数理解析研究所講究録 1240 巻 2001 年 192-203

A Simple Design of Chaotic Binary Sequences with Prescribed Auto-Correlation Properties Based on Piecewise Linear Onto Maps

Akio TSUNEDA

Department of Electrical and Computer Engineering,
Kumamoto University, Japan
2–39–1 Kurokami, Kumamoto 860-8555, Japan
Tel: +81-96-342-3853, Fax: +81-96-342-3630
E-mail : tsuneda@eecs.kumamoto-u.ac.jp

Abstract: This paper describes simple design methods of chaotic binary sequences with prescribed auto-correlation properties including higher-order statistics. We employ one-dimensional piecewise linear onto maps and simple threshold functions for generating such sequences. Some examples of such designs are also given. Furthermore, bounds on such statistics are discussed and compared to the result for general binary random variables.

1 Introduction

Simple deterministic systems can exhibit very complex and random behavior called *chaos*. Such phenomena are very interesting in both of theoretical and engineering point of view. One of the most useful applications of chaos is a random number generator which is required in several engineering applications such as Monte Carlo simulations, spread spectrum communications, and cryptosystems. In many kinds of pseudorandom numbers, binary sequences are most useful in such digital communication systems. The best known class of binary sequences is the so-called linear feedback shift register (LFSR) sequences such as M-sequences, Gold sequences, and Kasami sequences [1].

As quite different methods from LFSR sequences, there have been several attempts to use chaotic sequences which are generated by one-dimensional nonlinear maps. Though a chaotic sequence itself is real-valued, it can be easily transformed into binary sequences by appropriate threshold functions. In applications of such chaotic sequences, theoretical evaluation and design of statistical properties of such sequences are very important because there are many kinds of chaotic sequences with various properties which depend on their deterministic systems.

Design of many chaotic sequences of *i.i.d.* (independent and identically distributed) binary random variables from a single chaotic real-valued sequence generated by a class of one-dimensional maps has been established [2]. A generalized version of such design has also been given [3]. Sequences of i.i.d. binary random variables are very useful as random numbers. However, non-i.i.d. sequences, which have some correlations dependent on the chaotic maps and quantization functions, are also useful in some applications. Actually, it has been shown that sequences with exponentially vanishing auto-correlations have better performance in asynchronous DS/CDMA systems than i.i.d. sequences [4],[5]. Thus, it is very important to design chaotic sequences with prescribed statistical properties.

Design of chaotic real-valued orbits with prescribed statistical properties have been discussed in [6]. Also, design of dynamical systems which generates an arbitrarily prescribed tree source by using piecewise linear maps has been given [7]. We also remark that Kalman already gave a procedure for embedding a Markov chain into chaotic dynamics of piecewise linear maps [8],[9].

In this paper, we present simple design methods to obtain chaotic binary sequences with prescribed auto-correlation properties, including higher-order statistics, based on piecewise linear *onto* maps with a uniform invariant measure [10]–[12]. We also use a simple threshold function for generating chaotic binary sequences from a real-valued one.

2 One-Dimensional Maps and Chaotic Binary Sequences

One-dimensional nonlinear difference equation

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

can produce a *chaotic* sequence $\{x_n\}_{n=0}^{\infty}$, where $x_n = \tau^n(x_0)$. The ensemble-average defined by

$$\langle G \rangle = \int_I G(x) f^*(x) dx \tag{2}$$

is very useful in evaluating statistics of $\{G(\tau^n(x))\}_{n=0}^{\infty}$ under the assumption that $\tau(\cdot)$ is mixing on I with respect to an absolutely continuous invariant measure, denoted by $f^*(x)dx$. In this paper, we employ piecewise monotonic onto maps with N_τ subintervals.

We now define the Perron-Frobenius (PF) operator P_τ of the map τ with an interval $I = [d, e]$ by

$$P_\tau G(x) = \frac{d}{dx} \int_{\tau^{-1}([d,x])} G(y) dy \tag{3}$$

which can be rewritten as

$$P_\tau G(x) = \sum_{i=1}^{N_\tau} |g_i'(x)| G(g_i(x)) \tag{4}$$

for piecewise monotonic onto maps, where $g_i(x)$ is the i-th preimage of the map $\tau(\cdot)$ [13]. This operator is very useful in evaluating the correlation functions because it has the following important property:

$$\int_I G(x) P_\tau\{H(x)\} dx = \int_I G(\tau(x)) H(x) dx. \tag{5}$$

A real-valued chaotic sequence generated by such a map is easily transformed into a binary sequence by a threshold function defined by

$$\Theta_t(x) = \begin{cases} 0 & (x < t) \\ 1 & (x \geq t). \end{cases} \tag{6}$$

We will discuss statistical properties of a binary sequence $\{\Theta_t(\tau^n(x))\}_{n=0}^{\infty}$ generated by the threshold function.

3 Chaotic Binary Sequences with Prescribed Auto-Correlation Properties

3.1 2nd-Order Auto-Correlation

Firstly, we define the 2nd-order auto-correlation function of a sequence $\{G(\tau^n(x))\}_{n=0}^{\infty}$ by

$$\rho(\ell; G) = \int_I (G(x) - \langle G \rangle)(G(\tau^\ell(x)) - \langle G \rangle) f^*(x) dx. \tag{7}$$

For an i.i.d. binary sequence $\{B(\tau^n(x))\}_{n=0}^{\infty}$ as given in [2], we have

$$\rho(\ell; B) = (\langle B \rangle - \langle B \rangle^2)\delta(\ell), \tag{8}$$

where $\delta(0) = 1$ and $\delta(\ell) = 0$ for $\ell > 1$.

Now, we consider piecewise linear (PL) *onto* maps whose mapping function $\tau_i(\cdot)$ in each subinterval I_i $(i = 1, 2, \cdots, N_\tau)$ is given by

$$\tau_i(x) = a_i x + b_i, \quad |a_i| > 1, \quad \tau_i : I_i \to I \text{ (onto)}. \tag{9}$$

Without any loss of generality, we assume $I = [0, 1]$. For such maps, the invariant density function $f^*(x)$ is constant such that $\int_I f^*(x)dx = 1$, that is, $f^*(x) = 1$. We call eq.(9) the *onto condition* through this paper. Thus, we can obtain the following lemma.
Lemma 1: For the piecewise linear onto maps given by (9), we can get

$$P_\tau\{(\Theta_t(x) - \langle \Theta_t \rangle) f^*(x)\} = \frac{1}{a_r}(\Theta_{\tau(t)}(x) - \langle \Theta_{\tau(t)} \rangle) f^*(x) \tag{10}$$

where $t \in I_r$.

By using the above lemma, we can obtain the following theorem.
Theorem 1: Let c be a fixed point of the map satisfying $\tau(c) = c$. If we employ the threshold c $(\in I_r)$, we have

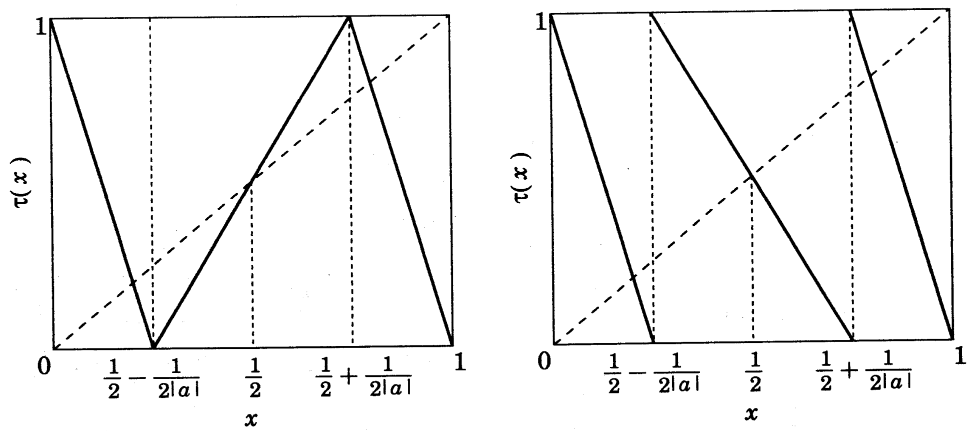
$$\rho(\ell; \Theta_c) = \frac{\rho(0; \Theta_c)}{a_r^\ell} = \frac{\langle \Theta_c \rangle - \langle \Theta_c \rangle^2}{a_r^\ell}. \tag{11}$$

It should be noted that eq.(11) is independent of the mapping functions $\tau_i(\cdot)$ $(i \neq r)$. Thus, we can control the auto-correlation property of the chaotic binary sequence by c and a_r, where we can use arbitrary values of a_r whose absolute value is greater than 1.
Example 1: Define a piecewise linear onto map with $I = [0, 1]$ by

$$\tau(x) = \begin{cases} \dfrac{2|a|}{1-|a|}x + 1 & (0 \le x < \frac{1}{2} - \frac{1}{2|a|}) \\ ax - \dfrac{a-1}{2} & (\frac{1}{2} - \frac{1}{2|a|} \le x < \frac{1}{2} + \frac{1}{2|a|}) \\ \dfrac{2|a|}{1-|a|}(x-1) & (\frac{1}{2} + \frac{1}{2|a|} \le x \le 1) \end{cases}, \quad |a| > 1. \tag{12}$$

Examples of the above map are shown in Fig.1. According to Theorem 2, the auto-correlation function of a binary sequence $\{\Theta_{\frac{1}{2}}(\tau^n(x))\}_{n=0}^{\infty}$ obtained by the PL onto map of eq.(12) is given by

$$\rho(\ell; \Theta_{\frac{1}{2}}) = \frac{1}{4a^\ell}. \tag{13}$$



(a) $a > 0$ (b) $a < 0$

Figure 1: Examples of the PL onto map of eq.(12)

Figure 2 shows examples of theoretical and empirical correlation values of $\{\Theta_{\frac{1}{2}}(\tau^n(x))\}_{n=0}^{\infty}$ generated by PL onto maps of eq.(12), where empirical values are obtained by a computer. We can find that the theoretical and empirical values are in good agreement with each other.

3.2 Run-Probability

When $B(\cdot)$ is a binary ($\{0,1\}$-valued) function, the probability of m successive 1's in the binary sequence $\{B(\tau^n(x))\}_{n=0}^{\infty}$ is given by

$$P_m(B) = \int_I B(x)B(\tau(x))\cdots B(\tau^{m-1}(x))f^*(x)dx, \tag{14}$$

which is one of higher-order statistics and is also useful for some statistical tests [14]. We call this probability *run-probability.* Of course, if the sequence is i.i.d., we have $P_m(B) = \langle B\rangle^m$.

Here, again, consider the piecewise linear onto maps given by (9). We give the following theorem.

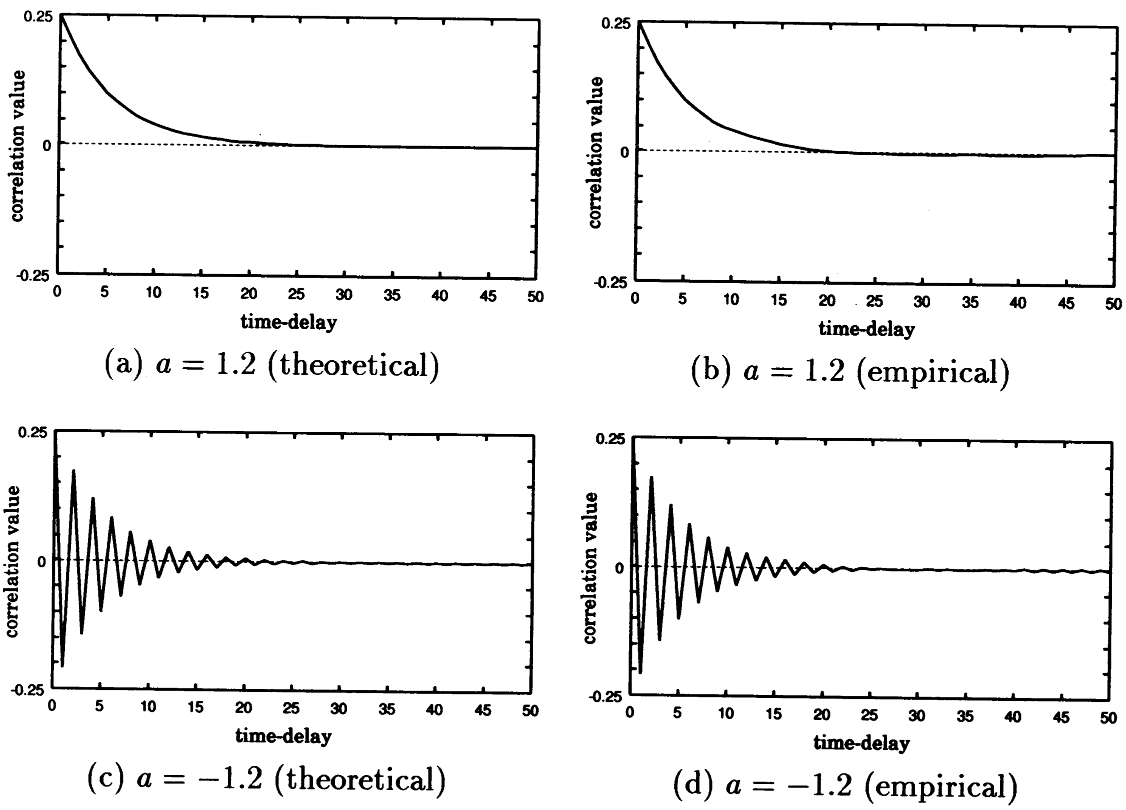
Theorem 3: Let t be a value such that $t < \tau(t), t < \tau^2(t), \cdots, t < \tau^{p-1}(t)$ and $t \geq \tau^p(t)$. Then, for the piecewise linear onto maps given by (9), we have

$$P_m(\Theta_t) = \left(\prod_{i=0}^{p-1}\frac{1}{a^{(i)}}\right) P_{m-p}(\Theta_t) + \sum_{j=1}^{p}\left(\prod_{i=0}^{j-2}\frac{1}{a^{(i)}}\right)\left(\langle\Theta_{\tau^{j-1}(t)}\rangle - \frac{\langle\Theta_{\tau^j(t)}\rangle}{a^{(j-1)}}\right) P_{m-j}(\Theta_t) \tag{15}$$

where $a^{(i)}$ is the slope of the mapping function of the subinterval in which $\tau^i(t)$ exists.

Proof: Using eq.(10), we can write

$$\begin{aligned} P_m(\Theta_t) &= \int_I P_\tau\{\Theta_t(x)f^*(x)\}\Theta_t(x)\cdots\Theta_t(\tau^{m-2}(x))dx \\ &= \int_I \left\{\frac{1}{a^{(0)}}(\Theta_{\tau(t)}(x) - \langle\Theta_{\tau(t)}\rangle)f^*(x)\right\}\Theta_t(x)\cdots\Theta_t(\tau^{m-2}(x))dx \end{aligned}$$



(a) $a = 1.2$ (theoretical)

(b) $a = 1.2$ (empirical)

(c) $a = -1.2$ (theoretical)

(d) $a = -1.2$ (empirical)

Figure 2: Auto-correlation functions of $\{\Theta_{\frac{1}{2}}(\tau^n(x))\}_{n=0}^{\infty}$ generated by PL onto maps with $a = \pm 1.2$.

$$
\begin{aligned}
&= \frac{1}{a^{(0)}} \int_I \Theta_{\tau(t)}(x)\Theta_t(\tau(x)) \cdots \Theta_t(\tau^{m-2}(x)) f^*(x)dx \\
&+ \left(\langle \Theta_t \rangle - \frac{\langle \Theta_{\tau(t)} \rangle}{a^{(0)}} \right) P_{m-1}(\Theta_t) \qquad (16)
\end{aligned}
$$

and thus by induction we have eq.(15).

Remark: For maps with the EDP, $P_m(\Theta_t)$ as in Theorem 3 is obtained by substituting $a^{(i)} = s((\tau^i)'(t))N_\tau$ into eq.(15).

From Theorem 3, we find that the run-probability of 1's in the sequence is also controllable to some extent. Note that eq.(15) is independent of slopes of the mapping functions of the subintervals in which $\tau^i(t)$ does not exist. We give simple design examples based on piecewise linear onto maps as follows.

Example 2: For $t \geq \tau(t)$ and $t \in I_r$, we have

$$
\begin{aligned}
P_m(\Theta_t) &= \left(\frac{1 - \langle \Theta_{\tau(t)} \rangle}{a_r} + \langle \Theta_t \rangle \right) P_{m-1}(\Theta_t) \qquad (17) \\
&= \left(\frac{1 - \langle \Theta_{\tau(t)} \rangle}{a_r} + \langle \Theta_t \rangle \right)^{m-1} \cdot \langle \Theta_t \rangle \qquad (18)
\end{aligned}
$$

Let us design a map with $I = [0, 1]$ such that $P_1(\Theta_t) = \langle \Theta_t \rangle = \frac{1}{2}$ and $P_2(\Theta_t) = \frac{2}{5}$. Firstly,

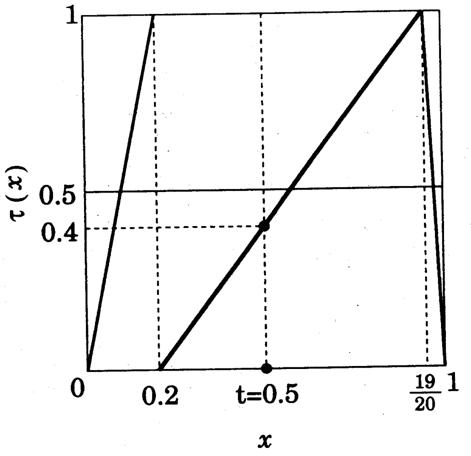


Figure 3: An example of PL onto maps satisfying $P_1(\Theta_t) = \frac{1}{2}$ and $P_2(\Theta_t) = \frac{2}{5}$.

we set $t = \frac{1}{2}$ in order to realize $\langle \Theta_t \rangle = \frac{1}{2}$. Substituting $\langle \Theta_t \rangle = \frac{1}{2}$ into eq.(18), we have

$$P_2(\Theta_{\frac{1}{2}}) = \left(\frac{1 - \langle \Theta_{\tau(t)} \rangle}{a_r} + \frac{1}{2} \right) \cdot \frac{1}{2} = \frac{2}{5} \tag{19}$$

which leads us to get $a_r = \frac{10}{3}(1 - \langle \Theta_{\tau(t)} \rangle)$. If we set $\tau(\frac{1}{2}) = \frac{2}{5}$ in order to satisfy $\frac{1}{2} \geq \tau(\frac{1}{2})$, we have $a_r = \frac{4}{3}$. Hence, we can obtain the mapping function in the subinterval I_r as

$$\tau_r(x) = \frac{4}{3}x - \frac{4}{15} \tag{20}$$

which satisfies $\tau(\frac{1}{2}) = \frac{2}{5}$. We can arbitrarily give mapping functions in other subintervals, $\tau_i(\cdot)$ $(i \neq r)$, satisfying eq.(9). An example of such maps is shown in Figure 3.

Example 3: For $t < \tau(t)$, $t \geq \tau^2(t)$, $t \in I_r$, and $\tau(t) \in I_s$, we have

$$\begin{aligned} P_m(\Theta_t) &= \left(\langle \Theta_t \rangle - \frac{\langle \Theta_{\tau(t)} \rangle}{a_r} \right) P_{m-1}(\Theta_t) + \frac{1 - \langle \Theta_{\tau^2(t)} \rangle + a_s \langle \Theta_{\tau(t)} \rangle}{a_r a_s} P_{m-2}(\Theta_t) && (21) \\ P_1(\Theta_t) &= \langle \Theta_t \rangle && (22) \\ P_2(\Theta_t) &= \frac{\langle \Theta_{\tau(t)} \rangle}{a_r}(1 - \langle \Theta_t \rangle) + \langle \Theta_t \rangle^2 && (23) \end{aligned}$$

Let us design a map with $I = [0,1]$ such that $P_1(\Theta_t) = \langle \Theta_t \rangle = \frac{1}{2}$, $P_2(\Theta_t) = \frac{1}{6}$, and $P_3(\Theta_t) = \frac{1}{12}$. Firstly, we set $t = \frac{1}{2}$ in order to realize $\langle \Theta_t \rangle = \frac{1}{2}$. Substituting $\langle \Theta_t \rangle = \frac{1}{2}$ into eq.(23), we have

$$P_2(\Theta_{\frac{1}{2}}) = \frac{\langle \Theta_{\tau(t)} \rangle}{2a_r} + \frac{1}{4} = \frac{1}{6} \tag{24}$$

which leads us to get

$$a_r = -6\langle \Theta_{\tau(t)} \rangle. \tag{25}$$

Here we assume $\tau(\frac{1}{2}) \in I_r$, that is, $a_r = a_s$. Thus, from eq.(21), we can get

$$P_3(\Theta_{\frac{1}{2}}) = \left(\frac{1}{2} + \frac{1}{6} \right) \cdot \frac{1}{6} + \frac{1 - \langle \Theta_{\tau^2(\frac{1}{2})} \rangle + a_r \langle \Theta_{\tau(\frac{1}{2})} \rangle}{a_r^2} \cdot \frac{1}{2} = \frac{1}{12}. \tag{26}$$

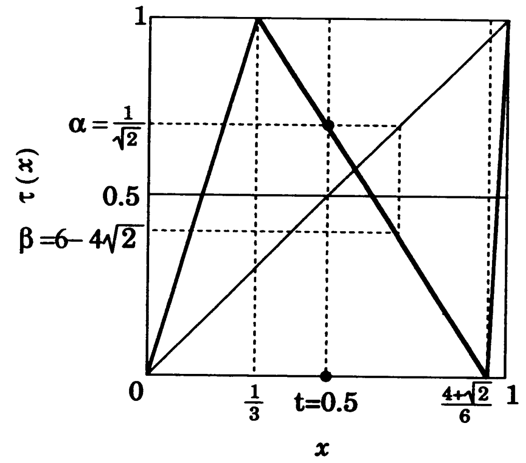


Figure 4: An example of PL onto maps satisfying $P_1(\Theta_t) = \langle\Theta_t\rangle = \frac{1}{2}$, $P_2(\Theta_t) = \frac{1}{6}$, and $P_3(\Theta_t) = \frac{1}{12}$.

Put $\alpha = \tau(\frac{1}{2})$ and $\beta = \tau^2(\frac{1}{2})$. Then we have

$$\begin{aligned} \langle\Theta_{\tau(\frac{1}{2})}\rangle &= 1-\alpha && (27)\\ \langle\Theta_{\tau^2(\frac{1}{2})}\rangle &= 1-\beta && (28)\\ \tau_r(x) &= a_r\left(x-\frac{1}{2}\right)+\alpha && (29)\\ \tau_r(\alpha) &= \beta. && (30) \end{aligned}$$

Using eq.(25)–(30), we can get each value of the parameters and obtain the mapping function in the subinterval I_r as

$$\tau_r(x) = 3(\sqrt{2}-2)x + 3 - \sqrt{2}. \tag{31}$$

We can also arbitrarily give mapping functions in other subintervals, $\tau_i(\cdot)$ $(i \neq r)$, satisfying eq.(9). An example of such maps is shown in Figure 4.

4 Discussion of Run-Probability

Now consider the simplest case $p = 1$ in eq.(15), that is, the case of eq.(18). Further, we focus our attention on the case $m = 2$. Using $\langle\Theta_t\rangle = 1 - t$, we have

$$P_2(\Theta_t) = \left(\frac{\tau(t)}{a_r} + 1 - t\right)(1-t). \tag{32}$$

We consider bounds on the run-probability $P_2(\Theta_t)$ given by eq.(32). There are three parameters $t$, $\tau(t)$, and a_r which determine the value of $P_2(\Theta_t)$. However, these parameters are not completely independent each other since the onto condition eq.(9) and $t \geq \tau(t)$ must be satisfied as long as eq.(32) is used. Hence, eq.(32) should have some bounds which are of our main interest in this section. Thus, we theoretically investigate such bounds for a given $P_1(\Theta_t) = \langle\Theta_t\rangle$ (*i.e.*, a given $t$).

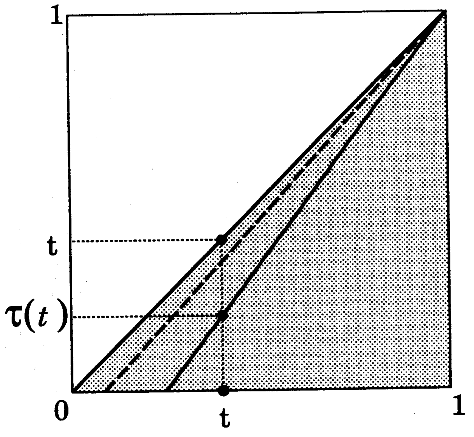


Figure 5: Case 1 ($a_r > 0$)

To do this, we consider the following cases. Note that each case corresponds to each of Figures 5–8. In these figures, the coordinate $(t, \tau(t))$, which is one of parameters determining the mapping function, must be located in shaded area in order to satisfy the given conditions.

- **Case 1:** $a_r > 0$ (Fig.5)

In this case, obviously, the minimum value of $P_2(\Theta)$ is $(1-t)^2$ to be obtained for $\tau(t) = 0$, where the sequence is i.i.d. On the other hand, consider the upper bound on $P_2(\Theta)$ which is obtained for the most correlated sequence while keeping the onto condition. As shown in Fig.5, the mapping function $\tau_r(x)$ is a linear one with $\tau_r(t) = \tau(t)$ and $\tau_r(1) = 1$, whose slope a_r is given by

$$a_r = \frac{1-\tau(t)}{1-t}. \tag{33}$$

Thus, the upper bound is $1-t$ to be obtained for $\tau(t) = t$. Note that when $\tau(t) = 1$, that is, $a_r = 1$, the map is no longer chaotic. Thus, in this case, we have

$$P_1(\Theta_t)^2 \le P_2(\Theta_t) < P_1(\Theta_t). \tag{34}$$

- **Case 2-1:** $a_r < 0$, $t \ge \frac{1}{2}$, and $\tau(t) > 1-t$ (Fig.6)

In this case, the upper bound on $P_2(\Theta)$ is $(1-t)^2$ to be obtained for $a_r \to \infty$. Next, consider the most correlated case. As shown in Fig.6, the mapping function $\tau_r(x)$ is a linear one with $\tau_r(t) = \tau(t)$ and $\tau_r(1) = 0$ for the most correlated case where the absolute value of the slope of $\tau_r(x)$, $|a_r|$, is closest to 1 while keeping the onto condition. In this case, we have

$$a_r = -\frac{\tau(t)}{1-t}. \tag{35}$$

Substituting eq.(35) into eq.(32), we can get $P_2(\Theta_t) = 0$ which is independent of $\tau(t)$ and is the minimum value in this case. Hence we have

$$0 \le P_2(\Theta_t) < P_1(\Theta_t)^2. \tag{36}$$

- **Case 2-2:** $a < 0$, $t \ge \frac{1}{2}$, and $\tau(t) \le 1-t$ (Fig.7)

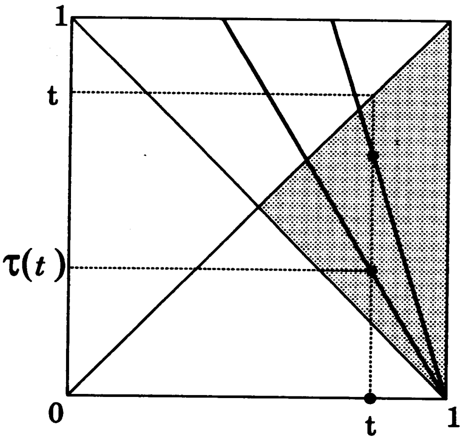


Figure 6: Case 2-1 ($a_r < 0$, $t \geq \frac{1}{2}$, and $\tau(t) > 1 - t$)

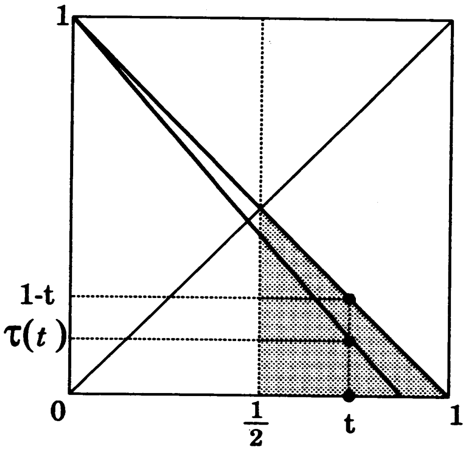


Figure 7: Case 2-2 ($a_r < 0$, $t \geq \frac{1}{2}$, and $\tau(t) \leq 1 - t$)

In this case, the maximum value of $P_2(\Theta)$ is also $(1-t)^2$ to be obtained for $\tau(t) = 0$. Similarly to Case 2-1, consider the most correlated case. As shown in Fig.7, the mapping function $\tau_r(x)$ is a linear one with $\tau_r(t) = \tau(t)$ and $\tau_r(0) = 1$ for the most correlated case while keeping the onto condition. The slope a_r is given by

$$a_r = -\frac{1-\tau(t)}{t}. \tag{37}$$

In this case, obviously, the lower bound on $P_2(\Theta_t)$ is 0 to be obtained for $\tau(t) = 1 - t$. Note that when $\tau(t) = 1 - t$, that is, $a_r = -1$, the map is no longer chaotic. Therefore, we have

$$0 < P_2(\Theta_t) \leq P_2(\Theta_t)^2. \tag{38}$$

- **Case 2-3:** $a < 0$, $t < \frac{1}{2}$ (Fig.8)

In this case, the maximum value of $P_2(\Theta)$ is also $(1-t)^2$ to be obtained for $\tau(t) = 0$. Similarly to Case 2-2, consider the most correlated case. As shown in Fig.8, the mapping function $\tau_r(x)$ is a linear one with $\tau_r(t) = \tau(t)$ and $\tau_r(0) = 1$ for the most correlated case

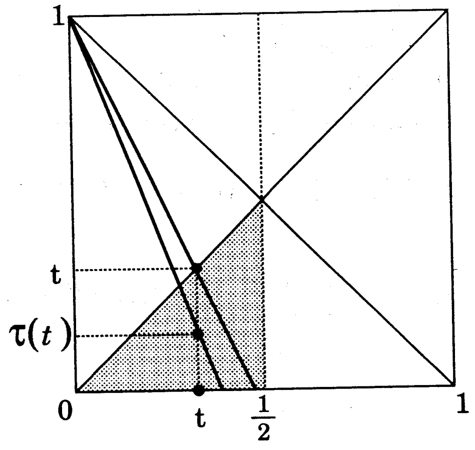


Figure 8: Case 2-3 ($a_r < 0$ and $t < \frac{1}{2}$)

while keeping the onto condition. In this case, the minimum value of $P_2(\Theta_t)$ is obtained for $\tau(t) = t$. For such a case, we have

$$a_r = -\frac{1-t}{t}. \tag{39}$$

Substituting eq.(39) and $\tau(t) = t$ into eq.(32), we can get $P_2(\Theta_t) = 1 - 2t$. Hence, we have

$$2P_1(\Theta_t) - 1 \leq P_2(\Theta_t) \leq P_2(\Theta_t)^2. \tag{40}$$

From the above four cases, the bounds on $P_2(\Theta_t)$ can be written as

$$\left.\begin{array}{rl} 0 \leq P_2(\Theta_t) < P_1(\Theta_t) & \text{for } P_1(\Theta_t) \leq \dfrac{1}{2} \\ 2P_1(\Theta_t) - 1 \leq P_2(\Theta_t) < P_1(\Theta_t) & \text{for } P_1(\Theta_t) > \dfrac{1}{2} \end{array}\right\} \tag{41}$$

which corresponds to the result for arbitrary binary random variables (see Appendix) [11].

5 Conclusion

We have given simple design methods of chaotic binary sequences with prescribed auto-correlation properties including higher-order statistics. Using a class of piecewise linear onto maps, we can control the auto-correlation property with exponential decay and the run-probability of 1's in a chaotic binary sequence. Furthermore, bounds on such a run-probability have also been discussed.

Appendix

Bounds on Run-Probability of Length 2 for General Binary Random Variables

Let $X$ and Y be binary random variables taking 0 or 1. We denote events $X = 1$, $X = 0$, $Y = 1$, and $Y = 0$ by $A$, $\overline{A}$, $B$, and $\overline{B}$, respectively. Moreover, probabilities with respect to these events are denoted by

$$\begin{aligned} P(A): &\ \text{probability of } A \\ P(A,B): &\ \text{probability of } A \text{ and } B \\ P(B|A): &\ \text{conditional probability of } B \text{ assuming } A. \end{aligned}$$

Let us assume $P(A) = P(B)$. Then, we have $P(A|B) = P(B|A)$ which is easily obtained from the formula

$$P(B|A) = \frac{P(A,B)}{P(A)} = \frac{P(B)P(A|B)}{P(A)}. \tag{A1}$$

Furthermore, by using $P(B|A) + P(\overline{B}|A) = 1$, we have

$$P(\overline{B}|A) = P(A|\overline{B}) = P(\overline{A}|B) = P(B|\overline{A}) \tag{A2}$$

which gives $P(A,\overline{B}) = P(\overline{A},B)$ because

$$P(A,\overline{B}) = P(\overline{B}|A)P(A) \tag{A3}$$

$$P(\overline{A},B) = P(\overline{A}|B)P(B). \tag{A4}$$

Now consider bounds on $P(A,B)$ under the assumption that $P(A) = P(B)$. We also assume that $P(B|A) = \delta$, where $0 \leq \delta < 1$. Thus, we have

$$P(A,B) = P(B|A)P(A) = \delta P(A) \tag{A5}$$

$$\begin{aligned} P(A,\overline{B}) &= P(\overline{A},B) = P(\overline{B}|A)P(A) \\ &= (1-\delta)P(A) \end{aligned} \tag{A6}$$

$$\begin{aligned} P(\overline{A},\overline{B}) &= 1 - (P(A,B) + P(A,\overline{B}) + P(\overline{A},B)) \\ &= 1 + \delta P(A) - 2P(A). \end{aligned} \tag{A7}$$

Since $0 \leq P(\overline{A},\overline{B}) \leq 1$, we have

$$\frac{2P(A)-1}{P(A)} \leq \delta < 1 \tag{A8}$$

which, in conjunction with (A5), gives

$$2P(A) - 1 \leq P(A,B) < 1. \tag{A9}$$

However, the probability $P(A,B)$ must satisfy $0 \leq P(A,B) \leq 1$. Therefore, we have

$$\left.\begin{aligned} 0 \leq P(A,B) < P(A) &\quad \text{for } P(A) \leq \frac{1}{2} \\ 2P(A) - 1 \leq P(A,B) < P(A) &\quad \text{for } P(A) > \frac{1}{2}. \end{aligned}\right\} \tag{A10}$$

If we set $X = \Theta_t(x_n)$ and $Y = \Theta_t(x_{n+1})$, then $P(A,B)$ implies $P_2(\Theta_t)$ and the two bounds (41) and (A10) correspond to each other. This means that chaotic binary sequences generated by a piecewise linear onto map and a threshold function can mimic arbitrary binary random variables with respect to run-probability of length 2.

References

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

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

[3] T. Sang, R. Wang, and Y. Yan, "Constructing Chaotic Discrete Sequences for Digital Communications Based on Correlation Analysis," *IEEE Trans., Signal Processing*, vol.48, no.9, pp.2557–2565, 2000.

[4] R. Rovatti and G. Mazzini, "Interference in DS-CDMA Systems with Exponentially Vanishing Autocorrelations: Chaos-Based Spreading Is Optimal," *Electronics Letters*, Vol.34, No.20, pp.1911–1913, 1998.

[5] T. Kohda and H. Fujisaki, "Variances of Multiple Access Interference Code Average against Data Average," *Electronics Letters*, Vol.36, No.20, pp.1717–1719, 2000.

[6] A. Baranovsky and D. Daems, "Design of One-Dimensional Chaotic Maps with Prescribed Statistical Properties", *Int. J. Bifurcation and Chaos*, vol.5, no.6, pp.1585–1598, 1995.

[7] Y. Oohama, M. Suemitsu and T. Kohda, "Construction of a Nonlinear Map Generating an Arbitrarily Prescribed Tree Sources", *Proc. of 1998 International Symposium on Nonlinear Theory and its Applications*, vol.2, pp.615–618, 1998.

[8] R. E. Kalman, "Nonlinear Aspects of Sampled-Data Control Systems," *Proc. Symp. Nonlinear Circuit Analysis VI*, pp.273–313, 1956.

[9] T. Kohda and H. Fujisaki, "Kalman's Recognition of Chaotic Dynamics in Designing Markov Information Sources," *IEICE Trans. Fundamentals*, Vol.E82-A, No.9, pp.1747–1753, 1999.

[10] A. Tsuneda, "Design of Chaotic Binary Sequences with Prescribed Auto-Correlation Properties Based on Piecewise Monotonic Onto Maps", *Proc. of 1999 International Symposium on Nonlinear Theory and its Applications*, vol.2, pp.605–608, 1999.

[11] A. Tsuneda, "On Run-Probability in Chaotic Binary Sequences Generated by Piecewise Linear Onto Maps", *Proc. of 2000 International Symposium on Nonlinear Theory and its Applications*, vol.1, pp.385–388, 2000.

[12] A. Tsuneda, "On Auto-Correlation Properties of Chaotic Binary Sequences Generated by One-Dimensional Maps," *Proc. of 2000 IEEE International Conference on Industrial Electronics, Control and Instrumentation*, pp.2025–2030, 2000.

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

[14] T. Kohda, "A New Theoretical Test for Pseudorandom Number Generators Which Is Based on Perron-Frobenius Operator," *IEICE Trans.*, Vol.E74, No.6, pp.1430–1436,