[Q\cdot\underline{u}_1+R\cdot\underline{v}_1]_{\mathrm{mod}\,M}=([Q\cdot u_1(t)+R\cdot v_1(t)]_{\mathrm{mod}\,M})_{t\geq 0}$. Moreover, it can be seen that $\underline{u}_1\in G'(f(x),R)$ and $\underline{v}_1\in G'(f(x),Q)$. Analogously, we have that

$$\underline{b}=[Q\cdot\underline{u}_2+R\cdot\underline{v}_2]_{\mathrm{mod}\,M}, \tag{8}$$

where $\underline{u}_2\in G'(f(x),R)$ and $\underline{v}_2\in G'(f(x),Q)$. Since $[\underline{a}]_{\mathrm{mod}\,R}=[\underline{b}]_{\mathrm{mod}\,R}$, it follows that $\underline{u}_1=\underline{u}_2$, and so

$$[\underline{a}-\underline{b}]_{\mathrm{mod}\,M}=[R\cdot(\underline{v}_1-\underline{v}_2)]_{\mathrm{mod}\,M}=R\cdot[\underline{v}_1-\underline{v}_2]_{\mathrm{mod}\,Q}.$$

Furthermore, for any prime divisor q of Q, since $[\underline{a}]_{\mathrm{mod}\,q}\neq[\underline{b}]_{\mathrm{mod}\,q}$, we have that $[\underline{v}_1]_{\mathrm{mod}\,q}\neq[\underline{v}_2]_{\mathrm{mod}\,q}$, and so $[\underline{v}_1-\underline{v}_2]_{\mathrm{mod}\,Q}\in G'(f(x),Q)$. Set

$$\underline{z}=[Q\cdot\underline{u}_1+R\cdot(\underline{v}_1-\underline{v}_2)]_{\mathrm{mod}\,M}.$$

Then it can be seen that $\underline{z}\in G'(f(x),M)$. Hence Condition (1) implies that $(u_1(t),[v_1(t)-v_2(t)]_{\mathrm{mod}\,Q})$ runs through the set $\mathbf{Z}/(R)\times\mathbf{Z}/(Q)$ as t runs from 0 to $per(\underline{z})-1$.

Choose an integer $t^*\geq 0$ such that $u_1(t^*)=u_2(t^*)=0$ and

$$[v_1(t^*)-v_2(t^*)]_{\mathrm{mod}\,Q}=1. \tag{9}$$

Then (7) and (8) yield

$$a(t^*)=R\cdot v_1(t^*)\ \text{ and }\ b(t^*)=R\cdot v_2(t^*).$$

Since $[a(t^*)]_{\mathrm{mod}\,2}=[b(t^*)]_{\mathrm{mod}\,2}$ and $[R]_{\mathrm{mod}\,2}=1$, we obtain that

$$[v_1(t^*)]_{\mathrm{mod}\,2}=[v_2(t^*)]_{\mathrm{mod}\,2}. \tag{10}$$

Combining (9) and (10) we can deduce that

$$v_1(t^*)=0\text{ and }v_2(t^*)=Q-1,$$

and so

$$a(t^*)=0\text{ and }b(t^*)=M-R.$$

Since $x^\theta\equiv\xi_f\bmod f(x)$ holds over $\mathbf{Z}/(M)$ for some positive integer θ, we have that

$$x^{\theta\cdot k}\equiv\xi_f^k\bmod f(x) \tag{11}$$

holds over $\mathbf{Z}/(M)$ for any integer $k\geq 0$. Applying (11) to $\underline{a}$ and $\underline{b}$, respectively, we get that

$$a(t^*+\theta\cdot k)=\left[a(t^*)\cdot\xi_f^k\right]_{\mathrm{mod}\,M}=0$$

and

$$b(t^*+\theta\cdot k)=\left[b(t^*)\cdot\xi_f^k\right]_{\mathrm{mod}\,M}=M-R\cdot\left[\xi_f^k\right]_{\mathrm{mod}\,Q}.$$

By the assumption of Condition (2) there exists an integer $k_R\geq 0$ such that $\left[\xi_f^{k_R}\right]_{\mathrm{mod}\,Q}$ is a positive even number, we get that

$$[a(t^*+\theta\cdot k_R)]_{\mathrm{mod}\,2}=0\neq 1=[b(t^*+\theta\cdot k_R)]_{\mathrm{mod}\,2},$$

a contradiction to the assumption that $[\underline{a}]_{\mathrm{mod}\,2}=[\underline{b}]_{\mathrm{mod}\,2}$.

Therefore, we have that $R=M$. This completes the proof. ■

IV. Conclusions

Let M be an odd integer that is composite and square-free and $\mathbf{Z}/(M)$ the integer residue ring modulo M. One of the most attractive problems for primitive sequences of order n over $\mathbf{Z}/(M)$ is whether their modulo 2 reductions are pairwise distinct, that is $\underline{a} = \underline{b}$ iff $[\underline{a}]_{\mathrm{mod}\,2} = [\underline{b}]_{\mathrm{mod}\,2}$, where $\underline{a}$ and $\underline{b}$ are two primitive sequences generated by a primitive polynomial of degree n over $\mathbf{Z}/(M)$. It is known that the problem is not true if $n = 1$. For example, $\underline{a} = (5, 4, 20, 16, 17, 1, 5, \ldots)$ and $\underline{b} = (13, 2, 10, 8, 19, 11, 13, \ldots)$ are two primitive sequences of order 1 generated by $x - 5$ over $\mathbf{Z}/(21)$. It can be seen that $[\underline{a}]_{\mathrm{mod}\,2} = [\underline{b}]_{\mathrm{mod}\,2}$ whereas $\underline{a} \neq \underline{b}$. However, until now no counterexample is found for $n \geq 2$. Based on extensive experiments and the results obtained in this paper, it is further believed that the problem should be true for $n \geq 2$. A complete solution to this problem will be one of the subjects of our future work and it may rely on more investigations on the distribution properties of primitive sequences over $\mathbf{Z}/(M)$, as well as more profound results in number theory.

References

[1] D. N. Bylkov and A. A. Nechaev, "An algorithm to restore a linear recurring sequence over the ring $R = \mathbf{Z}_{p^n}$ from a linear complication of its highest coordinate sequence," *Discr. Math. Appl.*, vol. 20, no. 5-6, pp. 591-609, 2010.

[2] A. H. Chan and R. Games, "On the linear span of binary sequences from finite geometries," in *Advances in Cryptology — Crypto'86*, Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 1987, vol. 263, pp. 405-417.

[3] H. J. Chen and W. F. Qi, "On the distinctness of maximal length sequences over $\mathbf{Z}/(pq)$ modulo 2," *Finite Fields Appl.*, vol. 15, pp. 23-39, 2009.

[4] Z. D. Dai, T. Beth and D. Gollman, "Lower bounds for the linear complexity of sequences over residue ring," in *Advances in Cryptology — EUROCRYPT'90*, Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 1991, vol. 473, pp. 189-195.

[5] Z. D. Dai, "Binary sequences derived from ML-sequences over rings I: periods and minimal polynomials," *J. Crypt.*, vol. 5, pp. 193-207, 1992.

[6] ETSI/SAGE Specification, "Specification of the 3GPP confidentiality and integrity algorithms 128-EEA3 & 128-EIA3. Document 4: Design and evaluation report; version: 2.0; data: 9th Sep. 2011," Tech. rep., 2011.

[7] S. Q. Fan and W. B. Han, "Random properties of the highest level sequences of primitive sequences over $\mathbf{Z}/(2^e)$," *IEEE Trans. Inf. Theory,* vol. 49, no. 6, pp. 1553–1557, 2003.

[8] H. G. Hu, D. G. Feng and W. L. Wu, "Incomplete exponential sums over galois rings with applications to some binary sequences derived from $\mathbf{Z}/(2^l)$," *IEEE Trans. Inf. Theory,* vol. 52, no. 5, pp. 2260–2265, 2006.

[9] 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. (in Chinese)

[10] M. Q. Huang and Z. D. Dai, "Projective maps of linear recurring sequences with maximal p-adic periods," *Fibonacci Quart.,* vol. 30, pp. 139-143, 1992.

[11] A. Klapper and M. Goresky, "2-Adic shift registers," in *Fast Software Encryption,* Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 1993, vol. 809, pp. 174-178.

[12] A. Klapper and M. Goresky, "Large period nearly deBruijn FCSR sequences (extended abstract)," in: *Advances in Cryptology — EUROCRYPT'95*, Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 1995, vol. 921, pp. 263-273.

[13] A. Klapper and M. Goresky, "Feedback shift registers, 2-adic span, and combiners with memory," *J. Crypt.,* vol. 10, no. 2, pp. 111-147, 1997.

[14] V. L. Kurakin, "The first coordinate sequence of a linear recurrence of maximal period over a Galois ring," *Discr. Math. Appl.,* vol. 4, no. 2, pp. 129–141, 1994.

[15] A. S. Kuzmin and A. A. Nechaev, "Linear recurring sequences over Galois ring," *Russian Math. Surv.*, vol. 48, pp. 171-172, 1993.

[16] A. S. Kuzmin, G. B. Marshalko and A. A. Nechaev, "Reconstruction of a linear recurrence over a primary residue ring," *Memoires in Discr. Math.*, vol. 12, pp. 155-194, 2009. (in Russian)

[17] A. S. Kuzmin, "Lower estimates for the ranks of coordinate sequences of linear recurrent sequences over primary residue rings of integers," *Russian Math. Surv.*, vol. 48, pp. 203-204, 1993.

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

[19] W. F. Qi and X. Y. Zhu, "Compressing mappings on primitive sequences over $\mathbf{Z}/(2^e)$ and its Galois extension," *Finite Fields Appl.*, vol. 8, pp. 570-588, 2002.

[20] P. Sole and D. Zinoviev, "The most significant bit of maximum length sequences over $\mathbf{Z}/(2^l)$: autocorrelation and imbalance," *IEEE Trans. Inf. Theory,* vol. 50, no. 8, pp. 1844–1846, 2004.

[21] T. Tian and W. F. Qi, "Injectivity of compressing maps on primitive sequences over $\mathbf{Z}/(p^e)$," *IEEE Trans. Inf. Theory*, vol. 53, pp. 2966-2970, 2007.

[22] T. Tian and W. F. Qi, "Typical primitive polynomials over integer residue rings," *Finite Fields Appl.*, vol. 15, pp. 796-807, 2009.

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

[24] H. Xu and W. F. Qi, "Partial period distribution of FCSR sequences," *IEEE Trans. Inf. Theory,* vol. 49, no. 3, pp. 761-765, 2003.

[25] Q. X. Zheng and W. F. Qi, "Distribution properties of compressing sequences derived from primitive sequences over $\mathbf{Z}/(p^e)$," *IEEE Trans. Inf. Theory*, vol. 56, pp. 555-563, 2010.

[26] Q. X. Zheng and W. F. Qi, "A new result on the distinctness of primitive sequences over $\mathbf{Z}/(pq)$ modulo 2," *Finite Fields Appl.*, vol. 17, pp. 254-274, 2011.

[27] Q. X. Zheng, W. F. Qi and T. Tian, "On the distinctness of binary sequences derived from primitive sequences modulo square-free odd integers," *IEEE Trans. Inf. Theory*, to be published. Available at: http://dx.doi.org/10.1109/TIT.2012.2212694.

[28] Q. X. Zheng, W. F. Qi and T. Tian, "On the distinctness of modular reductions of primitive sequences over $\mathbf{Z}/\left(2^{32}-1\right)$," *Des. Codes Cryptogr.,* to be published. Available at: http://dx.doi.org/10.1007/s10623-012-9698-y.

[29] Q. X. Zheng, W. F. Qi and T. Tian, "On the distinctness of modular reductions of primitive sequences modulo square-free odd integers," *Inf. Proc. Lett.,* vol. 112, no. 22, pp. 872-875, 2012.

[30] X. Y. Zhu and W. F. Qi, "Compression mappings on primitive sequences over $\mathbf{Z}/(p^e)$," *IEEE Trans. Inf. Theory*, vol. 50, pp. 2442-2448, 2004.

[31] X. Y. Zhu and W. F. Qi, "Further result of compressing maps on primitive sequences modulo odd prime powers," *IEEE Trans. Inf. Theory*, vol. 53, pp. 2985-2990, 2007.

[32] X. Y. Zhu and W. F. Qi, "Uniqueness of the distribution of zeroes of primitive level sequences over $\mathbf{Z}/(p^e)$," *Finite Fields Appl.*, vol. 11, pp. 30-44, 2005.

[33] X. Y. Zhu and W. F. Qi, "Uniqueness of the distribution of zeroes of primitive level sequences over $\mathbf{Z}/(p^e)$ (II)," *Finite Fields Appl.*, vol. 13, pp. 230-248, 2007.

[34] X. Y. Zhu and W. F. Qi, "On the distinctness of modular reductions of maximal length sequences modulo odd prime powers," *Math. Comp.*, vol. 77, pp. 1623-1637, 2008.