Commun Nonlinear Sci Numer Simulat 19 (2014) 2345–2353

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

Application of Gray codes to the study of the theory of symbolic dynamics of unimodal maps

David Arroyo [a,*], Gonzalo Alvarez [b]

[a] Grupo de Neurocomputación Biológica, Dpto. de Ingeniería Informática, Escuela Politécnica Superior, Universidad Autónoma de Madrid, 28049 Madrid, Spain
[b] Instituto de Seguridad de la Información, Consejo Superior de Investigaciones Científicas, Serrano 144, 28006 Madrid, Spain

ARTICLE INFO

Article history:
Received 2 June 2013
Accepted 10 November 2013
Available online 20 November 2013

Keywords:
Unimodal maps
Kneading sequences
Symbolic sequences
Gray Ordering Number
GON
Mandelbrot map

ABSTRACT

In this paper we provide a closed mathematical formulation of our previous results in the field of symbolic dynamics of unimodal maps. This being the case, we discuss the classical theory of applied symbolic dynamics for unimodal maps and its reinterpretation using Gray codes. This connection was previously emphasized but no explicit mathematical proof was provided. The work described in this paper not only contributes to the integration of the different interpretations of symbolic dynamics of unimodal maps, it also points out some inaccuracies that exist in previous works.

1. Introduction

A symbolic sequence is a transformation of a sequence of real numbers into a sequence consisting of a set of symbols. Regarding unimodal maps, the cardinality of that set is two and it is determined by the turning point of the iteration function of the map. Accordingly, each symbol represents the relative position of a real-value with respect to the turning point. In [1] it is pointed out the existence of an inner order of the symbolic sequences, along with the relationship between this order and the initial condition and the control parameter of the underlying chaotic system. The considerations and results of [1] were later improved and enlarged through different contributions, being the most important [2,3]. In [4] it was remarked that the order of the symbolic sequences can be interpreted using the concept of Gray codes. In this novel approach to the problem, the symbolic sequences are finally converted into a figure which is a real number between 0 and 1 called Gray Ordering Number or simply GON. Afterwards, [5] drew the bridge between the ideas of [4] and the main theory of applied symbolic dynamics as expressed in [3]. Finally, some theorems are offered in [6], which enlarge the theoretical framework of the GON of unimodal maps. In [6] it is explained that the dynamical properties of unimodal maps by means of the GON are a translation of the theoretical framework inherited from [1]. Nevertheless, there is no direct and explicit proof of this equivalence. One of the main applications of the concept of the GON is the estimation of the control parameter of unimodal maps for cryptanalysis [7–10]. The precise definition of the key space of a cryptosystem is a commitment in cryptography. In the context of chaotic cryptography, it implies that the control parameters and initial conditions of the chaotic system must be selected to guarantee chaoticity, and to avoid the estimation of either control parameters or initial conditions from partial information about the chaotic orbits [11, Rule 5]. In case that this partial information arises from the symbolic sequences of the chaotic map used for encryption, we must assess that it is not possible to get an accurate enough estimation of control

* Corresponding author.
E-mail addresses: david.arroyo@uam.es, david.arroyo@iec.csic.es (D. Arroyo).

1007-5704/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.cnsns.2013.11.005

parameters and/or initial conditions. Therefore, a rigorous and concrete theoretical framework is required to quantify the precision of the procedures for the estimation of the control parameter and the initial condition of unimodal maps from their symbolic sequences. This paper presents this concretion and also shows that some of the theorems in [6] are not totally accurate. In this sense, those theorems are not only criticized but also rewritten.

This paper is organized as follows. First of all, Section 2 introduces the class of maps under study and the main aspects of their symbolic dynamics. Section 3 remarks the existence of an inner order for the symbolic sequences of a certain class of unimodal maps and a relationship between that order and the order of the initial conditions employed in their generation. In Section 4 the order of the symbolic sequences is rewritten in terms of Gray codes and the concept of Gray Ordering Number is introduced. After that, Section 5 introduces a subclass of the class of considered unimodal maps. This subclass of unimodal maps is defined in a parametric way, i.e., their dynamics depend on a control parameter. This dependency is analyzed by means of the GON. This study will lead to the revision and proof of all theorems in [6]. Finally, Section 7 summarizes the main results of the present work.

2. Scenario

The work described in this paper is focused on a special class of functions. This class is denoted by $\mathcal{F}$. A function f belonging to the class $\mathcal{F}$ is defined in the interval $I = [a, b]$ for $a < b$ and satisfies:

1. f is a continuous function in I.
2. $f(a) = f(b) = a$.
3. $f(x)$ reaches its maximum value $f_{\max} \leqslant b$ in the sub-interval $[a_m, b_m] \subset I$ so that $a_m \leqslant b_m$.
4. $f(f_{\max}) < x_c$ and $f(f_{\max}) \geqslant a$, where x_c is the middle point of the interval $[a_m, b_m]$, i.e., $x_c = \frac{a_m + b_m}{2}$.
5. $f(x_c) > x_c$.
6. $f(x)$ is an strictly increasing function in $[a, a_m]$ and an strictly decreasing function in $[b_m, b]$.

Although the work in this paper is focused on the class of functions $\mathcal{F}$, it is possible to extend it to other class of functions considering the topological conjugacy of maps [12, p. 72]. This other class of functions is named $\mathcal{F}^*$ and any f included in $\mathcal{F}^*$ has the same properties as those in $\mathcal{F}$ with the exception of properties (3) and (6), since if f is in $\mathcal{F}^*$, then it possesses a minimum value in $[a_m, b_m]$ and is strictly decreasing in $[a, a_m]$ and strictly increasing in $[b_m, b]$.

Hereafter, the function $f(x)$ is considered as a way to generate a sequence of numbers $\{x_i\}$ from a certain initial value x_0. Each number x_i determines the next element of the sequence trough $x_{i+1} = f(x_i)$. After a transient number of iterations, all the x_i values are inside the interval $[x_{\min}, x_{\max}]$, where $x_{max} = f(x_c)$ and $x_{min} = f(x_{\max})$.

The tent map is included in the class $\mathcal{F}$ and is represented in Fig. 1. In this case $a_m = b_m = x_c$ and $f_{\max} = f(x_c) = b$. A certain value $x_{i+1} \neq x_c$ can be derived from two different values of x_i, as Fig. 1 informs. In other words, it is satisfied that $x_{i+1} = f(x_i^L) = f(x_i^R)$, where $x_i^L \neq x_i^R$, $x_i^L < x_c$ and $x_i^R > x_c$. This is a common characteristic of all the functions of the class $\mathcal{F}$. It means that the initial condition used in the generation of $\{x_i\}$ using $f(x)$ can be recovered from the last number of the sequence only if the relative position of every x_i with respect to x_c is known. Therefore, the recovery of the initial condition

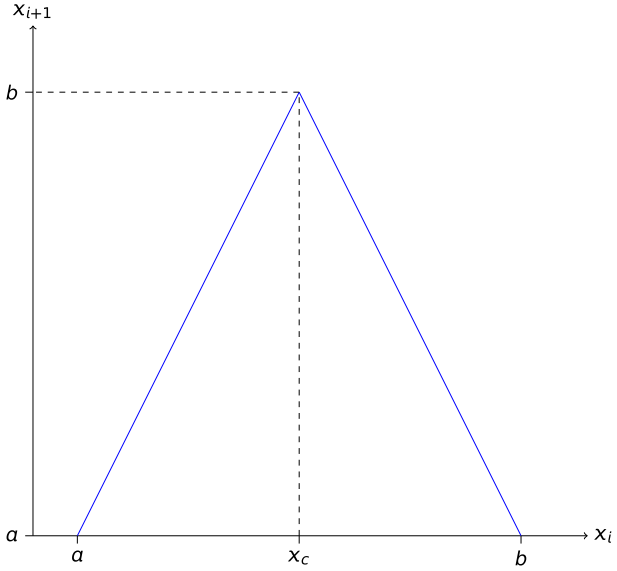

Fig. 1. Tent map.