Journal of Computational and Applied Mathematics 235 (2011) 3455–3463

Contents lists available at ScienceDirect

Journal of Computational and Applied Mathematics

journal homepage: www.elsevier.com/locate/cam

A novel dynamic model of pseudo random number generator

S. Behnia [a,*], A. Akhavan [b], A. Akhshani [c,d], A. Samsudin [b]

[a] Department of Physics, Urmia University of Technology, Orumieh, Iran
[b] School of Computer Sciences, Universiti Sains Malaysia, 11800 USM, Penang, Malaysia
[c] Department of Physics, IAU, Orumieh Branch, Orumieh, Iran
[d] School of Physics, Universiti Sains Malaysia, 11800 USM, Penang, Malaysia

ARTICLE INFO

Article history:
Received 2 August 2009
Received in revised form 4 February 2011

Keywords:
Chaotic function
Pseudo random sequence
Ergodic theory
Invariant measure
Perron–Frobenius operator

ABSTRACT

An interesting hierarchy of random number generators is introduced in this paper based on the review of random numbers characteristics and chaotic functions theory. The main objective of this paper is to produce an ergodic dynamical system which can be implemented in random number generators. In order to check the efficacy of pseudo random number generators based on this map, we have carried out certain statistical tests on a series of numbers obtained from the introduced hierarchy. The results of the tests were promising, as the hierarchy passed the tests satisfactorily, and offers a great capability to be employed in a pseudo random number generator.

1. Introduction

A random number generator is a critical component in modern cryptographic systems, communication systems, statistical simulation systems and any scientific area incorporating Monte Carlo methods [1,2] and many others. In the present era, there are few scientific fields that do not use random number generators. One of the most important applications of random number generators is in cryptography to generate cryptographic keys, and to randomly initialize certain variables in cryptographic protocols. Moreover, practical implementation of digital Fountain codes such as LT codes uses a pseudo random number generator to determine the degree and neighbors of an encoding symbol [3]. In [4] the pseudo randomness of chaotic sequence is applied in the encoding of LT codes. The obtained results showed that the implemented LT codes based on chaos can perform as well as the LT codes implemented by the traditional pseudo random number generator [4]. Recently, some efficient techniques for encoding based on discrete time chaotic systems are presented in [5,6]. A good random number generation improves the cryptographic security [7].

Random number generators can be classified in three classes; true random number generators, pseudo random number generators (PRNG) and hybrid random number generators. Pseudo random number generators are deterministic processes which generate a series of outputs from an initial seed state [8–10]. In this paper, we categorize pseudo random number generators as a subset of rational order families of chaotic maps with an invariant measure. An accomplishment of these chaotic maps is in their potential to simultaneously produce and use entropy [11]. Additionally, as they are measurable dynamical systems, they can be studied analytically. To ensure that a random number generator is secure, its output must be statistically proven unpredictable and indistinguishable from a true random sequence [8].

2. Rational order of chaotic maps

In this section, we firstly give a brief introduction about hierarchy of one-parameter chaotic maps which can be used in the construction of rational order chaotic maps with an invariant measure. One-parameter families of chaotic maps can be

* Corresponding author.
E-mail address: s.behnia@mee.uut.ac.ir (S. Behnia).

0377-0427/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.cam.2011.02.006

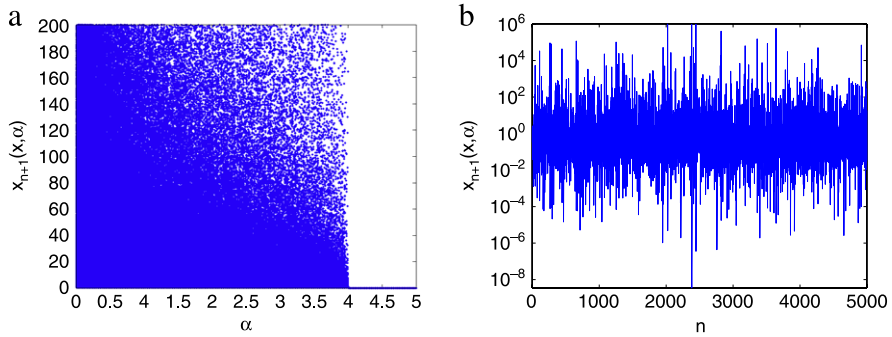

Fig. 1. (a) Bifurcation diagram of chaotic map Eq. (5); for $\alpha \in (0.5, \infty)$, it is ergodic and for $\alpha \in (0, .5)$, it has stable fixed point at $x = 0$. (b) Time series of selected example Eq. (5) while $\alpha = 1.5$.

defined as the ratio of polynomials of degree N (see [11] for more detail):

$$x_{n+1}(x, \alpha) = \frac{\alpha^2 F}{1 + (\alpha^2 - 1)F}, \tag{1}$$

where α is the control parameter that can potentially be used as the secret key for secure communication [7]. F is a substitute for Chebyshev polynomial of first kind with degree N: $T_N(x)$. Hence

$$x_{n+1}(x, \alpha) = \frac{\alpha^2 (T_N(\sqrt{x}))^2}{1 + (\alpha^2 - 1)(T_N(\sqrt{x}))^2}, \tag{2}$$

where N is an integer greater that 1 and all points lay in the bounded [0, 1] interval. It is shown that these maps have interesting properties, such as, for even values of N the $x_{n+1}(x, \alpha)$ maps have only one fixed point attractor $x = 1$ provided that α belongs to the interval (N, ∞), while at $\alpha \geq N$ they bifurcate to a chaotic regime without having any period doubling or period-n-tupling scenario and remain chaotic for all $\alpha \in (0, N)$. However for odd values of N, these maps tend to have a single fixed point attractor at $x = 0$. For $\alpha \in (\frac{1}{N}, N)$ again, they bifurcate to a chaotic regime since $\alpha \geq \frac{1}{N}$, and remain chaotic for $\alpha \in (0, \frac{1}{N})$ and finally they bifurcate at $\alpha = N$ to have $x = 1$ as fixed point attractor for all $\alpha \in (\frac{1}{N}, \infty)$ (see Figs. 1(a) and (b)). Here in this paper, we are concerned about their conjugate maps which are defined as:

$$\tilde{x}_{n+1}(x, \alpha) = h \circ x_{n+1}(x, \alpha) \circ h^{-1} = \frac{1}{\alpha^2} \tan^2(N \arctan \sqrt{x_n}). \tag{3}$$

Conjugacy means that invertible map $h(x) = \frac{1-x}{x}$, maps $I = [0, 1]$ into $[0, \infty)$ [12]. Of course, the function given in Eq. (2) is not the only choice leading to the hierarchy rational order of chaotic maps with invariant measure. Obviously, the following choices of the functions also lead to the hierarchy of chaotic maps of trigonometric types (with an invariant measure):

$$\begin{array}{ll} \bullet \frac{1}{\alpha^2} \tan^2(N\text{arccot}\sqrt{x}), & \diamond \frac{1}{\alpha^2} \cot^2(N\text{arccot}\sqrt{x}), \\ \bullet \frac{1}{\alpha^2} \cot^2\left(N \arctan \frac{1}{\sqrt{x}}\right), & \diamond \frac{1}{\alpha^2} |\cot^2(N\text{arccot}\sqrt{x})|, \\ \bullet \frac{1}{\alpha} |\tan(N \arctan |x|)|, & \diamond \frac{1}{\alpha} |\tan(N\text{arccot}|x|)|, \\ \bullet \frac{1}{\alpha} |\cot(N \arctan |x|)|, & \diamond \frac{1}{\alpha} |\cot(N\text{arccot}|x|)|. \end{array} \tag{4}$$

In this paper, the following chaotic map Eq. (5) is used to design a new pseudo random number generator algorithm

$$\tilde{x}_{n+1}(x, \alpha) = \frac{1}{\alpha^2} \tan^2(N \arctan \sqrt{x_n}) \tag{5}$$

while $N = 4$. Also it is possible to use composition of these chaotic maps as a pseudo random number generator too [12].

3. Ergodic dynamical system

"Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we believe that it is a mystery into which the mind will never penetrate" (Leonhard Euler) [13]. This is a representative description for the complexity of prime distribution. But according to the famous "Langlands program", a difficult problem in one area could always be converted into an easy problem in other areas. Many recent efforts on this topic are all cross researches of number theory, dynamical systems theory, statistical theory and ergodic theory, etc. [8,9].

The probabilistic dynamical system is characterized as ergodic or non-ergodic by its marginal probability distributions. If the distributions have infinite variances, so that a process-mean cannot be defined, the system is called non-ergodic. An ergodic system has "convergent" qualities over time, variances are finite and a time-independent process-mean is clearly defined. For ergodic systems, the time average is equal to the space (or phase) average [13]. Also, from the viewpoint of estimating complexity, ergodic dynamical systems are most important because according to the Birkhoff ergodic theorem many properties of such systems can be reconstructed from a single orbit with probability one. On other hand, the invariant measure which is not equal to zero or one, appears to be characteristic of non-ergodic behavior. Consequently, studies based on invariant measure analysis can be useful for confirming the ergodicity behavior of a map. Therefor, we first have to prove that our system is ergodic.

3.1. Invariant measure

Invariant measure or the stationary density [14] provides a useful way to study the asymptotic behavior of dynamical systems. It starts with a distribution of the initial conditions and studies their evolution as time goes towards the infinity. It is interesting to note that even for chaotic dynamical system, there usually exist a well behaved limit which can be used to study various average properties. There are various methods to find invariant measures. One of the approaches is called Perron–Frobenius (PF) operator. When this operator acts on $\mu(x)$, the density at the n-th time step, yields to the density at the $(n+1)$-th time step.

If an initial point x is chosen using a probability distribution with density $\mu(x)$, the $L\mu(x)$ will be the density for $x_{n+1}(x, \alpha)$.

$$\mu(y) = \int_0^1 \delta\left(y - x_{n+1}(x, \alpha)\right) \mu(x) \mathrm{d}x. \tag{6}$$

This is equivalent to $\mu(y) = \sum_{x \in x_{n+1}^{-1}(y,\alpha)} \mu(x) \frac{\mathrm{d}x}{\mathrm{d}y}$. The action of *PF* operator L for the map is defined as [15]:

$$Lf(y) = \sum_{x \in x_{n+1}^{-1}(y,\alpha)} f(x) \frac{\mathrm{d}x}{\mathrm{d}y}. \tag{7}$$

The invariant probability measure, $\mu(x)$, is the eigenstate of the *PF* operator, L, related to maximum eigenvalue 1. We have already derived an analytically invariant measure for One-parameter families of chaotic maps, Eq. (1), by using arbitrary values of the control parameter α, for each integer value of N [11]. Assuming that $\mu(x)$ has the following form:

$$\mu(x) = \frac{\sqrt{\beta}}{\pi(1 + \beta x^2)},$$

$$\mu(x) = \frac{1}{\pi} \frac{\sqrt{\beta}}{\sqrt{x(1-x)}(\beta + (1-\beta)x)} \tag{8}$$

with $\beta > 0$ the invariant measure of the maps will be $\tilde{x}_{n+1}(x, \alpha)$ provided that we choose the parameter α in the following form:

$$\alpha = \frac{\sum_{k=0}^{[\frac{N-1}{2}]} C_{2k+1}^N \beta^{-k}}{\sum_{k=0}^{[\frac{N}{2}]} C_{2k}^N \beta^{-k}}, \tag{9}$$

while N represents the odd values. If N takes even values, we would have the following equation:

$$\alpha = \frac{\beta \sum_{k=0}^{[\frac{N}{2}]} C_{2k}^N \beta^{-k}}{\sum_{k=0}^{[\frac{N-1}{2}]} C_{2k+1}^N \beta^{-k}}. \tag{10}$$

The symbol [ ] shows the greatest integer part. For the map that is used in this paper, $\tilde{x}_{n+1}(x, \alpha) = \frac{1}{\alpha^2} \tan^2(N \arctan \sqrt{x})$, the invariant measure is derived and the calculations are mentioned in Appendix.

3.2. Lyapunov exponent

A useful numerical way to describe chaotic behavior in dynamical systems is by means of the Lyapunov exponents that explain the separation rate of systems whose initial conditions differ by a small perturbation.

There is a close correlation between the Lyapunov exponent of the underlying chaotic map and the "randomness". Since randomness is desired to be seen clearly on a random number generator, it must be correlated to the diverging nature of

the trajectories of a chaotic map, which is tied to the existence of a positive Lyapunov exponent. It is natural to investigate just how good the correlation is. As we know, each dynamical system has specific characteristics. The following properties make a deterministic algorithm suitable to generate a pseudo random sequence of numbers: high value of entropy, high dimensionality of the parent dynamical system and very large period of the generated sequence [16–18]. In fact, the differences between discrete dynamical systems arise from these properties. By considering both bifurcation and Lyapunov exponent diagrams, it can be concluded that the presented dynamical systems are fully chaotic on the defined interval. Actually, in these dynamical systems, bifurcation is without any period doubling. In other words, bifurcation, from a stable single periodic state to chaotic one, does not have usual period doubling or period-n-tupling scenario. This point makes these dynamical systems distinctive and advantageous compared to the other dynamical systems. Taking into account that these dynamical systems are fully chaotic on the defined interval, it seems that calculation of discrete Lyapunov exponent may be avoided at the moment. Thus, the calculation of Lyapunov exponent is presented in general form. The Lyapunov exponent can be expressed as:

$$\lambda(x_0) = \lim_{n\to\infty} \sum_{i=0}^{n-1} \left| \frac{\mathrm{d}x_{n+1}(x_i)}{\mathrm{d}x_i} \right|. \tag{11}$$

where $x_i = x_{n+1}^i(x_0)$. In the case of a chaotic map, except for a set of zero measure, the Lyapunov exponent does not depend upon x_0. If the map is ergodic with respect to an invariant measure-μ, the Lyapunov exponent expressed as a time average can also be expressed by the space average. We have simulated Lyapunov exponent of introduced hierarchy for different values of α in order to distinguish the suitable domain of control parameter for random number generation process (see Fig. 2). Increasing the values and the number of positive Lyapunov exponents makes the probability distributions of the output chaotic sequences more homogeneous and reduces the correlations of chaotic outputs for different times and different space units. The main result provides a necessary and sufficient condition for the introduced model to have ergodicity.

4. Statistical complexity

Statistical complexity has reflects intricate structures hidden in the dynamics, emerging from a system which itself is much simpler than its dynamics. Specifically, complexity measures were developed and refined that quantify the degree of randomness and unpredictability generated by dynamical systems. The quantification of complexity is an important topic in the theory and application of dynamical systems. In essence, they are simply alternatives to measuring the same property-degrees of randomness. The measure of complexity C recently introduced in [19–21], the so-called *LMC* complexity, is defined as

$$C = H.D \tag{12}$$

where H represents the information content of the system and D is its disequilibrium. The disequilibrium D of a system can be taken as some kind of distance to an equiprobable distribution. Following the discussion in the introduction the definition of *LMC* complexity C is given by the formula [20]:

$$C(p_i) = H(p_i).D(p_i) = -k\left(\sum_{i=1}^{N} p_i \log p_i\right) \cdot \left(\sum_{i=1}^{N} \left(p_i - \frac{1}{N}\right)^2\right), \tag{13}$$

$$\bar{C}(x) = \bar{H}(x).D(x) = -\frac{1}{\log 2}\left[x \log\left(\frac{x}{1-x}\right) + \log(1-x)\right].2\left(x - \frac{1}{2}\right)^2 \tag{14}$$

where p_i, with $p_i \geq 0$ and $i = 1, 2, \ldots, N$, represents the distribution of the N accessible states to the system, and k is a constant.

Based on the calculations mentioned above, in Fig. 3 the complexity measure for the proposed map is drawn compared to the logistic map. Apparently, the presented dynamical system has good properties from the complexity point of view.

5. Randomness in deterministic chaos

Theory of chaos, a subfield of nonlinear dynamical systems, has suggested that low-dimensional dynamical systems may manifest complex and unpredictable behaviors. The existence of complexity and random behavior of the chaotic maps motivates the idea of using chaotic maps in designing pseudo random number generators.

5.1. Definition of random number generator

Pseudo random number generators are deterministic processes that take M bits as an input, often referred to as key (or seed) and expand it into an infinitely large sequence of K bits output. The generation of these random numbers uses entropy obtained from another source, which might be hard-ware or perhaps unpredictable system processes. According

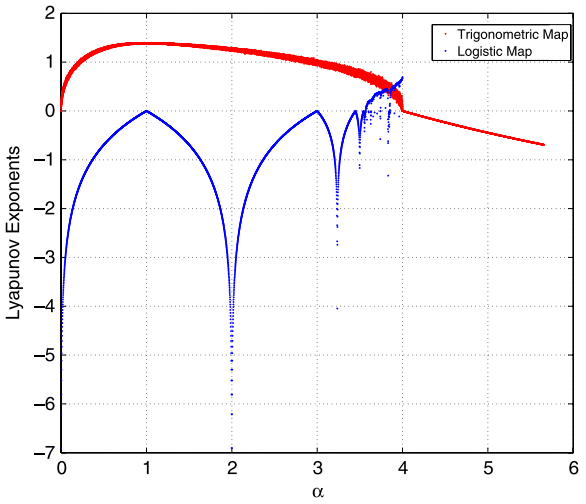

Fig. 2. Lyapunov exponents: red line shows the variation of Lyapunov exponents of selected example Eq. (5) in terms of the control parameter α, while blue line shows the variation of Lyapunov exponent of logistic map in terms of the control parameter. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

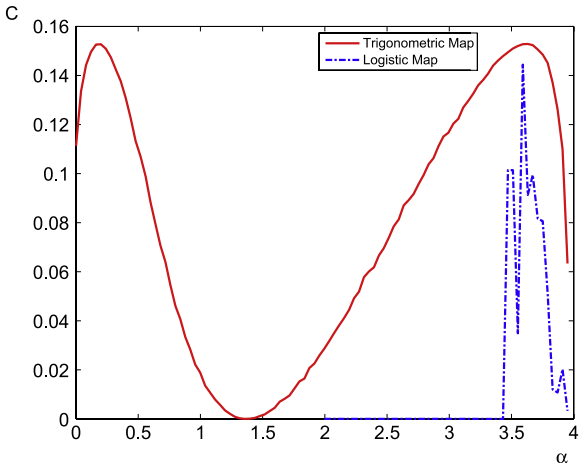

Fig. 3. Statistical complexity: red line shows the variation of complexity of selected example Eq. (5) in terms of the control parameter α, while blue line shows the variation of complexity of logistic map in terms of the control parameter. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

to information theory a system can never generate more entropy than what was supplied as input to the system. In many practical situations the demand for entropy is far more than available entropy; in such situations a PRNG comes handy. Logistic map has a very simple structure and it was first proposed as pseudo random number generator by von Neumann in 1947 [22]. The Logistic map has a known algebraic distribution which was later mentioned in 1969 in [23,24]. Logistic map can be used as a pseudo random number generator effectively when $r = 3.9 \sim 4$ and in which the behavior is chaotic. But a few years later it was found that Logistic map is a poor pseudo random number generator [25] as it generates sequences of extremely short period. On other hand, Logistic map contains only one quadratic term, therefore we are still unable to analytically find its natural invariant measure, the metric and topological entropy, except for the case of fully developed chaos [23].

6. Tests for randomness

A good random number generator must have some properties such as good distribution, long period and portability. In this paper, we used various types of tests to examine the quality of our proposed pseudo random number generator algorithm based on chaotic function, Eq. (5), and to draw conclusions on the randomness of the sequences produced by deterministic processes. Several tests are used to examine the randomness of the presented algorithm, these tests are DIEHARD [26], NIST statistical test suite [27] and ENT test suite. ENT test is a collective term for the three tests which are the

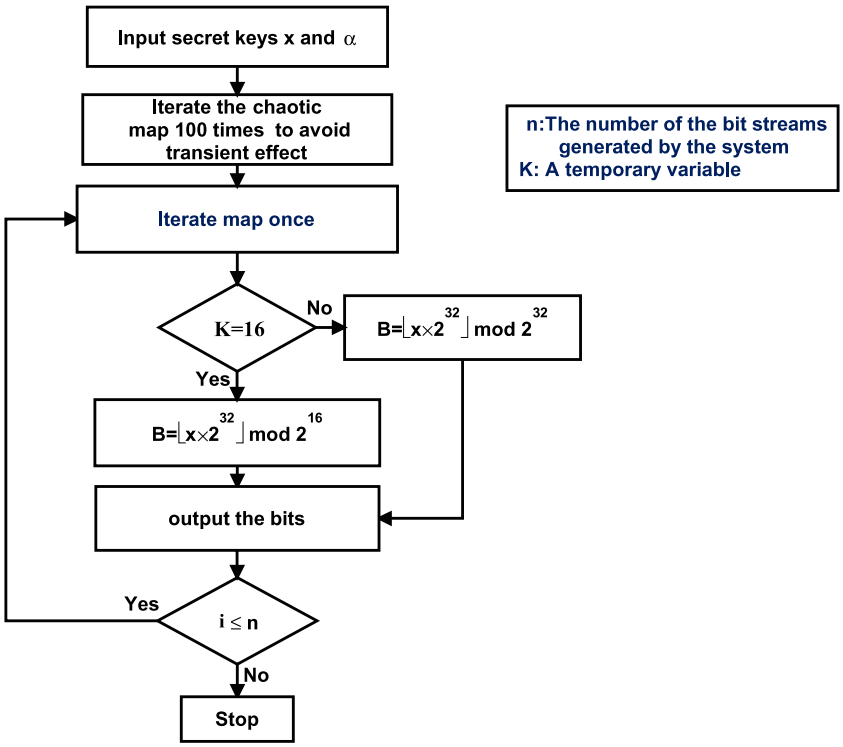

Fig. 4. Block diagram of the proposed PRNG.

Entropy, Chi-square, and Serial correlation coefficient (SCC) test. According to Tables A.1–A.4 which present NIST, DIEHARD and ENT test results respectively, the introduced generator passes all the tests and demonstrates better results in comparison to the other chaotic pseudo random number generators such as the Logistic map [28,29]. The flowchart of the algorithm is presented in Fig. 4.

6.1. Key space analysis

Random number generators are commonly used in encoding algorithms [5,6]. In the proposed random number generator algorithm, the combination of control parameter (α), initial condition (x) and degree of Chebyshev polynomial (N) of the chaotic system (Eq. (5)), can be used as encoding keys. The parameter N is originally the degree of the Chebyshev polynomials and a change in this parameter would lead to a change in the structure of the whole map and its characteristics, such as chaotic behavior, interval and the attractors. Therefore, the generated sequences by two maps with a single digit difference in their N parameter are completely random in respect to each other. The keys are chosen as follows: $x = 0.233456439$, $\alpha = 1.123659685694$ and $N = 4$. The key space for a cryptographic algorithm should not be less than 2^{128} in order to resist brute force attacks [30]. The presented chaotic map is highly sensitive to the all parameters mentioned above. If the precision is 10^{16}, therefore, the size of the key space for x and α is 10^{32}. For the space of parameter N we have 10^{14}, giving a total size for the key space of $10^{46} \approx 2^{152}$. Apparently, the key space is large enough to resist all kinds of brute force attacks.

7. Conclusion

According to the Information theory, a system can never generate more entropy than supplied as an input to the system, and in some situations there is a huge demand to the entropy, in such conditions PRNG can be used to supply the needed entropy. Logistic map turns out to be a poor pseudo random number generator because it generates sequences of extremely short period. In this paper a method for producing truly unpredictable sequences of random numbers is presented. The new proposed pseudo random generator algorithm is based on the generalized Logistic maps [11]. In our proposed algorithm we have used Eq. (5) as a prototype taken from the hierarchy of one dimensional chaotic map. Apparently, any introduced dynamical model of a 1D chaotic map (see Eq. (3)) can also be applied in the presented algorithm. The presented algorithm passes all the standard statistical tests in DIEHARD, NIST statistical test suite and Entropy test suite, therefore, it can be used for any application that requires randomness such as cryptographic applications.

Appendix. Derivation of the invariant measure

In order to prove that the measure (Eq. (6)) satisfies the Frobenius–Perron (FP) integral equation, we consider the map.

$$\tilde{x}_{n+1}(x,\alpha) = \frac{1}{\alpha^2}\tan^2(N \arctan\sqrt{x}) \tag{A.1}$$

with measure $\tilde{x}_{n+1}(x,\alpha)$ related to the measure $\mu_{\tilde{\Phi}_N}$ with the following relation:

$$\tilde{x}_{n+1}(x,\alpha) = \frac{1}{(1+x)^2}\mu_{\tilde{x}_{n+1}}\left(\frac{1}{1+x}\right).$$

Denoting $\tilde{x}_{n+1}(x,\alpha)$ on the left hand side of (A.1) by y and inverting it, we get :

$$x_k = \tan^2\left(\frac{1}{N}\arctan\sqrt{y\alpha^2} + \frac{k\pi}{N}\right) \quad k = 1,\ldots,N. \tag{A.2}$$

Then, taking derivative of x_k with respect to y, we obtain:

$$\left|\frac{dx_k}{dy}\right| = \frac{\alpha}{N}\sqrt{x_k}(1+x_k)\frac{1}{\sqrt{y}(1+\alpha^2 y)}.$$

Substituting the above result in Frobenius–Perron (FP) equation, we get:

$$\tilde{\mu}_{\tilde{x}_{n+1}}(y)\sqrt{y}(1+\alpha^2 y) = \frac{\alpha}{N}\sum_k \sqrt{x_k}(1+x_k)\tilde{\mu}_{\tilde{x}_{n+1}}(x_k),$$

Now, considering the following ansatz for the invariant measure $\tilde{\mu}_{\tilde{x}_{n+1}}(y)$:

$$\tilde{\mu}_{\tilde{x}_{n+1}}(y) = \frac{\sqrt{\beta}}{\sqrt{y}(1+\beta y)},$$

the above equation reduces to:

$$\frac{1+\alpha^2 y}{1+\beta y} = \frac{\alpha}{N}\sum_{k=1}^{N}\left(\frac{1+x_k}{1+\beta x_k}\right)$$

which can be written as:

$$\frac{1+\alpha^2 y}{1+\beta y} = \frac{\alpha}{\beta} + \left(\frac{\beta-1}{\beta^2}\right)\frac{\partial}{\partial\beta^{-1}}(\ln(\Pi_{k=1}^{N}(\beta^{-1}+x_k))).$$

Table A.1
Results of the SP800-22 test suite for the 32-bit proposed nonlinear PRBG.

Test name		P-value	Result
Frequency		0.444867	SUCCESS
Block-frequency		0.500934	SUCCESS
Runs ($M = 10000$)		0.500617	SUCCESS
Long runs of ones		0.644942	SUCCESS
Rank		0.517363	SUCCESS
Spectral DFT		0.295498	SUCCESS
No overlapping templates		0.976927	SUCCESS
Universal ($L = 7$, $Q = 1280$, $K = 141,577$)		0.802942	SUCCESS
Lempel ziv complexity		0.178278	SUCCESS
Linear complexity		0.416273	SUCCESS
Serial	P-value 1	0.798665	SUCCESS
	P-value 2	0.849237	SUCCESS
Approximate entropy		0.616827	SUCCESS
Cumulative sums forward		0.343168	SUCCESS
Cumulative sums reverse		0.888137	SUCCESS
Random excursions	$X = -4$	0.889127	SUCCESS
	$X = -3$	0.772858	SUCCESS
	$X = -2$	0.23113	SUCCESS
	$X = -1$	0.743415	SUCCESS
	$X = 1$	0.171268	SUCCESS
	$X = 2$	0.349231	SUCCESS
	$X = 3$	0.43468	SUCCESS
	$X = 4$	0.423174	SUCCESS

Table A.2
Results of the SP800-22 test suite for the 32-bit proposed nonlinear PRNG.

Random excursions variant (state x)			
	$X = -9$	0.768922	SUCCESS
	$X = -8$	0.991818	SUCCESS
	$X = -7$	0.995606	SUCCESS
	$X = -6$	0.93796	SUCCESS
	$X = -5$	0.899918	SUCCESS
	$X = -4$	0.604545	SUCCESS
	$X = -3$	0.908091	SUCCESS
	$X = -2$	0.845471	SUCCESS
	$X = -1$	0.811656	SUCCESS
	$X = 1$	0.047061	SUCCESS
	$X = 2$	0.037975	SUCCESS
	$X = 3$	0.393918	SUCCESS
	$X = 4$	0.892534	SUCCESS
	$X = 5$	0.55579	SUCCESS
	$X = 6$	0.314482	SUCCESS
	$X = 7$	0.161842	SUCCESS
	$X = 8$	0.139774	SUCCESS
	$X = 9$	0.191832	SUCCESS

Table A.3
DIEHARD test suite for the 32-bit proposed nonlinear PRNG.

Test name	Average value	Result
Entropy	7.999989	SUCCESS
Chi-square	127.4750	SUCCESS
SCC	−0.000262	SUCCESS
Birthday spacing	0.767240	SUCCESS
Overlapping permutation	0.959594	SUCCESS
Binary rank 3131	0.818691	SUCCESS
Binary rank 3232	0.477434	SUCCESS
Binary rank 68	0.363018	SUCCESS
Bitstream	0.629145	SUCCESS
OPSO	0.7334	SUCCESS
OQSO	0.40855	SUCCESS
DNA	0.5137	SUCCESS
Count the ones 01	0.745979	SUCCESS
Count the ones 02	0.589339	SUCCESS
Parking lot	0.319941	SUCCESS
Minimum distance	0.769923	SUCCESS
3DS spheres	0.124393	SUCCESS
Squeeze	0.068958	SUCCESS
Overlapping sum	0.852160	SUCCESS
Runs	0.822144	SUCCESS
Craps	0.41525	SUCCESS

Table A.4
Max grade of ENT test suite.

Test name	Average value	Result
Entropy	7.999989	SUCCESS
Chi-square	127.4750	SUCCESS
SCC	−0.000262	SUCCESS

To evaluate the second term in the right hand side of above formulas we can write the equation in the following form:

$$\begin{aligned} 0 &= \alpha^2 y \cos^2(N \arctan\sqrt{x}) - \sin^2(N \arctan\sqrt{x}) \\ &= \frac{(-1)^N}{(1+x)^N}\left(\alpha^2 y\left(\sum_{k=0}^{[\frac{N}{2}]} C_{2k}^N (-1)^N x^k\right)^2 - x\left(\sum_{k=0}^{[\frac{N-1}{2}]} C_{2k+1}^N (-1)^N x^k\right)^2\right), \\ &= \frac{\text{constant}}{(1+x)^N}\prod_{k=1}^{N}(x - x_k), \end{aligned}$$

where x_k are the roots of Eq. (A.1) and they are given by the formula (A.2). Therefore, we have:

$$\frac{\partial}{\partial\beta^{-1}}\ln\left(\prod_{k=1}^{N}(\beta^{-1}+x_k)\right)=\frac{\partial}{\partial\beta^{-1}}\ln[(1-\beta^{-1})^N(\alpha^2y\cos^2(N\arctan\sqrt{-\beta^{-1}})-\sin^2(N\arctan\sqrt{-\beta^{-1}}))]$$

$$=-\frac{N\beta}{\beta-1}+\frac{\beta N(1+\alpha^2y)A\left(\frac{1}{\beta}\right)}{\left(A\left(\frac{1}{\beta}\right)\right)^2\beta^2y+\left(B\left(\frac{1}{\beta}\right)\right)^2}.$$

In deriving of above formulas we have used the following identities

$$\cos(N\arctan\sqrt{x})=\frac{A(-x)}{(1+x)^{\frac{N}{2}}},\qquad \sin(N\arctan\sqrt{x})=\sqrt{x}\frac{B(-x)}{(1+x)^{\frac{N}{2}}},$$

$$\frac{1+\alpha^2y}{1+\beta y}=\frac{1+\alpha^2y}{\left(\frac{B\left(\frac{1}{\beta}\right)}{\alpha A\left(\frac{1}{\beta}\right)}+\beta\left(\frac{\alpha A\left(\frac{1}{\beta}\right)}{B\left(\frac{1}{\beta}\right)}\right)y\right)}.$$

Hence to get the final result we have to choose the parameter α as:

$$\alpha=\frac{B\left(\frac{1}{\beta}\right)}{A\left(\frac{1}{\beta}\right)}.$$

References

[1] H. Bauke, S. Mertens, Random numbers for large-scale distributed Monte Carlo simulations, Phys. Rev. E 75 (2007) 066701–14.
[2] A.M. Ferrenberg, D.P. Landau, Y.J. Wong, Monte Carlo simulations: hidden errors from good random number generators, Phys. Rev. Lett. 69 (1992) 3382–3384.
[3] J.W. Byers, M. Luby, M. Mitzenmacher, A digital fountain approach to reliable multicast, IEEE Journal on Selected Areas in Communications 20 (8) (2002) 1528–1540.
[4] Q. Zhou, L. Li, Z.-Q. Chen, J.-X. Zhao, Implementation of LT codes based on chaos, Chinese Physics B 17 (10) (2008) 3609–3615.
[5] M. Djema, J.P. Barbot, I. Belmouhoub, Discrete time normal form for left invertibility problem, European Journal of Control 15 (2) (2009) 194–204.
[6] I. Belmouhoub, M. Djema, J.P. Barbot, Observability quadratic normal forms for discrete-time systems, IEEE Trans. on Automatic Control 50 (7) (2005) 1031–1038.
[7] S. Behnia, A. Akhshani, H. Mahmodi, A. Akhavan, A novel algorithm for image encryption based on mixture of chaotic maps, Chaos, Solitons & Fractals 35 (2008) 408–419.
[8] R.M. DSouza, Y. Bar-Yam, M. Kardar, Sensitivity of ballistic deposition to pseudorandom number generators, Phys. Rev. E 57 (1998) 5044–5052.
[9] J.F. Fernandez, C. Criado, Algorithm for normal random numbers, Phys. Rev. E 60 (1999) 3361–3365.
[10] I. Vattulainen, T. Ala-Nissila, K. Kankaala, Physical models as tests of randomness, Phys. Rev. E 52 (1995) 3205–3214.
[11] M.A. Jafarizadeh, S. Behnia, S. Khorram, H. Nagshara, Hierarchy of chaotic maps with an invariant measure, J. Stat. Phys. 104 (2001) 1013–1028.
[12] M.A. Jafarizadeh, S. Behnia, Hierarchy of chaotic maps with an invariant measure and their compositions, J. Non. Math. Phys. 9 (2002) 26–41.
[13] T. Stojanovski, L. Kocarev, Chaos-based random number generators — part I: analysis, IEEE Trans. Circ. Sys. I 48 (2001) 281–288.
[14] T. Gilbert, C.D. Ferguson, J.R. Dorfman, Field driven thermostated systems: a nonlinear multibaker map, Phys. Rev. E 59 (1999) 364–371.
[15] J.R. Dorfman, An introduction to chaos in nonequilibrium statistical mechanics, Cambridge, 1999.
[16] P.-H. Lee, Y. Chen, S.-C. Pei, Y.-Y. Chen, Evidence of the correlation between positive Lyapunov exponents and good chaotic random number sequences, Comput. Phys. Comm. 160 (2004) 187–203.
[17] M. Falcioni, L. Palatella, S. Pigolotti, Properties making a chaotic system a good pseudo random number generator, Phys. Rev. E 72 (2005) 016220–10.
[18] C.M. Gonzlez, H.A. Larrondo, O.A. Rosso, Statistical complexity measure of pseudorandom bit generators, Physica A 354 (2005) 281–300.
[19] R. Lopez-Ruiz, H.L. Mancini, X. Calbet, A statistical measure of complexity, Phys. Lett. A 209 (1995) 321–326.
[20] X. Calbet, R. Lopez-Ruiz, Tendency towards maximum complexity in a nonequilibrium isolated system, Phys. Rev. E 63 (2001) 066116–9 pp.
[21] J.G. Catalan, R. Lopez-Ruiz, Features of the extension of a statistical measure of complexity to continuous systems, Phys. Rev. E 66 (2002) 011102–6.
[22] S. Ulam, J. Von Neumann, On combination of stochastic and deterministic processes, Bull. Am. Math. Soc. 53 (1947) 1120.
[23] S.C. Phatak, S.S. Rao, Logistic map: a possible random-number generator, Phys. Rev. E 51 (1995) 3670–3678.
[24] C.K. Peng, S. Prakash, H.J. Herrmann, H.E. Stanley, Randomness versus deterministic chaos: effect on invasion percolation clusters, Phys. Rev. A 42 (1990) 4537–4542.
[25] R. Ursulean, Elektronika ir elektrotechnika, Nr. 7 (56) (2004) 10.
[26] G. Marsaglia, Computer code DIE HARD, 1997, available at, http://stat.fsu.edu/pub/diehard/.
[27] National institute of standards and technology, computer code available at http://csrc.nist.gov/rng/SP800-22b.pdf.
[28] F. James, A review of pseudorandom number generators, Comput. Phys. Commun. 60 (1990) 329–344.
[29] A. Kanso, N. Smaoui, Logistic chaotic maps for binary numbers generations, Chaos, Solitons & Fractals 40 (2009) 2557–2568.
[30] ECRYPT II Yearly Report on Algorithms and Keysizes, 2010, http://www.ecrypt.eu.org/documents/D.SPA.13.pdf.