2004 International Symposium on Nonlinear
Theory and its Applications (NOLTA2004)
Fukuoka, Japan, Nov. 29 - Dec. 3, 2004

Equivalence of Periodic Sequences Generated by Bernoulli and Tent Maps with Finite Bits

Daisaburo Yoshioka, Akio Tsuneda, and Takahiro Inoue

Department of Electrical and Computer Engineering, Kumamoto University
2-39-1 Kurokami, Kumamoto, Kumamoto 860-8555, Japan
Email: yoshioka@ieee.org

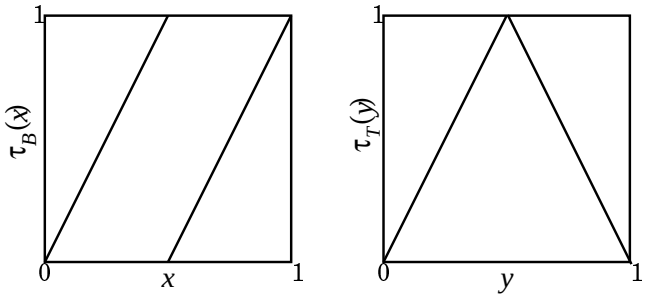
Abstract—There is a topological conjugation between the Bernoulli and tent maps. In this paper, it is proved that there is also a topological conjugation between two types of periodic sequences generated by nonlinear feedback shift registers which can be regarded as one-dimensional maps obtained by quantizing the Bernoulli and tent maps.

1. Introduction

Pseudo random numbers are required in several applications including Monte Carlo method, spread spectrum communication, cryptography, and so on. Representatives of pseudo random numbers are linear and nonlinear shift register sequences such as M-sequences and de Bruijn sequences [1]. On the other hand, as a quite different approach, random number generation based on chaos has been increasingly studied by many researchers. Chaos is random behavior produced by deterministic systems. The simplest chaotic system is a one-dimensional discrete-time nonlinear dynamical system.

Shift register sequences are mostly designed by means of finite field theory and chaotic ones are based on nonlinear dynamical systems treating real numbers. Therefore, there are seemingly no relationship between shift register sequences and chaotic ones even if there is a common sense that both sequences are generated by deterministic systems. However, the following works show some relations between shift register sequences and chaotic ones. An interesting insight is firstly pointed out in [2], which reveals that M-sequences generated from *linear feedback shift registers (LFSRs)* are one of finite-word-length approximation to the Bernoulli map. As in [3], it is easy to show that *nonlinear feedback shift registers (NFSRs)* are also one of finite-word-length approximation to the Bernoulli map. Furthermore, finite-word-length approximation of the tent map is realized by another type of nonlinear feedback shift register called *extended nonlinear feedback shift register (e-NFSR)* in [3]. Generation algorithm of maximal-period sequences (including m-ary de Bruijn sequences) generated by quantizing a class of chaos maps is proposed in [4].

It is well known that the Bernoulli map and tent map can be transformed into each other by a function. This relation is called a *topological conjugation* [5]. In [6], it is also revealed that there is a linear transformation between two forms of NFSR, whose concept is quite analogous to a topological conjugation. In this paper, we prove a topological conjugation between periodic sequences generated by NFSRs and e-NFSRs, which can be regarded as finite-word-length version of the relation between the Bernoulli and tent maps.



(a) Bernoulli map. (b) Tent map.

Figure 1: Bernoulli and tent maps.

2. Bernoulli and Tent map

We firstly introduce the Bernoulli and tent maps, which are well-known chaotic maps respectively defined by

$$x_{n+1} = \tau_B(x_n) = \begin{cases} 2x_n & (0 \le x_n < \frac{1}{2}) \\ 2x_n - 1 & (\frac{1}{2} \le x_n < 1), \end{cases} \tag{1}$$

$$y_{n+1} = \tau_T(y_n) = \begin{cases} 2y_n & (0 \le y_n < \frac{1}{2}) \\ 2(1-y_n) & (\frac{1}{2} \le y_n < 1). \end{cases} \tag{2}$$

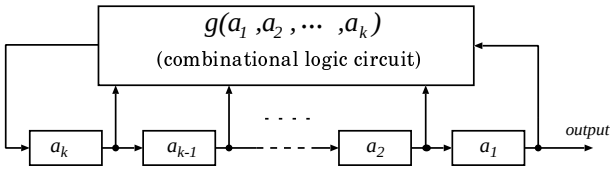
Figs.1 illustrate the Bernoulli and tent maps.

It is well known that the Bernoulli and tent maps are topologically conjugated, which means that they can be transformed into each other by a conjugation function $h(x)$ satisfying [5]

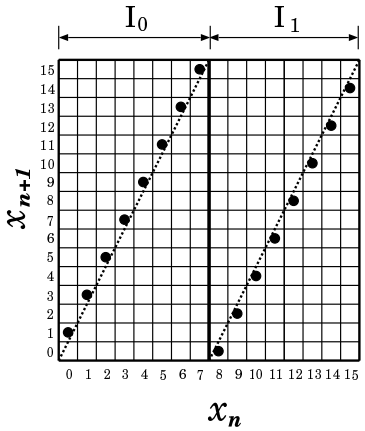
$$h(\tau_B(x)) = \tau_T(h(x)). \tag{3}$$

A diagram of the concept of the topological conjugation will be shown in Fig.4 (a). In [5], a conjugation function $h(x)$ is given by

$$h(x) = \sum_{j=1}^{\infty} b_j(x) 2^{-j}, \quad b_j(x) \in \{0, 1\}. \tag{4}$$

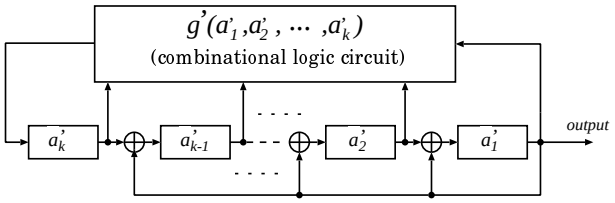


(a) NFSR.

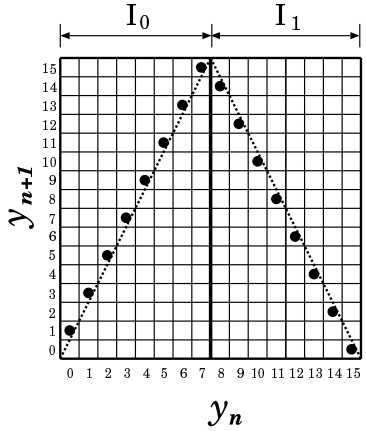


(b) An example of 1-D map ($k = 4$).

Figure 2: NFSR and its 1-D map.



(a) extended NFSR.



(b) An example of 1-D map ($k = 4$).

Figure 3: Extended NFSR and its 1-D map.

Here $b_j(x)$ are obtained by the following recurrence relation:

$$b_{j+1}(x) = b_j(x) \oplus a_{j+1}(x) \quad (j = 0, 1, 2, \cdots), \tag{5}$$

where $b_0(x) = 0$, $\oplus$ denotes modulo-2 addition, and a_j is determined by the binary expansion of x written as

$$x = \sum_{j=1}^{\infty} a_j(x) 2^{-j}, \quad a_j(x) \in \{0, 1\}. \tag{6}$$

Note that the Bernoulli map $\tau_B(x)$ can be expressed as

$$\tau_B(x) = \sum_{j=1}^{\infty} a_{j+1}(x) 2^{-j}. \tag{7}$$

3. Finite-Word-Length Approximation of Chaotic Sequences

We introduce NFSRs and extended NFSRs which can be considered as generators of *quasi-chaotic* sequences with finite precision [3].

3.1. NFSR

Fig.2 (a) shows a nonlinear feedback shift register (NFSR) with k memory cells, where the feedback function $g(\cdot)$ is a mapping of $GF(2)^k$ to $GF(2)$. Denote a state of the register by the column vector $\boldsymbol{a} = (a_1, a_2, \cdots, a_k) \in GF(2)^k$. Let T be the *next-state operator*, then $T(\boldsymbol{a})$ denotes the next state of an NFSR with current state $\boldsymbol{a}$. Namely, by clocking the NFSR, $\boldsymbol{a}$ is succeeded by $T(\boldsymbol{a}) = (a_2, a_3, \cdots, a_k, g(a_1, a_2, \cdots, a_k)) \in GF(2)^k$ which is represented by [6]

$$T(\boldsymbol{a}) = A\boldsymbol{a} \oplus g(\boldsymbol{a})\boldsymbol{u}, \tag{8}$$

where $g(\boldsymbol{a})$ indicates the nonlinear feedback function mapping $GF(2)^k$ to $GF(2)$, A is the $k \times k$ matrix defined by

$$A = \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & 1 \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots 0 & 1 \\ 0 & 0 & \cdots & 0 \end{bmatrix}, \tag{9}$$

and $\boldsymbol{u}$ is the column vector such that

$$\boldsymbol{u} = (0, 0, \cdots, 1) \in GF(2)^k. \tag{10}$$

Next, let us transform a state of the register at time n into a decimal integer $x_n \in [0, 2^k - 1]$ as

$$x_n = a_1(n) \cdot 2^{k-1} + a_2(n) \cdot 2^{k-2} + \cdots + a_k(n) \cdot 2^0, \tag{11}$$

where $a_i(n) \in GF(2)$ denotes a value of ith element of the register at time n. We can construct one-dimensional maps by plotting (x_n, x_{n+1}). An example of such a 1-D map is shown in Fig.2 (b), where $k = 4$. It is easily found from Fig.1 (a) and Fig.2 (b) that the shapes of such one-dimensional maps are similar to the Bernoulli map.

Namely, NFSRs are finite-word-length approximation to the Bernoulli map.

Maximal-period sequences generated from such NFSRs are called *de Bruijn sequences* whose period is 2^k. It is known that the number of possible NFSR sequences is equal to $2^{2^{k-1}}$ and the number of de Bruijn sequences is equal to $2^{2^{k-1}-k}$ [1], [7].

3.2. Extended NFSR

Fig.3 (a) shows an extended NFSR (e-NFSR) with k memory cells, where the feedback function is $g'(\cdot)$. We also denote a state of the register by the column vector $\boldsymbol{a}' = (a'_1, a'_2, \cdots, a'_k) \in GF(2)^k$. Similarly to NFSRs, the transition manner can be represented as

$$T'(\boldsymbol{a}') = A'\boldsymbol{a}' \oplus g'(\boldsymbol{a}')\boldsymbol{u}, \tag{12}$$

where T' is the next state operator for extended NFSRs and A' is the $k \times k$ matrix defined by

$$A' = \begin{bmatrix} 1 & 1 & \cdots & 0 \\ 1 & 0 & 1 \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots 0 & 1 \\ 0 & 0 & \cdots & 0 \end{bmatrix}. \tag{13}$$

Fig.3 (b) shows an example of a 1-D map obtained by transforming the register states into integer values with eq.(11) as well as the NFSR case. From Fig.1 (b) and Fig.3 (b), we can also find that such 1-D maps are similar to the tent map. Thus, e-NFSRs can be considered as finite-word-length approximation to the tent map.

4. Equivalence of Periodic Sequences Generated by NFSRs and e-NFSRs

We show here the fact that there is a one-to-one transformation $H\boldsymbol{a} = \boldsymbol{a}'$ satisfying

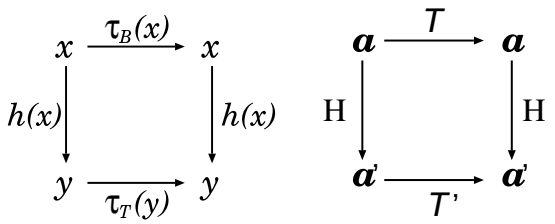
$$HT(\boldsymbol{a}) = T'(H\boldsymbol{a}) \tag{14}$$

which is a kind of topological conjugation between NFSRs and e-NFSRs corresponding to eq.(3) for the chaotic maps as shown in Fig.4.

Theorem: A one-to-one mapping $H\boldsymbol{a} = \boldsymbol{a}'$ satisfying $HT(\boldsymbol{a}) = T'(H\boldsymbol{a})$ for all state $\boldsymbol{a}$ exists.

Proof: Denote the mapping H by the $k \times k$ matrix:

$$H = \begin{bmatrix} h_{1,1} & h_{1,2} & \cdots & h_{1,k} \\ h_{2,1} & h_{2,2} & \cdots & h_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ h_{k,1} & h_{k,1} & \cdots & h_{k,k} \end{bmatrix}. \tag{15}$$



(a) Bernoulli and tent (b) NFSR and e-NFSR

Figure 4: The concept of topological conjugation between Bernoulli and tent maps (a) and the one-to-one transformation matrix H (b).

Using eqs.(8)–(10), (12), (13), and (15), we obtain

$$HT(\boldsymbol{a}) = H(A\boldsymbol{a} \oplus g(\boldsymbol{a})\boldsymbol{u}) = \begin{bmatrix} h_{1,1}a_2 \oplus h_{1,2}a_3 \oplus \cdots \oplus h_{1,k-1}a_k \oplus h_{1,k}g(\boldsymbol{a}) \\ h_{2,1}a_2 \oplus h_{2,2}a_3 \oplus \cdots \oplus h_{2,k-1}a_k \oplus h_{2,k}g(\boldsymbol{a}) \\ \vdots \\ h_{k,1}a_2 \oplus h_{k,2}a_3 \oplus \cdots \oplus h_{k,k-1}a_k \oplus h_{k,k}g(\boldsymbol{a}) \end{bmatrix} \tag{16}$$

$$T'(H\boldsymbol{a}) = A'H\boldsymbol{a} \oplus g'(\boldsymbol{a}')\boldsymbol{u} = \begin{bmatrix} (h_{1,1} \oplus h_{2,1})a_1 \oplus (h_{1,2} \oplus h_{2,2})a_2 \oplus \cdots \oplus (h_{1,k} \oplus h_{2,k})a_k \\ (h_{1,1} \oplus h_{3,1})a_1 \oplus (h_{1,2} \oplus h_{3,2})a_2 \oplus \cdots \oplus (h_{1,k} \oplus h_{3,k})a_k \\ \vdots \\ (h_{1,1} \oplus h_{k,1})a_1 \oplus (h_{1,2} \oplus h_{k,2})a_2 \oplus \cdots \oplus (h_{1,k} \oplus h_{k,k})a_k \\ g'(\boldsymbol{a}') \end{bmatrix}. \tag{17}$$

Thus, the proof will be complete if we can identify a nonsingular transition matrix H and the feedback function $g'(\cdot)$ from eqs.(14), (16), and (17).

Under the condition that eq.(14) holds for arbitrary $\boldsymbol{a}$ and $g(\cdot)$, we can get the following equations concerning the coefficients $h_{j,k}$ and the feedback function $g'(\cdot)$.

$$h_{j,1} = h_{1,1} \quad (2 \le j \le k) \tag{18}$$

$$h_{j,k} = 0 \quad (1 \le j \le k-1) \tag{19}$$

$$h_{j,l} = h_{1,l+1} \oplus h_{j+1,l+1} \quad (1 \le j, l \le k-1) \tag{20}$$

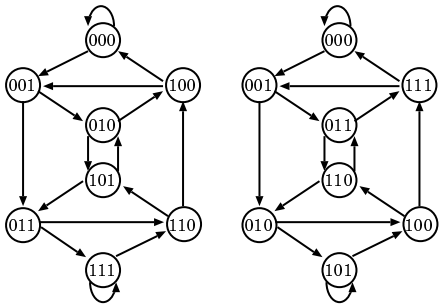
$$g'(\boldsymbol{a}') = h_{k,1}a_2 \oplus h_{k,2}a_3 \oplus \cdots \oplus h_{k,k-1}a_k \oplus h_{k,k}g(\boldsymbol{a}). \tag{21}$$

First, solving eqs.(18)–(20), we can get the nonsingular matrix H as

$$H = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{bmatrix}. \tag{22}$$

which is a lower triangular matrix and has its inverse matrix H^{-1} is given by

$$H^{-1} = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 1 & 1 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 1 \end{bmatrix}. \tag{23}$$



(a) NFSR (b) extended NFSR

Figure 5: The directed graphs, where $k = 3$. Each node is transformed into each other by the matrices H and H^{-1}.

Next, from eqs.(21) and (22), we have

$$g'(\boldsymbol{a}') = a_2 \oplus a_3 \oplus \cdots \oplus a_k \oplus g(\boldsymbol{a}). \tag{24}$$

Thus the proof is completed.

In [3], the number of maximal-period sequences generated from e-NFSRs is investigated by numerical experiments in the case for $k = 3, 4, 5$. Here we can show the following corollary concerning the number of maximal-period sequences generated from e-NFSRs.

Corollary: The number of maximal-period sequences generated from e-NFSRs is $2^{2^{k-1}-k}$, that is, as same as de Bruijn sequences.

Proof: The above theorem shows that every state and its next state of NFSRs can be transformed to those of e-NFSR by the one-to-one mapping H under the condition that $g'(\cdot)$ satisfies eq.(24). Hence, it is obvious that the total number of possible sequences and maximal-period sequences generated from e-NFSRs are equal to those of NFSR, that is, $2^{2^{k-1}}$ and $2^{2^{k-1}-k}$, respectively [1],[7].

Remark 1: Since $a'_0 = a_0$ in $\boldsymbol{a}$' $= H\boldsymbol{a}$, every output of NFSRs with an initial state is the same as that of e-NFSRs with the corresponding initial state under the assumption that eq.(24) is satisfied. This implies that all of de Bruijn sequences can also be generated by e-NFSRs.

Remark 2: The relation eq.(5) can also be expressed by

$$\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ \vdots \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots \\ 1 & 1 & 0 & 0 & \cdots \\ 1 & 1 & 1 & 0 & \cdots \\ 1 & 1 & 1 & 1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ \vdots \end{bmatrix}, \tag{25}$$

where x is dropped for simplicity. The transformation matrix of eq.(25) is equivalent to H given by eq.(22) except the difference of the size of dimension. This implies that H is a finite dimension version of $h(x)$ given in eq.(4).

Remark 3: The transition manner of states of NFSRs is represented by a directed graph with 2^k nodes [1],[7], where every node denotes a state of register and has in-degree and out-degree 2. Fig.5 (a) shows the directed graph for $k = 3$. A path in the graph is determined by $g(\cdot)$ under the restriction that every node can be gone through once and only once. By using $\boldsymbol{a}' = H\boldsymbol{a}$, we can easily obtain the directed graph of e-NFSRs, as shown in Fig.5 (b). We can also transform any path in one graph into a path in the other graph by the transition matrices (H, H^{-1}) and eq.(24). It is easy to see the equivalence of NFSRs and e-NFSRs in Fig.5.

5. Conclusion

In this paper, we have shown the one-to-one mapping between periodic sequences generated by NFSRs and e-NFSRs, which is quite analogous to a topological conjugation function between the Bernoulli and tent maps. We find that a lower triangular matrix can transform the states of NFSRs and e-NFSRs into each other. The relation can be considered as finite-word-length version of the topological conjugation between the Bernoulli and tent maps. This fact is somewhat surprising because such periodic sequences are no longer real chaos.

References

[1] S. W. Golomb, Shift register sequences, revised ed., Aegean Park Press, 1982

[2] T. Kohda and M. Fukushige, "Note on finite-word-length realization of Bernoulli shift by M sequences," *IEICE Trans.*, vol.E74, no.10, pp.3024–3028, Oct. 1991

[3] A. Tsuneda, Y. Kuga and T. Inoue, "New maximal-period sequences using extended nonlinear feedback shift registers based on chaotic maps," *IEICE Trans. on Fundamentals*, vol.E85-A, no.6, pp.1327–1332, June 2002

[4] D. Yoshioka, A. Tsuneda and T. Inoue, "An Algorithm for the generation of maximal-period sequences based on one-dimensional chaos maps with finite bits," *IEICE Trans. on Fundamentals*, vol.E87-A, no.6, pp.1371–1376, June 2004

[5] C. Beck and F. Schlögl, Thermodynamics of chaotic systems: an introduction, Cambridge University Press, ch.3, 1993

[6] J. L. Massey and R. W. Liu, "Equivalence of nonlinear shift-registers," *IEEE Trans. on Inform. Theory*, pp.378–379, 1964.

[7] N. G. De Bruijn, "A combinatorial problem," Nederl. Akad. Wetensch. Proc. vol.49, pp.758–764, 1946