Design of Maximal-Period Sequences with Prescribed Auto-Correlation Properties Based on One-Dimensional Maps with Finite Bits

Akio Tsuneda, Daisaburou Yoshioka, and Takahiro Inoue

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

Abstract: This paper shows design of maximal-period sequences with prescribed constant auto-correlation values based on one-dimensional (1-D) maps with finite bits. We construct such 1-D maps based on piecewise linear onto chaotic maps. Theoretical analyses and some design examples are given.

1. Introduction

Chaos-based random number generation has received significant attention, especially, for its applications to communications such as CDMA systems. The simplest system to exhibit chaos phenomenon is a one-dimensional discrete-time nonlinear dynamical system. A class of one-dimensional nonlinear maps can produce chaotic sequences whose properties can be designed and analyzed theoretically. Though a chaotic sequence itself is real-valued, it can be easily converted to binary sequences, called *chaotic binary sequences*, by appropriate threshold functions. Binary sequences are most useful in digital communication systems. In applications of such chaotic binary 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 [1]. 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 some sequences with exponentially vanishing auto-correlations have better performance in asynchronous DS/CDMA systems than i.i.d. sequences [2]. Thus, it is very important to design chaotic sequences with prescribed statistical properties. We have given simple design methods to obtain chaotic binary sequences with prescribed auto-correlation properties, including higher-order statistics, based on one-dimensional piecewise monotonic *onto* maps [3].

For practical applications, chaotic sequences are often generated by digital computers in order to guarantee the reproducibility at transmitter and receiver ends. Digital computers have sufficient precision for generating chaotic sequences of reasonable length for practical applications. However, their cost and speed are inferior to conventional sequences such as M-sequences which can be generated by simple shift registers [4]. For this problem, we have been trying to generate maximal-period sequences based on one-dimensional maps with finite bits whose shapes are similar to piecewise linear chaotic maps. Some of them are generated by nonlinear feedback shift registers and their extended versions [5].

In this paper, we construct one-to-one maps with finite bits based on piecewise linear onto maps. This implies that such one-to-one maps are one of approximations with finite precision (bits) to chaotic maps. We use maximal-period sequences generated by such maps. In other words, we use a minimum precision (the number of bits) for a certain sequence length. This is reasonable in terms of efficiency. It should be noted that statistical properties such as auto-correlation values of chaotic sequences of finite length have some fluctuations from their theoretical values. However, using such maximal-period sequences based on one-dimensional maps with finite bits, we can design binary sequences with constant auto-correlation values for some time delays. We discuss such design of maximal-period binary sequences in detail.

2. Chaotic Binary Sequences by Piecewise Linear Onto Maps

We can generate chaotic sequences by the one-dimensional difference equation

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

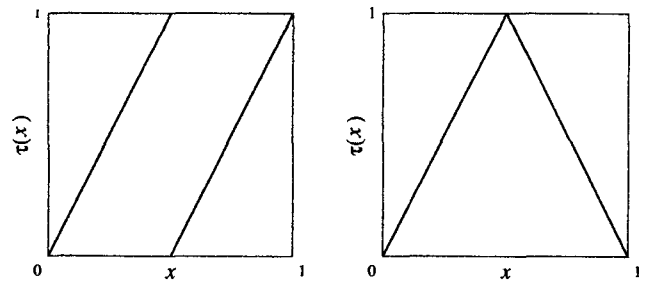
where $\tau(\cdot)$ is a nonlinear chaotic map. In this paper, we use piecewise linear onto maps whose mapping function $\tau_i(\cdot)$ in each subinterval I_i $(i = 1,2,\cdots,N_\tau)$ is given by

$$\tau_i(x) = a_i x + b_i, \quad |a_i| > 1, \quad \tau_i : I_i \to I \text{ (onto)}. \quad (2)$$

It is known that such maps have a uniform invariant measure.

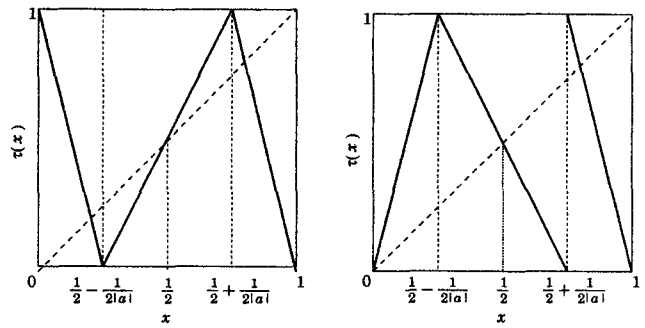
Furthermore, we convert chaotic real-valued sequences to binary sequences by using the threshold function defined by

$$\Theta_t(x) = \begin{cases} 0 & (x < t) \\ 1 & (x \geq t). \end{cases} \quad (3)$$



(a) Bernoulli Map (b) Tent Map

Figure 1. Well-known piecewise linear maps.



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

Figure 2. Examples of piecewise linear onto maps.

Statistical properties of such chaotic binary sequences depend on the chaotic maps and the threshold function.

2.1 I.I.D. Binary Sequences

Independent and identically distributed (*i.i.d*) binary sequences can be generated several types of chaotic maps and binary functions [1]. In this paper, we consider simple and well-known piecewise linear maps, the Bernoulli map and the tent map as shown in Figure 1. Using a threshold function with threshold $t = 0.5$ given by eq.(3), we can get balanced and i.i.d. binary sequences $\{\Theta_{\frac{1}{2}}(x_n)\}_{n=0}^{\infty}$ from real-valued sequences $\{x_n\}_{n=0}^{\infty}$ generated by the Bernoulli map and the tent map. Their auto-correlation function defined by

$$R(\ell;\Theta_{\frac{1}{2}}) = \frac{1}{N}\sum_{n=0}^{N-1}(2\Theta_{\frac{1}{2}}(x_n)-1)(2\Theta_{\frac{1}{2}}(x_{n+\ell})-1) \quad (4)$$

is known to tend to the delta function defined by

$$\delta(\ell) = \begin{cases} 1 & (\ell = 0) \\ 0 & (\ell \neq 0), \end{cases} \quad (5)$$

as $N \to \infty$.

2.2 Correlated Binary Sequences

Let us consider piecewise linear onto maps such that $\tau(\frac{1}{2}) = \frac{1}{2}$, that is, $x = \frac{1}{2}$ is a fixed point of the map. Thus, the mapping function in the subinterval $I_r(\ni \frac{1}{2})$ is given by

$$\tau_r(x) = ax - \frac{a-1}{2} \quad \left(\frac{1}{2} - \frac{1}{2|a|} \le x < \frac{1}{2} + \frac{1}{2|a|}\right). \quad (6)$$

An example of such maps is shown in Figure 2. The auto-correlation function of binary sequences $\{\Theta_{\frac{1}{2}}(x_n)\}_{n=0}^{\infty}$ obtained by such maps, which is also given by eq.(4), tends to $a^{-\ell}$ as $N \to \infty$ [3]. It should be noted that this is independent of the mapping functions in other subintervals. Thus we can control the auto-correlation property by the parameter a.

3. Maximal-Period Sequences Based on 1-D Maps with Finite Bits

We construct one-to-one maps with finite bits based on piecewise linear onto maps described in the previous section. This implies that such one-to-one maps are one of approximations with finite precision (bits) to chaotic maps. We use maximal-period sequences generated by such maps with finite bits. In other words, we use a minimum precision (the number of bits) for a certain sequence length. This makes it possible to realize cheap and high-speed generators of such sequences. It should be noted that statistical properties such as auto-correlation values of chaotic sequences of finite length have some fluctuations from their theoretical values which are obtained for sequences with infinite length.

In this section, we show that it is possible to design maximal-period sequences with constant auto-correlation values for some time delays.

Here, define a vector form of a periodic binary sequence $\{B(x_n)\}_{n=0}^{N-1}$ $(B(\cdot) \in \{0,1\})$ by

$$\mathbf{B}^{\ell} = (B(x_\ell), \cdots, B(x_{N-1}), B(x_0), \cdots, B(x_{\ell-1})), \quad (7)$$

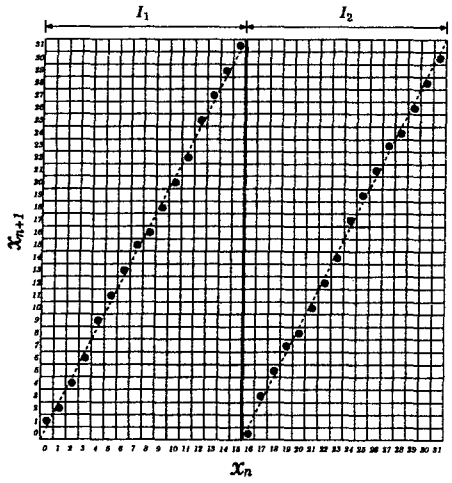
which is a cyclic shift version of $\mathbf{B}^0$. Using the above form, we can also write its auto-correlation function as

$$R(\ell;B) = 1 - \frac{2}{N}H(\mathbf{B}^0, \mathbf{B}^{\ell}), \quad (8)$$

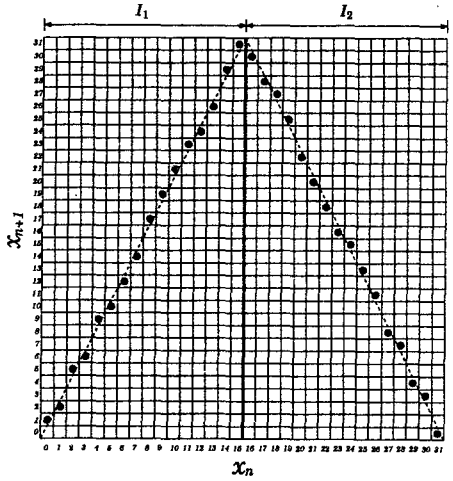
where $H(\mathbf{A},\mathbf{B})$ denotes the Hamming distance between the vectors $\mathbf{A}$ and $\mathbf{B}$.

3.1 Construction of 1-D Maps

We approximate piecewise linear chaotic maps by plotting N points on an $N \times N$ (x_n, x_{n+1})-plane. For appropriate plottings, we can generate a maximal-period integer sequence $\{x_n\}_{n=0}^{N-1}$ $(x_n \in \{0,1,\cdots,N-1\})$. In the following sections, assume that we have such appropriate plottings which generate maximal-period sequences. Furthermore, we obtain a binary sequence $\{\Theta_{N/2}(x_n)\}_{n=0}^{N-1}$. Note that N corresponds to 1 in the original chaotic map with $I = [0,1]$. We also assume that N is an even integer to get completely balanced binary sequences. We discuss auto-correlation properties of such periodic binary sequences.

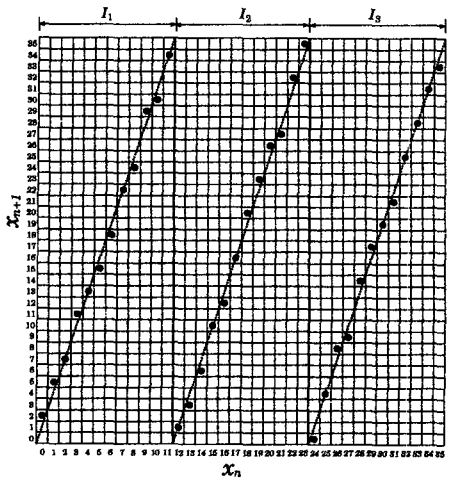


(a) Bernoulli-type

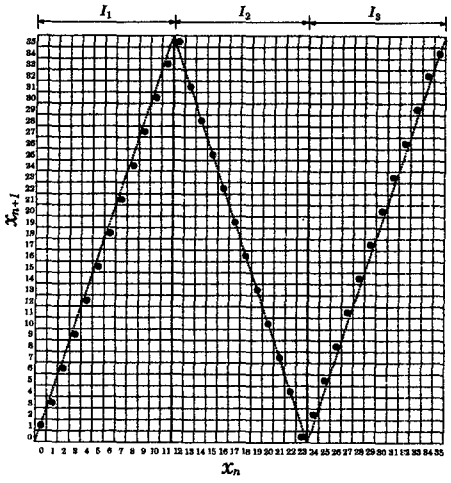


(b) tent-type

Figure 3. Examples of 1-D maps with finite bits, where $N = 32$.



(a) $a > 0$



(b) $a < 0$

Figure 4. Examples of 1-D maps with finite bits, where $N = 36$.

3.2 Uncorrelated Sequences

Figure 3 shows examples of 1-D maps with finite bits based on the Bernoulli map and the tent map, where $N = 32$. In the subinterval I_1 in both types of maps, x_n is mapped to $2x_n$ or $2x_n + 1$. On the other hand, in the subinterval I_2, x_n is mapped to $2x_n - N$ or $2x_n - N + 1$ for the Bernoulli-type map and $2N - 2x_n - 1$ or $2N - 2x_n - 2$ for the tent-type map. In each subinterval of both types of maps, just a half of the integers is mapped to I_1 and the other half is mapped to I_2. That is, $\Theta_{N/2}(x_n) = \Theta_{N/2}(x_{n+1})$ is satisfied for just a half of $n \in I = [0, N-1]$ and not satisfied for the other n. This implies that the Hamming distance between $\mathbf{\Theta}^0_{N/2}$ and $\mathbf{\Theta}^1_{N/2}$ is given by

$$H(\mathbf{\Theta}^0_{N/2}, \mathbf{\Theta}^1_{N/2}) = \frac{N}{2}, \tag{9}$$

which, in conjunction with eq.(8), gives $R(1; \Theta_{N/2}) = 0$. Furthermore, for $N = 2^k$ we can easily obtain

$$H(\mathbf{\Theta}^0_{N/2}, \mathbf{\Theta}^\ell_{N/2}) = \frac{N}{2} \quad \text{for } 1 \le \ell \le k-1, \tag{10}$$

which leads us to get $R(\ell; \Theta_{N/2}) = 0$ for $1 \le \ell \le k-1$. Note that for $N = 2^k$, we can generate such sequences by k-stage nonlinear feedback shift registers or their extended versions [5].

3.3 Correlated Sequences

Figure 4 shows examples of 1-D maps with finite bits based on piecewise linear onto maps with 3 subintervals which generate binary sequences with exponentially vanishing auto-correlations. The absolute value of the slope of the mapping function in each subinterval is 3. Hence we assume that N is a multiple of 6 in order to let the number of integers in each subinterval be an even number.

In each subinterval of Figure 4, just a half of the integers is mapped to $[0, N/2 - 1]$ and the other half is mapped to $[N/2, N]$. In subintervals I_1 and I_3, it is obvious that $\Theta_{N/2}(x_n) = \Theta_{N/2}(x_{n+1})$ is satisfied for just a half of $n \in [0, N/3 - 1]$ and $n \in [2N/3, N - 1]$ and not satisfied for the other n. However, $\Theta_{N/2}(x_n) =$

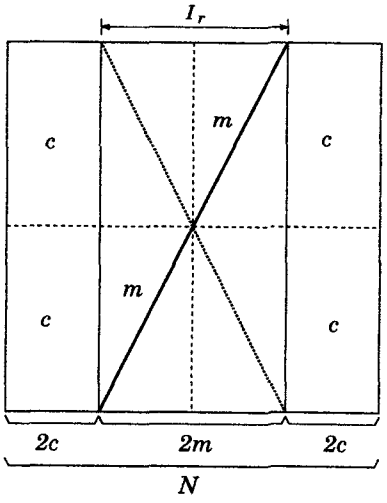


Figure 5. Conceptual diagram of constructed maps for general cases.

$\Theta_{N/2}(x_{n+1})$ is satisfied for all $n \in I_2$ in Figure 4 (a) and not satisfied for any $n \in I_2$ in Figure 4 (b). Hence we have

$$H(\Theta^0_{N/2}, \Theta^1_{N/2}) = \begin{cases} \dfrac{N}{3} & \text{for Figure 4 (a)} \\ \dfrac{2N}{3} & \text{for Figure 4 (b)} \end{cases} \tag{11}$$

which, in conjunction with eq.(8), gives

$$R(1; \Theta_{N/2}) = \begin{cases} \dfrac{1}{3} & \text{for Figure 4 (a)} \\ -\dfrac{1}{3} & \text{for Figure 4 (b).} \end{cases} \tag{12}$$

The above auto-correlation values agree with the theoretical ones for the original chaotic maps given by a^{-1}.

Now consider more general cases. We construct 1-D maps with finite bits based on piecewise linear onto maps as shown in Figure 2. Let us assume the slope of the center subinterval $I_r(\ni \frac{1}{2})$ is $a = \pm\frac{N}{2m}$, where $N = 2m + 4c$, m and c are positive integers. Figure 5 shows a conceptual diagram of the constructed map of integers.

Similarly to the previous special cases as in Figure 4, we plot mapping points so that just a half of the integers could mapped to $[0, N/2 - 1]$ and the other half could be mapped to $[N/2, N]$. Thus we have

$$H(\Theta^0_{N/2}, \Theta^1_{N/2}) = \begin{cases} 2c & \text{for } a = \dfrac{N}{2m} \\ 2c + 2m & \text{for } a = -\dfrac{N}{2m} \end{cases} \tag{13}$$

which, in conjunction with eq.(8), gives

$$R(1; \Theta_{N/2}) = \begin{cases} \dfrac{2m}{N} = \dfrac{1}{a} & \text{for } a = \dfrac{N}{2m} \\ -\dfrac{2m}{N} = -\dfrac{1}{a} & \text{for } a = -\dfrac{N}{2m}. \end{cases} \tag{14}$$

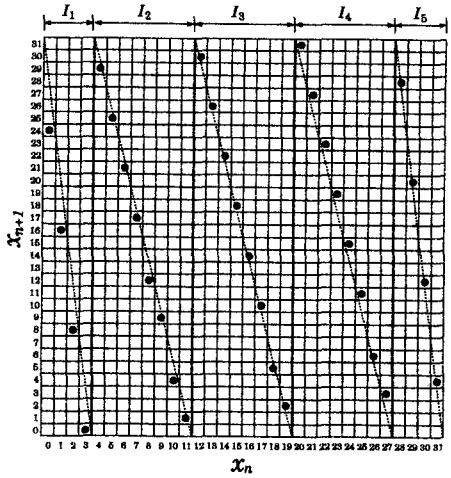


Figure 6. A design example of maps for $a = -4$.

This also agrees with the theoretical one a^{-1}. Therefore, we can design maximal-period binary sequences with a constant auto-correlation value at the time delay $\ell = 1$ by the above method. Figure 6 shows a design example of maps for $a = -4$.

4. Conclusion

We have given design methods of maximal-period sequences with prescribed constant auto-correlation values for some time delays. It has been shown that both of uncorrelated and correlated binary sequences can be designed for time delay 1. We will discuss such design for more time delays.

References

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

[2] 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.

[3] 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.

[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] A. Tsuneda, Y. Kuga, and T. Inoue, "New Maximal-Period Sequences Using Extended Nonlinear Feedback Shift Registers Based on Chaotic Maps", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol.E85-A, no.6, pp.1327–1332, 2002.