



Centro de  
Investigación  
Operativa



I-2006-03

## Order Patterns and Chaos

J.M. Amigó, L. Kocarev and

J. Szczepanski

January 2006

ISSN 1576-7264

Depósito legal A-646-2000

**Centro de Investigación Operativa**  
Universidad Miguel Hernández de Elche  
Avda. de la Universidad s/n  
03202 Elche (Alicante)  
cio@umh.es

TRABAJOS I+D

# Order Patterns and Chaos

José M. Amigó<sup>1\*</sup>, Ljupco Kocarev<sup>2</sup> and Janusz Szczepanski<sup>3</sup>

<sup>1</sup>Centro de Investigación Operativa, Universidad Miguel Hernández, 03202 Elche, Spain.

<sup>2</sup>Institute for Nonlinear Science, University of California, San Diego. 9500 Gilman Drive, La Jolla, CA 92093-0402.

<sup>3</sup>Institute for Fundamental Technological Research, Polish Academy of Sciences, Swietokrzyska 21, PL-00-049 Warsaw.

**Abstract.** Chaotic maps can mimic random behavior in a quite impressive way. In particular, those possessing a generating partition can produce any symbolic sequence by properly choosing the initial state. We study in this letter the ability of chaotic maps to generate order patterns and come to the conclusion that their performance in this respect falls short of expectations. This result reveals some basic limitation of a deterministic dynamic as compared to a random one. This being the case, we propose a non-statistical test based on ‘forbidden’ order patterns to discriminate chaotic from truly random time series with, in principle, arbitrarily high probability. Some relations with discrete chaos and chaotic cryptography are also discussed.

PACS numbers: 05.45.Vx, 89.70.+c

Keywords: Chaotic maps, order patterns, permutation entropy, discrete Lyapunov exponent, chaotic cryptography.

## 1. Introduction

Random systems and chaotic systems share some important features, both from the theoretical and practical point of view. Thus one can define truly random symbolic dynamics by means of chaotic maps, what boils down to the fact that the dynamical systems defined by the iteration of such maps are isomorphic (or conjugate) to shift systems on sequence spaces — standard models for stationary random processes — despite their different nature. For instance, the logistic map  $f(x) = 4x(1-x)$ ,  $0 \leq x \leq 1$ , and the Bernoulli shift  $\mathcal{B}(\frac{1}{2}, \frac{1}{2})$ , modelling the tossing of a fair coin,  $X_n : \{\text{head, tail}\} \rightarrow \{0, 1\}$ ,  $n = 0, 1, \dots$ , are isomorphic via the following recipe: if  $f^n(x_0) \in [0, \frac{1}{2})$ , set  $X_n = 0$ ; if  $f^n(x_0) \in [\frac{1}{2}, 1]$ , set  $X_n = 1$  (for any ‘typical’ initial point  $x_0$ ). This and similar properties are exploited v.g. in the generation of pseudo-random sequences in different applications.

Although we will address the isomorphy between random and chaotic systems with more detail below, the actual focus of this letter is rather on the differences between random and chaotic systems and, specifically, on the order relations (or *order patterns*) defined by chaotic orbits of piecewise monotone interval maps. Indeed, if an order pattern is missing, then its absence pervades all longer patterns in form of more missing order patterns. In other words, chaotic trajectory points, as random as they may look,

---

\*Corresponding author. E-mail address: jm.amigo@umh.es

cannot be ordered in arbitrary ways—in contrast to the orbits of random processes with arbitrary alphabets. Not occurring order patterns will be called *forbidden patterns* and (somewhat paradoxically) their ‘existence’ can be used to tell chaotic from random time series with, in principle, arbitrarily high probability. Furthermore, this method is also robust against noisy data and, under circumstances, it can be a practical alternative to more conventional techniques.

We will also refer to some relations to discrete chaos and chaotic cryptography. In fact, it was in the framework of discrete chaos and its applications to cryptography where the authors first noticed that determinism imposes some limitations on the permutations (i.e., order patterns) that a chaotic map can define directly by means of their orbits. Although the possible consequences for chaotic cryptography (and, eventually, for other application areas) are more of a theoretical sort, it seems nevertheless that there some basic limitations exist as for what can be done by means of chaotic maps if used in a straightforward, naive way.

In the last section we will come back to the relation between chaotic and symbolic dynamics since the different performance of deterministic and random systems, as measured by the order patterns, may seem at odds with the possibility of being isomorphic.

## 2. Order patterns

It is well-known [1] that given, say, the *logistic map*  $f(x) = 4x(1 - x)$ ,  $0 \leq x \leq 1$ , and any binary block of length  $L$ ,  $b_1^L = b_1 \dots b_L$  with  $b_i \in \{0, 1\}$ , then there exists  $x_0 \in [0, 1]$  such that the symbolic sequence generated by the orbit segment  $\{x_0, f(x_0), \dots, f^{L-1}(x_0)\}$  is precisely  $b_1^L$ . Here and below,  $f^n(x) := f(f^{n-1}(x))$  and  $f^0(x) := x$ . Let us remind that the symbol corresponding to  $f^k(x_0)$  is 0 or 1 depending on whether  $f^k(x_0) \in [0, 1/2)$  or  $f^k(x_0) \in [1/2, 1]$ , respectively, the partition  $\{[0, 1/2), [1/2, 1]\}$  being a generating partition for the logistic map. It follows easily that any finite-length binary block can be realized in this way starting from an initial point in a set of positive Lebesgue measure. This property can be generalized to any strong mixing map with a generating partition  $\alpha = \{\alpha_1, \dots, \alpha_{|\alpha|}\}$  and length  $L$  blocks (‘words’) made out of the symbols (‘letters’)  $1, 2, \dots, |\alpha|$ .

In a similar way, given an interval map  $f : I \rightarrow I$ , we can also associate to the orbit segment  $\{f^k(x) : 0 \leq k \leq L - 1\}$  its order pattern  $\pi(x) \in \sigma_L$ , where  $\sigma_L$  is the set of permutations on  $\{0, 1, \dots, L - 1\}$ , as follows. We say that  $x$  *defines the order pattern*  $\pi = \pi(x) = [\pi(0), \dots, \pi(L - 1)]$  (shorthand for  $0 \mapsto \pi(0), \dots, L - 1 \mapsto \pi(L - 1)$ ) of length  $L \geq 2$ , if

$$f^{\pi(0)}(x) < f^{\pi(1)}(x) < \dots < f^{\pi(L-1)}(x).$$

Alternatively, we say that  $\pi$  is realized by  $x$ . Furthermore, set

$$P_\pi = \{x \in I : x \text{ defines } \pi \in \sigma_L\}.$$

Numerical simulation shows that, contrarily to what happens with symbol blocks, not all possible order patterns  $\pi \in \sigma_L$  are realized by the points of  $I$  for  $L$  sufficiently large. In other words, there are  $L \geq 2$  and  $\pi \in \sigma_L$  such that  $P_\pi = \emptyset$ . If  $f$  is piecewise continuous and  $P_\pi \neq \emptyset$ , then  $P_\pi$  has positive Lebesgue measure.

**Example 1.** As a simple illustration, consider again the logistic map. For  $L = 2$  we have

$$P_{[0,1]} = \left(0, \frac{3}{4}\right), \quad P_{[1,0]} = \left(\frac{3}{4}, 1\right).$$

But already for  $L = 3$  ( $f^2(x) = -64x^4 + 128x^3 - 80x^2 + 16x$ ) there are permutations that are not realized:

$$\begin{aligned} P_{[0,1,2]} &= \left(0, \frac{1}{4}\right), & P_{[0,2,1]} &= \left(\frac{1}{4}, \frac{5-\sqrt{5}}{8}\right), \\ P_{[2,0,1]} &= \left(\frac{5-\sqrt{5}}{8}, \frac{3}{4}\right), & P_{[1,0,2]} &= \left(\frac{3}{4}, \frac{5+\sqrt{5}}{8}\right), \\ P_{[1,2,0]} &= \left(\frac{5+\sqrt{5}}{8}, 1\right), & P_{[2,1,0]} &= \emptyset. \end{aligned}$$

In turn, this implies that the pattern  $[*, 2, *, 1, *, 0, *]$  (where  $*$  stands eventually for any other entries of the pattern) cannot be realized by any  $x \in [0, 1]$  since the inequality  $f^2(x) < f(x) < f^0(x)$  cannot occur. By the same token, the pattern  $[*, n+2, *, n+1, *, n, *]$  (obtained by substituting  $x$  by  $f^n(x)$  in the previous pattern) cannot be realized either for the same reason.

Numerical experimentation strongly suggests that the number of  $P_\pi \neq \emptyset$ ,  $\pi \in \sigma_L$ , grows only exponentially with  $L$ , while the number of all such patterns grows as  $L! \propto (L/e)^L \sqrt{2\pi L}$  (Stirling's formula). The same follows for the *tent map*,

$$\Lambda(x) = \begin{cases} 2x & 0 \leq x \leq \frac{1}{2} \\ 2-2x & \frac{1}{2} \leq x \leq 1 \end{cases}. \quad (1)$$

In fact,  $\Lambda$  preserves Lebesgue measure  $d\lambda = dx$  and the logistic map  $f$  preserves  $d\mu = \frac{1}{\pi\sqrt{x(1-x)}}dx$ ; if  $\phi : (I, \lambda) \rightarrow (I, \mu)$  is the measure preserving isomorphism given by

$$\phi(x) = \sin^2\left(\frac{\pi}{2}x\right), \quad (2)$$

then the dynamical systems  $(\Lambda, \lambda)$  and  $(f, \mu)$  are *isomorphic* (or conjugate) by means of  $\phi$ , i.e.,  $f \circ \phi = \phi \circ \Lambda$ . Since, moreover,  $\phi$  is strictly increasing, forbidden patterns for  $f$  correspond to forbidden patterns for  $\Lambda$  in a one-to-one way.

From the last paragraph it should be clear that isomorphic dynamical systems need not have the same forbidden patterns: the isomorphism ( $\phi$  above) must also preserve the linear order of both spaces (supposing both spaces are linearly ordered), and this will be in general not the case. For example, the  $\lambda$ -preserving *shift map*  $x \mapsto 2x \pmod{1}$ ,  $0 \leq x \leq 1$ , has no forbidden patterns of length 3, although it is isomorphic to the logistic and tent maps.

At hand of these and other examples, we conclude that, when looking for order patterns in the orbits of a chaotic maps, they seem to be 'short' on supply. Somehow, the weird behavior that chaos entails to deterministic maps is not enough to display all possibilities that order patterns offer. This may seem puzzling when one thinks that the logistic and tent maps are, in turn, isomorphic to the  $(\frac{1}{2}, \frac{1}{2})$ -Bernoulli shift, a probabilistic model for the repeated tossing of a fair coin. We will elaborate on this below.

### 3. Permutation entropy

The sets  $P_\pi$  (each being, in general, a union of intervals) appear in the theory and practice of *permutation entropy*. Given a closed interval  $I \subset \mathbb{R}$  and a map  $f : I \rightarrow I$  with invariant measure  $\mu$  (i.e.,  $\mu(f^{-1}B) = \mu(B)$  for every Borel set  $B \subset I$ ), define the partition  $\mathcal{P}_L^*$  of  $I$  as

$$\mathcal{P}_L^* = \{P_\pi \neq \emptyset : \pi \in \sigma_L\}$$

and the *topological permutation entropy of order  $L \geq 2$*  as

$$\bar{H}_0^{(L)}(f) = \frac{1}{L-1} \log |\mathcal{P}_L^*|,$$

where  $|\cdot|$  denotes here cardinality. If  $f$  is a *piecewise monotone* interval map (i.e., there is a finite partition of  $I$  into intervals, such that  $f$  is continuous and monotone on each of those intervals), then [2]

$$\lim_{L \rightarrow \infty} \bar{H}_0^{(L)}(f) = h_{top}(f), \quad (3)$$

where  $h_{top}(f)$  is the topological entropy of  $f$ , an upper bound of Kolmogorov-Sinai (or measure-theoretic) entropy with better continuity properties. It follows that

$$|\mathcal{P}_L^*| = |\{P_\pi \neq \emptyset : \pi \in \sigma_L\}| \propto e^{Lh_{top}(f)}, \quad (4)$$

as anticipated above. Take now  $L$  finite in (3) to find that  $\bar{H}_0^{(L)}(f)$  can be used as an estimator of the topological entropy, albeit the convergence with  $L$  turns out to be slow.

Along similar lines one can also define a *measure-theoretic permutation entropy* [2, 3]. A very appealing aspect of permutation entropy is its no need for generating partitions nor suprema, as in the case of measure-theoretic and topological entropies. Both measure-theoretic and topological permutation entropy only resort to the family of partitions  $\mathcal{P}_L^*$ ,  $L \geq 2$ , whose intervals are given by the crossings of the curves  $y = x, y = f(x), \dots, y = f^{L-1}(x)$ .

Let us emphasize at this point that the (for physical applications, very mild) mathematical assumptions we made above, are important. For example, (3) and, hence, (4) do not hold if the number of monotony intervals is not finite [4]. Summarizing, we have:

**Proposition 1.** *If  $f$  is a piecewise monotone map on a one-dimensional closed interval, then there are  $L \geq 2$  and  $\pi \in \sigma_L$  such that  $P_\pi = \emptyset$ .*

This result, applied to chaotic maps, shows that deterministic chaotic dynamics is detectable by means of order patterns. In other words, chaos cannot mimic all features of randomness. The problem remains though in that randomness can mimic chaos against all odds. How high are the odds against?

### 4. Forbidden patterns

The bottom line of Proposition 1 is that, for every piecewise monotone interval map  $f$ , there are order patterns of minimal length which cannot occur in any orbit.

We will call them *forbidden patterns* for  $f$  and recall how their absence paradoxically pervades all longer patterns in form of *forbidden outgrowth patterns*: If  $\pi_{forb} = [\pi_1, \dots, \pi_{L_0}]$  is forbidden for  $f$ , then all the patterns  $[\ast, \pi_1 + n, \ast, \dots, \ast, \pi_{L_0} + n, \ast] \in \sigma_L$  with  $n = 0, 1, \dots, L - L_0$ , are also forbidden for  $f$ . Denote now by  $\sigma_L^{out}(\pi_{forb})$  the family of length  $L > L_0$  outgrowth patterns of  $\pi_{forb}$ . Alone the outgrowth patterns  $[\ast, \pi_1, \ast, \dots, \ast, \pi_{L_0}, \ast] \in \sigma_L$  (corresponding to  $n = 0$ ) amount to  $L!/L_0!$ , so that  $|\sigma_L^{out}(\pi_{forb})| = O(L!) = O(L^{L+1/2}e^{-L}) = O(e^{L(\log L - 1) + (1/2)\log L})$ . Thanks to this super-exponential magnifying effect, the probability of a false forbidden pattern vanishes extremely fast with  $L$  and, consequently, a missing pattern  $\pi \in \sigma_{L_0}$  can be promoted to forbidden with virtually absolute confidence if  $\sigma_L^{out}(\pi) = \emptyset$  for moderate values of  $L > L_0$ . Only those chaotic maps with all forbidden patterns of exceedingly long length seem to be intractable from the practical point of view. Knowing that  $|\mathcal{P}_L^\ast| \propto e^{h_{top}(f)L}$  and  $|\sigma_L| \propto (L/e)^L \sqrt{2\pi L}$ , we deduce that this can only happen if  $h_{top}(f) \gtrsim \ln L_0$ , where  $L_0 \gg 1$  is the shortest length of the forbidden patterns.

We conclude that the existence of forbidden patterns is a feature that chaotic dynamics does not share with random dynamics and, therefore, can be used as a *test* to tell random from pseudo-random orbit generation. A naive implementation of this test could be computationally costly, but one can easily devise different strategies (e.g., using many short orbit segments instead of a very long one) in order to lower the pattern lengths to manageable values —assuming the existence of forbidden patterns of moderate lengths.

Of course, given an information source that outputs a seemingly non periodic sequence of real numbers  $x_i$ , one can try to decide whether the ensuing time series is deterministic or random just by plotting the pairs  $(x_i, x_{i+1})$ . But depending on the length of the series and, given the case, on the complexity of the deterministic dynamics, this approach will work or fail. In such cases, the search and tracing of forbidden patterns and their outgrowths in sliding windows of increasing widths can make the difference. Moreover, order patterns are robust against experimental and numerical noise (since they are defined by inequalities), provided in the second case that data precision does not deteriorate with map iteration beyond some minimal and sufficiently high threshold. Forbidden patterns masked by noisy data can eventually be uncovered using different initial points.

## 5. Discrete Lyapunov exponent

Interestingly enough, the authors came across the fore-going questions when developing the theory of *discrete chaos* [5, 6] and, specifically, when generalizing the concept of Lyapunov exponent to maps on finite sets —a concept we call *discrete Lyapunov exponent*.

**Definition 1.** Let  $S = \{s_0, s_1, \dots, s_{M-1}\}$  be a linearly ordered set by means of the order  $<$ , endowed with a metric  $d(\cdot, \cdot)$ , and let  $F : S \rightarrow S$  be a bijection (or, equivalently, an  $M$ -permutation). We define the discrete Lyapunov exponent (DLE) of  $f$  on  $(S, <, d)$ ,  $\lambda_F$ , as

$$\lambda_F = \frac{1}{M-1} \sum_{i=0}^{M-2} \ln \frac{d(F(s_i), F(s_{i+1}))}{d(s_i, s_{i+1})}$$

As in the usual definition of Lyapunov exponent, we have also taken natural logarithms. Without loss of generality, we may assume  $S = \{0, 1, \dots, M - 1\} \equiv \mathbb{Z}_M$  setting, if necessary,  $F(i) \equiv F(s_i)$  and  $d(i, j) \equiv d(s_i, s_j)$ . Observe that  $\lambda_F$  depends both on the order  $<$  and on the metric  $d$ , but it is invariant under rescaling and, furthermore, has the same invariances as  $d$ .

**Example 2.** Suppose that  $M = 2m$ ,  $d$  is Euclidean distance, and define

$$F_M^{\max}(s) = \begin{cases} m + k & \text{if } s = 2k & 0 \leq k \leq m - 1 \\ k & \text{if } s = 2k + 1 & 0 \leq k \leq m - 1 \end{cases}$$

on  $\{0, 1, \dots, M - 1\}$ . The DLE of  $F_M^{\max}$  is

$$F_M^{\max} = \frac{m}{2m - 1} \ln m + \frac{m - 1}{2m - 1} \ln(m + 1).$$

It can be proved [6] that  $\lambda_F \leq \lambda_{F_M^{\max}}$  for all permutations  $F$  on  $\{0, 1, \dots, M - 1\}$  endowed with Euclidean distance  $d(i, j) = |i - j|$ . In this sense,  $F_M^{\max}$  is the most chaotic map on  $(\mathbb{Z}_M, <, |\cdot|)$ . Observe for further reference that  $\lim_{M \rightarrow \infty} \lambda_{F_M^{\max}} = \infty$ .

For simplicity, we will consider henceforth *chaotic* maps only on one-dimensional intervals. Specifically, let  $f : I \rightarrow I$  be a piecewise smooth map with invariant measure  $\mu$  and Lyapunov exponent  $\lambda_f = \int_I \ln |f'(z)| d\mu(z) > 0$ . Let  $z_{j+1} = f(z_j)$ ,  $j = 0, 1, \dots, M - 1$ , be a *typical* trajectory of length  $M$  of a one-dimensional chaotic map  $f$ , such that  $z_{j+1} \neq z_j$  for all  $j$  and  $|z_{M-1} - z_0| < \varepsilon$ . We define  $f(z_{M-1}) = z_0$  and order  $z_j$  according to the metric to obtain  $x_j$ , that is,  $x_0 < x_1 < \dots < x_{M-1}$ , so that  $x_i$  and  $x_{i+1}$  are neighbors in the metric sense. Define  $m_i = \lfloor x_i N \rfloor$ , where  $N$  is chosen such that  $m_i \neq m_j$  for all  $i$  and  $j$ . The map  $f$  induces then the obvious permutation  $F_M : \{m_0, \dots, m_{M-1}\} \rightarrow \{m_0, \dots, m_{M-1}\}$  with  $F(m_i) = m_j$  when  $f(x_i) = x_j$ . The following theorem justifies calling  $\lambda_{F_M}$  a discrete Lyapunov exponent.

**Theorem 1.** *Let  $f : I \rightarrow I$  be a one-dimensional chaotic map with piecewise continuous derivative. Then  $\lim_{M \rightarrow \infty} \lambda_{F_M} = \lambda_f$ , where  $\lambda_f$  is the Lyapunov exponent of  $f$ .*

A straightforward consequence of this result is that any family of  $M$ -permutations  $F_M$  (on  $\{m_0, \dots, m_{M-1}\}$  and thus) on  $\{0, \dots, M - 1\}$  obtained in the way just explained from a piecewise smooth chaotic map  $f$ , cannot be arbitrary (at least, for generic initial points) since all of them must deliver  $\lim_{M \rightarrow \infty} \lambda_{F_M} = \lambda_f < \infty$ . In particular, there are no typical initial points for any chaotic map such that  $F_M = F_M^{\max}$  for every  $M$ . Of course, measure zero sets can have infinite elements and be dense, but the probability of picking one or several of their elements in a random sample is zero, so that, from the practical point of view, they play no role.

Since permutations and order patterns can be identified as we did above, we arrive again at our previous result on the inability of chaotic maps to generate arbitrary order patterns—in contrast with their ability for producing arbitrary symbols patterns. The sort of limitation we are talking about might have some nontrivial consequences. Think, for example, of chaotic cryptography, where chaotic orbits are used in different ways to define cryptographic primitives and algorithms. As we have already pointed

out, Theorem 1 implies some restrictions on the structure of the permutation families that can be obtained via truncation and discretization from chaotic orbits. In particular, we cannot obtain the sequence of permutations  $F_M^{\max}$  with the optimal diffusion factors (i.e., greatest possible DLEs) for arbitrary  $M$ . As a consequence, truncation and discretization of chaotic orbits should be avoided when defining cryptographic substitutions; for better methods, see v.g. [7].

## 6. Chaos and symbolic dynamics

To close our excursion through order, chaos and randomness, we would like to return to one of their most intriguing aspects: the isomorphy of random and chaotic systems, despite the different quality of their orbits.

Any stationary stochastic process corresponds to a measure-preserving shift transformation on a sequence space in a standard way [3, 8]. Such shift systems, sometimes called sequence space models, allow to focus on the random process itself as given by the probability distribution of its outputs, dispensing with a perhaps complicated underlying probability space. Among them, the Bernoulli shift  $\mathcal{B}(p_1, \dots, p_k)$  (acting on two-sided or one-sided infinite strings made out of  $k$  symbols) models (or is) an independent identically distributed stochastic process indexed by the integers or by the non-negative integers (respectively), where  $p_i$  is the probability for obtaining the  $i$ th symbol in any draw. In particular,  $\mathcal{B}(\frac{1}{2}, \frac{1}{2})$  models an experimenter tossing a fair coin forever.

On the other hand, the stochastic process  $\mathcal{B}(\frac{1}{2}, \frac{1}{2})$  is isomorphic to the dynamical system defined by, say, the tent map on  $I = [0, 1]$  (see (1)). Indeed, let  $X = \prod_0^\infty \{0, 1\} = \{\xi = (\xi_0, \xi_1, \dots, \xi_n, \dots) : \xi_n = 0, 1\}$  be the space of one-sided infinite binary strings, each symbol  $a_i \in \{0, 1\}$  having measure  $p_{a_i} = \frac{1}{2}$  and the product measure  $\nu$  being given on the *cylinder sets*  $\{\xi \in X : \xi_{t+1} = a_1, \dots, \xi_{t+n} = a_n\}$  (they are the generators of the product sigma-algebra) by

$$\nu(\{\xi \in X : \xi_{t+1} = a_1, \dots, \xi_{t+n} = a_n\}) = p_{a_1} \dots p_{a_n}.$$

This measure is preserved by the one-sided *Bernoulli shift* transformation  $\Sigma : (\xi_0, \xi_1, \xi_2, \dots) \mapsto (\xi_1, \xi_2, \xi_3, \dots)$ . Furthermore, define the measure preserving *coding map*  $\varphi : I \rightarrow X$  ( $I$  endowed with the  $\Lambda$ -invariant Lebesgue measure  $\lambda$ ) by

$$\varphi(x) = (a_0, \dots, a_n, \dots) \text{ if } \Lambda^n(x) \in A_{a_n}$$

where  $A_0 = [0, \frac{1}{2})$  and  $A_1 = [\frac{1}{2}, 1]$  build a generating partition for  $\Lambda$ . Then  $\varphi \circ \Lambda = \Sigma \circ \varphi$ , i.e.,  $(\Lambda, \lambda)$  and  $(\Sigma, \nu)$  are isomorphic. Observe that  $\varphi$  converts the orbits of  $\Lambda$  (sequences of real numbers) into binary strings. It was precisely the map  $\varphi \circ f$ , with  $f$  the logistic map, whose orbits we stated in Sect. 2 can realize any possible binary string.

But, in spite of the dynamical equivalence of  $(\Sigma, \nu)$  and  $(\Lambda, \lambda)$  (or  $(f, \mu)$ ,  $f$  the logistic map, for that matter), we know that the orbits of  $\Lambda$  and  $f$  cannot realize any possible order, while the orbits of  $\Sigma$  can. The mechanism responsible for this hides in the coding map  $\varphi$ , since it clearly does not preserve the linear order of  $I$ . As a result, the coarse-grained dynamics  $(\Sigma, \nu)$  can be truly random (hence, without forbidden patterns), whereas the underlying fine-grained dynamics  $(\Lambda, \lambda)$  or  $(f, \mu)$  is deterministic (hence, with forbidden patterns).

## 7. Conclusion

Chaos manages easily to reproduce an exponentially growing manifold of patterns (like symbol blocks) but, subject to very mild mathematical conditions, cannot cope with a super-exponentially growing manifold such as that of order patterns. This shortcoming has been exposed by means of the permutation entropy and the discrete Lyapunov exponent. Only truly random dynamical systems (i.e., stationary random processes with arbitrary alphabets) are up to the task. A first consequence of this limitation is the possibility of distinguishing random from chaotic systems with, in principle, arbitrarily high probability, by tracing forbidden patterns and their outgrowths. Further consequences related to discrete chaos and chaotic cryptography have been also discussed.

## Acknowledgements

J.M.A. has been partially supported by the Spanish Ministry of Education and Science, grant GRUPOS 04/79. L.K. has been supported by the Spanish Ministry of Education and Science, grant SAB2004-0048. L.K. also thanks NSF for partial support.

## References

- [1] P. Collet and J.P. Eckmann, *Iterated Maps on the Interval as Dynamical Systems* (Birkhäuser, Boston, 1997).
- [2] C. Bandt, G. Keller and B. Pompe, *Nonlinearity* **15**, 1595 (2002).
- [3] J.M. Amigó, M.B. Kennel and L. Kocarev, *Physica D* **210**, 77 (2005).
- [4] M. Misiurewicz, *Nonlinearity* **16**, 971 (2003).
- [5] L. Kocarev and J. Szczepanski, *Phys. Rev. Lett.* **93**, 234101 (2004).
- [6] L. Kocarev, J. Szczepanski, J.M. Amigó and I. Tomovski, “Discrete Chaos – Part I: Theory” (submitted).
- [7] J. Szczepanski, J.M. Amigó, T. Michalek and L. Kocarev, *IEEE Trans. Circ. and Systems I* **52**, 443 (2005).
- [8] K. Petersen, *Ergodic Theory*, Cambridge University Press, 1983.