UDC 519.216.1

COMPUTER MODELING OF THE CHAOS FORMATION PROCESSES IN NONLINEAR DYNAMIC MAPS

G. Vostrov, A. Khrinenko
Odessa National Polytechnic University

Abstract. *In the course of the work we investigate dependences of iterative fixed points of nonlinear maps on the function properties and prime number properties. Dependences of the length of period of the iteration processes and randomness measure for pseudorandom sequences are analyzed according to the nature of used parameters.*

Key words*: chaos, pseudorandom sequences, nonlinear dynamic maps, statistical tests, prime numbers.*

Introduction

Many scientific papers raise a question: "What processes can be called chaotic?" Various important and simultaneously opposing tasks, namely theoretical and applied go with it. Up to now, there is no answer to the question – how to define the concept of randomness accurately and constructively, i.e. axiomatically. The lack of an answer creates great problems in such areas as probability theory, random processes, dynamic systems, and others [1, 2, 3, 4]. Processes that formed and occur in these areas are analyzed and interpreted as chaos. In this case many paradoxes arise, which are interpreted differently and sometimes they reveal the essence of the processes. In the theory of functions emerging of Weierstrass function at the time attracted great interest within the mathematical society. This was an example of nondifferential at no point function and behavior of the function was not predictable. A number of applied sciences at the same time require computer models of random sequences, dynamic information protection systems and constructive models of complex dynamic systems [5].

In modern science random number generators are of fundamental importance. They allow to generate sequences of numbers, that simulate randomness with certain degree of approximation to a given distribution law. Construction of random number generator enable to construct the concept of a formal and constructive definition of randomness, which is essential and necessary for modern probability theory, mathematical statistics and random processes. On the other hand, computer simulation of the processes of formation pseudorandom sequences (PRS) should be organized in such a way that will enable to generate near-random sequences that are absolutely unpredictable and, therefore, nonperiodical. However, issue of truly random sequences remains as open.

An independent research direction, which is commonly called as deterministic dynamic systems, has been formed apart from previously mentioned research areas. It is based on the study of the dynamics of iterative fixed points. Iterative cycles or orbits are considered as chaos. Dynamic systems that belong to deterministic class of systems appear as a consequence of an approximation of complex processes in the physical and mental world. And in the mathematical world dynamic systems are pseudo generators per se, that are created without purpose. However, they can be used as generators of pseudorandom sequences. The obtained sequences can be applied in cryptography for the formation of initial parameters of different algorithms, such as keys, initial vectors, etc. Another area of application of iterative processes is asymptotic methods and iterative procedures of computer simulation of computing for designed technical devices, search for extreme values of iterative processes and various applied fields, such as economics, processing and analysis of large data sets and machine learning theory.

It should be noted that in case of deliberately created generators of PRS and in case of dynamic systems it is necessary to take into account properties of iterated function. Main characteristic of these generators is the length of the iteration process period. Meanwhile, properties of the set of numbers on which given generators are built are not taken into account.

Prime numbers are of considerable interest when iterative processes are examined, because they are indecomposable into simple factors. For composite numbers of a large value the iterative cycle length can be significantly reduced.

Among a large number of PRS generators, a linear congruential method is often used, because it uses integer operations [5]:

$$(ax_n + b) \equiv l(\mathrm{mod} m),$$

where a,b,m – constants with $m>0$ and x_0 is specified. One of the varieties of this method is also used – a multiplicative congruential generator with a recursion step:

$$(cx_n) \equiv l(\mathrm{mod} m),$$

Where initial value x_0 and assumed to be relatively prime to the number m. The linear generator with some restrictions on the parameters will generate a sequence (x_n) with full period m and the multiplicative generator will generate a sequence with full period $m-1$. Necessary conditions for obtaining the maximum length of the period were formulated by Lehmer [6]:

A linear congruential generator has a period m if and only if next conditions are implemented:

1) $GCD(b,m)=1$,
2) $p \mid a-1$, if p – prime number and $p \mid m$,
3) $4 \mid a-1$, if $4 / m$.

Next, a multiplicative congruential generator has a period $m-1$ if and only if next conditions are implemented:

1) m – prime number,
2) c is a primitive root modulo m [7], that is $c^m = 1(\mathrm{mod} m)$ and for any $n<m \quad c^n \neq 1(\mathrm{mod} m)$.

For instance, one of the implementations of the multiplicative congruential generator uses Mersenne numbers, which allow comparatively fast calculations and provide a sufficiently long period length. The iterative dynamic process of this type is given in paper [8] and has the following form:

$$x_{n+1} = ((20^{30} - 2^{19})x_n) \bmod M_{61} \qquad (1)$$

Considering mentioned above and other methods of generating pseudorandom sequences, we can observe a direct connection with prime number theory. The nature of the prime numbers affects the behavior of functions, so it is important to consider not only the behavior of the function per se, but also the influence of the properties of numbers that are chosen as parameters. Some prime numbers also do not provide the longest cycle length; this circumstance refers to those numbers that belong to certain number classes. Such numbers include Fermat, Mersenne, Wagstaff prime numbers and their various generalizations [5]. For an arbitrary choice of prime number it is transpired, that there is a set of large prime numbers on which generators provide sequences where the cycle length is insignificant and clearly not chaotic. Although on adjacent prime numbers the cycle length is commensurable with dimension of the prime number. If these properties of prime numbers are not taken into account, the choice of such an exceptional prime number can lead to very significant errors in cryptography, pseudorandom number generation and incorrect conclusions in computer simulations of iterative processes in the examined technical devices, as well as in time series analysis.

1. Computer analysis of iterative processes in nonlinear maps

In this paper we analyze processes occurring in maps that are presented as examples of simple nonlinear dynamic systems. These maps are generally represented in the following form:

$$x_{n+1} = f(x_n) = \begin{cases} \varpi x_n, & x_n < \dfrac{1}{2} \\ \varpi(1-x_n), & x_n \geq \dfrac{1}{2} \end{cases},$$

where $\varpi \in (0;+\infty)$ and, if $\varpi = 2$, then the system takes segment $[0,1]$ into itself. In this case, the periodic points are dense on the segment and the map shows randomness. However, due to errors in rounding, the transition to a family of integer maps was performed. We examine chaotic processes in four types of nonlinear integer maps:

$$x_{n+1} = t_1(x_n) = \begin{cases} 2x_n, & 4x_n < p \\ p - 2x_n, & 4x_n \geq p \end{cases} \qquad (2)$$

$$x_{n+1} = t_2(x_n) = \begin{cases} 2x_n, & 2x_n < p \\ p - x_n, & 2x_n \geq p \end{cases} \qquad (3)$$

$$x_{n+1} = t_3(x_n) = \begin{cases} 2x_n, & 2x_n < p \\ 2x_n - p, & 2x_n \geq p \end{cases} \qquad (4)$$

$$x_{n+1} = t_4(x_n) = \begin{cases} 4x_n, & 4x_n < p \\ 4x_n (\mathrm{mod} p), & 4x_n \geq p \end{cases}, \qquad (5)$$

where p – prime number. Despite the simplicity of these maps their iterative cycles, based on prime numbers, have properties that support the above stated conjectures. According to them, not only properties of maps determine the structure of iteration cycles, but also the properties of numbers from their domain of definition can have a decisive influence on the structure and radically change it. It is worth to mention, that map (2) algebraically equivalent to map (5). But the map (3) does not satisfy the Fermat's little theorem since for any prime number p the number $(p-1)/m_{t_2}$ is a fraction, where m_{t_2} – period length for map (3). The above maps form cycles for which the length of the period m is equal to $(p-1)/2$ or some function $\varphi(p)$. Set of prime

numbers p where length of period is $m=(p-1)/2$ is considered as number class P_2 [12]. It should be noted that there is an infinite set of prime numbers for which the length of the period is significantly smaller than the dimension of the number. Table 1 shows the behavior of the triples of some consecutive prime numbers, where the first and third numbers belong to the class P_2 or number that provide large cycle length of sequence, while for the second number the length of the period is incommensurably smaller than the number dimension itself, and the PRS obtained for a given number forms a simple structure. Hereinafter, the calculations were performed with the help of Wolfram Mathematica 11.0.

Table 1

The lengths of PRS obtained with the maps (2, 3 4, 5)

position	number	m_{t_1}	m_{t_2}	m_{t_3}	m_{t_4}
1	126729749	63364874	95047311	126729748	63364874
2	126729751	707	1037	707	707
3	126729803	63364901	95047352	126729802	63364901
1	134396909	67198454	100797681	134396908	67198454
2	134396921	415	614	830	415
3	134396947	67198473	100797710	134396946	67198473
1	148587941	74293970	111440955	148587940	74293970
2	148587949	142	193	284	142
3	148587953	37146988	55717993	74293976	37146988
1	150327407	75163703	112745555	75163703	75163703
2	150327409	457	655	457	457
3	150327421	75163710	112745565	150327420	75163710
1	153500129	38375032	57557317	76750064	38375032
2	153500131	723	1054	1446	723
3	153500141	76750070	115125105	153500140	76750070
1	164511349	82255674	123383511	164511348	82255674
2	164511353	41	49	41	41
3	164511371	82255685	123383528	164511370	82255685
1	168410987	84205493	126308240	168410986	84205493
2	168410989	162	227	324	162
3	168411029	84205514	126308271	168411028	84205514
1	172384627	28730771	43099174	57461542	28730771
2	172384633	483	719	483	483
3	172384637	86192318	129288477	172384636	86192318

In this table columns m_{t_n} show the period length for the corresponding map t_n, where n – number of the corresponding map.

Considering the behavior of individual prime numbers, Fig. 1, 2 show the internal structure of the iterative process in the maps for the number 164511353, which has a short period length:

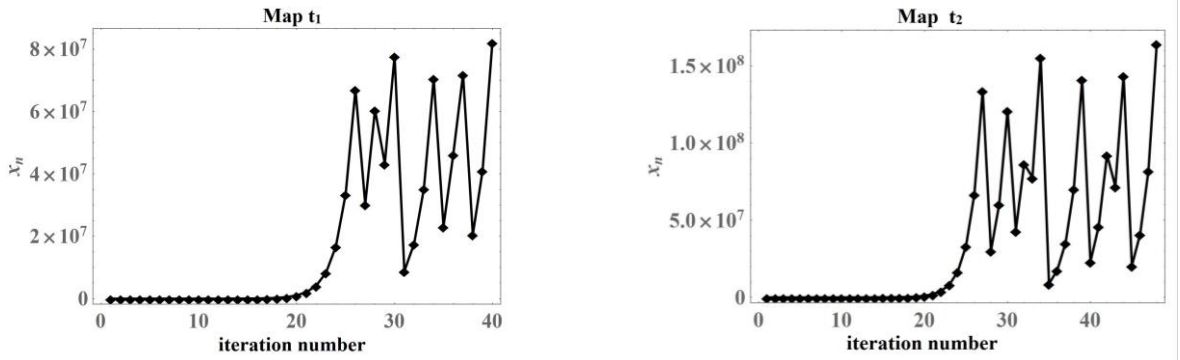

Fig. 1 The PRS structure based on the prime number 164511353

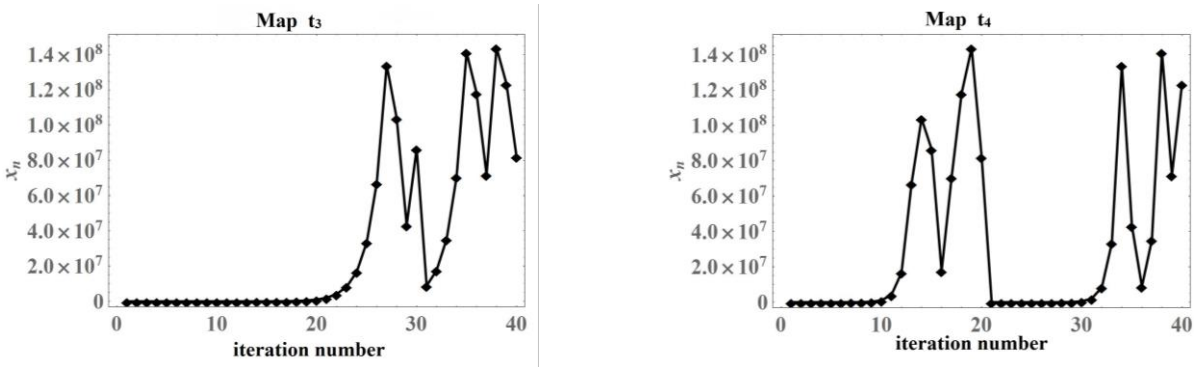

Fig. 2 The PRS structure based on the prime number 164511353

As it can be seen in Fig. 1, 2, the number contains the exponential component at the initial stage, so the number 164511353 cannot be used to generate PRS. In order to obtain a sequence close to the chaotic one, the 9th Mersenne number is used in the multiplicative congruential generator (1), which allows to escape the initial exponential component in sequences formed with maps (2,3,4,5) using the number 164511353. It should be noticed that the choice of a large number does not allow us to escape the exponential components inside the sequence, as, for instance, in the sequence generated with map (5) on the interval [21 – 34]. At the same time, for the number that precedes 164511353 and the next prime number, the length of the period is commensurate with the dimension of these numbers, which may indicate chaotic nature of the iterative process. Fig. 3, 4, 5, 6 show parts of the iterative processes based on the number 164511349, which is the preceding number for 164511353.

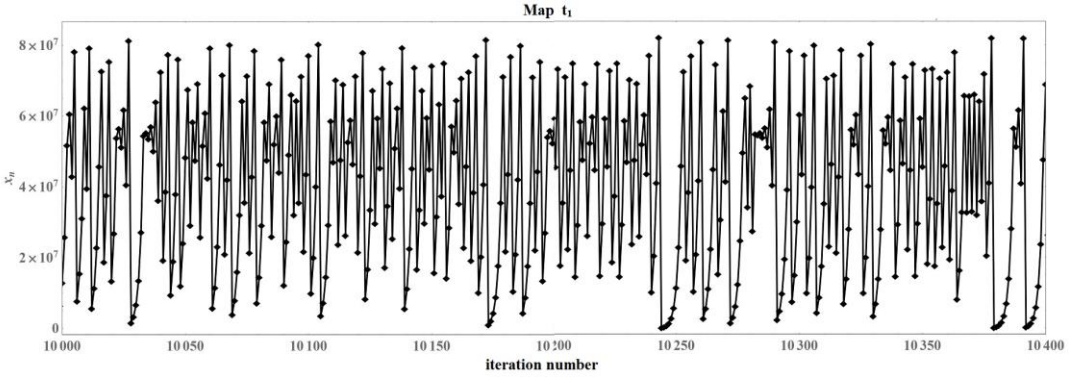

Fig. 3 Structure of part of the PRS [10000 - 10400] for map (2) based on number 164511349

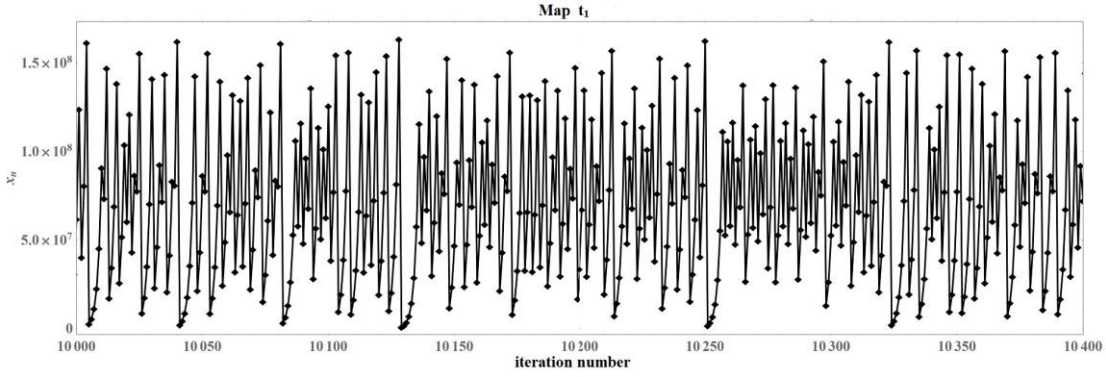

Fig. 4 Structure of part of the PRS [10000 - 10400] for map (3) based on number 164511349

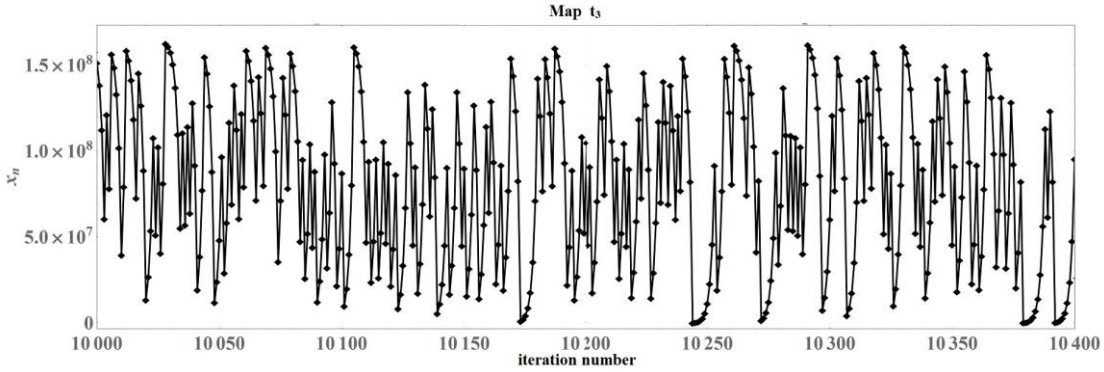

Fig. 5 Structure of part of the PRS [10000 - 10400] for map (4) based on number 164511349

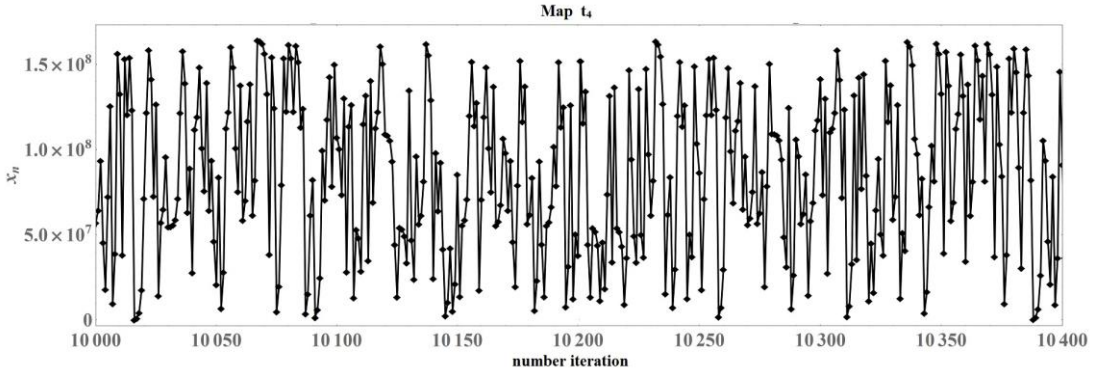

Fig. 6 Structure of part of the PRS [10000 - 10400] for map (5) based on number 164511349

For a given number the internal structure demonstrates some degree of chaos, and, on the other hand, it contains systematic exponential components. However, the approximation to 1 at certain iterations for the maps (2, 3, 4) leads to the appearance of exponential components that resemble to components at the beginning of the sequences for the number 164511353, thus the sequence for the map (5) shows the greatest degree of randomness, since it does not contain periodic exponential components. For a more fundamental analysis of sequences, formal measures of randomness are required [9].

Particular attention is attracted to prime numbers of a special kind, such as generalized Gaussian-Mersenne prime numbers p for which the number

$$((1+i)^p - 1)((1-i)^p - 1)$$

is also prime one. There are sequences that have a simple structure with exponential components that repeat with a certain frequency and are slightly different in amplitude. These numbers completely violate the randomness conditions imposed on PRS. It is proved that such an internal regular structure is characteristic of the Mersenne, Wagstaff numbers and their various generalizations. Fig. 7, 8 show the structure of the PRS for the generalized Gaussian-Mersenne prime 4327489.

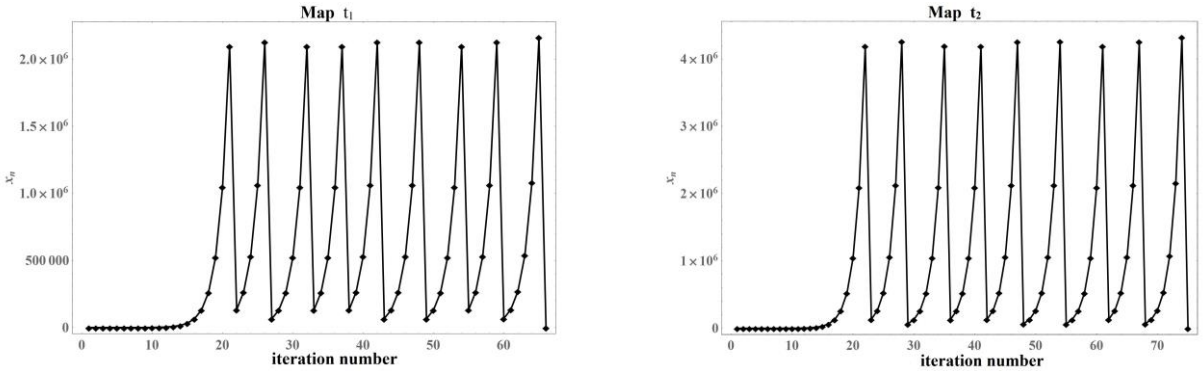

Fig. 7 Sequences with exponential components based on 4327489

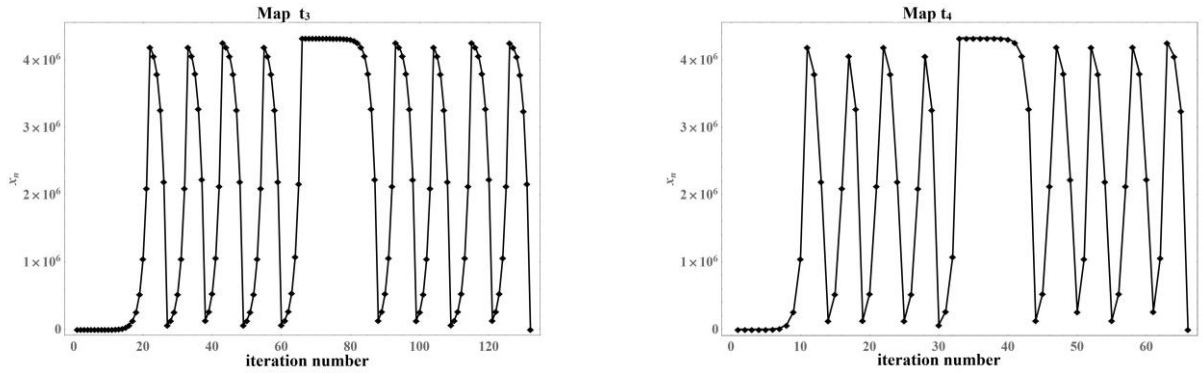

Fig. 8 Sequences with exponential components based on 4327489

2. Statistical methods for randomness estimation of the iterative processes

This section demonstrates methods for analyzing the quality of the generated PRS [9] [10]. The first group is connected with the search for regularities, which make it possible to reproduce the sequence over its segment. In this case, the basic requirements for the sequence are reduced to the absence of relatively simple interelement dependencies in it. For example, it is necessary to check the correlation between the elements of the sequence. This problem consists in performing an autocorrelation analysis, namely, the construction of a correlogram that shows the value of the correlation coefficient for various shifts (lags) of the original sequence. To estimate the randomness measure in the sequence, the autocorrelation statistics should be close to zero and not exceed the level of 0.01 to regard the sequence as chaotic and thereby random. The data obtained for the number 164511353 and shown in Fig. 9, 10, 11, 12 show that the correlation for a given number fluctuates at the level of 0.5 and, consequently, this number absolutely does not satisfy the requirements imposed to the PRS.

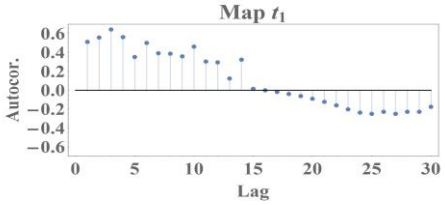

Fig. 9 Correlation for the PRS generated by map (2)

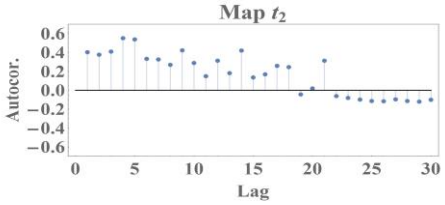

Fig. 10 Correlation for the PRS generated by map (3)

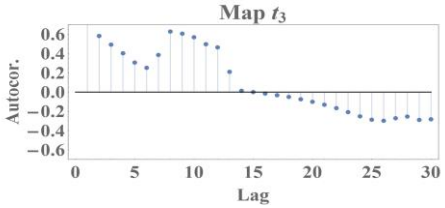

Fig. 11 Correlation for the PRS generated by map (4)

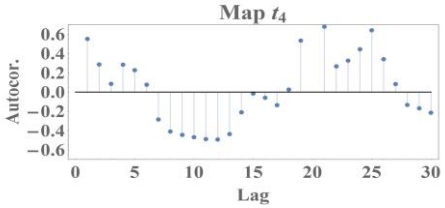

Fig. 12 Correlation for the PRS generated by map (5)

For prime number 164511349 the autocorrelation values calculated for a part of the sequence containing 200000 numbers and are shown in Fig. 13, 14, 15, 16 and closer to 0. Thus, this sequences show a large degree of randomness, but still does not satisfy the requirements of randomness.

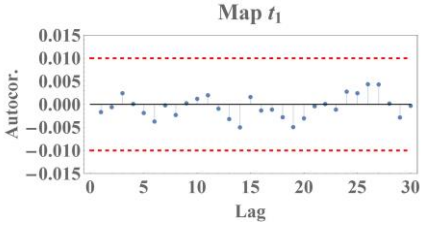

Fig. 13 Correlation for the PRS generated by map (2)

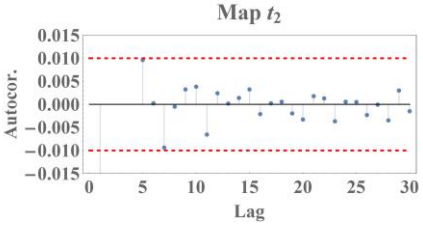

Fig. 14 Correlation for the PRS generated by map (3)

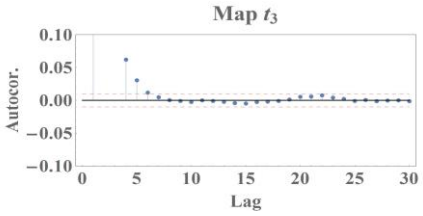

Fig. 15 Correlation for the PRS generated by map (4)

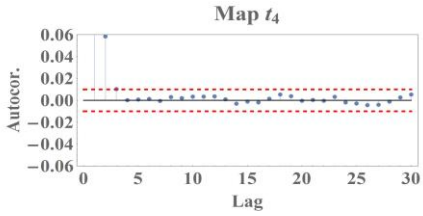

Fig. 16 Correlation for the PRS generated by map (5)

The obtained data for correlation make it possible to assume that a more acceptable result is achieved by using numbers which period length is commensurable with the dimension of the number itself.

The second method is aimed to estimate the statistical properties of sequences, for example, the frequency imbalance, which makes it possible to predict its further values from the known interval of the sequence. Proceeding from this, the requirements are advanced to consistency, so that the statistical properties of the sequence correspond to the properties of the truly random sequence, in particular, the frequency of occurrence of its elements should be evenly distributed in the sequence. Fig. 17 - 24 show the frequency distribution of the PRS elements obtained on the basis of successive prime numbers 164511349 and 164511353, in the form of a histogram for estimating the correspondence to the uniform distribution:

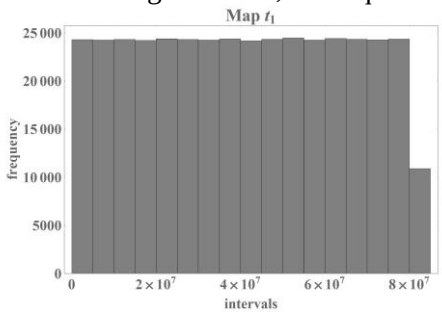

Fig. 17 Histogram for map (2) based on 164511349

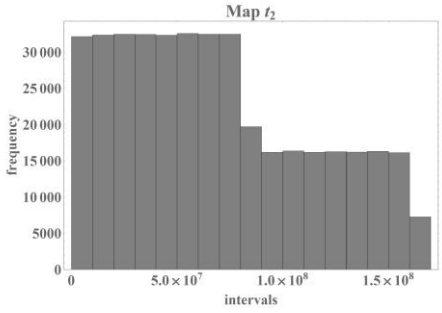

Fig. 18 Histogram for map (3) based on 164511349

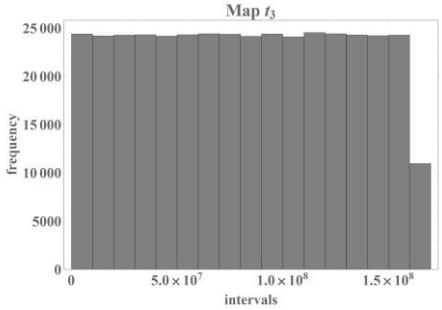

Fig. 19 Histogram for map (4) based on 164511349

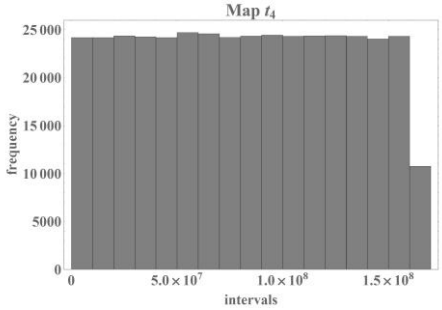

Fig. 20 Histogram for map (5) based on 164511349

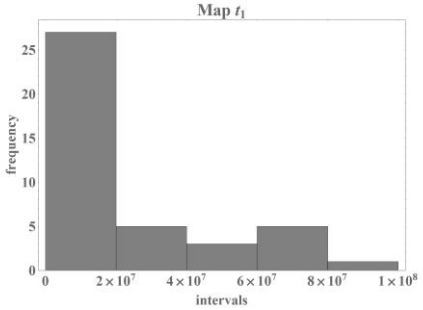

Fig. 21 Histogram for map (2) based on 164511353

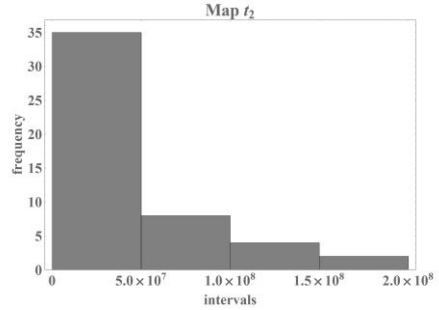

Fig. 22 Histogram for map (3) based on 164511353

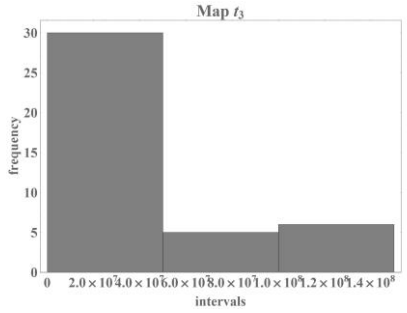

Fig. 23 Histogram for map (4) based on 164511353

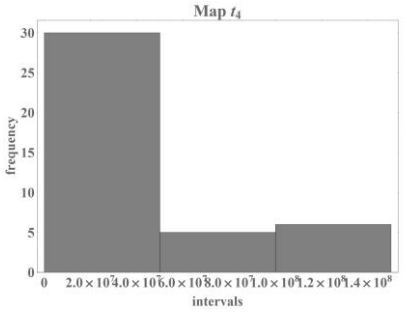

Fig. 24 Histogram for map (5) based on 164511353

As can be seen on the histograms for the maps (2, 4, 5) the frequency distribution for the sequences obtained on the basis of the prime number 164511349 is close to the uniform distribution. This is true for any primes that belong to the class P_2; hence, these numbers have the best statistical properties for use in PRS generators.

Since, analytical proof of some of the necessary properties is possible only for certain classes of sequences to justify the properties of sequences there are a wide range of different statistical tests that allow us to reveal regularities [9]. Since the maps considered in this paper generate integer sequences, to further testing them on a statistical test, all the elements of the sequences are converted to binary form. One of the tests is a runs test, which is primarily concerned with detecting an unusual (nonrandom) number of runs of zeros or ones in a binary sequence. The steps in computing the test statistic (the *pr*-value) are as follows [10]:

1. Compute the proportion of ones in the sequence:

$$\pi = (\varepsilon_1 + \cdots + \varepsilon_n)/n,$$

where n – length of the sequence and ε_n – individual bits of the sequence;

2. Compute the statistic:

$$V_n = \sum_{k=1}^{n-1} r(k) + 1 \ ,$$

where $r(k) = 0$, if $\varepsilon_k = \varepsilon_{k+1}$ and $r(k) = 1$ otherwise;

3. The *pr*-value is given as:

$$pr = erfc\left(\frac{V_n - 2n\pi(1-\pi)}{2\sqrt{2}n\pi(1-\pi)}\right),$$

where *erfc* – complementary error function and it is defined as

$$erfc(x) = \frac{2}{\sqrt{\pi}}\int_x^\infty e^{-t^2}\,dt\,.$$

4. If $pr \geq 0.01$, then we conclude the sequence is random.

The generator's construction must ensure that obviously weak sequences do not appear at the output, for which it is also necessary to analyze the properties of the numbers on which the generator is built.

Since analyzed in this paper maps for generating PRS are simple iterative maps sequences obtained on the basis of any arbitrary chosen numbers can not satisfy the randomness conditions. However, the value of *pr* will lead to a conclusion about which numbers possess better statistical properties. Table 2 shows the results of the runs test for the prime numbers 164511349 and 164511353.

Table 2

Runs test results

number	map	*pr*-value
164511353	map (2)	$3.6989 \cdot 10^{-12}$
	map (3)	$5.3161 \cdot 10^{-10}$
	map (4)	$8.8828 \cdot 10^{-7}$
	map (5)	$8.8828 \cdot 10^{-7}$
164511349	map (2)	$1.4904 \cdot 10^{-7}$
	map (3)	$6.2335 \cdot 10^{-431}$
	map (4)	$5.2501 \cdot 10^{-5}$
	map (5)	$2.0217 \cdot 10^{-4}$

The results of the runs test show that, although both sequences do not satisfy the chaotic conditions, a sequence based on the number 164511349, which belongs to the class P_2, allows to obtain a larger degree of randomness.

Conclusion

The results obtained in this paper show that best possible fit to randomness conditions for generating PRS by nonlinear dynamic maps require to take into account the properties of the set of numbers on which the pseudorandom number generator is built. The best possible fit to randomness conditions for generating PRS can be obtained using prime numbers for which the length of the period is commensurable with the value of the number itself (class P_2), since the internal sequence structure on the basis of such numbers does not contain simple periodic components and exhibit behavior closer to random and, thereby, chaotic.

References

1. Ruelle, D. (2001). Randomness and chaos [Sluchaynost' i khaos], transl. from French by N. Zubchenko. Izhevsk: R&C Dynamics, p.192.
2. Kuznetsov, S. (2006). Dynamic chaos [Dinamicheskiy khaos]. Moscow: Fizmatlit, p.347.
3. Kronover, R. (2006). Fractals and chaos in dynamic systems [Fraktaly i khaos v dinamicheskikh sistemakh]. Moscow: Tekhnosfera, p.488.
4. Goldreich, O. (2011). Studies in complexity and cryptography. 1st ed. Heidelberg: Springer, p.563
5. Crandall, R., Pomerance, K. (2011), Prime numbers: cryptographic and computational aspects [Prostye chisla: kriptograficheskie i vychislitel'nye aspekty], transl. from English / Ed. and with a preface by V. Chubarikova. Moscow: URSS Book House "LIBROKOM", p. 664
6. Lehmer, E. (1964). On the infinitude of Fibonacce Pseudo-Primes. The Fibonacci Quarterly, 2, p.230.
7. Vinogradov, I. (2009). Fundamentals of Number Theory [Osnovy teorii chisel]. St. Petersburg: Publishing house "Lan", p.176.
8. Wu, P. (1997). Multiplicative, congruential random-number generators. ACM Transactions on Mathematical Software, 23(2), p. 255-265.
9. Fomichev, V. (2010) , Methods of Discrete Mathematics in Cryptology [Metody diskretnoj matematiki v kriptologii]. Moscow: Dialogue- MEPhI, p. 424.
10. Wellin, P. (2013). Programming with Mathematica. 1st ed. Cambridge, UK: Cambridge University Press.
11. Menezes, A. (1996). Handbook of Applied Cryptography. 1st ed. Boca Raton: CRC Press.
12. Vostrov, G., Opiata, R. (2017). Effective computability of dynamic system structure of prime number formation [Effektivnaya vychislimost' struktury dinamicheskikh sistem formirovaniya prostykh chisel]. ELTECS, 244

КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ФОРМИРОВАНИЯ ХАОСА В НЕЛИНЕЙНЫХ ДИНАМИЧЕСКИХ ОТОБРАЖЕНИЯХ

Г. Н. Востров, А. О. Хриненко
Одесский национальный политехнический университет

Аннотация. *В работе рассмотрены проблемы, возникающие при моделировании формирования хаоса в нелинейных динамических отображениях. Исследована зависимость итерационных неподвижных точек нелинейных отображений, с одной стороны от свойств функций, а с другой стороны от свойств простых чисел. Рассмотрены зависимости длины периода итерационного процесса и меры случайности для псевдослучайных последовательностей на основе простых чисел.*

Ключевые слова: *хаос, псевдослучайные последовательности, нелинейные динамические отображения, статистические тесты, простые числа.*

Received on 14.05.2017

Востров Георгий Николаевич, кандидат технических наук, доцент кафедры прикладной математики и информационных технологий Одесского національного политехнического университета. Проспект Шевченко, 1, Одесса, Украина.
E-mail: vostrov@gmail.com, тел. +380503168776

George Vostrov, Ph. D. of Technical Sciences, Associate Professor of the Department of Applied Mathematics and Information Technologies, Odessa National Polytechnic University. Shevchenko ave., 1, Odessa, Ukraine.

ORCID ID: 0000-0003-3856-5392

Хриненко Андрей Олегович, студент кафедры прикладной математики и информационных технологий Одесского национального политехнического университета. Проспект Шевченко, 1, Одесса Украина.
E-mail: khrinenko.andrew@gmail.com, тел. +380637515228

Khrinenko Andrii, student of the Department of Applied Mathematics and Information Technologies, Odessa National Polytechnic University. Shevchenko ave., 1, Odessa, Ukraine.

ORCID ID: 0000-0001-6000-2102