dynamics

Article

Auto-Correlation Functions of Chaotic Binary Sequences Obtained by Alternating Two Binary Functions

Akio Tsuneda

Division of Informatics and Energy, Faculty of Advanced Science and Technology, Kumamoto University, Kumaomto 860-8555, Japan; tsuneda@cs.kumamoto-u.ac.jp

Abstract: This paper discusses the auto-correlation functions of chaotic binary sequences obtained by a one-dimensional chaotic map and two binary functions. The two binary functions are alternately used to obtain a binary sequence from a chaotic real-valued sequence. We consider two similar methods and give the theoretical auto-correlation functions of the new binary sequences, which are expressed by the auto-/cross-correlation functions of the two chaotic binary sequences generated by a single binary function. Furthermore, some numerical experiments are performed to confirm the validity of the theoretical auto-correlation functions.

Keywords: chaotic binary sequence; one-dimensional chaotic map; auto-correlation function; cross-correlation function; binary function

check for updates

Citation: Tsuneda, T. Auto-Correlation Functions of Chaotic Binary Sequences Obtained by Alternating Two Binary Functions. *Dynamics* **2024**, *4*, 272–286. https://doi.org/10.3390/dynamics4020016

Academic Editors: José Balthazar, Angelo Marcelo Tusset, Átila Madureira Bueno, Diego Colón, Marcus Varanis and Christos Volos

Received: 25 March 2024
Revised: 9 April 2024
Accepted: 15 April 2024
Published: 16 April 2024

1. Introduction

One-dimensional (1-D) nonlinear maps can generate chaotic real-valued sequences [1,2] and they can be used as random numbers due to their simplicity, despite their complex behavior [3–6]. Chaotic real-valued sequences can be transformed into discrete-valued (e.g., binary) sequences using discrete-valued functions, and they have been used in some applications (e.g., CDMA communications as spreading codes) [7]. In 1988, chaotic binary sequences based on a 1-D chaotic map (tent map) were proposed and proven to be independent and identically distributed *(i.i.d.)* [8]. In 1997, the statistical properties of chaotic binary sequences based on 1-D chaotic maps were deeply discussed and a sufficient condition to generate *i.i.d.* binary sequences was given for a class of chaotic maps and binary functions [9].

As described above, ideal random numbers are often assumed to be *i.i.d.* since the most prominent application of chaos-based random numbers is in the area of security, such as cryptography [3–6]. On the other hand, correlated chaotic sequences have also been discussed, and they are useful in some applications other than cryptography. The auto-correlation functions of chaotic real-valued sequences generated by the skew tent map were theoretically derived in [10], where the auto-correlation functions were exponentially decreasing. Chaotic discrete-valued sequences with exponential auto-correlation functions were discussed in [11–13], and some of them can be applied to CDMA communications as spreading codes. In Monte Carlo integration, the convergence rate can be drastically improved by using chaotic sequences with proper auto-correlations, which is called *super-efficient chaotic Monte-Carlo simulation* [14]. Thus, in applications of chaos-based random numbers, the controllability of the statistical properties is quite important. It should be noted that the desired (or optimal) statistical properties of the random numbers are different depending on the application.

Still, there have been many studies on chaos-based random number generation in both theoretical and experimental contexts (e.g., [15–17]). In order to adapt chaos-based random numbers for many applications, we have been attempting to realize chaotic binary (or discrete-valued) sequences with various auto-correlation properties [18]. To generate a chaotic binary sequence, a chaotic map and a binary function are normally used. Of course, there are many combinations of a chaotic map and a binary (or discrete-valued) function, which implies that various statistical properties can be realized. In this paper, however, we propose a different approach to generating chaotic binary sequences using 1-D chaotic maps. We use one chaotic map and two binary functions to generate a chaotic binary sequence, where the two binary functions are alternately used. The theoretical average and auto-correlation function of the new chaotic binary sequence are given, which is followed by numerical experiments using some chaotic maps and binary functions.

The rest of this paper is organized as follows. In Section 2, a brief review of conventional chaotic binary sequences based on 1-D chaotic map is given, where the theoretical average and auto-correlation function are defined. In Section 3, we propose two methods to generate chaotic binary sequences, where a chaotic map and two binary functions are used to generate a chaotic binary sequence. The two binary functions are alternately used. We derive the theoretical auto-correlation functions of the chaotic binary sequences generated by the proposed methods. Numerical results obtained using some chaotic maps and binary functions are shown in Section 4. Finally, Section 5 concludes this paper.

2. Chaotic Binary Sequences Based on a One-Dimensional Map and a Binary Function

A one-dimensional nonlinear difference equation defined by

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

can generate a *chaotic* real-valued sequence $\{x_n\}_{n=0}^{\infty}$ for a chaotic map $\tau(x)$ [1,2]. Moreover, we can obtain a binary sequence $\{B(x_n)\}_{n=0}^{\infty}$ using a binary function $B(x)(\in \{0,1\})$ from a real-valued sequence $\{x_n\}_{n=0}^{\infty}$. Then, the theoretical auto-correlation function of the binary sequence $\{B(x_n)\}_{n=0}^{\infty}$ is defined by

$$A(\ell; B) = \int_I (B(x) - E[B])(B(\tau^\ell(x)) - E[B]) f^*(x) dx, \tag{2}$$

under the assumption that $\tau(x)$ has an invariant density function $f^*(x)$, where $\tau^\ell(x)$ is the ℓ-th iterate of the map τ starting from an initial value $x = x_0$, and $E[B]$ denotes the average of the binary sequence $\{B(x_n)\}_{n=0}^{\infty}$ defined by

$$E[B] = \int_I B(x) f^*(x) dx. \tag{3}$$

We also define the normalized auto-correlation function by

$$\widetilde{A}(\ell; B) = \frac{A(\ell; B)}{A(0; B)}, \tag{4}$$

where $A(0;B)$ is the variance of $\{B(x_n)\}_{n=0}^{\infty}$. On the other hand, the auto-correlation function of $\{B(x_n)\}_{n=0}^{\infty}$ in time-average form is defined by

$$\widehat{A}_N(\ell; B(x_n)) = \frac{1}{N} \sum_{n=0}^{N-1} (B(x_n) - E[B])(B(x_{n+\ell}) - E[B]), \tag{5}$$

which can be used in numerical calculations of auto-correlation functions. According to the Birkhoff individual ergodic theorem [1,2], we have

$$\lim_{N\to\infty} \widehat{A}_N(\ell; B(x_n)) = A(\ell; B) \quad \text{for almost all } x_0. \tag{6}$$

Note that the time average of $\{B(x_n)\}_{n=0}^{\infty}$ is defined by

$$\widehat{E}_N[B(x_n)] = \frac{1}{N}\sum_{n=0}^{N-1} B(x_n), \tag{7}$$

and we also have

$$\lim_{N\to\infty} \widehat{E}_N[B(x_n)] = E[B] \quad \text{for almost all } x_0. \tag{8}$$

Next, for two chaotic binary sequences $\{B_1(x_n)\}_{n=0}^{\infty}$ and $\{B_2(x_n)\}_{n=0}^{\infty}$ generated from a common real-valued sequence $\{x_n\}_{n=0}^{\infty}$, their cross-correlation function is defined by

$$C(\ell; B_1, B_2) = \int_I (B_1(x) - E[B_1])(B_2(\tau^{\ell}(x)) - E[B_2]) f^*(x)dx. \tag{9}$$

Note that $C(\ell; B_1, B_2) = B(\ell; B_2, B_1)$ does not always hold. The normalized cross-correlation function is defined by

$$\widetilde{C}(\ell; B_1, B_2) = \frac{C(\ell; B_1, B_2)}{\sqrt{A(0; B_1)}\sqrt{A(0; B_2)}}. \tag{10}$$

The cross-correlation function between $\{B_1(x_n)\}_{n=0}^{\infty}$ and $\{B_2(x_n)\}_{n=0}^{\infty}$ in time-average form is defined by

$$\widehat{C}_N(\ell; B_1(x_n), B_2(x_n)) = \frac{1}{N}\sum_{n=0}^{N-1}(B_1(x_n) - E[B_1])(B_2(x_{n+\ell}) - E[B_2]). \tag{11}$$

Similar to (6), we have

$$\lim_{N\to\infty} \widehat{C}_N(\ell; B_1(x_n), B_2(x_n)) = C(\ell; B_1, B_2) \quad \text{for almost all } x_0. \tag{12}$$

3. Chaotic Binary Sequences Obtained by Alternating Two Binary Functions

We use two binary functions $B_1(x)$ and $B_2(x)$ to generate a new binary sequence from a chaotic real-valued sequence $\{x_n\}_{n=0}^{\infty}$. We propose the following two methods and discuss the auto-correlation functions of the generated binary sequences.

3.1. Method 1

Using $B_1(x)$ and $B_2(x)$ alternately, we generate a new binary sequence $\{D_n^{(1)}\}_{n=0}^{\infty}$ as

$$B_1(x_0), B_2(x_1), B_1(x_2), B_2(x_3), \cdots, \tag{13}$$

that is,

$$D_n^{(1)} = \begin{cases} B_1(x_n) & (n = 0, 2, 4, \cdots), \\ B_2(x_n) & (n = 1, 3, 5, \cdots). \end{cases} \tag{14}$$

Here, we assume $E[B_1] = E[B_2]$, which gives

$$E[D_n^{(1)}] = E[B_1] = E[B_2]. \tag{15}$$

Next, consider the auto-correlation function of the binary sequence $\{D_n^{(1)}\}_{n=0}^{\infty}$. First, the auto-correlation function in time-average form is expressed by

$$\widehat{A}_N(\ell; D_n^{(1)}) = \begin{cases} \frac{1}{N}(B_1(x_0)B_1(x_\ell) + B_2(x_1)B_2(x_{1+\ell}) + B_1(x_2)B_1(x_{2+\ell}) + B_2(x_3)B_2(x_{3+\ell}) + \cdots) \\ \qquad (\ell = 0, 2, 4, \cdots), \\ \frac{1}{N}(B_1(x_0)B_2(x_\ell) + B_2(x_1)B_1(x_{1+\ell}) + B_1(x_2)B_2(x_{2+\ell}) + B_2(x_3)B_1(x_{3+\ell}) + \cdots) \\ \qquad (\ell = 1, 3, 5, \cdots). \end{cases} \tag{16}$$

Thus, the theoretical auto-correlation function of $\{D_n^{(1)}\}_{n=0}^{\infty}$ is given by

$$A(\ell; D_n^{(1)}) = \begin{cases} \frac{1}{2}(A(\ell; B_1) + A(\ell; B_2)) & (\ell = 0, 2, 4, \cdots), \\ \frac{1}{2}(C(\ell; B_1, B_2) + C(\ell; B_2, B_1)) & (\ell = 1, 3, 5, \cdots). \end{cases} \tag{17}$$

Note that $A(\ell; D_n^{(1)})$ is invariant under exchanging $B_1(x)$ and $B_2(x)$.

3.2. Method 2

Similar to Method 1, we generate a new binary sequence $\{D_n^{(2)}\}_{n=0}^{\infty}$ using $B_1(x)$ and $B_2(x)$ alternately as

$$B_1(x_0), B_2(x_0), B_1(x_1), B_2(x_1), \cdots. \tag{18}$$

That is, for each real value x_n, two binary values $B_1(x_n)$, $B_2(x_n)$ are generated and $D_n^{(2)}$ is expressed by

$$D_n^{(2)} = \begin{cases} B_1(x_{\frac{n}{2}}) & (n = 0, 2, 4, \cdots), \\ B_2(x_{\frac{n-1}{2}}) & (n = 1, 3, 5, \cdots). \end{cases} \tag{19}$$

We also assume $E[B_1] = E[B_2]$, which gives

$$E[D_n^{(2)}] = E[B_1] = E[B_2]. \tag{20}$$

The auto-correlation function of $\{D_n^{(2)}\}_{n=0}^{\infty}$ in time-average form is expressed by

$$\widehat{A}_N(\ell; D_n^{(2)}) = \begin{cases} \frac{1}{N}(B_1(x_0)B_1(x_{\frac{\ell}{2}}) + B_2(x_0)B_2(x_{\frac{\ell}{2}}) + B_1(x_1)B_1(x_{1+\frac{\ell}{2}}) + B_2(x_1)B_2(x_{1+\frac{\ell}{2}}) + \cdots) \\ \qquad (\ell = 0, 2, 4, \cdots), \\ \frac{1}{N}(B_1(x_0)B_2(x_{\frac{\ell-1}{2}}) + B_2(x_0)B_1(x_{\frac{\ell+1}{2}}) + B_1(x_1)B_2(x_{1+\frac{\ell-1}{2}}) + B_2(x_1)B_1(x_{1+\frac{\ell+1}{2}}) + \cdots) \\ \qquad (\ell = 1, 3, 5, \cdots). \end{cases} \tag{21}$$

Thus, the theoretical auto-correlation function of $\{D_n^{(2)}\}_{n=0}^{\infty}$ is given by

$$A(\ell; D_n^{(2)}) = \begin{cases} \frac{1}{2}(A(\frac{\ell}{2}; B_1) + A(\frac{\ell}{2}; B_2)) & (\ell = 0, 2, 4, \cdots), \\ \frac{1}{2}(C(\frac{\ell-1}{2}; B_1, B_2) + C(\frac{\ell+1}{2}; B_2, B_1)) & (\ell = 1, 3, 5, \cdots). \end{cases} \tag{22}$$

Note that $A(\ell; D_n^{(2)})$ is not invariant under the exchange of $B_1(x)$ and $B_2(x)$.

4. Numerical Experiments

We perform numerical experiments on Method 1 and Method 2 using three chaotic maps ($I = [0, 1], f^*(x) = 1$) and some binary functions. Note that the chaotic maps and the binary functions are chosen as examples to obtain some interesting (or unique) auto-/cross-correlation functions.

4.1. Bernoulli Map and Binary Functions

The Bernoulli map with $I = [0, 1]$ is defined by [1,2]

$$\tau_B(x) = \begin{cases} 2x & (0 \leq x < \frac{1}{2}), \\ 2x - 1 & (\frac{1}{2} \leq x \leq 1). \end{cases} \tag{23}$$

For this map, we use the following two binary functions:

$$b_1(x) = \Theta_{\frac{1}{8}}(x) - \Theta_{\frac{1}{4}}(x) + \Theta_{\frac{1}{2}}(x) - \Theta_{\frac{3}{4}}(x) + \Theta_{\frac{7}{8}}(x), \tag{24}$$

$$b_2(x) = \Theta_{\frac{1}{4}}(x) - \Theta_{\frac{3}{8}}(x) + \Theta_{\frac{1}{2}}(x) - \Theta_{\frac{5}{8}}(x) + \Theta_{\frac{3}{4}}(x), \tag{25}$$

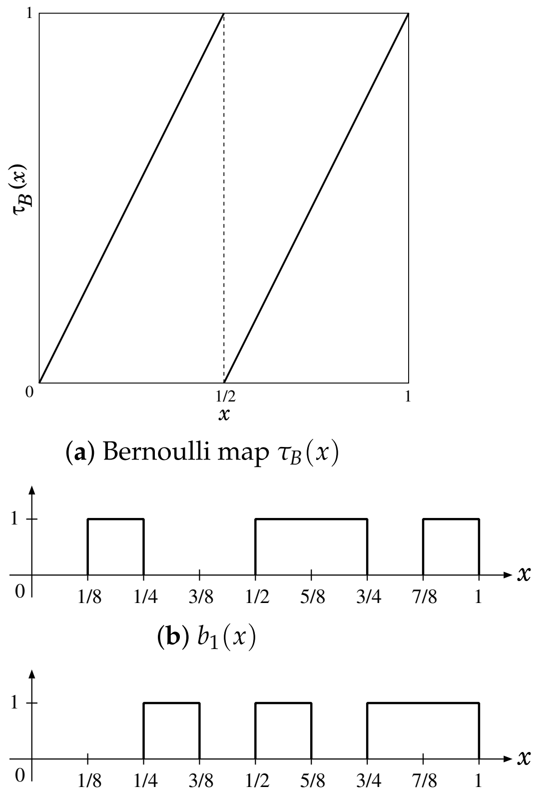
where $\Theta_t(x)$ is a *threshold function* with a threshold t defined by

$$\Theta_t(x) = \begin{cases} 0 & (x < t), \\ 1 & (x \geq t). \end{cases} \tag{26}$$

The Bernoulli map $\tau_B(x)$ and the binary functions $b_1(x)$, $b_2(x)$ are illustrated in Figure 1. Since the Bernoulli map has $f^*(x) = 1$ (uniform density), we have

$$E[b_1] = E[b_2] = \frac{1}{2}, \tag{27}$$

that is, the binary sequences $\{b_1(\tau_B^n(x))\}_{n=0}^{\infty}$ and $\{b_2(\tau_B^n(x))\}_{n=0}^{\infty}$ are balanced sequences. The theoretical correlation functions of the binary sequences can be derived by referring to [9,13] (see Appendix A for details). The normalized theoretical auto-/cross-correlation functions of the two binary sequences are summarized in Table 1 and illustrated in Figure 2. In Figure 2, numerical auto-/cross-correlation functions calculated by (5) and (11) with $N = 10^6$ are also shown.



(**a**) Bernoulli map $\tau_B(x)$

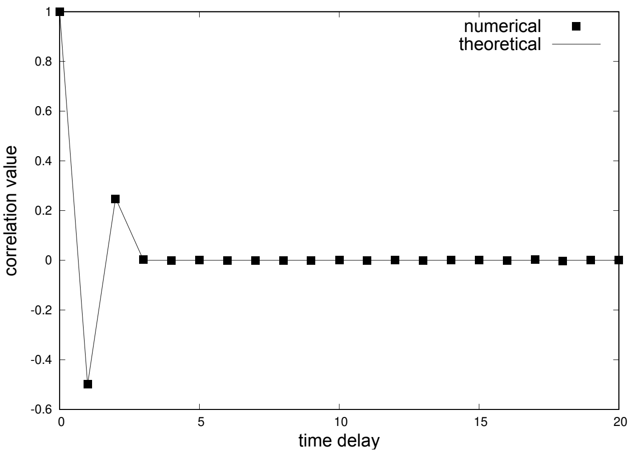
(**b**) $b_1(x)$

(**c**) $b_2(x)$

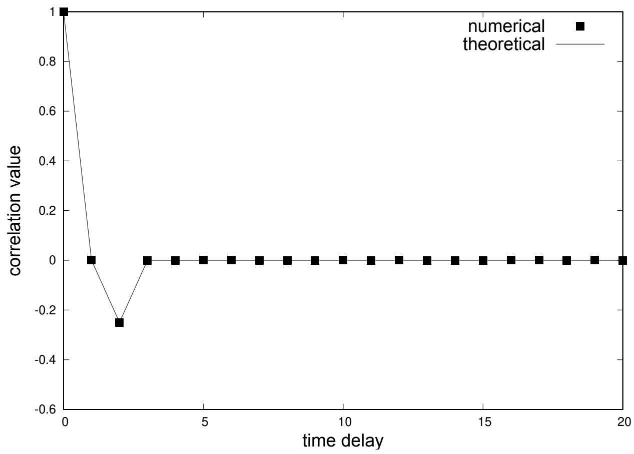
Figure 1. Bernoulli map and binary functions.

Table 1. Normalized theoretical auto-/cross-correlation functions of $\{b_1(\tau_B^n(x))\}_{n=0}^{\infty}$ and $\{b_2(\tau_B^n(x))\}_{n=0}^{\infty}$.

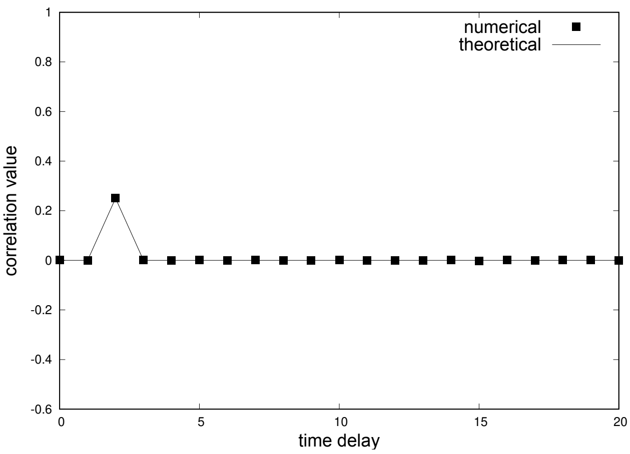
	$\ell = 0$	$\ell = 1$	$\ell = 2$	$\ell \geq 3$
$\widetilde{A}(\ell; b_1)$	1	$-\frac{1}{2}$	$\frac{1}{4}$	0
$\widetilde{A}(\ell; b_2)$	1	0	$-\frac{1}{4}$	0
$\widetilde{C}(\ell; b_1, b_2)$	0	0	$\frac{1}{4}$	0
$\widetilde{C}(\ell; b_2, b_1)$	0	$\frac{1}{2}$	$-\frac{1}{4}$	0



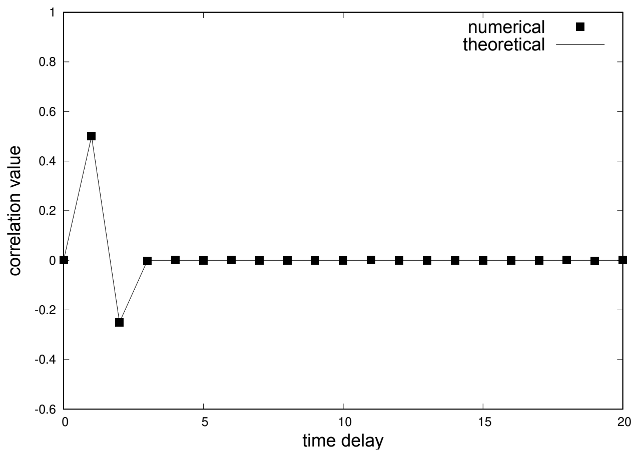
(**a**) $\widetilde{A}(\ell; b_1)$



(**b**) $\widetilde{A}(\ell; b_2)$



(**c**) $\widetilde{C}(\ell; b_1, b_2)$



(**d**) $\widetilde{C}(\ell; b_2, b_1)$

Figure 2. Normalized auto-/cross-correlation functions of $\{b_1(\tau_B^n(x))\}_{n=0}^{\infty}$ and $\{b_2(\tau_B^n(x))\}_{n=0}^{\infty}$.

4.2. Piecewise Linear Map with Three Sections and Binary Functions

Define a fully stretching piecewise linear (PL) map with $I = [0, 1]$ by [13]

$$\tau_{PL}(x) = \begin{cases} -4x + 1 & (0 \leq x < \frac{1}{4}), \\ \frac{12}{5}x - \frac{3}{5} & (\frac{1}{4} \leq x < \frac{2}{3}), \\ -3x + 3 & (\frac{2}{3} \leq x \leq 1). \end{cases} \tag{28}$$

For this map, we use the following two binary functions:

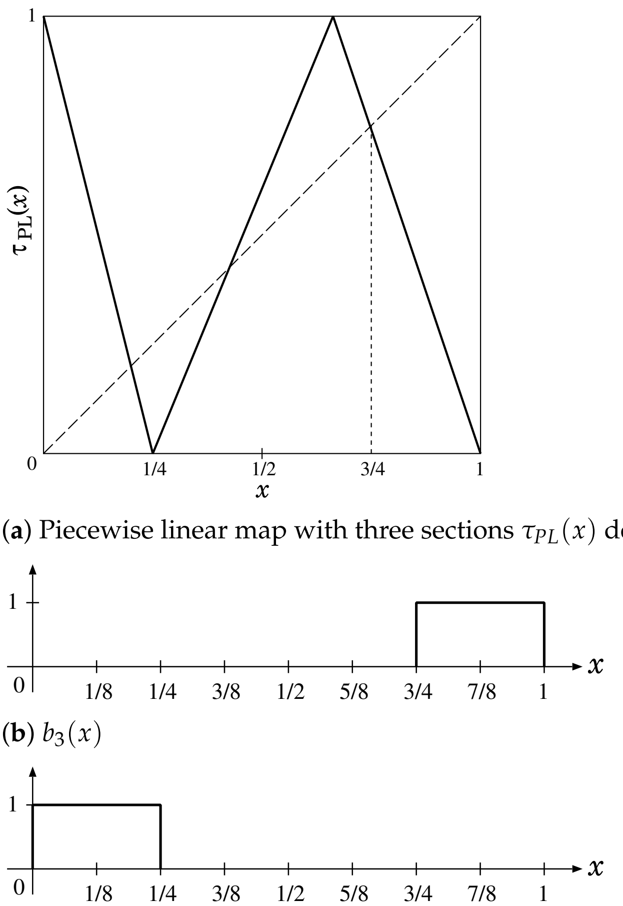
$$b_3(x) = \Theta_{\frac{3}{4}}(x), \tag{29}$$

$$b_4(x) = 1 - \Theta_{\frac{1}{4}}(x). \tag{30}$$

The PL map $\tau_{PL}(x)$ and the binary functions $b_3(x)$, $b_4(x)$ are illustrated in Figure 3. Since the PL map $\tau_{PL}(x)$ also has $f^*(x) = 1$, we have

$$E[b_3] = E[b_4] = \frac{1}{4}, \tag{31}$$

that is, the binary sequences $\{b_3(\tau_{PL}^n(x))\}_{n=0}^{\infty}$ and $\{b_4(\tau_{PL}^n(x))\}_{n=0}^{\infty}$ are unbalanced sequences. The theoretical correlation functions of the binary sequences can be derived by referring to [9,13] (see Appendix A for details). The normalized theoretical auto-/cross-correlation functions of the two binary sequences are summarized in Table 2 and illustrated in Figure 4. In Figure 4, numerical auto-/cross-correlation functions calculated by (5) and (11) with $N = 10^6$ are also shown.



(**a**) Piecewise linear map with three sections $\tau_{PL}(x)$ defined by (28)

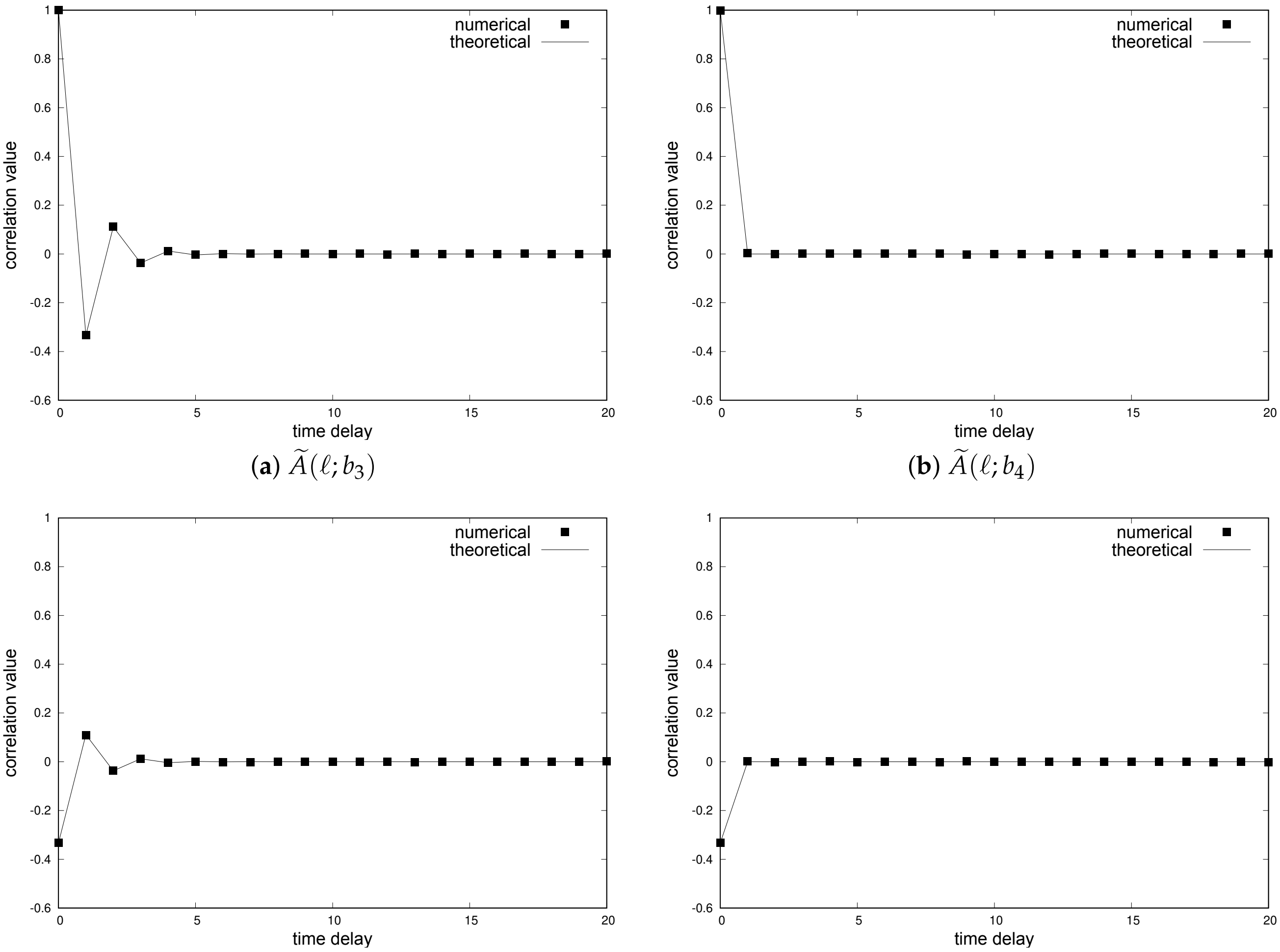
(**b**) $b_3(x)$

(**c**) $b_4(x)$

Figure 3. Piecewise linear map with three sections and binary functions.

Table 2. Normalized theoretical auto-/cross-correlation functions of $\{b_3(\tau_{PL}^n(x))\}_{n=0}^{\infty}$ and $\{b_4(\tau_{PL}^n(x))\}_{n=0}^{\infty}$.

	$\ell = 0$	$\ell = 1$	$\ell = 2$	$\ell \geq 3$
$\widetilde{A}(\ell; b_3)$	$(-3)^{-\ell}$			
$\widetilde{A}(\ell; b_4)$	1	0	0	0
$\widetilde{C}(\ell; b_3, b_4)$	$(-3)^{-\ell-1}$			
$\widetilde{C}(\ell; b_4, b_3)$	$-\frac{1}{3}$	0	0	0



(**a**) $\widetilde{A}(\ell; b_3)$ (**b**) $\widetilde{A}(\ell; b_4)$

(**c**) $\widetilde{C}(\ell; b_3, b_4)$ (**d**) $\widetilde{C}(\ell; b_4, b_3)$

Figure 4. Auto-/cross-correlation functions of $\{b_3(\tau_{PL}^n(x))\}_{n=0}^{\infty}$ and $\{b_4(\tau_{PL}^n(x))\}_{n=0}^{\infty}$.

4.3. Tent Map and Binary Functions

Define the tent map with $I = [0, 1]$ by [1,2,10]

$$\tau_T(x) = \begin{cases} 2x & (0 \le x < \frac{1}{2}), \\ 2(1 - x) & (\frac{1}{2} \le x \le 1). \end{cases} \tag{32}$$

For this map, we use the following two binary functions:

$$b_5(x) = \Theta_{\frac{1}{2}}(x), \tag{33}$$

$$b_6(x, d) = \Theta_d(x) - \Theta_{\frac{1}{2}}(x) + \Theta_{1-d}(x) \ (0 < d \le \frac{1}{2}). \tag{34}$$

The tent map $\tau_T(x)$ and the binary functions $b_5(x)$, $b_6(x)$ are illustrated in Figure 5. Since the tent map $\tau_T(x)$ also has $f^*(x) = 1$, we have

$$E[b_5] = E[b_6] = \frac{1}{2}, \tag{35}$$

that is, the binary sequences $\{b_5(\tau_T^n(x))\}_{n=0}^{\infty}$ and $\{b_6(\tau_T^n(x), d)\}_{n=0}^{\infty}$ are balanced sequences. The theoretical correlation functions of the binary sequences can be derived by referring to [9,13] (see Appendix A for details). Actually, $\{b_5(\tau_T^n(x))\}_{n=0}^{\infty}$ and $\{b_6(\tau_T^n(x), d)\}_{n=0}^{\infty}$ are *i.i.d.* and uncorrelated to each other for $\ell \ge 1$. Note that the cross-correlation function for $\ell = 0$, $C(0; b_5, b_6)$, can be controlled by d (parameter of the binary function $b_6(x, d)$).

The normalized theoretical auto-/cross-correlation functions of the two binary sequences are summarized in Table 3 and illustrated in Figure 6. In Figure 6, numerical auto-/cross-correlation functions calculated by (5) and (11) with $N = 10^6$ are also shown.

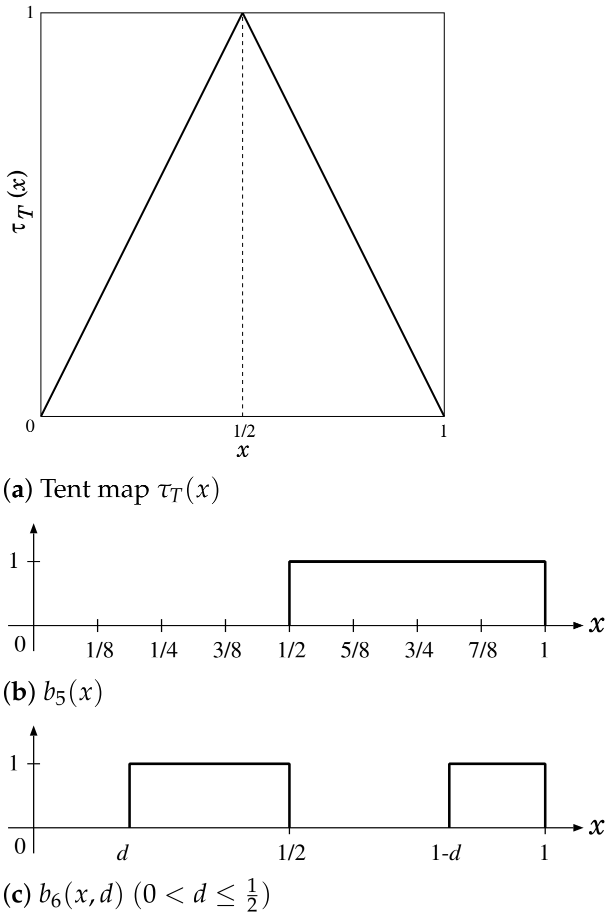


Figure 5. Tent map and binary functions.

Table 3. Normalized theoretical auto-/cross-correlation functions of $\{b_5(\tau_T^n(x))\}_{n=0}^{\infty}$ and $\{b_6(\tau_T^n(x), d)\}_{n=0}^{\infty}$.

	$\ell = 0$	$\ell \geq 1$
$\widetilde{A}(\ell; b_5)$	1	0
$\widetilde{A}(\ell; b_6)$	1	0
$\widetilde{C}(\ell; b_5, b_6)$	$4d - 1$	0

4.4. Auto-Correlation Functions of New Binary Sequences by Method 1 and Method 2

First, Figure 7 shows the normalized auto-correlation functions of new binary sequences $\{D_n^{(1)}\}_{n=0}^{\infty}$ in Method 1, where the theoretical auto-correlation functions are calculated by (17) and the numerical ones are calculated by (5), where $N = 10^6$. We can find that the auto-correlation functions of $\{D_n^{(1)}\}_{n=0}^{\infty}$ given in Figure 7a,b are different from those of the original binary sequences, but Figure 7c,d show the uncorrelated property, which is the same as in the original two binary sequences. We also confirm that the theoretical and numerical ones are in good agreement.

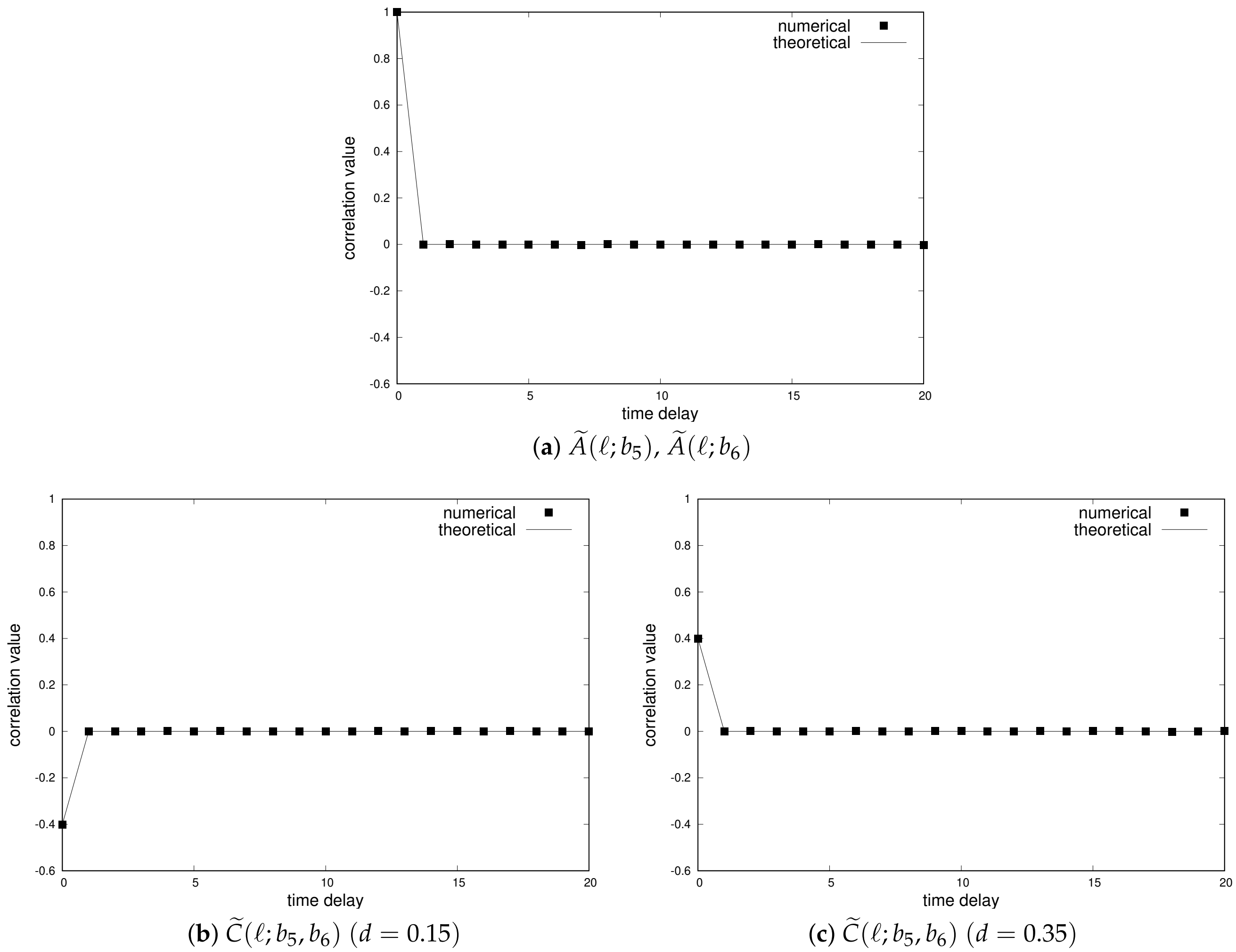


Figure 6. Auto-/cross-correlation functions of $\{b_5(\tau_T^n(x))\}_{n=0}^{\infty}$ and $\{b_6(\tau_T^n(x), d)\}_{n=0}^{\infty}$ $(d = 0.15, 0.35)$.

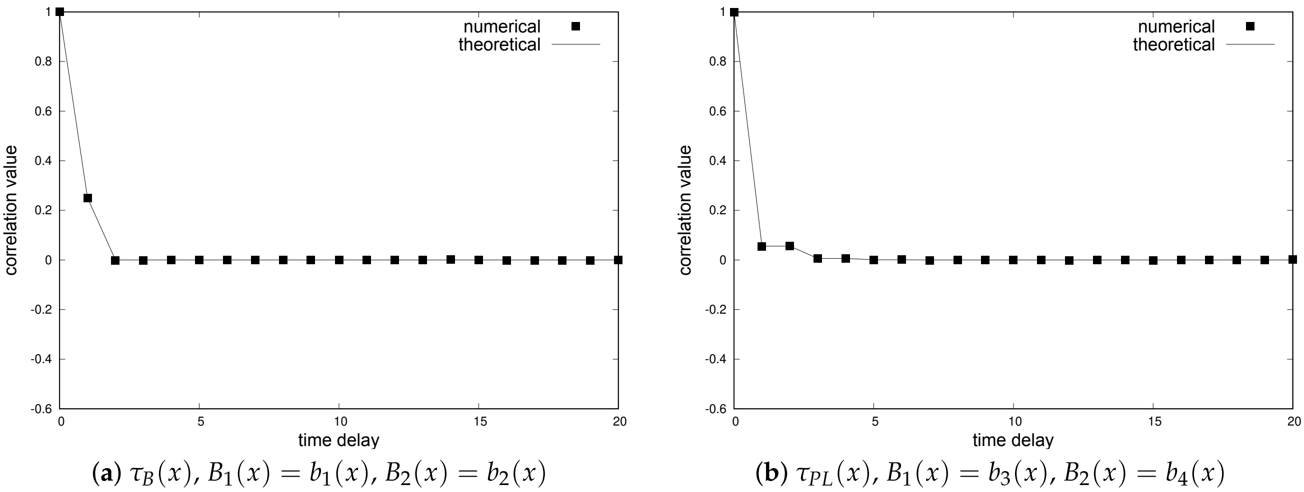
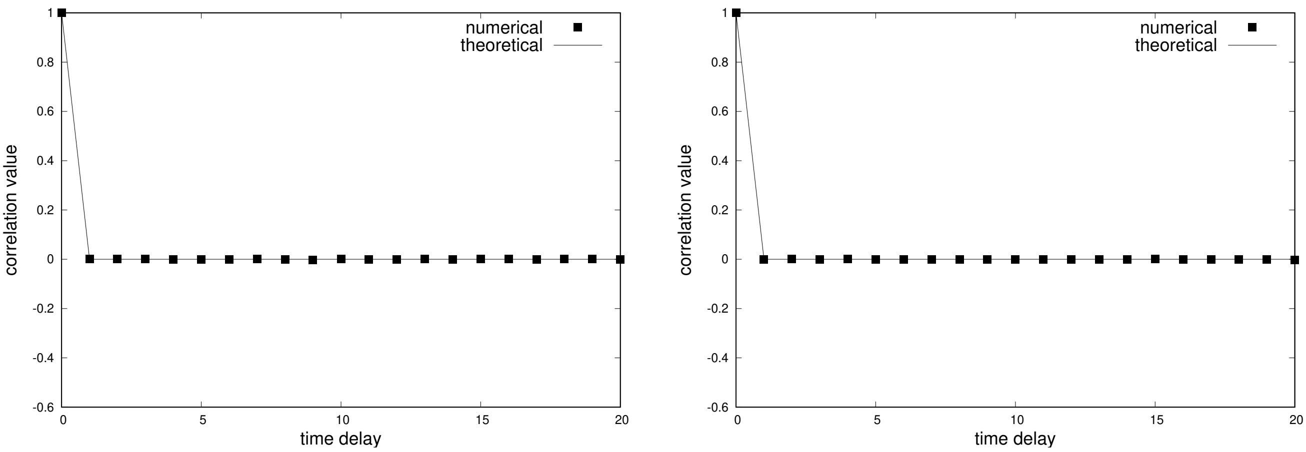


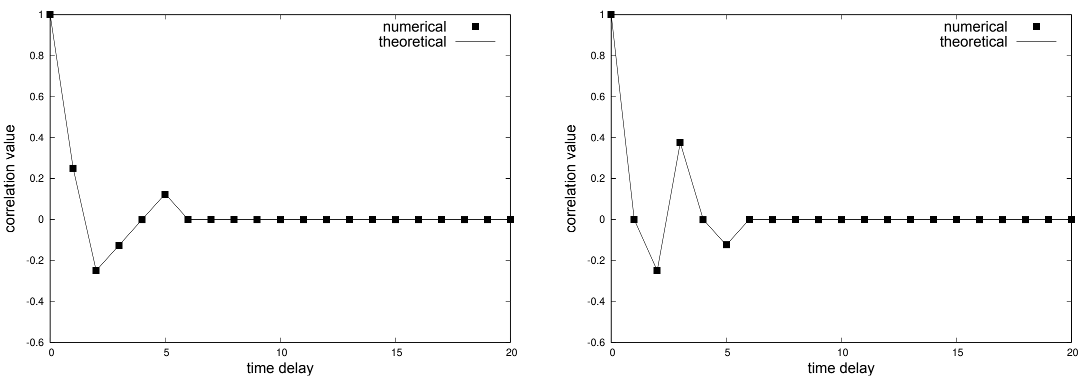
Figure 7. *Cont.*



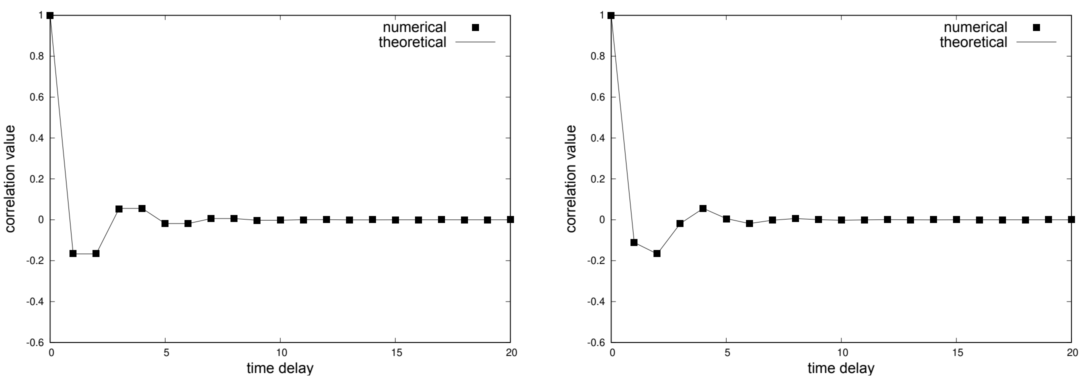
(c) $\tau_T(x)$, $B_1(x) = b_5(x)$, $B_2(x) = b_6(x, 0.15)$ **(d)** $\tau_T(x)$, $B_1(x) = b_5(x)$, $B_2(x) = b_6(x, 0.35)$

Figure 7. Normalized auto-correlation functions of new binary sequences $\{D_n^{(1)}\}_{n=0}^{\infty}$ in Method 1.

Next, Figure 8 shows the normalized auto-correlation functions of new binary sequences $\{D_n^{(2)}\}_{n=0}^{\infty}$ in Method 2, where the theoretical auto-correlation functions are calculated by (22) and the numerical ones are calculated by (5), where $N = 10^6$. We can find that the auto-correlation functions of $\{D_n^{(2)}\}_{n=0}^{\infty}$ are different from those of the original binary sequences, and the theoretical and numerical ones are in good agreement. Moreover, it is confirmed that the auto-correlation functions change if $B_1(x)$ and $B_2(x)$ are exchanged. It should be noted that the auto-correlation value at $\ell = 1$ in (e) and (f) (Figure 8) can be controlled by the parameter d.

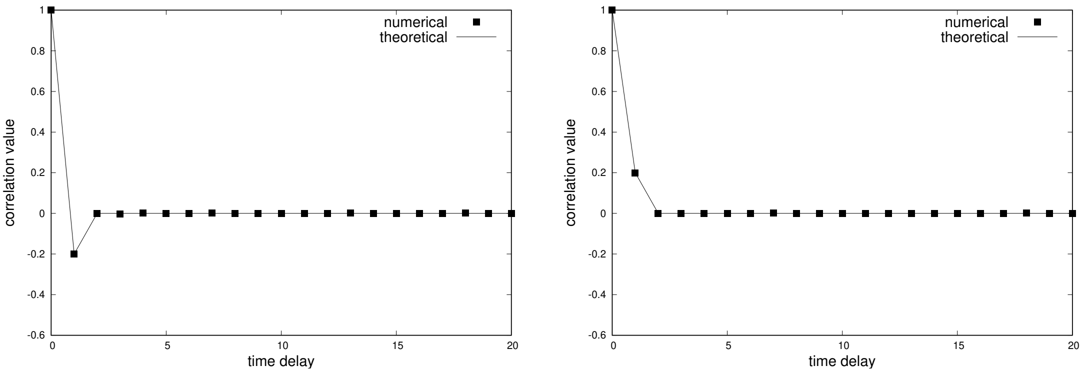


(a) $\tau_B(x)$, $B_1(x) = b_1(x)$, $B_2(x) = b_2(x)$ **(b)** $\tau_B(x)$, $B_1(x) = b_2(x)$, $B_2(x) = b_1(x)$



(c) $\tau_{PL}(x)$, $B_1(x) = b_1(x)$, $B_2(x) = b_2(x)$ **(d)** $\tau_{PL}(x)$, $B_1(x) = b_2(x)$, $B_2(x) = b_1(x)$

Figure 8. *Cont.*



(e) $\tau_T(x)$, $B_1(x) = b_5(x)$, $B_2(x) = b_6(x, 0.15)$ **(f)** $\tau_T(x)$, $B_1(x) = b_5(x)$, $B_2(x) = b_6(x, 0.35)$

Figure 8. Normalized auto-correlation functions of new binary sequences $\{D_n^{(2)}\}_{n=0}^{\infty}$ in Method 2.

5. Conclusions

The auto-correlation functions of chaotic binary sequences obtained by alternating two binary functions are discussed. Their theoretical auto-correlation function is given and verified by numerical experiments. The proposed methods give more flexibility in designing chaotic sequences with various auto-correlation properties (for example, they can be applied to the method in [18]). The number of binary functions can be extended to three or larger numbers, which will be discussed in future work.

Funding: This work was supported by JSPS KAKENHI, Grant Number JP19K12158.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The author declare no conflict of interest.

Appendix A. Derivation of Auto-/Cross-Correlation Functions of Chaotic Binary Sequences Used in Numerical Experiments

First, we define the Perron–Frobenius (PF) operator P_τ of the map τ with an interval $I = [0, 1]$ by

$$P_\tau G(x) = \frac{d}{dx} \int_{\tau^{-1}([0,x])} G(y) dy \tag{A1}$$

which can be rewritten as

$$P_\tau G(x) = \sum_i |g_i'(x)| G(g_i(x)), \tag{A2}$$

where $g_i(x)$ is the i-th preimage of the map $\tau(\cdot)$ [1,2]. The PF operator is very useful in analyzing correlation functions because it has the following important property [1,2]:

$$\int_I G(x) P_\tau \{H(x)\} dx = \int_I G(\tau(x)) H(x) dx. \tag{A3}$$

Using (A3), the cross-correlation function defined by (9) can be rewritten as

$$C(\ell; B_1, B_2) = \int_I P_\tau^\ell \{(B_1(x) - E[B_1]) f^*(x)\} (B_2(x) - E[B_2]) dx. \tag{A4}$$

Putting $B_1(x) = B_2(x) = B(x)$ in (A4), we have the auto-correlation function. Thus, it is important to calculate $P_\tau^\ell \{(B(x) - E[B]) f^*(x)\}$ $(\ell = 1, 2, \cdots)$ for the analysis of the auto-/cross-correlation functions.

Appendix A.1. Correlation Functions of Chaotic Binary Sequences Generated by Bernoulli Map

For Bernoulli map $\tau_B(x)$ defined by (23) and the threshold function $\Theta_t(x)$ defined by (26), we have [9]

$$P_\tau\{\Theta_t(x) - E[\Theta_t]\} = \frac{1}{2}(\Theta_{\tau(t)}(x) - E[\Theta_{\tau(t)}]), \tag{A5}$$

where $f^*(x) = 1$ is taken into account. For binary functions $b_1(x)$, $b_2(x)$ defined by (24), (25), we have [9]

$$\begin{cases} P_\tau\{b_1(x) - E[b_1]\} = P_\tau\{\Theta_{\frac{1}{8}}(x) - E[\Theta_{\frac{1}{8}}]\} - P_\tau\{\Theta_{\frac{1}{4}}(x) - E[\Theta_{\frac{1}{4}}]\} + P_\tau\{\Theta_{\frac{1}{2}}(x) - E[\Theta_{\frac{1}{2}}]\} \\ \qquad -P_\tau\{\Theta_{\frac{3}{4}}(x) - E[\Theta_{\frac{3}{4}}]\} + P_\tau\{\Theta_{\frac{7}{8}}(x) - E[\Theta_{\frac{7}{8}}]\}, \\ \qquad = \frac{1}{2}\{(\Theta_{\frac{1}{4}}(x) - E[\Theta_{\frac{1}{4}}]) - 2(\Theta_{\frac{1}{2}}(x) - E[\Theta_{\frac{1}{2}}]) + (\Theta_{\frac{3}{4}}(x) - E[\Theta_{\frac{3}{4}}])\}, \\ P_\tau^2\{b_1(x) - E[b_1]\} = \frac{1}{2}(\Theta_{\frac{1}{2}}(x) - E[\Theta_{\frac{1}{2}}]), \\ P_\tau^\ell\{b_1(x) - E[b_1]\} = 0 \quad (\ell \geq 3), \end{cases} \tag{A6}$$

$$\begin{cases} P_\tau\{b_2(x) - E[b_2]\} = P_\tau\{\Theta_{\frac{1}{4}}(x) - E[\Theta_{\frac{1}{4}}]\} - P_\tau\{\Theta_{\frac{3}{8}}(x) - E[\Theta_{\frac{3}{8}}]\} + P_\tau\{\Theta_{\frac{1}{2}}(x) - E[\Theta_{\frac{1}{2}}]\} \\ \qquad -P_\tau\{\Theta_{\frac{5}{8}}(x) - E[\Theta_{\frac{5}{8}}]\} + P_\tau\{\Theta_{\frac{3}{4}}(x) - E[\Theta_{\frac{3}{4}}]\}, \\ \qquad = \frac{1}{2}\{2(\Theta_{\frac{1}{2}}(x) - E[\Theta_{\frac{1}{2}}]) - (\Theta_{\frac{3}{4}}(x) - E[\Theta_{\frac{3}{4}}]) - (\Theta_{\frac{1}{4}}(x) - E[\Theta_{\frac{1}{4}}])\}, \\ P_\tau^2\{b_2(x) - E[b_2]\} = -\frac{1}{2}(\Theta_{\frac{1}{2}}(x) - E[\Theta_{\frac{1}{2}}]), \\ P_\tau^\ell\{b_2(x) - E[b_2]\} = 0 \quad (\ell \geq 3). \end{cases} \tag{A7}$$

Using (A6) and (A7), we can obtain

$$A(\ell; b_1) = \int_0^1 P_\tau^\ell\{(b_1(x) - E[b_1])\}(b_1(x) - E[b_1])dx = \begin{cases} \frac{1}{4} & (\ell = 0) \\ -\frac{1}{8} & (\ell = 1) \\ \frac{1}{16} & (\ell = 2) \\ 0 & (\ell \geq 3) \end{cases}, \tag{A8}$$

$$A(\ell; b_2) = \int_0^1 P_\tau^\ell\{(b_2(x) - E[b_2])\}(b_2(x) - E[b_2])dx = \begin{cases} \frac{1}{4} & (\ell = 0) \\ 0 & (\ell = 1) \\ -\frac{1}{16} & (\ell = 2) \\ 0 & (\ell \geq 3) \end{cases}, \tag{A9}$$

$$C(\ell; b_1, b_2) = \int_0^1 P_\tau^\ell\{(b_1(x) - E[b_1])\}(b_2(x) - E[b_2])dx = \begin{cases} 0 & (\ell = 0) \\ 0 & (\ell = 1) \\ \frac{1}{16} & (\ell = 2) \\ 0 & (\ell \geq 3) \end{cases}, \tag{A10}$$

$$C(\ell; b_2, b_1) = \int_0^1 P_\tau^\ell\{(b_2(x) - E[b_2])\}(b_1(x) - E[b_1])dx = \begin{cases} 0 & (\ell = 0) \\ \frac{1}{8} & (\ell = 1) \\ -\frac{1}{16} & (\ell = 2) \\ 0 & (\ell \geq 3) \end{cases}, \tag{A11}$$

which give the normalized auto-/cross-correlation functions given in Table 1.

Appendix A.2. Correlation Functions of Chaotic Binary Sequences Generated by PL Map Defined by (28)

For the PL map $\tau_{PL}(x)$ defined by (28) and the threshold function $\Theta_t(x)$ defined by (26), we have [13]

$$P_\tau\{\Theta_{\frac{3}{4}}(x) - E[\Theta_{\frac{3}{4}}]\} = -\frac{1}{3}(\Theta_{\frac{3}{4}}(x) - E[\Theta_{\frac{3}{4}}]), \tag{A12}$$

$$P_\tau\{\Theta_{\frac{1}{4}}(x) - E[\Theta_{\frac{1}{4}}]\} = 0, \tag{A13}$$

where $f^*(x) = 1$, $\tau_{PL}(\frac{3}{4}) = \frac{3}{4}$ (i.e., $x = \frac{3}{4}$ is a fixed point on the map), and $\tau_{PL}(\frac{1}{4}) = 0$ are taken into account. For binary functions $b_3(x)$, $b_4(x)$ defined by (29), (30), we immediately obtain, from (A12) and (A13),

$$P_\tau^\ell\{b_3(x) - E[b_3]\} = P_\tau^\ell\{\Theta_{\frac{3}{4}}(x) - E[\Theta_{\frac{3}{4}}]\} = \frac{1}{(-3)^\ell}(\Theta_{\frac{3}{4}}(x) - E[\Theta_{\frac{3}{4}}]), \tag{A14}$$

$$P_\tau^\ell\{b_4(x) - E[b_4]\} = P_\tau^\ell\{1 - \Theta_{\frac{1}{4}}(x) - (1 - E[\Theta_{\frac{1}{4}}])\} = 0 \quad (\ell \geq 1). \tag{A15}$$

Using (A14) and (A15), we can obtain

$$A(\ell; b_3) = \int_0^1 P_\tau^\ell\{(b_3(x) - E[b_3])\}(b_3(x) - E[b_3])dx = \frac{3}{16}(-3)^{-\ell}, \tag{A16}$$

$$A(\ell; b_4) = \int_0^1 P_\tau^\ell\{(b_4(x) - E[b_4])\}(b_4(x) - E[b_4])dx = \begin{cases} \frac{3}{16} & (\ell = 0) \\ 0 & (\ell \geq 1) \end{cases}, \tag{A17}$$

$$C(\ell; b_3, b_4) = \int_0^1 P_\tau^\ell\{(b_3(x) - E[b_3])\}(b_4(x) - E[b_4])dx = -\frac{1}{16}(-3)^{-\ell}, \tag{A18}$$

$$C(\ell; b_4, b_3) = \int_0^1 P_\tau^\ell\{(b_4(x) - E[b_3])\}(b_3(x) - E[b_3])dx = \begin{cases} -\frac{1}{16} & (\ell = 0) \\ 0 & (\ell \geq 1) \end{cases}, \tag{A19}$$

which give the normalized auto-/cross-correlation functions given in Table 2.

Appendix A.3. Correlation Functions of Chaotic Binary Sequences Generated by Tent Map

For the tent map $\tau_T(x)$ defined by (32) and the threshold function $\Theta_t(x)$ defined by (26), we have [9]

$$P_\tau\{\Theta_t(x) - E[\Theta_t]\} = \begin{cases} \frac{1}{2}(\Theta_{\tau(t)}(x) - E[\Theta_{\tau(t)}]) & (0 < t < \frac{1}{2}) \\ -\frac{1}{2}(\Theta_{\tau(t)}(x) - E[\Theta_{\tau(t)}]) & (\frac{1}{2} \leq t < 1) \end{cases}, \tag{A20}$$

where $f^*(x) = 1$ is taken into account. For binary functions $b_5(x)$, $b_6(x, d)$ defined by (33), (34), we have

$$P_\tau\{b_5(x) - E[b_5]\} = 0, \tag{A21}$$

$$P_\tau\{b_6(x, d) - E[b_6]\} = 0, \tag{A22}$$

where $\tau_T(d) = \tau_T(1 - d)$ is used. That is, $b_5(x)$ and $b_6(x, d)$ for the tent map satisfy the sufficient condition for the generation of *i.i.d.* binary sequences [9]. Using (A21) and (A22), the auto-correlation functions are given by

$$A(\ell; b_5) = \begin{cases} \frac{1}{4} & (\ell = 0) \\ 0 & (\ell \geq 1) \end{cases}, \tag{A23}$$

$$A(\ell; b_6) = \begin{cases} \frac{1}{4} & (\ell = 0) \\ 0 & (\ell \geq 1) \end{cases}, \quad (0 < d \leq \frac{1}{2}). \tag{A24}$$

From (A21) and (A22), it is obvious that

$$C(\ell; b_5, b_6) = C(\ell; b_6, b_5) = 0 \quad (\ell \geq 1). \tag{A25}$$

Additionally, we have

$$C(0; b_5, b_6) = C(0; b_6, b_5) = d - \frac{1}{4}. \tag{A26}$$

Thus, the normalized auto-/cross-correlation functions given in Table 3 have been derived.

References

1. Lasota, A.; Mackey, M.C. *Chaos, Fractals, and Noise*; Springer: New York, NY, USA, 1994.
2. Boyarsky, A.; Góra, P. *Laws of Chaos*; Birkhäuser Boston: Boston, MA, USA, 1997.
3. Gerosa, A.; Bernardini, R.; Pietri, S. A fully integrated chaotic system for the generation of truly random numbers. *IEEE Trans. Circuits Syst. I* **2001**, *49*, 993–1000. [CrossRef]
4. Stojanovski, T.; Kocarev, L. Chaos-based random number generators—Part I: Analysis. *IEEE Trans. Circuits Syst. I* **2001**, *48*, 281–288. [CrossRef]
5. Cicek, I.; Pusane, A.E.; Dundar, G. A novel design method for discrete time chaos based true random number generators. *Integr. VLSI J.* **2014**, *47*, 38–47. [CrossRef]
6. Li, C.; Feng, B.; Li, S.; Kurths, J.; Chen, G. Dynamic analysis of digital chaotic maps via state-mapping networks. *IEEE Trans. Circuits Syst. I* **2019**, *66*, 2322–2335. [CrossRef]
7. Kennedy, M.P.; Rovatti, R.; Setti, G. (Eds.) *Chaotic Electronics in Telecommunications*; CRC: Boca Raton, FL, USA, 2000.
8. Liu, Z.; Tang, J.; Yu, J. An application of chaos: Generating binary pseudo-random sequences. In Proceedings of the 1988 IEEE International Symposium on Circuits and Systems, Espoo, Finland, 7–9 June 1988; pp. 1–3.
9. Kohda, T.; Tsuneda, A. Statistics of chaotic binary sequences. *IEEE Trans. Inf. Theory* **1997**, *43*, 104–112. [CrossRef]
10. Sakai, H.; Tokumaru, H. Autocorrelations of a certain chaos. *IEEE Trans. Acoust. Speech Signal Process* **1980**, *28*, 588–590. [CrossRef]
11. Rovatti, R.; Mazzini, G. Interference in DS-CDMA systems with exponentially vanishing autocorrelations: Chaos-based spreading is optimal. *Electron. Lett.* **1998**, *34*, 1911–1913. [CrossRef]
12. Mazzini, G.; Rovatti, R.; Setti, G. Interference minimization by autocorrelation shaping in asynchronous DS-CDMA systems: Chaos-based spreading is nearly optimal. *Electron. Lett.* **1999**, *35*, 1054–1055. [CrossRef]
13. Tsuneda, A. Design of binary sequences with tunable exponential autocorrelations and run statistics based on one-dimensional chaotic maps. *IEEE Trans. Circuits Syst. I* **2005**, *52*, 454–462. [CrossRef]
14. Yang, C.A.; Yao, K.; Umeno, K.; Biglieri, E. Using deterministic chaos for superefficient Monte-Carlo simulations. *IEEE Circuits Syst. Mag.* **2013**, *13*, 26–35. [CrossRef]
15. Souza, C.E.C.; Chaves, D.P.B.; Pimentel, C. One-dimensional pseudo-chaotic sequences based on the discrete Arnold's cat map over $\mathbb{Z}_{3^m}$. *IEEE Trans. Circuits Syst. II* **2021**, *68*, 491–495.
16. Paul, P.S.; Sadia, M.; Hossain, M.R.; Muldrey, B.; Hasan, M.S. Cascading CMOS-based chaotic maps for improved performance and its application in efficient RNG design. *IEEE Access* **2022**, *10*, 33758–33770. [CrossRef]
17. Tang, J.; Zhang, Z.; Chen, P.; Huang, Z.; Huang, T. A simple chaotic model with complex chaotic behaviors and its hardware implementation. *IEEE Trans. Circuits Syst. I* **2023**, *70*, 3676–3688. [CrossRef]
18. Tsuneda, A. Various Auto-correlation functions of m-bit random numbers generated from chaotic binary sequences. *Entropy* **2021** *23*, 1295. [CrossRef]