Chaos, Solitons and Fractals 78 (2015) 245–248

Contents lists available at ScienceDirect

Chaos, Solitons and Fractals

Nonlinear Science, and Nonequilibrium and Complex Phenomena

journal homepage: www.elsevier.com/locate/chaos

A new discrete chaotic map based on the composition of permutations

Dragan Lambić*

Faculty of Education, University of Novi Sad, Podgorička 4, Sombor, Srbija

ARTICLE INFO

Article history:
Received 19 February 2015
Accepted 3 August 2015
Available online 1 September 2015

Keywords:
Chaotic map
Discrete chaos
Permutations
Composition

ABSTRACT

In this paper a new one-dimensional discrete chaotic map based on the composition of permutations is presented. Proposed map is defined over finite set and represents fully digital approach which is significantly different from previous ones. Dynamical properties of special case of proposed map are analyzed. Analyzed map does not have fixed points and exhibits chaotic behavior.

1. Introduction

The notion of chaos is used to encapsulate unpredictable behavior of dynamical systems that are highly sensitive to initial conditions [1]. Chaos has been widely used in several disciplines including cryptography, meteorology, sociology, physics, engineering, economics, biology and philosophy [2–6].

May [5] demonstrated that very simple one-dimensional quadratic equation could exhibit chaotic behavior. Besides Logistic map, some of the better known examples of one-dimensional chaotic maps are Tent Map [7] and Sine Map [8].

Research activity in the field of dynamical systems and application of chaos in many cases involves the use of computers [9]. However, digital computers cannot support the continuous nature of chaotic systems. They can only describe mappings from finite sets to finite sets [9]. Continuous value chaotic signals may be used only as a modulation technique [9]. Analog random number generators based on chaos may encounter problems which can occur due to high sensitivities within system dynamics [6].

Therefore, a fully digital approach is necessary for application of chaos in cryptography or spread-spectrum communication [6]. However, digital implementations of chaotic maps are reduced to the discretization of continuous values or to the discrete approximations of existing continuous systems.

In this paper, new discrete one dimensional chaotic map based on the composition of permutations is presented. This map represents fully digital approach, because it is defined over finite set. Also, this approach is significantly different from previous ones, because it introduces the use of composition in chaotic map design.

The rest of the paper is organized as follows. In Section 2, proposed discrete chaotic map is described. Dynamical properties of proposed map are discussed in Section 3. In Section 4, conclusions are drawn.

2. New discrete chaotic map

2.1. Notation

Let $P = p_0 p_1 \dots p_{n-2} p_{n-1}$ denote a permutation of the set $\{0, 1, \dots, n-1\}$. Permutation $P^r = p_{n-1} p_{n-2} \dots p_1 p_0$ is the reverse permutation of the permutation P.

The composition $h = f \circ g$ of two permutations f and g of the same set A, is the permutation mapping each $x \in A$ into $h(x) = f(g(x))$.

* Tel.: +381643616671.
E-mail address: draganposao@yahoo.com

http://dx.doi.org/10.1016/j.chaos.2015.08.001
0960-0779/

Let S_n denote the set of all permutations of the set $\{0, 1, \ldots, n-1\}$. Lehmer code [10] is bijective function $l: S_n \to \{0, 1, 2, \ldots, n!-1\}$. Function $l(P) = \sum_{0 \le i < n} c_i \cdot (n-1-i)!$ where $P \in S_n$ and c_i is the number of elements of the set $\{j > i | p_j < p_i\}$. Inverse Lehmer code is bijective function $l^{-1}: \{0, 1, 2, \ldots, n!-1\} \to S_n$.

2.2. Proposed map

In this paper a one-dimensional discrete chaotic map is proposed by

$$X_{i+1} = X_i \circ f(X_i, C) \tag{1}$$

where $X_i, C \in S_n$ and f: $S_n \to S_n$. If $x_i = l(X_i)$ and $c = l(C)$, this map can also be represented as

$$x_{i+1} = l[l^{-1}(x_i) \circ f(l^{-1}(x_i), l^{-1}(c))] \tag{2}$$

where $x_i, c \in \{0, 1, 2, \ldots, n!-1\}$ and f: $S_n \to S_n$. In this paper, we consider the case when

$$f(X_i, C) = l^{-1}(|l(C \circ X_i) - l((C \circ X_i)^r)|). \tag{3}$$

On the basis of (1) and (3) we obtain map $F_n: \{0, 1, 2, \ldots, n!-1\} \to \{0, 1, 2, \ldots, n!-1\}$ by:

$$F_n(x) = l(l^{-1}(x) \circ l^{-1}(|l(C \circ l^{-1}(x)) - l([C \circ l^{-1}(x)]^r)|)). \tag{4}$$

3. Dynamical properties of new discrete chaotic map

We begin with some definitions in this section. Let $A_n = \{a_0, a_1, \ldots, a_k\} \subset \{0, 1, 2, \ldots, n!-1\}$. In [11] the neighboring set of A_n is defined as $\partial A_n = \{a_0 \pm 1, a_1 \pm 1, \ldots, a_k \pm 1\}$ (if $a_0 = 0$ or $a_k = n!-1$, then the neighboring points are 1 and $n!-2$, respectively). Set A is an invariant set of the map F, if $F(A) = A$.

Discrete Lyapunov exponent of function F is defined as $\lambda_F = \frac{1}{m}\sum_{0 \le i < m} \ln|F(x_i) - F(i)|$ where x_i is neighboring point of i [9]. Family of maps F_n is discretely chaotic on the corresponding sets $\{0, 1, 2, \ldots, n!-1\}$, if $\lim_{n\to\infty}\lambda_{F_n} > 0$ [9].

In the following text we will deal with the dynamical properties of the proposed map. Denote by Id identical permutation. The proposed map (Eq. (4)) does not have fixed points because $f(X_i, C) \ne Id$ for all $X_i, C \in S_n$.

Proposed map F_n is not bijective on the set $\{0, 1, 2, \ldots, n!-1\}$ which is divided into elements belonging to one of the periodic orbits $o_0, o_1, \ldots, o_t$ of F_n and the elements that do not belong to any periodic orbit. Let $O_n = o_0 \cup o_1 \cup \ldots \cup o_t$. $F_n(O_n) = O_n$ so the set O_n is invariant set of the map F_n. Set O_n is an attractor of the map F_n, because O_n is an invariant set of F_n and there exists $x \in \partial O_n$ such that $F_n(x) \in O_n$ [11]. Map F_n restricted to the set O_n is a bijection.

Periodic orbit o_i of F_n is unstable if $F_n(x)$ does not belong to o_i for all $x \in \partial o_i \backslash o_i$ [12]. If all periodic orbits of F_n are unstable then the proposed map is discrete chaotic because there is a set O_n on which F_n is bijection [9]. For each value of parameter c, map F_n is a bijection on the set O_n which implies that $F_n(x_i) \ne F_n(i)$ for all neighboring points $x_i, i \in O_n$. If all periodic orbits of F_n are unstable then $F_n(x)$ does not belong to o_i for all $x \in \partial O_n \backslash O_n$. For this reason, in the case when the neighboring point x_i is not from the set O_n inequality $F_n(x_i) \ne F_n(i)$ also apply, thus avoiding the possibility that $\ln(0)$ occurs when neighboring points $x_i, i \in O_n \cup \partial O_n$.

Let us write G_n for the map F_n restricted to the set O_n. Map G_n is a bijection and can be viewed as a permutation of elements of the set O_n. Because $x_i, i \in \{0, 1, 2, \ldots, n!-1\}$ it follows that $|G_n(x_i) - G_n(i)| \ge 1$. Because the $\ln(x) \ge 0$ if $x \ge 1$ it follows that $\lambda_{G_n} \ge 0$. Therefore we can consider that family of maps G_n is discrete chaotic for each value of parameter c. As set O_n is an attractor of the map F_n, in the case when all periodic orbits of F_n are not unstable, map F_n will eventually come into the set O_n where it can be regarded as a discrete chaotic.

If we consider the proposed map when $c = 1$, for $n = 6$ map has five periodic orbits of length 2. For $n = 8$ for example, there is orbit of length 184. When $c = 2$, for $n = 6$ the maximum length of the orbit is again 2 whereas for $n = 8$ there is periodic orbit of length 214.

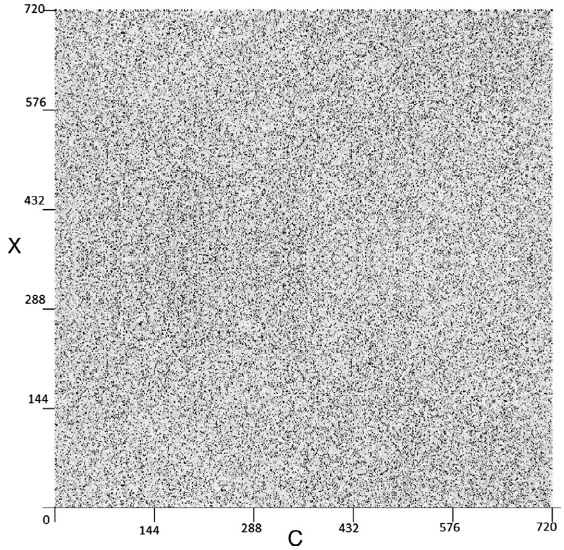

Fig. 1. The frequency of appearance of output values of the proposed map for $n = 6$.

Fig. 1 shows the frequency of appearance of each output value x of the proposed map for different values of the parameter c, when $n = 6$. Darker shade indicates increased probability of the output x acquiring corresponding value on the vertical axis for the given value of the parameter c.

The family of maps F_n is not necessarily discretely chaotic for each value of parameter c. Proposed map is not bijective on set $\{0, 1, 2, \ldots, n!-1\}$ so the discrete Lyapunov exponent may take the value $-\infty$. In [9] $\ln(0) = 0$ is used in order to avoid this situation. In the following considerations the same approach will be used. In that case $\ln|F(x_i) - F(i)| = 0$ if $F(x_i) = F(i)$ or $F(x_i) = F(i) \pm 1$. The probability that $\lambda_{F_n} = 0$ is $(\frac{3}{n!})^{n!}$. As $\lim_{n\to\infty}(\frac{3}{n!})^{n!} = 0$ probability of such occurrence is very small for larger n, so there is a high probability that $\lim_{n\to\infty}\lambda_{F_n} > 0$.

In Fig. 2 discrete Lyapunov exponents of the proposed map (obtained by using $\ln(0) = 0$) are presented. In Table 1, average, maximum and minimum values of discrete Lyapunov exponents and values of c for which discrete Lyapunov exponent takes maximum and minimum values are