Open Mathematics

Research Article

Marcin Lawnik*

Generation of pseudo-random numbers with the use of inverse chaotic transformation

https://doi.org/10.1515/math-2018-0004
Received October 29, 2016; accepted December 22, 2017.

Abstract: In (Lawnik M., Generation of numbers with the distribution close to uniform with the use of chaotic maps, In: Obaidat M.S., Kacprzyk J., Ören T. (Ed.), International Conference on Simulation and Modeling Methodologies, Technologies and Applications (SIMULTECH) (28-30 August 2014, Vienna, Austria), SCITEPRESS, 2014) Lawnik discussed a method of generating pseudo-random numbers from uniform distribution with the use of adequate chaotic transformation. The method enables the "flattening" of continuous distributions to uniform one. In this paper a inverse process to the above-mentioned method is presented, and, in consequence, a new manner of generating pseudo-random numbers from a given continuous distribution. The method utilizes the frequency of the occurrence of successive branches of chaotic transformation in the process of "flattening". To generate the values from the given distribution one discrete and one continuous value of a random variable are required. The presented method does not directly involve the knowledge of the density function or the cumulative distribution function, which is, undoubtedly, a great advantage in comparison with other well-known methods. The described method was analysed on the example of the standard normal distribution.

Keywords: Chaos, Pseudo-random number generator, Standard normal distribution

MSC: 37M25, 11K45, 62E99

1 Introduction

The generation of pseudo-random numbers is crucial in many fields of science like cryptography, where cryptographically secure pseudo-random numbers are needed e.g. [1] or scientific computations, where often numbers from another than uniform distribution are crucial e.g. [2, 3].

There are many published algorithms that enable the derivation of values from the given probability distribution. One of the most popular is the method of inverse cumulative distribution function determined by the equation [4]:

$$X = F^{-1}(U), \tag{1}$$

where U is a random variable from the uniform distribution on interval $(0, 1)$, F^{-1} is a quantile function and X is a random variable with distribution corresponding to F.

Another very popular method for pseudo-random numbers generation is the rejection (also called acceptance and rejection) method, which is the implication of the following observation [5]:

if a random point (X, Y) is uniformly distributed in the region G_f between the graph of the density function f and the x-axis, then random variable X has density f.

***Corresponding Author: Marcin Lawnik:** Faculty of Applied Mathematics, Silesian University of Technology, Gliwice, Poland, E-mail: marcin.lawnik@polsl.pl

Additionally, in professional literature the methods which allow the generation of pseudo random numbers from a concrete distribution can be found, for example, from the normal one [6–9]. One of such algorithms is the Box-Muller transformation given by the equations [6]:

$$N_1 = \sqrt{-2\ln U_1}\cos(2\pi U_2) \text{ and } N_2 = \sqrt{-2\ln U_1}\sin(2\pi U_2), \tag{2}$$

where N_1 and N_2 are standard normal random variables, whereas U_1 and U_2 are random variables from uniform distribution.

Apart from these classical methods, there are also ways of constructing chaotic maps solving the so-called inverse Frobenious-Perron problem [10–12], which enables the construction of recurrences with predefined invariant densities. Iterating such dynamical systems is an easy way of generating pseudo-random numbers. One of such recurrences is in the following form [13]:

$$x_{k+1} = F^{-1}\left(U\left(F(x_k)\right)\right), \tag{3}$$

where F is a given cumulative distribution function, F^{-1} is the inverse function to F and U is the skew tent map. The skew tent map (also called as the asymmetric tent map) is given by the relation:

$$x_{k+1} = f(x_k) = \begin{cases} \frac{x_k}{p} & 0 < x_k \leq p \\ \frac{1-x_k}{1-p} & p < x_k < 1 \end{cases}. \tag{4}$$

For each value of parameter $p \in (0, 1)$, the recurrence (4) is chaotic and has a uniform distribution of the iterated variable. Due to these properties, reccurence (4) is very popular as a component of pseudorandom number generators in cryptographic applications [14–16].

Transformations in the form of (3) were analyzed in [17]. The derived results indicate that for values of parameter p close to 0 or 1, the desired probability distribution of the iterative variable cannot be derived. The reason is a small -– close to zero – value of the Lyapunov exponent, which measures the rates of convergence or divergence of nearby trajectories. The Lyapunov exponent of the dynamical system $x_{k+1} = f(x_k)$ is given by the formula:

$$\lambda = \lim_{m\to\infty}\frac{1}{m}\sum_{i=0}^{m-1}\ln|f'(x_i)|. \tag{5}$$

Furthermore, methods for generating pseudo-random numbers with the use of chaotic maps related only to a specific distribution can be shown, for example the normal distribution with the use of the Weierstrass recurrence, which was firstly shown in [18] and futher analized in [19]. The Weierstrass recurrence can be expressed by the formula:

$$x_{k+1} = \sum_{i=0}^{N} a^i \cos(b^i \pi x_k), \tag{6}$$

where $0 < a < 1$, b is a odd number and $ab > 1 + \frac{3}{2}\pi$. As shown in [19], iterating (6) with parameter value a close to 1, generates values from the normal distribution.

Another method which applies chaotic maps in pseudo-random numbers generation was shown in [20], where values from uniform distribution are generated. This method may be described by the following procedure:

Method 1. *Let $U^n(x)$ denote the n-th iteration of the chaotic map with a uniform distribution starting from initial condition x. Furthermore, let:*

$$X = \{x_0, x_1, \ldots, x_{N-1}\} \tag{7}$$

be a certain pseudo-random set of numbers from continuous distribution with finite support. In such case, the set

$$U = \{u_0 = U^n(|ax_0|), u_1 = U^n(|ax_1|), \ldots, u_{N-1} = U^n(|ax_{N-1}|)\} \tag{8}$$

where a is a normative coefficient, has the distribution similar to uniform.

The above procedure enables the ”flattening” of continous distribution, i.e. reducing it to the uniform distribution. Furthermore, the accuracy of this process depends on the number of iterations n - if it is too small, then the obtained distribution only ”flattens” the oryginal density functions of (7). The transformation f may be chosen as the skew tent map (4). Other examples of chaotic maps with uniform distribution may be found in [21, 22]. Likewise, as recurrence (4), they consist of several independent functions, which may be called as *branches*.

While analyzing the above-described method a natural question arises: Is the process of reduction of any distribution to the uniform distribution reversible? If yes, then in consequence, a new method enabling the generation of pseudo-random numbers from any distribution could be derived. The fact that the transformation described in (8) is a 1D chaotic map means that it is irreversible. However, by additional assumptions the process may become reversible, which is discussed in the next section of this paper.

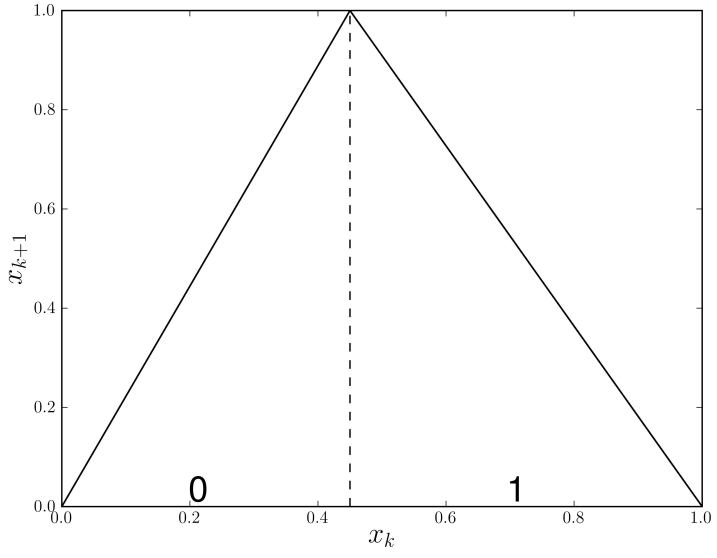
2 Method and analysis

The inversion of a chaotic transformation given, for example, by (4) does not render an unequivocal solution. Yet, knowing which of the *branches* of the transformation were iterated, the chaotic map may be inverted. This may be achieved by finding successive inverse images by means of a inverse function to an appropriate *branch*. Assuming that we have two *branches* that are denoted as ”0” and ”1” (see Fig. 1), any orbit starting from an initial point in (7) creates a certain binary sequence. Thus, by replacing every binary sequence with the appropriate integer number, in consequence, a set of integers is derived. Next, for such set it is possible to calculate the frequency of the occurrence w_i of particular integers, in accordance with the dependence:

$$w_i = \frac{n_i}{N}, \tag{9}$$

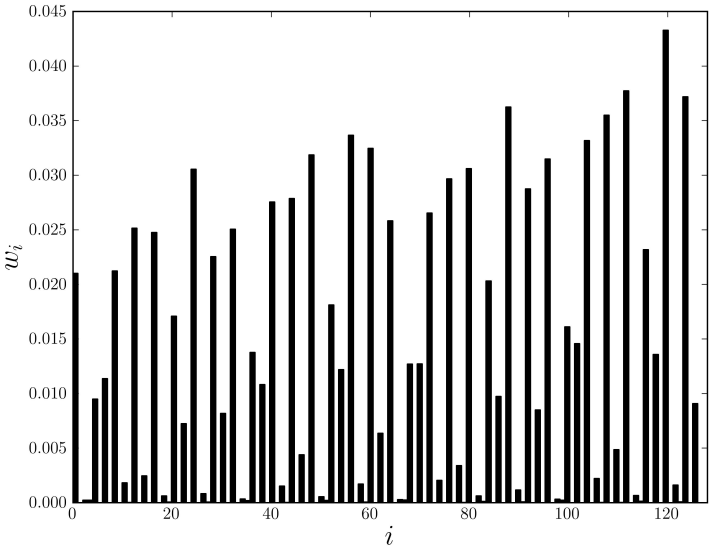
where n_i denotes the amount of successive integers in the above-mentioned set and $i = 0, 1, \ldots, 2^n - 1$.

Fig. 1. Skew tent map (4) with the assignment of the values of 0 and 1 to successive branches.



An example of such numerical normalized frequency set is shown in Fig. 2. Conducted numerical analysis has shown, that this set is invariant if the number of elements in (7) changes and the values of parameters p, a and n are fixed. Changing values in the mentioned parameters provides a new set of elements in the form (9).

Fig. 2. Frequency w_i of particular combinations of the branches of recurrence (4) with $n = 7$ and $p = 0.45$.



Thus, the algorithm of generating pseudo-random numbers from the given distribution with the use of transformation f may be described by the following procedure:

1. Set the values of the frequency of the occurrence w_i.
2. In accordance with w_i, generate an adequate value of discrete random variable i from the set $\{0, 1, \ldots, 2^n - 1\}$.
3. Generate a value of random variable $u \in (0, 1)$ from the uniform distribution.
4. In accordance with i inverse the value of u by calculating $x = f^{-i}(u)$, where f is the mapping used to get (9).
5. Return x.

Above-described algorithm is an approximate method of generation of pseudo-random numbers. It can be seen as a form of decomposition method of distributions. The accuracy of the method depends on the values of w_i, which must be designated for properly large set X with adequate number of iterations n. Next, the derived values of w_i may be catalogued. Then, to generate the values from the given distribution it is not necessary to know the density function or the cumulative distribution function. This eliminates the first step in above proposed algorithm. In comparison with other methods, such as inversion of the cumulative distribution function, or method of acceptance-rejection, it is, undoubtedly, a great advantage. Nevertheless, the algorithm requires to generate two values of random variables (one discrete and one from uniform distribution) which in comparison with the inversion cumulative distribution method is a disadvantage.

3 Example

The implementation of the above-described method shall be presented on the example of standard normal distribution. Accordingly, taking advantage of (8) and (4) the frequency of the occurrence of specific combinations of the *branches* w_i (9) was calculated. The results are presented in Fig. 2. Next, on the grounds of the frequencies using presented algorithm, a sequence of pseudo-random numbers was generated which numerically calculated density function shown in Fig. 3. The obtained results show good matching of the obtained distribution with the standard normal distribution. Moreover, a series of statistical tests was carried

out to verify the properties of the analysed method. The results are compiled in Table 1, certifying that the discussed method enables the generation of pseudo-random numbers from standard normal distribution.

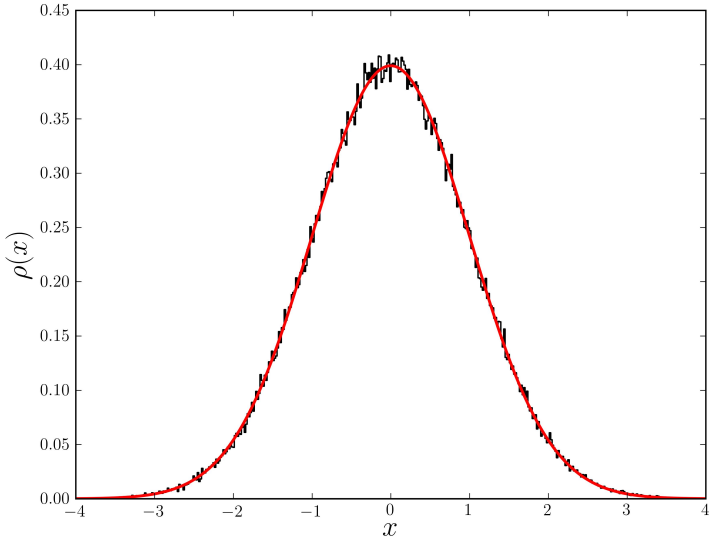
Table 1. Normality tests (from scipy.stats - Python module for statistics [23]) results for 500000 computed values with presented algorithm with skew tent map (4).

Test			Statistics value	p-value
Anderson-Darling	$n = 6$	$p = 0.3$	3.5324	
		$p = 0.5$	0.3252	
		$p = 0.7$	80.3513	
	$n = 7$	$p = 0.3$	1.7116	
		$p = 0.5$	0.7574	
		$p = 0.7$	8.5477	
	$n = 8$	$p = 0.3$	0.5129	
		$p = 0.5$	0.3032	
		$p = 0.7$	1.2678	
Kurtosistest	$n = 6$	$p = 0.3$	2.1539	0.0312
		$p = 0.5$	0.6770	0.4983
		$p = 0.7$	9.8800	5.0827e-23
	$n = 7$	$p = 0.3$	1.0719	0.2837
		$p = 0.5$	0.2584	0.7960
		$p = 0.7$	2.3718	0.0176
	$n = 8$	$p = 0.3$	0.6035	0.5461
		$p = 0.5$	1.8936	0.0582
		$p = 0.7$	1.3720	0.1700
Normaltest	$n = 6$	$p = 0.3$	4.8205	0.0897
		$p = 0.5$	1.5407	0.4628
		$p = 0.7$	97.808	5.7683e-22
	$n = 7$	$p = 0.3$	1.8172	0.4030
		$p = 0.5$	2.5114	0.2848
		$p = 0.7$	5.8378	0.0539
	$n = 8$	$p = 0.3$	0.8244	0.6621
		$p = 0.5$	3.6235	0.1633
		$p = 0.7$	2.1188	0.3466
Skewtest	$n = 6$	$p = 0.3$	-0.4255	0.6704
		$p = 0.5$	1.0403	0.2981
		$p = 0.7$	0.4408	0.6592
	$n = 7$	$p = 0.3$	0.8174	0.4136
		$p = 0.5$	1.5635	0.1179
		$p = 0.7$	0.4605	0.6450
	$n = 8$	$p = 0.3$	0.6783	0.4975
		$p = 0.5$	0.1936	0.8464
		$p = 0.7$	0.4861	0.6268

4 Conclusions

The method discussed in the paper enables the generation of pseudo-random numbers from a given distribution. It requires the knowledge of the frequency of the occurrence of particular branches of the transformation during the process of generating the uniform distribution described in [20]. However, neither the density function nor the cumulative distribution function are directly used in the method. The method was numerically analysed on the example of standard normal distribution. The obtained results prove its accuracy. It may be applied to create a series of generators of pseudo-random numbers from continuous probability distribution.

Fig. 3. Numerically obtained density function of the set of numbers derived by means of the presented algorithm (black line), red line shows the standard normal distribution.



References

[1] Blum L., Blum M., Shub M., A Simple Unpredictable Pseudo-Random Number Generator. SIAM Journal on Computing, 1986, 15 (2), 364–383

[2] Woźniak M., Połap D., On some aspects of genetic and evolutionary methods for optimization purposes, Int. J. Electron. Telecommun, 2015, 61(1), 7–16

[3] Słota D., Using genetic algorithms for the determination of an heat transfer coefficient in three-phase inverse Stefan problem, Int. Commun. Heat Mass Transf., 2008, 35(2), 149–156

[4] Devroye L., Non-Uniform Random Variate Generation, Springer, 1986

[5] Hörmann W., Leydold J., Derflinger G., Automatic Nonuniform Random Variate Generation, Springer-Verlag, Berlin Heidelberg, 2004

[6] Box G.E.P., Muller M.E, A Note on the Generation of Random Normal Deviates, Ann. Math. Stat., 1958, 29(2), 610–611

[7] Marsaglia G., Bray T.A., A convenient method for generating normal variables, SIAM Rev., 1964, 6, 260–264

[8] Leva J.L., A fast normal random number generator, ACM T. Math. Softw., 1992, 18, 449–453

[9] Afflerbach L., Wenzel K., Algorithm Normal random numbers lying on spirals and clubs, Stat. Pap., 1998, 29, 237–244

[10] Pingel D., Schmelcher P., Diakonos F.K., Theory and examples of the inverse Frobenius–Perron problem for complete chaotic maps, Chaos, 1999, 9(2), 357–366

[11] Koga S., The Inverse Problem of Flobenius-Perron Equations in 1D Difference Systems: 1D Map Idealization, Prog. Theory. Phys., 1991, 86(5), 991–1002

[12] Grossmann S., Thomae S., Invariant Distributions and Stationary Correlation Functions of One-Dimensional Discrete Processes, Z. Naturforsch, 1977, 32, 1353–1363

[13] Lai D., Chen G., Generating Different Statistical Distributions By The Chaotic Skew Tent Map, Int. J. Bifurcat. Chaos, 2000, 10, 1509–1512

[14] Palacios-Luengas L., Delgado-Gutiérrez G., Díaz-Méndez J.A., et al., Symmetric cryptosystem based on skew tent map, Multimed Tools Appl, 2017, 1–32

[15] Li C., Luo G., Qin K., Li C., An image encryption scheme based on chaotic tent map, Nonlinear Dynamics, 2017, 87(1), 127–133

[16] Khan J., Ahmad J., Hwang S.O., An efficient image encryption scheme based on: Henon map, skew tent map and S-Box, In: 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO) (27-29 May 2015 Istanbul, Turkey), 2015, 1–6

[17] Lawnik M., Analysis of the chaotic maps generating different statistical distributions, J. Phys.: Conf. Ser., 2015, 633(012086), 1–4

[18] Berezowski M., Lawnik M., Identification of fast-changing signals by means of adaptive chaotic transformations, Nonlinear Anal. Model. Control, 2014, 19(2), 172–177

[19] Lawnik M., The approximation of the normal distribution by means of chaotic expression, J. Phys.: Conf. Ser., 2014, 490(012072), 1–4

[20] Lawnik M., Generation of numbers with the distribution close to uniform with the use of chaotic maps, In: Obaidat M.S., Kacprzyk J., Ören T. (Ed.), International Conference on Simulation and Modeling Methodologies, Technologies and Applications (SIMULTECH) (28-30 August 2014, Vienna, Austria), SCITEPRESS, 2014, 451–455
[21] Huang W., Characterizing chaotic processes that generate uniform invariant density, Chaos, Soliton Fract., 2005, 25(2), 449–460
[22] Anikin V.M., Arkadaksky S.S., Kuptsov S.S., Remizov A.S., Vasilenko L.P., Lyapunov exponent for chaotic 1D maps with uniform invariant distribution, B. Russ. Aca. Sci. Phys., 2008, 72(12), 1684–1688
[23] Python scipy.stats module, http://docs.scipy.org/doc/scipy/reference/stats.html (last access 23.03.2016)