Acta Technica *62* (2017), No. 5A, 827–836

Randomness analysis of chaotic sequences by permutation entropy

Bocheng Liu[2], Lingfeng Liu[2]

Abstract. Permutation entropy is a widely used criterion in evaluating the randomness of sequences. In this paper, we use permutation entropy to evaluating the randomness of two kinds of popular chaotic maps, Tent map and Logistic map. The interesting results show that the permutation entropy of chaotic iterative sequences generated by these two chaotic maps is much smaller than the permutation entropy of ideal random sequences, which means that the chaotic iterative sequences can not be regarded as random sequences. Both theoretical and numerical methods are provided to prove this conclusion.

Key words. permutation entropy, chaotic iterative sequences, randomness.

1. Introduction

Pseudorandom bit sequences are widely used in a large amount of different scientific fields, such as spread spectrum communications and cryptography [1]. At the beginning, pseudorandom bit sequences are always generated by using linear algebra theory, eg, linear feedback shift register or linear congruential method. However, some researches show that this kind of pseudorandom bit sequence would be attacked due to its inner linear structure. Therefore, using a nonlinear source for pseudorandom bit sequences generation is the major idea.

The chaotic system, which performs complex dynamical characteristics, such as highly sensitive to its initial condition and parameters, unpredictability and randomness, et al, is regarded as a new kind of pseudorandom source in the generation of pseudorandom bit sequences. In practical applications, the one-dimensional chaotic maps are the most widely used ones for their simple structures [2-4], which are easy to implement.

[1]Acknowledgement - This work is supported by the National Natural Science Foundation of China (61601215); Science & technology research project of Education Department of Jiangxi Province (GJJ150104). Primary Research &Developement Plan of Jiangxi Province (20171BBE50064); Subsidy scheme for academic and technological leaders of major disciplines in Jiangxi (20172BCB22035)

[2]Workshop 1 - School of Software, Nanchang University, Nanchang, 330031, China

The most important criteria to judge whether a pseudorandom sequence can be used is its randomness. Until now, some statistical test suites for randomness test are proposed, notably, FIPS140-1, Crypt-XS, SP800 and recently, TestU01. In 2002, Bandt proposed a new natural complexity measure for time series/sequences, called permutation entropy (PE) [5]. PE compares the size of some consecutive values in the sequence, and summed up different order types, then use Shannon's entropy to measure the uncertainty of these ordering. This new complexity measure is easily implemented and is computationally much faster than other comparable methods, such as Lyapunov exponents, while also being robust to noise [6], which makes it as a popular criterion in evaluating the characteristics of sequences [7-10]. [7] uses PE to investigate the complexities of different traffic series. [8] uses PE to characterize the complexity of chaotic signals generated by an external-cavity semiconductor laser. PE are used to analyze fluctuating time series of three different turbulent plasmas in [9]. [10] develops a method based on PE to characterize electrocardiograms and electroencephalographic records from different stages in the treatment of a chronic epileptic patient, et al.

In this paper, we use PE to evaluate the randomness of two kinds of popular one-dimensional chaotic maps, Tent map and Logistic map. Although some studies on these maps have already existed, they only consider the situation with order $m = 2$ [11]. In this paper, we extend the analysis of these two maps to order $m = 3$, and to > 3 as well. The interesting results show that the PE of chaotic iterative sequences generated by these two chaotic maps are much smaller than the PE of ideal random sequences, which means that the chaotic iterative sequences cannot be regarded as random sequences in this sense. This result is contradictory with our general view that chaotic map is randomness. Both theoretical and numerical methods are provided to prove this conclusion. This conclusion shows that the chaotic iterative sequences can not be regarded as ideal random sequences for practical uses.

The rest of this paper is organized as follows. Some preliminaries for chaotic map and PE are introduced in Section 2. The PE of iterative sequences by Tent map and Logistic map are analyzed in Section 3 and 4, respectively. Finally, Section 5 concludes the whole paper.

2. Preliminaries

Perhaps the simplest mathematical objects that can display chaotic behavior are a class of one-dimensional maps [12], which can be described as follows.

$$x_{k+1} = f(x_k) = f^{k+1}(x_0) \tag{1}$$

where, x_k is the state variable, x_0 is an arbitrary initial value, f: II is the mapping function, where I denotes an interval. $f^n(x_0)$, n=0, 1, 2, ..., means n times of iterations by using function f from initial value x_0. Once we select an initial value x_0, we can generate a sequence $\{f^n(x_0)\}_{n=0}^{\infty}$according to Eq. (1). We call this sequence a chaotic iterative sequence if function f is chaotic on interval I. Almost all the chaotic iterative sequences perform high dynamical complexity except for a

set with Lebesgue measure zero.

Now, we briefly review the descriptions of PE in [14]. PE compares the size of some consecutive values in the sequence, and summed up different order types, then use Shannon's entropy to measure the uncertainty of these orderings. The mathematical definition is as follows.

Definition 1 [14]: Consider a time series $\{x_t\}_{t=1,...,T}$. We study all $m!$ permutations$M$ of order m which are considered here as possible order types of m different numbers. For each M we determine the relative frequency (# means number)

$$p(M) = \frac{\#\{t|t \leq T-m, (x_{t+1}, ..., x_{t+m}) \text{ has type } M\}}{T-m+1}$$

This estimates the frequency of M as good as possible for a finite series of values. The permutation entropy of order m 2 is defined as$H(n) = -\sum p(M) \log p(M)$where the sum runs over all $m!$ permutations$M$ of order m.

The following example maybe helpful in understanding this definition.

Example: Consider a time series/sequence with eight values x = (2.14, 3.48, 5.09, 4.11, 8.65, 8.97, 3.95, 9.26). First, we take order $m = 2$. Comparing the seven pairs of neighbors, then we have 2.14 < 3.48, 3.48 < 5.09, 5.09 > 4.11, 4.11 < 8.65, 8.65 < 8.97, 8.97 > 3.95 and 3.95 < 9.26. In total, there are five of seven satisfy x_i<x_{i+1}, and two of seven satisfy x_i<x_{i+1}. Then, according to definition 1, the PE of order m = 2 can be calculated as –(5/7)log(5/7) – (2/7)log(2/7) 0.5983. Then, we can take order $m = 3$. Now we should compare the order of three consecutive values. (2.14, 3.48, 5.09) and (4.11, 8.65, 8.97) satisfy x_i<x_{i+1}<x_{i+2}; (3.48, 5.09, 4.11) satisfies x_i<x_{i+2}<x_{i+1}; (5.09, 4.11, 8.65) and (8.97, 3.95, 9.26) satisfy x_{i+1}<x_i<x_{i+2}; (8.65, 8.97, 3.95) satisfies x_{i+2}<x_i<x_{i+1}. Then, according to definition 1, the PE of order m = 3 can be calculated as –2(1/6)log(1/6) – 2(2/6)log(2/6) 1.3297. Furthermore, PE of order m = 4, 5, ... can also be calculated similarly.

It is clear that for an ideal random sequence, all kinds of possible permutations will appear with the same probability. Thus, the PE of an ideal random sequence will approach to the maximum value log$m!$. This is a value which is related to order m.[14] recommends the selection of order m be 3, 4, 5, 6 and 7. In practical uses, the following normalized PE is always used

$$\text{PE} = \text{PE}(m)/\log m!$$

Normalized PE is a independent with order m. For an ideal random sequence, no matter how much the order m is, PE will closely approach to value 1. On the other hand, a sequence with PE much smaller than 1 can not be regarded as a random sequence.

3. Pe of tent map

Tent map is a kind of piecewise linear map with its mathematical model described as follows

$$x_{k+1} = f(x_k) = \begin{cases} \frac{x_k}{h}, & 0 < x_k < h \\ \frac{1-x_k}{1-h}, & h < x_k < 1 \end{cases} \tag{2}$$

where, 0 <h <1 is the control parameter. The most excellent property of Tent map for practical uses is that the chaotic iterative sequence is uniformly distributed in the interval [0, 1], for each parameter h.

Now, we consider the PE of chaotic iterative sequences by Tent map.

Order $m = 2$

For $m = 2$, we should compare the order of all neighbors. Choose an arbitrary x, by comparing the order of x and $f(x)$, we have that the critical condition $x = f(x)$ holds if$x = \frac{1}{2-h}$Then, if x[0, 1/(2–h)], we have x<$f(x)$; Else, if x,[1/(2–h), 1], we have x>$f(x)$. Due to the uniform distribution property of Tent map, according to definition 1, the PE of order m = 2 can be calculated as

$$\mathrm{PE} = -\frac{1}{2-h}\log(\frac{1}{2-h}) - (1-\frac{1}{2-h})\log(1-\frac{1}{2-h}) = \log(2-h) - \frac{1-h}{2-h}\log(1-h) \tag{3}$$

The relationship between normalized PE of order $m = 2$ and parameter h is plotted in Figure 1. In Figure 1, The blue dots present the PE values of order $m = 2$ for actual sequences of Tent map, the red line is the theoretical curve of Eq. (3), and the green line is the ideal value of PE for ideal random sequences. From Figure 1 we have that the numerical values are extremely close to the theoretical curve. With the growth of parameter h, the PE will decrease. The PE is close to the ideal PE line only with h approaches to zero. The reason is that the size of intervals [0, 1/(2–h)] and [1/(2–h), 1] is different for h> 0.

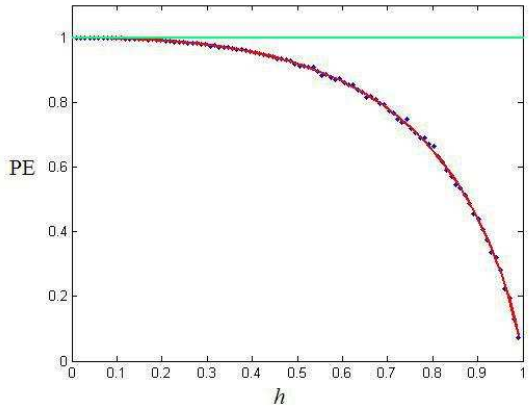

Fig. 1. Figure 1

Figure 1 Relationship between normalized PE of order $m = 2$ and parameter h

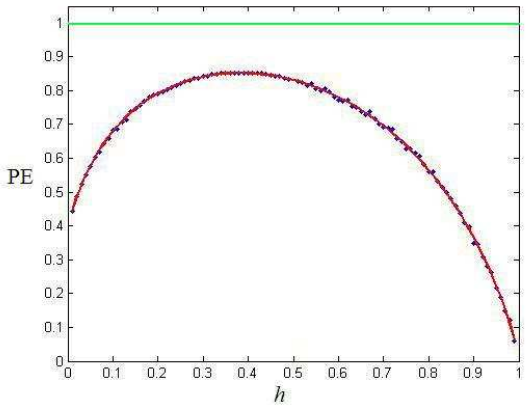

Fig. 2. Figure 2

for Tent map. The blue dots present the PE values for actual sequences of Tent map, the red line is the theoretical curve of Eq. (3), and the green line is the ideal value of PE for ideal random sequences.

2) Order $m = 3$

Once we take $m = 3$, we should compare the order of three consecutive values. For an arbitrary x, in order to compare the order of x, $f(x)$ and $f^2(x)$, we should first determine the order of $f(x)$ and h, for the piecewise linear characteristic of Tent map. Let $f(x) < h$, we can derive that $0 < x < h^2$ or $1 - h + h^2 < x < 1$. Then, according to the order of three critical values h^2, h and$1 - h + h^2$, we can divide the while interval [0, 1] into four sub-intervals, [0, h^2], [h^2, h], [h,$1 - h + h^2$] and [$1 - h + h^2$,1].

If x[0, h^2], for any x, we have $f(x) = x/h$ and $f^2(x) = x/h^2$. Obviously, we can derive the order $x < f(x) < f^2(x)$ for $0 < h < 1$.

If x[h^2, h], for any x, we have $f(x) = x/h$ and $f^2(x) = \frac{1-x/h}{1-h}$.

Obviously, $x < f(x)$ always holds. Next we compare the order of x, $f^2(x)$ and $f(x)$, $f^2(x)$.

Assume $f(x) < f^2(x)$, we have $x < h/(2-h)$. Moreover, assume $x < f^2(x)$, we have $x < h/(1+h-h^2)$. Due to $0 < h < 1$, we have that $h^2 < h/(2-h) < h/(1+h-h^2) < h$. Therefore, if $x \in [h^2, h/(2-h)]$, the order satisfies $x < f(x) < f^{\,2}(x)$; If x,[$h/(2-h)$, $h/(1+h-h^2)$], the order satisfies $x < f^2(x) < f(x)$; If x,[$h/(1+h-h^2)$, h], the order satisfies $f^2(x) < x < f(x)$.

If x[h,$1 - h + h^2$], for any x, we have $f(x) = \frac{1-x}{1-h}$, $\quad f^2(x) = \frac{1-\frac{1-x}{1-h}}{1-h} = \frac{x-h}{(1-h)^2}$

In this sub-interval, once $x < f(x)$, then there must have $f(x) > f^2(x)$. On the contrary, there must have $f(x) < f^2(x)$. Thus, we only need to compare the orders of x, $f(x)$ and x, $f^2(x)$.

Assume $x < f\ (x)$, we have $x < 1/(2-h)$; Moreover, assume $x < f^2(x)$, we have $x > 1/(2-h)$. Due to $0 < h < 1$, we have $h < 1/(2-h) < 1 - h + h^2$. Therefore, if x??[h, $1/(2-h)$], we have the order $f^2(x) < x < f(x)$; If x [$1/(2-h)$, $1 - h + h^2$],

we have the order $f(x) < x < f^2(x)$.Finally, if x [1 $-h$ + h^2,1], for any x, we have $f(x) = \frac{1-x}{1-h}$, $f^2(x) = \frac{1-x}{h(1-h)}$

In summary, for any x, if xI1, we have x < f(x) < f2(x); if xI2, we have x < f2(x) < f(x); if xI3, we have f2(x) < x < f(x); if xI4, we have f(x) < x < f2(x); and if xI5, we have f(x) < f2(x) < x, where I1, I2, I3, I4 and I5 are presented as

$$I_1 = [0, \frac{h}{2-h}] I_2 = [\frac{h}{2-h}, \frac{h}{1+h-h^2}] I_3$$

$$= [\frac{h}{1+h-h^2}, \frac{1}{2-h}], I_4 = [\frac{1}{2-h}, \frac{1}{1+h-h^2}] I_5$$

$$= [\frac{1}{1+h-h^2}, 1]$$

Due to the uniform distribution property of Tent map, according to definition 1, the PE of order m = 3 can be calculated as

$$T = \frac{ab}{2}\omega^2 \int_A h(\xi)\rho w^2 \, \mathrm{d}A \tag{4}$$

By using Eq. (4), we can derive that the PE has reached its maximum when h 0.382. The relationship between normalized PE of order $m = 3$ and parameter h is plotted in Figure 2. In Figure 2, The blue dots present the PE values of order $m =$ 3 for actual sequences of Tent map, the red line is the theoretical curve of Eq. (4), and the green line is the ideal value of PE for ideal random sequences. From Figure 2 we have that the numerical values are also extremely close to the theoretical curve. With the growth of parameter h, the PE will first increase, and then decrease after reaching the maximum value. The maximum value of PE is still lower than the ideal value 1. The following two reasons induce this conclusion.

1. For $m = 3$, there should have 3! = 6 types of order for an ideal random sequence. However, only 5 types of order appear in the chaotic iterative sequences of Tent map. The order $x > f(x) > f^2(x)$ never appears.

2. The size of intervals I_1, I_2, I_3, I_4 and I_5 are different from each other, which makes the frequency of each type of order different.

Figure 2 Relationship between normalized PE of order $m = 3$ and parameter h for Tent map. The blue dots present the PE values for actual sequences of Tent map, the red line is the theoretical curve of Eq. (4), and the green line is the ideal value of PE for ideal random sequences.

3) Order $m > 3$

Similarly, PE of order $m > 3$ can also be theoretically calculated by using the above method. Since it is getting harder for mathematical calculations, here, we use numerical simulation by Matlab for PE analysis. The relationship between normalized PE of order $m = 2, 3, \ldots, 10$ with parameter h is shown in Figure 3.

From Figure 3, we know that the whole PE curve gradually decreases with the order m increases. PE reaches its maximum value when $h = 0.5$ for large m, which is consistent with the chaotic characteristics of Tent map (The Lyapunov exponent

reaches its maximum value when $h = 0.5$). [14] recommends the selection of order m be 3, 4, 5, 6 and 7, from Figure 3 we can see that the PE values are much smaller than the ideal value 1, which means that the chaotic iterative sequences can not be regarded as ideal random sequences in this sense. This result is in contradiction with the pseudorandom property of chaotic maps.

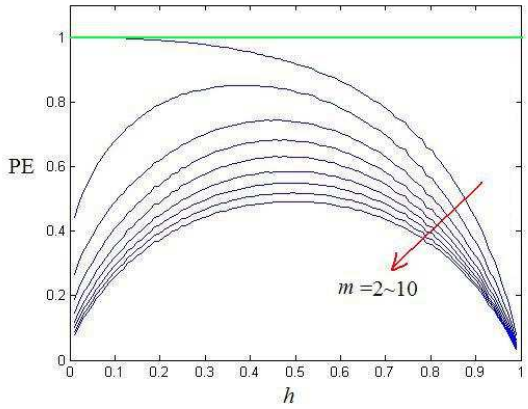

Fig. 3. Figure 3

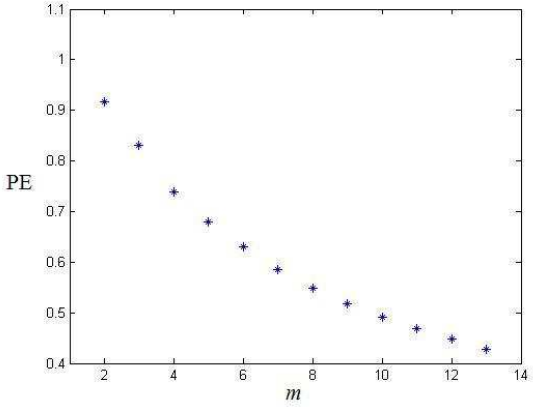

Fig. 4. Figure 4

Figure 3 Relationship between normalized PE of order $m = 2$ to 10 and parameter h for Tent map. The blue curves present the PE of order 2 to 10 from top to bottom, the green line is the ideal value of PE for ideal random sequences.

4. Pe of logistic map

In this section, we analyze the PE of following zero-mean Logistic map

$$x_{k+1} = g(x_k) = 1 - rx_k^2 \tag{5}$$

where, r is the control parameter. When $r = 2$, Eq. (5) is bounded in the interval [–1, 1], and has excellent ergodicity. In this paper, we set $r = 2$. Statistically, the iterative value satisfies the following probability density function $p(x) = \frac{1}{\pi\sqrt{1-x^2}}$

Now we analyze the PE of the chaotic iterative sequences by Eq. (5). First, we consider the case of $m = 2$. Compare the order of x and $g(x)$. The critical condition $x = g(x)$ holds when $x = 1/2$. Therefore, when x[–1, 1/2], we have $x<g(x)$; When x[1/2, 1], we have $x>g(x)$. According to its probability distribution, for any x, the probability of $x<g(x)$ holds can be written as

$$p_1 = \int_{-1}^{1/2} \frac{1}{\pi\sqrt{1-x^2}} = \frac{1}{\pi}\arcsin x|_{-1}^{1/2} = \frac{2}{3}$$

Then, the probability that $x>f(x)$ holds is 1/3. According to the definition of PE, the PE of order $m = 2$ can be calculated as

$$\text{PE} = -(1/3)\log(1/3) - (2/3)\log(2/3) = 0.6365 \tag{6}$$

Then, we consider the case of $m = 3$. In this case, we should compare the order of three consecutive values. For any x, we have

$$g(x) = 1 - 2x^2, \qquad g^2(x) = 1 - 2(1-2x^2)^2 = 8x^2 - 8x^4 - 1$$

Assume $x<g(x)$, we have $-1 < x < 1/2$. Assume $g(x) < g^2(x)$, we have $-1 < x < -1/2$ or $1/2 < x < 1$.

Next, we compare the order of x and $g^2(x)$. Construct a new function as follows, $G(x) = 8x^2 - 8x^4 - 1 - x$

Let $G(x) = 0$, we can get four critical values. They are $x_1 = -1$, $x_2 = \frac{1-\sqrt{5}}{4}$, $x_3 = 1/2$, $x_4 = \frac{1+\sqrt{5}}{4}$, from small to large, respectively. Thus, if x [x_1, x_2]∪[x_3, x_4], the order $x<g^2(x)$ holds; If x,[x_2, x_3]∪[x_4, 1], the order $x>g^2(x)$ holds.

In summary, for any x, if xU1, we have x < g(x) < g2(x); if xU2, we have x < g2(x) < g(x); if xU3, we have g2(x) < x < g(x); if xU4, we have g(x) < x < g2(x); and if xU5, we have g(x) < g2(x) < x, where U1, U2, U3, U4 and U5 are presented as

$$U_1 = [-1, -1/2] U_2 = [-1/2, \frac{1-\sqrt{5}}{4}]$$

$$U_3 = [\frac{1-\sqrt{5}}{4}, 1/2], U_4 = [1/2, \frac{1+\sqrt{5}}{4}] U_5 = [\frac{1+\sqrt{5}}{4}, 1]$$

According to its probability distribution, the probability of an arbitrary x located in each interval can be written as $p_i = \int_{U_i} \frac{1}{\pi\sqrt{1-x^2}}$ where $i = 1, 2, 3, 4$ and 5. Therefore,

according to the definition of PE, the PE of order $m = 3$ can be calculated as

$$\mathrm{PE} = -\sum_{i=1}^{5} p_i \log p_i \approx 1.4898 \tag{7}$$

As with the Tent map, only 5 types of order appear in the chaotic iterative sequences of the Logistic map. The order $x > g(x) > g^2(x)$ never appears. Furthermore, the probability of each type of order is different from each other. These two reasons make the PE much smaller than the ideal PE value of ideal random sequences.

Finally, we consider the case with a larger m. Choose m from 2 to 13, the normalized PE is plotted in Figure 4 with the growth of order m.

Figure 4 The relationship between normalized PE and order m for Logistic map. Figure 4 indicates that the normalized PE gradually decreases with the growth of order m, which becomes far away from the ideal normalized PE value 1 of random sequences. This result means that the chaotic iterative sequences of Logistic map also can not be regarded as random sequences as Tent map.

5. Conclusion

In this paper, both theoretical and numerical methods are used to analyze the PE of chaotic iterative sequences of two kinds of one-dimensional chaotic maps, Tent map and Logistic map. The results indicate that for any order m, The PE of chaotic iterative sequences are much smaller than the ideal PE of completely random sequences. In this sense, the chaotic iterative sequences can not be regarded as ideal random sequences, which is contradict with the pseudorandom property of chaotic map. The authors believe that PE should be an important criteria in the randomness test. Otherwise, some information may be lost due to the non-uniform distribution of order types. In future work, we will study the deciphering method of time series based on PE.

References

[1] N. Kalouptsidis: *Signal processing systems, in Telecommunications and Signal Processing Series.* New York: Wiley (1996).

[2] A. Kanso, N. Smaoui: *Logistic chaotic maps for binary numbers generations.* Chaos Solitons & Fractals*40* (2009), No. 2, 211–220.

[3] V. Patidar, K. K. Sud: *A pseudo random bit generator based on chaotic logistic map and its statistical testing.*Informatica *33* (2009), No. 2, 257–262.

[4] L. F. Liu, S. X. Miao, H. P. Hu, Y. S. Deng: *Pseudorandom bit generator based on non-stationary logistic maps.* Applied Acoustics *18* (2015).

[5] C. Bandt, B. Pompe: *Permutation entropy: A natural complexity measure for time series.* Phys. Rev. Lett *88* (2002).

[6] J. Toomey, D. Kane: *Mapping the dynamic complexity of a semiconductor laser with optical feedback using permutation entropy.* Opt. Express *29* (2014), No. 9, 797–804.

[7] J. N. Xia, P. J. Shang, J. Wang, W. B. Shi: *Permutation and weighted-permutation*

entropy analysis for the complexity of nonlinear time series. Communications in Nonlinear Science and Numerical Simulation *31* (2015) 521–528.

[8] L. Yang, W. Pan, L. S. Yan, B. Luo, N. Q. Li: *Mapping the dynamic complexity and synchronization in unidirectionally coupled external-cavity semiconductor lasers using permutation entropy.* Journal of the optical society of America B *32* (2015), No. 7, 555–563.

[9] P. J. Weck, D. A. Schaffner, M. R. Brown, R. T. Wicks: *Permutation entropy and statistical complexity analysis of turbulence in laboratory plasmas and the solar wind.* Physical Review E *91* (2015), Nos. 1–5, 198–210.

[10] D. Mateos, J. M. Diaz, P. W. Lamberti: *Permutation Entropy Applied to the Characterization of the Clinical Evolution of Epileptic Patients under Pharmacological-Treatment.* Entropy *16* (2014),5668–5676.

[11] O. A. Rosso, H. A. Larrondo, M. T. Martin, A. Plastino, M. A. Fuentes: *Distinguishing noise from chaos.* Phys. Rev. Lett *99* (2007), 154102.

[12] A. Lasota, M. C. Mackey: *Chaos, Fractals, and Noise.* New York: Springer-Verlag (1994).

Received November 16, 2017