Title	Random Number Generation and Dynamical System : Statistical Properties of Binary Sequences Generated by One-dimensional Maps (5th Workshop on Stochastic Numerics)
Author(s)	Oohama, Yasutada; Kohda, Tohru
Citation	数理解析研究所講究録 (2001), 1240: 204-215
Issue Date	2001-12
URL	http://hdl.handle.net/2433/41617
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録 1240 巻 2001 年 204-215

Random Number Generation and Dynamical System
-Statistical Properties of Binary Sequences Generated by One-dimensional Maps-

Yasutada Oohama and Tohru Kohda
(大濱靖匡, 香田 徹)
Faculty of Information Science and Electrical Engineering, Kyushu University
(九州大学大学院システム情報科学研究院)
E-mail: {oohama,kohda}@csce.kyushu-u.ac.jp

Abstract- There are several attempts to generate chaotic binary sequences by using one-dimensional maps. From the standpoint of engineering applications, it is necessary to evaluate statistical properties of sample sequences of finite length. In this paper we attempt to evaluate the statistics of chaotic binary sequences of finite length. The large deviation theory for dynamical systems is useful for investigating this problem.

1 Introduction

Let A be a closed interval and $\tau : A \to A$ be a nonlinear map. A real valued sequence $\{x_t\}_{t=0,1,2,\cdots}$ generated by the difference equation

$$x_{t+1} = \tau(x_t) \tag{1}$$

is perhaps the simplest object which can display *chaos*. There are several attempts to generate digital sequences by using such a *chaotic* real valued sequence and apply it to several digital communication systems [1],[2].

The ensemble average technique enables us to know statistical properties of such digital sequences of infinite length when the system is ergodic [3],[4]. On the other hand, from the standpoint of engineering applications, it is necessary to evaluate statistical properties of sample sequences of finite length.

In this paper we attempt to evaluate the deviation from the statistics of chaotic sequences originated from the finiteness of their length. The large deviation theory for dynamical systems [5]-[7] plays an important role in discussing such problems.

2 Chaotic Binary Sequences Generated by One-Dimensional Maps

In this section we shall explain the one-dimensional map dealt with in this paper and the method of generating binary sequences using the above one-dimensional maps. Furthermore, we shall present a framework of evaluating statistical properties of the obtained binary sequences of finite lengths.

We first present several notations used throughout this paper. Let $\mathcal{B} = \{0, 1\}$, and let $\mathcal{B}^n$ denote the set of all binary strings which have length n and $\mathcal{B}^*$ denote the set of all finite binary strings. We denote by b_m^n the string $b_m b_{m+1} \cdots b_n$. For $m > n$, the string b_m^n is empty, denoted by λ.

It is well known that tent maps, logistic maps and Chebyshev maps are examples of one dimensional maps whose properties are extensively studied. In this paper, we deal with a case when $A = [0, 1]$, and τ is a dyadic map defined by

$$\tau(x) = \begin{cases} 2x & \text{for } 0 \le x < 1/2 \\ 2x - 1 & \text{for } 1/2 \le x \le 1 \end{cases} \tag{2}$$

Although the above case is an example of one-dimensional maps displaying chaos, the arguments we shall develop here will be extended to a more general case that the map τ is an r-ardic map. Moreover, by using some conformal transformation, an extension to the case of Chebyshev maps is also possible. Using the following threshold function

$$\sigma_c(x) = \begin{cases} 1 & \text{for } 0 \le x < c \\ 0 & \text{for } c \le x \le 1 \end{cases}, \tag{3}$$

we obtain the binary sequence $\{\sigma_c(\tau^n(x))\}_{n=0}^{\infty}$ from the real-valued sequence $\{\tau^n(x)\}_{n=0}^{\infty}$. It is well known that if $c = 1/2$, $\left\{\sigma_{1/2}(\tau^n(x))\right\}_{n=0}^{\infty}$ gives a dyadic expansion of the real number x. It is also well known that $\left\{\sigma_{1/2}(\tau^n(x))\right\}_{n=0}^{\infty}$ can be regarded as a random process equivalent to a realization of fair coin tosses.

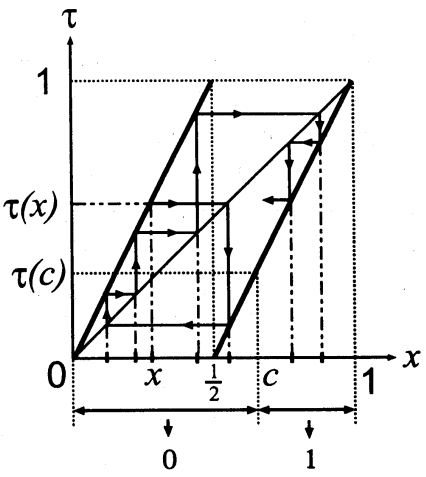

Fig. 1: Generation of binary sequences using the dyadic map and the threshold function

From a theoretical as well as practical engineering point of view, we are interested in the statistical properties of the above binary sequence for general value of c. In this paper we shall demonstrate that the binary sequences $\{\sigma_c(\tau^n(x))\}_{n=0}^{\infty}$ can be considered as a functional process on some transformation of the random process of fair coin tosses.

To examine statistical properties of the above binary sequence we consider the relative frequency of the letter 1 appearing in the sequence $\sigma_c(x)$, $\sigma_c(\tau(x)), \cdots, \sigma_c(\tau^n(\ x))$, i.e.

$$S_n^{(c)}(x) = \frac{1}{n}\sum_{k=0}^{n-1} \sigma_c(\tau^k(x)) \,. \tag{4}$$

By Birkhoff's individual ergodic theorem we have

$$\lim_{n\to\infty} S_n^{(c)}(x) = \int_A \sigma_c(s)\mu(s)ds = 1 - c \quad \text{a.e. } x \,, \tag{5}$$

where μ is an invariant measure calculated from τ. When τ is the dyadic map, μ is the uniform distribution on $[0, 1]$. The above equality means that the measure of the set of the initial value for which $S_n^{(c)}(x)$ does not converge to c as $n \to \infty$ is zero. Our purpose is to examine the asymptotic behavior of such measure for large n. To this end, let B be an arbitrary subset of $[0, 1]$ and set

$$D_n^{(c)}(B) = \left\{x : x \in A, S_n^{(c)}(x) \in B\right\}.$$

We say that the sequence of the probability measure $\left\{\mu\left(D_n(B)\right)\right\}_{n=1}^{\infty}$ on A has the *large deviation property with a rate function* $I^{(c)}(y)$, if

$$\limsup_{n\to\infty} \frac{1}{n} \log \mu\left(D_n^{(c)}(B)\right) \le -\inf_{y\in B} I^{(c)}(y) \text{ for closed } B,$$

$$\liminf_{n\to\infty} \frac{1}{n} \log \mu\left(D_n^{(c)}(B)\right) \ge -\inf_{y\in B} I^{(c)}(y) \text{ for open } B.$$

Roughly speaking, this means

$$\mu\left(D_n^{(c)}(B)\right) \approx \exp\left[-nI^{(c)}(B)\right] , \tag{6}$$

where $I^{(c)}(B) = \inf_{y \in B} I^{(c)}(y)$. It can be seen from (5) that the sequence $\{\sigma_c(\tau^n(x))\}_{n=0}^{\infty}$ is the pseudo-random sequence approximating the binomial distribution $p_c = (c, 1-c)$. The function $I^{(c)}(y)$ indicates how well the random number sequence approximates the distribution p_c for the finite period n, and therefore, is considered as one of the criterion to evaluate the quality of random numbers. It is important to know $I^{(c)}(y)$ in a closed form. When $c = 1/2$, the binary sequence can be regarded as stochastically equivalent to a random process of fair coin tossing. In this case, $S_n^{(1/2)}(\cdot)$ is considered as a sample mean of the random sequence from this stochastic process. Then, it follows from Cramér's theorem in the large deviation theory that we obtain

$$I^{(c)}(y) = \log 2 - h(y), \tag{7}$$

where $h(y) = -y \log y - (1-y)\log(1-y)$. In this paper we try to derive an explicit form of $I^{(c)}(y)$ for some rational numbers c.

3 Functional Process on Prefix Transformations

In this subsection we examine the structure of the generation of the binary sequence $\{\sigma_c(\tau^n(x))\}_{n=0}^{\infty}$ for some rational number c. We show that the generation of the above binary sequences can be considered as a functional process on some transformation of the random process of fair coin tosses.

We consider the case that the threshold value c is a rational number having a finite dyadic expression given by

$$c = 0.a_1 a_2 \cdots a_l, \tag{8}$$

where $a_i \in \mathcal{B}, i = 1, 2, \cdots, l$ and $a_l = 1$. Let $l = l(c)$ denote the length of the dyadic expression of c. Based on the above binary expression of c, set

$$\left.\begin{array}{ll} s_1 = \bar{a}_1, & u_1 = a_1, \\ s_2 = a_1\bar{a}_2, & u_2 = a_1 a_2, \\ \quad\vdots & \quad\vdots \\ s_j = a_1 a_2 \cdots a_{j-1}\bar{a}_j, & u_j = a_1 a_2 \cdots a_j, \\ \quad\vdots & \quad\vdots \\ s_l = a_1 a_2 \cdots a_{l-1}\bar{a}_l, & u_l = a_1 a_2 \cdots a_l, \end{array}\right\} \tag{9}$$

and define the subset of $\mathcal{B}^*$ by $\mathcal{S} = \{s_1, s_2, \cdots, s_l, u_l\}$. The set $\mathcal{S}$ of $\mathcal{B}^*$ satisfies the following property.

1. No string in $\mathcal{S}$ is a prefix of any other string in $\mathcal{S}$.
2. Each string in $\mathcal{B}^*$ has a prefix that belongs to $\mathcal{S}$.

In general we call $\mathcal{S} \subset \mathcal{B}^*$ a *prefix set* if it satisfies the above two conditions. Set $\mathcal{U} = \{u_1, u_2, \cdots, u_{l-1}\}$. The prefix set $\mathcal{S}$ makes it possible to define the function which maps strings in $\mathcal{B}^* - \mathcal{U}$ onto their unique prefix $s \in \mathcal{S}$. We denote this map by $\beta^{(c)} : \mathcal{B}^* - \mathcal{U} \to \mathcal{S}$ and call it a *prefix function*. Furthermore, define $\varphi : \mathcal{S} \to \{0, 1\}$ by $\varphi(b_1^m) = 0$ if $b_m = 0$, $\varphi(b_1^m) = 1$, if $b_m = 1$.

For example, we consider the case $c = 5/8$. In this case the dyadic resentation of c is $c = 0.101$. In this case we have

$$\left.\begin{array}{ll} s_1 = 0, & u_1 = 1, \\ s_2 = 11, & u_2 = 10, \\ s_3 = 100, & u_3 = 101 \end{array}\right\} \tag{10}$$

and $\mathcal{S} = \{0, 11, 100, 101\}$. The prefix set $\mathcal{S}$ and the function φ on the set $\mathcal{S}$ can be described with a binary tree as shown in Fig. 2. The following theorem states that the binary sequence generated by (σ_c, τ) is characterized with $(\beta^{(c)}, \sigma_{1/2}, \tau)$.

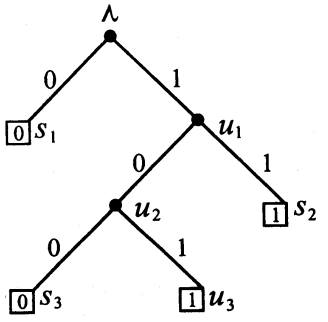

Fig. 2: An example of binary tree describing $\mathcal{S}$ and φ on $\mathcal{S}$

Theorem 1 *Suppose that the threshold value c has a dyadic expression with finite length $l = l(c)$. Then, for any $n \geq l - 1$ and any $x \in A$, we have*

$$\sigma_c(\tau^n(x)) = \varphi\left(\beta^{(c)}\left(\prod_{j=0}^{l-1} \sigma_{1/2}(\tau^{n+j-l+1}(x))\right)\right). \tag{11}$$

Proof: To prove (11), it suffices to show that for any $x \in A$,

$$\sigma_c(\tau^{l-1}(x)) = \varphi\left(\beta^{(c)}\left(\prod_{j=0}^{l-1} \sigma_{1/2}(\tau^{j}(x))\right)\right). \tag{12}$$

The above equality is merely a consequence of a simple computation. We omit the detail. □

Next, we investigate an explicit characterization of the rate function $I^{(c)}(y)$. To this end we define

$$\Omega_n^{(c)}(\theta) = \int_A \exp\left\{\theta \sum_{k=0}^{n-1} \sigma_c(\tau^k(x))\right\} \mu(x)\mathrm{d}x\,, q^{(c)}(\theta) = \lim_{n\to\infty} \frac{1}{n} \log \Omega_n^{(c)}(\theta)\,. \tag{13}$$

According to Gärtner-Ellis [8], under some regularly conditions for $q^{(c)}(\theta)$ we have

$$I^{(c)}(y) = \sup_{\theta} \left\{\theta y - q^{(c)}(\theta)\right\}. \tag{14}$$

Hence, the determination problem of $I^{(c)}(y)$ results in the problem of calculating $\Omega_n(\theta)$ and $q^{(c)}(\theta)$.

By the definition of $\Omega_n^{(c)}(\theta)$ and Theorem 1, we obtain the following another form of $\Omega_n^{(c)}(\theta)$.

Theorem 2 *Suppose that the threshold value c is a rational number having a dyadic expression of finite length $l = l(c)$. Then, for any $n \geq l$, we have*

$$\Omega_n^{(c)}(\theta) = \frac{1}{2^n} \sum_{b_1^n \in \mathcal{B}^n} \exp\left[\theta \sum_{j=1}^{n-l+1} \varphi(\beta^{(c)}(b_j^n))\right]. \tag{15}$$

The above form is useful for computing $\Omega_n^{(c)}(\theta)$. Set

$$M_n^{(c)}(\theta) = \sum_{b_1^n \in \mathcal{B}^n} \exp\left[\theta \sum_{j=1}^{n-l+1} \varphi(\beta^{(c)}(b_j^n))\right], \quad \rho^{(c)}(\theta) = \lim_{n\to\infty} \frac{1}{n} \log M_n^{(c)}(\theta)\,. \tag{16}$$

It is obvious that $q^{(c)}(\theta) = (1/2)\rho^{(c)}(\theta)$. Thus, it suffices to examine the properties of $M_n^{(c)}(\theta)$ for the computation of the rate function.

4 Rate Function for Threshold Values with Finite Dyadic Expression

In this section we deal with the problem of computing the rate functions for threshold values c of some rational numbers. From arguments of the previous section it suffices to discuss the calculation of $M_n^{(c)}(\theta)$ for the computation of the rate function.

4.1 Threshold Values with General Finite Dyadic Expression

We first deal with the case that the rational number c has a general dyadic expression with finite length. Suppose that c has the finite dyadic expression given by (8) in the previous section. Throughout this subsection we assume that the threshold value c is given by (8). Furthermore, the definition of s_i, u_i $i = 1, 2, \cdots, l$ and $\mathcal{S}$ and $\mathcal{U}$ are the same as those in the previous section.

For $b_1^m \in \mathcal{B}^*$, define $M_{n,b_1^m}^{(c)}(\theta)$ by

$$M_{n,b_1^m}^{(c)}(\theta) = \sum_{b_{m+1}^n \in \mathcal{B}^{n-m}} \exp\left[\theta \sum_{j=1}^{n-l+1} \varphi(\beta^{(c)}(b_j^n))\right]. \tag{17}$$

In particular if b_1^m is the null string λ, $M_{n,b_1^m}^{(c)}(\theta)$ is regarded as $M_n^{(c)}(\theta)$. The quantity defined as above have the following properties.

Property 1 *For any prefix set $\tilde{\mathcal{S}} \subset \mathcal{B}^*$, we have*

$$M_n^{(c)}(\theta) = \sum_{s \in \tilde{\mathcal{S}}} M_{n,s}^{(c)}(\theta). \tag{18}$$

Property 2

a)

$$M_{n,s_1}^{(c)}(\theta) = e^{\theta \bar{a}_1} M_{n-1}^{(c)}(\theta) \tag{19}$$

$$M_{n,s_j}^{(c)}(\theta) = e^{\theta \bar{a}_j} M_{n-1,a_2^{j-1}\bar{a}_j}^{(c)}(\theta) \text{ for } j = 2, \cdots, l \tag{20}$$

$$M_{n,u_l}^{(c)}(\theta) = e^{\theta} M_{n-1,a_2^l}^{(c)}(\theta) \tag{21}$$

b) *For any $b_1^m \in \mathcal{B}^*$, there exists the minimum integer i, $0 \le i \le m$ such that $b_{i+1}^m = u_{m-i}$. When $i = m$, u_{m-i} is regarded as the null string λ. Then, we have the following:*

$$M_{n,b_1^m}^{(c)}(\theta) = \exp\left[\theta \sum_{j=1}^{i} \varphi(\beta^{(c)}(b_j^m))\right] M_{n-i,u_{m-i}}^{(c)}(\theta). \tag{22}$$

The following two lemmas provide useful formulas for deriving recursive equations with respect to $M_n^{(c)}(\theta)$.

Lemma 1

$$M_n^{(c)}(\theta) = (e^{\theta} + e^{\theta \bar{a}_1}) M_{n-1}^{(c)}(\theta) - (e^{\theta} - 1) \sum_{j=2}^{l} a_j M_{n-1,a_2^{j-1}\bar{a}_j}^{(c)}(\theta). \tag{23}$$

Proof: By Properties 1 and 2-a), we have

$$M_n^{(c)}(\theta) = \sum_{j=1}^{l} M_{n,s_j}^{(c)}(\theta) + M_{n,u_l}^{(c)}(\theta)$$
$$= e^{\theta\bar{a}_1} M_{n-1}^{(c)}(\theta) + \sum_{j=2}^{l} e^{\theta\bar{a}_j} M_{n-1,a_2^{j-1}\bar{a}_j}^{(c)}(\theta) + e^{\theta} M_{n-1,a_2^l}^{(c)}(\theta)\,. \tag{24}$$

We note here the following identity:

$$e^{\theta\bar{a}_j} = 1 + e^{\theta} - e^{a_j} = e^{\theta} - (e^{\theta} - 1)a_j\,. \tag{25}$$

Substituting (25) into the second term in the right member of (24), we have

$$M_n^{(c)}(\theta) = e^{\theta\bar{a}_1} M_{n-1}^{(c)}(\theta) + e^{\theta}\left[\sum_{j=2}^{l} M_{n-1,a_2^{j-1}\bar{a}_j}^{(c)}(\theta) + M_{n-1,a_2^l}^{(c)}(\theta)\right]$$
$$-(e^{\theta} - 1)\sum_{j=2}^{l} a_j M_{n-1,a_2^{j-1}\bar{a}_j}^{(c)}(\theta)\,. \tag{26}$$

We note here that the set consisting of l−sequences $a_2^{j-1}\bar{a}_j$, $j = 2, 3, \cdots, l$ and a_2^l becomes a prefix set. Then, by Property 1, the second term in the right member of (26) is equal to $e^{\theta} M_{n-1}^{(c)}(\theta)$. Hence (23) of Lemma 1 follows. □

Lemma 2 *For any* $1 \le k \le l-1$,

$$M_{n,a_1^k}^{(c)}(\theta) = \sum_{j=k+1}^{l} a_j M_{n-1,a_2^{j-1}\bar{a}_j}^{(c)}(\theta) + e^{\theta}\left\{\sum_{j=k+1}^{l} \bar{a}_j M_{n-1,a_2^{j-1}\bar{a}_j}^{(c)}(\theta) + M_{n-1,a_2^l}^{(c)}(\theta)\right\}. \tag{27}$$

Proof: By Properties 1 and 2-a), we have

$$M_{n,a_1^k}^{(c)}(\theta) = M_n^{(c)}(\theta) - \sum_{j=1}^{k} M_{n,s_j}^{(c)}(\theta) = \sum_{j=k+1}^{l} M_{n,s_j}^{(c)}(\theta) + M_{n,u_l}^{(c)}(\theta)$$
$$= \sum_{j=k+1}^{l} e^{\theta\bar{a}_j} M_{n-1,a_2^{j-1}\bar{a}_j}^{(c)}(\theta) + e^{\theta} M_{n-1,a_2^l}^{(c)}(\theta). \tag{28}$$

Furthermore, observe the following identity

$$e^{\theta\bar{a}_j} = e^{\theta}\bar{a}_j + a_j\,. \tag{29}$$

Substituting (29) into the second term in the right member of (28), we have (27) of Lemma 2. □

Lemma 3 *For any* $b_1^m \in \mathcal{B}^*$, $M_{n,b_1^m}^{(c)}(\theta)$ *can be written as a linear function of* $M_n^{(c)}(\theta)$, $M_{n-1}^{(c)}(\theta), \cdots, M_{n-m}^{(c)}(\theta)$. *Let* $\tilde{c}$ *be a threshold value whose dyadic expression has the prefix equal to the dyadic expression of* c. *Then, if* $m \le l$, *the expression of* $M_{n,b_1^m}^{(\tilde{c})}(\theta)$ *with the linear combination of* $M_n^{(\tilde{c})}(\theta)$, $M_{n-1}^{(\tilde{c})}(\theta), \cdots, M_{n-m}^{(\tilde{c})}(\theta)$ *is the same as that of* $M_{n,b_1^m}^{(c)}$.

Proof: We first prove the first statement. By Property 2-b), it suffices to show that for $j = 1, 2, \cdots, l$ and for $n \geq l$, $M^{(c)}_{n,u_j}(\theta)$ can be written as a linear function of $M^{(c)}_n(\theta)$, $M^{(c)}_{n-1}(\theta), \cdots, M^{(c)}_{n-j}(\theta)$. Since

$$M^{(c)}_{n,u_1}(\theta) = M^{(c)}_n(\theta) - M^{(c)}_{n,s_1}(\theta) = M^{(c)}_n(\theta) - e^{\theta \bar{a}_1} M^{(c)}_{n-1}(\theta)\,, \tag{30}$$

Lemma 3 is true for $j = 1$. Suppose that Lemma 3 holds for some $j \geq 1$. Then, we have

$$M^{(c)}_{n,u_{j+1}}(\theta) = M^{(c)}_{n,u_j}(\theta) - M^{(c)}_{n,s_{j+1}}(\theta) = M^{(c)}_{n,u_j}(\theta) - e^{\theta \bar{a}_{j+1}} M^{(c)}_{n-1,a_2^j \bar{a}_{j+1}}(\theta)\,, \tag{31}$$

which together with Property 2-b) and the induction hypothesis yields that Lemma 3 holds for $j+1$. The second statement follows from that $\beta^{(\tilde{c})}$ coincides with $\beta^{(c)}$ on the set $\cup_{1 \leq j \leq l} \mathcal{B}^j - \mathcal{U}$. □

Combining Lemmas 1 and 3, we obtain the following theorem.

Theorem 3 *There exist some polynomial functions $\nu_j = \nu_j(e^\theta)$, $j = 1, 2, \cdots, l$ of e^θ such that*

$$\sum_{j=2}^{l} a_j M^{(c)}_{n-1,a_2^{j-1}\bar{a}_j}(\theta) = \sum_{j=1}^{l} \nu_j(e^\theta) M^{(c)}_{n-j}(\theta)\,. \tag{32}$$

Then, for $n \geq l$, $M^{(c)}_n(\theta)$ satisfies a linear difference equation given by

$$M^{(c)}_n(\theta) - (e^\theta + e^{\theta \bar{a}_1}) M^{(c)}_{n-1}(\theta) + (e^\theta - 1) \sum_{j=1}^{l} \nu_j(e^\theta) M^{(c)}_{n-j}(\theta) = 0\,. \tag{33}$$

Let $f^{(c)}(z)$ be denoted by the characteristic polynomial associated with this linear difference equation. It has a form

$$f^{(c)}(z) = 1 - (e^\theta + e^{\theta \bar{a}_1}) z + (e^\theta - 1) \sum_{j=1}^{l} \nu_j(e^\theta) z^j\,. \tag{34}$$

The quantity $\rho^{-1} = (\rho^{(c)}(\theta))^{-1}$ is the minimum positive root of $f^{(c)}(z) = 0$.

We can compute the characteristic polynomial $f^{(c)}(z)$ for an arbitrary prescribed threshold value c with finite dyadic expression. We shall demonstrate it for an example. Consider the previous example in which the threshold value c is given by $c = 5/8 = 0.101$. In this example, we explicitly derive a linear difference equation that $M^{(5/8)}_n(\theta)$ satisfies. Furthermore, we derive an explicit parametric form of the rate function. By Lemma 1, we have

$$M^{(5/8)}_n(\theta) = (e^\theta + 1) M^{(5/8)}_{n-1} - (e^\theta - 1) M^{(5/8)}_{n-1,00}(\theta)\,. \tag{35}$$

By Property 2-b), we have

$$M^{(5/8)}_{n-1,00}(\theta) = M^{(5/8)}_{n-3}(\theta)\,. \tag{36}$$

Thus, we obtain a recursion

$$M^{(5/8)}_n(\theta) - (e^\theta + 1) M^{(5/8)}_{n-1} + (e^\theta - 1) M^{(5/8)}_{n-3}(\theta) = 0\,. \tag{37}$$

The corresponding characteristic polynomial is

$$f^{(5/8)}(z) = 1 - (e^\theta + 1) z + (e^\theta - 1) z^3\,. \tag{38}$$

Since ρ^{-1} is the root of the above polynomial, we have

$$e^{\theta} = \frac{\rho^3 - \rho^2 - 1}{\rho^2 - 1}. \tag{39}$$

We denote the right member of (39) by $g(\rho)$. It can easily be verified that $g(\rho)$ is a monotone increasing and concave function of ρ for $\rho > 1$. Let $g^{-1}(z)$ is an unique branch of inverse functions of $g(z)$ that satisfies $g^{-1}(z) > 1$. Then, we have $\rho = g^{-1}(e^{\theta})$ and ρ is monotone increasing and lower convex function of θ. An expression of the rate function using parameter ρ is given by

$$I^{(5/8)}(y) = \sup_{\rho>1} \left[y \log \left(\frac{\rho^3 - \rho^2 - 1}{\rho^2 - 1} \right) - \log \left(\frac{\rho}{2} \right) \right]. \tag{40}$$

The above supreme is attained by some y for which the derivative of the quantity in the above bracket with respect to ρ is zero. Hence we have

$$y \left[\frac{2\rho - 3\rho^3}{1 + \rho^2 - \rho^3} - \frac{-2\rho}{1 - \rho^2} \right] - \frac{1}{\rho} = 0. \tag{41}$$

Thus, we obtain the following parametric form of the rate function.

$$y = \frac{1}{\rho^2} \cdot \frac{(\rho^2 - 1)(\rho^3 - \rho^2 - 1)}{\rho^3 - 3\rho + 4}, \quad I^{(5/8)}(y) = y \log \left(\frac{\rho^3 - \rho^2 - 1}{\rho^2 - 1} \right) - \log \left(\frac{\rho}{2} \right). \tag{42}$$

4.2 Threshold Values with Some Periodical Finite Dyadic Expression

In this subsection we shall argue a more explicit form of the characteristic polynomials in some special case that c has some periodic property. Furthermore, we establish an explicit characterization of the rate function in this case.

Let $[b_1 b_2 \cdots b_l]^m \in \mathcal{B}^{ml}$ denote $m-$ concatenation of the binary sequence $b_1 b_2 \cdots b_l$. For example $[011]^2 01$ means 01101101. Consider the threshold value c having the following dyadic expression:

$$c = c_m = 0.a_1 a_2 \cdots a_{l-1} \underbrace{[0 a_1 a_2 \cdots a_{l-1}]^m}_{l}. \tag{43}$$

We assume that $a_{l-1} = 1$ and the minimum period of the above binary sequence is l. Througout this subsection we always assume that the threshold value c has the above dyadic expression.

To state our results, we observe that by virtue of Lemma 3, we have

$$\sum_{j=2}^{l-1} a_j M^{(c_m)}_{n-1, a_2^{j-1} \bar{a}_j}(\theta) = \sum_{j=1}^{l-1} \nu_{1,j}(e^{\theta}) M^{(c_m)}_{n-j}(\theta), \tag{44}$$

$$\sum_{j=1}^{l-1} a_j M^{(c_m)}_{n-1, a_2^{j+l-1} \bar{a}_{j+l}}(\theta) = \sum_{j=1}^{2l-1} \nu_{2,j}(e^{\theta}) M^{(c_m)}_{n-j}(\theta), \tag{45}$$

where $\nu_{1,j}(e^{\theta}), j = 1, 2, \cdots, l-1$ and $\nu_{2,j}(e^{\theta}), j = 1, 2, \cdots, 2l-1$ are polynomial functions of e^{θ}. Let π be a cyclic shift of binary sequences with length l. Since l is the minimum length of the period, any of the $(l-1)$-sequences $\pi^j(a_1 a_2 \cdots a_{l-1} 0), j = 1, 2, \cdots, l-1$ do not coincide with $u_l = a_1 a_2 \cdots a_{l-1} 0$. This means that those $(l-1)$-sequences are in the domain $\mathcal{B}^* - \mathcal{U}$ of $\beta^{(c_m)}$. Hence, the quantity

$$\exp \left[\sum_{j=1}^{l-1} \varphi \left(\beta^{(c_m)}(\pi^j(a_1 a_2 \cdots a_{l-1} 0)) \right) \right] \tag{46}$$

is well defined. We denote it by K. Our result is as follows.

Theorem 4 *Suppose that the rational number c has a binary presentation given by (43). Then, for $n \geq lm + l - 1$, $M_n^{(c_m)}(\theta)$ satisfies a linear difference equation given by*

$$M_n^{(c_m)}(\theta) = (e^\theta + e^{\theta\bar{a}_1})M_{n-1}^{(c_m)}(\theta) - (e^\theta - 1)\left[\sum_{j=2}^{l-1} \nu_{1,j}(e^\theta)M_{n-j}^{(c_m)}(\theta) + \sum_{i=1}^{m}\sum_{j=1}^{2l-1} e^{\theta K(i-1)}\nu_{2,j}(e^\theta)M_{n-(i-1)l-j}^{(c_m)}(\theta)\right] \quad (47)$$

Let $f^{(c_m)}(z)$ be denoted by the characteristic polynomial associated with this linear difference equation. Set

$$f_1(z) = 1 - (e^\theta + e^{\theta\bar{a}_1})z + (e^\theta - 1)\sum_{j=1}^{l-1}\nu_{1,j}(e^\theta)z^j\,, \quad f_2(z) = (e^\theta - 1)\sum_{j=1}^{2l-1}\nu_{2,j}(e^\theta)z^j\,. \quad (48)$$

Using $f_1(z)$ and $f_2(z)$, $f^{(c_m)}(z)$ is computed as

$$f^{(c_m)}(z) = f_1(z) + \frac{1 - (e^{\theta K}z^l)^m}{1 - e^{\theta K}z^l}\cdot f_2(z)\,. \quad (49)$$

The quantity $\rho^{-1} = (\rho^{(c_m)}(\theta))^{-1}$ is the minimum positive root of $f^{(c_m)}(z) = 0$.

Proof: By Lemma 1 and the periodic property of the dyadic expression of c_m, we have

$$M_n^{(c_m)}(\theta) = (e^\theta + e^{\theta\bar{a}_1})M_{n-1}^{(c_m)}(\theta) - (e^\theta - 1)\left[\sum_{j=2}^{l} a_j M^{(c_m)}_{n-1,a_2^{j-1}\bar{a}_j}(\theta) + \sum_{i=1}^{m}\sum_{j=1}^{l-1} a_j M^{(c_m)}_{n-1,a_2^{il+j-1}\bar{a}_{il+j}}(\theta)\right]. \quad (50)$$

Suppose that $a_j = 1$. Using Properties 2-a) and b) and periodic property of the binary presentation of c, for $i = 1, 2, \cdots, m$, we obtain the following

$$M^{(c_m)}_{n-1,a_2^{il+j-1}\bar{a}_{il+j}}(\theta) = e^{\theta K}M^{(c_m)}_{n-l,a_2^{(i-1)l+j-1}\bar{a}_{(i-1)l+j}}(\theta) = e^{\theta(i-1)K}M^{(c_m)}_{n-(i-1)l-1,a_2^{l+j-1}\bar{a}_{l+j}}(\theta)\,, \quad (51)$$

which together with (44), (45), and (50), yields (47) of Theorem 4. □

Consider an example given by $l = 2$. In this case $c = c_m = 0.1[01]^m = \frac{2}{3}\left[1 - 2^{-2(m+1)}\right]$. Characteristic polynomial is given by

$$f^{(c_m)}(z) = 1 - (e^\theta + 1)z + (e^\theta - 1)\frac{1 - z^{2m}}{1 - z^2}\cdot z^3\,. \quad (52)$$

Since ρ^{-1} is the root of the above polynomial, we have

$$e^\theta = \frac{\rho^3 - \rho^2 - \rho + \rho^{-2m}}{\rho^2 - 2 + \rho^{-2m}}\,. \quad (53)$$

By the argument quite similar to the previous example we obtain the following parametric form of the rate function.

$$\left.\begin{aligned} y &= \frac{1}{\rho}\left[\frac{3\rho^2 - 2\rho + 1 - 2m\rho^{-2m-1}}{\rho^3 - \rho^2 + \rho - \rho^{-2m}} - \frac{2\rho - 2m\rho^{-2m-1}}{\rho^2 - 2 + \rho^{-2m}}\right]^{-1} \\ I^{(c_m)}(y) &= y\log\left\{\frac{\rho^3 - \rho^2 - \rho + \rho^{-2m}}{\rho^2 - 2 + \rho^{-2m}}\right\} - \log\left(\frac{\rho}{2}\right) \end{aligned}\right\} \quad (54)$$

5 Rate Function for Threshold Values with Infinite Dyadic Expression

In this section we shall argue an explicit form of the rate function for c with infinite periodical dyadic expression. Consider the threshold value c that is obtained by taking a limit of c_m as $m \to \infty$:

$$c = \lim_{m\to\infty} c_m = 0.a_1a_2\cdots a_{l-1}\underbrace{0a_1a_2\cdots a_{l-1}}_{l}\cdots . \tag{55}$$

On $|z| < e^{-(K/l)\theta}$, the characteristic polynomial $f^{(c_m)}(z)$ converges to the following rational function $f^{(c)}(z)$ as $m \to \infty$:

$$\lim_{m\to\infty} f^{(c_m)}(z) = f^{(c)}(z) = f_1(z) + \frac{f_2(z)}{1 - e^{\theta K} z^l}\,. \tag{56}$$

Our result is as follows.

Theorem 5 *Suppose that the rational number c has a binary presentation given by (55). Then, the quantity $\rho^{-1} = (\rho^{(c)}(\theta))^{-1}$ is the minimum root of the equation $f^{(c)}(z) = 0$. This implies that*

$$I^{(c)}(y) = \lim_{m\to\infty} I^{(c_m)}(y)\,. \tag{57}$$

The proof of Theorem 5 will be stated later.

Consider an example given by $l = 2$. In this case $c = \lim_{m\to\infty} c_m = 0.10101\cdots = \frac{2}{3}$. By letting $m \to \infty$ in (54), we obtain the following parametric expression of the rate function

$$y = \frac{1}{\rho}\left[\frac{3\rho^2 - 2\rho + 1}{\rho^3 - \rho^2 + \rho} - \frac{2\rho}{\rho^2 - 2}\right]^{-1}, \quad I^{(2/3)}(y) = y\log\left\{\frac{\rho^3 - \rho^2 - \rho}{\rho^2 - 2}\right\} - \log\left(\frac{\rho}{2}\right). \tag{58}$$

The remaining part of this section is devoted to the proof of Theorem 5. Consider the case that the threshold value c has the following dyadic expression:

$$\tilde{c}_m = 0.a_1a_2\cdots a_{l-1}[\underbrace{0a_1a_2\cdots a_{l-1}}_{l}]^m 1\,. \tag{59}$$

It is obvious that $\sigma_{\tilde{c}_m}(x) \le \sigma_c(x) \le \sigma_{c_m}(x)$ for any real number x. Then, by the definition of $q^{(c)}(\theta)$, we have

$$\frac{1}{2}\rho^{(\tilde{c}_m)}(\theta) \le q^{(c)}(\theta) \le \frac{1}{2}\rho^{(c_m)}(\theta)\,. \tag{60}$$

Hence, to prove Theorem 5, it suffices to show that on some suitable open disc of z, $f^{(\tilde{c}_m)}(z)$ converges to $f^{(c)}(z)$ as $m \to \infty$. Before proving this, we define some polynomial functions. By virtue of Lemma 3, we have

$$\sum_{j=1}^{l-1} a_j M^{(\tilde{c}_m)}_{n-1,a_2^{j+l-1}\bar{a}_{j+l}}(\theta) = \sum_{j=1}^{2l-1} \nu_{2,j}(e^\theta) M^{(\tilde{c}_m)}_{n-j}(\theta)\,, \tag{61}$$

where $\nu_{2,j}(e^\theta), j = 1, 2, \cdots, 2l-1$ are the same as those in (45). Furthermore, again by Lemma 3, there exist some polynomial functions $\nu_{3,j}(e^\theta), j = 1, 2, \cdots, 2l-1$ and $\nu_{4,j}(e^\theta)$, $j = 1, 2, \cdots, l$ of e^θ such that

$$\sum_{j=1}^{l} \bar{a}_j M^{(\tilde{c}_m)}_{n-1,a_2^{j+l-1}\bar{a}_{j+l}}(\theta) = \sum_{j=1}^{2l} \nu_{3,j}(e^\theta) M^{(\tilde{c}_m)}_{n-j}(\theta)\,, \tag{62}$$

$$M^{(\tilde{c}_m)}_{n-1,a_2^{l-1}\bar{a}_l}(\theta) = \sum_{j=1}^{l} \nu_{4,j}(e^\theta) M^{(\tilde{c}_m)}_{n-j}(\theta)\,. \tag{63}$$

$$\tilde{f}_2(z) = \sum_{j=1}^{2l-1} \nu_{2,j}(e^\theta) z^j \,, f_3(z) = \sum_{j=1}^{2l} \nu_{3,j}(e^\theta) z^j \,, f_4(z) = \sum_{j=1}^{l} \nu_{4,j}(e^\theta) z^j \,. \tag{64}$$

Then, we have the following lemma.

Lemma 4

$$f^{(\tilde{c}_m)}(z) - f^{(c_m)}(z) = \left(e^{\theta K} z^l\right)^m \tilde{f}_2(z) + (e^{\theta(K+1)} z^l)^m \left[f_3(z) + e^{\theta(K+1)} z^l f_4(z)\right] \,. \tag{65}$$

Since Theorem 5 immediately follows from the above lemma, we omit the detail of the proof of this theorem. In the following we shall give the proof of Lemma 4.

Proof of Lemma 4: By Lemma 3, there exist some polynomial functions $\kappa_j(e^\theta)$, $1 \le j \le (m+1)l - 1$ of e^θ such that

$$M^{(\tilde{c}_m)}_{n-1,a_2^{(m+1)l-1}\bar{a}_{(m+1)l}}(\theta) = \sum_{j=1}^{(m+1)l-1} \kappa_j(e^\theta) M^{(\tilde{c}_m)}_{n-j}(\theta) \,. \tag{66}$$

Set

$$\eta(z) = \sum_{j=1}^{(m+1)l-1} \kappa_j(e^\theta) z^j \,. \tag{67}$$

Then, by Lemmas 1 and 3, we have

$$f^{(\tilde{c}_m)}(z) - f^{(c_m)}(z) = \eta(z) \,. \tag{68}$$

Hence, it suffices to examine a form of (66). By Properties 2-a) and b) and the periodic property of the binary presentation of $\tilde{c}_m$, we have the following

$$M^{(\tilde{c}_m)}_{n-1,a_2^{(m+1)l-1}\bar{a}_{(m+1)l}}(\theta) = e^{\theta K} M^{(\tilde{c}_m)}_{n-l,a_1^{ml}}(\theta) \,. \tag{69}$$

Applying Lemma 2 to the right member of (69) and using the periodic property of the dyadic expression of $\tilde{c}_m$, we obtain

$$\begin{aligned} & M^{(\tilde{c}_m)}_{n-1,a_2^{(m+1)l-1}\bar{a}_{(m+1)l}}(\theta) \\ &= e^{\theta K} \sum_{j=1}^{l-1} a_j M^{(\tilde{c}_m)}_{n-l-1,a_2^{ml+j-1}\bar{a}_{ml+j}}(\theta) \\ &\quad + e^{\theta(K+1)} \left\{ \sum_{j=1}^{l} \bar{a}_j M^{(\tilde{c}_m)}_{n-l-1,a_2^{ml+j-1}\bar{a}_{ml+j}}(\theta) + M^{(\tilde{c}_m)}_{n-l-1,a_2^{(m+1)l}}(\theta) \right\} . \end{aligned} \tag{70}$$

Using Properties 2-a) and b) and periodic property of the dyadic expression of $\tilde{c}_m$, for $a_j = 1$, we obtain the following

$$\begin{aligned} M^{(\tilde{c}_m)}_{n-l-1,a_2^{ml+j-1}\bar{a}_{ml+j}}(\theta) &= e^{\theta K} M^{(\tilde{c}_m)}_{n-2l-1,a_2^{(m-1)l+j-1}\bar{a}_{(m-1)l+j}}(\theta) \\ &= e^{\theta(m-1)K} M^{(\tilde{c}_m)}_{n-ml-1,a_2^{l+j-1}\bar{a}_{l+j}}(\theta) \,. \end{aligned} \tag{71}$$

Similarly, for $a_j = 0$, we obtain the following

$$\begin{aligned} M^{(\tilde{c}_m)}_{n-l-1,a_2^{ml+j-1}\bar{a}_{ml+j}}(\theta) &= e^{\theta(K+1)} M^{(\tilde{c}_m)}_{n-2l-1,a_2^{(m-1)l+j-1}\bar{a}_{(m-1)l+j}}(\theta) \\ &= e^{\theta(m-1)(K+1)} M^{(\tilde{c}_m)}_{n-ml-1,a_2^{l+j-1}\bar{a}_{l+j}}(\theta) \,. \end{aligned} \tag{72}$$

Furthermore, we have

$$M^{(\tilde{c}_m)}_{n-l-1,a_2^{(m+1)l-1}a_{(m+1)l}}(\theta) = e^{\theta(K+1)}M^{(\tilde{c}_m)}_{n-2l-1,a_2^{ml-1}\bar{a}_{ml}}(\theta)$$
$$= e^{\theta m(K+1)}M^{(\tilde{c}_m)}_{n-(m+1)l-1,a_2^{l-1}\bar{a}_l}(\theta)\,. \qquad (73)$$

Combining (70) - (73), we have

$$M^{(\tilde{c}_m)}_{n-1,a_2^{(m+1)l-1}\bar{a}_{(m+1)l}}(\theta)$$
$$= e^{\theta mK}\sum_{j=1}^{l-1} a_j M^{(\tilde{c}_m)}_{n-ml-1,a_2^{l+j-1}\bar{a}_{l+j}}(\theta)$$
$$+e^{\theta m(K+1)}\left\{\sum_{j=1}^{l}\bar{a}_j M^{(\tilde{c}_m)}_{n-ml-1,a_2^{l+j-1}\bar{a}_{l+j}}(\theta) + e^{\theta(K+1)}M^{(\tilde{c}_m)}_{n-(m+1)l-1,a_2^{l-1}\bar{a}_l}(\theta)\right\}, \qquad (74)$$

which together with (61)-(64) and (66)-(68) yields (65) of Lemma 4. □

References

[1] T. Kohda and A. Kakimoto, "Pseudorandom number generators and chaotic orbits in the logistic map," *Trans. Information Processing Soc. Jpn.*, vol. 27, no. 3, pp. 289-296, 1986.

[2] T. Kohda and A. Tsuneda, "Pseudonoise sequences by chaotic nonlinear maps and their correlation properties," *IEICE Trans.*, E76-B, no. 8, pp. 855-862, 1993.

[3] T. Geisel and V. Fairen, "Statistical properties of chaos in Chebyshev maps," *Physics Letters*, 105A-6, pp. 263-266, 1984.

[4] T. Kohda and A. Tsuneda, "Explicit evaluations of correlation functions of Chebyshev binary and bit sequences based on Perron-Fronbenius operator," *IEICE Trans.*, E77-A, no. 11, pp. 1794-1800, 1994.

[5] Y. Oono and Y. Takahashi, "Chaos, external noise and Fredholm theory," *Prog. Theor. Phys.*, vol. 63, no. 5, pp. 1804-1807, 1980.

[6] Y. Takahashi and Y. Oono, "Towards the statistical mechanics of chaos," *Prog. Theor. Phys.*, vol. 71, no. 4, pp.851-854, 1984.

[7] Y. Oono, "Large deviation and statistical physics," *Prog. Theor. Phys. Suppl.*, no. 99, pp.165-205, 1989.

[8] J. A. Bucklew, *Large Deviation Techniques in Decision, Simulation, and Estimation.* John Wiley & Sons, 1990.