2005 RISP International Workshop on Nonlinear
Circuit and Signal Processing (NCSP'05)
Hawaii, USA, Mar. 4-6, 2005.

Run Test of Pseudo-Random Numbers Generated by Chaotic Maps

Yuki Nakaaji, Shuichi Aono and Yoshifumi Nishio

Deapartment of Electrical and Electronic Engineering,
Tokushima University
2-1 Minami-Josanjima, Tokushima 770-8506, Japan
TEL: +81-88-656-7470, FAX: +81-88-656-7471
Email: {nakaaji, aoichi, nishio}@ee.tokushima-u.ac.jp

1. Introduction

Pseudo-random numbers are useful for wide-ranging applications [1][2]. However, it is not easy to generate truely random numbers. There are several tests to investigate the randomness of limited amount of numbers; the frequency test, the run test, the random walk test, etc.

Recently, several researchers have investigated pseudo-random numbers generated from chaotic systems [3][4].

In this study, the run test is executed for the pseudo-random numbers generated by some chaotic maps, and the features of the run length of the pseudo-random numbers are investigated.

2. Chaotic Maps

We consider the cut map and the tent map as basic chaotic maps generating pseudo-random numbers.

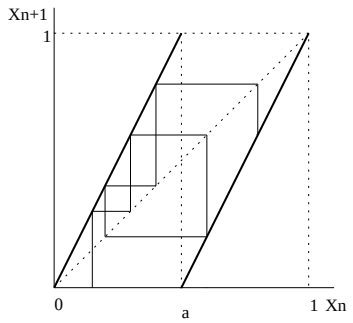

Figure 1: Cut map.

[Cut Map]

The cut map is shown in Fig. 1 and the equation of the map is given as

$$x_{n+1} = f_C(x_n) = \begin{cases} \dfrac{1}{a}x_n & (0 \le x_n \le a) \\ \dfrac{1}{1-a}x_n - \dfrac{a}{1-a} & (a < x_n \le 1). \end{cases} \tag{1}$$

The parameter a is usually chosen to be 0.5.

[Tent Map]

The tent map is shown in Fig. 2 and the equation of the map is given as

$$x_{n+1} = f_T(x_n) = \begin{cases} \dfrac{1}{a}x_n & (0 \le x_n \le a) \\ \dfrac{1}{1-a} - \dfrac{1}{1-a}x_n & (a < x_n \le 1). \end{cases} \tag{2}$$

The parameter a is usually chosen to be 0.5.

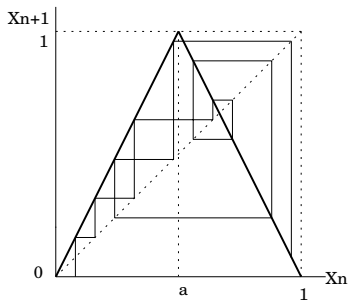

Figure 2: Tent map.

3. Run Test

The *runs* within a sequence is one of important statistics of pseudo-random numbers. A run is a monotonic subsequence; *Run up* is increasing subsequences and *Run down* is decreasing subsequences. The expected distribution of the number of

runs for a truly random sequence is known as follows [1].

$$r_d^* = \frac{2n(d^2+3d+1)}{(d+3)!} - \frac{2(d^3+3d^2-d-4)}{(d+3)!} \quad (3)$$

where r_d^* is the expected number of runs with the length d and n is the length of the total sequence. The expected distribution is compared against the sample distributions using the standard χ^2 formula.

We investigated the distributions of runs in pseudo-random numbers generated by the cut map and the tent map. Further, for comparison, we also investigated the sequence generated by *random()* function in FreeBSD C Library. As a result, the pseudo-random numbers generated by the cut map and the tent map do not pass the run test, though those from the random function pass.

In order to investigate the reason why the pseudo-random numbers generated by the chaotic maps do not pass the run test, we examin the distributions of the generated runs. Figures 3, 4 and 5 show the probability distribution function of the runs in the psudo-random numbers generated by the cut map, the tent map and the random function, respectively.

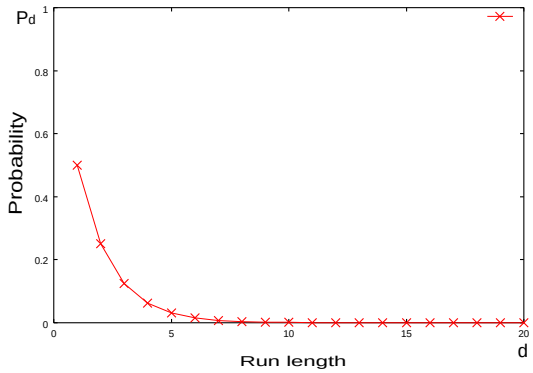

Figure 3: Distribution of runs (cut map).

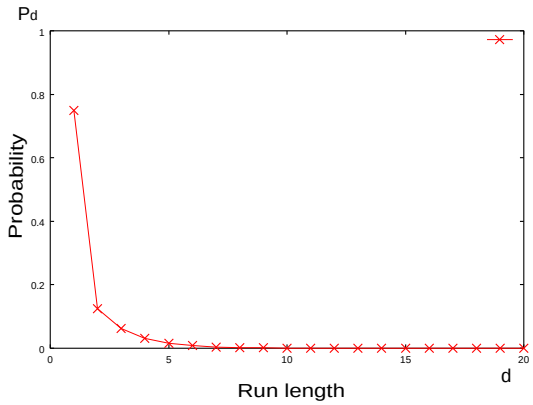

Figure 4: Distribution of runs (tent map).

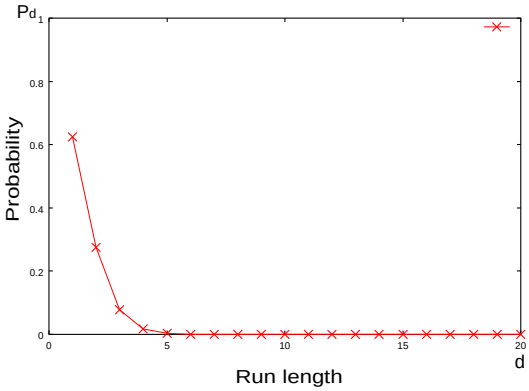

Figure 5: Distribution of runs (random function).

From the figures, we can see that the probability of length 1 for the cut map is smaller than that for the random function, while that for the tent map is larger than that for the random function. We consider that these are the special features of the corresponding chaotic maps.

4. Theoretical Analysis

In this section, we consider the theoretical analysis of the runs in the pseudo-random numbers generated by the chaotic maps.

The characteristic of the cut map generating runs is symmetric with respect to the center a as shown in Fig. 6. Namely, a run up with the length 1 is generated from an interval $[r1,\ a]$, and a run down with the length 1 is genarated from an interval $[a,\ r1']$. The values of $r1$ and $r1'$ can be calculated easily because the map is piecewise linear. Moreover, intervals generating runs with the length 2 are also calculated as $[r2,\ r1]$ and $[r1',\ r2']$. In the same way, intervals generating runs with the length d can be calculated. Hence, for the case of $a = 0.5$, the probability of runs generated by the cut map can be expressed as

$$P_d = \left(\frac{1}{2}\right)^d. \quad (4)$$

Figure 7 shows the theoretical probability distribution function of runs generated by the cut map, which is calculated from Eq. (5). The result in Fig. 7 agree well with the result in Fig. 3.

The characteristic of the tent map generating runs differs from the cut map, namely the tent map is not symmetric with respect to the center a as shown in Fig. 8. Namely, the length of all run down is equal to be 1 and they are generated from an interval $[r1',\ 1]$. Moreover, after every run up ends, the run down is generated without fail. Considering this feature, the probability of runs generated by the tent map with $a = 0.5$

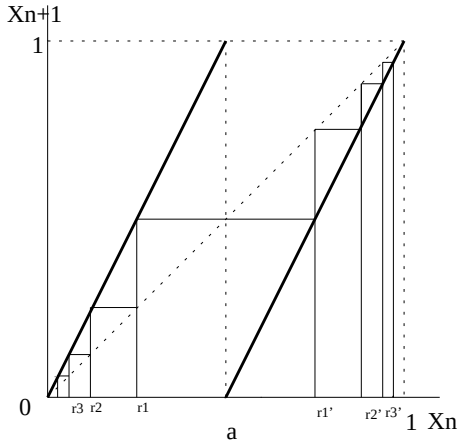

Figure 6: Generation of runs (cut map).

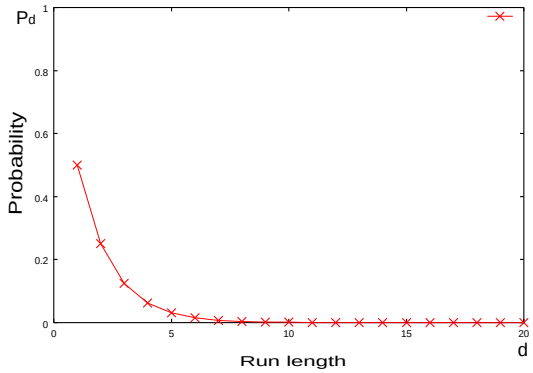

Figure 7: Theoretical distribution of runs (cut map).

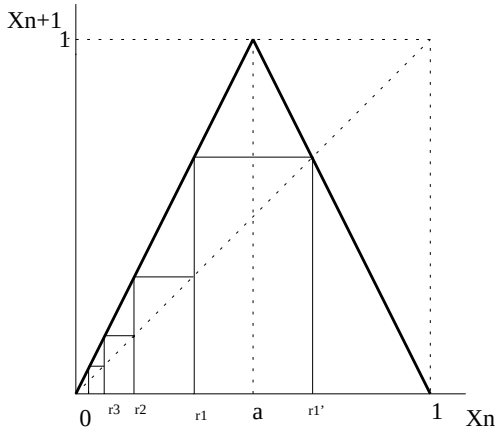

Figure 8: Generation of runs (tent map).

can be expressed as

$$\begin{aligned} P_1 &= \left(\frac{1}{2}\right)^2 + \frac{1}{2} \\ &\vdots \\ P_d &= \left(\frac{1}{2}\right)^{d+1}. \end{aligned} \tag{5}$$

Figure 9 shows the theoretical probability distribution function of runs generated by the tent map, which is calculated from Eq. (6). The result in Fig. 9 agree well with the result in Fig. 4.

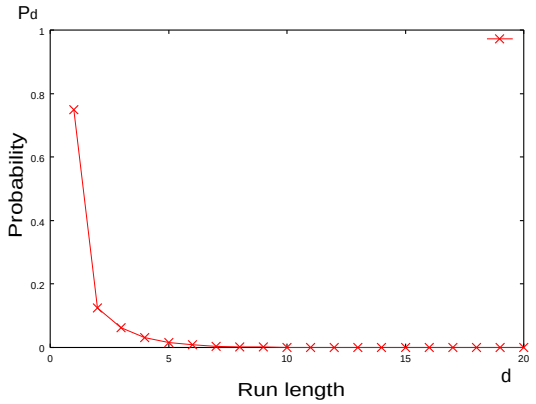

Figure 9: Theoretical distribution of runs (tent map).

From the above theoretical analysis, we can understand that the distributions of runs generated by chaotic maps depend on the characteristics of the maps. This is why the psudo-random numbers generated by chaotic maps do not pass the run test. However, we consider that this is an advantage of chaotic maps as pseudo-random number generators, because they could produce colored pseudo-random numbers.

5. Further Examples

5.1. Composite Maps

In this section we consider the composite maps of the cut map as a pseudo-random number generator. Because some random functions in computer libraries passing the run test use the linear congruential method and the method uses a similar function to the composite maps of the cut map.

Figure 10 shows the composite maps of the cut map and the probability distribution function of runs of pseudo-random numbers generated by the corresponding composite maps.

We can see that the distribution becomes closer to that of the random function, as the composite number increases. Further, we excute the run test for the pseudo-random numbers generated by the composite map. As a result, the

pseudo-random numbers generated by the composite maps in Figs. 10(a), (b) and (c) do not pass the testm but the pseudo-random number generated by Fig. 10(d) pass the test.

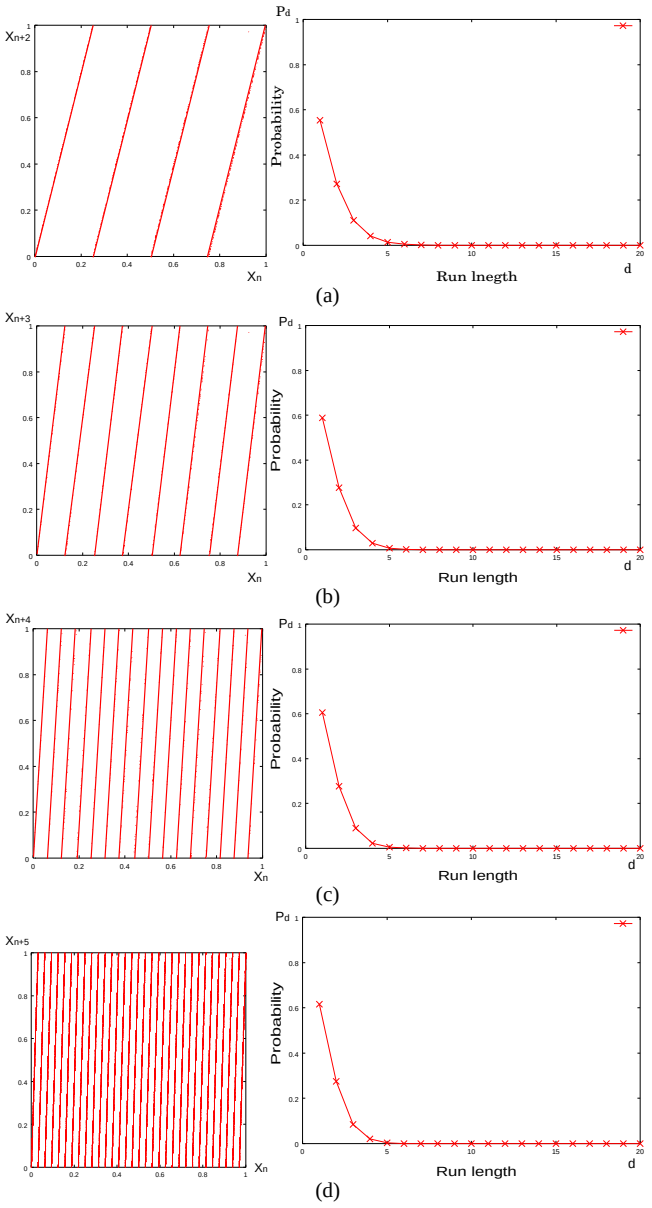

Figure 10: Composite maps and the distribution of runs. (a) Two times composite. (b) Three times composite. (c) Four times composite. (d) Five times composite.

5.2. Asymmetric Maps

Next, we consider the effect of changing the value of a. Figure 11(a) shows the map for the case of $a = 0.8$ and Fig. 11(b) shows the probability distribution function of runs of pseudo-random numbers generated by the cut maps with different values of a. The theoretical distribution of runs can be calculated as

$$P_d = \frac{1}{2}a^{d-1}(1-a) + \frac{1}{2}a(1-a)^{d-1} \tag{6}$$

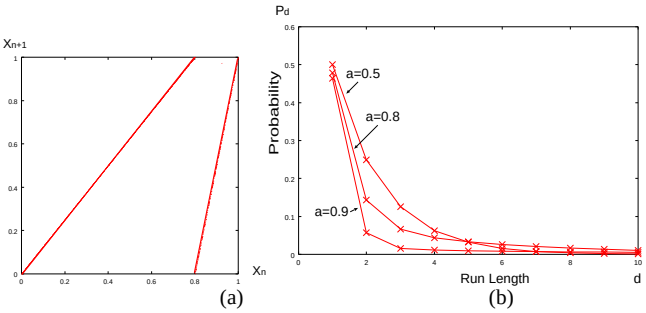

Figure 11: (a) Cut map with $a = 0.8$. (b) Distribution of runs (cut map with different a).

6. Conclusions

In this study, the run of the pseudo-random numbers generated by the chaotic maps was tested, and the reason why the generation probability of the length of the run was different from truly random numbers was clarified theoretically. Further, various characteristics of the runs generated by chaotic maps were investigated.

References

[1] O. Miyatake and K. Wakimoto, “Random Number and Monte Carlo Method,” Morikita Shuppan Co., 1978.

[2] D.E. Knuth, “Art of Computer Programming, Volume 2: Seminumerical Algorithms, 3rd Edition,” Addison-Wesley, 1997.

[3] S. Kawamura, H. Yoshida and M. Mimura, “Characteristics of Pseudo-Random Numbers Generated by Chaos Nural Networks,” Technical Report of IEICE, vol. NLP2004-6, pp. 29-34, 2004.

[4] M.E. Yalcin, J.A.K. Suykens and J. Vandewalle, “True Random Bit Generation from a Double-Scroll Attractor,” IEEE Trans. on Circuits Syst. I, vol. 51, no. 7, pp. 1395-1404, 2004.