Quantifiers for randomness of chaotic pseudo-random number generators

L. De Micco, H. A. Larrondo, A. Plastino and O. A. Rosso

Phil. Trans. R. Soc. A 2009 367, 3281-3296
doi: 10.1098/rsta.2009.0075

References

Rapid response

Subject collections

Email alerting service

This article cites 44 articles
http://rsta.royalsocietypublishing.org/content/367/1901/3281.full.html#ref-list-1

Respond to this article
http://rsta.royalsocietypublishing.org/letters/submit/roypta;367/1901/3281

Articles on similar topics can be found in the following collections

mathematical physics (130 articles)
chaos theory (13 articles)

Receive free email alerts when new articles cite this article - sign up in the box at the top right-hand corner of the article or click here

To subscribe to Phil. Trans. R. Soc. A go to:
http://rsta.royalsocietypublishing.org/subscriptions

This journal is © 2009 The Royal Society
Quantifiers for randomness of chaotic pseudo-random number generators

BY L. DE MICCO¹, H. A. LARRONDO¹,* , A. PLASTINO² AND O. A. ROSSO³,⁴

¹Departamentos de Física y de Ingeniería Electrónica, Facultad de Ingeniería, Universidad Nacional de Mar del Plata, Juan B. Justo 4302, 7600 Mar del Plata, Argentina
²Instituto de Física, Facultad de Ciencias Exactas, Universidad Nacional de La Plata, CC 727, 1900 La Plata, Argentina
³Centre for Bioinformatics, Biomarker Discovery and Information-Based Medicine, and Hunter Medical Research Institute, School of Electrical Engineering and Computer Science, University of Newcastle, University Drive, Callaghan NSW 2308, Australia
⁴Instituto de Cálculo, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, 1428 Ciudad Universitaria, Buenos Aires, Argentina

We deal with randomness quantifiers and concentrate on their ability to discern the hallmark of chaos in time series used in connection with pseudo-random number generators (PRNGs). Workers in the field are motivated to use chaotic maps for generating PRNGs because of the simplicity of their implementation. Although there exist very efficient general-purpose benchmarks for testing PRNGs, we feel that the analysis provided here sheds additional didactic light on the importance of the main statistical characteristics of a chaotic map, namely (i) its invariant measure and (ii) the mixing constant. This is of help in answering two questions that arise in applications: (i) which is the best PRNG among the available ones? and (ii) if a given PRNG turns out not to be good enough and a randomization procedure must still be applied to it, which is the best applicable randomization procedure? Our answer provides a comparative analysis of several quantifiers advanced in the extant literature.

Keywords: random number; statistical complexity; recurrence plots; excess entropy; rate entropy; permutation entropy

1. Introduction

Chaos theory started more than 30 years ago and changed our world view regarding the role of randomness and determinism. As the statistical characteristics of chaotic systems were better understood (Lasota & Mackey 1994; Brown & Chua 1996; Beck & Schlögl 1997; Setti et al. 2002), a wide variety of situations emerged in which chaos, instead of stochastic systems, became a ‘controller of noise’.

*Author for correspondence (larrondo@fi.mdp.edu.ar).

One contribution of 14 to a Theme Issue ‘Topics on non-equilibrium statistical mechanics and nonlinear physics’.
Chaos illustrates the rather striking fact that complex behaviour arises from simple rules when nonlinearities are present. Since simple chaotic maps are capable of generating stochastic-like signals, implementations based on chaotic systems are usually less involved than those based on more complex algorithms (Stojanovski & Kocarev 2001; Kocarev & Jakimoski 2003). One tries to apply this notion to generate pseudo-random number generators (PRNGs) because random numbers are widely used not only in cryptography and Monte Carlo applications but also in less obvious applications (Pecora et al. 1990; L’Ecuyer 1994; Kocarev & Parlitz 1995; Hidalgo et al. 2001; Fernandez et al. 2003). We mention just a couple of them. (i) In spread spectrum techniques, a binary signal is mixed with a random number sequence, to spread the spectrum over a wider frequency range. Using different random number sequences, it is possible to share a communication channel among several users (Mazzini et al. 1997; Dinan & Jabbari 1998; Shan et al. 2006; De Micco et al. 2007). Reduction of electromagnetic interference is another important benefit of the spread spectrum effect (Setti et al. 2000; Callegari et al. 2002). (ii) Consider a low-frequency signal immersed in a high-frequency digital noise. Sampling at time intervals defined by a random number sequence, the resultant signal becomes filtered without using any coil or capacitors that are expensive, especially in power systems (Petrocelli et al. 2007).

Truly random numbers are not attainable from computers, and it is unlikely that we will ever be able to get them from ‘natural’ sources, since one commonly assumes that any system is governed by underlying physical rules and consequently it is deterministic. A successful strategy to build up a PRNG is to start with the time series of a simple nonlinear chaotic map and to apply to it an adequate randomizing procedure so as to ‘heighten/boost’ its stochastic nature. Such strategy requires a quantitative evaluation of the improvement achieved after effecting the procedure. González et al. (2005) used the statistical complexity measure originally proposed by López-Ruiz et al. (1995) and later modified by Lamberti et al. (2004) to quantify the effectiveness of such randomizing modus operandi when applied to a Lorenzian chaotic system. It was also shown there that a widely employed course of action—the mixing of two chaotic signals—is not effective in this respect, contrary to what one might expect. In this vein, it is important to note that general-purpose tests available in the open literature (http://csrc.nist.gov/rng/; http://stat.fsu.edu/pub/diehard/; http://www.iro.umontreal.ca/~simardr/random.html) are not designed taking into account the particular characteristics of a chaotic map. Instead, one can appreciate in Rosso et al. (2007a) the fact that the deterministic nature of chaotic dynamics leaves special manifestations in the associated time series, which can be revealed only by recourse to adequate statistical quantifiers.

De Micco et al. (2008) randomized chaotic maps by means of two different randomizing procedures, namely discretization and skipping. The idea of concocting an ‘information’ plane, called the entropy-complexity plane, was advanced in order to use it as a means to ascertain the effectiveness of each of these two modi operandi. The main difference of this information plane from other complexity-entropy diagrams is the joint use of two different probability distribution functions (PDFs) in it, both associated to the pertinent time series.

Other important tools at our disposal are to be mentioned as well. In a recent and excellent report, Marwan et al. (2007) reviewed applications of so-called recurrence plots for a wide variety of fields and endeavours. They also proposed
several measures to quantify the recurrence plots’ characteristics (Marwan et al. 2007). Additionally, two useful information-theoretic quantifiers of randomness, the rate entropy and the excess entropy, were proposed in Feldman et al. (2008) as coordinates of a complexity-entropy diagram.

In the present work, we explore combinations of all the above-mentioned quantifiers with the purpose of answering the following questions: (i) among several chaotic maps, just which is the one that generates the best time series? and (ii) which is the best strategy—discretization or skipping—to randomize a given chaotic time series? The ensuing quantifiers testing will be performed by means of two representative chaotic maps (and their iterates).

The paper is organized as follows: the statistical properties of a chaotic map and its iterates are reviewed in §2. Section 3 describes each of the analysed quantifiers. Section 4 deals with results for two representative maps and, finally, conclusions are presented in §5.

2. Statistical properties of a chaotic map

Let \( f \) be a chaotic map on the interval \([0,1]\). Suppose the map has an invariant measure \( \mu(x) \). Then the map is ergodic if for any integrable test function \( Q(x) \), and for an arbitrary initial condition \( x_0 \) (up to a set of zero \( \mu \)-measure), the time average is equal to the ensemble average

\[
\bar{Q} = \langle Q \rangle. \tag{2.1}
\]

Equation (2.1) is a consequence of the famous Birkhoff ergodic theorem (Cornfeld et al. 1982). Mixing is an even stronger requirement than ergodicity. A map is called ‘mixing’ if any smooth initial probability density \( \rho(x) \) converges to the invariant measure \( \mu(x) \) after enough successive iterations. Mixing implies ergodicity. The reverse, however, is not true (Beck 1990).

There exists an equivalent definition of mixing via correlation functions. Let \( \phi_1(x) \) and \( \phi_2(x) \) be two integrable test functions and define the generalized correlation function of the map \( f \) by

\[
C(\phi_1, \phi_2, n) = \lim_{J \to \infty} \frac{1}{J} \sum_{j=0}^{J-1} \phi_1(x_{j+n})\phi_2(x_j) - \langle \phi_1 \rangle \langle \phi_2 \rangle, \tag{2.2}
\]

where

\[
\langle \phi_i \rangle = \lim_{J \to \infty} \frac{1}{J} \sum_{j=0}^{J-1} \phi_i(x_j). \tag{2.3}
\]

The map is mixing if, for arbitrary \( \phi_1 \) and \( \phi_2 \),

\[
\lim_{n \to \infty} C(\phi_1, \phi_2, n) = 0. \tag{2.4}
\]

Let us stress that it is not easy to prove that \( f \) is a mixing map because the mixing condition given in equation (2.4) must be fulfilled for arbitrary test functions. Formally, every mixing map \( f \) has an associated
Perron–Frobenius operator $\mathcal{L}$ (Beck 1990) that determines the time evolution of any initial density $\rho_0(x)$ towards the invariant measure $\mu(x)$

$$\rho_{n+1} = \mathcal{L}[\rho_n].$$

The explicit formal expression for the Perron–Frobenius operator for a one-dimensional map $f$ is given by (Beck 1990)

$$\mathcal{L}[\rho_y] = \sum_{x \in f^{-1}(y)} \frac{[\rho_0(x)]}{|f'(x)|}.$$  

(2.6)

This operator $\mathcal{L}$ has a set of eigenfunctions $\psi_\alpha(x)$ and eigenvalues $\eta_\alpha$. The invariant measure $\mu(x)$ is the eigenfunction corresponding to the largest eigenvalue $\eta_0 = 1$. The full set of eigenfunctions and eigenvalues may be used as a basis to express any density

$$\rho_0(x) = \sum_\alpha c_\alpha \psi_\alpha(x),$$

$$\rho_n(x) = \mathcal{L}^n \rho_0(x) = \sum_\alpha \eta_\alpha^n c_\alpha = c_0 \psi_0(x) + R_n.$$  

(2.7)

The eigenvalue with the second largest absolute value, $\eta_1$, has a ‘distinguished’ physical meaning: it is related with the mixing constant $r_{\text{mix}}$ that governs the relaxation of exponentially mixing maps

$$|R_n| \sim |\eta_1|^n \sim \exp \left( -\frac{n}{r_{\text{mix}}} \right).$$

(2.8)

The invariant measure $\mu(x)$ gives the histogram of the time series, and the ideal PRNG must have $\mu(x) = \text{const}$. The mixing constant $r_{\text{mix}}$ gives the transient characteristic time (Mazzini et al. 1997; Rovatti et al. 2004a,b; De Micco et al. 2007; Petrocelli et al. 2007), and its ideal value is $r_{\text{mix}} = 0$. In many applications of PRNGs, both the invariant measure and the mixing constant are relevant.

The analytical expression of the invariant measure $\mu(x)$ of a given map $f$ is usually not known. Exceptions are the logistic map in full chaos and the piecewise-linear maps. The mixing constant $r_{\text{mix}}$ has been analytically obtained only for piecewise-linear maps. For other maps, it must be numerically obtained by means of a piecewise-linear approximation of the map (Lasota & Mackey 1994; Beck & Schlögl 1997).

It is then obviously convenient to have quantifiers for measuring the uniformity of the invariant measure $\mu(x)$, and the mixing constant $r_{\text{mix}}$, for any chaotic map. These quantifiers are useful to compare time series coming from different chaotic maps and also to assess the improvements produced by randomization procedures.

It is possible to show that the invariant measure of $f^d$ is identical to the invariant measure of $f$. Also, the mixing constant $r_{\text{mix}}$ for $f^d$ is lower than the mixing constant for $f$. The iteration of a map is one of the randomization procedures proposed in the literature, being used to diminish $r_{\text{mix}}$. This procedure is also known as skipping because iterating is tantamount to skipping values in the original time series, which does not change $\mu(x)$ and, consequently, is not conductive to a randomization of chaotic maps with $\mu(x) \neq \text{const}$. In this paper, we will use ‘skipping’ as a method of quantifier analysis.
3. Quantifiers for the invariant measure and mixing constant

In this section, we review several quantifiers proposed for measuring the main statistical properties of chaotic PRNGs. The quantifiers are classified according to their origin into three classes: (i) quantifiers based on information theory (López-Ruiz et al. 1995; Lamberti et al. 2004; Rosso et al. 2007a), (ii) quantifiers based on recurrence plots (Eckmann et al. 1987; Marwan et al. 2007), and (iii) quantifiers based on intrinsic computation (Feldman et al. 2008).

(a) Quantifiers based on information theory

They are appropriate functionals of the PDF. Let \{x_i\} be the time series under analysis, with length M. There are infinite possibilities to assign a PDF to a given time series, a subject that will be given due consideration below. In the meantime, suppose that the PDF is discrete and is given by \( P = \{p_i; i = \ldots, N\} \). One then defines various quantities, as follows.

(i) Normalized Shannon entropy \( H[P] \). Let \( S[P] \) be the Shannon entropy

\[
S[P] = -\sum_{i=1}^{N} p_i \ln(p_i). \tag{3.1}
\]

It is well known that the maximum \( S_{\text{max}} = \ln(N) \) is obtained for \( P_e = \{1/N, \ldots, 1/N\} \), that is, the uniform PDF. A ‘normalized’ entropy \( H[P] \) can also be defined in the fashion

\[
H[P] = S[P]/S_{\text{max}}. \tag{3.2}
\]

(ii) Statistical complexity measure. A full discussion about statistical complexity measures exceeds the scope of this presentation. For a comparison among different complexity measures, see the excellent paper by Wackerbauer et al. (1994). In this paper, we adopt the definition of the seminal paper of López-Ruiz et al. (1995) with the modifications advanced in Lamberti et al. (2004) so as to ensure that the concomitant SCM version becomes (i) able to grasp essential details of the dynamics, (ii) an intensive quantity, and (iii) capable of discerning both among different degrees of periodicity and chaos (Rosso et al. 2007a). The ensuing measure, to be referred to as the intensive statistical complexity, is a functional \( C[P] \) that reads

\[
C[P] = Q_J[P, P_e] \cdot H[P], \tag{3.3}
\]

where \( Q_J \) is the ‘disequilibrium’, defined in terms of the so-called extensive Jensen–Shannon divergence (which induces a squared metric; Lamberti et al. 2004). One has

\[
Q_J[P, P_e] = Q_0 \cdot [S[(P + P_e)/2] - S[P]/2 - S[P_e]/2], \tag{3.4}
\]

with \( Q_0 \) a normalization constant \( (0 \leq Q_J \leq 1) \) that reads

\[
Q_0 = -2 \left\{ \left( \frac{N+1}{N} \right) \ln(N+1) - 2 \ln(2N) + \ln N \right\}^{-1}. \tag{3.5}
\]
We see that the disequilibrium $Q_J$ is an intensive quantity that reflects on the system’s ‘architecture’, being different from zero only if there exist ‘privileged’, or ‘more likely’ states among the accessible ones. $C[P]$ quantifies the presence of correlational structures as well (Martin et al. 2003; Lamberti et al. 2004). The opposite extremes of perfect order and maximal randomness possess no structure to speak of and, as a consequence, $C[P] = 0$. In between these two special instances, a wide range of possible degrees of physical structure exist, degrees that should be reflected in the features of the underlying probability distribution. In the case of a PRNG, the ‘ideal’ values are $H[P] = 1$ and $C[P] = 0$.

As pointed out above, $P$ itself is not a uniquely defined object, and several approaches have been employed in the literature so as to ‘extract’ $P$ from the given time series. Just to mention some frequently used extraction procedures: (i) time series histogram (Martin 2004), (ii) binary symbolic dynamics (Mischaikow et al. 1999), (iii) Fourier analysis (Powell & Percival 1979), (iv) wavelet transform (Blanco et al. 1998; Rosso et al. 2001), (v) partition entropies (Ebeling & Steuer 2002; Keller & Sinn 2005), (vi) permutation entropy (Bandt & Pompe 2002; Keller & Sinn 2005), (vii) discrete entropies (Amigó et al. 2007), etc. There is ample liberty to choose among them. De Micco et al. (2008) proposed two probability distributions as relevant for testing the uniformity of $\mu(x)$ and the mixing constant: (i) a $P$ based on time-series’ histograms and (ii) a $P$ based on ordinal patterns (permutation ordering) that derives from using the Bandt–Pompe method (Bandt & Pompe 2002).

For extracting $P$ via the histogram, one divides the interval $[0, 1]$ into a finite number $N_{bin}$ of non-overlapping subintervals $A_i$: $[0, 1] = \bigcup_{i=1}^{N_{bin}} A_i$, and $A_i \cap A_j = \emptyset \ \forall i \neq j$. Note that $N$ in equation (3.1) is equal to $N_{bin}$. Of course, in this approach, the temporal order of the time series plays no role at all. In this paper, the quantifiers obtained via the ensuing PDF are called $H^{(\text{hist})}$ and $C^{(\text{hist})}$. Let us stress that for time series within a finite alphabet, it is relevant to consider an optimal value of $N_{bin}$ (e.g. De Micco et al. 2008).

In extracting $P$ by recourse to the Bandt–Pompe method, the resulting probability distribution $P$ is based on the details of the attractor-reconstruction procedure. Causal information is, consequently, duly incorporated into the construction process that yields $P$. In this paper, the quantifiers obtained via the ensuing PDF are called $H^{(\text{BP})}$ and $C^{(\text{BP})}$. A notable Bandt–Pompe result consists in getting a clear improvement in the quality of information theory-based quantifiers (Larrondo et al. 2005, 2006; Kowalski et al. 2007; Rosso et al. 2007a,b, 2008; Zunino et al. 2007, 2008).

The extracting procedure is as follows. For the time series $\{x_t: t = 1, \ldots, M\}$ and an embedding dimension $D > 1$, one looks for ‘ordinal patterns’ of order $D$ (Bandt & Pompe 2002; Keller & Lauffer 2003; Keller & Sinn 2005) generated by

\[(s) \mapsto (x_{s-(D-1)}, x_{s-(D-2)}, \ldots, x_{s-1}, x_s), \quad (3.6)\]

which assign to each ‘time s’ a $D$-dimensional vector of values pertaining to the times $s, s-1, \ldots, s-(D-1)$. Clearly, the greater the $D$-value, the more is the information on ‘the past’ incorporated into these vectors. By the ‘ordinal pattern’ related to the time $(s)$, we mean the permutation $\pi = (r_0, r_1, \ldots, r_{D-1})$.
of \((0, 1, \ldots, D - 1)\) defined by
\[
x_{s-r_{D-1}} \leq x_{s-r_{D-2}} \leq \cdots \leq x_{s-r_1} \leq x_{s-r_0}.
\]
(3.7)

In order to get a unique result, we consider that \(r_i < r_{i-1}\) if \(x_{s-r_i} = x_{s-r_{i-1}}\). Thus, for all the \(D!\) possible permutations \(\pi\) of order \(D\), the probability distribution \(P = \{p(\pi)\}\) is defined by
\[
p(\pi) = \frac{\# \{ s | s \leq M - D + 1 ; (s) \text{ has type } \pi \} }{M - D + 1}.
\]
(3.8)

In the last expression, the symbol \(\#\) stands for 'number'.

The advantages of the Bandt–Pompe method reside in (i) its simplicity, (ii) the associated extremely fast calculation process, (iii) its robustness in the presence of observational and dynamical noise, and (iv) its invariance with respect to nonlinear monotonous transformations. The Bandt–Pompe methodology is not restricted to a 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 \(t\); Bandt & Pompe 2002). 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. In relation to this last point, Bandt and Pompe suggest, for practical purposes, working with \(3 \leq D \leq 7\) with a time lag \(\tau = 1\). This is what we do here (in the present work \(D = 6\) is used).

(b) Quantifiers based on recurrence plots

Recurrence plots were introduced by Eckmann et al. (1987) so as to visualize the recurrence of states during phase space evolution. The recurrence plot is a two-dimensional representation in which both axes are time ones. The recurrence of a state appearing at two given times \(t_i, t_j\) is pictured in the two-dimensional graph by means of either black or white dots, where a black dot signals a recurrence. Of course only periodic continuous systems will have exact recurrences. In any other case, one detects only approximate recurrences, up to an error \(\epsilon\). The so-called recurrence function can be mathematically expressed as
\[
R(i, j) = \Theta(\epsilon - \| \tilde{x}(i) - \tilde{x}(j) \|),
\]
(3.9)
with \(\tilde{x}(i) \in \mathbb{R}^m\) and \(i, j = 1, \ldots, N, N\) being the number of discrete states \(\tilde{x}(i)\) considered, \(\| \cdot \|\) is a norm and \(\Theta(\cdot)\) is the Heaviside step function.

In the particular case of the PRNGs analysed in this paper, only \(1D\) series are considered, but the recurrence function idea can be extended to \(D\)-dimensional phase spaces or even to suitably reconstructed embedding phase spaces. Of course, the visual impact produced by the recurrence plot is insufficient to compare the quality of different PRNGs because of the ‘small-scale’ structures that may be present in our scenario. Several kinds of measures have been defined to quantify these small-scale structures (Marwan et al. 2007), each measure being a functional

\[\text{Phil. Trans. R. Soc. A} (2009)\]
of the recurrence function (equation (3.9)). In this paper, two kinds of recurrence plot measures are considered.

(i) **Measures based on the recurrence density (measured by the number of points in the recurrence plot).** In this paper, we use the recurrence rate (RR), given by

$$RR(\varepsilon) = \frac{1}{N^2} \sum_{i,j=1}^{N} R_{ij}(\varepsilon).$$  \hspace{1cm} (3.10)

Note that in the limit $N \to \infty$, RR is the probability that a state recurs to its $\varepsilon$-neighbourhood in phase space. For PRNGs, the ideal value would be $RR = 0$. But in practice, if no points are to be found in the recurrence plot, a larger $\varepsilon$ must be adopted in order that the quantifier may make sense.

(ii) **Diagonal measures.** These are measures related to the histogram $P(\varepsilon, l)$ of diagonal line lengths, given by

$$P(\varepsilon, l) = \sum_{i,j=1}^{N} \left[ 1 - R_{i-1,j-1}(\varepsilon) \right] \left[ 1 - R_{i+l,j+l}(\varepsilon) \right] \cdot \prod_{k=0}^{l-1} R_{i+k,j+k}(\varepsilon).$$  \hspace{1cm} (3.11)

Processes with uncorrelated or weakly correlated behaviour originate no (or just very short) diagonals, whereas deterministic processes give rise to ‘long’ diagonals and smaller amount of single, isolated recurrence points. In this paper, three measures based on the statistics of diagonal lines are considered.

(a) **The deterministic quantifier DET.** The ratio of recurrence points that form diagonal structures of at least length $l_{\text{min}}$ to all recurrence points

$$\text{DET} = \frac{\sum_{l=l_{\text{min}}}^{N} l \cdot P(\varepsilon, l)}{\sum_{l=1}^{N} l \cdot P(\varepsilon, l)}. \hspace{1cm} (3.12)$$

(b) **The average diagonal line length $L$** given by

$$L = \frac{\sum_{l=l_{\text{min}}}^{N} l \cdot P(\varepsilon, l)}{\sum_{l=1}^{N} P(\varepsilon, l)}. \hspace{1cm} (3.13)$$

(c) **The entropy ENTR** given by

$$\text{ENTR} = - \sum_{l=l_{\text{min}}}^{N} P(\varepsilon, l) \ln P(\varepsilon, l). \hspace{1cm} (3.14)$$

(c) **Quantifiers based on intrinsic computation**

We consider in this paper two quantifiers introduced in Feldman et al. (2008), i.e. the entropy rate $h_{\mu}$ and the entropy excess $E$. They are defined for time series with a finite alphabet $A$, which is not a limitation because the $x_i$’s may be thought of as real numbers only in analytical studies. In any practical case, they are in fact floating point numbers and, consequently, they have only a finite number of allowed $A$-values. A subsequence $s^L = \{x_i, x_{i+1}, \ldots, x_{i+L}\}$ is called an $L$-block.
Let $P(s^L)$ denote the probability of a particular $L$-block. Then the block entropy $H(L)$ is

$$H(L) \equiv -\sum_{s^L} P(s^L) \log_2 P(s^L).$$

The sum runs over all possible blocks of length $L > 0$ and $H(0) \equiv 0$ by definition. For stationary processes and sufficiently large $L$, $H(L) \sim L$. On the other hand, the entropy rate $h_\mu$ is defined as

$$h_\mu(L) = \frac{H(L)}{L},$$

and

$$h_\mu = \lim_{L \to \infty} h_\mu(L).$$

The entropy rate is also known as the metric entropy in dynamical systems theory and it is equivalent to the thermodynamic entropy density familiar from equilibrium statistical mechanics (Feldman et al. 2008). The entropy rate provides a reliable and well-understood measure of the randomness or disorder intrinsic to a process. However, this tells us little about the underlying system’s organization, structure or correlations. A measure of the system’s organization may be obtained by looking at the manner in which $h_\mu(L)$ converges to its asymptotic value $h_\mu$. When only observations over length $L$-blocks are taken into account, a process appears to have an entropy rate of $h_\mu(L)$ larger than the asymptotic value of $h_\mu$. As a result, the process seems to be of a more random nature than it really is by the ‘excess’ amount of $h_\mu(L) - h_\mu$ bits. Summing these entropy over estimates over $L$, one obtains the excess entropy (Crutchfield & Packard 1983)

$$E \equiv \sum_{L=1}^{\infty} [h_\mu(L) - h_\mu].$$

### (d) Expected behaviour for PRNG

Summing up, the quantifiers to be compared here are: $H^{(\text{hist})}$, $C^{(\text{hist})}$, $H^{(\text{BP})}$, $C^{(\text{BP})}$, RR, DET, ENTR, $L$, $h_\mu$ and $E$. These quantities should tell us how good our PRNG is as compared to the ideal condition $\mu(x) = \text{const.}$, $r_{\text{mix}} = 0$. $H^{(\text{hist})}$ is the natural quantifier to measure a non-constant $\mu(x)$, with value 1 for the ideal PRNG. It does not depend on the order of appearance of a given time-series event, but only on the number of times such event takes place. As for $H^{(\text{hist})}$, it is not able to uncover any change in $r_{\text{mix}}$-values. Thus, to get a good representation plane, we ought to demand a quantifier that changes with $r_{\text{mix}}$ and not with $\mu(x)$. To look for such a kind of quantifier, we must study $H^{(\text{hist})}$, $C^{(\text{hist})}$, $H^{(\text{BP})}$, $C^{(\text{BP})}$, RR, DET, ENTR, $L$, $h_\mu$ and $E$ as functions of $r_{\text{mix}}$. A family of iterated maps $f^d$ may be used to that end because they share the same invariant measure and $r_{\text{mix}}$ is a decreasing function of $d$. The best quantifier for $r_{\text{mix}}$ would be that which has maximal variation over the entire family of maps.

### 4. Application to logistic map and three-way Bernoulli map

In this section, we present results for the families of iterates of two chaotic well-known maps, the logistic map (LOG) and the three-way Bernoulli map (TWB), that have been selected, among other possibilities, because they are representative of two different classes of systems.
Table 1. Mixing constant ($r_{mix}$ as a function of the iteration-order $d$ for LOG and TWB).

| $d$ | TWB     | LOG     |
|-----|---------|---------|
| 1   | 0.56789 | 0.333333333 |
| 2   | 0.31848 | 0.111111111 |
| 3   | 0.13290 | 0.037037037 |
| 4   | 0.05788 | 0.012345679 |
| 5   | 0.03646 | 0.004115226 |
| 6   | 0.01791 | 0.001371742 |
| 7   | 0.01152 | 0.000457247 |
| 8   | 0.00515 | 0.000152416 |

(i) LOG is given by

$$x_{n+1} = 4x_n(1 - x_n),$$

and its natural invariant density can be exactly determined, being expressed in the fashion

$$\rho_{inv}(x) = \frac{1}{\pi \sqrt{x(1-x)}}.$$  \hspace{1cm} (4.2)

LOG is paradigmatic because it is representative not only of maps with a quadratic maximum, but also emerges when the Lorenz procedure is applied to many continuous attractors with basins that may be approached with the Lorenz method via a one-dimensional map (like the Lorenz, Rossler and Colpits ones among others). A non-uniform natural invariant density is an important feature in this instance (Beck & Schlögl 1997). The ensuing $r_{mix}$-values are also displayed in table 1. They have been obtained by recourse to the transfer operator method, as described in Beck & Schlögl (1997).

(ii) TWB is given by

$$x_{n+1} = \begin{cases} 
3x_n & \text{if } 0 \leq x_n \leq \frac{1}{3} \\
3x_n - 1 & \text{if } \frac{1}{3} < x_n \leq \frac{2}{3} \\
3x_n - 2 & \text{if } \frac{2}{3} < x_n \leq 1.
\end{cases}$$

TWB is representative of the class of piecewise-linear maps as, for example, the four-way tailed shift map, the skew tent map, the three-way tailed shift map, etc. All these maps share a uniform natural invariant density (Beck & Schlögl 1997). The mixing constant $r_{mix}$ of the whole family of maps $f^d$ is given by $r_{mix}^d = (1/3)^d$ (table 1).

For the evaluation of the different quantifiers, we used files with $M = 50 \times 10^6$ floating point numbers. In the Band–Pompe approach, we consider $D = 6$ while
for histograms we have taken $N_{\text{bin}} = 2^{16}$. All recurrence plots measures depend on several parameters.

(i) The dimension $D_e$ of the embedding space. In this paper $D_e = 1$.
(ii) $\varepsilon$, a parameter crucial so as to define just when recurrences occur. We adopted $\varepsilon = 1/(2^{16} - 1)$ corresponding to 16-bit numbers.
(iii) $l_{\text{min}}$ is the minimum length accepted for diagonal lines. $l_{\text{min}} = 2$ is used in this paper for all diagonal measures except for $L$ ($l_{\text{min}} = 1$ is used for $L$).
(iv) $N$ is the number of values used for each realization. In this paper, values of RR, DET, ENTR and $L$ are mean values over 10 surrogate series with $N = 10000$ data each.

Figures 1–3 illustrate the behaviour of all the quantifiers for the iterates of LOG (figures 1a, 2a and 3a) and the iterates of TWB (figures 1b, 2b and 3b). These figures show that the following quantifiers are the ones usable for measuring $r_{\text{mix}}$: $C^{(BP)}$, DET, ENTR and $L$. On the other hand, the following quantifiers depend on the invariant density, but they do not depend on $r_{\text{mix}}$: $H^{(\text{hist})}$, $C^{(\text{hist})}$ and RR.

Phil. Trans. R. Soc. A (2009)
Intrinsic computation quantifiers display a completely different behaviour for LOG and for TWB. In LOG, both quantifiers have no dependence with \( r_{\text{mix}} \), but in TWB, \( h_\mu \) decreases as \( r_{\text{mix}} \) increases while \( E \) is an increasing function of \( r_{\text{mix}} \). Thus, these parameters do not seem to be convenient ones.

Comparing LOG with TWB by recourse to these parameters shows that TWB is slightly better than LOG. The problem with TWB and with other piecewise-linear maps is they are not realistic enough and that their implementation is more involved than for other maps like LOG.

As an application of the above quantifiers, we study two usual randomization procedures by means of the representation plane depicted in figure 4, employing a quantifier depending on \( \mu(x) \) as \( x \)-axis (\( H^{(\text{hist})} \) is selected) and a quantifier depending on \( r_{\text{mix}} \) as \( y \)-axis (DET is selected). The first procedure is skipping and the second one is discretization (De Micco et al. 2008). Skipping has been used as a randomization procedure for piecewise-linear maps. The representation plane evidences the fact that this procedure is better than discretization because these maps already have the ideal invariant measure (they have \( H^{(\text{hist})} = 1 \)) and only \( r_{\text{mix}} \)
must be diminished to get the ideal PRNG. Figure 4b shows that discretization is a better procedure for LOG because the ideal point [1, 0] is not reached by skipping.

5. Conclusions

In summary, we were able to show here the following.

(i) Two classes of quantifiers are required for the evaluation of the quality of a PRNG: (i) quantifiers depending on $r_{\text{mix}}$ only (and not on $\mu(x)$), like $H^{(\text{hist})}$, $C^{(\text{hist})}$ and RR and (ii) quantifiers depending on $\mu(x)$ only (and not on $r_{\text{mix}}$), as $C^{(\text{BP})}$, $H^{(\text{BP})}$, DET, L and ENTR.

(ii) Intrinsic computation quantifiers are dependent on both $\mu(x)$ and $r_{\text{mix}}$ and then they are not convenient for PRNG analysis with our methodology.

(iii) Representation planes with one quantifier of each class as coordinate axes allow for different chaotic PRNGs to be compared with each other so as to determine the best one. Furthermore, these representation planes permit one to judiciously select the best randomizing procedure.
Figure 4. DET as a function of $H_{(\text{hist})}$, as evaluated in De Micco et al. (2008), for both randomization procedures applied to: (a) LOG; (b) TWB. Squares and dashed lines, discretization; circles and solid lines, skipping.

Our present results are consistent with those of previous works (Gonzalez et al. 2005; Larrondo et al. 2005; De Micco et al. 2008).

This work was partially supported by the Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), Argentina (PIP 5569/04, PIP 5687/05, PIP 6036/05), ANPCyT, Argentina (PICT 11-21409/04) and Universidad Nacional de Mar del Plata. O.A.R. gratefully acknowledges support from the Australian Research Council (ARC) Centre of Excellence in Bioinformatics, Australia.

References

Amigó, J. M., Kocarev, L. & Tomovski, I. 2007 Discrete entropy. Physica D 228, 77–85. (doi:10.1016/j.physd.2007.03.001)

Bandt, C. & Pompe, B. 2002 Permutation entropy: a natural complexity measure for time series. Phys. Rev. Lett. 88, 174102-1. (doi:10.1103/PhysRevLett.88.174102)

Beck, C. 1990 Ergodic properties of a kicked damped particle. Commun. Math. Phys. 130, 51–60.

Beck, C. & Schlögl, F. 1997 Thermodynamics of chaotic systems: an introduction. Cambridge, UK: Cambridge University Press.

Blanco, S., Figliola, A., Quian Quiroga, R., Rosso, O. A. & Serrano, E. 1998 Time–frequency analysis of electroencephalogram series (iii): wavelet packets and information cost function. Phys. Rev. E 57, 932–940. (doi:10.1103/PhysRevE.57.932)
Marwan, N., Romano, M. C., Thiel, M. & Kurths, J. 2007 Recurrence plots for the analysis of complex systems. *Phys. Rep.* **438**, 237–329. (doi:10.1016/j.physrep.2006.11.001)

Mazzini, G., Setti, G. & Rovatti, R. 1997 Chaotic complex spreading sequences for asynchronous DS-CDMA. Part 1: system modeling and results. *IEEE Trans. Circuits Syst. I* **44**, 937–947.

Mischaikow, K., Mrozek, M., Reiss, J. & Szymczak, A. 1999 Construction of symbolic dynamics from experimental time series. *Phys. Rev. Lett.* **82**, 1144. (doi:10.1103/PhysRevLett.82.1144)

Pecora, M., Carroll, L. & Thomas, L. 1990 Synchronization in chaotic systems. *Phys. Rev. Lett.* **64**, 821–824. (doi:10.1103/PhysRevLett.64.821)

Petrocelli, R. A., De Micco, L., Carrica, D. O. & Larrondo, H. A. 2007 Acquisition of low frequency signals immersed in noise by chaotic sampling and fir filters. *Proc. WISP2007, Alcalá de Henares, Spain*, pp. 351–356.

Powell, G. E. & Percival, I. C. 1979 A spectral entropy method for distinguishing regular and irregular motion of hamiltonian systems. *J. Phys. A Math. Gen.* **12**, 2053–2071. (doi:10.1088/0305-4470/12/11/017)

Rosso, O. A., Blanco, S., Jordanova, J., Kolev, V., Figliola, A., Schurmann, M. & Başar, E. 2001 Wavelet entropy: a new tool for analysis of short duration brain electrical signals. *J. Neurosci. Methods* **105**, 65–75. (doi:10.1016/S0165-0270(00)00356-3)

Rosso, O. A., Larrondo, H. A., Martin, M. T., Plastino, A. & Fuentes, M. A. 2007a Distinguishing noise from chaos. *Phys. Rev. Lett.* **99**, 154 102–154 106. (doi:10.1103/PhysRevLett.99.154102)

Rosso, O. A., Zunino, L., Pérez, D. G., Figliola, A., Larrondo, H. A., Garavaglia, M., Martín, M. T. & Plastino, A. 2007b Extracting features of Gaussian self-similar stochastic processes via the Bandt and Pompe approach. *Phys. Rev. E* **76**, 061114. (doi:10.1103/PhysRevE.76.061114)

Rosso, O. A., Vicente, R. & Mirasso, C. R. 2008 Encryption test of pseudo-aleatory messages embedded on chaotic laser signals: an information theory approach. *Phys. Lett. A* **372**, 1018–1023. (doi:10.1016/j.physleta.2007.08.063)

Rovatti, R., Mazzini, G. & Setti, G. 2004 On the ultimate limits of chaos-based asynchronous DS-CDMA—i: basic definitions and results. *IEEE Trans. Circuits Syst. I* **51**, 1336–1347. (doi:10.1109/TCSI.2004.830700)

Rovatti, R., Mazzini, G. & Setti, G. 2004 On the ultimate limits of chaos-based asynchronous DS-CDMA—ii: analytical results and asymptotics. *IEEE Trans. Circuits Syst. I* **51**, 1348–1364. (doi:10.1109/TCSI.2004.830698)

Setti, G., Balestra, M. & Rovatti, R. 2000 Experimental verification of enhanced electromagnetic compatibility in chaotic FM clock signals. *Proc. ISCAS’00* **3**, 229–232.

Setti, G., Mazzini, G., Rovatti, R. & Callegari, S. 2002 Statistical modeling of discrete-time chaotic processes: basic finite-dimensional tools and applications. *Proc. IEEE* **90**, 662–689. (doi:10.1109/JPROC.2002.1015001)

Shan, X., Xia, Y., Ren, Y. & Yuan, J. 2006 Spatiotemporal chaotic spreading sequences for CDMA communications. *Commun. Tech. Proc.* **1**, 530–535.

Stojanovski, T. & Kocarev, L. 2001 Chaos-based random number generators: I. Analysis. *IEEE Trans. Circuits Syst. I* **48**, 281–288.

Wackerbauer, R., Witt, A., Atmanspacher, H., Kurths, J. & Scheingraber, H. 1994 A comparative classification of complexity measures. *Chaos Soliton. Fract.* **4**, 133–173. (doi:10.1016/0960-0779(94)90023-X)

Zunino, L., Pérez, D. G., Martín, M. T., Plastino, A., Garavaglia, M. & Rosso, O. A. 2007 Characterization of Gaussian self-similar stochastic processes using wavelet-based informational tools. *Phys. Rev. E* **75**, 021115. (doi:10.1103/PhysRevE.75.021115)

Zunino, L., Pérez, D. G., Martín, M. T., Garavaglia, M., Plastino, A. & Rosso, O. A. 2008 Permutation entropy of fractional Brownian motion and fractional Gaussian noise. *Phys. Lett. A* **372**, 4768–4774. (doi:10.1016/j.physleta.2008.05.026)