Auto-Correlation Properties of Binary Sequences Obtained by Switching Two Bernoulli Chaotic Binary Sequences

Akio Tsuneda and Masahiro Fujikawa

Department of Computer Science and Electrical Engineering,
Kumamoto University
Kumamoto, Japan
E-mail: tsuneda@cs.kumamoto-u.ac.jp

***Abstract*—In Monte-Carlo simulations, various types of random numbers are necessary for simulating various kinds of stochastic phenomena. Using one-dimensional chaotic maps, we can design statistical properties of the chaotic sequences, which implies that chaotic sequences may be useful for Monte-Carlo methods. In this paper, we examine auto-correlation properties of binary sequences obtained by switching two chaotic binary sequences generated by Bernoulli map. It is shown that binary sequences with various new types of auto-correlation properties can be generated.**

***Index Terms*—Auto-correlation function, chaotic binary sequence, Bernoulli map**

I. Introduction

Chaotic sequences can be used as random numbers for some applications such as Monte-Carlo methods, stochastic computing, secure communications (cryptography) [1]. Especially, in Monte-Carlo simulations, random numbers with appropriate statistical properties are needed for simulating stochastic phenomena [2]. Using one-dimensional chaotic maps and binary functions, we can generate chaotic binary sequences with various auto-correlation properties [3], [4].

In this paper, we generate new binary sequences obtained by switching two chaotic binary sequences generated by Bernoulli map. The auto-correlation properties of the new binary sequences are investigated. It will be shown that we can generate binary sequences with much more variety of statistical properties by the proposed method.

II. Chaotic Binary Sequences Generated by Bernoulli Map

In this paper, we use Bernoulli map defined by [5]

$$\tau_B(x) = \begin{cases} 2x & (0 \leq x < \frac{1}{2}), \\ 2x-1 & (\frac{1}{2} \leq x \leq 1), \end{cases} \tag{1}$$

which is shown in Fig.1. Using one-dimensional nonlinear difference equation given by

$$x_{n+1} = \tau_B(x_n),\ x_n \in I = [0,1],\ n = 0,1,2,\cdots, \tag{2}$$

we can generate a chaotic real-valued sequence $\{x_n\}_{n=0}^{\infty}$.

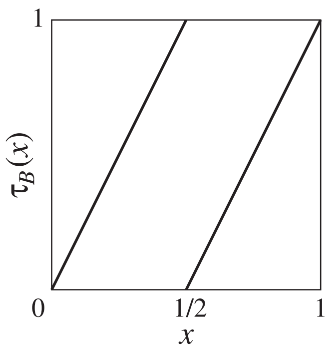


Fig. 1. Bernoulli map

Next, define a pulse (binary) function by

$$P_{[a,b)}(x) = \begin{cases} 1 & \text{for } x \in [a,b), \\ 0 & \text{for } x \notin [a,b). \end{cases} \tag{3}$$

Using $P_{[a,b)}(x)$, we also define a binary function by

$$B_i^{(m)}(x) = \sum_{j=0}^{2^m-1} h_j^{(i)} P_{[\frac{j}{2^m},\frac{j+1}{2^m})}(x) \quad (i = 1,2,\cdots,2^{2^m}), \tag{4}$$

where $h_j^{(i)} \in \{0,1\}$.

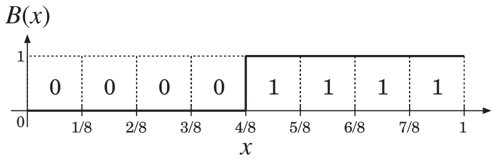
Here, we define the normalized auto-correlation function of a sequence $\{a_n\}_{n=0}^{\infty}$ by

$$C(\ell;a_n) = \frac{E[(a_n - E[a_n])(a_{n+\ell} - E[a_n])]}{E[a_n^2] - E[a_n]^2}, \tag{5}$$

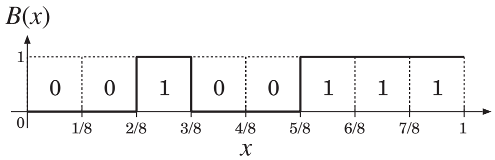
where ℓ is a time delay and $E[\cdot]$ denotes expectation. It is known that chaotic binary sequences, $\{B_i^{(m)}(x_n)\}_{n=0}^{\infty}$, generated by Bernoulli map and $B_i^{(m)}(x)$ have the normalized auto-correlation function given by [6]

$$C(\ell;B_i^{(m)}) = \begin{cases} 1 & (\ell = 0), \\ \varepsilon_\ell & (\ell = 1,2,\cdots,m-1) \\ 0 & (\ell \geq m). \end{cases} \tag{6}$$

In this paper, we use chaotic binary sequences $\{B_i^{(3)}(x_n)\}_{n=0}^{\infty}$ ($m = 3$). Some examples of binary functions $B_i^{(3)}(x)$ are



(a) binary function "00001111"



(b) binary function "00100111"

Fig. 2. Examples of binary functions $B_i^{(3)}(x)$

TABLE I
BINARY FUNCTIONS AND AUTO-CORRELATION VALUES

binary function, where $I_j = [\frac{j}{8}, \frac{j+1}{8})$								correlation value	
I_0	I_1	I_2	I_3	I_4	I_5	I_6	I_7	$\ell = 1$	$\ell = 2$
0	0	0	0	1	1	1	1	0	0
0	1	1	1	0	0	0	1	0	−0.25
0	0	1	0	1	0	1	1	0	−0.25
0	1	1	0	1	1	0	0	0.25	0
0	0	1	1	0	1	1	0	0.25	0
0	0	0	1	1	0	1	1	0.25	0
0	0	1	0	0	1	1	1	0.25	0
0	0	1	1	0	1	0	1	0.25	0
0	1	0	1	0	0	1	1	0.25	0
0	1	1	1	0	1	0	0	0.25	−0.25
0	0	1	0	1	1	1	0	0.25	−0.25
0	0	0	1	0	1	1	1	0.5	0.25
0	0	1	1	1	0	1	0	−0.25	0
0	1	1	1	0	0	1	0	−0.25	0
0	0	1	1	1	0	0	1	−0.25	0
0	1	1	0	0	0	1	1	−0.25	0
0	1	0	1	1	1	0	0	−0.25	0
0	1	0	0	1	1	1	0	−0.25	0
0	0	0	1	1	1	0	1	−0.25	0.25
0	1	0	0	0	1	1	1	−0.25	0.25
0	1	0	0	1	1	0	1	−0.5	0.25

shown in Fig.2, where the binary functions are denoted by "00001111" and "00100111" for simplicity. Also, Table I shows the auto-correlation values of the binary sequences for $\ell = 1, 2$. Note that the number of 1s (and 0s) of each binary function in Table I is 4, that is, the binary sequences $\{B_i^{(3)}(x_n)\}_{n=0}^{\infty}$ are balanced since Bernoulli map has a uniform invariant density. In this paper, we consider such balanced binary sequences.

III. Synthesis of Two Chaotic Binary Sequences

Let $\{a_n\}$ and $\{b_n\}$ be two chaotic binary sequences and assume they are independent of each other. We generate a new binary sequence $\{c_n\}$ by switching $\{a_n\}$ and $\{b_n\}$ as follows.

- The initinal value of $\{c_n\}$ is $c_0 = 0$.

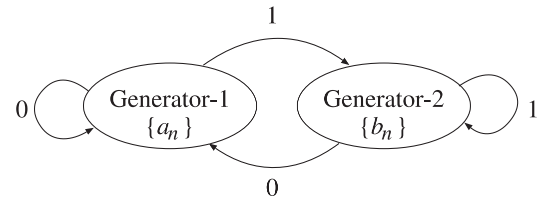


Fig. 3. Proposed sequence generation scheme

- If $c_n = 0$, then c_{n+1} is given by taking the value of $\{a_n\}$ in order.
- If $c_n = 1$, then c_{n+1} is given by taking the value of $\{b_n\}$ in order.

This is illustrated in Fig.3. If each of $\{a_n\}$ and $\{b_n\}$ is an *i.i.d.* (independent and identically distributed) sequence, c_n is a Markov information source.

We investigate the auto-correlation properties of $\{c_n\}$. Assuming $\{c_n\}$ is also balanced ($E[c_n] = \frac{1}{2}$), its numerical (normalized) auto-correlation function is calculated by

$$\widehat{C}(\ell; c_n) = \frac{1}{N} \sum_{n=0}^{N-1} (2c_n - 1)(2c_{n+\ell} - 1), \tag{7}$$

where we set $N = 1,000,000$. Figure 4 shows the auto-correlation functions of $\{c_n\}$ generated by some pairs of $\{a_n\}$ and $\{b_n\}$. We find that various auto-correlation properties are obtained by the proposed method. Also, we find that the following common properties.

- $\widehat{C}(1; c_n) \simeq 0$
- $\widehat{C}(2; c_n) \simeq (\widehat{C}(1; a_n) + \widehat{C}(1; b_n))/2$

IV. Conclusions

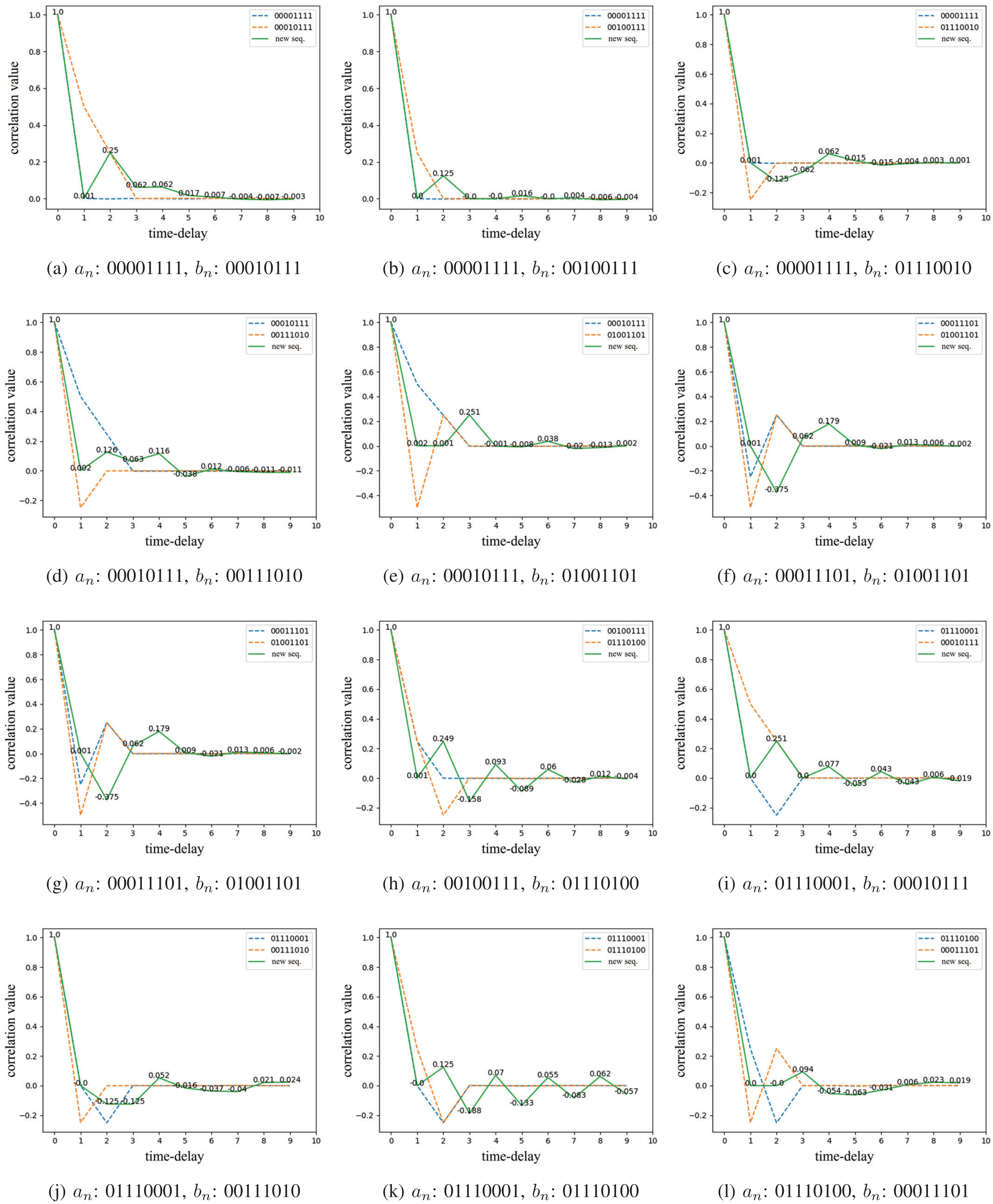
Auto-correlation properties of binary sequences obtained by switching two chaotic binary sequences generated by Bernoulli map have been investigated. It has been shown that various auto-correlation properties can be obtained by the proposed sequence generation method. We will theoretically analyze the auto-correlation function in future study.

Acknowledgment

This work was supported by JSPS KAKENHI Grant Number JP19K12158.

References

[1] M. P. Kennedy, R. Rovatti, and G. Setti, Eds., "Chaotic electronics in telecommunications". Boca Raton, FL: CRC, 2000.
[2] J. E. Gentle, *Random Number Generation and Monte-Carlo Method*, 2nd ed., Springer, 2003.
[3] T. Kohda and A. Tsuneda, "Statistics of Chaotic Binary Sequences," *IEEE Trans. Information Theory*, vol.43, no.1, pp.104–112, 1997.
[4] A. Tsuneda, "Design of binary sequences with tunable exponential autocorrelations and run statistics based on one-dimensional chaotic maps", *IEEE Trans. Circuits Syst. I*, vol.52, no.2, pp.454–462, 2005.
[5] Lasota, A.; Mackey, M. C. *Chaos, Fractals, and Noise*, New York: Springer-Verlag, 1994.
[6] Tin Ni Ni Kyaw and A. Tsuneda, "Generation of Chaos-Based Randam Bit Sequences with Prescribed Auto-Correlations by Post-Processing Using Linear Feedback Shift Registers," *Nonlinear Theory and Its Applications, IEICE*, vol.8, no.3, pp.224–234, 2017.



(a) a_n: 00001111, b_n: 00010111 (b) a_n: 00001111, b_n: 00100111 (c) a_n: 00001111, b_n: 01110010

(d) a_n: 00010111, b_n: 00111010 (e) a_n: 00010111, b_n: 01001101 (f) a_n: 00011101, b_n: 01001101

(g) a_n: 00011101, b_n: 01001101 (h) a_n: 00100111, b_n: 01110100 (i) a_n: 01110001, b_n: 00010111

(j) a_n: 01110001, b_n: 00111010 (k) a_n: 01110001, b_n: 01110100 (l) a_n: 01110100, b_n: 00011101

Fig. 4. Auto-correlation functions of new binary sequences $\{c_n\}$