Properties of the Tent map for decimal fractions with fixed precision

V M Chetverikov

Department of Applied Mathematics of Moscow Institute of Applied Mathematics, National Research University Higher School of Economics, Moscow, Russia
E-mail: vchetverikov@hse.ru

Abstract. The one-dimensional discrete Tent map is a well-known example of a map whose fixed points are all unstable on the segment [0,1]. This map leads to the positivity of the Lyapunov exponent for the corresponding recurrent sequence. Therefore in a situation of general position, this sequence must demonstrate the properties of deterministic chaos. However if the first term of the recurrence sequence is taken as a decimal fraction with a fixed number "k" of digits after the decimal point and all calculations are carried out accurately, then the situation turns out to be completely different. In this case, first, the Tent map does not lead to an increase in significant digits in the terms of the sequence, and secondly, demonstrates the existence of a finite number of eventually periodic orbits, which are attractors for all other decimal numbers with the number of significant digits not exceeding "k".

1. Introduction

Interest in deterministic chaos among mathematicians and physicists was accompanied by a huge number of publications after the 70s of the last century [1-5]. A large survey of only one of the important areas of these studies [6] contained 216 references.

Significant interest of cryptologists towards deterministic chaos began, apparently from work [7], where the author gave a symmetric encryption scheme based on ergodic property of chaos.

Deterministic chaos is interesting for cryptologists because on the one hand it looks like a random process, but on the other hand it allows to restore the process accurately if the generating model and the initial conditions are known. A detailed discussion of the prospects and problems of new cryptosystems is devoted to the work [8-11]. Statistical analysis of the Tent map properties by constructing a four-level discrete model is devoted to work [12].

It is known that when chaotic systems are realized with a finite precision in digital computers, their dynamical properties are often found to be entirely different from the original versions in the continuous setting. To emphasize the essential difference between continuous chaos and digital chaos, the latter is also called pseudo chaos [13]. Similarly, digital chaotic orbits are also called pseudo (chaotic) orbits [14].

2. Mathematical definitions and assertions

The paper [15] reports some findings on a new series of dynamical indicators, which can quantitatively reflect the degradation effects on digital 1D piecewise linear chaotic maps realized with a fixed-point finite precision. To describe the processes taking place with limited accuracy of the representation of numbers, the authors used n-bit fixed-point binary decimals in the form $0.b_1b_2\ldots b_n \in [0,1)$, $b_i \in \{0,1\}$

In this paper we consider orbits of a recurrent sequence
\[ x_{n+1} = T(x_n) \quad n = 0, 1, 2 \ldots \quad x_0 \in [0, 1), \]  
where  
\[ T(x) = 2 \cdot \min\{x, 1 - x\} = 1 - 2 \cdot \lfloor x - 1/2 \rfloor \]  
is a simplest Tent map without any parameter which maps \([0,1]\) into \([0,1]\). In contrast to [15], it is assumed that the initial point of the orbit can be represented as a decimal fraction containing a given number of digits after the decimal point, and that all calculations related to the mapping (2) are carried out exactly without rounding. This possibility is implemented in mathematical packages in the form of symbolic calculations (for example, in the package "Mathematica").

We introduce several definitions that make it possible to formulate the results most simply.

**Definition 1.** The set \( I_0 \) is represented by one number 0. The set \( I_k \) \((k=1,2,\ldots)\) is a collection of numbers of the form \( 0.\alpha_1\alpha_2\alpha_3\ldots\alpha_k = \sum_{i=1}^{k} \alpha_i \cdot 10^{-i} \in I_k \), where \( \alpha_i \) are integers from 0 to 9, and \( \alpha_k \neq 0 \). The set \( \widetilde{I}_k \subset I_k \) \((k=1,2,\ldots)\) is a collection of numbers in \( I_k \) for which \( \alpha_k \neq 5 \).

**Definition 2.** The set \( J_k \) is defined as the union of sets \( J_k = \bigcup_{q=0}^{2} I_q \).

Obviously, for symbolic computations, if \( x_0 \in J_k \) then \( T(x) \in J_k \) since \( T(x) \) is a 1D piecewise linear mapping. It is easy to prove that the number of elements of this set is \( NI_k = 9 \cdot 10^{k-1} \) if \( k > 0 \) and \( NI_0 = 1 \). The number of elements of the set \( \widetilde{I}_k \) is \( N\widetilde{I}_k = 8 \cdot 10^{k-1} \). Then the number of elements of the set \( J_k \) equals to \( NJ_k = 10^k \).

**Definition 3.** The sequence of numbers defined by the recurrence relation (1) is called the orbit of the map (2) induced by the quantity \( x_0 \).

**Definition 4.** We call an eventually periodic orbit with period \( m \) an orbit that has the structure such as \( x_0, x_1, x_2, \ldots, x_p, x_{p+1}, x_{p+2}, \ldots, x_{p+m}, \) where \( x_{p+m} = x_{p+1} \).

**Definition 5.** We call a cycle \( S_k(m_k) \) of length \( m_k \) of the mapping \( T(x) \) the set of elements in \( I_k \) for which the following property holds: for any \( x \in S_k(m_k) \) the mapping \( T(x) \in S_k(m_k) \). In other words, the cycle is an invariant mapping set.

The above definitions allow us to formulate the main assertions.

**Assertion 1.** Let the orbit of the mapping be induced by an element \( x_0 \in I_k \). Then:  
1). if \( x_0 \) looks like \( x_0 = 0.\alpha_1\alpha_2\alpha_3\ldots\alpha_{k-1}S \), then \( x_k = T(x_0) \in I_{k-1} \) and all further elements of the orbit will belong to the set \( J_{k-1} \); 
2). if \( x_0 \in \widetilde{I}_k \), then all further elements of the orbit will be eventually periodic with the elements \( \in I_k \). The only attractor on this set is a cycle \( S_k(m_k) \).

**Assertion 2.** The length of a cycle \( S_k(m_k) \) is determined by a number \( k \) by the formula. 
\[ m_k = 2 \cdot 5^{k-1} \]  
The minimum and maximum elements of a cycle \( S_k(m_k) \) are defined by the formulas:  
\[ \min S_k(m_k) = 2^{k+1} \cdot 10^{-k} ; \quad \max S_k(m_k) = 1 - 2^k \cdot 10^{-k} \]
If you arrange the elements of the cycle $S_k (m_k)$ in ascending order, then the differences between two adjacent elements will be equal to either $2^{k+1} \cdot 10^{-k}$ or $2^{k+2} \cdot 10^{-k}$. In this case, the following rigid order of alternation is realized: at the beginning of the ordered series, a smaller difference is repeated three times, and then a large difference appears once. Then the situation repeats.

Assertion 3. Since the number of elements in the set $I_k$ is $N_k$ and the cycle $S_k (m_k)$ attracting these elements contains $m_k$ elements, the information compression ratio is $N_k \cdot (m_k)^{-1} = 2^{k+2}$.

The union of all cycles contained in a set $J_k$ is the set of numbers $G_k (M_k) = 0 \cup \bigcup_{q=1}^{k} S_q (m_q)$. The number of elements in the collection of cycles is

$$M_k = 1 + \sum_{q=1}^{k} m_q = \frac{1}{2} (5^k + 1) \quad \text{(odd number).}$$

In this case, all possible orbits induced by all the different elements $x_0 \in J_k$ are attracted by the $M_k$ elements of the $k$ cycles and, consequently, the degree of information compression is $N_k \cdot (M_k)^{-1} = 2 \cdot 10^k \cdot (5^k + 1)^{-1}$.

Figure 1 shows a diagram of all possible orbits initiated by different values $x_0 \in I_1$. Bold lines indicate the links between the two elements of the cycle $S_1 (2) = \{0.4, 0.8\}$. There are ten elements from the initial set $x_0 \in I_2 \setminus I_2$ which go to the level $I_1$: $x_i = T(x_0) \in I_1$, and only the element 0.5 leaves the level $I_1$ to the level $I_0$.

![Diagram of possible orbits](image)

Figure 1. Orbits passing through the elements $x \in I_1$, as well as transitions from $I_2$ to $I_1$ and from $I_1$ to $I_0$ as a result of the transformation (1).

Each element in the set $I_k$ of the orbit has two incoming lines and one output line.

This means that there are two different elements $\bar{x}, \bar{x} \in I_k \cup I_{k+1}$, for each element $x_i$ of the orbit $x_i \in I_k$ such that
\[ T(\bar{x}) = x_i, \quad T(\bar{x}) = x_i \]  

Equations (5) imply the irreversibility of motion along the orbit and, consequently, the inability to completely restore the orbit in reverse time. For orbits from the set \( J_k \), the ergodicity condition is not satisfied. This condition is essential for the encryption scheme proposed in [7], using the chaotic sequence of the logistic mapping.

However, it can be suggested to use the scheme proposed in [7] for the deterministic sequence (1), (2) having a definite cycle system if the calculations (1), (2) are carried out symbolically.

In addition to the above cycles built on decimals, there are a large number of cycles built on various other denominators. We introduce the notation for cycles based on a fraction with the denominator \( q \), where the number \( m \) denotes the cycle length (the number of elements in the cycle), and \( l \) is the number of the cycle of length \( m \). In case the cycle of the given period is the only one, then the superscript is not mentioned. Some of them are listed below.

Three of these cycles are often encountered in the literature
\[ C_7(3) = \{2/7, 4/7, 6/7\}, \quad C_9(1) = \{2/9, 4/9, 8/9\}, \]
\[ C_{11}(5) = \{2/11, 4/11, 6/11, 8/11, 10/11\}. \]

Five others do not attract great care of the researchers:
\[ C_{31}^{(1)}(5) = \{2/31, 4/31, 8/31, 16/31, 30/31\}, \quad C_{31}^{(2)}(5) = \{6/31, 12/31, 14/31, 24/31, 28/31\}, \]
\[ C_{31}^{(3)}(5) = \{10/31, 18/31, 20/31, 22/31, 26/31\}, \]
\[ C_{41}^{(1)}(10) = \{2/41, 4/41, 8/41, 10/41, 16/41, 18/41, 20/41, 32/41, 36/41, 40/41\}, \]
\[ C_{41}^{(2)}(10) = \{6/41, 12/41, 14/41, 22/41, 24/41, 26/41, 28/41, 30/41, 34/41, 38/41\}. \]

3. Conclusion
The Tent map (1) has the following two important properties. First, this transformation does not increase the number of significant digits for each subsequent transformation. Secondly, this transformation has attractors, which are determined by the number of digits after the decimal point. These properties are proposed to be used in the Baptista’s encryption scheme instead of logistic mapping.

The advantage of the proposed mapping is that there is no need to partition the interval (0,1) into discrete subsets to fix a number. The drawbacks of the proposed scheme include the need for symbolic calculations.

Acknowledgment
In conclusion, the author expresses his gratitude to professor E A. Krouk for his consultations on cryptography.

References
[1] Lorenz E N 1963 Deterministic nonperiodic flow, J. Atmos. Sci. 20 130
[2] Sparrow C 1982 The Lorenz equations: bifurcations, chaos and strange attractors Appl. Math.Sci.V.41 (Berlin: Springer)
[3] Schuster H G 1984 Deterministic Chaos (Weinheim: Physik-Verlag)
[4] Shapiro A P and Luppov S P 1983 Recurrent equations in the theory of population biology (Moscow: Nauka)
[5] Nedostupov E V, Sarancha D A, Chigerov E N and Yurezanskaya Yu S 2010 On some properties of one-dimensional unimodal mappings. Reports of the Academy of Sciences 430 No 1 pp 23–28
[6] Marwan N, Carmen Romano M, Thiel M and Kurths J 2007 Recurrence plots for the analysis of complex systems Physics Reports 438 237 – 329
[7] Baptista M S 1998 Cryptography with chaos Physics Letters A, 240 (12) 50-54
[8] Alvarez G, Montoya F, Romera M and Pastor G 2003 Cryptanalysis of a chaotic secure communication system Physics Letters, A 306 200–205
[9] Alvarez G, Montoya F, Romera M and Pastor G 2003 Cryptanalysis of a discrete chaotic cryptosystem using external key Physics Letters, A 319 334–339
[10] Alvarez G and Li S Some Basic 2006 Cryptographic Requirements for Chaos-Based Cryptosystems International Journal of Bifurcation and Chaos 16 no 8 pp 2129-2151
[11] Nitharwal B, Rani M and Saini H C Improving security of the Baptista’s cryptosystem using two-step logistic map 2015 I J Computer Network and Information Security 5 34-40
[12] Diaconu A V 2012 Multiple bitstreams generation using chaotic sequences. The annals of “Dunarea de Jos” University of galati fascicle 35, no 1, 1221
[13] Chirkikov B V and Vivaldi F 1999 An algorithmic view of pseudochaos Physica D 129, 223
[14] Levy Y E 1982 Some remarks about computer studies of dynamical systems Physics Letters A 88 1–3
[15] Li S, Chen G and Mou X 2005 On the dynamical degradation of digital piecewise linear chaotic maps International Journal of Bifurcation and Chaos 15 no 10 pp 3119-3151