UDC 519.216.1

MATHEMATICAL FOUNDATION OF INFORMATION TECHNOLOGIES IN MODERN NONLINEAR DYNAMICAL SYSTEMS

G. Vostrov, A. Khrinenko
Odessa National Polytechnic University

Abstract. *In this paper it is considered and generalized hypothesis about existence of 3 classes of processes: physical, mental and mathematical. It is shown that in all nonlinear dynamical systems the key factor in determining their quantitative and qualitative characteristics is the information about fixed points of dynamical systems and their orbit properties.*

Key words: *dynamical systems, nonlinear maps, randomness, orbits, chaotic processes.*

Introduction

Systems of physical, mental, and mathematical spaces contain numerous complicated processes of effective management that represent the necessary condition for the successful evolutionary development of human society. It is known that the creation of effective control methods in all known forms is possible upon the condition that information on the laws of evolutionary development does exist and available [11, 13]. The existence of information is a necessary, but insufficient requirement for its use. There is need for technology of obtaining, analyzing and processing information. The combination of such methods is developed on the basis of modern information technologies. The accumulation, processing and analysis of information, as a rule, is a stochastic nature of the laws of its processing and application [14]. One of the most common formation, processing and analysis systems is self-organized nonlinear dynamic systems. Research of such systems is one of the mathematical methods of obtaining and further application in information technologies, which is currently actively developing in all known directions of modern science. Modeling of stochastic processes based on the theory of dynamic systems is currently a prerequisite for the development of information technology [15, 16].

Simulation of stochastic processes is an important direction in mathematics, which is also used in such fields as dynamical systems simulation, functional analysis, function theory, cryptography, etc. Relevant processes are used to generate numeric sequences. The resulting sequences are widely used in various example tasks such as, for example, the theory of machine learning for the learning and test sequences [1], and others.

Various methods for generating numerical sequences are based on chaotic nonlinear processes. Currently there is no precise and constructive axiomatic meaning of the notion of chance. Computer generators of numerical sequences are deterministic, respectively, modeling a pseudo-random variable with a definite degree of approximation to randomness by a given order distribution. Thus, the generators of pseudorandom numbers are a way to determine the formal concept of cascade, which is important and necessary in modern probability theory, the theory of random processes, and others. The problem of the pseudorandom sequence sequence (PRS) approaching the ideal [2] is set because the ideal random sequence is a mathematical model, which is a completely non-predicted, and therefore non-periodic, infinite posteriori, and, accordingly, does not allow to receive its representation in computer systems.

The notion of randomness finds its application in game theory in the definition of such a concept as "rational-flail behavior". Suppose there is a certain set of agents that interact with each other and each agent influences the results of others. Each agent has a set of arbitrary strategies to determine further actions. The question arises: "What set of separate strategies will be rational behavior of the entire group of agents?". It is proved that a set of strategies for individual agents will produce the best result if none of the agents can improve their results in the transition to another strategy by having information about the strategies of other participants. Intuitively, an arbitrary selection of optimal strategies by agents allows us to obtain a universal notion of rational behavior. However, the problem of true randomness and the non-resolution of the question of the formal definition of chance appears again. In the Kolmogorov axiomatic, truly random sequences were left beyond the bounds of the theory, and only general approaches were proposed for the definition of randomness, for example, von Mises' approach.

However, although the exact definition of randomness does not exist yet, the above-recognized application problems can be solved with the help of pseudo-packet variables representing values satisfying a certain set of requirements. An example

of such a task is the Monte Carlo method, which raised the question whether or not it is really necessary to use true chance or can it be replaced by an appropriate deterministic procedure for the solution? The theorem is proposed in [3], provided that any settlement problem is difficult to solve, randomness does not allow to improve algorithmic efficiency. Each probabilistic algorithm can be replaced by a deterministic algorithm with the same degree of efficiency. The key to the proof of this theorem is the construction of generators of pseudo-randomness, forming sequences, not distinguishing from random sequences when used by their respective algorithms. The question arises whether it is possible to effectively form such sequences that would be close to random by means of deterministic methods. This problem can be solved both in terms of mathematics and in terms of computer science. The proof that the deterministic systems and structures satisfy the conditions of randomness is carried out by methods of the theory of numbers, algebras, and others. While computer methods begin with the definition of necessary properties and subsequent attempts to effectively form structures with specified properties. Such analytical and synthetic approaches are usually combined to improve the end result.

In the case of PRS generators or dynamic systems, it is necessary to consider and analyze the properties of the iterative functions that determine the length of the iteration process period, which is one of the main properties of the generators, as well as the internal structure of the data of the iterative processes. At the same time, the power of the set of numbers on which the data are determined, iterative functions are given much less attention. In this matter, there is a direct connection with number theory. Prime numbers are of considerable interest because they are used in a wide range of applications. For example, in the RSA cryptosystem, in the first stage, there is a selection of primes that require verification to match the conditions of reliability of their theoretic-numeric properties.

In accordance with previous statements, the purpose of the work is to model nonlinear iterative processes, analyze them in accordance with the properties of functions, analyze the effects of fixed points and the internal structure of the cycles on the degree of randomness, as well as the set of primes using statistical and structural methods.

1. Nonlinear dynamic systems and its iterative processes

To investigate and analyze previously stated problems this paper considers the processes observed in a group of nonlinear maps that represents behavior of nonlinear dynamical systems. The following maps are considered: "Tent", "Asymmetric tent", "Sawtooth" map and multiplicative order map. Real functions $f : R \to R$ are considered. Then f^n denotes the *n*th iteration of the function f, i.e. f^n is a *n*-fold composition of the function f with itself. If $x_0 \in R$, then an orbit or a trajectory for x_0 is some sequence that can be represented as $x_0, x_1 = f(x_0), \ldots, x_n = f^n(x_0), \ldots$. An important role is played by fixed points when considering dynamical systems. An initial point x_0 is defined as a fixed point if $f(x_0) = x_0$. It is obvious that the fixed point orbit represents a constant sequence $x_0, x_0, x_0, \ldots$. An analogue of a closed orbit for differential equations is determined by periodic fixed points. These are the points x_0 for which $f^n(x_0) = x_0, n > 0$ and, as well as closed orbits, periodic orbits repeat themselves: $x_0, \ldots x_{n-1}, x_0 \ldots$.Periodic orbits of period *n* are also called *n*-cycles (periods).

The maps that were chosen for an investigation and analysis of iterative fixed point and inner structure of sequences, obtained on the basis on these maps have next representation:

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

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

$$t_3(x_n) = x_{n+1} = \begin{cases} 2x_n, & x_n < 1/2 \\ 2x_n - 1, & x_n \geq 1/2 \end{cases} \quad (3)$$

Graphical representation for t_1^n contains 2^{n-1} tents with 2^{1-n} width. The distance between adjacent *n*-cycles is no more than 2^{2-n}. For any compact subinterval $[a,b] \subset]0,1[$ there exists a constant *c(a, b)* independent from *n*, so that the distance between adjacent *n*-cycles satisfies the condition $c2^{-n} < distance < 2^{-n}$. For the map (1) special attention is drawn to the fact that it shares many properties with the logistic map $g(x) = 4x(1-x)$ in the process of iterating. This special feature indicates their conjugation. If we assume that *I* and *J* represent some interactions for maps $f : I \to I, g : J \to J$ then we can say that the maps *f* and *g* are conjugated if there is a homeomorphism $h : I \to J$, that *h* satisfies the conjugation equality $h \circ f = g \circ h$. Conjugation compares orbits *f* to orbits *g*. This follows from the fact that $h(f^n(x)) = g^n(h(x))$ for all $x \in I$ such that *h* matches the *n*th point of the orbit for *f* from *x* to *n*th

point of the orbit g from $h(x)$. In paper [4], it is proved that the "Tent" map is topologically linked to a logistic map.

Transitioning from a formal model to a computer calculation, the question whether the results obtained during the calculations can be considered a solution to the problem arises, since the computer system operates in calculations with computer numbers, while mathematics operates with numbers of infinite length and these circumstances lead to mistakes when working with fractional numbers. Under the computer numbers the set Q_n is understood to mean numbers whose entries contain no more than n digits for the record of the whole and the fractional part of the number (this number can be large, but always limited). In this case, the set Q_n is closed with respect to arithmetic operations. In the end, the aforementioned circumstance creates a problem of reliability and gives false conclusions about processes in dynamic systems due to the fact that one of the properties of any dynamic system is sensitivity to initial conditions [5]. In the computer calculation of the iterations of reflections, the results show that all orbits are eventually fixed to 0, which does not correspond to reality and raises the question of the transition to an integer form. In order to reduce this circumstance to a minimum, the transition to integer maps presented in the following form is completed:

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

$$t_2(x_n) = x_{n+1} = \begin{cases} 2x_n, & 2x_n < p \\ p - x_n, & 2x_n \geq p \end{cases} \quad (5)$$

$$t_3(x_n) = x_{n+1} = \begin{cases} 2x_n, & 2x_n < p \\ 2x_n - p, & 2x_n \geq p \end{cases} \quad (6)$$

$$t_4(x_n) = x_{n+1} = \begin{cases} 4x_n, & 4x_n < p \\ 4x_n (\mathrm{mod}\ p), & 4x_n \geq p \end{cases}, \quad (7)$$

were p is prime number. It is important to note that the maps 4-6 are continuous functions, whereas the map 7 is defined only on the integer set. It is also worth noting that the map t_1^n is algebraically congruent to the map t_4^n on the set of integers, that is, the lengths of the cycles for all prime numbers coincide.

It should also be noted that the transition to the integer form for given maps leads to the expansion of the values of the basic functions in the transition between prime numbers to infinity while dimension of prime number increases. Figure 1 shows the behavior of map 4 when using prime numbers of different dimensions, where p_n - prime numbers and $fp\ n$ - corresponding fixed points.

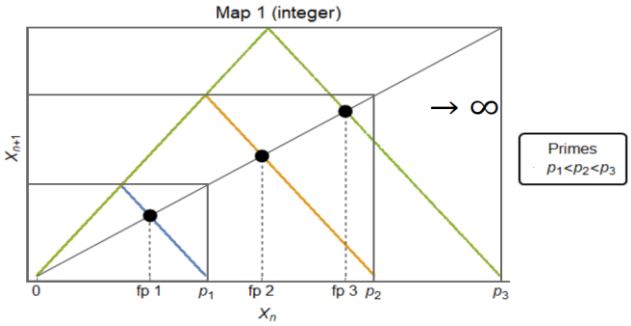

Fig. 1 – Representation of 1 iteration for map 4 and prime numbers

Despite the simplicity of the above maps, their iteration cycles have the properties that support the above statements. According to them, the structure of iterative cycles is determined not only by the properties of the maps itself, but also by the properties of the numbers that are used and which have a significant influence on the structure and can significantly change it. The presented nonlinear maps allow to divide the set of primes p into a system of classes based on the length of the iterative process for given primes [6]. We note that there is an infinite set of prime numbers for which the length of a period is substantially smaller than the dimension of a number. and the sequence obtained for this number forms a simple structure. The structure of this type is characteristic for the numbers belonging to the class of Fermat, Mersenne numbers and their various generalizations. At the same time, other prime numbers generate sequences for which the length of the period is commensurable with the dimensionality of the number and, accordingly, can show a greater degree of approximation to the randomness, but also have periodic components, as shown in figures 2 - 5.

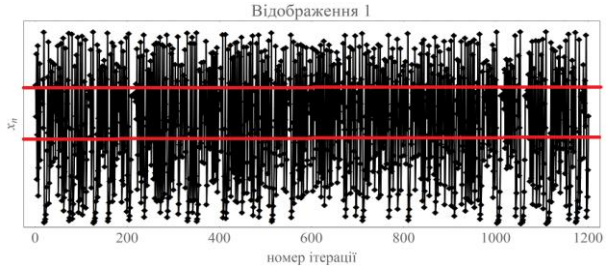

Fig. 2 – Sequence structure for p=160465519 and map 4

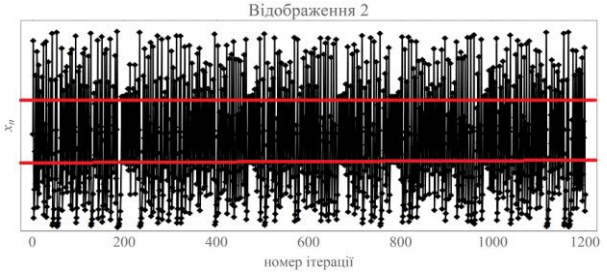

Fig. 3 – Sequence structure for p=160465519 and map 5

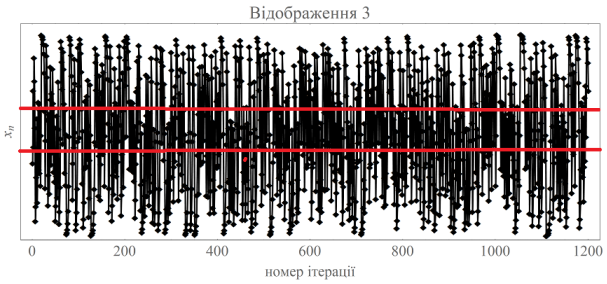

Fig. 4 – Sequence structure for p=160465519 and map 6

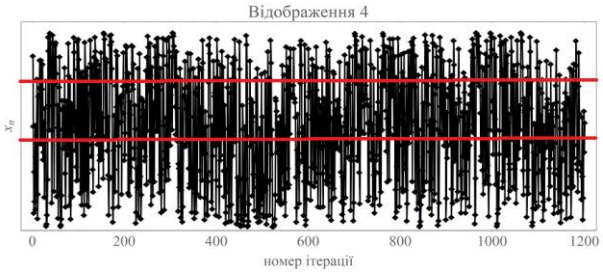

Fig. 5 – Sequence structure for p=160465519 and map 7

At the same time, the sequences obtained on the basis of maps 4 and 7 demonstrate a better approximation to the uniform distribution law, which represents one of the requirements for pseudorandom sequences.

However, considering the internal structure, it is necessary to introduce some similarity measure for the internal structures to conduct more complete analysis. For example, for given simple numbers in figures 6 - 9 it is presented an internal structure of the iterative processes for the maps, where the dashed line shows obtained sequences and the solid line shows the inner parts within the sequences that give the maximum value of similarity measure.

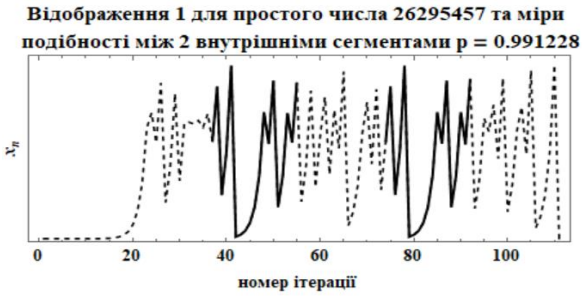

Fig. 6 – Inner structure for map 4

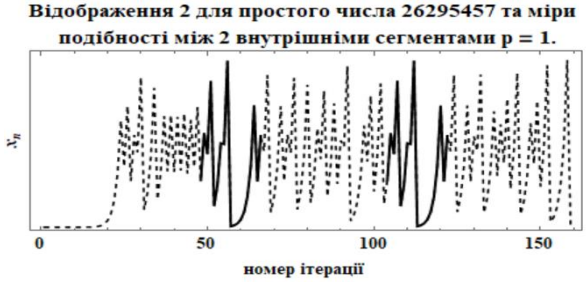

Fig. 7 – Inner structure for map 5

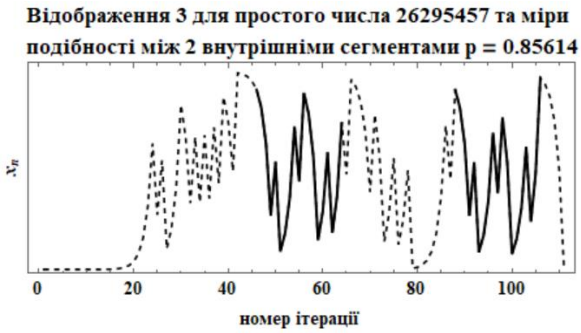

Fig. 8 – Inner structure for map 6

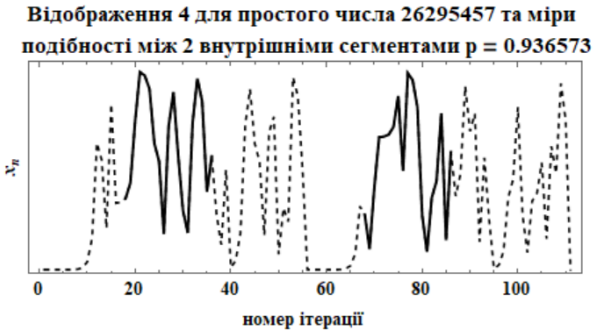

Fig. 9 – Inner structure for map 7

As can be seen from these figures, the sequences obtained with the help of maps 4 and 7 for some subsequences give similarity measure values close to 1, which indicate the effect of fixed points on the internal structure of the sequence, while map 7 demonstrates the least measure for its subsequences.

2. Methods of randomness measure estimation

There are several approaches to determining randomness and, accordingly, methods for evaluating the degree of randomness of a particular sequence. In [7], four algorithmic properties are differed for the description of randomness: frequency stability, chaotic behavior, typicality, nonpredictability. Each of them presents its own algorithmic aspect of randomness, and each of them, with greater or lesser connotation, can claim mathematical definition of the concept of randomness. In this case, sequences are considered in binary format. According to the definition of von Mises, the sequences are divided into 2 groups: random and non-random. From a mathematical point of view, random sequences form a plurality of complete measure and all without exception satisfy all the laws of probability theory. In this approach, the sequence is considered to be random, if the stability of the frequencies 0 and 1 is observed both in the sequence itself and in any "correctly" chosen part thereof. According to von Mises, the admissible selection rule is that the decision to include a member in the subsequence cannot depend on the value. It is worth noting that the classes of "admissible" frequency-stable se-

quences, for which the basic laws of probability theory have been fulfilled, have not yet been determined. It has also been proved that there are sequences that satisfy the von Mises requirements, but do not satisfy the law of a second-order logarithm.

The approach proposed by Martin-Lof is that the sequence is considered to be random if it passes a set of statistical tests. The essence of testing is to verify the "zero hypothesis" in relation to the sequence being studied. The statistical test T for binary sequences of length l can be considered as a Boolean function $T: V_l \to \{1,0\}$, that divides the set of sequences V_l into a set of "non-random" sequences $V_{l,0}$ (usually small) and a set of random sequences $V_{l,1}$. The probability pr that randomly chosen sequence of length l is rejected by the test is equal to $pr = |V_{l,0}| \cdot 2^{-l}$. Typically, pr in tests has a small value, $pr \le 0.01$. Since some of the necessary properties can be analytically proven only for some classes of sequences, a wide range of different statistical tests can be found to justify the properties of the sequences, which allow the patterns to be revealed. The results of statistical tests show that for maps 1.6 and 1.7 of the sequence the best randomness measure is shown on individual tests, however, this is not performed for the entire test group, and this does not allow viewing the displayed mappings as generators of pseudorandom numbers, as the necessary condition for randomness is not provided.

In this paper, we also analyze the chaotic nature and unpredictability of the internal structure of generated sequences for the formation of a truly random sequence concept. When considering the concept of randomness, Kolmogorov's complexity theory is used, where the basic idea is based on the fact that the complexity of an object is determined by the length of its description. The complexity of a sequence y for a given map f is the number $R_f(y) = \min\{|x|: x \in f\text{-}опис\ y\}$, where |x| - the length of the sequence. If an object cannot be described, then its complexity approaches infinity. When the internal structure of numerical sequences is considered, the presence of internal analogous sequences means that these internal structures can be grouped into separate classes and a description can be assigned to each class, which reduces the size of the description of the entire sequence. Thus, when considering the internal structure of the formed sequences, it is necessary to construct generators that give sequences, where the subsequence will have the least degree of similarity.

Passing to the consideration of unpredictability, we understand the sequence as unpredictable, if for the arbitrary selection of its elements knowledge about these elements does not allow to predict the values of the following elements of the sequence. As this work explores processes in nonlinear dynamic systems, unpredictability is the result of sensitivity to the initial conditions of systems. A sequence is called predicted if there is a mapping for it that allows you to get a sequence element based on the previous values. Thus, periodic similar subsequences allow the calculation of elements of the sequence with a certain level of similarity. It is known that any chaotic sequence is unpredictable. However, the issues of coincidence of classes of chaotic and unpredictable sequences remain open.

Given the internal structure of the sequences derived from the above-mentioned maps, there is a problem of finding and evaluating such structures. The presence or absence of which reflects a degree of approximation of this sequence to randomness. Accordingly, a mapping that generates sequences with fewer similar sequences and a smaller length of these subsequences can be considered for further analysis on the possibility of using it as a pseudorandom sequence generator. Hence the problem of choosing a measure of similarity to evaluate the resulting sequences. In general, a measure of similarity allows us to generalize the structural representation of an object. To obtain reliable results of the similarity measure, the ideal measure $D(x, y)$ for evaluating x and y of the subsequences must have the following properties (ε - a small value, given in advance):

1) Positivity: $D(x, y) \ge 0$;
2) Coincide axiom: $D(x, y) = 1 \text{ if } x = y$;
3) Symmetry: $D(x, y) = D(y, x)$;
4) Triangle inequality: $D(x, y) < D(x, z) + D(z, y)$, where z represents another object;
5) Compactness: If x and y are very similar, then $1 - D(x, y) < \varepsilon$;
6) True representation: if $D(x, y) < \varepsilon$, then x and y are very similar;
7) Continuity of D.

However, not all measures meet all these requirements and, accordingly, the similarity measures are chosen in accordance with the task and subjects of the study.

Consider the existing approaches and methods for assessing the degree of similarity. The first type of similarity measurement evaluates and compares the overall shape of the sequences based on the actual values of the sequence. There are two subcategories: rigid step-by-step and elastic measures. The rigid step-by-step measures require that the two se-

quences be the same length, while the elastic measures are more flexible and allow "single-valued" and "one-to-one" comparison for the elements of the sequences [8]. The second type of similarity measurement are characteristic measures, which first determine the properties of the subsequence, and then measure the distance between these characteristics. Characteristic measures are often used to reduce the size of the evaluated objects. The third category, the distance of the editing, expresses the discrepancy between the two sequences based on the minimum number of operations required to convert one subsequence to another.

The simplest measure of similarity for comparing subsequences is any L_n norm of the form:

$$d_{L_n}(x, y) = (\sum_{i=1}^{M}(x_i - y_i)^n)^{1/n} \quad (7)$$

where n is an integer, M is the length of the subsequence. Measures based on L_n are categorized as rigid step-by-step measures and compare structures of the same length. In the case when $n = 2$ we get the Euclidean norm whose evaluation process is shown on figure 10.

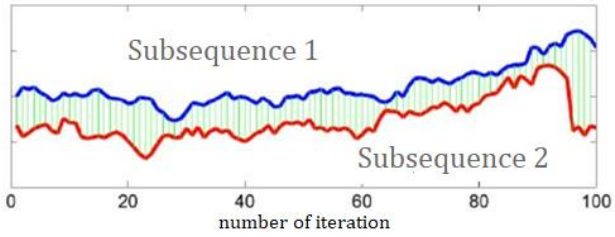

Fig. 10 – Comparison process for rigid step-by-step measure

However, such measures do not identify the similarity of sequences if they are not aligned with the X axis. Accordingly, the problem of "deforming" the values of the X axis for one of the sub sequences appears. This problem allows us to solve elastic measures, such as the method of Dynamic Time Warping (DTW) [9], but such measures increase the complexity of calculations and the time required to obtain the result. In the case of DTW measurements, the local cost metric (LC) ($n \times m$) is calculated initially, where each element of the matrix determines the distance between the corresponding elements of the sequence. The next step is determining the path of transformation:

$$W = w_1, w_2, \ldots w_K, \max(n, m) \le K \le m + n - 1 \quad (8)$$

This path circumvents the LC matrix with conditions such as: boundary condition, continuity, monotony. The total distance for the path W is determined by summing up the individual elements of the LC matrix that cover the path. To obtain a DTW measure, it should be selected a path with a minimum total distance. The complexity of the calculation in this case is $O(nm)$ with the use of dynamic programming methods (DPs). The following recurrence ratio of DP can be used to calculate a path with a minimum length of:

$$d_{cum}(i, j) = d(x_i, y_j) + \min\{d_{cum}(i-1, j-1), d_{cum}(i-1, j), d_{cum}(i, j-1)\} \quad (9)$$

Several scales have been developed for direct measure of DTW, one of which is the root of the sum of the elements of the path with a minimum length:

$$d_{DTW}(x, y) = \min \sqrt{\sum_{k=1}^{K} w_k} \quad (10)$$

It is worth noting that the DTW measure is equal to the Euclidean norm if $n = m$, and also does not satisfy the 4th condition, which is advanced to the degree of similarity. Due to the need to calculate matrices, this method is one of the most time consuming, even in optimization conditions, so it is not considered in this paper.

The following groups of measures of similarity represent the characteristic measures, among which the main is the discrete Fourier transform (DFT). As noted above, this measure evaluates the characteristics of the comparable structures and, since it is calculated only for half of the subsequence elements $q = n/2$ in accordance with the Nyquist-Shannon sampling theorem, it allows to obtain a gain in the general time of the calculation. The DFT is obtained by computing the product between the subsequence and the sinusoid and is defined as:

$$X(l) = \sum_{k=0}^{N-1} x_k e^{-i2\pi lk/n} \quad (11)$$

As a result, we obtain a vector $X(l)$ of complex numbers. According to Parseval's theorem, the DFT retains the Euclidean distance between sequences. That is, when all frequencies in the frequency domain $X(f)$ are used, the Euclidean distance between the two DFTs is equal to the distance between the initial sequences for these transformations, since the DFT is a linear transformation. The calculation of the distance between sequences on the basis of Fourier coefficients is $O(q)$ and therefore the whole process of computing the DFT measures for all sequences is $O(N n \log n + qN^2)$, where N is the number of all subsequences.

3. Computer modeling and estimation for nonlinear dynamical systems

Computer representation of the structure and behavior of dynamic systems is at the center of development of modern complex systems. Such representations are created and reviewed based on the use of graphical modeling languages that support

specification, analysis, development and testing of systems.

To accomplish the tasks and program realization, the Wolfram language and Wolfram Mathematica 11.0 [17] have been selected. The programming language of Wolfram is supported by a variety of programming paradigms with an emphasis on functional programming. It has a large set of built-in functions, graphing tools, and also allows you to implement dynamic interactive computations that allow you to manipulate data and analyze dynamically changing results. The Mathematica system provides a wide set of higher-order functions, meta-algorithms through which a progressive multi-level environment is implemented with automation when constructing user interfaces. Built-in function sets allow you to implement algorithms of various mathematical directions, such as number theory, dynamic systems, and others. Mathematica also implements parallel programming capabilities, which reduces computing time. The system supports numbers of any accuracy, and also for the purpose of increasing the accuracy of the environment, uses symbol-no calculations that allow expressions to be transformed.

In this paper we consider the application of measures of form estimation and DFT measure as an example of the characteristic measure, since they provide a simple process for the implementation of calculations and allow us to draw conclusions about the internal structure of the sequences considered in this paper. As a rigid step-by-step measure, the measure is based on the correlation coefficient. Among the various correlation coefficients we will use the Spirman correlation, since the Spirman correlation coefficient does not contain any assumptions about the distribution. Sequences will be called similar if the measure takes a value greater than 0.5. The Spirman correlation coefficient can be calculated using the following equation:

$$r_s = 1 - \frac{6\sum d_i^2}{N(N^2 - 1)}, \qquad (12)$$

where d_i - the difference between the rank for each pair of data, and the value N - the number of data pairs. The Spearman correlation coefficient calculates the p-value in the same way as the linear regression and Pearson correlation, except that the calculation takes place for ranks, not magnitudes. It is worth noting that the price for the best properties of the Spirman correlation is the greater complexity of the calculations, which is *O(n log n)*, while the Pearson correlation calculation has the complexity of *O(n)*. However, modern methods of parallel computing can minimize this time difference. To evaluate the internal structure of the sequences derived from maps, next method is used that includes the following steps:

Step 1. The first peak position is computed in order to remove the initial exponential component from calculation;

Step 2. Determines the size of the initial succession for evaluation with the following elements of the sequence;

Step 3. Using the single step, the Spearman correlation value of the reference subsequence with the corresponding subsequences is calculated;

Step 4. The obtained correlation values are finite according to the specified level of similarity;

Step 5. The size of the initial subsequence decreases by 1 if it exceeds 10 elements, and steps 1-4 are repeated.

Thus, this method allows obtaining a hierarchy of internal cycles according to the length of the cycle, as well as the degree of similarity of the found structures. This hierarchy can be used to further evaluate the sequence. In accordance with a step-by-step approach to the search for similar subsequences, we obtain a set of values that could identify a subsequence that exceeds the initial value.

Considering the results for the individual sequences, the results of the evaluation of the degree of similarity allow us to obtain a hierarchy of similar sequences based on the length of the internal cycles and the level of similarity presented in table 1. In this table: s – length of the pattern, l – searched similarity measure, pat – initial position of used pattern, comp – some compared pattern, SM – obtained similarity measure for two subsequences.

Table 1.

Similar subsequences for the map 2.4 and p=521

s	**l**	**pat**	**comp**	**lag**	**SM**
11	0,7	{9, 19}	{20, 30}	36	0,772727
11	0,8	{17, 27}	{28, 38}	33	0,836364
11	0,9	{40, 50}	{51, 61}	53	0,972727
15	0,7	{19, 33}	{34, 48}	67	0,717857
15	0,8	{36, 50}	{51, 65}	49	0,817857
15	0,9	{13, 27}	{28, 42}	67	0,907143
20	0,7	{11, 30}	{31, 50}	62	0,795489
20	0,8	{13, 32}	{33, 52}	62	0,842105
25	0,7	{50, 74}	{75, 99}	6	0,731538
30	0,6	{10, 39}	{40, 69}	52	0,631146
30	0,6	{46, 75}	{76, 105}	1	0,63337

Comparing the chosen similarity measures, the best results from the search for similar sequences demonstrate the DFT measure, since it represents the estimation of the subsequence in the form of the sum of harmonic oscillations, respectively, allows for a more precise estimation. Also, the DFT measure has better computational performance by reducing the

dimension, which significantly affects the total time of the calculation for sequences that display a proportional to a prime number of length of the period. The time complexity for the DFT using the fast Fourier transform algorithm is *O(n log n)*.

The obtained results show that, from the point of view of chaos and unpredictability, the considered maps 1.4 and 1.5 show a very high degree of similarity for many internal cycles. Correlation method used in this work allowed to identify these internal sequences for further analysis.

Conclusion

The results of the work show that the best approximation to the requirements of probability theory with the use of nonlinear dynamic maps is provided by analyzing the power of the set of numbers on which the generator is based. The best sequences ensure the use of prime numbers for which the length of the period corresponds to the dimension of the number itself, since such sequences show chaotic behavior. The best results in the number of such internal cycles show sequences based on the map 1.7, which confirms the results previously obtained for this mapping, when statistical tests were used to estimate the randomness measure. At the same time, the largest number of similar internal cycles is demonstrated by sequences based on the maps 1.6, even assuming that the length of period for this map is greater compared to other maps. For reliable pseudorandom generation methods should be considered maps that generate sequences with fewer similar internal structures and smaller lengths of these subsequences.

References

1. Balasubramanian, V. (2014). Conformal Prediction for Reliable Machine Learning: Theory, Adaptations and Applications. Elsevier. p. 299.
2. Shiryaev, A. (2009). Probability and the concept of randomness: the 75th anniversary of the publication of the monograph by Kolmogorov "Basic concepts of probability theory". Moscow: MIAN. p. 92.
3. Impagliazzo, R. (2001). Randomness vs Time: Derandomization under a Uniform Assumption. JCSS. p. 672-688.
4. Rauch, J. . (2014). Math 558. Advanced ordinany differential equations and dynamical systems: Course Materials. University of Michigan. 5. Hirsch, M., Smale, S. and Devaney, R. (2013). Differential equations, dynamical systems, and an introduction to chaos. Academic Press. p. 423.
6. Vostrov, G., Opiata, R. (2017). Effective computability of the structure of the dynamic processes of the formation of primes. ELTECS №25(101).
7. Uspenskiy, V.(2009). Four algorithmic faces of randomness [Chetyre algoritmicheskikh litsa sluchaynosti]. Moscow: MCNMO, p 40.
8. Wang, X., Mueen, A., Ding, H., Trajcevski, G., Scheuermann, P., Keogh, E. (2012). Experimental comparison of representation methods and distance measures for time series data. Data Mining and Knowledge Discovery №26(2). p. 275–309.
9. Berndt, D., Clifford, J. (1994). Using Dynamic Time Warping to Find Patterns in Time Series. AAAI Press. p. 359–370.
10. Vostrov, G. Opiata, R. (2018). Computer modeling of dynamic processes in analytic number theory. ELTECS №28(104). p. 240–247.
11. Haken, H. (1983). Advanced Synergetics. Springer Berlin Heidelberg. p. 316.
12. Kholodnyuk, M., Klich, A., Kubichek, M., Marek, M. (1991). Methods for analyzing nonlinear dynamic models. Moscow: Mir. p. 368.
13. Nicolis, J. The Dynamics of Hierarchical Systems: An Evolutionary Representation. (1989). Moscow: Mir. p. 490.
14. Penrose, R. (2007). The Road to Reality: A Complete Guide to the Laws of the Universe. Vintage. p. 1136.
15. Skiadas, Ch., Skiadas, Ch. (2016). Handbook of Applications of Chaos Theory. CRC Press. p. 910.
16. Crandall R., Pomerance K. (2005). Prime numbers: cryptographic and computational aspects. Springer. p. 597.
17. Lynch, S. (2007). Dynamical Systems with Applications using Mathematica. Birkhauser Boston. p. 477.

МАТЕМАТИЧНІ ОСНОВИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В СУЧАСНИХ НЕЛІНІЙНИХ ДИНАМІЧНИХ СИСТЕМАХ

Г. М. Востров, А. О. Хріненко
Одеський національний політехнічний університет

Анотація. *Розглянута і узагальнена гіпотеза про існування 3х класів процесів: фізичних, ментальних та математичних. У відповідності до визначення узагальненої моделі взаємодія цих процесів має місце як прямий, так і зворотній зв'язок. Доведено, що взаємодія між цими процесами адекватно описується за допомогою математичної моделі нелінійних динамічних систем. Встановлено, що*

першорядними елементами даних моделей є інформація та відповідні інформаційні технології. Доведено, що в усіх нелінійних динамічних системах ключовим фактором визначення їхніх кількісних та якісних характеристик є інформація про нерухомі точки динамічної системи та властивості їхніх траєкторій. Встановлено, що в нелінійних динамічних системах будь-якого типу потенційно існує нескінченна множина нерухомих точок з потенційно нескінченною довжиною траєкторій. Досліджена проблема узгодженості різних класів динамічних систем та показано, що міра невизначеності структури траєкторій зі збільшенням довжини циклу наближається до нескінченності. Відповідно, розкриття цієї невизначеності є джерелом потенційно нескінченної кількості інформації. Встановлено, що отримана інформація може бути використана для керування процесами прийняття рішень, а в ідеалі і задачах оптимального управління. Показано, що перенесення інформації на конгруентні динамічні системи представляє собою основу інформаційних систем. Доведено, що дослідження структури циклів траєкторій є важливим джерелом інформації щодо структури хаотичних процесів, що протікають в таких системах. Такого роду дані стосовно хаотичних процесів представляють собою носій інформації, що є необхідним в системах інформаційних технологій в наступних класах задач: комп'ютерне моделювання еволюційного розвитку динамічних систем, генерація випадкових чисел, дослідження динамічної структури формування класів простих чисел, побудова методів криптографічного захисту інформації, побудова методів геш-функцій, дослідження нерухомих точок, прогнозування часових рядів та ряд інших прикладних задач. Досліджені методи оцінки узгодженості різних типів динамічних систем, що задаються за допомогою нелінійних відображень.

Ключові слова: *динамічні системи, відображення, випадковість, траєкторії, хаотичні процеси.*

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СОВРЕМЕННЫХ НЕЛИНЕЙНЫХ ДИНАМИЧЕСКИХ СИСТЕМАХ

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

Аннотация. *Рассмотрена и обобщенная гипотеза о существовании 3х классов процессов: физических, ментальных и математических. Доказано, что во всех нелинейных динамических системах ключевым фактором определения их количественных и качественных характеристик является информация о неподвижных точках динамической системы и свойствах их траекторий.*

Ключевые слова: *динамические системы, отображения, случайность, орбиты, хаотические процессы*

Received on 28.02.2019

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. E-mail: vostrov@gmail.com, тел. +380503168776

Востров Георгій Миколайович, кандидат технічних наук, доцент кафедри прикладної математики та інформаційних технологій Одеського національного політехнічного університету. Проспект Шевченко, 1, Одеса, Україна.
E-mail: vostrov@gmail.com, тел. +380503168776

ORCID ID: 0000-0003-3856-5392

Khrinenko Andrii, master of the Department of Applied Mathematics and Information Technologies, Odessa National Polytechnic University. Shevchenko ave., 1, Odessa, Ukraine. E-mail: khrinenko.andrew@gmail.com, тел. +380637515228

Хріненко Андрій Олегович, магістр кафедри прикладної математики та інформаційних технологій Одеського національного політехнічного університету. Проспект Шевченко, 1, Одеса, Україна.
E-mail: khrinenko.andrew@gmail.com, тел. +380637515228

ORCID ID: 0000-0001-6000-2102