Quantized system of chaotic pulse-train generator

Hiroyuki Torikai and Toshimichi Saito

EECE Dept., HOSEI University
Kajino-cho, Koganei-shi, Tokyo 184-8584, Japan
Phone:+81-42-387-6216, Fax: +81-42-387-6122
Email: {torikai, tsaito}@k.hosei.ac.jp

1. Abstract

As a state of a chaotic pulse-train generator is quantized, an original chaotic pulse-train is changed into a set of co-existing super-stable periodic pulse-trains. We derive two theorems that guarantee (a) binary informations can be coded into pulse-trains having the same period, and (b) the quantized system generates periodic pulse-trains having the possible maximum period.

2. Introduction

We consider quantized dynamics of a chaotic pulse position map (Qmap). Due to the state quantization, an original chaotic pulse-train is changed into a set of co-existing various super-stable periodic pulse-trains (SSPTs) and the Qmap generates one of them depending on the initial state. We have clarified some basic characteristics of the Qmap, e.g., the number of co-existing SSPTs and their periods [1][2]. In this paper, we derive two theorems that guarantee generation of the following SSPTs.

- Based on pulse-interval modulation, binary informations can be coded into SSPTs having the same period.
- The Qmap generates SSPTs having the possible maximum period.

The ultrawide-bandwidth (UWB) impulse-radio communication system is recently attracting great interests and will be promising for short-range wireless communications [3]. The UWB system utilizes pulse-trains and has advantages of low power consumption, low intercept probability and so on. In the UWB system, one of the important basic problems is the coding method of informations into pulse-trains [3]. Note that our coded SSPTs have the same period and will be useful for multiplexing [4]. Then our results may be fundamentals for developing a Qmap-based pulse coder suitable for a UWB multiplex communication system. On the other hand, various discrete state dynamical systems have been investigated intensively [5]-[9]. The shift register generator is often used to generate spread sequences for code division multiple access communications systems. The linear congruential sequence generator is used as a pseudo-random number generator. However, co-existence phenomena and pulse coding have not been studied sufficiently in the literatures. A simple electrical circuit realizing the Qmap can be found in [1].

3. Quantized chaotic pulse-train dynamics

We consider dynamics of a pulse-train $y(\tau)$ which is governed by a pulse position map:

$$\begin{aligned} &\tau_{n+1} = f(\tau_n) = 2\tau_n + 1 \ \text{ for } \ 0 \le \tau_n < 1, \\ &f(\tau_n + 1) = f(\tau_n) + 1, \ \ f : \boldsymbol{R}^+ \to \boldsymbol{R}^+, \end{aligned} \tag{1}$$

where τ_n, $n = 1, 2, ...$, is the n-th pulse position and $\boldsymbol{R}^+$ is the positive reals. The pulse position map f is shown in Fig.1. Because of the periodicity, we can define a return map $\tau_{n+1} = F(\tau_n) = f(\tau_n)$ (mod 1), $F : [0,1) \to [0,1)$ as shown in Fig.2(a). The return map F generates chaos and the pulse position map f generates a chaotic pulse-train $y(\tau)$.

Here we quantize the state of the pulse position map f:

$$\tau_2 = \frac{1}{M} Int(Mf(\tau_1) + \frac{1}{2}) \in \boldsymbol{L}_M = \{\frac{0}{M}, \frac{1}{M}, ...\},$$

where $\tau_1 \in \boldsymbol{R}^+$, M is a positive integer and is called the quantization frequency, and $Int(\tau)$ gives the integer part of τ. Since the pulse position τ_n, $n \ge 2$, is restricted on the lattice points in $\boldsymbol{L}_M$, the pulse-train $y(\tau)$ is super-stable for the initial state τ_1 [1]. Then the system dynamics can be analyzed using a quantized pulse position map (Qmap):

$$\begin{aligned} &\tau_{n+1} = g(\tau_n) = \frac{1}{M} Int(Mf(\tau_n) + \frac{1}{2}), \\ &g : \boldsymbol{L}_M \to \boldsymbol{L}_M = \{\frac{0}{M}, \frac{1}{M}, ...\}. \end{aligned} \tag{2}$$

The Qmap g is shown in Fig.1. We can define a quantized return map $\theta_{n+1} = G(\theta_n) = g(\theta_n)$ (mod 1), $G : \boldsymbol{K}_M \to \boldsymbol{K}_M = \{\frac{0}{M}, \frac{1}{M}, ..., \frac{M-1}{M}\}$ as shown in Fig.2(b). We give some definitions on the Qmap.

Definition 1: A pulse position τ^* is said to be super-stable periodic with period p and cycle q if p is the minimum integer such that $g^q(\tau^*) - \tau^* = p$, where g^q is the q-fold composition of g. A pulse-train y is said to be the super-stable periodic pulse-train (SSPT) with period p and cycle q if its pulse position is given by $\tau_n = g^{n-1}(\tau^*)$. A point τ^e is said to be eventually periodic if τ^e is not periodic but $g^l(\tau^e)$ is periodic for some $l > 1$.

In Fig.1 and Fig.2(b), we can see that SSPTs co-exist and the Qmap generates one of them depending on the initial state. Fig.3 shows co-existing SSPTs.

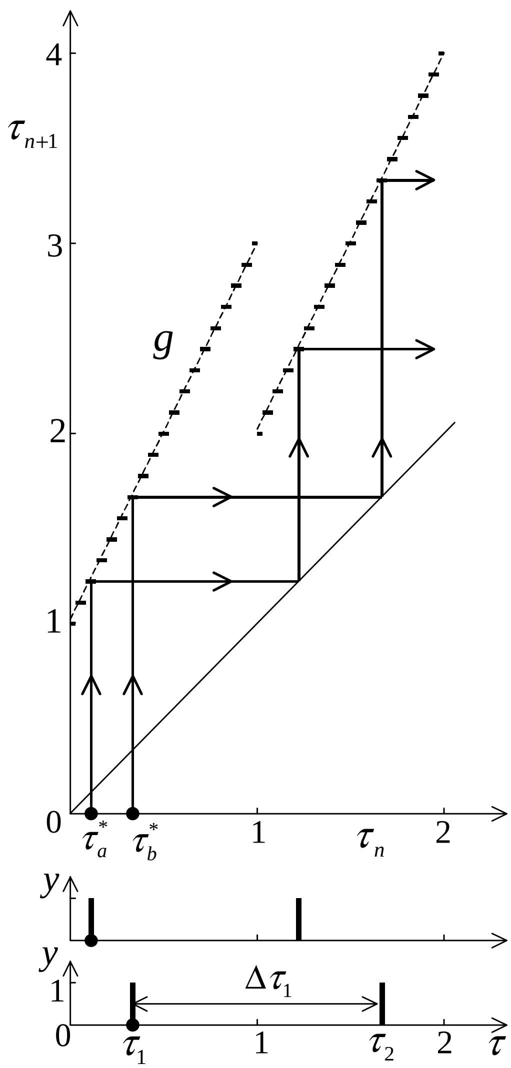

Figure 1: Chaotic pulse position map f (broken) and quantized pulse position map g (stepwise) with the quantization frequency $M = 9$.

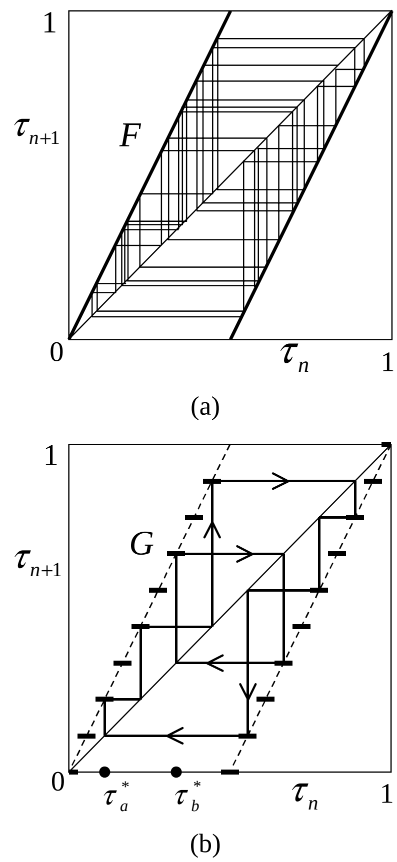

Figure 2: (a) Chaotic return map F. (b) Quantized return map G with the quantization frequency $M = 9$.

4. Pulse interval modulation

Let $\Delta\tau_n = \tau_{n+1} - \tau_n$ be the n-th pulse interval (see Fig.1). We then introduce binary coding $(\omega_1 ... \omega_k)$ of an SSPT based on pulse interval modulation:

$$\omega_n = \begin{cases} 0, & \text{for } 1 \leq \Delta\tau_n < 1.5, \\ 1, & \text{for } 1.5 \leq \Delta\tau_n < 2. \end{cases} \tag{3}$$

For simplicity, the bit-length k is assume to equal the cycle q or its multiple. A SSPT coded by $(\omega_1 ... \omega_k)$ is said to have the length $L = \tau_{1+k} - \tau_1$. The relationship between the code and the length is given by

$$L = k + \sum_{n=1}^{k} \omega_n. \tag{4}$$

In Fig.3, the SSPTs can be coded in the form of $(b_1 ... b_3 \bar{b}_1 ... \bar{b}_3)$ and have the same length $L = 9$, where $\bar{b} = |b - 1|$. We can give the following theorem.

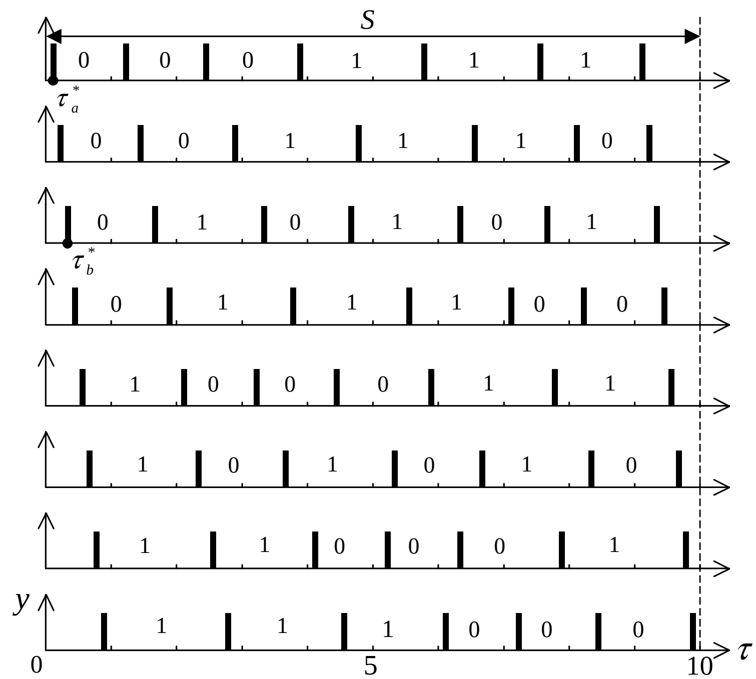

Figure 3: Co-existing SSPTs in the Qmap g with $M = 9$. The SSPTs have cycle $q = 6$ and length $L = 9$, and are coded in the form of $(b_1b_2b_3\bar{b_1}\bar{b_2}\bar{b_3})$. The SSPTs exist in $S = 10$ time slots.

Theorem 1: Let $M = 2^k + 1$, where k is some positive integer. Let $(b_1 ... b_k)_2$ represent a k-bit binary number. Then each k-bit binary information $(b_1 ... b_k)$ corresponds to a SSPT starting from $\tau_1 = \frac{i}{M}$ such that $i - 1 = (b_1 ... b_k)_2$. The SSPT is coded by $(b_1 ... b_k\bar{b_1} ... \bar{b_k})$ and has the length $L = 3k$. If M is prime, the period of each SSPT is $p = 3k$.

Outline of the proof: Let an SSPT start from $\tau_1 = \frac{i}{2^k+1}$, $i \in \{1, 2, ..., 2^k\}$, and let $(b_1 ... b_k)_2 = i - 1$. Using $2k$-bit binary numbers, the pulse positions τ_1 and $g(\tau_1)$ can be expressed by

$$\tau_1 = \frac{(2^k - 1)i}{2^{2k} - 1} = \frac{(b_1 ... b_k\bar{b_1} ... \bar{b_k})_2}{(11 ... 11)_2},$$

$$g(\tau_1) = \frac{(b_2 ... b_k\bar{b_1} ... \bar{b_k}b_1)_2}{(11 ... 11)_2} + b_1 + 1.$$

Noting $\omega_1 = b_1$ and repeating similar considerations for $g^l(\tau_1)$, $l = 2, 3 ....$, the SSPT is coded by $(\omega_1 ... \omega_{2k}) = (b_1 ... b_k\bar{b_1} ... \bar{b_k})$. Then Equ.(4) gives $L = 3k$. For contradiction, let M be prime and let the SSPT has a cycle $q < 2k$. In this case $\tau_1 = \frac{i}{M}$ must be expressed by $\frac{j}{2^q - 1}$ [2], and this is a contradiction.

Let a unit time interval be called a slot and let S be the number of slots in which a coded SSPT exist. In Ref.[2], we have shown that the Qmap g has SSPTs coded by all k-bit informations $(b_1 ... b_k)$ except for $(1 ... 1)$ if $M = 2^k - 1$. In this case, however, the number of slots depends on the code: $k + 1 \le S \le 2k + 1$. In the case of Theorem 1, the number of slots is $S = 3k + 1$ for each k-bit information (see Fig.3). Such SSPTs may be useful for time-division multiplex communications systems as discussed in [4].

5. Maximum period SSPT

For the quantization frequency M, the possible maximum cycle of an SSPT is $M - 1$ since the pulse position $\tau_n = \frac{0}{M}$ is always a fixed point. In Fig.4, the Qmap generates such an SSPT. We can give the following theorem.

Theorem 2: Assume the following. (a) $M \ge 3$ is odd. (b) Letting $k = \frac{M-1}{2}$, $2^k + 1$ can be divided by M. (c) M and $2^l - 1$ have no common divisor for every l dividing $M - 1$, where $1 < l < M - 1$. Then the SSPT have the possible maximum cycle $M - 1$ and the possible maximum period $\frac{3}{2}(M - 1)$. The SSPT starting from $\tau_1 = \frac{i}{M}$, $i \in \{1, 2, ..., M - 1\}$, is coded by $(b_1 ... b_k\bar{b_1} ... \bar{b_k})$ such that $(b_1 ... b_k)_2 = (2^k + 1)\frac{i}{M}$.

Outline of the proof: The Qmap g has the domain $\boldsymbol{L}_M$. Let a Qmap g' have a quantization frequency $2^k + 1$ and have a domain $\boldsymbol{L}_{2^k+1}$. Conditions (a) and (b) guarantee $\boldsymbol{L}_M \subset \boldsymbol{L}_{2^k+1}$. Then Theorem 1 guarantees that an SSPT of g can be coded by a $2k$-bit binary code. Assume for contradiction that the

SSPT has a cycle $l < 2k$. In this case, $\tau_1 = \frac{i}{M}$ must be expressed by $\frac{j}{2^l-1}$. This contradicts to (c). Hence the SSPT has the possible maximum cycle $2k = M - 1$. Equ.(4) gives the period $\frac{3}{2}(M-1)$. The proof of Theorem 1 gives the code of the SSPT.

6. Discussion

The linear congruential sequence generator is described by

$$X_{n+1} = aX_n + c \pmod{m}, \tag{5}$$

where $n = 0, 1, ...$ is the discrete time; $X_n \in \{0, 1, ..., m-1\}$ is a state; and $a \in \{2, 3, ...\}$, $c \in \{0, 1, ...\}$ and $m \in \{2, 3, ...\}$ are parameters. The possible maximum cycle of this generator is m as shown in Fig.5(a). The shift register generator is described by

$$X_{n+K} = a_0X_n + a_1X_{n+1} + \cdots + a_{K-1}X_{n+K-1} \pmod{2}, \tag{6}$$

where K is the number of registers, $X_n \in \{0, 1\}$ is a state and $a_k \in \{0, 1\}$ is a parameter. The possible maximum cycle of this generator is $2^K - 1$. Using a variable $x_n = \sum_{k=0}^{K-1} 2^{K-k-1}X_{n+k}$, dynamics of the generator can be illustrated as shown in Fig.5(b). For these generators, conditions for generating the maximum cycle sequences have been investigated [7].

The quantized return map G and the above sequence generators have some relations. G can realize the linear congruential sequence generator (5) by adjusting the shape of f and the parameter M. The dynamics of G for $M = 2^K + 1$ can be described by a similar formula of the shift register generator (6): $X_{n+K} = X_n + 1$ (mod 2). In this paper we have considered not only the maximum period SSPT but also the co-existence phenomena and the pulse interval modulation.

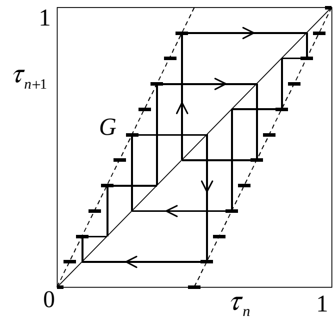

Figure 4: Quantized return map G with the quantization frequency $M = 11$. The SSPT has the possible maximum cycle 10.

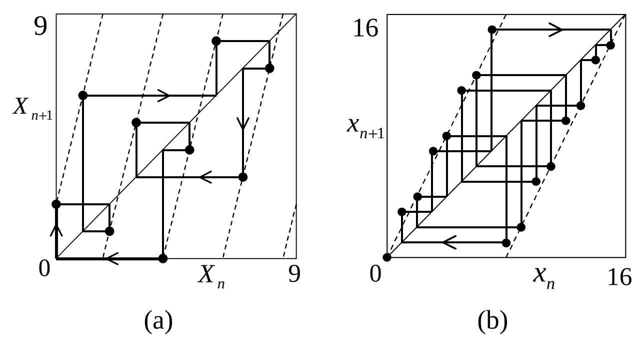

Figure 5: (a) Linear congruential sequence generator. $a = 4$, $c = 2$ and $m = 9$. (b) Shift register generator. $K = 4$, $a_0 = a_3 = 1$ and $a_1 = a_2 = 0$.

7. Conclusions

We have analyzed the set of co-existing SSPTs in the Qmap. It has been shown that binary informations can be coded into SSPTs having the same period. Also the condition for generating SSPTs with the possible maximum period has been derived. Future problems include: (a) analysis of the Qmap for wider parameter range, (b) development of a synthesis method of the Qmap having useful pulse coding ability, and (c) design of simple circuit that realizes the Qmap.

References

[1] H.Torikai and T.Saito, Analysis of a quantized chaotic system, Int. J. Bif. and Chaos, 12, 5, 1207-1218, 2002.

[2] H.Torikai and T.Saito, Return map quantization from an integrate-and-fire model with two periodic inputs, IEICE Trans. Fundamentals, E82-A, 7, 1336-1343, 1999.

[3] G.M.Maggio, N.Rulkov and L.Reggiani, Pseudo-chaotic time hopping for UWB impulse radio, IEEE Trans. CAS-I, vol.48, no.12, pp.1424-1435, 2001.

[4] Y.Kawasaki, T.Saito and H.Torikai, Quantized chaotic dynamics and communications systems, Proc. of IEEE/ISCAS, vol.3, pp.133-136, 2001.

[5] D.R.Frey, Chaotic digital encoding: an approach to secure communication, IEEE Trans. CAS-II, vol.40, no.10, pp.660-666, 1993.

[6] A.C.Davies, Digital counters and pseudorandom number generators from a perspective of dynamics, in Nonlinear Dynamics of Electronic Systems (World Scientific Singapore), 373-382, 1994.

[7] D.E.Knuth, The art of computer programming, vol.2, 3rd edn., Addison Wesley, 1998.

[8] M.Jessa, Data transmission with adjustable security exploiting chaos-based pseudorandom number generators, Proc. of IEEE/ISCAS, 3, 476-479, 2002.

[9] A.Tsuneda, D.Yoshida and T.Inoue, Design of maximum-period sequence with prescribed auto-correlation properties based on one-dimensional maps with finite bits, Proc. of ITC-CSCC, pp.1882-1885, 2002.