ISSN 1392 – 1215 ELEKTRONIKA IR ELEKTROTECHNIKA. 2004. Nr. 7(56)

T 191 AUKŠTŲJŲ DAŽNIŲ TECHNOLOGIJA, MIKROBANGOS

Reconsidering the Generalized Logistic Map as a Pseudo Random Bit Generator

R. Ursulean

Faculty of Electrical Engineering, "Gh.Asachi" Technical University
Bd. D. Mangeron 53, Iasi 700050, Romania, e-mail: ursulean@ee.tuiasi.ro

Introduction

Due to the need of secure communications, no matter the type of the channel used, recent trends in cryptology are focused on the possibilities that chaotic maps can offer as pseudo random bit generators.

The opportunity to generate pseudo random bits from some discrete chaotic maps was under investigation and a review of the recent developments was published in [1]. Nevertheless, a general method to fit every discrete chaotic map cannot be yet developed in spite of some attempts [2], [3], that gave some useful suggestions.

These principles can be viewed as useful hints to develop new criteria in pseudo random bit generators based on discrete chaotic maps.

The logistic map is one of the most studied discrete chaotic maps. It was first proposed as pseudo random number generator by von Neumann in 1947 partly because it had a "known algebraic distribution" and mentioned later, in 1969, by Knuth. It is given by

$$x_{n+1} = r x_n (1 - x_n) \tag{1}$$

and is supposed to have good qualities as pseudo random number generator [1], [4], [5] when $r = 3.9 \div 4$ and its behaviour is chaotic.

A decision criterion for pseudo random bit generators

Since the probability density function of the pseudo random bits must be the uniform one, it is necessary to establish a certain level in order to decide, from the relation that gives the discrete chaotic map, for which x_n a zero or a one is generated. For the distributions that have symmetrical probability density functions there is a clear answer: choosing the mean of the x_n values will assure the generating of the same numbers of bits according to the following formula:

$$b_n = \begin{cases} 0 & x_n \le \bar{x} \\ 1 & x_n > \bar{x} \end{cases}, \tag{2}$$

where $\bar{x}$ denotes the mean value and b_n is the bit generated by the n-th iteration of the map.

Another possibility is to choose the middle of the interval between the minimum and the maximum of the generated values, [6], but unfortunately this works only if the function is symmetrical.

In fact, when symmetrical probability density functions are involved, it is easy to show that the mean value is identical with the median, the value that splits the probability density function into two equally filled regions and with the middle of the interval. A true indicator for symmetrical distributions is the skewness, which is zero in this case.

From the point of view of the discrete chaotic maps used as pseudo random bit generators it is important that the co-domain of the mapped function to be symmetrical, but this usually doesn't happen. In what follows we shall consider the important observation that the median is the most suitable statistical characteristic that may split the domain into two equally filled sub domains and in this way one can achieve the goal of equal numbers of zero and one bits. Because of this statement, the criterion for generation of a one or a zero bit (2) becomes

$$b_n = \begin{cases} 0 & x_n \le med \\ 1 & x_n > med \end{cases}, \tag{3}$$

where *med* denotes the median of the values generated by the discrete chaotic map.

Let us see the difference between the two ways of generating pseudo random bits using the generalized logistic map

$$x_{n+1} = (\beta + 1)\left(1 + \frac{1}{\beta}\right)^{\beta} x_n (1 - x_n), \tag{4}$$

with $x_0 \in [0,1]$ and $\beta \in [1,4]$, whose graphic image is presented in Fig.1 for $\beta = 3$.

It is clearly seen that the map is not symmetric and the middle of the interval is 0.5 (since all the values are between 0 and 1). The results of 20,000 bits generation for different values of β and the statistical indicators are summarized in the Table 1.

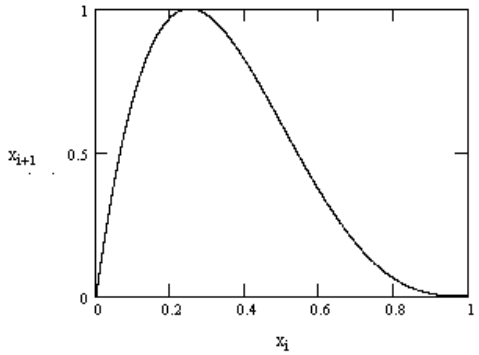

Fig. 1. The generalized logistic map, $x_i \in [0;1]$, for β=3

Table 1. Statistical indicators and 0 and 1 bit count for the generalized logistic map in [0,1] interval

		$\beta = 1$	$\beta = 2$	$\beta = 3$	$\beta = 4$
mean		0.348	0.358	0.282	0.238
median		0.348	0.212	0.08	0.03
skewness		0.0002	0.564	0.936	1.185
0	mean	10028	11699	12873	13595
	median	10000	10000	10000	10000
	middle	10027	13132	14703	15512
1	mean	9972	8301	7127	6405
	median	10000	10000	10000	10000
	middle	9973	6868	5297	4488

The above results show that the use of the mean and the middle of the interval are not suitable since the number of bits that are generated differ significantly. It is also worth noticing the fact that as β increases, the difference between the mean and the median is significant and also is the difference between the number of the bits 0 and 1 that are generated by the map.

This situation changes dramatically if we consider a much narrower interval to generate the map. To make things more clear, let us consider the above case, with β in the same range, but with a much narrower interval, let this be [0.3;0.4]. It is easy to understand that we shall generate the entire map and choose only the values belonging to this interval; therefore, the time needed to get the numbers is slightly longer.

From the statistical point of view, the skewness is not significant since its value is so close to zero and the values of the median and the mean are different by 0.1. It is as well easy to notice that the number of bits of each kind are almost equal, no matter which statistical indicator was used, the mean, the median or the middle of the interval, as indicated in Table 2.

The problem appears elsewhere: let us take a closer look at the generated numbers by screening some of them for different values of β, as in Figs. 2 to 4. This procedure, suggested in [7], is a good indicator when one is able to "magnify" the map, plotted as two-dimensional consecutive values.

These figures clearly show that, except for β=2, there are spaces that are not filled and this puts in doubt the quality of the numbers, even for well established cases (β=1), where the map should behave as an random number generator with uniform distribution.

Table 2. Statistical indicators and 0 and 1 bit count for the generalized logistic map in [0.3,0.4] interval

		$\beta = 1$	$\beta = 2$	$\beta = 3$	$\beta = 4$
mean		0.349	0.349	0.349	0.349
median		0.349	0.349	0.348	0.348
skewness		0.019	0.048	0.047	0.036
0	mean	10070	10085	10075	10092
	median	10000	10000	10000	10000
	middle	10193	10304	10364	10344
1	mean	9930	9915	9925	9908
	median	10000	10000	10000	10000
	middle	9807	9696	9636	9656

Therefore, much testing will be needed to be able to decide in each case if the quality of the numbers is the one that was expected.

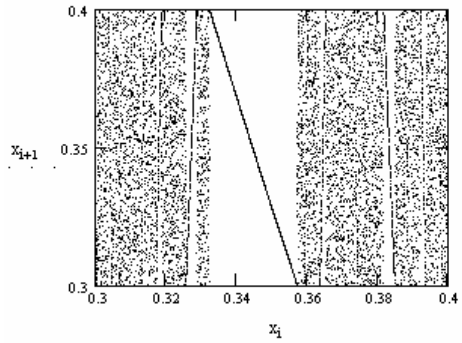

Fig. 2. The generalized logistic map, $x_i \in [0.3;0.4]$, for β=1

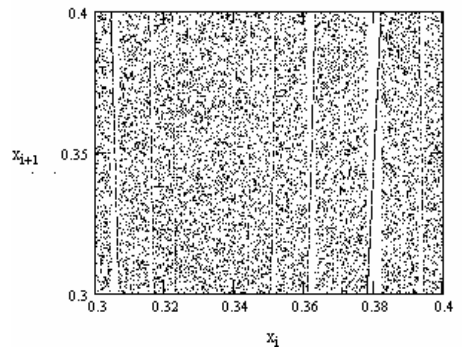

Fig. 3. The generalized logistic map, $x_i \in [0.3;0.4]$, for β=2

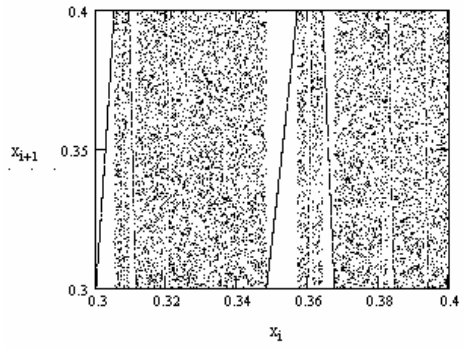

Fig. 4. The generalized logistic map, $x_i \in [0.3;0.4]$, for β=4

A brief review of the statistical tests for bit sequences

To test the validity of our initial supposition, that narrowing the interval will led to better quality of the numbers (because in this case the median and the mean will have virtually the same value), we must recall the standard [8], whose requirements are reviewed in brief in what follows.

The standard is taking into account sequences of 20,000 bits that must pass four statistical tests: the Monobit Test, the Poker Test, the Runs Test and the Long Runs Test.

The Monobit Test is projected to evidence if the number of ones and zeros are nearly equal; the standard specify the value of the number of ones to be somewhere between 9,654 and 10,346 in order to pass it.

The Poker Test requires the dividing of the initial sequence into 4 bit contiguous segments, the counting and the storing of each of the 16 possible 4 bit values. Denoting as *f(k)* the number of each value, $0 \le k \le 15$, the *X* statistic is computed by means of the formula (5):

$$X = \frac{16}{5000}\left(\sum_{k=0}^{15}(f(k))^2\right) - 5000\,. \qquad (5)$$

The test is passed only if $X \in [1.03;57.4]$.

If we describe a run as the maximal sequence of consecutive bits of the same kind then the incidence of runs (for both consecutive zeros and consecutive ones) of all lengths between 1 and 6 in the sample stream should be in the corresponding interval specified in the following table.

Table 3. The number of occurrences for each length of consecutive bits of the sequence

Length	1	2	3	4	5	6&6+
Number of occurrences	2,267 ÷ 2,733	1,079 ÷ 1,421	502 ÷ 748	223 ÷ 402	90 ÷ 223	90 ÷ 223

It is worth noticing the fact that the sequences longer than 6 are considered of length 6 when counting them. The test is passed if for the generated sequence the number of consecutive bits of each length is between the limits given in Table 3.

The Long Runs Test is proposed to get rid of those sequences that have long runs greater than 34.

Testing the generalized logistic map as a pseudo random bit generator

First, the histogram of the frequencies of the initial data was computed; no matter the value for β, there were obtained histograms like the one in Fig. 5, distinctive for uniform probability density function.

The map was first generated for several initial values knowing the sensitivity to initial condition of the chaotic maps. From the statistical point of view no noteworthy changes have been recorded, as can be seen from the following results, presented in Table 4.

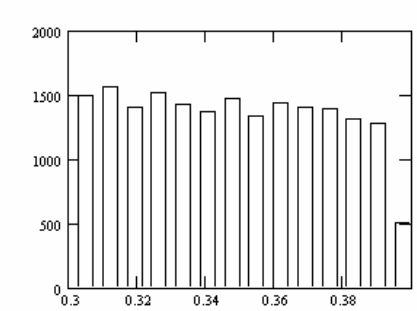

Fig. 5. The histogram of the real numbers generated by the generalized logistic map, $x_i \in [0.3;0.4]$, for β=2

Table 4. The statistical indicators and the representative values of the tests for three different initial values of the generalized logistic map for β=2 and the interval [0.3;0.4]

Initial value		$x_0 = 0.1$	$x_0 = 0.5$	$x_0 = 0.9$
Mean		0.349	0.349	0.349
Median		0.348	0.349	0.349
Standard dev.		0.029	0.029	0.029
Monobit Test		10000	10000	10000
Poker Test		7.725	2.822	6.227
Runs Test	1	2547	2517	2474
	2	1204	1245	1224
	3	622	653	620
	4	303	314	299
	5	152	148	155
	6&6+	162	150	183
Long Run Test	**0**	11	11	11
	1	12	11	11

As a general remark the sequence generated by the initial condition $x_0 = 0.5$ led significantly to the best results for the Poker Test.

Let us now consider the different values for the β parameter and do the similar testing, this time considering the same initial condition $x_0 = 0.51$. The initial condition needs to be slightly different than 0.5 since for this value and $\beta = 1$ the map won't behave chaotically, as it can be seen from (4). The results of the simulations are those in Table 5.

Table 5. The statistical indicators and the values of the tests for different values of the β parameter of the generalized logistic map in the interval [0.3;0.4]

		$\beta = 1$	$\beta = 3$	$\beta = 4$
Mean		0.349	0.349	0.349
Median		0.349	0.348	0.349
Standard dev.		0.029	0.029	0.029
Monobit Test		10000	10000	10000
Poker Test		315.84	34.259	3.706
Runs Test	1	3065	2601	2488
	2	1347	1249	1212
	3	597	610	629
	4	219	300	310
	5	101	125	143

	6&6 +	57	159	165
Long Run Test	0	9	11	13
	1	11	11	11

The shaded areas in Table 5 indicate that the sequence failed the test and this happened only for the case $\beta = 1$.

Conclusion

The statistical tests carried out for the generalized logistic map in the case of narrow intervals surprisingly showed that, except for the usual value of the β parameter, β=1, when considering the median as the decision criterion, the map could be a source of pseudo random bits and the sequences pass the usual tests for this kind of bit streams.

References

1. **Shujuan l., Huanquin M., Yuanlong C.** Pseudo Random Bit Generator Based on Couple Chaotic Systems and its Applications In Stream-Chipher Cryptography // Proceedings of "Progress in Cryptology", "INDOCRYPT 2001", Chennai. – P. 316–329.
2. **Szcepanski J., Kotulski Z.,** Chaotic Pseudorandom Generators Based on Chaotic Dynamical Systems // Open Sys. & Information Dyn., 2000. – 7. – P. 1–10.
3. **Kotulski Z., Szcepanski J.** Application of Discrete Chaotic Dynamical Systems in Cryptography - Dcc Method // Int. J. Bifurcation and Chaos, 1999. – 9. – P. 1121–1135.
4. **Kocarev L., Jakimoski G.,** Logistic Map as a Block Encryption Algorithm // Physics Letters A, 2001. – 289. – P.199–206.
5. **Baptista M.S.** Cryptograpy with Chaos // Physics Letters A, 1998. – 240. – P. 50–54.
6. **Kotulski Z., Szcepanski J., Gorski K., Gorska A., Paszkiewicz A.** On Constructive Approach to Chaotic Pseudorandom Number Generators // Proc. Of "RCMCIS '2000", Zegrze. – P. 191–203.
7. **Janke W.** Pseudo Random Numbers: Generation and Quality Checks / in Quantum Simulations of Complex Many-Body Systems: From Theory to Algorithms // John von Neumann Institute for Computing, NIC Series, 2002. – Vol. 10. – P. 447–458.
8. **Security** Requirements for Cryptographic Modules // FIPS PUB 140-1, U.S. National Institute of Standards and Technology, 1994.

Pateikta spaudai 2004 09 04

R. Ursulean. Pseudoatsitiktinių bitų generatoriaus loginės schemos sudarymo įvertinimas // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2004. – Nr. 7(56). – P. 10–13.

Aprašomos loginės schemos vartojimo galimybės, akivaizdžiai įrodančios nesugebėjimą formuoti vienarūšius pseudoatsitiktinio signalo skaičius. Tokių skaičių resursas įvertinamas tam tikrais apribojimais. Tuo atveju, kai tai įmanoma, įrodoma, kad statistinių testų panaudojimo rezultatai yra atskleidžiami. Pseudoatsitiktinių bitų generatorius įvertinamas statistiniais testais ir yra tinkamas kriptografiniams algoritmams optimaliai sudaryti. Aprašomos trys sąlygos, leidžiančios atlikti šį veiksmą: skaičių išsidėstymas turi būti vienodas; vienetų ir nulių skaičius turi būti reliatyviai vienodas; vienetų ir nulių skaičius neturi viršyti nustatytų ribų. Il. 5, bibl. 8 (anglų kalba; santraukos lietuvių, anglų ir rusų k.).

R. Ursulean. Reconsidering the Generalized Logistic Map as a Pseudo Random Bit Generator // Electronics and Electrical Engineering. – Kaunas: Technologija, 2004. – No. 7(56). – P. 10-13.

The purpose of the paper is to evidence the possibilities to use the generalized logistic map, known until now for its inability to generate uniform pseudo random numbers, as a source for such numbers when certain restriction have been imposed. The cases when this is possible are shown and the results of the statistical tests applied for to the numbers are revealed. A good pseudo random bit generator must pass certain statistical tests to be a good candidate for cryptographic algorithms. There are three principles that are crucial for such a task and we shall remind them in brief: the distribution of the numbers must be uniform; the number of ones and zeros must be relatively equal and the number of long sequences of ones and zeros must not exceed certain, well established, limits. Ill. 5, bibl. 8 (in English; summaries in Lithuanian, English and Russian).

Р. Урсулеан. Оценка формирования генератора логической схемы псевдослучайных битов // Электроника и электротехника. – Каунас: Технология, 2004. – №. 7(56). – С. 10-13.

Описываются возможности применения логической схемы, когда невозможно генерировать однозначные цифры псевдо сигналов. Оцениваются ресурсы таких цифр при определенных ограничениях. В случаях, когда это возможно, доказывается, что при помощи статических тестов есть возможность полностью открыть результаты использования. Доказано, что генераторы псевдослучайных битов оцениваются статистическими тестами и показано, что они используются для составления оптимальных криптографических алгоритмов. Приводятся три условия, позволяющие выполнить данную операцию: распределение цифр должно быть одинаковым; число единиц и нолей относительно одинаковым; число единиц и нолей не превышать ограниченных пределов. Ил. 5, библ. 8 (на английском языке; рефераты на литовском, английском и русском яз.).

DOI: 10.5755/j02.eie.10884