Title	I.I.D. Chaotic Binary Sequences
Author(s)	KOHDA, Tohru
Citation	数理解析研究所講究録 (1997), 1011: 1-15
Issue Date	1997-08
URL	http://hdl.handle.net/2433/61531
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録
1011巻 1997年 1-15

I.I.D. Chaotic Binary Sequences

Tohru KOHDA
Department of Computer Science and Communication Engineering,
Kyushu University

Abstract: Statistical properties of binary sequences generated by a class of ergodic maps with some symmetric properties are discussed on the basis of an ensemble-average technique. We give a simple sufficient condition for such a class of maps to produce a Bernoulli sequence, that is, a sequence of independent and identically distributed (i.i.d.) binary random variables. This condition is expressed in terms of binary function, which is a generalized version of the Rademacher function for the dyadic map.

I. Introduction

A lot of pseudorandom numbers with good properties are frequently used for variety of engineering applications in computer science [1]. It is also well known that a sequence of independent and identically distributed (i.i.d.) binary random variables is necessary as a model for an information source in information theory and communication theory [2]–[4]. In particular, in modern digital communication systems, such as spread spectrum (SS) communications or cryptosystems, binary sequences play an important role. For such binary sequences, linear feedback shift register (LFSR) sequences have often been used [5]–[8].

It is, however, worth noting that as earlier stated [9][10], some nonlinear ergodic maps are good candidates of pseudorandom number generators. It is well known that the Bernoulli map (or the dyadic map) and the tent map can produce sequences of i.i.d. binary random variables. However, if we calculate such dynamics with the help of a computer with its necessarily limited accuracy, the period of the sequences generated from such piecewise linear maps is very short. Such a situation motivated us to use the logistic [9] and the Chebyshev maps [11]. In most of various applications of chaos, a number of investigators have proposed techniques to use a chaotic real-valued trajectory itself rather than its binary version, that is, analogue techniques. Binary sequences play an important role in modern digital communication systems. Such a situation led us to define two types of binary sequence based on a chaotic real-valued orbit generated by ergodic maps [12]; one is referred to as a *chaotic threshold sequence* and the other as a *chaotic bit sequence*. The ensemble-average technique is useful in theoretically evaluating statistical properties of chaos. Note that statistics of chaotic real-valued sequences have already been studied [13]–[15]. Nevertheless, there is few discussion about binary sequences. We shall concentrate our attention on correlation functions of binary sequences which are recognized to be the most important statistics. Furthermore, in practical engineering applications, it is also important to

evaluate statistics of finite-period sequences which are random variables as functions of a seed. The empirical measures of such random variables are also important in estimating the performance of communication systems. If the random variables are i.i.d., the central limit theorem holds automatically [4]. Fortet [16] & Kac [17] showed that the central limit theorem holds for random variables generated by the R-adic map. This implies that the empirical measures of statistics of such random variables tend to the Gaussian distribution. In order to evaluate the variance of the distribution, not only the 2nd-order but also the higher-order correlation functions have to be estimated.

We define various types of binary function to get binary sequences based on a chaotic real-valued orbit generated by ergodic maps, each of which is formed by adding modulo 2 threshold sequences. We exactly evaluate the mean and the correlation function of threshold sequences. Furthermore, using the Perron-Frobenius operator of some ergodic maps, we give a simple sufficient condition for a class of binary functions to produce a fair Bernoulli sequence, that is, a sequence of i.i.d. binary random variables. Such a class of binary functions enables us to define a new Boolean function whose variable is not binary-valued but real-valued, that is, a generalized version of the Rademacher function for the dyadic map [2]–[4].

II. Chaotic Threshold and Bit Sequences and Their Correlation Functions

Perhaps the simplest mathematical objects that can display *chaotic* behavior are a class of one-dimensional maps [15]

$$\omega_{n+1} = \tau(\omega_n), \tag{1}$$

where $\omega_n = \tau^n(\omega_0) \in I, n = 0, 1, 2, \cdots$ and $\tau(\cdot) : I \to I$ is a nonlinear map, where I denotes an interval. It is known that the ensemble-average defined by

$$\langle F \rangle_\tau = \int_I F(\omega) f^*(\omega) d\omega \tag{2}$$

is useful in evaluating statistics of $\{F(\tau^n(\omega))\}_{n=0}^\infty$ under the assumption that $\tau(\omega)$ is mixing on I with respect to an absolutely continuous invariant (or briefly ACI) measure, denoted by $f^*(\omega)d\omega$.

Let $G(\omega)$ and $H(\omega)$ be any two L_1 functions of bounded variation. Consider two sequences $\{G(\tau^n(\omega))\}_{n=0}^\infty$ and $\{H(\tau^n(\omega))\}_{n=0}^\infty$. The 2nd-order cross-correlation function between the two sequences from a seed $\omega = \omega_0$ is defined by

$$\langle \rho^{(2)}(\ell; G, H) \rangle = \int_I G(\omega) H(\tau^\ell(\omega)) f^*(\omega) d\omega, \tag{3}$$

where $\ell = 0, 1, 2, \cdots$. The cross-covariance function is also defined as

$$\langle \tilde{\rho}^{(2)}(\ell; G, H) \rangle = \int_I (G(\omega) - \langle G \rangle)(H(\tau^\ell(\omega)) - \langle H \rangle) f^*(\omega) d\omega \tag{4}$$

$$= \langle \rho^{(2)}(\ell; G, H) \rangle - \langle G \rangle \langle H \rangle. \tag{5}$$

Note that when $G = H$, these denote the auto-correlation function and auto-covariance function, respectively.

If the interval I is given by $I = [d, e]$, then the P-F operator P_τ of the map τ is defined by [15]

$$P_\tau H(\omega) = \frac{d}{d\omega} \int_{\tau^{-1}([d,\omega])} H(y) dy. \tag{6}$$

This operator is very useful in evaluating the correlation functions because it has the following important property:

$$\int_I G(\omega) P_\tau \{H(\omega)\} d\omega = \int_I G(\tau(\omega)) H(\omega) d\omega. \tag{7}$$

Using this property, we get

$$\langle \rho^{(2)}(\ell; G, H) \rangle = \int_I P_\tau^\ell \{G(\omega) f^*(\omega)\} H(\omega) d\omega. \tag{8}$$

The above cross-correlation function $\langle \rho^{(2)}(\ell; G, H) \rangle$ is of major importance to the investigation of statistical properties of sequences $\{G(\tau^n(\omega))\}_{n=0}^\infty$ and $\{H(\tau^n(\omega))\}_{n=0}^\infty$.

For several maps, such as the tent map, the logistic map, and the Chebyshev maps whose invariant density functions are known, the auto-correlation functions of real-valued sequences were already evaluated [13].

In our previous study, we proposed three simple methods to obtain binary sequences from chaotic real-valued sequences $\{\tau^n(\omega)\}_{n=0}^\infty$ with an ergodic map $\tau(\cdot)$ as follows [12]. As will be seen, both of them can give efficient methods to generate simultaneously different sequences of i.i.d. binary random variables for some ergodic maps, the first of which is used by the second and the third.

Method-1: We define a threshold function $\Theta_t(\omega)$ as

$$\Theta_t(\omega) = \begin{cases} 0 & \text{for } \omega < t \\ 1 & \text{for } \omega \geq t \end{cases} \tag{9}$$

and define its complementary function

$$\overline{\Theta}_t(\omega) = 1 - \Theta_t(\omega). \tag{10}$$

Using these functions, we can obtain a binary sequence $\{\Theta_t(\tau^n(\omega))\}_{n=0}^\infty$, which is referred to as a *chaotic threshold sequence*. Here define

$$p_\tau(t) = \langle \Theta_t \rangle = \int_t^\epsilon f^*(\omega) d\omega, \tag{11}$$

$$q_\tau(t) = \langle \overline{\Theta}_t \rangle = \int_d^t f^*(\omega) d\omega. \tag{12}$$

Note that $p_\tau(t)$ is a monotonically decreasing function of t.

Method-2: We write the value of $\omega\,(|\omega| \leq 1)$ in a binary representation:

$$|\omega| = 0.A_1(\omega)A_2(\omega)\cdots A_i(\omega)\cdots, \qquad A_i(\omega) \in \{0,1\}. \tag{13}$$

The i-th bit $A_i(\omega)$ can be expressed as

$$A_i(\omega) = \sum_{r=1}^{2^i-1}(-1)^{r-1}\left\{\Theta_{\frac{r}{2^i}}(\omega) + \overline{\Theta}_{-\frac{r}{2^i}}(\omega)\right\}. \tag{14}$$

Thus we can obtain a binary sequence $\{A_i(\omega_n)\}_{n=0}^{\infty}$ which we call a *chaotic bit sequence.* Since $\Theta_t(\omega)$ can be regarded as a Boolean function whose variable, seed ω, is not binary but real-valued, $A_i(\omega)$ can be rewritten by

$$A_i(\omega) = \bigoplus_{r=1}^{2^i}\left\{\Theta_{-\frac{r}{2^i}}(\omega) \oplus \Theta_{\frac{r}{2^i}}(\omega)\right\} \tag{15}$$

where $\oplus$ denotes modulo 2 addition.

III. Correlation Functions of Chebyshev Threshold and Bit Sequences

The Chebyshev map of degree k with $I = [-1,1]$ is defined by[11]

$$\tau(\omega) = \cos(k\cos^{-1}\omega) \tag{16}$$

whose invariant measure $f^*(\omega)d\omega$ is known to be

$$f^*(\omega)d\omega = \frac{d\omega}{\pi\sqrt{1-\omega^2}}. \tag{17}$$

Now we give the following theorem.

Theorem 1: For the Chebyshev map of degree k, we have

$$P_\tau\{(\Theta_t(\omega) - \langle\Theta_t\rangle)f^*(\omega)\} = \frac{1}{k}s(\tau'(t))(\Theta_{\tau(t)}(\omega) - \langle\Theta_{\tau(t)}\rangle)f^*(\omega) \tag{18}$$

where

$$\langle\Theta_t\rangle = \frac{1}{\pi}\cos^{-1}t, \tag{19}$$

$$s(\omega) = \begin{cases} -1 & (\omega < 0) \\ 1 & (\omega \geq 0). \end{cases} \tag{20}$$

Thus we can get

$$P_\tau^\ell\{(\Theta_t(\omega) - \langle\Theta_t\rangle)f^*(\omega)\} = \frac{1}{k^\ell}s((\tau^\ell)'(t))(\Theta_{\tau^\ell(t)}(\omega) - \langle\Theta_{\tau^\ell(t)}\rangle)f^*(\omega), \tag{21}$$

where

$$(\tau^\ell)'(\omega) = \frac{d}{d\omega}\cos(k^\ell \cos^{-1}\omega) \tag{22}$$

$$= \frac{k^\ell}{\sqrt{1-\omega^2}}\sin(k^\ell \cos^{-1}\omega). \tag{23}$$

If we apply this to eq.(8), we obtain the following corollary.

Corollary 1: The correlation function of the Chebyshev binary sequences of degree k is evaluated as

$$\langle\tilde{\rho}^{(2)}(\ell;\Theta_t,\Theta_{t'})\rangle = \frac{1}{k^\ell}s((\tau^\ell)'(t))\langle\tilde{\rho}^{(2)}(0;\Theta_{\tau^\ell(t)},\Theta_{t'})\rangle, \tag{24}$$

where for $a, b \in I$,

$$\langle\tilde{\rho}^{(2)}(0;\Theta_a,\Theta_b)\rangle = \langle\Theta_{\max[a,b]}\rangle - \langle\Theta_a\rangle\langle\Theta_b\rangle. \tag{25}$$

Next consider the correlation function of Chebyshev bit sequences, $\langle\tilde{\rho}^{(2)}(\ell;A_i,A_j)\rangle$, which is rewritten as

$$\begin{aligned}\langle\tilde{\rho}^{(2)}(\ell;A_i,A_j)\rangle = \sum_{r=1}^{2^i-1}\sum_{s=1}^{2^j-1}(-1)^{r+s}\Big\{&\langle\tilde{\rho}^{(2)}(\ell;\Theta_{\frac{r}{2^i}},\Theta_{\frac{s}{2^j}})\rangle - \langle\tilde{\rho}^{(2)}(\ell;\Theta_{\frac{r}{2^i}},\Theta_{-\frac{s}{2^j}})\rangle \\ &-\langle\tilde{\rho}^{(2)}(\ell;\Theta_{-\frac{r}{2^i}},\Theta_{\frac{s}{2^j}})\rangle + \langle\tilde{\rho}^{(2)}(\ell;\Theta_{-\frac{r}{2^i}},\Theta_{-\frac{s}{2^j}})\rangle\Big\}.\end{aligned} \tag{26}$$

Therefore, we can get the following corollary.

Corollary 2. The correlation function of the Chebyshev bit sequences of degree k is evaluated as

$$\begin{aligned}\langle\tilde{\rho}^{(2)}(\ell;A_i,A_j)\rangle = \frac{1}{k^\ell}\sum_{r=1}^{2^i-1}\sum_{s=1}^{2^j-1}(-1)^{r+s} \\ \cdot\Big\{s((\tau^\ell)'(\frac{r}{2^i}))(\langle\tilde{\rho}^{(2)}(0;\Theta_{\tau^\ell(\frac{r}{2^i})},\Theta_{\frac{s}{2^j}})\rangle - \langle\tilde{\rho}^{(2)}(0;\Theta_{\tau^\ell(\frac{r}{2^i})},\Theta_{-\frac{s}{2^j}})\rangle) \\ -s((\tau^\ell)'(-\frac{r}{2^i}))(\langle\tilde{\rho}^{(2)}(0;\Theta_{\tau^\ell(-\frac{r}{2^i})},\Theta_{\frac{s}{2^j}})\rangle - \langle\tilde{\rho}^{(2)}(0;\Theta_{\tau^\ell(-\frac{r}{2^i})},\Theta_{-\frac{s}{2^j}})\rangle)\Big\}.\end{aligned} \tag{27}$$

IV. Piecewise Monotonic Maps

Now we consider a piecewise monotonic map $\tau : [d,e] \to [d,e]$ that satisfies the following properties:

(i) There is a partition $d = d_0 < d_1 < \cdots < d_{N_\tau} = e$ of $[d,e]$ such that for each integer $i = 1, \cdots, N_\tau (N_\tau \geq 2)$ the restriction of τ to the interval $[d_{i-1}, d_i)$, denoted by $\tau_i (1 \leq i \leq N_\tau)$, is a C^2 function; as well as

(ii) $\tau((d_{i-1}, d_i)) = (d,e)$, that is, τ_i is onto;

(iii) τ has a unique ACI measure denoted by $f^*(\omega)d\omega$.

The conditions for τ to have a unique ACI measure are discussed in ref. [18].

For the above map, we have [15]

$$P_\tau H(\omega) = \sum_{i=1}^{N_\tau} |g_i'(\omega)| H(g_i(\omega)) \tag{28}$$

where $g_i(\omega) = \tau_i^{-1}(\omega)$.

For any map $\tau(\cdot)$ defined on the interval $I = [d, e]$, we can give here a generalized version of Method-2, referred to as *Method-3*, as follows [20].

Method-3: We write the value of $\dfrac{\omega - d}{e - d} \in [0, 1]$ in a binary representation:

$$\frac{\omega - d}{e - d} = 0.B_1(\omega)B_2(\omega)\cdots B_i(\omega)\cdots, \quad \omega \in [d, e], \quad B_i(\omega) \in \{0, 1\}. \tag{29}$$

The i-th bit $B_i(\omega)$ can be expressed as

$$B_i(\omega) = \sum_{r=1}^{2^i - 1} (-1)^{r-1} \Theta_{(\epsilon - d)\frac{r}{2^i} + d}(\omega). \tag{30}$$

Its complementary function is given by

$$\overline{B_i}(\omega) = 1 - B_i(\omega). \tag{31}$$

We can obtain a binary sequence $\{B_i(\tau^n(\omega))\}_{n=0}^{\infty}$. Note that $B_i(\omega)$ can also be rewritten in the form of modulo 2 addition of threshold sequences. If the interval $I = [0, 1]$, then $A_i(\omega) = B_i(\omega)$. Thus each of $\{A_i(\tau^n(\omega))\}_{n=0}^{\infty}$ and $\{B_i(\tau^n(\omega))\}_{n=0}^{\infty}$ is referred to as a *chaotic bit sequence.*

Tausworthe [5] and Lewis & Payne [6] gave the methods to obtain a real-valued random variable represented in a binary expansion by using shift register binary sequences. In our methods, on the contrary, we intend to get binary sequences from chaotic real-valued trajectories. This implies that our methods are inversions of Tausworthe and Lewis & Payne's generators.

Next consider $H(\omega) = \Theta_t(\omega) f^*(\omega)$. For $t \in (d_{m-1}, d_m)$, we have

$$\Theta_t(g_i(\omega)) = \begin{cases} 0 & \text{for } i < m \\ 1 & \text{for } i > m. \end{cases} \tag{32}$$

Hence it suffices to consider only the case where $i = m$. We can easily get

$$\Theta_t(g_m(\omega)) = \begin{cases} \Theta_{\tau(t)}(\omega) & \text{for } \tau'(t) > 0 \\ \overline{\Theta}_{\tau(t)}(\omega) & \text{for } \tau'(t) < 0. \end{cases} \tag{33}$$

Thus, for $t \in (d_{m-1}, d_m)$, we can obtain

$$P_\tau\{\Theta_t(\omega)f^*(\omega)\} = \begin{cases} |g_m'(\omega)|\Theta_{\tau(t)}(\omega)f^*(g_m(\omega)) + \sum_{i=m+1}^{N_\tau} |g_i'(\omega)|f^*(g_i(\omega)) & \text{for } \tau'(t) > 0 \\ |g_m'(\omega)|\overline{\Theta}_{\tau(t)}(\omega)f^*(g_m(\omega)) + \sum_{i=m+1}^{N_\tau} |g_i'(\omega)|f^*(g_i(\omega)) & \text{for } \tau'(t) < 0. \end{cases} \tag{34}$$

We now consider a class of the above piecewise monotonic maps satisfying

$$|g_i'(\omega)|f^*(g_i(\omega)) = \frac{1}{N_\tau}f^*(\omega),\ 1 \le i \le N_\tau \tag{35}$$

which is referred to as an *equidistributivity property* [20]. Note that this class contains well known maps, such as the R-adic map, the tent map, the logistic map, and the Chebyshev map of degree k, where $N_\tau = R, 2, 2, k$, respectively. Thus we give the following interesting lemma [20] which is very useful in evaluating correlation functions of chaotic threshold and bit sequences.

Lemma 1: For the piecewise monotonic maps satisfying eq.(35), we can get

$$P_\tau\{(\Theta_t(\omega) - p_\tau(t))f^*(\omega)\} = \frac{1}{N_\tau}s(\tau'(t))(\Theta_{\tau(t)}(\omega) - p_\tau(\tau(t)))f^*(\omega) \tag{36}$$

where $s(\omega)$ is the signum function defined by

$$s(\omega) = \begin{cases} -1 & \text{for } \omega < 0 \\ 1 & \text{for } \omega \ge 0. \end{cases} \tag{37}$$

Corollary 3: The covariance function between two chaotic threshold sequences $\{\Theta_t(\tau^n(\omega))\}_{n=0}^\infty$ and $\{\Theta_{t'}(\tau^n(\omega))\}_{n=0}^\infty$ generated by the piecewise monotonic maps satisfying eq.(35) is evaluated as

$$\langle\tilde{\rho}^{(2)}(\ell; \Theta_t, \Theta_{t'})\rangle = \frac{1}{N_\tau^\ell}s((\tau^\ell)'(t))\langle\tilde{\rho}^{(2)}(0; \Theta_{\tau^\ell(t)}, \Theta_{t'})\rangle, \tag{38}$$

where

$$\langle\tilde{\rho}^{(2)}(0; \Theta_t, \Theta_{t'})\rangle = p_\tau(\max[t, t']) - p_\tau(t)p_\tau(t'), \tag{39}$$

$$(\tau^\ell)'(\omega) = \begin{cases} 1 & \text{for } \ell = 0 \\ \prod_{r=1}^{\ell} \tau'(\tau^{r-1}(\omega)) & \text{for } \ell \ge 1. \end{cases} \tag{40}$$

This corollary makes it easier to calculate the covariance function between bit sequences $\{A_i(\tau^n(\omega))\}_{n=0}^\infty$ (respectively, $\{B_i(\tau^n(\omega))\}_{n=0}^\infty$) and $\{A_j(\tau^n(\omega))\}_{n=0}^\infty$ (respectively, $\{B_j(\tau^n(\omega))\}_{n=0}^\infty$) as follows.

Remark 1: The covariance functions $\langle\tilde{\rho}^{(2)}(\ell;A_i,A_j)\rangle$ and $\langle\tilde{\rho}^{(2)}(\ell;B_i,B_j)\rangle$ are represented respectively as

$$\langle\tilde{\rho}^{(2)}(\ell;A_i,A_j)\rangle = \sum_{r=1}^{2^i-1}\sum_{s=1}^{2^j-1}(-1)^{r+s}\Big\{\langle\tilde{\rho}^{(2)}(\ell;\Theta_{\frac{r}{2^i}},\Theta_{\frac{s}{2^j}})\rangle - \langle\tilde{\rho}^{(2)}(\ell;\Theta_{\frac{r}{2^i}},\Theta_{-\frac{s}{2^j}})\rangle$$
$$-\langle\tilde{\rho}^{(2)}(\ell;\Theta_{-\frac{r}{2^i}},\Theta_{\frac{s}{2^j}})\rangle + \langle\tilde{\rho}^{(2)}(\ell;\Theta_{-\frac{r}{2^i}},\Theta_{-\frac{s}{2^j}})\rangle\Big\}, \tag{41}$$

$$\langle\tilde{\rho}^{(2)}(\ell;B_i,B_j)\rangle = \sum_{r=1}^{2^i-1}\sum_{s=1}^{2^j-1}(-1)^{r+s}\langle\tilde{\rho}^{(2)}(\ell;\Theta_{(\epsilon-d)\frac{r}{2^i}+d},\Theta_{(\epsilon-d)\frac{s}{2^j}+d})\rangle. \tag{42}$$

Note that, as will be seen, $\langle\tilde{\rho}^{(2)}(\ell;B_i,B_j)\rangle$ has a simple form for some ergodic maps.

Remark 2: For piecewise monotonic maps satisfying the equidistributivity property eq.(35), we have

$$\langle\tilde{\rho}^{(2)}(\ell;\Theta_{d_i},\Theta_t)\rangle = \begin{cases} p_\tau(\max[d_i,t]) - p_\tau(d_i)p_\tau(t) & \text{for } \ell=0 \\ 0 & \text{for } \ell\geq 1 \end{cases} \tag{43}$$

which implies that there are some correlations between $\{\Theta_{d_i}(\tau^n(\omega))\}_{n=0}^{\infty}$ and $\{\Theta_t(\tau^n(\omega))\}_{n=0}^{\infty}$ only when $\ell=0$. Of course, if the sequences are completely independent of each other, the covariance functions should have zero value for all ℓ.

V. Symmetric Binary Functions

Now, we introduce here a new binary function. To do this, define a partition $d=t_0<t_1<\cdots<t_{2M}=e$ of $[d,e]$ such that

$$t_r + t_{2M-r} = d+e, \quad r=0,1,\cdots,2M, \tag{44}$$

and T denotes the set of symmetric thresholds $\{t_r\}_{r=0}^{2M}$. Then we get a binary function

$$C_T(\omega) = \sum_{r=1}^{2M-1}(-1)^{r-1}\Theta_{t_r}(\omega), \tag{45}$$

which is referred to as a *binary function with symmetric thresholds* (or briefly a *symmetric binary function*) [20].

Next let us restrict our attention to the map satisfying

$$f^*(d+e-\omega) = f^*(\omega), \quad \omega\in[d,e], \tag{46}$$

which is referred to as a *symmetric property of the invariant measure.* Note that such a class of maps contains well known maps, such as the R-adic map, the tent map, the logistic map, and the Chebyshev map.

Remark 3: For the maps with the symmetric property of the invariant measure eq.(46), we get

$$\langle C_T \rangle = \frac{1}{2}. \tag{47}$$

Furthermore, we consider a somewhat restricted class of piecewise monotonic maps satisfying eq.(35) which also satisfy the *symmetric property of the map*

$$\tau(d+e-\omega) = \tau(\omega), \quad \omega \in [d,e]. \tag{48}$$

Such a class includes the tent map, the logistic map, and the Chebyshev map of even degree k. The fact that τ is monotonic and onto gives

$$\tau\left(\frac{d+e}{2}\right) = d \text{ or } e. \tag{49}$$

The following lemma [20] plays an important role in estimating the covariance functions of symmetric binary sequences $\{C_T(\tau^n(\omega))\}_{n=0}^{\infty}$ as shown in Corollary 4.

Lemma 2: For the piecewise monotonic maps satisfying both eq.(35) and eq.(48), and their symmetric binary functions, we can get

$$P_\tau\{C_T(\omega)f^*(\omega)\} = \langle C_T \rangle f^*(\omega). \tag{50}$$

Corollary 4: Consider the piecewise monotonic maps with both eq.(35) and eq.(48). Denote two different sets of symmetric thresholds by $T = \{t_r\}_{r=0}^{2M}$ and $T' = \{t'_r\}_{r=0}^{2M'}$, where

$$d = t_0 < t_1 < \cdots < t_{2M} = e, \tag{51}$$

$$d = t'_0 < t'_1 < \cdots < t'_{2M'} = e, \tag{52}$$

$$t_r + t_{2M-r} = d + e, \quad r = 0, 1, \cdots, 2M, \tag{53}$$

$$t'_r + t'_{2M'-r} = d + e, \quad r = 0, 1, \cdots, 2M'. \tag{54}$$

Then we can obtain

$$\langle \tilde{\rho}^{(2)}(\ell; C_T, C_{T'}) \rangle = \begin{cases} Q^C_{TT'} - \langle C_T \rangle \langle C_{T'} \rangle & \text{for } \ell = 0 \\ 0 & \text{for } \ell \geq 1 \end{cases} \tag{55}$$

where

$$Q^C_{TT} = \langle C_T \rangle = \frac{1}{2}, \tag{56}$$

$$Q^C_{TT'} = \int_I C_T(\omega) C_{T'}(\omega) f^*(\omega) d\omega = \int_{I^C_{TT'}} d\omega, \tag{57}$$

$$I^C_{TT'} = \left(\bigcup_{r=1}^{2^{i-1}} I^C_T(r) \right) \bigcap \left(\bigcup_{s=1}^{2^{j-1}} I^C_{T'}(s) \right), \tag{58}$$

$$I^C_T(r) = [p_\tau(t_{2r}), p_\tau(t_{2r-1})]. \tag{59}$$

Remark 4: Assume

$$M = 2^{i-1}, \quad t_r = p_\tau^{-1}(1 - \frac{r}{2M}), \quad i \geq 1, \tag{60}$$

$$M' = 2^{j-1}, \quad t'_r = p_\tau^{-1}(1 - \frac{r}{2M'}), \quad j \geq 1. \tag{61}$$

Then we can get

$$Q^C_{TT'} = \frac{1}{4} \quad \text{for } T \neq T' \tag{62}$$

or

$$\langle \tilde{\rho}^{(2)}(\ell; C_T, C_{T'}) \rangle = 0 \quad \text{for all } \ell \geq 0. \tag{63}$$

Remark 5: When $M = 2^{i-1}$ and $t_r = (e-d)r/2^i + d$, we have

$$C_T(\omega) = B_i(\omega). \tag{64}$$

This implies that for the piecewise monotonic maps with both eq.(35) and eq.(48), we can obtain

$$\langle \tilde{\rho}^{(2)}(\ell; B_i, B_j) \rangle = \begin{cases} Q_{ij} - \langle B_i \rangle \langle B_j \rangle & \text{for } \ell = 0 \\ 0 & \text{for } \ell \geq 1 \end{cases} \tag{65}$$

where

$$Q_{ii} = \langle B_i \rangle = \frac{1}{2}, \tag{66}$$

$$Q_{ij} = \int_I B_i(\omega) B_j(\omega) f^*(\omega) d\omega = \int_{I_{ij}} d\omega, \tag{67}$$

$$I_{ij} = \left(\bigcup_{r=1}^{2^{i-1}} I_i(r) \right) \bigcap \left(\bigcup_{s=1}^{2^{j-1}} I_j(s) \right), \tag{68}$$

$$I_i(r) = \left[p_\tau((e-d)\frac{2r}{2^i} + d), p_\tau((e-d)\frac{2r-1}{2^i} + d) \right]. \tag{69}$$

Note that we can easily get $Q_{ij} = \frac{1}{4}$ for $i \neq j$, that is, $\langle \tilde{\rho}^{(2)}(0; B_i, B_j) \rangle = 0$, for the maps with the uniform invariant density $f^*(\omega) = 1$. On the other hand, for the maps with the nonuniform invariant densities, such as the logistic and the Chebyshev map, we can get

$$\lim_{\substack{i \to \infty \\ \text{or } j \to \infty}} Q_{ij} = \frac{1}{4} \quad \text{for } i \neq j. \tag{70}$$

Remark 6: Consider the R-adic map $S_R(\omega)$ defined by

$$S_R(\omega) = R\omega \mod 1, \; R = 2, 3, 4, \cdots, \quad \omega \in [0, 1]. \tag{71}$$

For the R-adic map with even R,

$$\langle \tilde{\rho}^{(2)}(\ell; B_i, B_j) \rangle_{S_R} = 0 \quad \text{for all } \ell. \tag{72}$$

Note that the symmetric binary function is a generalized version of the Rademacher function for the dyadic map [2]–[4].

VI. m-Distributivity of Chaotic Binary Sequences

In the previous section, we discussed the second-order correlation functions of chaotic binary sequences. Now consider m binary functions $G_i(\omega)$ $(i = 1, 2, \cdots, m)$. For m binary events $g_1, g_2, \cdots, g_m$ $(g_i \in \{0, 1\}, i = 1, 2, \cdots, m)$, a joint probability defined by

$$\begin{aligned}&\mathrm{Prob}(g_m, g_{m-1}, \cdots, g_1) = \\ &\quad \mathrm{Prob}(G_m(\omega) = g_m, G_{m-1}(\tau^{\ell_{m-1}}(\omega)) = g_{m-1}, \cdots, G_1(\tau^{\ell_{m-1}+\ell_{m-2}+\cdots+\ell_1}(\omega)) = g_1), \quad (73)\\ &\qquad\qquad \ell_i \geq 0\ (1 \leq i \leq m-1)\end{aligned}$$

must be investigated to test the independency of sequences $\{G_i(\tau^n(\omega))\}_{n=0}^{\infty}$ from a statistical point of view. To do this, the higher-order (the m-th order) correlation function is introduced as follows.

$$\begin{aligned}&\langle \rho^{(m)}(\ell_{m-1}, \ell_{m-2}, \cdots, \ell_1; H_m, H_{m-1}, \cdots, H_1)\rangle \\ &\quad = \int_I H_m(\omega) H_{m-1}(\tau^{\ell_{m-1}}(\omega)) H_{m-2}(\tau^{\ell_{m-1}+\ell_{m-2}}(\omega)) \cdot \\ &\qquad \cdots H_1(\tau^{\ell_{m-1}+\ell_{m-2}+\cdots+\ell_1}(\omega)) f^*(\omega) d\omega \quad \text{for all integers } \ell_i \geq 0, \qquad (74)\end{aligned}$$

where each of $H_i(\omega)$ denotes an L_1 real-valued function $(i = 1, 2, \cdots, m)$. It is, in general, difficult to evaluate such higher-order correlation functions explicitly. However, it is simplified if the following condition is satisfied.

Now define a class of piecewise monotonic maps for which there is a nontrivial real-valued function $H(\omega)$ satisfying

$$P_\tau\{H(\omega) f^*(\omega)\} = \langle H \rangle f^*(\omega). \qquad (75)$$

which is a general version of eq.(50). Note that it is obvious that $H(\omega) \equiv 1$, called the trivial function, satisfies eq.(75) for any map if $f^*(\omega)$ exists. However, we concentrate our attention on nontrivial functions satisfying eq.(75) primarily because eq.(75) is of crucial importance as a sufficient condition for a binary function to produce a sequence of i.i.d. binary random variables [20], as well as one of necessary conditions for a real-valued sequence $\{\tau^n(\omega)\}_{n=0}^{\infty}$ to be independent.

Theorem 2: For any real-valued functions $H_n(\omega)$ $(n = 2, 3, \cdots, m)$ satisfying eq.(75), and for $\ell_n \geq 1$ $(n = 1, 2, \cdots, m-1)$,

$$\langle \rho^{(m)}(\ell_{m-1}, \ell_{m-2}, \cdots, \ell_1; H_m, H_{m-1}, \cdots, H_1)\rangle = \prod_{n=1}^{m} \langle H_n \rangle. \qquad (76)$$

Note that, in the above theorem, $H_1(\omega)$ need not satisfy eq.(75).

Next, let $\vec{U}_m = U_0 U_1 \cdots U_{m-1}$ be an arbitrary string of m binary digits where $U_n \in \{0, 1\}$ $(0 \leq n \leq m-1)$. Then there are 2^m possible strings. Let $\vec{u}_m^{(r)} = u_0^{(r)} u_1^{(r)} \cdots u_{m-1}^{(r)}$ be

the r-th string with binary elements $u_n^{(r)} \in \{0,1\}$. Furthermore, for any L_1 binary function $G(\omega)$, introduce a binary random variable

$$\Gamma_n(\omega; G, \vec{u}_m^{(r)}) = G(\omega)u_n^{(r)} + \overline{G}(\omega)\overline{u}_n^{(r)} \tag{77}$$

where $\overline{G}(\omega) = 1 - G(\omega)$ and $\overline{u}_n^{(r)} = 1 - u_n^{(r)}$. Then the probability of the event $\vec{u}_m^{(r)}$ in an infinite binary sequence $\{G(\tau^n(\omega))\}_{n=0}^{\infty}$ is given by

$$\begin{aligned} \text{Prob}(\vec{u}_m^{(r)}; G) &= \int_I \left\{ \prod_{n=0}^{m-1} \Gamma_n(\tau^n(\omega); G, \vec{u}_m^{(r)}) \right\} f^*(\omega) d\omega \\ &= \langle \rho^{(m)}(\underbrace{1, 1, \cdots, 1}_{m-1}; \Gamma_0(G, \vec{u}_m^{(r)}), \Gamma_1(G, \vec{u}_m^{(r)}), \cdots, \Gamma_{m-1}(G, \vec{u}_m^{(r)})) \rangle. \end{aligned} \tag{78}$$

We can give the following corollary [20].

Corollary 5: For any binary function $\mathcal{B}(\omega)$ satisfying eq.(75), we can easily get

$$\text{Prob}(\vec{u}_m^{(r)}; \mathcal{B}) = \langle \mathcal{B} \rangle^s (1 - \langle \mathcal{B} \rangle)^{m-s}, \tag{79}$$

where s is the number of 1 in $\{u_n^{(r)}\}_{n=0}^{m-1}$.

The above corollary implies that $\{\mathcal{B}(\tau^n(\omega))\}_{n=0}^{\infty}$ is a sequence of i.i.d. binary random variables in the sense that it can realize a Bernoulli sequence with probability $\langle \mathcal{B} \rangle$. Note that we can get a fair Bernoulli sequence when $\langle \mathcal{B} \rangle = \frac{1}{2}$, that is, an m-distributed binary random sequence.

Example 1: For the piecewise monotonic maps satisfying eq.(35), the binary function $\Theta_{d_i}(\omega)$ satisfies eq.(75). It follows that

$$\text{Prob}(\vec{u}_m^{(r)}; \Theta_{d_i}) = p_\tau(d_i)^s q_\tau(d_i)^{m-s}. \tag{80}$$

Example 2: For the piecewise monotonic maps with both eq.(35) and eq.(48), the binary functions $B_i(\omega)$ and $C_T(\omega)$ satisfy eq.(75). It follows that

$$\text{Prob}(\vec{u}_m^{(r)}; B_i) = \frac{1}{2^m} \quad \text{for all } r, \tag{81}$$

$$\text{Prob}(\vec{u}_m^{(r)}; C_T) = \frac{1}{2^m} \quad \text{for all } r, \tag{82}$$

which implies that each of $\{B_i(\tau^n(\omega))\}_{n=0}^{\infty}$ and $\{C_T(\tau^n(\omega))\}_{n=0}^{\infty}$ is a sequence of i.i.d. binary random variables [2].

Example 3: For the R-adic map with even R, eq.(81) holds.

We now give a simple mean of generating a sequence of multi-dimensional i.i.d. binary random vectors. For simplicity, we consider an infinite sequence of two-dimensional (2-D)

binary random vectors $\{(G_1(\tau^{2n}(\omega)), G_2(\tau^{2n+1}(\omega)))\}_{n=0}^{\infty}$, where the probability of the event $(\vec{u}_m^{(r)}, \vec{u}_m^{(r')})$ is given by

$$\mathrm{Prob}((\vec{u}_m^{(r)}, \vec{u}_m^{(r')}); (G_1, G_2)) = \int_I \left\{ \prod_{n=0}^{m-1} \Gamma_n(\tau^{2n}(\omega); G_1, \vec{u}_m^{(r)}) \Gamma_n(\tau^{2n+1}(\omega); G_2, \vec{u}_m^{(r')}) \right\} f^*(\omega) d\omega$$
$$= \langle \rho^{(2m)}(\underbrace{1, 1, \cdots, 1}_{2m-1}; \Gamma_0(G_1, \vec{u}_m^{(r)}), \Gamma_0(G_2, \vec{u}_m^{(r')}), \cdots, \Gamma_{m-1}(G_1, \vec{u}_m^{(r)}), \Gamma_{m-1}(G_2, \vec{u}_m^{(r)})) \rangle. \quad (83)$$

Thus we can give the following corollary [20].

Corollary 6: For the piecewise monotonic maps with both eq.(35) and eq.(48), we can obtain

$$\mathrm{Prob}((\vec{u}_m^{(r)}, \vec{u}_m^{(r')}); (B_i, B_j)) = \frac{1}{4^m} \quad \text{for all } r \text{ and } r', \quad (84)$$

$$\mathrm{Prob}((\vec{u}_m^{(r)}, \vec{u}_m^{(r')}); (C_T, C_{T'})) = \frac{1}{4^m} \quad \text{for all } r \text{ and } r'. \quad (85)$$

This implies that using a decimation by 2 of the bit sequences $\{B_i(\tau^n(\omega))\}_{n=0}^{\infty}$ and $\{B_j(\tau^n(\omega))\}_{n=0}^{\infty}$ (or $\{C_T(\tau^n(\omega))\}_{n=0}^{\infty}$ and $\{C_{T'}(\tau^n(\omega))\}_{n=0}^{\infty}$), we can easily get a sequence of 2-D i.i.d. binary random vectors $\{(B_i(\tau^{2n}(\omega)), B_j(\tau^{2n+1}(\omega)))\}_{n=0}^{\infty}$ (or $\{(C_T(\tau^{2n}(\omega)), C_{T'}(\tau^{2n+1}(\omega)))\}_{n=0}^{\infty}$).

Note that Corollary 6 can be generalized to the case for a sequence of N-dimensional binary random vectors.

It is also important to investigate distributions of statistics of chaotic binary sequences. Note that sequences of such statistics are not, in general, i.i.d. even if the binary sequences are i.i.d.. Fortet [16] & Kac [17] showed that the central limit theorem holds for random variables generated by the R-adic map. According to the Fortet-Kac's theorem, the variance σ^2 of the distribution of the sum $\frac{1}{\sqrt{N}} \sum_{n=1}^{N} G(S_R^n(\omega))$ is given by

$$\sigma^2 = \langle \rho^{(2)}(0; G, G) \rangle_{S_R} + 2 \sum_{n=1}^{\infty} \langle \rho^{(2)}(n; G, G) \rangle_{S_R}, \quad (86)$$

where $G : [0, 1] \to \Re$ is of bounded variation or satisfies Hölder's condition and $\langle G \rangle_{S_R} = 0$. In order to evaluate the variance of such distributions, not only the 2nd-order correlation functions but also higher-order ones ought to be investigated. To do this, the following remark is useful.

Remark 7: If the map τ satisfies eq.(35), the higher-order correlation function of chaotic threshold sequences for any real $t_n \in [d, e]$ and integer $\ell_n \geq 0$ can be calculated by its recursive form as

$$\langle \rho^{(m)}(\ell_{m-1}, \ell_{m-2}, \cdots, \ell_1; \Theta_{t_m}, \Theta_{t_{m-1}}, \cdots, \Theta_{t_1}) \rangle =$$

$$\frac{1}{N_\tau^{\ell_{m-1}}} s((\tau^{\ell_{m-1}})'(t_m))\langle\rho^{(m-1)}(\ell_{m-2},\cdots,\ell_1;\Theta_{\max[\tau^{\ell_{m-1}}(t_m),t_{m-1}]},\Theta_{t_{m-2}},\cdots,\Theta_{t_1})\rangle$$
$$+\left\{p_\tau(t_m)-\frac{1}{N_\tau^{\ell_{m-1}}}s((\tau^{\ell_{m-1}})'(t_m))p_\tau(\tau^{\ell_{m-1}}(t_m))\right\}$$
$$\cdot\langle\rho^{(m-1)}(\ell_{m-2},\cdots,\ell_1;\Theta_{t_{m-1}},\Theta_{t_{m-2}},\cdots,\Theta_{t_1})\rangle, \qquad m\geq 2, \tag{87}$$

where

$$\langle\rho^{(1)}(\Theta_{t_1})\rangle = p_\tau(t_1). \tag{88}$$

Note that eq.(87) enables us to calculate the higher-order correlation function of chaotic bit sequences even if the map τ doesn't satisfy the symmetric property eq.(48).

VII. Concluding Remarks

We have given simple methods to generate a sequence of i.i.d. binary random variables by means of modulo 2 addition of threshold sequences. The correlation functions of various types of chaotic binary sequence have been exactly evaluated by the ensemble-average technique based on the Perron-Frobenius operator. We have also given a sufficient condition for a binary function to produce a sequence of i.i.d. binary random variables. Such a binary function is a generalized version of the Rademacher function for the dyadic map [2]–[4].

References

[1] D. Knuth, *The art of Computer Programming 2, Seminumerical Algorithms*, 2nd ed. Addison-Wesley, Reading, Mass, 1981.

[2] M. Kac, *Statistical Independence in Probability Analysis and Number Theory*, The Mathematical Association of America, 1959.

[3] C. M. Goldie and R. G. E. Pinch, *Communication Theory*, Cambridge University Press, 1991.

[4] P. Billingsley, *Probability and Measure*. John Wiley & Sons, 1995.

[5] R. C. Tausworthe, "Random numbers generated by linear reccurence modulo two," *Mathematics of Computation*, vol. 19, pp. 201–209, 1965.

[6] T. G. Lewis and W. H. Payne, "Generalized feedback shift register pseudorandom number algorithm," *J. ACM*, vol. 20, pp. 456–468, 1973.

[7] D. V. Sarwate and M. B. Pursley, "Crosscorrelation Properties of Pseudorandom and Related Sequences," Proc. IEEE, vol. 68, no. 3, pp.593–619, 1980.

[8] J. L. Massey, "An Introduction to Contemporary Cryptology," Proc. IEEE, vol. 76, no. 5, pp.533–549, May 1988.

[9] S. L. Ulam and J. von Neumann, "On combination of stochastic and deterministic processes," *Bull. Math. Soc.* **53**, p.1120, 1947.

[10] D. S. Ornstein, "Ergodic Theory, Randomness, and 'Chaos'," *Science* vol. 243, pp. 182 186, 1989.

[11] R. L. Adler and T. J. Rivlin, "Ergodic and mixing properties of Chebyshev polynomials, " *Proc. Amer. Math. Soc.* vol. 15, pp. 794–796, 1964.

[12] T. Kohda and A. Tsuneda, "Pseudonoise Sequences by Chaotic Nonlinear Maps and Their Correlation Properties," *IEICE Trans.* vol. E76-B, no. 8, pp. 855–862, 1993.

[13] S. Grossmann and S. Thomae, "Invariant distributions and stationary correlation functions of one-dimensional discrete processes," *Z. Naturforsch.* vol. 32a, pp. 1353–1363, 1977.

[14] T. Geisel and V. Fairen, "Statistical Properties of Chaos in Chebyshev Maps," *Physics Letters* vol. 105A, no. 6, pp. 263–266, 1984.

[15] A. Lasota and M. C. Mackey, *Chaos, Fractals, and Noise*, Springer-Verlag, 1994.

[16] R. Fortet, "Sur une suite egalement répartie," *Studia Math.* vol. 9, pp. 54–69, 1940.

[17] M. Kac, "On the distribution of values of sums of the type $\sum f(2^k t)$," *Ann. Math.* vol. 47, pp. 33–49, 1946.

[18] A. Boyarsky and M. Scarowsky, "On A Class of Transformations Which Have Unique Absolutely Continuous Invariant Measures," *Trans. Am. Math. Soc.* vol. 255, pp. 243–262, 1979.

[19] T. Kohda and A. Tsuneda, "Explicit Evaluations of Correlation Functions of Chebyshev Binary and Bit Sequences Based on Perron-Frobenius Operator," *IEICE., Trans.* vol. E77-A, no. 11, pp. 1794–1800, 1994.

[20] T. Kohda and A. Tsuneda, "Statistics of Chaotic Binary Sequences", *IEEE Trans. Information Theory*, vol.43, no.1, pp.104–112, Jan. 1997.