Discrete Chaos—I: Theory

Ljupco Kocarev, *Fellow, IEEE*, Janusz Szczepanski, José M. Amigó, and Igor Tomovski

***Abstract*—We propose a definition of the discrete Lyapunov exponent for an arbitrary permutation of a finite lattice. For discrete-time dynamical systems, it measures the local (between neighboring points) average spreading of the system. We justify our definition by proving that, for large classes of chaotic maps, the corresponding discrete Lyapunov exponent approaches the largest Lyapunov exponent of a chaotic map when $M \to \infty$, where M is the cardinality of the discrete phase space. In analogy with continuous systems, we say the system has discrete chaos if its discrete Lyapunov exponent tends to a positive number, when $M \to \infty$. We present several examples to illustrate the concepts being introduced.**

***Index Terms*—Chaos, discrete chaos, Lyapunov components.**

I. Introduction

THE WORD "chaos" was introduced in mathematics in the 1970s [1] to encapsulate the bizarre dynamics of some continuous maps on one-dimensional (1-D) intervals. What came afterwards is well known, as it is also well known that a significant part of it could not have been achieved without the aid of computers. Indeed, most of the research activity in the field of dynamical systems at that time was supported—and often inspired—by computer calculations due to the mind-boggling complexity of the phenomena under scrutiny. Thus, bifurcation diagrams, basins of attraction, Julia sets, or fractal attractors were displayed numerically, as many other hallmarks of chaos and complex dynamics. Certainly, the researchers were aware from the beginning of the impossibility of their pursuit: no computer can show, for instance, that an orbit is aperiodic since all orbits on a computer (or a finite-state machine for this matter) are eventually periodic. Aperiodicity is just one among several key properties (like sensitivity to initial conditions or density of periodic points) of chaotic motion, which belong in the realm of continuous phase space. In other words, *there is no chaos in a discrete phase space—at least in a strict sense*. Since, chaos is a particular characteristic of motion in continuous spaces, strictly speaking, continuous value chaotic signals may be used to transmit information only as a modulation technique. Other functional blocks of a digital communication system, such as compression, coding, and/or encryption, describe transformations (or mappings) from finite sets to (in general different) finite sets.

What makes chaotic systems so attractive both for theoreticians and practitioners is their random-like behavior—in spite of being deterministic. As a way of illustration, let us mention that, already in 1949, Shannon [2] proposed this kind of transformations to construct secure cryptosystems. It is thus no surprise that, when chaos theory flourished in the 1980s and 1990s, several cryptosystems were proposed based on the discretization of chaotic maps, e.g., the generalized baker's map, cat map, standard map, and many others. Viewing how the resulting permutations mix the pixels of digital pictures [3], one cannot but admit that their "confusion" and "diffusion" properties are seemingly unsurpassed—in spite of being periodic. The examples could be multiplied with the same message: there must be some sense in which discrete maps may be also called chaotic. One can imagine that the pioneers of random number generation by arithmetic methods faced a similar, uneasy situation. Just as, thanks to their insight, we can talk now of pseudorandomness in a definite sense or of some sequences as being more random than others, it should be also meaningful to talk of would-be chaos or of some discrete maps as being more chaotic (and hence better for, say, cryptographic applications) than others.

Let us remind the readers at this point that the convenience of extending the idea of chaos to discrete-space systems rose also in quantum systems, since their phase spaces are effectively discretized by Heisenberg's uncertainty principle and the indistinguishability of identical particles. Not surprisingly, the quantum physicists coined the term *pseudochaos* for the sort of irregular phenomena they were interested in. The concept of pseudochaos has been introduced in attempts to interpret quantum chaos, and to understand its mechanism and physical meaning [4]–[6]. Pseudochaos occurs in classical mechanics as well. Digital computer is a very specific classical "dynamical system": It is an "overquantized" system [6], meaning that any quantity is discrete, while in quantum mechanics only the product of two conjugated variables are so. Owing to the discreteness, any dynamical trajectory in computer becomes eventually periodic, the effect being well known in the theory and practice of pseudorandom number generators. Since pseudochaos holds thus connotations of quantum phenomenology, we propose the more neutral term *discrete chaos* in the context of discrete mathematics.

A set is *chaotic* if its asymptotic measure (natural measure) has a positive Lyapunov exponent. If the largest Lyapunov exponent is positive, a volume element is expanded in some direction at exponential rate and neighboring trajectories are

Manuscript received March 7, 2005; revised August 30, 2005 and November 18, 2005. This work was supported by the Spanish Ministry of Education and Science under Grant MTM2005-04948. The work of L. Kocarev was supported in part by the National Science Foundation and by the Spanish Ministry of Education and Science under Grant SAB2004-0048. The work of J. Szczepanski was supported in part by KBN under Grant 8T07A04520. This paper was recommended by Associate Editor B. Shi.

L. Kocarev is with the Institute for Nonlinear Science, University of California, San Diego, La Jolla, CA 92093-0402 USA and also with the Graduate School of Electrical Engineering, University "Kiril i Metodij," Skopje 100, Macedonia (e-mail: lkocarev@ucsd.edu).

J. Szczepanski is with the Institute for Fundamental Technological Research, Polish Academy of Sciences, PL-00-049 Warsaw, Poland (e-mail: jszczepa@ippt.gov.pl).

J. M. Amigó is with the Centro de Investigación Operativa, Universidad Miguel Hernández, 03202 Elche, Spain (e-mail: jm.amigo@umh).

I. Tomovski is with the Institute of Earthquake Engineering and Engineering Seismology, Skopje 100, Macedonia (e-mail: igor@pluto.iziis.ukim.edu.mk).

Digital Object Identifier 10.1109/TCSI.2006.874181

diverging. This property is called *sensitive dependence on initial conditions*. Therefore, among many indicators of chaotic motion, positivity of the largest Lyapunov exponent is perhaps the most significant, both in theory [7] and applications [8]. The exponential divergence of two trajectories evolving under identical equations of motion from slightly different initial conditions is a fingerprint of chaos. For ergodic systems, the exponential rate of growth converges to the Lyapunov exponent, independently of the particular trajectory chosen (for almost all initial conditions). A useful generalization of Lyapunov exponents are finite-time Lyapunov exponents [7] calculated over a finite time interval along a given trajectory. In this paper we try to come to grips with the concept of discrete chaos by proposing a first tool to measure it, namely, the discrete Lyapunov exponent.

Previous Work—Despite of the fact that chaotic-like systems with finite phase space have been used in digital communication systems, for examples as chaotic digital encoders [9], chaotic turbo codes [10], pseudochaotic time hopping for ultra wind band impulse radio [11], and chaos-based cryptography [12]–[14], the question "what is chaos in finite phase space systems?" has still been unanswered. There are several references to the problem of chaos-like properties in finite phase space systems, although none of them define discrete chaos. Masuda and Aihara [15] considered a discrete version of the skew-tent map, which exploits important chaotic properties such as the sensitive dependence on initial conditions and the exponential information decay. They discussed the difference between the discretized map and the original map, explaining the ergodic-like and chaotic-like properties of the discretized map. In [14], the authors explored the feasibility of designing cryptographically secure substitutions via approximation of mixing maps by periodic transformations. The periodic approximation of mixing maps are dynamical systems with finite phase-space. The expectation behind this approach is, of course, that the nice diffusion properties of such maps will be inherited by their approximations, at least if the convergence rate is appropriate and the associated partitions are sufficiently fine.

Our Work—In this paper, we propose a definition of *discrete Lyapunov exponent*. As its continuous counterpart, the discrete Lyapunov exponent measures local (between neighboring points) average spreading of the discrete-time discrete-space dynamical system considered. Let M be a cardinality of the discrete phase-space. We justify our definition by showing that, for large classes of chaotic maps, the corresponding discrete Lyapunov exponent approaches the largest Lyapunov exponent of a chaotic map when $M \to \infty$. We further propose a plausible definition of discrete chaos using similar tools as for (classical) chaos. Since the notion pseudochaos has already been reserved for the statistical behavior of the dynamical system with discrete energy and/or frequency spectrum, we suggest the term *discrete chaos* to describe chaos-like properties in finite phase-space systems. More precisely, we define *discrete chaos* in terms of discrete Lyapunov exponent in a similar way as for continuous systems: the system is said to be discretely chaotic if its discrete Lyapunov exponent approaches a positive number, when $M \to \infty$. Preliminary short version of this work has appeared in [16].

The paper is organized as follows. Section II introduces the discrete Lyapunov exponent for maps on 1-D and higher dimensional regular lattices, although for simplicity we consider in the second case only two-dimensional (2-D) lattices. In Section III, we establish the connection explained before between the discrete Lyapunov exponent of a permutation on M elements and the Lyapunov exponent of a related continuous map: The former converges to the latter when $M \to \infty$. The speed of this convergence is studied numerically in Section IV with the tent, logistic, Henon, and coupled logistic maps. Section V contains the basic concepts of our new approach to discrete chaos, not least the very definition of discrete chaos. All these sections have been supplied with plenty of examples to illustrate the concepts being introduced. In Section VI we close our paper with conclusions.

II. Discrete Lyapunov Exponent

A. Preliminaries

Among many indicators of chaotic motion, positivity of the largest Lyapunov exponent is perhaps the most significant. The exponential divergence of two trajectories evolving under identical equations of motion from slightly different initial conditions is a fingerprint of chaos. Therefore, for computing the largest Lyapunov exponent of a chaotic map, one considers two trajectories evolving from "slightly" different initial conditions x and $x+\Delta x$, and puts $\Delta x \to 0$. More precisely, let $f : I \to I$, $I = [0,1]$ be a piecewise smooth map, μ be a Borel probability f-invariant measure, and $x \in I$ be a μ-typical point. Then, the quantity

$$\lambda_f = \lim_{n\to\infty} \frac{1}{n} \ln |Df^n(x)| = \int_0^1 \ln |f'(x)|\, d\mu(x)$$

is said to be the Lyapunov exponent of f.

Let us now consider a permutation $F : \{0,1,\dots M-1\} \to \{0,1,\dots M-1\}$. Clearly, all trajectories of F are periodic. We say that $i \pm 1$ are neighboring points of i. We further assume that $\{0,1,\dots,M-1\} \subset \mathbb{R}$, so that the "end" points 0 and $M-1$ have only one neighbor. Let $U_i = \{i-1, i+1\}$, $i = 1,2,\dots,M-2, U_0 = \{1\}$, and $U_{M-1} = \{M-2\}$. Clearly, the set U_i contains all neighbors of the point i. Let c_i be an arbitrary element of the set U_i, $c_i \in U_i$; we write $d(c_i, i) = F(c_i) - F(i)$. We argue in the next sections that the quantity

$$\lambda_F = \frac{1}{M} \sum_{i=0}^{M-1} \ln |d(c_i, i)|$$

plays the role of the Lyapunov exponent of F. The quantity λ_F preserves many of the properties of the Lyapunov exponents; in addition, if F is an appropriate discretization of a chaotic map f (see below), then, for all $c_i \in U_i$, $\lim_{M\to\infty} \lambda_F = \lambda_f$. However, we stress that the the property that two conjugate maps of intervals have same Lyapunov exponents, does not hold for discrete systems.

What are the main differences between the quantities λ_f and λ_F? When extending (generalizing) the definition of Lyapunov exponent to discrete systems, one faces several obstacles. Lyapunov exponent measures the exponential divergence of

two trajectories evolving under equations of motion from slightly different initial conditions. For continuous systems, the limit $\Delta x \to 0$ is well defined, while for discrete systems the term "slightly different initial conditions of the point i" means $i \pm 1$, and therefore, it is not uniquely defined. There exists a simple way to resolve this problem: when the set U_i has more than one element, we pick up the neighboring point c_i of the point i according to some rule. The main results of this paper are not affected by c_i, however the value of λ_F depends on c_i, so the rule should be stated clearly.

B. One-Dimensional Maps

Let us consider a map

$$F : \{0, 1 \ldots, M-1\} \to \{0, 1 \ldots, M-1\}. \tag{1}$$

We assume that the map F is 1:1 and onto (bijection). Clearly, all trajectories of F are periodic; let α_j be a periodic orbit of F with period T_j. Since F is a bijection, it follows that $\cup_j \alpha_j = \{0, 1 \ldots, M-1\}$ and $\sum_j T_j = M$. We say that $i \pm 1$ are neighboring points of i. We further assume that $\{0, 1, \ldots, M-1\} \subset \mathbb{R}$, so that the "end" points 0 and $M-1$ have only one neighbor.

Let $U_i = \{i-1, i+1\}$, $i = 1, 2, \ldots, M-2$, $U_0 = \{1\}$, and $U_{M-1} = \{M-2\}$. Clearly, the set U_i contains all neighbors of the point i. Let $c_i \in U_i$. If the set U_i has more than one element, we adopt the following rule: The neighbor of i is $c_i = i+1$. We define the *discrete Lyapunov exponent of the permutation* F as

$$\lambda_F = \frac{1}{M} \sum_{i=0}^{M-1} \ln |F(c_i) - F(i)| = \frac{1}{M} \sum_{i=0}^{M-1} \ln d[F(c_i), F(i)] \tag{2}$$

where $d(x, y)$ is the Euclidean distance (in $\mathbb{R}$) between two integers x and y, $d(x, y) = |x - y|$. In (2), all terms measure the divergence of two trajectories evolving in one iteration from two "slightly" different initial conditions: an initial point i and its neighbor $i+1$. Note that in the last term the neighbor of $M-1$ is the point $M-2$. Thus, the discrete Lyapunov exponent measures the average spreading of the map F.

Remark 1: Note that we assume that the phase space of our dynamical system is a subset of the real numbers. The other possibility that the phase space is a subset of the unit circle is not treated in this paper.

Remark 2: One can also define the discrete Lyapunov exponent with randomly choosing in (2), from two neighboring points $i+1$ and $i-1$, the neighbor c_i of i. There exist 2^{M-2} such discrete Lyapunov exponents. In a typical case, all discrete Lyapunov exponents are close to each other. We stress that all the results of this paper (theorems 1 through 4) hold for all 2^{M-2} discrete Lyapunov exponents.

Let $\alpha = \{a_0, a_1 = F(a_0), \ldots a_{T-1} = F(a_{T-2})\}$ be a periodic orbit with period T. In other words, let $a_0 \neq a_1 \neq \ldots \neq a_{T-1}$ and $F^T(a_0) = a_0$. We define the *discrete Lyapunov exponent of the map F for the periodic orbit α* as

$$\lambda_{(F,\alpha)} = \frac{1}{T} \sum_{k=0}^{T-1} \ln |F(a_k + 1) - F(a_k)|. \tag{3}$$

Observe that the discrete Lyapunov exponent of the map F can also be rewritten as a weighted sum of the discrete Lyapunov exponents of all periodic orbits

$$\lambda_F = \sum_j \frac{T_j}{M} \lambda_{(F,\alpha_j)}. \tag{4}$$

Clearly, $0 \leq \lambda_F \leq \ln(M-1)$. The map with null discrete Lyapunov exponent is $F(x) = x$ for each $x \in \{0, 1, \ldots, M-1\}$. The set of all different maps F can be divided into equivalent classes, each class having same discrete Lyapunov exponent.

We now present four examples. In all these examples, we consider permutations F of the set $\{0, 1, \ldots, M-1\}$.

Example 1: The maps $F^{(i)}$ defined as

$$F_M^{(i)}(x) = \begin{cases} x, & \text{if } 0 \leq x \leq i \\ i+3, & \text{if } x = i+1 \\ i+1, & \text{if } x = i+2 \\ i+2, & \text{if } x = i+3 \\ x, & \text{if } x \geq i+4 \end{cases}$$

have, for each $i = 0, 1, \ldots M-5$, the same discrete Lyapunov exponent: $\lambda_F = (\ln 3 + 2 \ln 2)/M$.

Example 2: Let $M = 2m$ and let m be an even number. Consider the map F defined as

$$F(x) = \begin{cases} x + m (\mathrm{mod}\ M), & \text{for } x = 2p, \\ x, & \text{for } x = 2p+1 \end{cases}$$

where $0 \leq p \leq m-1$. Since $|F(i+1) - F(i)| \geq m-1$, it follows that $\lambda_F \geq \ln(m-1)$.

Example 3: Let $M = 2m$. We define F_{non} as

$$F_{\mathrm{non}}(x) = \begin{cases} k, & \text{if } x = 2k, \quad k = 0, 1, \ldots m-1 \\ M-1-k, & \text{if } x = 2k+1, \quad k = 0, 1, \ldots m-1. \end{cases}$$

The discrete Lyapunov exponent of this map is equal to

$$\lambda_{F_{\mathrm{non}}} = \frac{1}{M} \ln(M-1)!.$$

We adopt the following definition of *perfect nonlinearity* (note that our definition is weaker than the usual one): F has a perfect nonlinearity if the differences $|F(i+1) - F(i)|$, $i = 0, 1, \ldots, M-2$ take all possible values $1, 2, \ldots, M-1$. This example shows the existence of maps with perfect nonlinearity; the discrete Lyapunov exponent of all such maps is equal to $\lambda_{F_{\mathrm{non}}}$.

Remark 3: As $M \to \infty$, the discrete Lyapunov exponent of the permutation F may approach zero, a finite positive number, or infinity. For example, it is easy to see that $\lim_{M\to\infty}(\ln 3 + 2 \ln 2)/M = 0$ and $\lim_{M\to\infty}(1/M) \ln(M-1)! = \infty$.

Example 4: Let $M = 2m$ be an even number. We define $F_{\max}$ as

$$F_{\max}(x) = \begin{cases} m+k, & \text{if } x = 2k, \quad k = 0, 1, \ldots m-1 \\ k, & \text{if } x = 2k+1, \quad k = 0, 1, \ldots m-1. \end{cases}$$

The discrete Lyapunov exponent of this map is equal to

$$\lambda_{F_{\max}} = \frac{m+1}{2m}\ln m + \frac{m-1}{2m}\ln(m+1). \tag{5}$$

Remark 4: Let F_M be a family of permutations (parameterized by M) of the set $\{0,1,2,\ldots,M-1\}$. Then, the set of all families (of permutations) can be divided into three subsets A_0, A_{finite}, and A_∞ for which the corresponding discrete Lyapunov exponents tend to zero when $M \to \infty$, approach a finite number when $M \to \infty$, and tend to infinity when $M \to \infty$, respectively. Although it is quite intriguing to analyze these sets, especially the properties of A_{finite} and A_∞, this is beyond the scope of the paper and will be treated separately.

Remark 5: Let $f : I \to I$ be a chaotic map, $I = [0,1]$. Let F_M be a family of permutations of the set $\{0,1,2,\ldots,M-1\}$ induced by the map f as described in the next section. We prove in Section III that in this case $\lim_{M\to\infty} \lambda_{F_M} = \lambda_f$, where λ_f is the Lyapunov exponent of f. Clearly, $F_M \in A_{\text{finite}}$. Let A_{chaos} be a set of all families of permutations induced by chaotic maps. Then, obviously $A_{\text{chaos}} \subsetneqq A_{\text{finite}}$.

C. Higher Dimensional Maps

We now consider the case of higher dimensional maps. For notational simplicity, we will consider only 2-D maps. Let U_i be the set of all neighboring points of $i = (x,y)$. If U_i has more than one point, we adopt the following rule: If $(x,y+1) \in U_i$, then we say $(x,y+1) \in U_i$ is the neighbor of i. If $(x,y+1) \notin U_i$ and $(x,y-1) \in U_i$, we say $(x,y-1) \in U_i$ is the neighbor of i; and if $(x,y+1) \notin U_i$ and $(x,y-1) \notin U_i$, we say $(x+1,y) \in U_i$ is the neighbor of i; Consider the set $C = \{m_0, m_1, \ldots, m_{M-1}\} \subseteq \{(i,j) | 0 \le i \le I_1 - 1, 0 \le j \le J_1 - 1\}$, endowed with the metric d, such that $d(m_0,(0,0)) \le d(m_i,(0,0))$ for all $i > 0$ and m_0 is a neighbor of (0,0), and $d(m_i, m_{i-1}) \le d(m_j, m_{i-1})$ for all $j > i$ and m_i is a neighbor of m_{i-1}. Let $F : C \to C$ be a permutation.

We define the *discrete Lyapunov exponent of order s for the permutation F* as follows:

$$\lambda_F^{(s)} = \frac{1}{Ms}\sum_{i=0}^{M-1}\sum_{k=1}^{s}\ln\frac{d\left[F^k(m_{i+1}), F^k(m_i)\right]}{d[F^{k-1}(m_{i+1}), F^{k-1}(m_i)]} \tag{6}$$

where F^k is the composition of F with itself k times, $k = 1,2,\ldots s$, and F^0 is the identity permutation. Equivalently, the last formula can be rewritten as

$$\lambda_F^{(s)} = \frac{1}{Ms}\sum_{i=0}^{M-1}\ln\frac{d[F^s(m_{i+1}), F^s(m_i)]}{d\,[m_{i+1}, m_i]}.$$

Remark 6: Since there exists N_1 such that $F^{N_1}(x) = x$ is the identity permutation, it follows that $\lambda_F^{(N_1)} = 0$. Therefore, we assume s is always finite, $s = 1,2,\ldots,N_1 - 1$.

Remark 7: If d is the Euclidean distance (in $\mathbb{R}^2$), and $x = (x_1,x_2)$, $y = (y_1,y_2)$, then $d(x,y) = \sqrt{(x_1-y_1)^2 + (x_2-y_2)^2}$. In the special case of 1-D lattice endowed with the Euclidean metric and $s = 1$, the above definition reduces to (2).

Remark 8: For a given permutation, it may happen that: 1) all discrete Lyapunov exponents of order s, $\lambda_F^{(s)}$, are "different" for all s; but also 2) there exists s_0 such that for some $l \ge 2$, the discrete Lyapunov exponents $\lambda_F^{(s_0)}, \lambda_F^{(s_0+1)}, \ldots, \lambda_F^{(s_0+l)}$ are "close" to each other.

Remark 9: Equation (6) defines the discrete Lyapunov exponent of order s for a permutation. In a similar way as in (3), one can define the discrete Lyapunov exponent of order s of a permutation for a periodic orbit.

We now consider an analytical example. Consider the 2-D lattice $\mathcal{S} = \{m = (j,k) \in \mathbb{N}^2 : 0 \le j,k \le N-1\}$ with N *prime*, endowed with the metric

$$d(m,m') = |(j-j')| + |k-k'|\,.$$

for $m = (j,k)$, $m' = (j',k')$ (the continuous counterpart of d is equivalent to Euclidean metric on $\mathbb{R}^2$). Furthermore, assume that $\mathcal{S}$ is lexicographically ordered left-to-right bottom-to-top: $m_0 = (0,0) < \ldots < m_i = (j,k) < m_{i+1} = (j',k') < \ldots < m_{N^2-1} = (1,1)$, where $(j',k') = (j+1,k)$ if $j < N-1$ and $(j',k') = (0,k+1)$ if $j = N-1$.

Define the N^2-permutation $F : \mathcal{S} \to \mathcal{S}$

$$F((j,k)) = (j, k + j \bmod N)$$

whose continuous counterpart is a skew vertical translation on the 2-D torus. Note that F^N is the identity so that we only need to consider the iterates F^s with $s = 1,2,\ldots,N-1$.

In *Case 1* ($j \ne N-1$) we have $F^s(m_i) = (j, k+sj \bmod N)$, $F^s(m_{i+1}) = (j+1, k+s(j+1) \bmod N)$ and thus

$$d\left(F^s(m_i), F^s(m_{i+1})\right) = \begin{cases} s+1 & \text{if } k+sj \bmod N < k+s(j+1) \bmod N \\ N-s+1 & \text{if } k+s(j+1) \bmod N < k+sj \bmod N \end{cases}.$$

It follows that, for $s = 1,2,\ldots,N-1$

$$\begin{aligned}
&\sum_{j=0}^{N-2}\sum_{k=0}^{N-1}\ln\frac{d(F^s(m_i), F^s(m_{i+1}))}{d(m_i, m_{i+1})} \\
&\quad= \ln(s+1)\sum_{k=0}^{N-1}\left(N-1-\left\lfloor\frac{s(N-1)+k}{N}\right\rfloor\right) \\
&\qquad+ \ln(N-s+1)\sum_{k=0}^{N-1}\left\lfloor\frac{s(N-1)+k}{N}\right\rfloor \\
&\quad= N(N-1)\ln(s+1) + \left(\sum_{k=0}^{N-1}\left\lfloor\frac{s(N-1)+k}{N}\right\rfloor\right) \\
&\qquad\times \ln\frac{N-s+1}{s+1} \\
&\quad= N(N-1)\ln(s+1) + s(N-1)\ln\frac{N-s+1}{s+1}.
\end{aligned}$$

If, else, $m_i = (N-1, k)$ (*Case 2*) and thus $m_{i+1} = (0, k+1)$, $0 \le k \le N-2$, then $F^s(m_i) = (N-1, k+s(N-1) \bmod N) = (N-1, k-s \bmod N)$, $F^s(m_{i+1}) = (0, k+1)$ and

$$d(F^s(m_i), F^s(m_{i+1}) = N - 1 + |k + 1 - (k - s \bmod N)| = \begin{cases} N-s, & \text{if } s \le k \\ 2N-s-2, & \text{if } s > k. \end{cases}$$

It follows that

$$\sum_{j=N-1, 0\le k\le N-2} \ln \frac{d(F^s(m_i), F^s(m_{i+1}))}{d(m_i, m_{i+1})} = \sum_{k=0}^{s-1} \ln \frac{2N-s-2}{N} + \sum_{k=s}^{N-2} \ln \frac{N-s}{N} = \begin{cases} s \ln \frac{2N-s-2}{N} \\ \quad -(N-s-1)\ln \frac{N}{N-s}, & \text{if } 1 \le s \le N-2 \\ (N-1)\ln \frac{N-1}{N}, & \text{if } s = N-1. \end{cases}$$

III. Properties of Discrete Lyapunov Exponent

A. One-Dimensional Maps

In this section, we prove several properties of the discrete Lyapunov exponent for the permutations of 1-D sets. The first theorem states that for ergodic permutations (for permutations on lattices, ergodicity is equivalent to transitivity or cyclicity: the orbit of any point visits all the state space), the discrete Lyapunov exponent computed as the space average is equal to the discrete Lyapunov exponent computed as time average (along the trajectory). The second theorem proves what permutation has the largest discrete Lyapunov exponent. Finally, the third theorem, which is our main result in this section, justifies the use of the term "discrete Lyapunov exponent." The proof of the next theorem is obvious.

Theorem 1: If the permutation is cyclic, then the discrete Lyapunov exponent computed as the space average, (2), is equal to the discrete Lyapunov exponent computed as time average, (3).

The map $F_{\max}$, see Example 4, has the largest discrete Lyapunov exponent among all permutations of the set $\{0, 1, \ldots, M-1\}$. The proof of following theorem will be given elsewhere.

Theorem 2: For any permutation F of the set $\{0, 1, \ldots, M-1\}$ we have $\lambda_F \le \lambda_{F_{\max}}$.

Let us now consider a map

$$F : \{m_0, m_1 \ldots, m_{M-1}\} \to \{m_0, m_1 \ldots, m_{M-1}\} \quad (7)$$

where F is 1:1 and m_i are integers, $m_0 \ge 0$, and $m_i < m_j$ if $i < j$. Then, we define discrete Lyapunov exponent as

$$\lambda_F = \frac{1}{M} \sum_{i=0}^{M-1} \ln \frac{d[F(m_{i+1}), F(m_i)]}{d[m_{i+1}, m_i]} \quad (8)$$

where, by definition, $m_M = m_{M-2}$. We stress that in (8), d is the Euclidean distance (in $\mathbb{R}$) of the points x and y, that is $d(x, y) = |x - y|$. Note that (8) reduces to (2) if $m_i = i$ for $i = 0, 1, \ldots, M-1$.

Let $z_{j+1} = f(z_j)$, $j = 0, 1, \ldots, M-1$, be a "typical" trajectory of length M of a 1-D chaotic map $f : [0, 1] \to [0, 1]$, such that $z_{j+1} \ne z_j$ for all j and $|z_{M-1} - z_0| < \varepsilon$. We define $f(z_{M-1}) = z_0$ and order z_j to obtain x_j. Therefore, we consider a set $\{x_i\}$ of M points, $x_0 < x_1 < \ldots < x_{M-1}$, such that $f(x_i) = x_j$ for some j. Define $m_i = \mathrm{Fl}(x_i N)$, where $\mathrm{Fl}(z)$ denote the floor of z and N is chosen such that $m_i \ne m_j$ for all i and j. The map f induces a permutation

$$F : \{m_0, m_1, \ldots m_{M-1}\} \to \{m_0, m_1, \ldots m_{M-1}\}$$

as $F(m_i) = m_j$ when $f(x_i) = x_j$.

Theorem 3: Let $z_{j+1} = f(z_j)$ be a "typical" trajectory of a 1-D chaotic map $f : [0, 1] \to [0, 1]$ with Lyapunov exponent λ_f. Consider only the first M points of this trajectory, $j = 0, 1, \ldots, M-1$. Let F be the permutation of the set $\{m_0, m_1, \ldots, m_{M-1}\}$ induced by the map f as described above. Then $\lim_{M\to\infty} \lambda_F = \lambda_f$

Proof: Define the map $\bar{f}$ as follows. Let $\bar{z}_i = m_i/N$. Note $\bar{z}_i \approx z_k$. We define

$$\bar{f}(\bar{z}_i) = \bar{z}_j \Leftrightarrow \bar{z}_j = \frac{m_j}{N} = \frac{F(m_i)}{N}.$$

It follows that $\bar{f}(\bar{z}_i) = \bar{z}_j \approx z_l = f(z_k)$. Therefore, $\bar{f}(\bar{z}_i) \approx f(z_k)$. Let z_p be the closest point to z_k; we write $z_p = z_k + \varepsilon_k$. Clearly $\bar{z}_{i+1} \approx z_k + \varepsilon_k$ and $\bar{f}(\bar{z}_{i+1}) \approx f(z_k + \varepsilon_k)$. Denote $\delta = \max|\varepsilon_k|$. It is easy to see that as $M \to \infty$, $N \to \infty$ and $\delta \to 0$. Moreover, when $N \to \infty$, $\bar{z}$ approaches z as well as $\lim_{N\to\infty} \bar{f}(\bar{z}) = f(z)$.

Now we have

$$\begin{aligned} &\lim_{M\to\infty} \lim_{N\to\infty} \lambda_F \\ &= \lim_{M\to\infty} \lim_{N\to\infty} \frac{1}{M} \sum_{i=0}^{M-1} \ln \left| \frac{F(m_{i+1}) - F(m_i)}{m_{i+1} - m_i} \right| \\ &= \lim_{M\to\infty} \lim_{N\to\infty} \frac{1}{M} \sum_{i=0}^{M-1} \ln \left| \frac{\bar{f}(\bar{z}_{i+1}) - \bar{f}(\bar{z}_i)}{(m_{i+1} - m_i)/N} \right| \\ &= \lim_{M\to\infty} \lim_{N\to\infty} \frac{1}{M} \sum_{i=0}^{M-1} \ln \left| \frac{\bar{f}(\bar{z}_{i+1}) - \bar{f}(\bar{z}_i)}{\bar{z}_{i+1} - \bar{z}_i} \right| \\ &= \lim_{M\to\infty} \frac{1}{M} \sum_{k=0}^{M-1} \ln \left| \frac{f(z_k + \varepsilon_k) - f(z_k)}{\varepsilon_k} \right| \\ &= \lim_{M\to\infty} \lim_{\delta\to 0} \frac{1}{M} \sum_{k=0}^{M-1} \ln \left| \frac{f(z_k + \varepsilon_k) - f(z_k)}{\varepsilon_k} \right| \\ &= \lim_{M\to\infty} \frac{1}{M} \sum_{k=0}^{M-1} \ln |f'(z_k)| \\ &= \lambda_f. \end{aligned}$$

■

B. Higher Dimensional Maps

We now consider the case of higher dimensional maps. For notational simplicity we will again consider only 2-D maps. In this section, we generalize the Theorem 3 for 2-D permutations. We note that the Theorem 1 holds also for 2-D permutations, in contrast to 2-D chaotic maps.

Let $z_{j+1} = f(z_j)$, $j = 0, 1, \ldots, M-1$, be a "typical" trajectory of length M of a 2-D chaotic map $f : \mathbb{R}^2 \to \mathbb{R}^2$,

such that $z_{j+1} \neq z_j$ for all j and $d(z_{M-1}, z_0) < \varepsilon$. We define $f(z_{M-1}) = z_0$. For simplicity only we assume now that the chaotic attractor is located in $[0,1]^2$. Therefore, for all z_j, $z_j \in [0,1]^2$. Define $x_i = \mathrm{Fl}(z_i N)$, where N is chosen such that $x_i \neq x_j$ for all i and j. Thus, we obtain the set

$$B = \{x_0, x_1, \ldots, x_{M-1}\}$$

where $x_i = (u_i, v_i)$, and $u_i \geq 0, v_i \geq 0$ are integers. We reorder the set B to obtain the set C

$$C = \{m_0, m_1, \ldots, m_{M-1}\}$$

such that $d(m_0, (0,0)) \leq d(y, (0,0))$ for all $y \in B$, and $d(m_i, m_{i-1}) \leq d(y, m_{i-1})$ for all $y \in B \setminus \{m_0, m_1, \ldots, m_{i-1}\}$. This reordering defines a permutation $P : C \to B$. Let $P(m_i) = x_k$ and $P(m_j) = x_l$. Then, the map f induces the permutation F on the set C as $F(m_i) = m_j$ when $f(z_k) = z_l$. Note that for a typical trajectory, the permutation F has a single periodic trajectory with period M.

We first give the definition of a chaotic attractor. A closed invariant set $\mathcal{A}$ is called chaotic attractor if: 1) for almost (with respect to Lebesgue measure) every point in the neighborhood of $\mathcal{A}$ its forward orbit is dense on an unstable manifold; and 2) there exists a Sinai–Ruelle–Bowen (SRB) measure which is smooth along the unstable manifold.

Theorem 4: Assume that $\mathcal{A}$ is a chaotic attractor of a 2-D map $f : \mathbb{R}^2 \to \mathbb{R}^2$. Assume further that μ is an SRB invariant measure supported on $\mathcal{A}$, and let $\lambda_f > 0$ be the largest Lyapunov exponent for this measure. Let $z_{j+1} = f(z_j)$ be a "typical" trajectory on $\mathcal{A}$. Consider only the first M points of this trajectory $j = 0, 1, \ldots, M-1$. Let $F : \{m_0, \ldots, m_{M-1}\} \to \{m_0, \ldots, m_{M-1}\}$ be the permutation induced by the map f as described above. Then there is a sequence $s(M)$ such that

$$\lim_{M \to \infty} \lambda_F^{(s(M))} = \lambda_f.$$

Proof: It is well known that for randomly chosen initial vector u_0, the maximal Lyapunov exponent of the trajectory $f^s(x)$ λ_f is given by

$$\lambda_f = \lim_{s \to \infty} \frac{1}{s} \ln \left\| Df^s(x)(u_0) \right\|.$$

This means that for a given $\varepsilon > 0$ and for randomly chosen u_0, there exists s_0 such that

$$\left| \lambda_f - \frac{1}{s} \ln \left\| Df^s(x)(u_0) \right\| \right| < \frac{\varepsilon}{2} \tag{9}$$

for $s_0 \leq s$. On the other hand, we have, by definition of Frechet derivative, that for a given s and for sufficiently small u_0,

$$\frac{\|f^s(x+u_0) - f^s(x) - Df^s(x)(u_0)\|}{\|u_0\|} < \frac{\varepsilon}{2}.$$

Consequently

$$A \equiv \left\| \frac{f^s(x+u_0) - f^s(x)}{\|u_0\|} - Df^s(x)\left(\frac{u_0}{\|u_0\|}\right) \right\| < \frac{\varepsilon}{2}. \tag{10}$$

We write

$$B = \left\| \frac{f^s(x+u_0) - f^s(x)}{\|u_0\|} \right\| \quad \text{and} \quad C = \left\| Df^s(x)\left(\frac{u_0}{|u_0|}\right) \right\|.$$

Next, we have

$$|B - C| < A \tag{11}$$

and by the Mean Value Theorem

$$|\ln B - \ln C| = \left| \frac{1}{\theta_s} |B - C| \right| \tag{12}$$

where θ_s is between B and C.

Thus, by (10), (11), and (12) for a given s large enough and sufficiently small randomly chosen u_0, we have

$$\left| \frac{1}{s} \ln B - \frac{1}{s} \ln C \right| \leq \frac{1}{s\theta_s} \frac{\varepsilon}{2}.$$

Now, since C for large s is close to $\exp(s\lambda_f)$, $\lambda_f > 0$, and taking into account (10), we can assume that $\theta_s > 1$, so we have

$$\left| \frac{1}{s} \ln B - \frac{1}{s} \ln C \right| \leq \frac{1}{s} \frac{\varepsilon}{2} \leq \frac{\varepsilon}{2}. \tag{13}$$

From (9) and (13), we have

$$\left| \frac{1}{s} \ln \frac{\|f^s(x+u_0) - f^s(x)\|}{\|u_0\|} - \lambda_f \right| < \varepsilon. \tag{14}$$

Moreover, for a given l we can choose u_0 sufficiently small, such that the above estimation holds for all $s_0 \leq s \leq s_0 + l$.

Let $z_{k+1} = f(z_k)$, $k = 0, 1, \ldots, M-1$, be a trajectory on $\mathcal{A}$. Define $\varepsilon_k = z_k - z_{j(k)}$ where the element of trajectory $z_{j(k)}$ is the nearest point to z_k. Observe that we have $\lim_{M \to \infty} \max_{0 \leq k \leq M-1} \|\varepsilon_k\| = 0$. Assumptions that $\mathcal{A}$ is a chaotic attractor and μ is a SRB measure imply that for almost (with respect to Lebesgue measure) every initial point in the basin of attraction of $\mathcal{A}$, the points z_k, when $M \to \infty$ are dense on the unstable manifold (as computer experiment indicates). We write $x_i \equiv z_k$ and $x_{i+1} \equiv z_{j(k)}$. Due to mixing, taking M large we can assume that the vectors $x_{i+1} - x_i$ have random directions and arbitrarily small lengths. For all x_i, we consider

$$\frac{1}{s} \ln \frac{\|f^s(x_{i+1}) - f^s(x_i)\|}{\|x_{i+1} - x_i\|}.$$

Now, assuming M is large enough and taking as $s(M)$ a value of s for which (14) is satisfied, we have

$$\left| \frac{1}{s(M)} \ln \frac{\left\|f^{s(M)}(x_{i+1}) - f^{s(M)}(x_i)\right\|}{\|x_{i+1} - x_i\|} - \lambda_f \right| < \varepsilon$$

for all i. Therefore

$$\left| \frac{1}{Ms(M)} \sum_{i=1}^{M} \ln \frac{\left\| f^{s(M)}(x_{i+1}) - f^{s(M)}(x_i) \right\|}{\|x_{i+1} - x_i\|} - \lambda_f \right| < \varepsilon.$$

Since $\varepsilon > 0$ can be chosen arbitrary, we have

$$\lim_{M\to\infty} \frac{1}{Ms(M)} \sum_{i=1}^{M} \ln \frac{\left\| f^{s(M)}(x_{i+1}) - f^{s(M)}(x_i) \right\|}{\|x_{i+1} - x_i\|} = \lambda_f. \tag{15}$$

Define the map $\bar{f}$ as follows. Let $\bar{z}_i = m_i/N$. Note $\bar{z}_i \approx z_k$ since $P(m_i) = x_k$. We define:

$$\bar{f}(\bar{z}_i) = \bar{z}_j \Leftrightarrow \bar{z}_j = \frac{m_j}{N} = \frac{F(m_i)}{N}.$$

Since $P(m_j) = x_l$ it follows that $\bar{f}(\bar{z}_i) = \bar{z}_j \approx z_l = f(z_k)$. Therefore, $\bar{f}(\bar{z}_i) \approx f(z_k)$. Let z_p be the closest point to z_k; we write $z_p = z_k + \varepsilon_k$. Clearly $\bar{z}_{i+1} \approx z_k + \varepsilon_k$ and $\bar{f}(\bar{z}_{i+1}) \approx f(z_k + \varepsilon_k)$. Denote $\delta = \max \|\varepsilon_k\|$. It is easy to see that as $M \to \infty$, $N \to \infty$ and $\delta \to 0$. Moreover, when $N \to \infty$, $\bar{z}$ approaches z as well as $\lim_{N\to\infty} \bar{f}(\bar{z}) = f(z)$.

Now we have

$$\begin{aligned}
&\lim_{M\to\infty} \lim_{N\to\infty} \lambda_F^{(s(M))} \\
&\quad = \lim_{M\to\infty} \lim_{N\to\infty} \frac{1}{Ms(M)} \\
&\qquad \times \sum_{i=0}^{M-1} \ln \frac{\left\| F^{s(M)}(m_{i+1}) - F^{s(M)}(m_i) \right\|}{\|m_{i+1} - m_i\|} \\
&\quad = \lim_{M\to\infty} \lim_{N\to\infty} \frac{1}{Ms(M)} \\
&\qquad \times \sum_{i=0}^{M-1} \ln \frac{\left\| \bar{f}^{s(M)}(\bar{z}_{i+1}) - \bar{f}^{s(M)}(\bar{z}_i) \right\|}{\|(m_{i+1} - m_i)/N\|} \\
&\quad = \lim_{M\to\infty} \lim_{N\to\infty} \frac{1}{Ms(M)} \\
&\qquad \times \sum_{i=0}^{M-1} \ln \frac{\left\| \bar{f}^{s(M)}(\bar{z}_{i+1}) - \bar{f}^{s(M)}(\bar{z}_i) \right\|}{\|\bar{z}_{i+1} - \bar{z}_i\|} \\
&\quad = \lim_{M\to\infty} \frac{1}{Ms(M)} \\
&\qquad \times \sum_{k=0}^{M-1} \ln \frac{\left\| f^{s(M)}(z_k + \varepsilon_k) - f^{s(M)}(z_k) \right\|}{\|\varepsilon_k\|} \\
&\quad = \lambda_f.
\end{aligned}$$

The last equality follows from (15) and the fact $\delta \to 0$ when $M \to \infty$ and the directions ε_k are random for large M. ■

Remark 10: The above theorem holds for arbitrary dimensional maps.

IV. Examples

In this section, we present several examples. The example with the tent map can be found in [16].

A. Logistic Map

We now consider the logistic map $f(x) = 4x(1-x)$ and consider its trajectory $z_0, z_1, \ldots, z_{M-1}$ of length M. We define $f(z_{M-1}) = z_0$ and order z_j to obtain x_j. Let $m_i = \mathrm{Fl}(x_i N)$, where $\mathrm{Fl}(z)$ denote the floor of z and N is chosen such that $m_i \neq m_j$ for all i and j. Therefore, we consider a set $\{m_i\}$ of M points, $m_0 < m_1 < \ldots < m_{M-1}$. On this set the logistic map f induces the permutation F, such that $F(m_i) = m_j$ if $f(x_i) = x_j$. In general $f(z_{M-1})$ may not be close to z_0, which means that $f(z_{M-1})$ does not reflect the original dynamics of the logistic map. Let m_k correspond to z_{M-1}, where $k \neq 0$, $M-2$. By the same argument, $F(m_k)$ does not reflect the original dynamics of the logistic map, and therefore we compute the discrete Lyapunov exponent using the following expression:

$$\lambda_F = \frac{1}{M-2} \left(\sum_{i=0}^{k-2} \ln \frac{d[F(m_{i+1}), F(m_i)]}{d[m_{i+1}, m_i]} + \sum_{i=k+1}^{M-1} \ln \frac{d[F(m_{i+1}), F(m_i)]}{d[m_{i+1}, m_i]} \right). \tag{16}$$

For $k = M-2$, instead of (16), one should compute the discrete Lyapunov exponent as

$$\lambda_F = \frac{1}{M-3} \sum_{i=0}^{M-4} \ln \frac{d[F(m_{i+1}), F(m_i)]}{d[m_{i+1}, m_i]} \tag{17}$$

while for $k = 0$, as

$$\lambda_F = \frac{1}{M-1} \sum_{i=1}^{M-1} \ln \frac{d[F(m_{i+1}), F(m_i)]}{d[m_{i+1}, m_i]}. \tag{18}$$

Let $\{0.123, 0.431\,484\,0.981\,222\,0.737\,006\,0.273\,075, 0.794\,021\,0.654\,206\,0.904\,881\}$ be a trajectory of the logistic map of length $M = 8$. Reordering this set, we have

$$\{0.123, 0.273\,075\,0.431\,484\,0.654\,206\,0.737\,006, 0.794\,021\,0.904\,881\,0.981\,222\}.$$

The logistic map induces the permutation

$$F : \{12, 27, 43, 65, 73, 79, 90, 98\} \to \{12, 27, 43, 65, 73, 79, 90, 98\}$$

with $F(12) = 43$, $F(27) = 79$, $F(43) = 98$, $F(65) = 90$, $F(73) = 27$, $F(79) = 65$, $F(98) = 73$ and we define $F(90) = 12$. Note that $m_6 = 90$ corresponds to z_7. Therefore, we compute the discrete Lyapunov exponent using (17) as $\lambda_F = 0.789$, which is close to the Lyapunov exponent of the logistic map $\lambda_f = \ln 2$. For $M = 16$, we compute the discrete Lyapunov exponent for three different values of N, $N = 10^3$, $N = 10^4$, and $N = 10^5$ and obtain (averaged over 100 trajectories) 0.628, 0.658, and 0.664, respectively.

The values of the discrete Lyapunov exponent, computed using one of the expressions (16)–(18), are $\lambda_F = 0.609\,286$ for $M = 8$, $\lambda_F = 0.669\,12$ for $M = 32$, $\lambda_F = 0.681\,690$ for $M = 64$, $\lambda_F = 0.687\,43$ for $M = 128$, and $\lambda_F = 0.691\,484$

TABLE I
DISCRETE LYAPUNOV EXPONENT $\lambda_F^{(s)}$ OF THE HENON MAP FOR DIFFERENT VALUES OF s. THE PARAMETERS OF THE MAP ARE $a = 1.4$ AND $b = 0.3$. THE LARGEST LYAPUNOV EXPONENT FOR THE HENON MAP IS $\lambda_f = 0.4169$

s	$\lambda_F^{(s)}$	s	$\lambda_F^{(s)}$
1	0.302160	16	0.388738
2	0.365007	17	0.379391
3	0.374142	18	0.367462
4	0.395656	19	0.354218
5	0.393760	20	0.343144
6	0.401879	21	0.328626
7	0.404930	22	0.317969
8	0.407093	23	0.308499
9	0.407391	24	0.292478
10	0.406174	25	0.280957
11	0.403202	26	0.274287
12	0.406164	27	0.263852
13	0.404751	28	0.254212
14	0.405888	29	0.246234
15	0.394061	30	0.239540

for $M = 512$. For each M, the discrete Lyapunov exponent for 1000 different trajectories is calculated and the average value is presented.

B. Henon Map

Consider the Henon map $f : \mathbb{R}^2 \to \mathbb{R}^2$ given with $(x, y) \to (1 - ax^2 + by, x)$. For $a = 1.4$, $b = 0.3$ the Henon map has a chaotic attractor, for which the largest Lyapunov exponent is $\lambda_f = 0.4169$. The Henon map induces a permutation of the set $\{m_0, m_1, \ldots, m_{M-1}\}$ as described in the Section III-B. Discrete Lyapunov exponents $\lambda_F^{(s)}$ for different values of s are shown in Table I. It can be seen that for $6 \leq s \leq 14$, the values of $\lambda_F^{(s)}$ are close to each other and to the actual value $\lambda_f = 0.4169$. Table II shows $\lambda_F^{(s)}$ and $|\lambda_F^{(s)} - \lambda_f|$ for different values of s and M.

C. Coupled Logistic Maps

We now consider a system of coupled logistic maps

$$x_{1t+1} = rx_{1t}(1 - x_{1t}) + e(x_{2t} - x_{1t})$$
$$x_{2t+1} = rx_{2t}(1 - x_{2t}) + e(x_{1t} - x_{2t})$$

which exhibits hyperchaos for $r = 3.7$ and $e = 0.006$. Discrete Lyapunov exponents $\lambda_F^{(s)}$ for different values of s are: $\lambda_F^{(1)} = 0.498\,189$, $\lambda_F^{(2)} = 0.395\,201$, $\lambda_F^{(3)} = 0.407\,670$, $\lambda_F^{(4)} = 0.374\,480$, $\lambda_F^{(5)} = 0.383\,502$, $\lambda_F^{(6)} = 0.364\,136$, $\lambda_F^{(7)} = 0.370\,106$, $\lambda_F^{(8)} = 0.357\,860$, $\lambda_F^{(9)} = 0.362\,121$, $\lambda_F^{(10)} = 0.353\,725$ $\lambda_F^{(11)} = 0.356\,582$, $\lambda_F^{(12)} = 0.346\,782$, $\lambda_F^{(13)} = 0.347\,391$, $\lambda_F^{(14)} = 0.335\,135$, and $\lambda_F^{(15)} = 0.331\,621$. Again, as in the case of the Henon map, we see that for $4 \leq s \leq 7$, the values of $\lambda_F^{(s)}$ are close to each other and the average value is equal to $\approx 0.373\,305$, which is close to the actual value $\lambda_f = 0.373\,484$.

V. DISCRETE CHAOS

In this section we consider the question: when is a finite phase-space dynamical system discretely chaotic?

Definition 1: Let F_M be a family of permutations (parameterized by M) of the sets $\{0, 1, \ldots, M-1\}$. We say that F_M is a discretely-chaotic family of permutations if $\lim_{M\to\infty} \lambda_{F_M}$ is a finite positive number, that is $0 < \lim_{M\to\infty} \lambda_{F_M} < \infty$.

Remark 11: Sometimes, the concept of discretely chaotic map is applied to a single map F rather than to a family. In most applications though, F is obtained via phase space discretization and truncation of the orbits of a continuous map and, therefore, it does belong to a family of maps (generated by f) by construction. Otherwise, if e.g., F is a permutation on $\{0, 1, \ldots, M-1\}$, the comparison of λ_F to the corresponding $\lambda_{F_{\max}}$ can be used to gauge the "distance" from F to $F_{\max}$—the permutation on the same set having the largest discrete Lyapunov exponent.

The set of all permutations of the set $\{0, 1, \ldots, M-1\}$ can be divided into three classes: the class of all permutations for which $\lim_{M\to\infty} \lambda_F = 0$; the class of all permutations for which $0 < \lim_{M\to\infty} \lambda_F < \infty$; and the class of all permutations for which $\lim_{M\to\infty} \lambda_F = \infty$. Examples of such permutations are given in the Section II-B. Since the discrete Lyapunov exponent for the maps $F_M^{(i)}$, see Example 1, tends to zero, when M goes to infinity, the maps are not discretely-chaotic, although for each finite M their discrete Lyapunov exponent is a positive number. We stress again that since F is a permutation of the set $\{0, 1, \ldots, M-1\}$, its discrete Lyapunov exponent is always a nonnegative number, that is $\lambda_F \geq 0$.

Let now consider the case when $F : \{0, 1, \ldots, M-1\} \to \{0, 1, \ldots, M-1\}$ is an arbitrary map (not necessarily 1:1 and/or onto). In this case, the map may have eventually periodic orbits. We say that the fixed point i is an eventually fixed point for j if there exists $n \geq 1$ such that $F^n(j) = i$.

Definition 2: We say that i is a stable fixed point for the map F if $F(i) = i$ and i is an eventually fixed point for at least one of its neighbor points $i \pm 1$. In other words, when $F(i+1) = i$ and/or $F(i-1) = i$. In a similar way, one can define stable periodic orbits.

Example 5: Let $F : \{0, 1, \ldots, 9\} \to \{0, 1, \ldots, 9\}$ be the map defined as $F(0) = 1$, $F(1) = 2$, $F(2) = 8$, $F(3) = 6$, $F(4) = 5$, $F(5) = 5$, $F(6) = 5$, $F(7) = 3$, $F(8) = 9$, and $F(9) = 0$. This map has one period-5 orbit $0 \to 1 \to 2 \to 8 \to 9 \to 0$, a fixed point $5 \to 5$, and four points, 3,4,6, and 7, for which the fixed point 5 is an eventually fixed point: $3 \to 6 \to 5$, $4 \to 5$, $6 \to 5$, and $7 \to 3 \to 6 \to 5$. 5 is stable fixed point. The discrete Lyapunov exponent of the period-5 orbit is equal to $(\ln 6 + \ln 9)/5$.

Remark 12: If F is a permutation of the set $\{0, 1, \ldots, M-1\}$, the discrete Lyapunov exponent is a nonnegative number, that is $\lambda_F \geq 0$. However, for a map $F : \{0, 1, \ldots, M-1\} \to \{0, 1, \ldots, M-1\}$ which is not 1:1 and/or onto, the discrete Lyapunov exponent may take the value $-\infty$. For example, the discrete Lyapunov exponent of the fixed point 5 in the above example is equal to $-\infty$. In order to avoid this value,

TABLE II
DISCRETE LYAPUNOV EXPONENT $\lambda_F^{(s)}$ AND THE DIFFERENCE $|\lambda_F^{(s)} - \lambda_f|$ FOR THE HENON MAP FOR DIFFERENT VALUES OF s AND M. THE PARAMETERS OF THE MAP ARE $a = 1.4$ AND $b = 0.3$

	M=10.000		M=20.000		M=30.000		M=40.000	
s	$\lambda_F^{(s)}$	$\mid \lambda_F^{(s)} - \lambda_f \mid$	$\lambda_F^{(s)}$	$\mid \lambda_F^{(s)} - \lambda_f \mid$	$\lambda_F^{(s)}$	$\mid \lambda_F^{(s)} - \lambda_f \mid$	$\lambda_F^{(s)}$	$\mid \lambda_F^{(s)} - \lambda_f \mid$
10	0.401692	0.017308	0.408686	0.010314	0.406863	0.012137	0.409812	0.009188
11	0.402144	0.016856	0.409427	0.009573	0.407647	0.011353	0.410702	0.008298
12	0.401663	0.017337	0.409635	0.009365	0.408109	0.010891	0.411237	0.007763
13	0.400057	0.018943	0.409583	0.009417	0.408125	0.010875	0.411412	0.007588
14	0.396502	0.022498	0.408257	0.010743	0.407368	0.011632	0.410965	0.008035
15	0.390822	0.028178	0.405267	0.013733	0.405607	0.013393	0.409723	0.009277

if we define $\ln 0 = 0$, then the discrete Lyapunov exponent of the map F is always a nonnegative number. For maps $F : \{m_0, m_1, \ldots, m_{M-1}\} \rightarrow \{m_0, m_1, \ldots, m_{M-1}\}$ which are not 1:1 and/or onto, the discrete Lyapunov exponents may take any real value (positive, zero, and negative). For example, for the map $F : \{0, 2, 3, 4, 5\} \rightarrow \{0, 2, 3, 4, 5\}$ defined as $F(0) = 4$, $F(2) = 5$, $F(3) = 4$, $F(4) = 5$, and $F(5) = 4$, its discrete Lyapunov exponent is equal to $-\ln 2/5$.

Let $C_M = \{c_0, c_1, \ldots, c_m\} \subsetneq \{0, 1, \ldots, M-1\}$. We define $\partial C_M = \{c_0 \pm 1, c_1 \pm 1, \ldots, c_m \pm 1\}$ to be the *neighboring set* of C_M (if $c_0 = 0$ or $c_m = M-1$, then the neighboring points are 1 and $M-2$, respectively). We say the set C is an *invariant set* of the map F (or an F-invariant set), if $F(C) = C$.

Definition 3: We say C is an *attractor* of the map F, if C is an invariant set of F and there exists $i \in \partial C$ such that $F(i) \in C$.

Let C_M be a set invariant under the action of the map F_M such that the map F_M restricted to the set C_M is a bijection. Let us write G_M for the map F_M restricted to the set C_M.

Definition 4: We say that a family of maps F_M is *discretely chaotic* on the sets C_M, if $\lim_{M\rightarrow\infty} \lambda_{G_M}$ is a finite positive number.

Definition 5: Let F_M be a family of maps. We say that the F_M-invariant sets C_M define discretely chaotic attractors for the maps F_M if the set C_M is an attractor of F_M for each M and $\lim_{M\rightarrow\infty} \lambda_{G_M}$ is a finite positive number.

Let

$$\mathcal{C} = \{\mathcal{F}_\mathcal{M} | \mathcal{F}_\mathcal{M} \text{ is a bijection and } \mathcal{F}_\mathcal{M} \neq \text{Id}\}$$

where Id denotes the identity, be the set of all bijections different from the identity. It is clear that for all $F_M \in \mathcal{C}$, the discrete Lyapunov exponent of F_M (defined with (2)) is always a positive number. This also reflects the fact that all periodic orbits of F_M are unstable (we say that the orbit is unstable if it is not stable). The existence of the horseshoe is a fingerprint of chaos in continuous-space systems. In discrete-space systems, however, the existence of a set, on which F_M is 1:1 and onto, and for which all periodic orbits are unstable, is a fingerprint of discrete chaos.

VI. CONCLUSION

We have suggested an answer to the question "What is chaos in finite phase-space dynamical systems?" by proposing definitions of discrete Lyapunov exponent and discrete chaos. The main results of our paper can be summarized as follows.

- We propose a generalization of the largest Lyapunov exponent for permutations defined on (arbitrary) finite lattices. As its continuous counterpart, the discrete Lyapunov exponent measures the local (between neighboring points) average spreading of the discrete-time discrete-space dynamical system considered.
- We show, in the special case when the permutation is an approximation of a chaotic map, that the discrete Lyapunov exponent and its continuous counterpart are close to each other. More precisely, let M be the cardinality of the discrete phase-space. We prove that, for large classes of chaotic maps, the corresponding discrete Lyapunov exponent approaches the largest Lyapunov exponent of a chaotic map when $M \rightarrow \infty$.
- We propose a definition of discrete chaos using similar tools as for (classical) chaos. We define discrete chaos in terms of the discrete-space Lyapunov exponent in a similar way as for continuous-space systems: the system (consisting of a map on a set of M elements) is said to be discretely chaotic if its discrete Lyapunov exponent approaches a positive number when $M \rightarrow \infty$.

Discrete chaos plays an important role in numerical computation, cryptography, digital electronics and communications and, potentially, whenever a complex continuous phenomenon is implemented on a finite-state machine. In a forthcoming paper, "Discrete chaos part II: Applications," we will report on some of them, especially those related to cryptography and secure communications. Rather than insisting here on the relevance of any of the aforementioned applications, we will just give a flavor of one we are currently exploring. In most modern block ciphers including both the former and current standards for commercial encryption data encryption standard (DES) and advanced encryption standard (AES), the confusion-diffusion strategy proposed by Shannon is implemented, roughly speaking, by means of bit permutations with strong nonlinearity (S-boxes) on subblocks of the input block and permutations with fast spreading factor on whole blocks, respectively. This being the case, the security of all these ciphers relies ultimately on such permutations delivering the right mixing and propagation properties. Here is where discrete chaos comes in: it provides tools like Lyapunov

exponent and others being developed to quantify the said properties. The design and certification of special-purpose permutations is just an example of possible and interesting applications of discrete chaos to cryptography. Others include the design of cryptographic algorithms, hash functions and the like—a new and exciting research area.

REFERENCES

[1] T. Y. Li and J. A. Yorke, "Period three implies chaos," *Amer. Math. Month.*, vol. 82, pp. 985–992, 1975.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1949.

[3] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurc. Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[4] M. C. Gutzwiller, *Chaos in Classical and Quantum Mechanics*. New York: Springer-Verlag, 1990.

[5] F. Haake, *Quantum Signatures of Chaos*. Berlin, Germany: Springer-Verlag, 1992.

[6] B. V. Chirikov and F. Vivaldi, "An algorithmic view of pseudochaos," *Physica D*, vol. 129, no. 3–4, pp. 223–235, May 1999.

[7] E. Ott, *Chaos in Dynamical Systems*. New York: Cambridge University Press, 1993.

[8] H. D. I. Abarbenel, *Analysis of Observed Chaotic Data*. New York: Springer-Verlag, 1995.

[9] D. R. Frey, "Chaotic digital encoding: an approach to secure communications," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 40, no. 10, pp. 660–666, Oct. 1993.

[10] S. A. Barbulescu, A. Guidi, and S. P. Pietrobon, "Chaotic turbo codes," presented at the Proc. ISIT'00, Sorrento, Italy, Jun. 25–30, 2000, Paper no. 165, unpublished.

[11] G. M. Maggio, N. Rulkov, and L. Reggiani, "Pseudo-chaotic time hopping for UWB impulse radio," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 48, no. 12, pp. 1424–1435, Dec. 2001.

[12] L. Kocarev, "Chaos-based cryptography: A brief overview," *IEEE Circuits Syst. Mag.*, vol. 1, no. 3, pp. 6–21, Mar. 2001.

[13] F. Dachselt and W. Schwarz, "Chaos and cryptography," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 48, no. 12, pp. 1498–1509, Dec. 2001.

[14] J. Szczepanski, J. M. Amigo, T. Michalek, and L. Kocarev, "Cryptographically secure substitutions based on the approximation of mixing maps," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 52, no. 2, pp. 443–453, Feb. 2005.

[15] N. Masuda and K. Aihara, "Cryptosystems with discretized chaotic maps," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 49, no. 1, pp. 28–40, Jan. 2002.

[16] L. Kocarev and J. Szczepanski, "Finite-space Lyapunov exponents and pseudochaos," *Phys. Rev. Lett.*, vol. 93, p. 234 101, 2004.

[17] R. Ash, *Information Theory*. New York: Interscience, 1965.

Ljupco Kocarev (F'06) is a Research Scientist at the Institute for Nonlinear Science, University of California San Diego, and Professor at the Graduate School of Electrical Engineering, University "Kiril i Metodij," Skopje, Macedonia. His scientific interests include nonlinear systems and circuits, coding and information theory, networks and networks on chip, and cryptography. He has coauthored more than 100 journal papers in 18 different international peer-reviewed journals ranging from mathematics to physics and from electrical engineering to computer sciences.

Dr. Kocarev is a foreign member of the Macedonian Academy of Sciences and Arts. According to the *Science Citation Index*, his work has been cited more than 2500 times.

Janusz Szczepanski received the M.Sc. degree in mathematics and the Ph.D. degree in applied mathematics from Warsaw University, Warsaw, Poland, and the Polish Academy of Sciences, Warsaw, Poland, in 1979 and 1985, respectively.

He is a Researcher at the Institute of Fundamental Technological Research, Polish Academy of Sciences. In 2001–2004, he was a Consultant on Cryptography with the Polish Certification Authority (Root) for Public Key Infrastructure (Trust and Certification Centre "CENTRAST" Co.), Warsaw, Poland. In 2000 and 2003, he was a Visiting Scientist at the Miguel Hernández University, Elche, Spain, and in 2004, he was a Visiting Scholar at the University of California, San Diego. His research interests include cryptography, information theory, and application of dynamical systems and stochastic processes to biological systems.

Dr. Szczepanski received the PAS Award in 1989.

José M. Amigó received the Ph.D. degree in theoretical physics from the University of Gottingen, Gottingen, Germany, in 1987.

He was a Postdoctoral Fellow at the National Aerospace Laboratory, Tokyo, Japan, in 1989–1990, and a System Analyst with Construcciones Aeronauticas S.A., Madrid, Spain, in 1991–1997. Currently, he is an Associate Professor of Applied Mathematics at Miguel Hernandez University, Elche, Spain, and affiliated with its Operations Research Centre.

Igor Tomovski received the B.Sc. degree in electrical engineering from the University "Kiril and Metodij," Skopje, Macedonia, in 1997. He is currently working toward the Ph.D. degree at the same university. His Ph.D. dissertation relates to chaos synchronization.

He is also a System Manager at the Institute of Earthquake Engineering and Engineering Seismology, Skopje, Macedonia. His research interests include nonlinear and chaotic phenomena in the microelectronic devices.