Title	Chaotic Sequences of I.I.D Binary Random Variable with Their Applications to Communications
Author(s)	Kohda, Tohru
Citation	Chaos Memorial Symposium in Asuka : selected papers dedicated to professor Yoshisuke Ueda on the occasion of his 60th birthday, p.35-44
Issue Date	1997
URL	http://hdl.handle.net/2433/24264
Right	
Type	Book
Textversion	publisher

Chaotic Sequences of I.I.D. Binary Random Variables with Their Applications to Communications

Tohru KOHDA

Department of Computer Science and Communication Engineering, Kyushu University

6-10-1 Hakozaki, Higashi-ku, Fukuoka 812-81, Japan

Abstract: The Bernoulli shift is a fundamental theoretic model of a sequence of independent and identically distributed(i.i.d.) binary random variables in probability theory, ergodic theory, information theory, and so on. We give a simple sufficient condition for a class of ergodic maps with some symmetric properties to produce a chaotic sequence of 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. Applications of such a sequene to communications are also discussed briefly

1 Introduction

Binary sequences[1] play an important role in modern digital communication systems, such as spread spectrum (SS) communications or cryptosystems. Although such a binary sequence can be generated in various ways, linear feedback shift register (LFSR) sequences are employed in nearly all the methods [2]−[6]. It is, however, noteworthy that a sequence of independent and identically distributed (i.i.d.) binary random variables is a typical theoretic model of pseudorandom number generators with good properties[7]−[9].

As is well known in the fields of probability theory and ergodic theory, Rademacher functions for the Bernoulli map (or the dyadic map) can produce sequences of i.i.d. 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. On the other hand, it is also well known that the performance of digital communication systems depends primarily on the statistical properties of binary sequences. Neverthless, in most of various applications of chaos to communications, a number of investigators have proposed techniques to use a chaotic real-valued trajectory itself rather than its binary version, that is, analogue techniques. Such a situation motivated us to define [10] several types of binary sequence based on a chaotic real-valued orbit generated by ergodic maps such as logistic [11] and the Chebyshev maps [12]. Furthermore, using the Perron-Frobenius operator of some ergodic maps, we have given a simple sufficient condition for a class of binary functions to produce a sequence of i.i.d. binary random variables.[13],[14]

In this paper, we shortly review several types of method for generating chaotic sequences of i.i.d. binary random variables. Furthermore, we briefly discuss applications of such chaotic sequences to spread spectrum communications and cryptosystems.

2 Chaotic Binary Sequences

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 $I = [d, e]$ 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

$$\begin{aligned} \langle \bar{\rho}^{(2)}(\ell; G, H) \rangle &= \int_I (G(\omega) - \langle G \rangle)(H(\tau^\ell(\omega)) - \langle H \rangle) f^*(\omega) d\omega & (4) \\ &= \langle \rho^{(2)}(\ell; G, H) \rangle - \langle G \rangle \langle H \rangle. & (5) \end{aligned}$$

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 [16], [17].

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 [10].

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

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

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

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

Method-2: We write the value of ω ($|\omega| \leq 1$) 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.

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

$$\frac{\omega - d}{e - d} = 0.B_1(\omega)B_2(\omega)\cdots B_i(\omega)\cdots, \quad \omega \in [d,e], \quad B_i(\omega) \in \{0,1\}. \tag{16}$$

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

$$B_i(\omega) = \sum_{r=1}^{2^i-1} (-1)^{r-1} \Theta_{(e-d)\frac{r}{2^i}+d}(\omega). \tag{17}$$

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 [2] and Lewis & Payne [3] 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.

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 τ_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]

$$P_\tau H(\omega) = \sum_{i=1}^{N_\tau} |g_i'(\omega)| H(g_i(\omega)) \tag{18}$$

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

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

$$|g_i'(\omega)| f^*(g_i(\omega)) = \frac{1}{N_\tau} f^*(\omega), \ 1 \leq i \leq N_\tau \tag{19}$$

which is referred to as the *equidistributivity property* [14]. 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 [14] which is very useful in evaluating correlation functions of chaotic threshold and bit sequences.

Lemma 1: For the piecewise monotonic maps satisfying eq.(19), we can get

$$P_\tau\{(\Theta_t(\omega) - p_\tau(t)) f^*(\omega)\} = \frac{1}{N_\tau} s(\tau'(t))(\Theta_{\tau(t)}(\omega) - p_\tau(\tau(t))) f^*(\omega) \tag{20}$$

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

$$s(\omega) = \begin{cases} -1 & \text{for } \omega < 0 \\ 1 & \text{for } \omega \geq 0. \end{cases} \tag{21}$$

Corollary 1: 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.(19) is evaluated as

$$\langle \tilde{\rho}^{(2)}(\ell; \Theta_t, \Theta_{t'}) \rangle = \frac{1}{N_\tau^\ell} s((\tau^\ell)'(t)) \langle \tilde{\rho}^{(2)}(0; \Theta_{\tau^\ell(t)}, \Theta_{t'}) \rangle, \tag{22}$$

where

$$\langle \tilde{\rho}^{(2)}(0;\Theta_t,\Theta_{t'})\rangle = p_\tau(\max[t,t']) - p_\tau(t)p_\tau(t'), \tag{23}$$

$$(\tau^\ell)'(\omega) = \begin{cases} 1 & \text{for } \ell = 0 \\ \prod_{r=1}^{\ell} \tau'(\tau^{r-1}(\omega)) & \text{for } \ell \geq 1. \end{cases} \tag{24}$$

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: For piecewise monotonic maps satisfying the equidistributivity property eq.(19), we have

$$\langle \tilde{\rho}^{(2)}(\ell;\Theta_{d_i},\Theta_t)\rangle = \begin{cases} p_\tau(\max[d_i,t]) - p_\tau(d_i)p_\tau(t) & \text{for } \ell = 0 \\ 0 & \text{for } \ell \geq 1 \end{cases} \tag{25}$$

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.

3 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

$$t_r + t_{2M-r} = d + e, \quad r = 0, 1, \cdots, 2M, \tag{26}$$

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

$$C_T(\omega) = \sum_{r=0}^{2M} (-1)^r \Theta_{t_r}(\omega), \tag{27}$$

which is referred to as a *binary function with symmetric thresholds* (or briefly a *symmetric binary function*) [14].

Next let us restrict our attention to the map satisfying

$$f^*(d + e - \omega) = f^*(\omega), \quad \omega \in [d,e], \tag{28}$$

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 2: For the maps with the symmetric property of the invariant measure eq.(28), we get

$$\langle C_T \rangle = \frac{1}{2}. \tag{29}$$

Furthermore, we consider a somewhat restricted class of piecewise monotonic maps satisfying eq.(19) which also satisfy the *symmetric property of the map*

$$\tau(d + e - \omega) = \tau(\omega), \quad \omega \in [d,e]. \tag{30}$$

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

$$\tau\left(\frac{d+e}{2}\right) = d \text{ or } e. \tag{31}$$

The following lemma [14] 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 2.

Lemma 2: For the piecewise monotonic maps satisfying both eq.(19) and eq.(28), and their symmetric binary functions, we can get

$$P_\tau\{C_T(\omega)f^*(\omega)\} = \langle C_T\rangle f^*(\omega). \tag{32}$$

Corollary 2: Consider the piecewise monotonic maps with both eq.(19) and eq.(28). Denote two different sets of symmetric thresholds by $T = \{t_r\}_{r=0}^{2M}$ and $T' = \{t'_r\}_{r=0}^{2M'}$, where

$$d = t_0 < t_1 < \cdots < t_{2M} = e, \tag{33}$$
$$d = t'_0 < t'_1 < \cdots < t'_{2M'} = e, \tag{34}$$
$$t_r + t_{2M-r} = d + e, \quad r = 0, 1, \cdots, 2M, \tag{35}$$
$$t'_r + t'_{2M'-r} = d + e, \quad r = 0, 1, \cdots, 2M'. \tag{36}$$

Then we can obtain

$$\langle \bar{\rho}^{(2)}(\ell; C_T, C_{T'})\rangle = \begin{cases} Q^C_{TT'} - \langle C_T\rangle\langle C_{T'}\rangle & \text{for } \ell = 0 \\ 0 & \text{for } \ell \geq 1 \end{cases} \tag{37}$$

where

$$Q^C_{TT} = \langle C_T\rangle = \frac{1}{2}, \tag{38}$$
$$Q^C_{TT'} = \int_I C_T(\omega)C_{T'}(\omega)f^*(\omega)d\omega = \int_{I^C_{TT'}} d\omega, \tag{39}$$
$$I^C_{TT'} = \left(\bigcup_{r=1}^{M} I^C_T(r)\right) \bigcap \left(\bigcup_{s=1}^{M'} I^C_{T'}(s)\right), \tag{40}$$
$$I^C_T(r) = [p_\tau(t_{2r}), p_\tau(t_{2r-1})]. \tag{41}$$

Remark 3: Assume

$$M = 2^{i-1}, \quad t_r = p_\tau^{-1}(1 - \frac{r}{2M}), \quad i \geq 1, \tag{42}$$
$$M' = 2^{j-1}, \quad t'_r = p_\tau^{-1}(1 - \frac{r}{2M'}), \quad j \geq 1. \tag{43}$$

Then we can get

$$Q^C_{TT'} = \frac{1}{4} \quad \text{for } T \neq T' \tag{44}$$

or

$$\langle \bar{\rho}^{(2)}(\ell; C_T, C_{T'})\rangle = 0 \quad \text{for all } \ell \geq 0. \tag{45}$$

Remark 4: When $M = 2^{i-1}$ and $t_r = (e-d)r/2^i + d$, we have

$$C_T(\omega) = B_i(\omega). \tag{46}$$

This implies that for the piecewise monotonic maps with both eq.(19) and eq.(30), we can obtain

$$\langle \tilde{\rho}^{(2)}(\ell; B_i, B_j) \rangle = \begin{cases} Q_{ij} - \langle B_i \rangle \langle B_j \rangle & \text{for } \ell = 0 \\ 0 & \text{for } \ell \geq 1 \end{cases} \tag{47}$$

where

$$Q_{ii} = \langle B_i \rangle = \frac{1}{2}, \tag{48}$$

$$Q_{ij} = \int_I B_i(\omega) B_j(\omega) f^*(\omega) d\omega = \int_{I_{ij}} d\omega, \tag{49}$$

$$I_{ij} = \left(\bigcup_{r=1}^{2^i-1} I_i(r) \right) \bigcap \left(\bigcup_{s=1}^{2^j-1} I_j(s) \right), \tag{50}$$

$$I_i(r) = \left[p_\tau((e-d)\frac{2r}{2^i} + d), p_\tau((e-d)\frac{2r-1}{2^i} + d) \right]. \tag{51}$$

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

$$\lim_{\substack{i \to \infty \\ \text{or } j \to \infty}} Q_{ij} = \frac{1}{4} \quad \text{for } i \neq j. \tag{52}$$

Remark 5: Consider the R-adic map $S_R(\omega)$ defined by

$$S_R(\omega) = R\omega \mod 1, \ R = 2, 3, 4, \cdots, \quad \omega \in [0, 1]. \tag{53}$$

For the R-adic map with even R,

$$\langle \tilde{\rho}^{(2)}(\ell; B_i, B_j) \rangle_{S_R} = 0 \quad \text{for all } \ell. \tag{54}$$

Note that the symmetric binary function is a generalized version of the Rademacher function for the dyadic map [7]–[9].

4 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

$$\begin{aligned} &\text{Prob}(g_m, g_{m-1}, \cdots, g_1) = \\ &\quad \text{Prob}(G_m(\omega) = g_m, G_{m-1}(\tau^{\ell_{m-1}}(\omega)) = g_{m-1}, \cdots, G_1(\tau^{\ell_{m-1}+\ell_{m-2}+\cdots+\ell_1}(\omega)) = g_1), \\ &\qquad\qquad \ell_i \geq 0 \ (1 \leq i \leq m-1) \end{aligned} \tag{55}$$

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.

$$\begin{aligned}&\langle\rho^{(m)}(\ell_{m-1},\ell_{m-2},\cdots,\ell_1;H_m,H_{m-1},\cdots,H_1)\rangle\\&=\int_I H_m(\omega)H_{m-1}(\tau^{\ell_{m-1}}(\omega))H_{m-2}(\tau^{\ell_{m-1}+\ell_{m-2}}(\omega))\cdot\\&\quad\cdots H_1(\tau^{\ell_{m-1}+\ell_{m-2}+\cdots+\ell_1}(\omega))f^*(\omega)d\omega\quad\text{for all integers }\ell_i\geq 0,\end{aligned}\tag{56}$$

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

$$P_\tau\{H(\omega)f^*(\omega)\}=\langle H\rangle f^*(\omega).\tag{57}$$

which is a general version of eq.(32).

Theorem 2: For any real-valued functions $H_n(\omega)$ ($n=2,3,\cdots,m$) satisfying eq.(57), and for $\ell_n\geq 1$ ($n=1,2,\cdots,m-1$),

$$\langle\rho^{(m)}(\ell_{m-1},\ell_{m-2},\cdots,\ell_1;H_m,H_{m-1},\cdots,H_1)\rangle=\prod_{n=1}^{m}\langle H_n\rangle.\tag{58}$$

Note that, in the above theorem, $H_1(\omega)$ need not satisfy eq.(57).

Next, let $\vec{U}_m=U_0U_1\cdots U_{m-1}$ 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

$$\Gamma_n(\omega;G,\vec{u}_m^{(r)})=G(\omega)u_n^{(r)}+\overline{G}(\omega)\overline{u}_n^{(r)}\tag{59}$$

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

$$\begin{aligned}\mathrm{Prob}(\vec{u}_m^{(r)};G)&=\int_I\left\{\prod_{n=0}^{m-1}\Gamma_n(\tau^n(\omega);G,\vec{u}_m^{(r)})\right\}f^*(\omega)d\omega\\&=\langle\rho^{(m)}(\underbrace{1,1,\cdots,1}_{m-1};\Gamma_0(G,\vec{u}_m^{(r)}),\Gamma_1(G,\vec{u}_m^{(r)}),\cdots,\Gamma_{m-1}(G,\vec{u}_m^{(r)}))\rangle.\end{aligned}\tag{60}$$

We can give the following corollary [14].

Corollary 3: For any binary function $\mathcal{B}(\omega)$ satisfying eq.(57), we can easily get

$$\mathrm{Prob}(\vec{u}_m^{(r)};\mathcal{B})=\langle\mathcal{B}\rangle^s(1-\langle\mathcal{B}\rangle)^{m-s},\tag{61}$$

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.

5 Applications to Communications

Spread spectrum techniques are due primarily to properties of spreading sequences (or pseudonoise (PN) sequences)[4]. Various classes of PN sequences have been proposed most of which are generated by LFSR sequences such as the families of the Gold sequences and of the Kasami sequences with low even-correlation values [4],[5]. Let us consider information data with different significant bits to be transmitted, such as (color) image data. In such a situation, we can assign spreading sequences of longer period to more significant bits than to less ones in order to reduce the error probabilities of significant bits by using spreading sequences of variable-period [19],[20]. Such a system becomes asynchronous. Since in asynchronous direct-sequence spread-spectrum multiple access (DS/SSMA), the bit error probabilities depend primarliy on both even and odd correlation values of spreading sequences causing multiple-access interference(MAI), we propose to use a spreading sequence of i.i.d. binary random variables whose statistical properties, such as distributions of correlation values, can be evaluated theoretically.

On the other hand, stream ciphers provide probably the most important method of modern encipherment[6]. The central problem in stream cipher cryptography is the difficulty of efficiently generating unpredictable running-key sequences of binary signals from a short and random key. Although such an unpredictable sequence can be generated in various ways, LFSR sequences are employed in nearly all methods regardless of their possible cryptographic weaknesses. Since a chaotic sequence of i.i.d. binary random variables has several cryptographic characteristics, we can implement a stream cipher system using such a chaotic running-key sequence of i.i.d. binary random variables [21],[22].

6 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. 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 [7]–[9]. Furthermore, applications of such a sequence to communications are also briefly given.

References

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

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

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

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

[5] M. K. Simon, J. K. Omura, R. A. Scholtz, and B.K.Levitt, *Spread Spectrum Communications Handbook*, McGraw-Hill, 1994.

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

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

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

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

[10] 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.

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

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

[13] 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.

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

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

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

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

[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, A. Tsuneda, A. Osiumi and K. Ishii, "A study on pseudonoise-coded image communications" Proc. of SPIE's Visual Communications and Image Processing '94, pp.874–884, 1994.

[20] T. Kohda, K. Ishii, and A. Tsuneda, "Image Transmission Systems through CDMA Channels Using Spreading Sequences of Variable-Period", Proc. of IEEE Fourth International Symposium on Spread Spectrum Techniques & Applications, pp.781–784, 1996.

[21] T. Kohda, and A. Tsuneda, "Chaotic Bit Sequences for Stream Cipher Cryptography and Their Correlation Functions", Proc. SPIE's Inter. Sympo. on Information, Communications and Computer Technology, Applications and Systems, vol. 2612, (Chaotic Circuits for Communication), pp.86-97,1995

[22] T. Kohda, and A. Tsuneda, "Stream Cipher Systems Based on Chaotic Binary Sequences", Proc. SCIS'96, SCIS96-11C, (1996)