Analysis of a Digital Non Linear System Implementation

L. De Micco, M. Antonelli and H. A. Larrondo
Departamentos de Física y de Ingeniería Electrónica
Facultad de Ingeniería, Universidad Nacional de Mar del Plata
Juan B. Justo 4302, Mar del Plata, Argentina and CONICET Email: ldemicco@fi.mdp.edu.ar

***Abstract*—This paper introduces an analysis of a fixed point implementation of a multiatractor chaotic system. The aim of the analysis is to find a threshold bus width where the system keep the desired properties that the real one has. These properties depend on each particular application, but here we determine a range of behavior. The Shannon Entropy (H), applied to two different Probability Density Functions (PDFs), and the Maximum Lyapunov Exponent (MLE) are the quantifiers employed here. These quantifiers result to reflect the changes in period lengths of the system output on a wide range of initial conditions (CIs).**

I. Introduction

Digital implementation in hardware of systems forces the usage of finite number of bits to represent the state variables' values.

Floating point architecture allows to recreate the system's trajectories close to the real (ideal) ones.

However, from the engineering point of view the usage of floating point arithmetic is not efficient when compared to fixed point operations because the first ones consume lot of system resources and require several clock cycles.

If the system to be implemented is known, i.e. the maximal values of its variables and the precision required are pre-established, fixed point arithmetic would allow to get better results in terms of velocity, usage resources and power consumption.

In general, for linear systems the digitalization process is not a defining issue since, roughly, linear systems remain almost their behavior. Therefore, discretized values can be modelled with a small noise called *quantization noise*.

In nonlinear systems the necessary amount of bits for representing the integer and fractional part of each value is critical. This is because of the high sensitivity of the systems that provokes to totally change their dynamics. The integer part is easily determined by the maximum value that the system could reach, and its optimum value can be rapidly found by a fast analysis. On the other hand, the number of bits needed for representing the fractional part is determined by the required accuracy.

In this systems by varying the precision used, completely different behaviors are obtained, from unstable systems to converging to fixed points, and within a range, a good approximation to the real system.

Several strategies can be used for selecting the optimal amount of bits for hardware implementations. However, the methods proposed in the literature are limited to linear systems [1], [2].

Recently, hardware implementation of chaotic oscillators has gained interest and several new schemes have been proposed [3], [**?**], [4].

In the literature, there does not seem to be much work on quantitative analysis of the degradation due to digitalization of chaos and how to reduce its negative influence on chaos-based digital systems. Grebogi's work [5] showed that the average length of periodic orbits (T) of a dynamical system scales as a function of computer precision (e) and the correlation dimension (d) of the chaotic attractor: $T \sim e^{-d/2}$. In [**?**] 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. They are restricted to $1D$ piecewise linear chaotic maps (PWLCM).

In this work we developed a detailed analysis of a fixed point implementation of a multiatractor chaotic system. The aim of the analysis is to find a threshold bus width where the system keep the desired properties that the real one has.

Of course these properties depend on each particular application, but here we determine a range of behaviour. The Maximum Lyapunov Exponent and the Normalized Shannon Entropy are the quantifiers employed here, they are applied to two different PDFs. This quantifiers result to reflect the changes in period lengths of the system output on a wide range of initial conditions.

The work is organized as follows: in section II an analysis of the allowed initial conditions of the system is performed. Section II-A gives a brief description of the chaotic system analyzed, and a detailed explanation of how the digitalization is performed.

Section III theoretical background of the quantifiers employed here.

Section IV describes our proposed method in detail. We give experimental result in Section V.

Finally, the conclusions and future work are given in section VI.

II. Attraction domain analysis

Generally, the usefulness of the nonlinear systems implementations are the “random” generated sequences to be employed as controlled noises generators (PRNGs), encryption

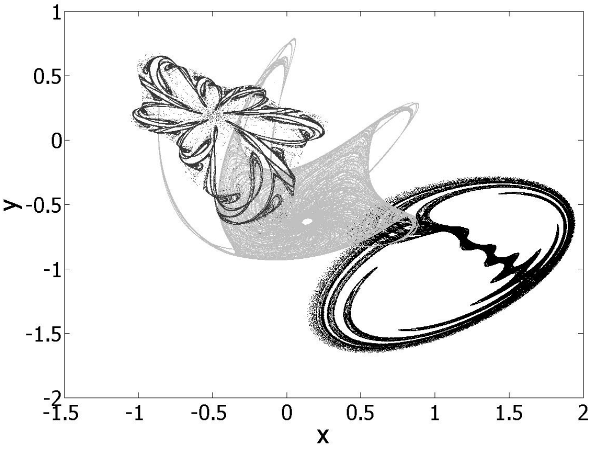

Fig. 1. Three attractors for three different values of the coefficients a_n.

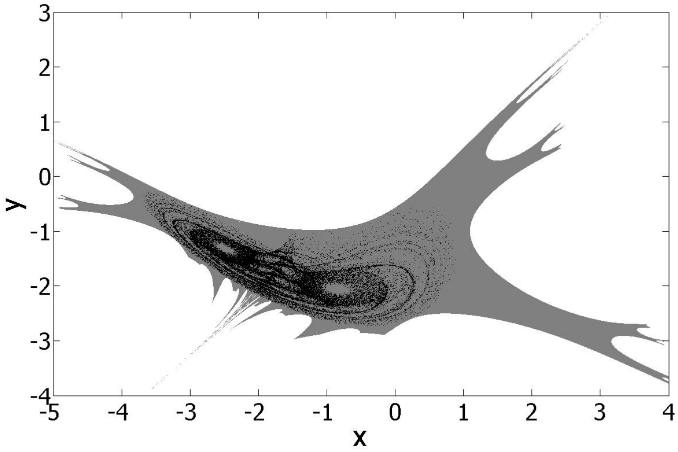

Fig. 2. Atraction Domain and attractor of the system analyzed.

sequences for privacy, multiplexing techniques, and so on. For this reason, unpredictable long periods are desired.

In this way, it is necessary to know the seeds, i. e. initial conditions, that generate random-like outputs of the system and also the degree of “randomness”.

In the universe of all the possible initial conditions, some converge to attractors (this group is called the attractor domain) and the remaining points diverge, go to infinity.

An attractor is a point or a collection of points on which the system limits. When using finite precision these take the form of fixed points and periodic orbits.

If the precision employed is adequate, attractors of really long periods can be reached. Moreover the “randomness” degree of the sequences must be taken into account, to this aim we have employed some quantifiers (section III).

A. Chaotic System analyzed

With the purpose of showing the method of analysis it has been chosen a family of bi-dimensional quadratic maps which structure consists of a pair of coupled quadratic difference equations (eq. 1) to be analyzed. Its 12 coefficients correspond to the parameters of the chaotic system. The main characteristic of this system is that each set of parameters a_n, produces a different evolution of it. This is called *multiattractor*, and means that the chaotic behavior of the system changes with the parameters values. Fig. 1 shows three different attractors that correspond to three different sets of parameters.

$$\begin{aligned} x_{(i+1)} &= a_0 + a_1 x_{(i)} + a_2 x^2_{(i)} + a_3 x_{(i)} y_{(i)} + a_4 y^2_{(i)} + a_5 y_{(i)} \\ y_{(i+1)} &= a_6 + a_7 x_{(i)} + a_8 x^2_{(i)} + a_9 x_{(i)} y_{(i)} + a_{10} y^2_{(i)} + a_{11} y_{(i)} \end{aligned} \tag{1}$$

The system behavior in real arithmetic has been widely studied, however real variables are not possible to implement in hardware, so finite precision operations should be employed.

The utilization of finite number of bits limits the quantity of available symbols used to represent the state variables. Therefore, finite arithmetic implies that the implemented system will always have a finite repetition period, and it will be determined when all the state variables, in this case x and y, repeat their values. Accordingly, the maximum theoretical period that can be reached is determined by the quantity of bits of all the state variables, and is: $2^{(\sharp state\_variables * n_{bits})}$, where n_{bits} is the bus width and $\sharp state\_variables$ is the quantity of states variables of the system.

For example if we use 10 bits for the numeric representation ($n_{bits} = 10$), the maximum theoretical period would be $2^{(2*10)} = 1048576$. Actually, the periods obtained are in general lower than the theoretical one and they depend on the initial condition of the sequence.

In Fig. 2 the attraction domain scheme of the system for parameters: $a_n = -1, 0.9, 0.4, -0.2, -0.6, -0.5, 0.4, 0.7, 0.3, -0.5, 0.7, -0.8$ can be seen. Axes x and y are the values of the initial conditions. In chaotic systems all initial conditions within the basin of attraction look the same after many iterations. The grey colored area are the points of all the initial conditions that, after a transient, converge to the attractor, which has been highlighted in black color.

B. Analysis of sequences’ periods

As mentioned above, digitalization changes the statistical properties of the implemented systems. Because of this fact, it is necessary to check that the system still satisfies the application’s requirements.

We have systematically studied the behavior of the system’s output using different precisions in a fixed point architecture, emulating a FPGA implementation. This was done for various initial conditions in order to obtain the attraction domain scheme of the system. Our interest is to understand how the attraction domain evolves with the variation of the bits employed in the precision, and also to find a threshold value above which the chaotic behavior of the system appears.

To this aim we have employed different quantifiers, the Normalized Shannon Entropy applied to two different probability density functions, and the Maximum Lyapunov Exponent that determines the presence of chaos.

III. Quantifiers

In the present work we compare the results of employing various precision using two type of quantifier that have demonstrated to accurately differentiate between various systems. One comes from the Information Theory, the Shannon Entropy, that after a proper evaluation of PDF is made by recourse to one of the two distinct approaches in coordinate space, namely, *(i)* the Bandt-Pompe technique, and *(iii)* PDF based on histograms; The Maximum Lyapunov Exponent characterizes how fast two trajectories drift apart, if this rate is exponential the system is said to be chaotic, because of this it is known as a detector of "chaoticity", [6], [7], [8].

A. Shannon Entropy

Any discrete alphabet time series has two important properties: (1) the list of elements of the alphabet and the probability of each element, and (2) the order of the elements inside the time series (mixing). Each property my be characterized by means of probability distribution functions $P = \{p_j, j = 1, \cdots, N\}$ and their corresponding entropies. To evaluate (1) it is possible to use the normalized histogram of the time series as a PDF. Once the PDF is known the entropy is defined by the very well known Shannon expression:

$$S[P] \; = \; -\sum_{j=1}^{N} p_j \; \ln(p_j),$$
$$H[P] = \mathrm{S}[P] \; / \; \mathrm{S}[P_e]. \tag{2}$$

With P_e being the uniform distribution and N the number of possible states of the system under study.

1) PDF based on Band and Pompe methodology: To use the Bandt and Pompe [**?**] methodology for evaluating of probability distribution P associated to the time series (dynamical system) under study one starts by considering partitions of the pertinent D-dimensional space that will hopefully "reveal" relevant details of the ordinal-structure of a given one-dimensional time series $\{x_t : t = 1, \cdots, M\}$ with embedding dimension $D > 1$. We are interested in "ordinal patterns" of order D [**?**], [**?**] generated by

$$(s) \; \mapsto \; \Big(x_{s-(D-1)}, \; x_{s-(D-2)}, \; \cdots, \; x_{s-1}, \; x_s \Big) \;, \tag{3}$$

which assign to each time s the D-dimensional vector of values at times $s, s-1, \cdots, s-(D-1)$. Clearly, the greater the $D-$value, the more information on the past is incorporated into our vectors. By the "ordinal pattern" related to the time (s) we mean the permutation $\pi = (r_0, r_1, \cdots, r_{D-1})$ of $(0, 1, \cdots, D-1)$ defined by

$$x_{s-r_{D-1}} \; \le \; x_{s-r_{D-2}} \; \le \; \cdots \; \le \; x_{s-r_1} \; \le \; x_{s-r_0} \; . \tag{4}$$

In order to get a unique result we set $r_i < r_{i-1}$ if $x_{s-r_i} = x_{s-r_{i-1}}$. Thus, for all the $D!$ possible permutations π of order D, the probability distribution $P = \{p(\pi)\}$ is defined by

$$p(\pi) \; = \; \frac{\sharp\{s | s \le M-D+1; \; (s), \; \texttt{has type } \pi\}}{M-D+1} \; . \tag{5}$$

In this expression, the symbol $\sharp$ stands for "number".

The Bandt-Pompe's methodology is not restricted to time series representative of low dimensional dynamical systems but can be applied to any type of time series (regular, chaotic, noisy, or reality based), with a very weak stationary assumption (for $k = D$, the probability for $x_t < x_{t+k}$ should not depend on t [**?**]). One also assumes that enough data are available for a correct attractor-reconstruction. Of course, the embedding dimension D plays an important role in the evaluation of the appropriate probability distribution because D determines the number of accessible states $D!$. Also, it conditions the minimum acceptable length $M \gg D!$ of the time series that one needs in order to work with a reliable statistics.

2) PDF based on histograms: In order to extract a PDF via amplitude-statistics, divide first the interval $[0, 1]$ into a finite number $nbin$ of non overlapping subintervals A_i: $[0, 1] = \bigcup_{i=1}^{nbin} A_i$ and $A_i \bigcap A_j = \emptyset \; \forall i \neq j$. One then employs the usual histogram-method, based on counting the relative frequencies of the time series values within each subinterval. It should be clear that the resulting PDF lacks any information regarding temporal evolution. The only pieces of information we have here are the x_i-values that allow one to assign inclusion within a given bin, ignoring just where they are located (this is, the subindex i.)

B. Maximum Lyapunov Exponent

The Lyapunov exponents are quantifiers that characterize how the separation between two trajectories evolves, [8]. It is generally well known that chaotic behaviors are characterized mainly by Lyapunov numbers of the dynamic systems. If one or more Lyapunov numbers are greater than zero, then the system behaves chaotically, 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 approaches, 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 is growing, and is an indicator of chaos. [8]

There is a non-analytical way to measure it if only the inputs and outputs of the system are accessible. The procedure is the following: The system must be started from two neighbor points in the phase plane, lets call them (x_a, y_a) and (x_b, y_b), as the system is iterated the Euclidean distance between the two trajectories is measured (d_n in the n_{th} sample) (eq. 6), and the b trajectory is relocalized on each iteration (eq. 8), obtaining the points (x_{br}, y_{br}) to feed the system. Then the Lyapunov exponent can be calculated as shown in eq. (7). The process can be seen in Fig. **??**.

$$\begin{aligned} d_{0(i-1)} &= \sqrt{(x_{a(i-1)} - x_{br(i-1)})^2 + (y_{a(i-1)} - y_{br(i-1)})^2} \\ d_{1(i)} &= \sqrt{(x_{a(i)} - x_{b(i)})^2 + (y_{a(i)} - y_{b(i)})^2} \end{aligned} \tag{6}$$

$$MLE \;\; = \;\; \frac{1}{M} \sum_{i=2}^{M} \log_2 \frac{d_{1(i)}}{d_{0(i-1)}} \tag{7}$$

$$\begin{aligned} x_{br(i)} &= x_{a(i)} + (x_{b(i)} - x_{a(i)}) d_{o(i-1)} / d_{1(i)} \\ y_{br(i)} &= y_{a(i)} + (y_{b(i)} - y_{a(i)}) d_{o(i-1)} / d_{1(i)} \end{aligned} \tag{8}$$

IV. Hardware Digital simulation.

A *C* code that simulates a nonlinear system was developed. In this case the quadratic map was reproduced as it would be implemented in a digital hardware dispositive, for example a FPGA implementation. The Code employs signed integer arithmetic and it is equivalent to employ fixed point precision.

The system is intended to be working in decimal fixed point architecture. It employs 4 bits for representing the integer part in Ca_2 convention ($m = 4$) and it automatically scans the number of bits to represent the fractional part of the number (n), in order to analyze how the system reacts when the precision changes.

For example in Table I there is the equivalence when using $n_{bits} = 6$, 4 bits for the integer part and 2 bits for the decimal part in Ca_2 convention ($m = 4$ and $n = 2$).

Internally the FPGA works with binary numbers, designers must interpret the bits based on the desired architecture. In order to use the parameterizable operations provided by the FPGA's libraries, that work with Signed Integer variables, an equivalence between Decimal

TABLE I
TABLE OF EQUIVALENCES.

Binary	Decimal Fixed point	Signed Integer
$0111,11$	$7,75$	31
$0111,10$	$7,5$	30
$0111,01$	$7,25$	29
...	...	...
$0000,00$	0	0
$1111,11$	$-0,25$	-1
$1111,10$	$-0,5$	-2
...	...	...
$1000,00$	-8	-32

fixed point numbers and Signed Integers can be done as shown in Table I.

The same binary number can be interpreted as an integer number or, as in this case, if one wish to employ decimal numbers, interpret a decimal point located at a desired position. This means:

$$number = -2^{(m-1)}...2^{0},2^{-1}2^{-n} \tag{9}$$

where $n\_bits = m + n$.

In order to make this conversion, each decimal number must be multiplied by 2^n to obtain the equivalent Signed Integer number. Where n is the quantity of bits used to represent the decimal part of the number. This is equivalent to right-shift n positions the decimal point.

$$number = -2^{(m-1+n)}...2^{0} \tag{10}$$

where $n\_bits = m + n$.

The following considerations must be taken into account when operating with this equivalence:

- Addition, this operation does not need any consideration just to make sure not to exceed the limits of the arithmetic used.
- Multiplication, the result of this operation must be divided by 2^n to adjust the result to the correct range.
- Division, the result must be always rounded towards minus infinity: 7.28 to 7 , -14.9 to -15.

The developed code iterates the Quadratic map (eq. 1) with the following coefficients: $a_0 = -1.0$, $a_1 = 0.9$, $a_2 = 0.4$, $a_3 = -0.2$, $a_4 = -0.6$, $a_5 = -0.5$, $a_6 = 0.4$, $a_7 = 0.7$, $a_8 = 0.3$, $a_9 = -0.5$, $a_{10} = 0.7$ and $a_{11} = -0.8$.

Hence, the operations are done using signed integer variables that are equivalent to decimal fixed point numbers, as it has been explained in the previous section.

After each operation the corresponding adjustment is performed to work exactly as the FPGA does.

The map has been iterated with initial conditions x_0 and y_0 from -2 to 2 in steps of 0.001, that means 16008001 different points. On each case it was determined whether the systems evolves to a fixed point, diverges or goes towards a periodic cycle. It was also reported the repetition period of these cycles.

For every value of precision n we obtained a 4001x4001 matrix whose elements correspond to each initial condition. This means, the program outputs on each position the final state of the system for that initial condition.

There are some desirable properties that constitutes a "good" PRNG, some of the most important ones are large period, few fixed points and, of course, that do not diverge.

V. RESULTS

Figures 3 to 9 display some of the results (i.e. for some values of n) obtained, these are the set of final states for each initial condition.

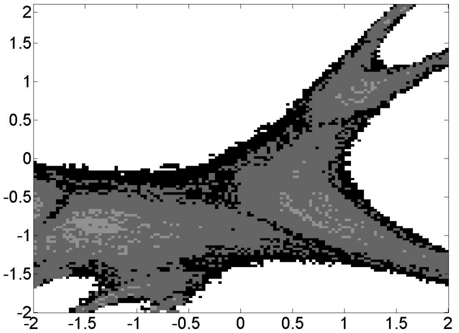

Fig. 3. Domains of attraction $n = 5$

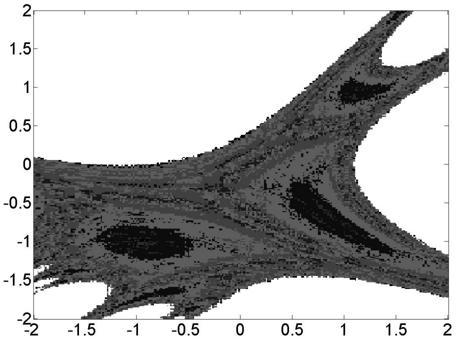

Fig. 4. Domains of attraction $n = 6$

With final state we mean: fixed point, divergent point or the value of the period when the CI converges to a cycle.

The abscissa and ordinate axis correspond to initial values of x and y respectively. They have been swept from -2 to 2 in steps of 0.001.

It can be seen that for small values of n the zone presents bigger areas of divergent and fixed points. As the value of n increases, it can be seen that the area of divergent points tends to the one of the floating point (Fig. 2).

Lower values of n present rough surfaces, with predominant dark colors indicating that there is a prevalence of short periods cycles. As the value of n increases the area smoothes and the color tends to be lighter, indicating that the CIs converge to higher periods cycles. This means that the range of initial values that generate useful sequences increases for higher values of n.

Also, it is interesting to note that the edges of the attraction domain is irregular for small values of n, and it defines as n increases.

An analysis of these outputs can be seen in Figures 10 to 12.

Fig. 11 and 10 show the quantity of points that diverge and converge to fixed points respectively as the value of n increases, in both cases the final value tends to the floating point case. It is clear from these figures that for $n \sim 12$ the system seems to behave sufficiently accurate to the real one. However Figure 12 shows that a value of 12 for n the system still have a quite short maximum period.

Figure 13 shows the quantity of initial conditions that presents periods T higher and lower than 1000. Again, a value of 12 for n seems to be the limit to obtain a good approximation of system.

We realized that the analysis performed up to this point was not enough to determine a conclusion, so we decided to further analysis the data obtained by employing some statistical quantifiers the Entropy applied to the $hist$ and $BandandPompe$ distributions.

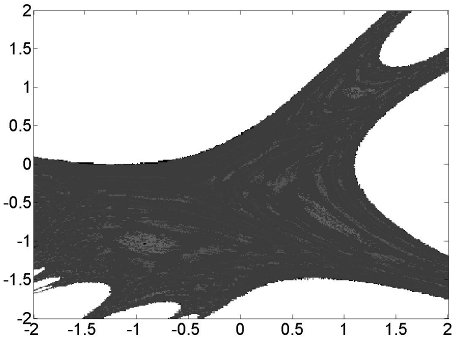

Fig. 5. Domains of attraction $n = 7$

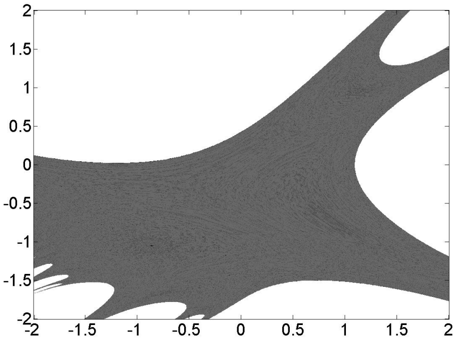

Fig. 6. Domains of attraction $n = 10$

Figure 14 shows the values of the quantifier normalized Shannon entropy applied over two PDFs, the histogram (H_{hist}) and Bandt-Pompe distribution (H_{BP}). In the figure it can be seen that the two quantifiers tend to the value calculated using floating-point arithmetic. While H_{BP} is concordant with the previous analysis and shows that it stabilizes for $n \sim 12$, H_{hist} reaches the theoretical value for $n \sim 19$, showing that there are properties of the output sequences that only this quantifier can detect.

In Table V the value of MLE for some values of n. The cases for $n = 11, 12, 13$ and 25 are showed. Also, the theoretical value calculated with Matlab using floating point arithmetic. It can be seen that as the value of m increases the MLE tends to the theoretical

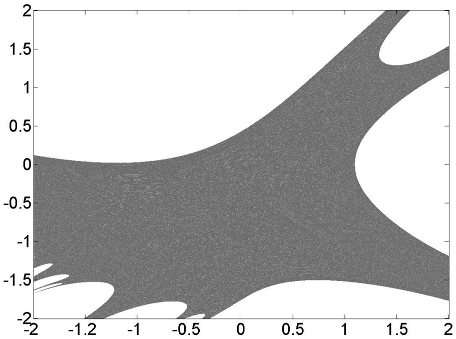

Fig. 7. Domains of attraction $n = 11$

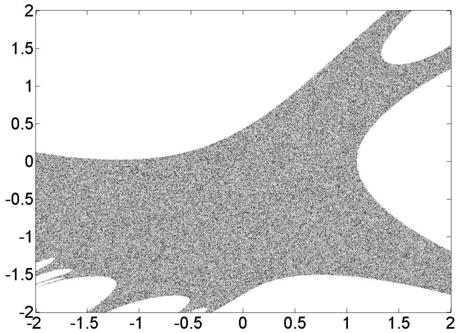

Fig. 8. Domains of attraction $n = 14$

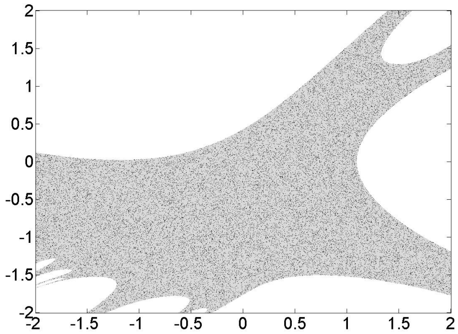

Fig. 9. Domains of attraction $n = 16$

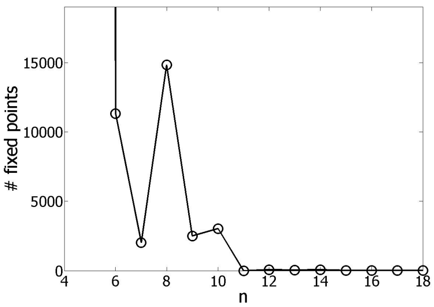

Fig. 10. Quantity of fixed points.

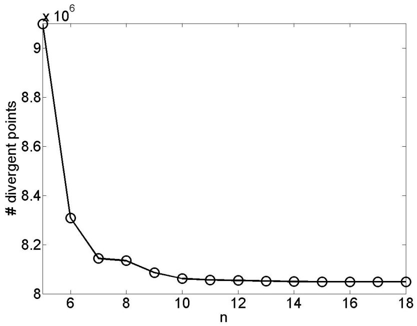

Fig. 11. Quantity of divergent points.

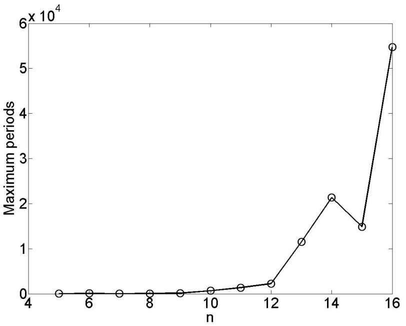

Fig. 12. Maximum periods reached.

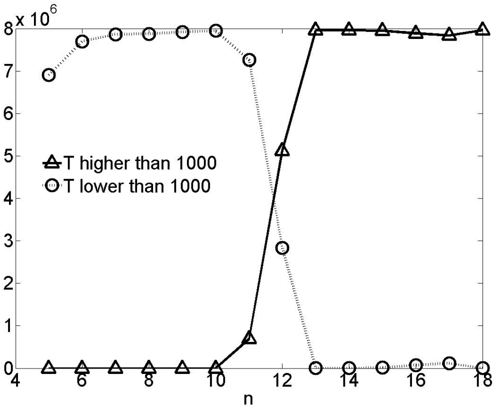

Fig. 13. Quantity of initial conditions with period (T) higher and lower than 1000.

value. Figure V displays MLE vs. n, there again the quantifier reaches the theoretical value at $n \sim 13$.

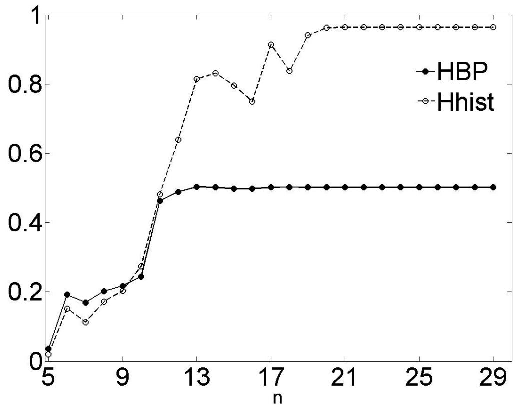

Fig. 14. Quantifiers H_{BP} and H_{hist}.

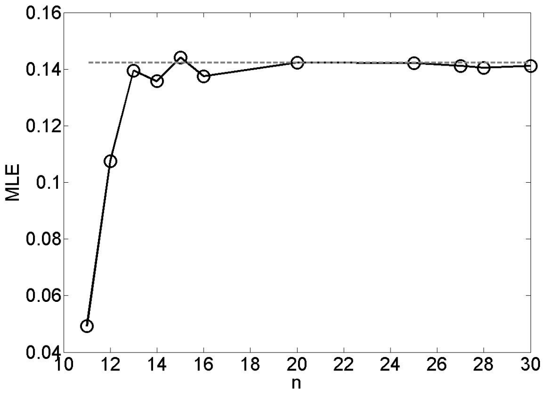

Fig. 15. MLE for different quantity of decimal bits n.

n	MLE
11	0.049214459144086
12	0.107498218078192
13	0.139472468153184
14	0.135756935006498
15	0.144155039896011
16	0.137514471652835
25	0.142134613438658
27	0.141180317168284
float	0.142275657734227

VI. Conclusion

The results show that, compared to floating-point, fixed-point arithmetic executed on an integer datapath has a limited impact on the accuracy.

Acknowledgment

This work was partially financed by CONICET (PIP2008), and UNMDP.

References

[1] G.A. Constantinides, P.Y.K. Cheung, and W. Luk. Optimum wordlength allocation. In *Field-Programmable Custom Computing Machines, 2002. Proceedings. 10th Annual IEEE Symposium on*, pages 219–228, 2002.

[2] George A. Constantinides, Peter Y. K. Cheung, and Wayne Luk. Wordlength optimization for linear digital signal processing. *IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems*, 22:1432–1442, 2003.

[3] Qun Ding, Jing Pang, Jinqing Fang, and Xiyuan Peng. Designing of chaotic system output sequence circuit based on fpga and its applications in network encryption card. *International Journal of Innovative Computing, Information and Control*, 3:1 – 6, 2007.

[4] M.S. Azzaz, C. Tanougast, S. Sadoudi, A. Bouridane, and A. Dandache. Fpga implementation of new real-time image encryption based switching chaotic systems. *Signals and Systems Conference (ISSC 2009)*, pages 1 – 6, 2009.

[5] Celso Grebogi, Edward Ott, and James A. Yorke. Roundoff-induced periodicity and the correlation dimension of chaotic attractors. *Phys. Rev. A*, 38:3688–3692, Oct 1988.

[6] S Strotgartz. *Nonlinear Dynamics and Chaos*. Perseus Books, 1994.

[7] A. Kantz. A robust method to estimate the maximal lyapunov exponent of a time series. *Phys. Lett. A*, 185(77), 1994.

[8] J Sprott. *Chaos and Time-Series Analysis*. Oxford University Press, 2003.