Chaotic Sampling, Very Weakly Coupling, and Chaotic Mixing: Three Simple Synergistic Mechanisms to Make New Families of Chaotic Pseudo Random Number Generators

René Lozi

ENOC 2008, Saint Petersburg, Russia, June, 30-July, 4 2008

CHAOTIC SAMPLING, VERY WEAKLY COUPLING, AND CHAOTING MIXING: THREE SIMPLE SYNERGISTIC MECHANISMS TO MAKE NEW FAMILIES OF CHAOTIC PSEUDO RANDOM NUMBER GENERATORS

René Lozi

Laboratoire J.A. Dieudonné – UMR du CNRS N° 6621, University of Nice-Sophia-Antipolis, Parc Valrose, 06108 Nice Cedex 02, France

and

Institut Universitaire de Formation des Maîtres Célestin Freinet-académie de Nice, University of Nice-Sophia-Antipolis, 89 avenue George V, 06046 Nice Cedex 1, France

rlozi@unice.fr

Abstract

We introduce and combine synergistically three simple new mechanisms: very weakly coupling of chaotic maps, chaotic sampling and chaotic mixing of iterated points in order to make new families of enhanced Chaotic Pseudo Random Number Generators (CPRNG).

The key feature of these CPRNG is that they use chaotic numbers themselves in order to sample and to mix chaotically several subsequences of chaotic numbers.

We analyze numerically the properties of these new families and underline their very high qualities and usefulness as CPRNG when series are computed up to 10^{13} iterations.

Key words

Chaos, pseudo random numbers, coupled maps.

1. Introduction

When a dynamical system is realized on a computer using floating point or double precision numbers, the computation is of a discretization, where finite machine arithmetic replaces continuum state space. For chaotic dynamical systems, the discretization often has collapsing effects to a fixed point or to short cycles [Lanford III, 1998; Gora, Boyarsky, Islam and Bahsoun, 2006].

In order to preserve the chaotic properties of the continuous models in numerical experiments we have introduced as a first one mechanism the very weak multidimensional coupling of p one-dimensional dynamical systems which is noteworthy [Lozi, 2006].

Moreover each component of these numbers belonging to $\mathbb{R}^p$ are equally distributed over a given finite interval $\mathbf{J} \subset \mathbb{R}$. Numerical computations show that this distribution is obtained with a very good approximation. They have also the property that the length of the periods of the numerically observed orbits is very large.

However chaotic numbers are not pseudo-random numbers because the plot of the couples of iterated points (x_n, x_{n+1}) in the phase plane shows up the map f used as one-dimensional dynamical systems to generate them.

A second simple mechanism is then used to hide the graph of this genuine function f in the phase space $\left(x_n^l, x_{n+1}^l\right)$. The pivotal idea of this mechanism is to sample chaotically the sequence $\left(x_0^l, x_1^l, x_2^l, \ldots, x_n^l, x_{n+1}^l, \ldots\right)$ selecting x_n^l every time the value of x_n^m is strictly greater than a threshold $T \in \mathbf{J}$, with $l \neq m$, for $1 \leq l, m \leq p$.

A third mechanism can improve the unpredictability of the chaotic sequence generated as above, using synergistically all the components of the vector X, instead of two. This simple third mechanism is based on the chaotic mixing of the *p-1* sequences $\left(x_0^1, x_1^1, x_2^1, \ldots, x_n^1, x_{n+1}^1, \ldots\right)$, $\left(x_0^2, x_1^2, x_2^2, \ldots, x_n^2, x_{n+1}^2, \ldots\right), \ldots,$ $\left(x_0^{p-1}, x_1^{p-1}, x_2^{p-1}, \ldots, x_n^{p-1}, x_{n+1}^{p-1}, \ldots\right)$ using the last one $\left(x_0^p, x_1^p, x_2^p, \ldots, x_n^p, x_{n+1}^p, \ldots\right)$ with respect to a given partition $\mathbf{r_1}, \mathbf{r_2}, \ldots, \mathbf{r_{p-1}}$ of $\mathbf{J}$, to distribute the iterated points.

$$X = \begin{pmatrix} x^1 \\ \vdots \\ x^p \end{pmatrix}$$

In this paper we explore numerically the properties of these new families and underline their very high qualities and usefulness as CPRNG when series are computed up to 10^{13} iterations.

Generation of random or pseudorandom numbers, nowadays, is a key feature of industrial mathematics. Pseudorandom or chaotic numbers are used in many areas of contemporary technology such as modern communication systems and engineering applications. Everything we do to achieve privacy and security in the computer age depends on random numbers. More and more European or US patents using discrete mappings for this purpose are obtained by researchers of discrete dynamical systems [Petersen and Sorensen, 2007; Ruggiero, Mascolo, Pedaci and Amato, 2006].

The idea of construction of chaotic pseudorandom number generators (CPRNG) applying discrete chaotic dynamical systems,

intrinsically, exploits the property of extreme sensitivity of trajectories to small changes of initial conditions, since the generated bits are associated with trajectories in an appropriate way [Bofetta, Cencini, Falcioni and Vulpiani, 2002].

Recently some authors proposed the use of the Arnol'd cat maps as a PNRG [Barash and Schchur, 2006].

The process of chaotic sampling and mixing of chaotic sequences, which is pivotal for these new families, works perfectly in numerical simulation when floating point (or double precision) numbers are handled by a computer.

It is noteworthy that the new models of very weakly coupled maps are more powerful than the usual formulas used to generate chaotic sequences mainly because only additions and multiplications are used in the computation process; no division being required. Moreover the computations are done using floating point or double precision numbers, allowing the use of the powerful Floating Point Unit (FPU) of the modern microprocessors (built by both Intel and Advanced Micro devices (AMD)). In addition, a large part of the computations can be parallelized taking advantage of the multicore microprocessors.

2. Very Weakly Multi-dimensional Coupling

2.1. Two-dimensional Coupled Symmetric Tent Map

First, we recall the basic equation of the coupled symmetric tent maps. In sections 2, 3 and 4 of this paper, we will consider only the symmetric tent map defined by

$$f_a(x) = 1 - a|x| \qquad (2.1)$$

with the value $a = 2$, later denoted simply as f, even though others map of the interval (as the logistic map) can be used for the same purpose. The associated dynamical system [Sprott, 2003; Alligood, Sauer and Yorke, 1996] is defined by the equation on the interval $\mathbf{J} = [-1, 1]$

$$x_{n+1} = 1 - a|x_n| \qquad (2.2)$$

Two tent maps are coupled in the following way, using a two dimensional coupling constant $\varepsilon = (\varepsilon_1, \varepsilon_2)$

$$\begin{cases} x_{n+1} = (1-\varepsilon_1) f(x_n) + \varepsilon_1 f(y_n) \\ y_{n+1} = \varepsilon_2 f(x_n) + (1-\varepsilon_2) f(y_n) \end{cases} \qquad (2.3)$$

In this paper for the numerical studies we fix constant the ratio between ε_1 and ε_2. We chose to set it equal to 2.

$$\varepsilon_2 = 2\varepsilon_1 \qquad (2.4)$$

However, different ratios can also lead to good results and be used since a multidimensional variable can be instrumental in the increasing of the number of dimensions of the systems.

The coupling constant ε varies from (0, 0) to (1, 1). When ε = (0, 0) the maps are decoupled, when ε = (1, 1) they are fully cross coupled. Generally, researchers do not consider very small values of ε (as small as 10^{-7} for floating point numbers or 10^{-14} for double precision numbers), because it seems that the maps are quasi decoupled with those values. Hence no special effect of the coupling is expected. In fact it is not the case and this very very small coupling constant allows the construction of very long periodic orbits, leading to sterling chaotic generators.

The dynamical system (2.3) can be described more generally by

$$X_{n+1} = F(X_n) = A \cdot \left(\underline{f}(X_n)\right) \qquad (2.5)$$

with

$$X = \begin{pmatrix} x \\ y \end{pmatrix}, \quad \underline{f}(X) = \begin{pmatrix} f(x) \\ f(y) \end{pmatrix} \qquad (2.6)$$

and

$$A = \begin{pmatrix} (1-\varepsilon_1) & \varepsilon_1 \\ \varepsilon_2 & (1-\varepsilon_2) \end{pmatrix} \qquad (2.7)$$

where F is a map of the square [-1, 1] x [-1, 1] = $\mathbf{J}^2$ into itself.

2.2 p-coupled Symmetric Tent Map

To improve the length of the period and the convergence of the invariant measure towards a given measure, we consider the dynamical system (2.5) in which p maps are coupled

with $$X = \begin{pmatrix} x^1 \\ \vdots \\ x^p \end{pmatrix}, \qquad \underline{f}(X) = \begin{pmatrix} f(x^1) \\ \vdots \\ f(x^p) \end{pmatrix} \qquad (2.8)$$

and

$$A = \begin{pmatrix} 1-(p-1)\varepsilon_1 & \varepsilon_1 & \cdots & \varepsilon_1 & \varepsilon_1 \\ \varepsilon_2 & 1-(p-1)\varepsilon_2 & \cdots & \varepsilon_2 & \varepsilon_2 \\ \vdots & \ddots & & \vdots & \vdots \\ \vdots & & \ddots & \vdots & \vdots \\ \varepsilon_p & \cdots & \cdots & \varepsilon_p & 1-(p-1)\varepsilon_p \end{pmatrix} \qquad (2.9)$$

with $\varepsilon_i = i\,\varepsilon_1 \qquad i = 2, \ldots, p \qquad (2.10)$

As stated earlier, others choices are possible. In this case, F is a map of $\mathbf{J}^p$ into itself.

2.3 Uniform distribution of chaotic numbers

We give some numerical results about chaotic numbers produced by 2-, 3- and 4-coupled maps which show that they are equally distributed over the interval $\mathbf{J}$. In order to compute numerically an

approximation of the invariant measure [3] also called the probability distribution function $P_{\mathbf{N}}(x)$ linked to the one dimensional map f we consider a regular partition of M small intervals (boxes) of $\mathbf{J}=\bigcup_{0}^{M-2} r_i$

$$r_i = [s_i\ ,\ s_{i+1}[\ \ ,\ i = 0, M-2 \qquad (2.11)$$

$$r_{M-1} = [s_{M-1}\ ,\ 1] \qquad (2.12)$$

$$s_i = \ -1+\frac{2i}{M} \qquad i = 0, M \qquad (2.13)$$

Its length is

$$s_{i+1} - s_i = \ \frac{2}{M} \qquad (2.14)$$

All iterates $f^{(n)}(x)$ belonging to these boxes are collected (after a transient regime of q iterations decided *a priori*, i.e. the first q iterates are neglected). Once the computation of $N+q$ iterates is completed, the relative number of iterates with respect to N/M in each box r_i represents the value $P_{\mathbf{N}}(s_i)$. The approximated $P_{\mathbf{N}}(x)$ defined in this article is then a step function, with M steps. As M may vary, we define

$$P_{M,N}(s_i) = \frac{1}{2}\frac{M}{N}(\#r_i) \qquad (2.15)$$

where $\#r_i$ is the number of iterates belonging to the interval r_i and the constant 1/2 allows the normalisation of $P_{M,N}(x)$ on the interval **J**.

$$P_{M,N}(x) = P_{M,N}(s_i) \quad \forall x \in r_i \qquad (2.16)$$

In the case of coupled maps, we are interested by the distribution of each component $x^1,\ \ldots,\ x^p$ of X rather than the distribution of the variable X itself in $\mathbf{J}^{\mathbf{p}}$. We then consider the approximated probability distribution function $P_{\mathbf{N}}(x^j)$ associated to one among several components of $F(X)$ defined by (2.5) which are one-dimensional maps.

The discrepancies $\boldsymbol{E_1}$ (in norm L_1) and $\boldsymbol{E_2}$ (in norm L_2) between $P_{N_{disc},N_{iter}}(x)$ and the Lebesgue measure which is the invariant measure associated to the symmetric tent map, are defined by

$$E_1(N_{disc},N_{iter}) = \left\| P_{N_{disc},N_{iter}}(x) - 0.5 \right\|_{L_1} \qquad (2.17)$$

$$E_2(N_{disc},N_{iter}) = \left\| P_{N_{disc},N_{iter}}(x) - 0.5 \right\|_{L_2} \qquad (2.18)$$

Fig. 1 shows the error $E_1(N_{disc},N_{iter})$ versus the number of iterates of the approximated distribution functions with respect to the first variable x^1 for 2, 3 and 4-coupled symmetric tent map. $\boldsymbol{N}_{\text{disc}}$ is fixed to 10^4, ε_1 to 10^{-14}, $\boldsymbol{N}_{\text{iter}}$ varies from 10^5 to 10^{11} for the 2-coupled case and to 3.10^{12} for the 3 and 4-coupled one.

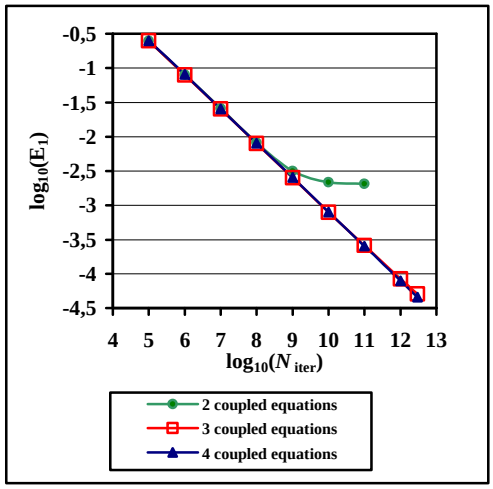

Figure 1. Error $\boldsymbol{E_1}$ for 2, 3 and 4-coupled Symmetric Tent Maps. Computations done using double precision numbers (~14-15 digits), $\varepsilon_i = i.\varepsilon_1$, $\varepsilon_1 = 10^{-14}$, $\boldsymbol{N}_{\text{disc}} = 10^4$. Initial values $x_0^1 = 0.330000013113$, $x_0^2 = 0.338756413113$, $x_0^3 = 0.331353442113$, $x_0^4 = 0.333213583113$.

Same results are obtained in norm L_2.
The corresponding numerical results are displayed in Tab. 1 for $E_1(N_{disc},N_{iter})$ for and Tab. 2 for $(E_2(N_{disc},N_{iter}))^2$.

Remark: in order to made easier the comparison of the results, we display the square of the discrepancy E_2^2 instead of $\boldsymbol{E_2}$ itself, the discrepancy being divided by 10 each time the number of iterations is multiplied by 10.

One can observe that for 3 and 4-coupled equations the convergence is excellent up to 3×10^{12} iterates. For 2-coupled equations the convergence seems lower bounded by a minimal error.

$\boldsymbol{N}_{\text{iter}}$	$E_1(N_{disc},N_{iter})$ **2-coupled equation**	$E_1(N_{disc},N_{iter})$ **3-coupled equation**	$E_1(N_{disc},N_{iter})$ **4-coupled equation**
10^5	**0.25071335**	**0.25035328**	**0.2499133**
10^6	**0.079655103**	**0.079437105**	**0.080739109**
10^7	**0.025794703**	**0.025343302**	**0.025266304**
10^8	**0.0081966502**	**0.0079505501**	**0.0080771501**
10^9	**0.003147609**	**0.002513533**	**0.002562893**
10^{10}	**0.002171746**	**0.0007908719**	**0.00079702**
10^{11}	**0.002055097**	**0.000257910**	**0.000252414**
10^{12}		**$8.4195287.10^{-5}$**	**$7.8803383.10^{-5}$**
3.10^{12}		**$5.0625114.10^{-5}$**	**$4.5317128.10^{-5}$**

Table 1. Error $\boldsymbol{E_1}$ for 2, 3 and 4-coupled Symmetric Tent Maps.

N_{iter}	$E_2^2(N_{disc}, N_{iter})$ **2-coupled equation**	$E_2^2(N_{disc}, N_{iter})$ **3-coupled equation**	$E_2^2(N_{disc}, N_{iter})$ **4-coupled equation**
10^5	0.100199	0.099820996	0.099610992
10^6	0.01006199	0.0098781898	0.01022057
10^7	0.0010442081	0.0010014581	0.0010055967
10^8	0.0001055816	$9.8853067.10^{-5}$	0.00010197872
10^9	$1.567597.10^{-5}$	$1.0047459.10^{-5}$	$1.0326474.10^{-5}$
10^{10}	$7.3577797.10^{-6}$	$9.7251536.10^{-7}$	$9.9932242.10^{-7}$
10^{11}	$6.6338453.10^{-6}$	$1.0434293.10^{-7}$	$1.0070523.10^{-7}$
10^{12}		$1.116009.10^{-8}$	$9.6166733.10^{-9}$
3.10^{12}		$4.0443118.10^{-9}$	$3.2530773.10^{-9}$

Table 2. Error E_2^2 for 2, 3 and 4-coupled Symmetric Tent Maps.

There is no significant difference between 3 and 4-coupled equations, the numerical experiments have to be pursued up to 10^{13} or 10^{14} in order to discriminate the results.

Equivalent results are obtained for the variables x^2, x^3 or x^4.

No periodic solutions are observed up to 3×10^{12} iterates (even up to 10^{13} iterates as tested in Sec. 4). This is a key point when producing chaotic numbers, because the use of a computer discretizes the phase space of a dynamical system, canceling (at least) its asymptotic properties. Every orbit is periodic according to the finite number of states (i.e., the number of double precision numbers belonging to $\mathbf{J}^p$). However, if the period of the realized sequence is long enough, these properties reasonably survive as a chaotic transient.

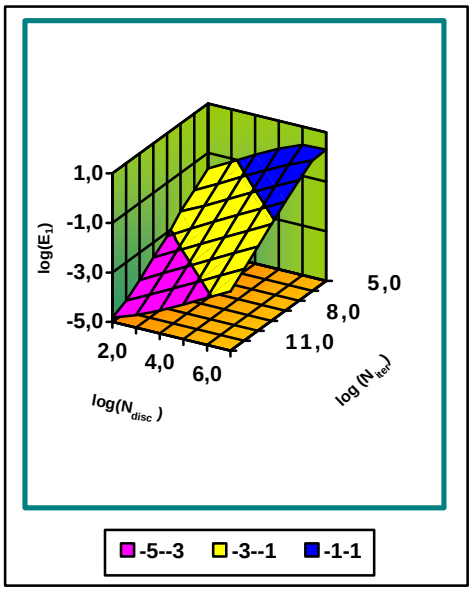

Figure 2. Error $\boldsymbol{E_1}$ for 3-coupled Symmetric Tent Maps. Computations done using double precision numbers (~14-15 digits) with respect to both $\boldsymbol{N}_{\text{iter}}$ and $\boldsymbol{N}_{\text{disc}}$, $\varepsilon_i = i.\varepsilon_1$, $\varepsilon_1 = 10^{-14}$, $\boldsymbol{N}_{\text{iter}} = 10^5$ to 10^{12}, $\boldsymbol{N}_{\text{disc}} = 10^2$ to 10^7. Initial values $x_0^1 = 0.330000013113$, $x_0^2 = 0.338756413113$, $x_0^3 = 0.331353442113$, $x_0^4 = 0.333213583113$.

In Fig. 2, we display the mutual influence of both $\boldsymbol{N}_{\text{iter}}$ and $\boldsymbol{N}_{\text{disc}}$ on the errors in L_1 norm. The results show a tremendous regularity. The corresponding numerical results are displayed in Tab. 3.

N_{disc} \ N_{iter}	$E_1(N_{disc}, N_{iter})$ 10^2	$E_1(N_{disc}, N_{iter})$ 10^3	$E_1(N_{disc}, N_{iter})$ 10^4
10^5	0.023590236	0.074390944	0.25035328
10^6	0.0077829878	0.024115036	0.079437105
10^7	0.0027963003	0.0078734998	0.025343302
10^8	0.00070102901	0.0024396098	0.0079505501
10^9	0.00024907298	0.00078846501	0.002513533
10^{10}	$7.4041294.10^{-5}$	0.0002472693	0.0007908719
10^{11}	$2.821469.10^{-5}$	$8.540793.10^{-5}$	0.00025791013
10^{12}	$1.4600127.10^{-5}$	$3.2358931.10^{-5}$	$8.4195287.10^{-5}$

N_{disc} \ N_{iter}	$E_1(N_{disc}, N_{iter})$ 10^5	$E_1(N_{disc}, N_{iter})$ 10^6	$E_1(N_{disc}, N_{iter})$ 10^7
10^5	0.73832	1.810124	1.9801114
10^6	0.24974733	0.735708	1.809666
10^7	0.079959311	0.25029673	0.7353684
10^8	0.02518029	0.079508971	0.25000429
10^9	0.008005619	0.025207567	0.079757051
10^{10}	0.0025136649	0.0079736449	0.025230797
10^{11}	0.00080110625	0.002522144	0.0079771447
10^{12}	0.00025407246	0.00079907514	0.0025234708

Table 3. Error $\boldsymbol{E_1}$ for 3-coupled Symmetric Tent Maps with respect to both $\boldsymbol{N}_{\text{iter}}$ and $\boldsymbol{N}_{\text{disc}}$.

2.4 Impact of the initial values on the results

It is well known that the choice of the seed of a PRNG is very important. Some seed can lead to the collapse of the period of the computed random numbers. In order to check if the choice of the initial condition (equivalent to the choice of the seed of a PRNG) is dramatically for the previous results, we have tested several series of different initial values.

Fig. 3 shows the distribution of the error $\boldsymbol{E_1}$ for 500,000 initial values for 4-coupled symmetric tent maps. The computations are done using double precision numbers (~14-15 digits),

$\varepsilon_i = i.\varepsilon_1$, $\varepsilon_1 = 10^{-14}$, $N_{iter} = 10^6$, $N_{disc} = 10^2$.
The initial values are selected following:

$$x^1_{0,k} = -0.92712 + 10^{-7}\times k\ ,$$
$$x^2_{0,k} = -0.9183636 + 10^{-7}\times 7k,$$
$$x^3_{0,k} = -0.92576657 + 10^{-7}\times 13k,$$
$$x^4_{0,k} = -0.92390643 + 10^{-7}\times 17k,$$
$$k = 1 \text{ to } 500{,}000.$$

The distribution follows more or less a Gaussian distribution, maximal and minimal results are displayed in Tab. 4. Others series tested with several values of N_{disc} give the same kind of results.

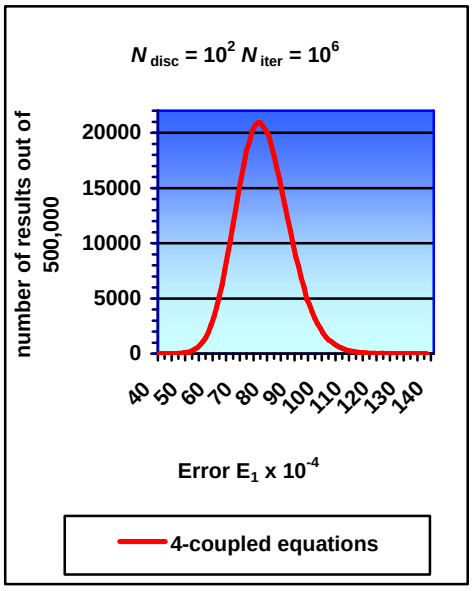

Figure 3. Distribution of the error E_1 for 500,000 initial values for 4-coupled symmetric tent maps.

N_{disc}	10^2	10^3	10^4
min $E_1(N_{disc}, N_{iter})$	0.0040021	0.0207400	0.0751521
max $E_1(N_{disc}, N_{iter})$	0.013872	0.0301160	0.0843841
min $E_2^2(N_{disc}, N_{iter})$	0.0000275	0.0006769	0.0089217
max $E_2^2(N_{disc}, N_{iter})$	0.0002834	0.001435	0.0110719

Table 4. Minimal and maximal values of the E_1 and E_2^2 errors for 500,000 initial values for 4-coupled symmetric tent maps.

2.5 Independency of the chaotic subsequences generated by each component

In next section, we propose the chaotic sampling of the chaotic sequences generated by Eq. (2.5) to enhance the properties of this chaotic number generator. The key feature of these enhanced chaotic number generators being their use of chaotic numbers themselves in order to do the sampling process. The main idea leading to this particular sampling is that the series of chaotic numbers produced by each component is independent of the others.

We need before to verify this independency.

Let consider now the coordinates of the iterated points $X_0, X_1, X_2, \cdots, X_n, X_{n+1}, \cdots$

$X_n = \begin{pmatrix} x_n^1 \\ \vdots \\ \vdots \\ x_n^p \end{pmatrix}$ of the multidimensional map F defined by (2.5). In order to check that they are uncorrelated, we plot every pair of coordinates of this sequence in the phase subspace (x^l, x^m) imbedded in the phase space $\mathbf{J}^p$ and we check if they are uniformly distributed in the square $\mathbf{J}^2$.

If no particular pattern is displayed and if the difference between the distribution of these points later called the correlation distribution function $C_N(x, y)$ converges towards the uniform distribution on the square when the number of iterations goes to the infinity, we can conclude the independency or the uncorrelation of the sequences of numbers generated by each component of the iterated points.

In order to compute numerically an approximation of the correlation distribution function $C_N(x, y)$ we build a regular partition of M^2 small squares (boxes) of $\mathbf{J}^2$ imbedded in the phase subspace (x^l, x^m)

$$r_{i,j} = [s_i\ ,\ s_{i+1}[\ \times\ [t_j\ ,\ t_{j+1}[\quad ,\ i, j = 0, M-2 \qquad (2.19)$$

$$r_{M-1,j} = [s_{M-1}\ ,\ 1]\times[t_j\ ,\ t_{j+1}[\quad ,\ j = 0, M-2 \qquad (2.20)$$

$$r_{i,M-1} = [s_i\ ,\ s_{i+1}[\times[t_{M-1}\ ,\ 1]\quad ,\ i = 0, M-2 \qquad (2.21)$$

$$r_{M-1,M-1} = [s_{M-1}\ ,\ 1]\times[t_{M-1}\ ,\ 1] \qquad (2.22)$$

$$s_i = -1+\frac{2i}{M}, t_j = -1+\frac{2j}{M},\ i, j = 0, M \qquad (2.23)$$

the measure of the area of each box is :

$$(s_{i+1}-s_i)\cdot(t_{i+1}-t_i) = \left(\frac{2}{M}\right)^2 \qquad (2.24)$$

Once $N + q$ iterated points $\left(x_n^l, x_n^m\right)$ belonging to these boxes are collected the relative number of iterates with respect to N/M^2 in each box $r_{i,j}$ represents the value $C_N(s_i, t_j)$. The approximated probability distribution function $C_N(x, y)$ defined in this article is then a 2-dimensional step function, with M^2 steps. As M can vary in the next sections, we define

$$C_{M,N}(s_i, t_j) = \frac{1}{4}\frac{M^2}{N}\left(\#r_{i,j}\right) \qquad (2.25)$$

where $\#r_{i,j}$ is the number of iterates belonging to the square $r_{i,j}$ and the constant 1/4 allows the normalisation of $C_{M,N}(x, y)$ on the square $\mathbf{J}^2$.

$$C_{M,N}(x, y) = C_{M,N}(s_i, t_j)\quad \forall (x, y)\in r_{i,j} \qquad (2.26)$$

The discrepancies E_{C1} (in norm L_1 between $C_{N_{disc},N_{iter}}(x,y)$ and the uniform distribution on the square is defined by

$$E_{C1}(N_{disc},N_{iter}) = \left\| C_{N_{disc},N_{iter}}(x,y) - 0.25 \right\|_{L_1} \qquad (2.27)$$

Fig. 4 shows the error $E_{C1}(N_{disc},N_{iter})$ versus the number of iterated points of the approximated correlation function between the first and the second components (x^1, x^2) for the 4-coupled symmetric tent map. Moreover, every couple of components checked simultaneously gives the same results.

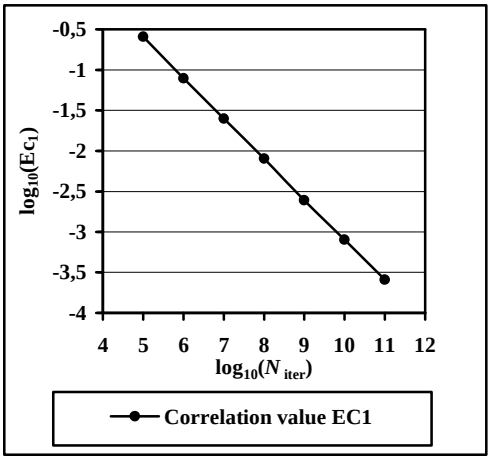

Figure 4. Error E_{C1} for the first and the second components (x^1, x^2) of the 4-coupled symmetric tent map. N_{disc} is fixed to 10^2 x 10^2, $\varepsilon_i = i.\varepsilon_1$, $\varepsilon_1 = 10^{-14}$, N_{iter} varies from 10^5 to 10^{11}. Computations are done using double precision numbers (~14-15 digits).
$x^1_0 = 0.330$, $x^2_0 = 0.3387564$, $x^3_0 = 0.50492331$, $x^4_0 = 0.0$.

3. Chaotic Sampling of Chaotic Numbers

If we plot the chaotic numbers produced by any component x^l , $1 \le l \le p$ of the p-dimensional dynamical system Eq. (2.5) in the phase space $\left(x_n^l, x_{n+1}^l\right)$, the iterated points show the graph of the symmetrical tent map f used to define Eq. (2.5) (more exactly a graph with two lines having ε thickness). These numbers are not randomly produced. If we plot these points in the phase spaces $\left(x_n^l, x_{n+2}^l\right)$, $\left(x_n^l, x_{n+3}^l\right)$ or $\left(x_n^l, x_{n+r}^l\right)$ they will display the graph of $f^{(2)}$, $f^{(3)}$ or $f^{(r)}$ (see Fig. 5). Hence someone knowing a sequence of few iterated points is able to find the initial value X_0 of the dynamical system.

In order to hide the graph of the genuine function f in the phase space $\left(x_n^l, x_{n+q}^l\right)$ for any q, a pivotal idea is to sample chaotically the sequence $\left(x_0^l, x_1^l, x_2^l, \ldots, x_n^l, x_{n+1}^l, \ldots\right)$ selecting x_n^l every time the value of x_n^m is greater than a threshold T, $-1 < T < 1$, with $l \neq m$, for $1 \le l, m \le p$.

The chaotically sampled subsequence $\left(\overline{x_0}, \overline{x_1}, \overline{x_2}, \cdots, \overline{x_q}, \overline{x_{q+1}}, \ldots\right)$ is defined as

$$\overline{x_q} = x_n^l \quad iff \quad x_n^m \in \left]T, 1\right[\qquad (3.1)$$

Choosing $T > 0.5$ implies that the selected subsequence

$$\left(\overline{x_0}, \overline{x_1}, \overline{x_2}, \cdots, \overline{x_q}, \overline{x_{q+1}}, \ldots\right) = \left(x_{p_0}^l, x_{p_1}^l, x_{p_2}^l, \ldots, x_{p_q}^l, x_{p_{q+1}}^l, \ldots\right)$$

is such that the difference between p_q and p_{q+1} is always greater than a minimal value K_m depending upon T. The graph of the chaotically sampled chaotic number is a mix of the graphs of all the $f^{(r)}$ for $r > K_m$.

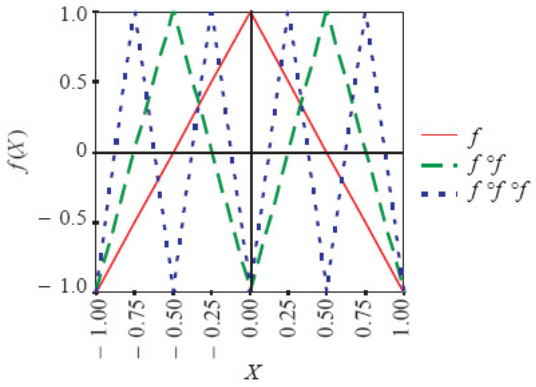

Figure 5. Graphs of the symmetric tent map f, $f^{(2)}$ and $f^{(3)}$ on the interval [-1,1].

As seen in Sect. 2.5 every pair of components $\left(x_n^l, x_n^m\right)$ of $X_0, X_1, X_2, \cdots, X_n, X_{n+1}, \cdots$ is uncorrelated. Hence, the proposed chaotic sampling is a powerful tool to generate enhanced chaotic numbers. Let $AC_{M,N}(x,y)$ the autocorrelation distribution function which is the correlation function $C_{M,N}(x,y)$ (2.26) defined in the phase space $\left(x_n^l, x_{n+1}^l\right)$ instead of the phase space (x^l, x^m). In order to control that the enhanced chaotic numbers $\left(\overline{x_0}, \overline{x_1}, \overline{x_2}, \cdots, \overline{x_q}, \overline{x_{q+1}}, \ldots\right)$ are uncorrelated, we plot them in the phase subspace $\left(\overline{x_n}, \overline{x_{n+1}}\right)$ and we check if they are uniformly distributed in the square $\mathbf{J^2}$.

If no particular pattern is displayed and if the autocorrelation distribution function $AC_{\mathbf{N}}$ (x, y) converges towards the uniform distribution on the square when the number of iterations goes to the infinity, we can conclude that the knowledge of a sequence of iterated points do not allow finding the initial value X_0 of the dynamical system.

Fig. 6 shows the values of

$$E_{AC1}(N_{disc}, NSampl_{iter}) = \left\| AC_{N_{disc},NSampl_{iter}}(x,y) - 0.25 \right\|_{L_1}$$

for a system of 4 coupled-equations for both the threshold values 0.98 and 0.998 of x_n^4. The

enhanced chaotic numbers are produced by the first component x^1_n of the dynamical system.

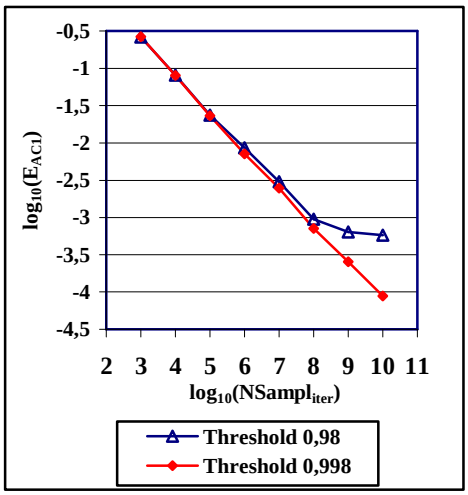

Figure 6. Error E_{AC1} for the first component x^1, sampled by x^4 for the threshold values 0.98 and 0.998 of the 4-coupled symmetric tent map. N_{disc}=10×10, $\varepsilon_i = i.\varepsilon_1$, $\varepsilon_1 = 10^{-14}$, $NSampl_{iter}$ varies from 10^3 to 10^{10}. Computations done using double precision numbers (~14-15 digits).
$x^1_0 = 0.330$, $x^2_0 = 0.3387564$, $x^3_0 = 0.50492331$, $x^4_0 = 0.0$.

As the chaotic numbers are regularly distributed on the interval **J,** when $T > 0.98$ one chaotic number over approximately 100 is sampled, when $T > 0.998$ one chaotic number over approximately 1,000 is sampled. We call $NSampl_{iter}$ the number of sampled points.

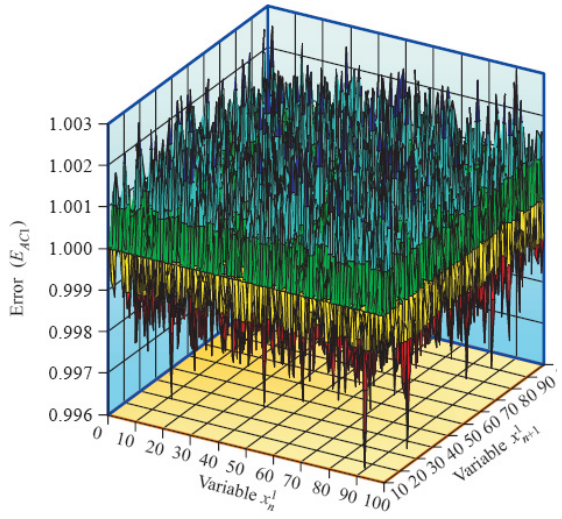

Figure 7. Difference between the autocorrelation distribution function $AC_{NSAMPLDISC}\left(x^1_n, x^1_{n+1}\right)$ and the uniform distribution of the 4-coupled symmetric tent map sampled by x^4 for the threshold value 0.998. $N_{disc} = 10^2 \times 10^2$, $NSampl_{iter} = 10^{10}$, $\varepsilon_i = i.\varepsilon_1$, $\varepsilon_1 = 10^{-14}$. Initial values:
$x^1_0 = 0.330$, $x^2_0 = 0.3387564$, $x^3_0 = 0.50492331$, $x^4_0 = 0.0$.

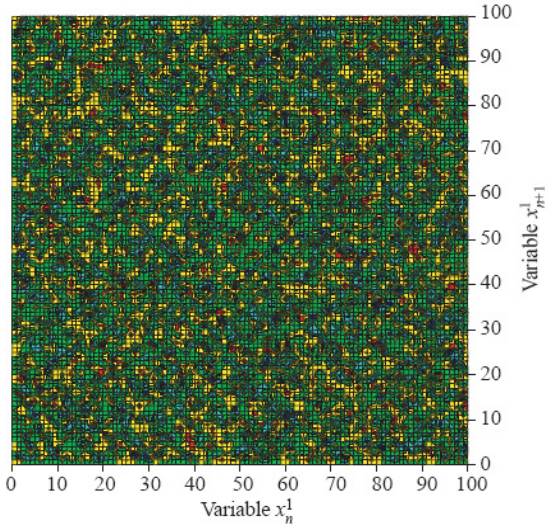

Figure 8. Projection of the Fig. 7 on the plane $\left(x^1_n, x^1_{n+1}\right)$.

Nevertheless the computing process is very fast. A desktop computer can produce more than 50,000,000 chaotic numbers per second, thus 50,000 iterated sampled points per second for $T > 0.998$. The sampling threshold 0.998 gives very good results.

The difference between the autocorrelation distribution function $AC_{NSAMPLDISC}\left(\overline{x_n}, \overline{x_{n+1}}\right)$ and the uniform distribution is shown on Fig. 7 and its projection on the phase subspace $\left(\overline{x_n}, \overline{x_{n+1}}\right)$ is shown on Fig. 8.

Fig. 9 and Tab. 5 show $E_{AC1}(N_{disc}, NSampl_{iter})$ with respect to N_{disc}

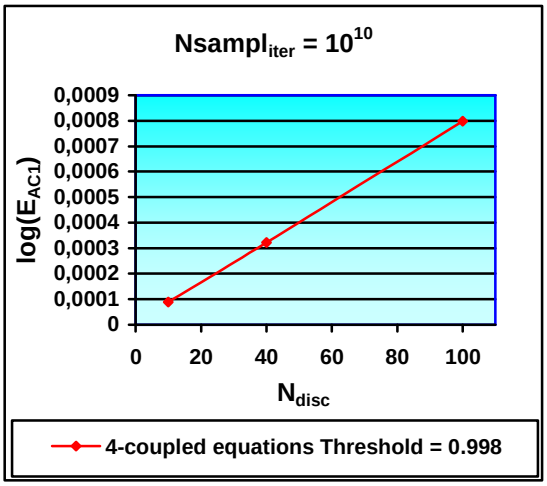

Figure 9. $E_{AC1}(N_{disc}, NSampl_{iter})$ for the first component x^1, sampled by x^4 for the threshold value 0.998 of the 4-coupled symmetric tent map versus N_{disc}, $NSampl_{iter} = 10^{10}$, $\varepsilon_i = i.\varepsilon_1$, $\varepsilon_1 = 10^{-14}$.
Initial values $x^1_0 = 0.330$, $x^2_0 = 0.3387564$, $x^3_0 = 0.50492331$, $x^4_0 = 0.0$.

N_{disc}	$NSampl_{iter}$	$E_{AC1}(N_{disc}, NSampl_{iter})$
10 x 10	**10,000,042,552**	**0.0000884451**
40 x 40	**10,000,042,552**	**0.000322549**
100 x 100	**10,000,042,552**	**0.000798014**

Table 5. $E_{AC1}(N_{disc}, NSampl_{iter})$.

4 Chaotic Mixing and Chaotic Sampling of Chaotic Numbers

One can improve again the unpredictability of the chaotic numbers generated as above, using all the components of the vector X instead of one. For example for 4-coupled equations, the value of x_n^4 command the sampling process as follows

Let us set three threshold values T_1, T_2 and T_3

$$-1 < T_1 < T_2 < T_3 < 1 \qquad (4.1)$$

we sample and mix together chaotically the sequences $(x_0^1, x_1^1, x_2^1, \ldots, x_n^1, x_{n+1}^1, \ldots)$, $(x_0^2, x_1^2, x_2^2, \ldots, x_n^2, x_{n+1}^2, \ldots)$ and $(x_0^3, x_1^3, x_2^3, \ldots, x_n^3, x_{n+1}^3, \ldots)$ defining $(\overline{x_0}, \overline{x_1}, \overline{x_2}, \cdots, \overline{x_q}, \overline{x_{q+1}}, \ldots)$ by

$$\overline{x_q} = \begin{cases} x_n^1 & iff \quad x_n^4 \in]T_1, T_2[\\ x_n^2 & iff \quad x_n^4 \in [T_2, T_3[\\ x_n^3 & iff \quad x_n^4 \in [T_3, 1[\end{cases} \qquad (4.2)$$

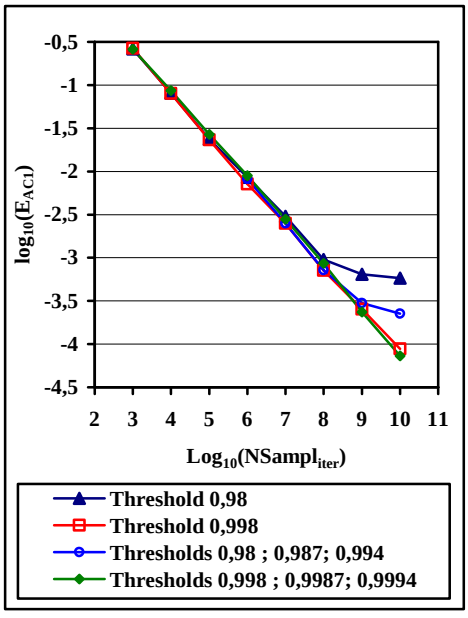

Figure 10. Error of $E_{AC1}(N_{disc}, NSampl_{iter})$ $N_{disc}=10^2\times10^2$, $NSampl_{iter}= 10^3$ to 10^{10}, $\varepsilon_i = i.\varepsilon_1$, $\varepsilon_1=10^{-14}$.

Fig. 10 and Tab. 6 show the values of $E_{AC1}(N_{disc}, NSampl_{iter})$ for a system of 4 coupled-equations when the first component x^1 is sampled by x^4 for both the threshold values 0.98 and 0.998 and when the three components x^1 , x^2 , x^3 are mixed and sampled by x^4 for the threshold values $T_1 = 0.98$, $T_2 = 0.987$, $T_3 = 0.994$ or $T_1 = 0.998$, $T_2 = 0.9987$, $T_3 = 0.9994$.

N_{iter}	$NSampl_{iter}$	$E_{AC1}(N_{disc}, NSampl_{iter})$ **4-coupled equation** $T = 0.998$
10^5	**95**	**0.70947368**
10^6	**971**	**0.26570546**
10^7	**10,095**	**0.079871223**
10^8	**100,622**	**0.023190157**
10^9	**1,001,408**	**0.0071386288**
10^{10}	**9,998,496**	**0.002493667**
10^{11}	**100,013,867**	**0.00071561417**
10^{12}	**999,994,003**	**0.00025442753**
10^{13}	**10,000,042,552**	**0.000088445108**

N_{iter}	$NSampl_{iter}$	$E_{AC1}(N_{disc}, NSampl_{iter})$ **4-coupled equation** $T_1 = 0.998$, $T_2 = 0.9987$, $T_3 = 0.9994$
10^5	**93**	**0.68924731**
10^6	**1015**	**0.25881773**
10^7	**10,139**	**0.086706776**
10^8	**100,465**	**0.026815309**
10^9	**1,000,549**	**0.0089111078**
10^{10}	**9,998,814**	**0.0027932033**
10^{11}	**100,001,892**	**0.00085967214**
10^{12}	**999,945,728**	**0.0002346851**
10^{13}	**10,000,046,137**	**0.000073234736**

Table 6. Error of $E_{AC1}(N_{disc}, NSampl_{iter})$ for a system of 4 coupled-equations when the first component x^1 is sampled by x^4 for the threshold value 0.998 and when the three components x^1 , x^2 , x^3 are mixed and sampled by x^4 for the threshold values $T_1 = 0.998$, $T_2 = 0.9987$, $T_3 = 0.9994$.

5. Further improvements

As said in Sec. 2.1, we have only considered the symmetric tent map (2.1). We have now to consider others maps of the interval: non symmetric tent map, baker map. We have also to consider the coupling (2.5) with maps having different parameters values

$$\underline{f}(X) = \begin{pmatrix} f_{a_1}(x^1) \\ \vdots \\ f_{a_p}(x^p) \end{pmatrix} \qquad (5.1)$$

($a_i \in \mathbb{R}^m$ being for example a general parameter value characterizing the general baker map)

6. Conclusion

We have introduced and combined synergistically three simple new mechanisms: very weakly coupling of chaotic maps, chaotic sampling and chaotic mixing of iterated points in order to make new families of enhanced Chaotic Pseudo Random Number Generators (CPRNG). The properties of these new families are explored numerically up to 10^{13} iterations. The numerical experiments give good results. Now other tests have to be performed in order to check their usefulness as Chaotic PRNG. Others functions and combination of functions have also to be explored in order to obtain

References

Alligood, K. T., Sauer, T. D., and Yorke, J. A. (1996). *Chaos. An introduction to dynamical systems.* Springer, Textbooks in mathematical sciences. New-York.

Barash, L., Shchur, L. N. (2006). Periodic orbits of the ensemble of Sinai-Arnold cat maps and pseudorandom number generation. *Physical Review E.* **73**, Issue 3, pp.036701.

Boffetta, G., Cencini, M., Falcioni, M., Vulpiani, A. (2002). Predictability : a way to characterize complexity. *Physics Reports*. **356**, pp. 367-474.

Gora, P., Boyarsky, A., Islam, MD. S., Bahsoun, W. (2006). Absolutely continuous invariant measures that cannot be observed experimentally. *SIAM J. Appl. Dyn. Syst.* **5**:1, pp. 84-90 (electronic).

Lanford III, O. E. (1998). Some informal remarks on the orbit structure of discrete approximations to chaotic maps. *Experimental Mathematics*. **Vol. 7**, 4, pp. 317-324.

Lozi, R. (2006). Giga-Periodic Orbits for Weakly Coupled Tent and Logistic Discretized Maps. *(International Conference on Industrial and Applied Mathematics,* New Delhi, december 2004*). Modern Mathematical Models, Methods and Algorithms for Real World Systems*. A.H. Siddiqi, I.S. Duff and O. Christensen (Editors). Anamaya Publishers. New Delhi, India. pp 80-124.

Petersen, M. V., Sorensen, H. M. (2007). Method of generating pseudo-random numbers in an electronic device, and a method of encrypting and decrypting electronic data. *United States Patent*. 7170997.

Ruggiero, D., Mascolo, D., Pedaci, I., Amato, P. (2006). Method of generating successions of pseudo-random bits or numbers. *United States Patent Application.* 20060251250.

Sprott, J. C. (2003). *Chaos and Time-Series Analysis*. Oxford University Press. Oxford, UK.