Chaos, Solitons and Fractals 104 (2017) 477–484

Contents lists available at ScienceDirect

Chaos, Solitons and Fractals

Nonlinear Science, and Nonequilibrium and Complex Phenomena

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

Stochastic degradation of the fixed-point version of 2*D*-chaotic maps

L. De Micco [a,b,*], M. Antonelli [a], H.A. Larrondo [a,b]

[a] *ICYTE (Instituto de Investigaciones Científicas y Tecnológicas en Electrónica) Facultad de Ingeniería, Universidad Nacional de Mar del Plata, Juan B. Justo 4302, Mar del Plata, Buenos Aires, Argentina*

[b] *CONICET (Consejo Nacional de Investigaciones Científicas y Técnicas), Argentina*

ARTICLE INFO

Article history:
Received 20 April 2017
Revised 8 August 2017
Accepted 5 September 2017

Keywords:
2*D*-Quadratic map
Randomness quantifier
Finite precision
Chaotic map's degradation

ABSTRACT

This paper deals with a family of interesting 2*D*-quadratic maps proposed by Sprott, in his seminal paper [1], related to "chaotic art". Our main interest about these maps is their great potential for using them in digital electronic applications because they present multiple chaotic attractors depending on the selected point in the parameter's space. Only results for the analytical representation of these maps have been published in the open literature. Consequently, the objective of this paper is to extend the analysis to the digital version, to make possible the hardware implementation in a digital medium, like field programmable gate arrays (FPGA) in fixed-point arithmetic. Our main contributions are: (a) the study of the domains of attraction in fixed-point arithmetic, in terms of period lengths and statistical properties; (b) the determination of the *threshold* of the bus width that preserves the integrity of the domain of attraction and (c) the comparison between two quantifiers based on respective probability distribution functions (PDFs) and the well known maximum Lyapunov exponent (MLE) to detect the above mentioned threshold.

1. Introduction

Chaotic systems have an increasing number of applications and their implementation is specially involved due to the extreme sensitivity to initial conditions. In general, these systems are used for the generation of controlled noises, these digital pseudo-random noise generators (PRNGs) can be employed in a large number of electronic applications, such as encryption sequences for privacy, multiplexing techniques, electromagnetic compatibility [2–6]. In computers and digital devices only *pseudo chaotic* attractors can be generated. But discretization may destroy the *pseudo chaotic* behavior and consequently is a nontrivial process.

Several strategies have been proposed in the literature for a correct selection of the optimal number of bits in hardware implementations. However, most of these procedures are limited to linear systems [7,8]. In digital chaotic systems, a completely different behavior may be obtained by varying the precision. This issue has gained interest recently, and several new schemes have been proposed [9–11].

In short, in spite of the arithmetic used, i. e. fixed-point or floating-point arithmetic, the set of numbers that can be represented is limited. Even using extremely high precision as done by Liao and Wang [12] the generated sequences by a chaotic system using digital hardware will always be periodic.

Grebogi's et al. work [13] showed that the average length T of periodic orbits of a dynamical system implemented in a computer, scales as a function of the computer precision ξ and the correlation dimension of the chaotic attractor, as $T \sim \xi^{-D/2}$. In [14] some findings on a new series of dynamical indicators, which can quantitatively reflect the degradation effects on a digital chaotic map realized with a fixed-point finite precision, have been reported, but they are restricted to 1*D* piecewise linear chaotic maps (PWLCM). In [15] the effect of numerical precision on the mean distance and on the mean coalescence time between trajectories of deterministic maps with either multiplicative noise parameter or with an additive noise term was investigated. Nepomuceno and Mendes [16] studied the changes in the pseudo orbits of continuous chaotic systems when varying the time and discretization schemes.

Liao [17–19] proposed a numerical algorithm, namely the clean numerical simulation (CNS). He claimed that the CNS gives an extremely precise numerical approach for chaotic dynamic systems in a given finite interval. If the initial condition were exact, then the long-term prediction of chaos would be possible in theory, unfortunately, the required CPU time increases exponentially as the number of digits precision and Taylor expansion order increases

* Corresponding author at: ICYTE (Instituto de Investigaciones Científicas y Tecnológicas en Electrónica) Facultad de Ingeniería, Universidad Nacional de Mar del Plata, Juan B. Justo 4302, Mar del Plata, Buenos Aires, Argentina.

E-mail addresses: ldemicco@fi.mdp.edu.ar, lucianadm55@hotmail.com (L. De Micco).

http://dx.doi.org/10.1016/j.chaos.2017.09.007
0960-0779/

(for continuous systems), so that it is practically impossible to give true trajectories of chaos in a very long interval. Unlike our analysis, which is carried out on a map, we do not address the issue arising from the time discretization. What is more, in [19], lower precisions are despised because they are very far from the real trajectory. In contradistinction our approach comes from the hardware implementation point of view, where using minimum resources is mandatory, does not dismiss any precision. Instead, our goal is to investigate the characteristics for each precision so that the designer has a complete overview of the options to be used in its implementation. So that designers will be able to decide which properties to rescind according to the available resources and requirements.

One important thing to note is that besides analyzing the changes in the period lengths, the statistical properties of the sequences will be different from those of the real system and so they also should be analysed. In [20] an excellent work about the consequences finite precision has on the periodicity of a PRNG based on the logistic map was developed. There, the number, delay, and period of the orbits of the logistic map at varying degrees of precision were determined, however they lacked a statistical analysis. Our research complements their work by adding statistical quantifiers. What is more, they analysed the floating-point architecture of the map, while here we have chosen fixed-point architecture as it is the optimal architecture for hardware implementations. From an engineering point of view, fixed-point arithmetic is more efficient than floating-point, it consumes fewer resources and their operations require lower number of clock cycles. As a consequence, power consumption is also diminished.

Among many chaotic systems available in the literature, we are interested in a family of 2*D*-maps proposed by Sprott [1]. The main characteristic of this system is it presents multiple chaotic attractors depending on the selected point in the parameter's space, this feature is very attractive to be used in electronic applications. Only results for the analytical representation of the maps in [1] have been published in the open literature.

The objective of this paper is to extend the analysis to the digital version, to make possible the hardware implementation in fixed-point arithmetic. For which it is imperative to know both characteristics, period length and degree of randomness, of the sequences. We developed a detailed analysis of the *degradation* of the multiattractor chaotic system as a fixed-point implementation is used. By *degradation* we mean: (a) the appearance of stable fixed points and stable periodic orbits with short periods, inside a floating-point domain of attraction without stable orbits; (b) the attractor itself becomes periodic and its statistical characteristics change, making the system more deterministic.

The main contributions of this paper are:

- The analysis of the domains of attraction of the chaotic attractors for a given set of parameters as the number of bits increases; in terms of period lengths and the appearance of stable fixed points and periodic orbits with short periods are specially considered;
- The determination of the consequent *threshold width* for the bus, in order to make the statistical properties of the digital implementation close to those of the floating-point implementation;
- Two different probability distribution functions (PDF) are assigned to evaluate the stochasticity of the time series for different bus widths. Each PDF P is measured by the respective normalized Shannon entropy $H(P)$. These entropies have abrupt changes at specific bus widths. Period's lengths and *MLE* are also evaluated and results are compared with *H*s.

This work is organized as follows: Section 2 discusses the fundamental of the problem that concerns us, including a brief description of the chaotic system analyzed, and describes the employed quantifiers. Then, we give experimental results in Section 3. Finally, the conclusions are given in Section 4.

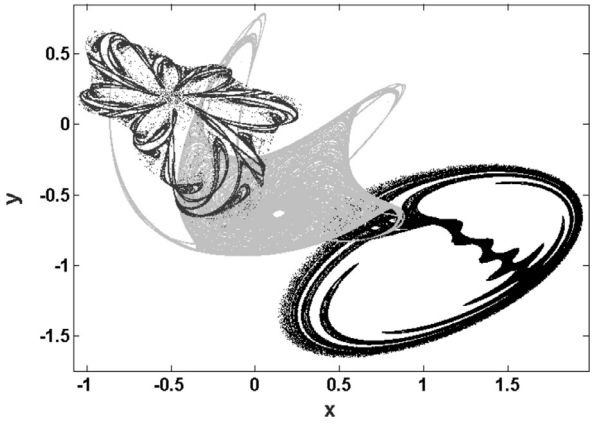


Fig. 1. Three attractors for three different sets of coefficients of 2*D*-quadratic map.

2. Preliminary concepts

When iterating chaotic maps in $\mathbb{R}^2$, after a transient that depends on the mixing parameter (r_{mix}), the generated sequence limits in a point or a collection of points called an attractor. A chaotic map can have one or more attractors. Attractor domain is called to all the initial conditions (ICs) that converge to each attractor. The ergodic sequences of the attractors, generated by the map, have a determined distribution called Invariant Probability Density Function (IPDF). Main characteristics of chaotic maps, IPDF and r_{mix}, can be obtained by calculating the Frobenius-Perron operator (FPO), which depends on the map's structure. The fixed points of its spectrum are the invariant densities and they correspond to the eigenvectors with eigenvalue equal to one, the mixing constant corresponds to the second largest eigenvalue of the FPO [21,22].

When using finite precision, this analysis is not valid, all attractors take the form of fixed points or periodic orbits. The FPO of the map no longer describes the sequences' characteristics. Regarding the attractor domain, it will also change when digitalized, each initial value will be part of, or will converge to, a certain fixed point or periodic orbit. Generally, many new periodic orbits appear, and change when the number of bits employed varies.

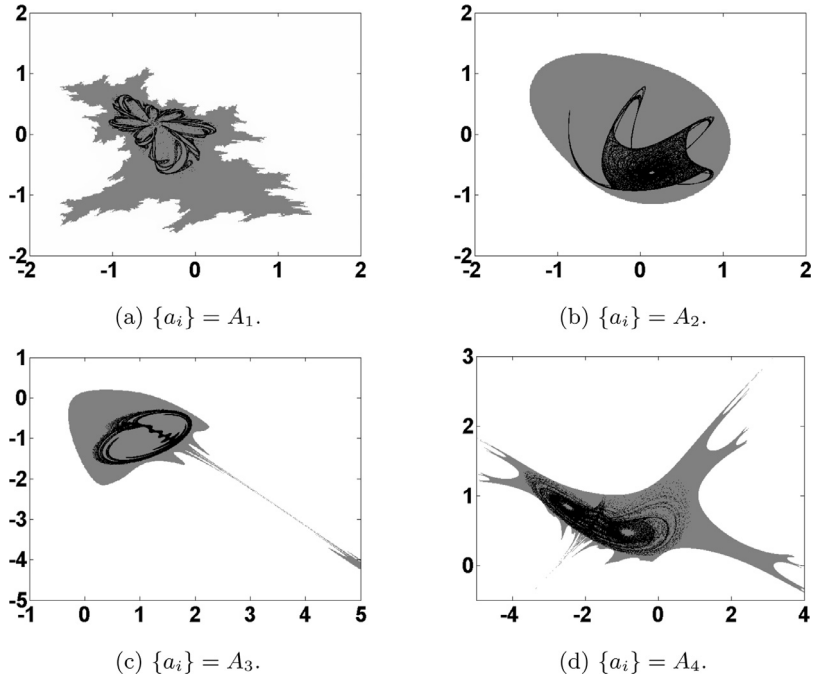
With the purpose of utilizing these systems in electronic applications it becomes necessary to understand how the attraction domain evolves with the variation of bits employed. It is mainly important to know which is the period's length and the *randomness degree* of the cycle at which each seed converges. For this reason, we have included randomness quantifiers that indirectly estimate a sort of r_{mix} and IPDF of the digitalized system.

In this paper we have emulated the behaviour of a digital hardware implementation, such as FPGA, Complex Programmable Logic Device (CLPD) or Application Specific Integrated Circuit (ASIC), to exactly replicate the operation of the device. Our interest is to measure how the domains of attraction degrade with a change in the number of bits n employed, as well as to find the threshold value $n_{\min}$.

2.1. Chaotic system under study

The family of 2*D*-quadratic maps studied here are modelled by a pair of coupled quadratic equations:

$$\begin{cases} x_{n+1} = a_1 + a_2 x_n + a_3 x_n^2 + a_4 x_n y_n + a_5 y_n + a_6 y_n^2 \\ y_{n+1} = a_7 + a_8 x_n + a_9 x_n^2 + a_{10} x_n y_n + a_{11} y_n + a_{12} y_n^2 \end{cases} \quad (1)$$



(a) $\{a_i\} = A_1$. (b) $\{a_i\} = A_2$.

(c) $\{a_i\} = A_3$. (d) $\{a_i\} = A_4$.

Fig. 2. Four chaotic attractors and their domains of attraction in floating-point arithmetics.

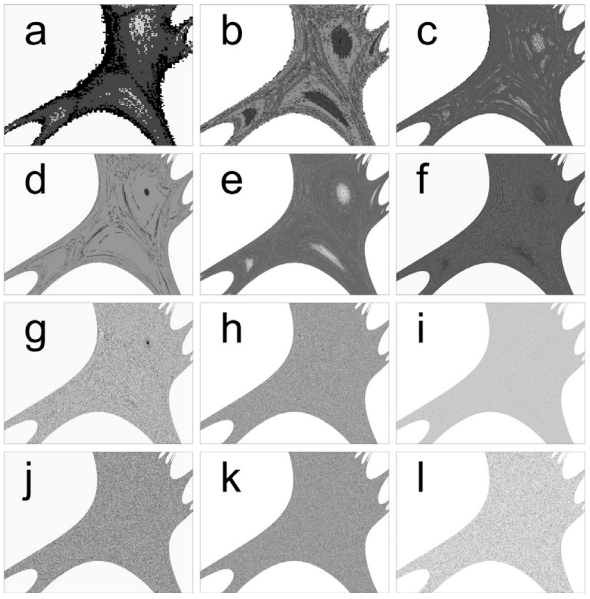


Fig. 3. Coexisting areas in attraction domains for: (a) $n_f = 5$, (b) $n_f = 6$, (c) $n_f = 7$, (d) $n_f = 8$, (e) $n_f = 9$, (f) $n_f = 10$, (g) $n_f = 11$, (h) $n_f = 12$, (i) $n_f = 13$, (j) $n_f = 14$, (k) $n_f = 17$, (l) $n_f = 18$.

where $\{x, y\}$ are the state variables and $\{a_i, i = 1, \ldots, 12\}$ are the parameters. The main characteristic of this system is it presents multiple chaotic attractors depending on the selected point in the parameter's space. The $12D$ parameters space generated by coefficients $A = \{a_1, \ldots, a_{12}\}$ is very hard to be explored.

The reasons to study this particular system are two-fold:

1. Using floating-point arithmetic Sprott saw that by automatic swept of parameters a_i a huge number of points in the parameter's space (about 6.10^{16}) having a chaotic permanent regime may be detected. He also found a correlation between the correlation dimension and the Lyapunov exponents of these chaotic attractors, with their *visual appeal*, an interesting issue for automatic *art* generation.

Table 1
Lengths of the periods within the attractor domain x and $y \in [-2, 2]$.

n_f	T (Percentage of ICs that converge to this period's length cycle)
5	2 (92.7%);6 (7.3%)
6	88 (41.6%);44 (36.7%);12 (13.8%);16 (6.2%);2 (0.8%);24 (0.6%);26 (0.2%)
7	12 (83.5%);14 (8.9%);24 (5.2%);34 (1.8%);2 (0.6%)
8	68 (91.7%);14 (6.2%);12 (1.8%);17 (0.2%);15 (0.1%)
9	140 (54.5%);123 (25.4%);34 (8.6%);44 (4.3%);38 (3.9%);22 (2.9%);48;2;12;4 (<0.1%)
10	655 (78.2%);212 (21.1%);143 (0.5%);12 (0.1%);2;36;13;20;10;4 (<0.1%)
11	153 (78.1%);461 (10.8%);1381 (8.7%);434 (2.3%);18;30;53;32;34;10;2 (<0.1%)
12	2,278 (64.4%);438 (22.4%);598 (7.6%);886 (4.7%);12 (0.7%);87;2;42;23;32;10 (<0.1%)
13	11,510 (98.9%);1052 (1%);12;26;2;10 (<0.1%)
14	21,333 (69.2%);5.804 (16.5%);4,795 (7.9%);1,264 (5.8%);2,429 (0.5%) 46;23;21;10;12;17 (<0.1%)
15	10,099 (58.6%);1.762 (19.4%);14,887 (18.3%);1,598 (3.4%);750;105;23;14;2;10 (<0.1%)
16	54,718 (87.5%);5,017 (4.7%); $> 10^5$ (3.7%);5,367 (2.5%);703 (0.9%) 1,159;1,802 (0.2%);377;75;10 (<0.1%)
17	37,812 (53.1%);38,456 (24.1%); $> 10^5$ (16.0%);34,749 (3.0%);3,362;718 (1.5%) 3,006,5,222 (0.1%);15 (<0.1%)
18	$> 10^5$ (87.4%);52,069 (12.5%);2,471 (0.1%);146;51 (<0.1%)
float	$> 10^5$ (100%)

2. It is possible to employ them in a wide variety of electronic applications, such as generate novel encryption systems either by replacing the S-box in AES [23,24], or even by developing new encryption algorithms [2,3].

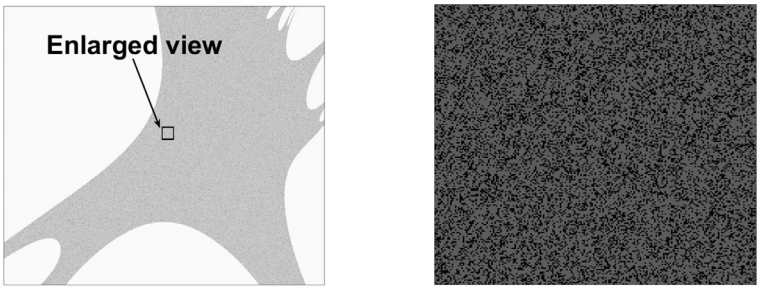
Three of these chaotic attractors are shown together in Fig. 1. Their parameters sets A_i are:

$A_1 = \{-0.7, -0.4, 0.5, -1.0, -0.9, -0.8, 0.5, 0.5, 0.3, 0.9, -0.1, -0.9\}$,

$A_2 = \{-0.6, -0.1, 1.1, 0.2, -0.8, 0.6, -0.7, 0.7, 0.7, 0.3, 0.6, 0.9\}$,

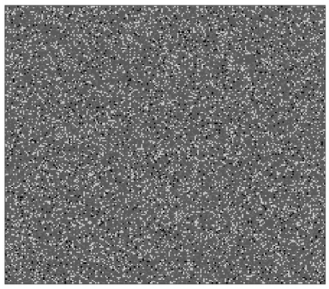
$A_3 = \{-0.1, 0.8, -0.7, -1.1, 1.1, -0.7, -0.4, 0.6, -0.6, -0.3, 1.2, 0.6\}$.

As it can be seen in the figure it is possible to get very different outputs just modifying the value of the parameters and maintaining the structure of the system. In an electronic implementation this would be equivalent to keeping the hardware structure and by

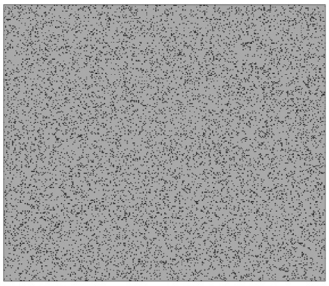


(a) Rectangular section of the attraction domain, section $[0.3 \pm 0.001, -0.2 \pm 0.001]$.

(b) $n_f = 14$.



(c) $n_f = 17$.



(d) $n_f = 18$.

Fig. 4. Enlarged views of sections of the attraction domains for higher values of n_f.

modifying the parameters through, for example, an input it would be possible to vary the output.

Fig. 2a–d show the same three attractors A_1 to A_3 of Fig. 1 and together with attractor $A_4 = \{-1, 0.9, 0.4, -0.2, -0.6, -0.5, 0.4, 0.7, 0.3, -0.5, 0.7, -0.8\}$, superimposed with their basins of attraction (in grey). The white areas of each figure correspond to those initial conditions generating divergent trajectories of the system (useless seeds regarding their use as PRNGs).

2.2. Analysis tools

The normalized Shannon entropy applied to two different PDFs and the maximum Lyapunov exponent along with the mean period's lengths are the quantifiers employed here to estimate the system's properties. The entropies help us to evaluate the two properties that determine the randomness degree, the equiprobability among all possible values and the statistical independence between consecutive values, while the MLE determines the presence of chaos[1].

2.2.1. Period lengths analysis

Using n bits to represent the state variables of a D-dimensional system the maximum theoretical period $T_{\max}$ that can be reached is $T_{\max} = 2^{D.n}$. Actually, the periods obtained are much lower than the maximum and are heavily dependent on the IC.

We have developed an algorithm that emulates the operation of the system in a digital environment. One task of this code is to analyze the reached period when starting iteration from each initial condition using different precisions in a fixed-point architecture. Each seed could converge to a limit cycle, or it could be one value of the limit cycle itself. This procedure was repeated for all the initial conditions to obtain the attraction domain scheme of the system.

[1] A positive MLE is a necessary condition for the presence of chaos.

2.2.2. Quantifiers of randomness

The new quantifiers proposed here bring us information about the degree of randomness, that is not available in "pass-nonpass" tests like those used as standard to evaluate random number generators.

Based on results of previous research [25–27] the normalized Shannon entropy was adopted as quantifier to characterize determinism and stochasticity of the generated sequences. This quantifier derives from the Information Theory, and it is a functional of the PDF. Once the PDF is determined the entropy is defined by the very well known normalized Shannon expression:

$$H = -\frac{\sum_{i=1}^{M} p_i \; log \; p_i}{log(M)}, \tag{2}$$

where M is the number of elements of the alphabet.

From a statistical point of view, a chaotic system is the *source* of a symbolic time series with an alphabet of M symbols. To evaluate entropy one needs first to define a probability distribution function of the time series. It should be noted that the classical probability distribution, here termed PDF based on histograms, takes only into account the ocurrence of values, but it is not able to detect the order of appearance of them. For example, a sequence of random values generated by any noise generator will exhibit a constant PDF between 0 and 1. On the other hand, a saw-tooth sequence will also present a constant PDF between 0 and 1. In both cases the values appear in the series the same number of times but in a different order. This characteristic is crucial because it differentiates a random signal from an entirely predictable one.

There exist different procedures to obtain a PDF [25,28–32] and the determination of the best PDF P is a fundamental problem because P and the sample space are inextricably linked. Their applicability depends on particular characteristics of the data, such as stationarity, time series length, variation of the parameters, level of noise contamination, etc. In previous work devoted to PRNGs, the use of two PDFs was successful for the comparison between different systems. One PDF is the normalized histogram, and its

Fig. 5. Period's lengths evolution of the attraction domains for: (a) $n_f = 5$, (b) $n_f = 6$, (c) $n_f = 7$, (d) $n_f = 8$, (e) $n_f = 9$, (f) $n_f = 10$, (g) $n_f = 11$, (h) $n_f = 12$, (i) $n_f = 13$, (j) $n_f = 14$, (k) $n_f = 17$, (l) $n_f = 18$.

normalized Shannon entropy is denoted here H_{hist}. The other one is the ordering PDF proposed by Bandt and Pompe [32] and its normalized Shannon entropy is here denoted as H_{BP}. By this selection of the PDFs it is possible to cover the two mentioned properties, namely, (1) the probability of occurrence of each element of the alphabet (PDF based on histograms), and (2) the order of the items in the time series (PDF based on Bandt-Pompe technique). One may consider the statistics of individual symbols or the statistics of sequences of d consecutive symbols. In the first case P is *non-causal* because it does not change if the outcomes are mixed up and the number of different possible outcomes is M. In the second case, the outcome changes if the output is mixed and then one says that P is *causal*. In the second case the number of different outcomes is equal to M^d and increases rapidly with d. Bandt and Pompe made a proposal in [32] that is computationally efficient, because it limits the outcomes to $d!$, but retains causal effects.

The representation plane H_{BP} vs H_{hist} is considered in [25]. A higher value in any of the entropies, H_{BP} and H_{hist}, implies an increase in the uniformity of the involved PDFs. The point (1, 1) represents the ideal point for a system with uniform histogram and uniform distribution of ordering patterns. A discussion about the convenience of using these quantifiers is beyond the scope of this paper but there is an extensive literature [25,33,34].

2.2.3. Maximum Lyapunov exponent

The Lyapunov exponents are quantifiers that characterize how the separation between two trajectories evolves [35]. It is well known that chaotic behaviors are characterized mainly by Lyapunov numbers of the dynamic systems. A chaotic behavior requires that one or more Lyapunov numbers to be greater than zero. Otherwise, the system is stable. In this paper, we employ the maximum Lyapunov number as it is one of the most useful indicators of chaos.

The distance between trajectories changes in 2^{MLE} for each iteration, on average. If $MLE<0$ the trajectories converge, this may be due to a fixed point, if $MLE = 0$ the trajectories keep their distance, this may be due to a limit cycle, if $MLE > 0$, the distance between trajectories diverges, and is an indicator of chaos [36].

In this case we have adopted a non-analytical way to measure it as here only the inputs and outputs of the system are accessible [35].

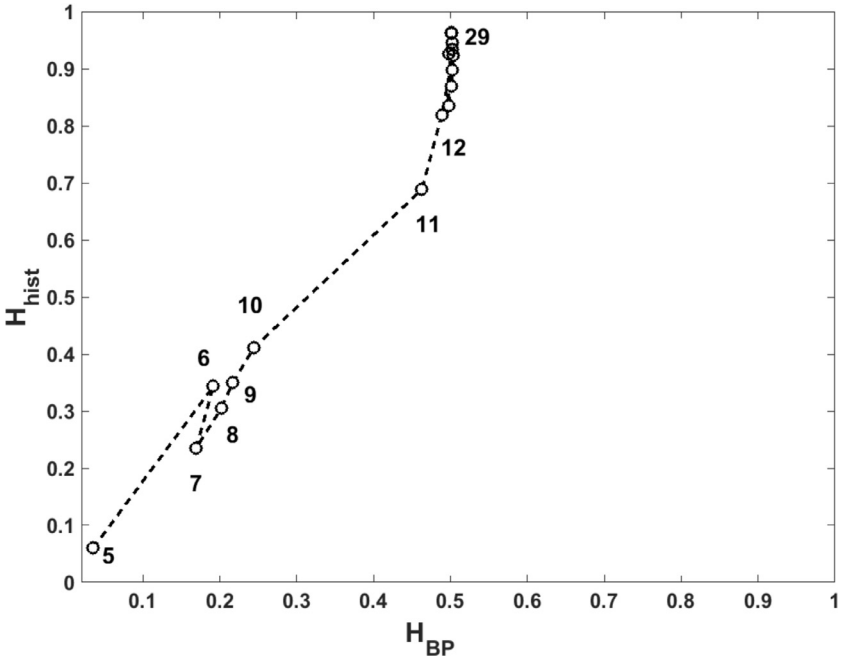
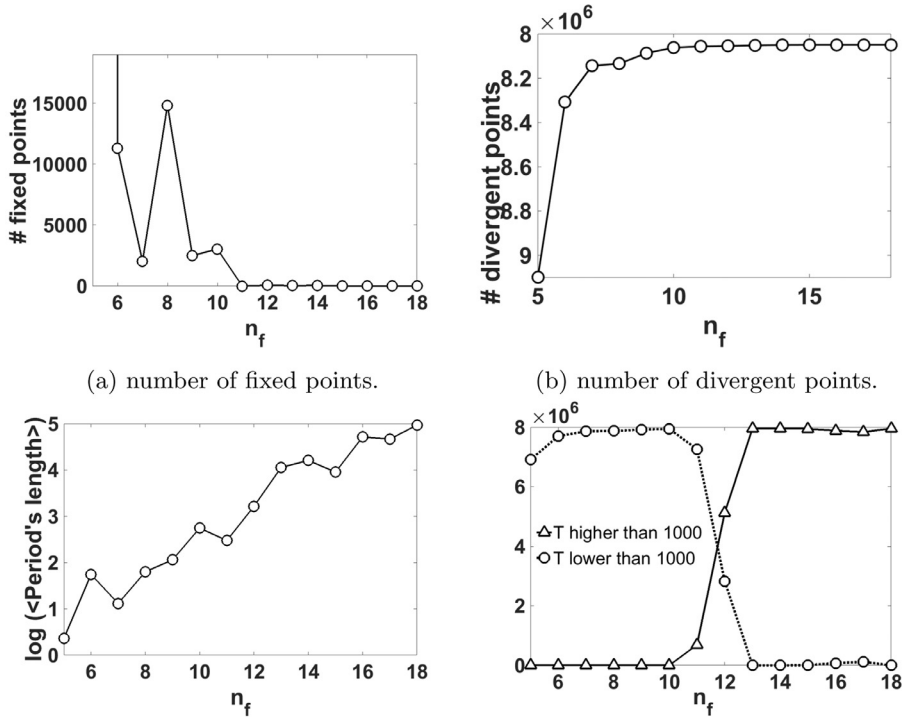


Fig. 6. Plane H_{hist} - H_{BP} for different number of bits.



(a) number of fixed points.

(b) number of divergent points.

(c) logarithm of the length's cycles weighted average.

(d) initial conditions with period length higher and lower than $1,000$.

Fig. 7. Summary of initial conditions' behavior.

3. Results

An ANCI C code that simulates iterating a nonlinear system, the quadratic map, in any digital electronic device was developed in order to generate sequences which were then analyzed.

It iterates the 2D-quadratic map 10^5 times, in this case coefficients a_0 to a_{11} have the values:

$\{a_i\} = \{-1.0, 0.9, 0.4, -0.2, -0.6, -0.5, 0.4, 0.7, 0.3, -0.5, 0.7, -0.8\}$. The system was intended to be working in fractional fixed-point architecture with n bits, where $n = n_i + n_f$, in two's complement representation (Ca_2). In this case we employed $n_i = 4$ bits for representing the integer part, and the code automatically varies the number of bits representing the fractional part of the number, n_f, in order to analyze how the system reacts when the precision changes. The code runs through all the ICs within the interval

$[-2, 2]$ in steps determined by the current n_f, so, the step_grid will be:

$$step\_grid = \frac{1}{n_f.2^{n_f}}. \quad (3)$$

On each case it was determined whether the systems evolves to a fixed point, diverges or goes towards a periodic cycle, also sequences for each cycle of that IC using n_f bits of precision were generated. These data were then evaluated using the randomness quantifiers previously introduced in Section 2.2.

Fig. 3 displays the obtained domains of attraction for $n_i = 4$ and some values of n_f. The abscissa and ordinate axis correspond to initial values of x and y respectively. Each point represents an IC and the colour is associated to its final state, the darker the tone of grey the shorter the cycle, fixed points are in black and divergent points in white. So, the different domain attractors (including the attractors) that coexist in the system can be seen here.

With the purpose of being able to distinguish the different coexisting areas, a diverse range of gray tones have been used on each figure. It must be taken into account that each figure has its own gray range, this means that, for example, an almost white area when $n_f = 5$ (Fig. 3a) corresponds to a period of 6, while a darker area in a figure with higher n_f may correspond to a period higher than a thousand (Fig. 3e). These figures allow reflecting the complex domains of attraction that appear when digitalizing.

It can be seen in Fig. 3 that the smaller the value of n_f the bigger the area of ICs that tends to diverge and to converge to fixed points. As n_f increases, the area of divergent and fixed points decreases. These figures along with Table 1 allows an easy interpretation of the system's behavior. In Table 1 the sequence lengths that appear in the attractor domain for every n_f are sorted by the more to the less numerous ICs that converges to that cycle. It can be seen the rate of occurrence. Indeed, figures with lower values of n_f present irregular, or rough surfaces, pointing out that different lengths cycles coexist there. For example, for $n_f = 5$ there is a prevalence of short periods cycles. In that case, there exist just two limit cycles, the lighter grey zone corresponds to the attraction domain of the limit cycles of length six, that is the less numerous cycle, according to Table 1, and, the darker zone corresponds to the attraction domain of length two cycle.

Although for $n_f \geq 13$ (Fig. 3i–l) the attractor domain appears to be smooth and uniform, however, if we enlarge a section of the figures (Fig. 4) it can be seen that there are still cycles with different periods that coexist in the attractor for $n_f = 14, 17$ and 18.

Nevertheless, when we want to make a general comparison of what happens to the periods when the precisions are varied a color scale is required, see Fig. 5. Fig. 5 shows that as the value of n_f increases the colour of the area becomes more smooth and clear, indicating that the ICs converge to higher periods cycles. This is the range of initial values that generate useful sequences increases for higher values of n_f.

This can also be seen in Table 1, where as n_f increases the predominant limit cycle's length increases. In order to compare the obtained values with the real sequences we have simulated in floating-point with 236−bit mantissa (IEEE 754 octuple-precision binary floating-point format) we call this here *floating-point* or just *float*, it is the arithmetic closest to real numbers. Then, using float precision all the limit cycles are higher than 10^5, they converge to the chaotic attractor seen in Fig. 2d.

In relation to the randomness quantifiers, we realized that the analysis performed up to this point was not enough to fully describe the changes in the dynamic of a digitalized chaotic system. To reach long periods does not ensure that the systems' exhibit good properties with respect to randomness. So we decided to further study the data obtained by employing statistical quantifiers.

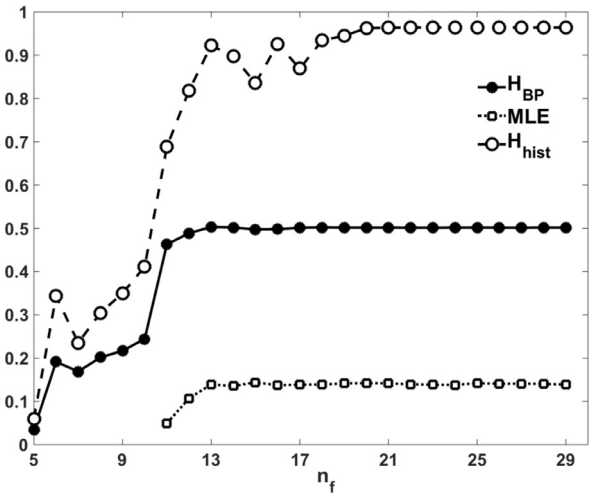


Fig. 8. Weighted average of quantifiers H_{BP}, H_{hist} and *MLE* as functions of the number of bits.

As said, in Fig. 3a the two gray zones correspond to the initial conditions that converge to the two coexisting cycles of period two and six respectively. Then this two cycles will have a determined value of H_{hist} and H_{BP}, $H_{hist}\,|_{T=2} = 0.0625$, $H_{hist}\,|_{T=6} = 0.1199$, $H_{BP}\,|_{T=2} = 0.1053$ and $H_{BP}\,|_{T=6} = 0.2723$. However, the reported value of these quantifiers can not be the average of both, since the rate of occurrence of cycle two is much greater than that of cycle six (period two appears 92.7% times while period six only 7.3%, see Table 1). Therefore, we have calculated the averaged quantifiers by weighting each quantifier by its rate of occurrence.

The H_{hist} vs H_{BP} plane, shown in Fig. 6, allows a quick visualization of the behavior in terms of randomness of the system, in this plane the "ideal" point, from the statistical point of view, is (1, 1). Here, the system seems to stabilize for n_f higher than 12. It can be seen that while the H_{hist} stabilizes close to the maximum value ($H_{hist} = 1$), the H_{BP} tends to stabilizes to 0.5. This value of H_{BP} is characteristic of chaotic systems and is due to the inner structures of their attractors.

A summary of the observed analysis of these outputs can be seen in Fig. 7.

Fig. 7a and b show the number of points that diverge and converge to fixed points respectively as the value of n_f increases, in both cases, the final value tends to the floating-point case. It is clear from these figures that for $n_f \sim 12$ the system seems to have stabilized. Fig. 7c shows that the averaged period of cycles increases at a logarithmic rate. Finally, Fig. 7d shows the number of initial conditions that present periods T higher and lower than 1,000. Again, a value of 12 for n_f seems to be the limit to obtain a good approximation of the system.

Fig. 8 shows the weighted average of quantifiers H_{hist}, H_{BP} and *MLE*. In the figure it can be seen that the three quantifiers tend to the value calculated using floating-point arithmetic. While H_{BP} and *MLE* stabilize for $n_f \sim 12$ or 13, H_{hist} reaches the floating-point value for $n_f \sim 19$, showing that there are properties of the output sequences that only this quantifier can detect. This confirms the need to use both quantifiers to characterize the randomness of the sequences.

As can be seen from the above analysis, the minimum number of bits is determined by H_{hist} quantifier and results to be $n_f = 19$ plus the number of bits used to represent the integer part $n_i = 4$, therefore $n_{\min}$ turns out to be equal to 23.

4. Conclusion

In this work, we have developed a detailed analysis of the changes in behaviour of a 2*D*-quadratic map fixed-point implementation. Our goal is to report the rate of degradation for each systems' property, so as to be used by authors at the time of designing their particular applications. Results show that it is possible to determine a threshold for the number of bits employed in the fixed point representation of the system, whereas the domain of attraction preserves its integrity and the characteristics of the generated sequences are kept. With the help of the quantifiers of randomness introduced it was possible to determine that limit, in the case of study it was 23 bits. The same procedure should be repeated for any other system if it is desired to be used in a digital electronic application, such as controlled noise generators or to develop novel encryption systems. In the particular case of Sprott's chaotic system, if the minimum number of 23 bits is satisfied at the time of digitalizing, we conclude that it is possible to successfully use it as a component of new encryption algorithms.

Acknowledgements

This work was partially supported by the Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), Argentina (PIP 112-201101-00840), ANPCyT (PICT-2013-2066), UNMDP and the International Centre for Theoretical Physics (ICTP) Associateship Scheme.

References

[1] Sprott JC. Automatic generation of strange attractors. Comput Graph 1993;17(3):325–32. http://dx.doi.org/10.1016/0097-8493(93)90082-K.
[2] Machado RF, Baptista MS, Grebogi C. Cryptography with chaos at the physical level. Chaos Solitons Fract 2004;21(5):1265–9.
[3] Smaoui N, Kanso A. Cryptography with chaos and shadowing. Chaos Solitons Fract 2009;42(4):2312–21.
[4] De Micco L, Petrocelli RA, Larrondo HA. Constant envelope wideband signals using arbitrary chaotic maps. In: Proceedings of XII RPIC; 2007.
[5] De Micco L, Petrocelli RA, Carrica DO, Larrondo HA. Muestreo caótico para la adquisición de señales de baja frecuencia con ruido de alta frecuencia. In: Proceedings de la XII Reunión de Trabajo en Procesamiento de la Información y Control; 2007.
[6] De Micco L, Arizmendi CM, Larrondo HA. Zipping characterization of chaotic sequences used in spread spectrum communication systems. In: Institute of physics conference proceedings 913; 2007. p. 139–44.
[7] Constantinides G, Cheung P, Luk W. Optimum wordlength allocation. In: Field-programmable custom computing machines, 2002. Proceedings. 10th Annual IEEE symposium on; 2002. p. 219–28. doi:10.1109/FPGA.2002.1106676.
[8] Constantinides GA, Cheung PYK, Luk W. Wordlength optimization for linear digital signal processing. IEEE Trans Comput Aided Des Integr Circuits Syst 2003;22:1432–42.
[9] Ding Q, Pang J, Fang J, Peng X. Designing of chaotic system output sequence circuit based on FPGA and its applications in network encryption card. Int J Innov Comput Inf Control 2007;3:1–6.
[10] Asseri MA, Sobhy MI, Lee P. Lorenz chaotic model using field programmable gate array. The 2002 45th midwest symposium on circuits and systems, 2002 MWSCAS-2002, 1; 2002.
[11] Azzaz M, Tanougast C, Sadoudi S, Bouridane A, Dandache A. FPGA implementation of new real-time image encryption based switching chaotic systems. In: Signals and systems conference (ISSC 2009); 2009. p. 1–6.
[12] Liao S, Wang P. On the mathematically reliable long-term simulation of chaotic solutions of Lorenz equation in the interval [0, 10000]. Sci China Phys Mech Astro 2014;57(2):330–5.
[13] Grebogi C, Ott E, Yorke JA. Roundoff-induced periodicity and the correlation dimension of chaotic attractors. Phys Rev A 1988;38:3688–92. doi:10.1103/PhysRevA.38.3688.
[14] LI S, Chen G, Mou X. On the dynamical degradation of digital piecewise linear chaotic maps. Int J Bifur Chaos 2005;15.
[15] Dias SP, Longa L, Curado E. Influence of the finite precision on the simulations of discrete dynamical systems. Commun Nonlinear Sci Numer Simul 2011;16:1574–9. doi:10.1016/j.cnsns.2010.07.003.
[16] Nepomuceno EG, Mendes EM. On the analysis of pseudo-orbits of continuous chaotic nonlinear systems simulated using discretization schemes in a digital computer. Chaos Solitons Fract 2017;95:21–32.
[17] Liao S. On the numerical simulation of propagation of micro-level inherent uncertainty for chaotic dynamic systems. Chaos Solitons Fract 2013;47:1–12.
[18] Liao S. Chaos: a bridge from microscopic uncertainty to macroscopic randomness. Commun Nonlinear Sci Numer Simul 2012;17(6):2564–9.
[19] Liao S. On the reliability of computed chaotic solutions of non-linear differential equations. Tellus A 2009;61(4):550–64.
[20] Persohn K, Povinelli RJ. Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation. Chaos Solitons Fract 2012;45(3):238–45.
[21] Lasota A, Mackey MC. Chaos, fractals, and noise: stochastic aspects of dynamics.. Applied mathematical sciences 97. second ed. Springer Verlag; 1994.
[22] Lasota A, Yorke JA. On the existence of invariant measure for piecewise monotonic transformations. Trans Amer Math Soc 1973;186:481–8.
[23] Ahmad M, Chugh H, Goel A, Singla P. A chaos based method for efficient cryptographic s-box design. Berlin, Heidelberg: Springer; 2013. p. 130–7. ISBN 978-3-642-40576-1.
[24] Hussain I, Shah T, Gondal MA, Mahmood H. Efficient method for designing chaotic s-boxes based on generalized baker's map and tderc chaotic sequence. Nonlinear Dyn 2013;74(1):271–5. doi:10.1007/s11071-013-0963-z.
[25] De Micco L, González CM, Larrondo HA, Martin MT, Plastino A, Rosso OA. Randomizing nonlinear maps via symbolic dynamics. Physica A 2008;387:3373–83.
[26] Antonelli M, De Micco L, Larrondo H. Measuring the jitter of ring oscillators by means of information theory quantifiers. Commun Nonlinear Sci Numer Simul 2016.
[27] De Micco L, Fernández JG, Larrondo HA, Plastino A, Rosso OA. Sampling period, statistical complexity, and chaotic attractors. Physica A 2012;391(8):25642575.
[28] Rosso OA, De Micco L, Larrondo HA, Martin MT, Plastino A. Generalized statistical complexity measure: a new tool for dynamical systems. Int J Bifur Chaos 2010;20(3):775785.
[29] Mischaikow K, Mrozek M, Reiss J, Szymczak A. Construction of symbolic dynamics from experimental time series. Phys Rev Lett 1999;82:1114–47.
[30] Powell GE, Percival IC. A spectral entropy method for distinguishing regular and irregular motion of Hamiltonian systems. J Phys A 1979;12:2053–71.
[31] Rosso OA, Blanco S, Jordanova J, Kolev V, Figliola A, Schürmann M, et al. Wavelet entropy: a new tool for analysis of short duration brain electrical signals. J Neurosci Methods 2001;105:65–75.
[32] Bandt C, Pompe B. Permutation entropy: a natural complexity measure for time series. Phys Rev Lett 2002;88. 174102–1.
[33] Rosso OA, Larrondo HA, Martin MT, Plastino A, Fuentes MA. Distinguishing noise from chaos. Phys Rev Lett 2007;99:154102–6.
[34] Martín MT, Plastino A. Generalized statistical complexity measures: geometrical and analytical properties. Physica A 2006;369:439–62.
[35] Sprott J. Chaos and time-Series analysis. Oxford University Press; 2003.
[36] Strotgartz S. Nonlinear dynamics and chaos. Perseus Books; 1994. ISBN 0-201-54344-3.