ELSEVIER

Physica A 316 (2002) 259–288

PHYSICA A

www.elsevier.com/locate/physa

Chaos-induced true randomness

J.A. González[a,b,*], L.I. Reyes[a,b,c], J.J. Suárez[b,c], L.E. Guerrero[c], G. Gutiérrez[c]

[a] *The Abdus Salam International Centre for Theoretical Physics, Strada Costiera 11, 34100, Trieste, Italy*

[b] *Centro de Física, Instituto Venezolano de Investigaciones Científicas, Apartado Postal 21827, Caracas 1020-A, Venezuela*

[c] *Departamento de Física, Universidad Simón Bolívar, Apartado Postal 89000, Caracas 1080-A, Venezuela*

Received 24 September 2001; received in revised form 6 March 2002

Abstract

We investigate functions of type $X_n = P(\theta z^n)$, where $P(t)$ is a periodic function, θ and z are real parameters. We show that these functions produce truly random sequences. We prove that a class of autonomous dynamical systems, containing nonlinear terms described by periodic functions of the variables, can generate random dynamics. We generalize these results to dynamical systems with nonlinearities in the form of noninvertible functions. Several examples are studied in detail. We discuss how the complexity of the dynamics depends on the kind of nonlinearity. We present real physical systems that can produce random time-series. We report the results of real experiments using nonlinear circuits with noninvertible I–V characteristics. In particular, we show that a Josephson junction coupled to a chaotic circuit can generate unpredictable dynamics.

PACS: 05.45.−a; 02.50.Ey; 05.40.−a; 05.45.Tp

Keywords: Choatic systems; Random systems; Experimental chaos

1. Introduction

Nonlinear dynamics has provided new theoretical and conceptual tools that allow us to understand many complex behaviors that appear in almost every field of

* Corresponding author. Centro de Física, Inst. Venezolano de Invest. Científicas, Apartado 21827, 1020 Caracas, Venezuela. Fax: +58-212-504-1148.

E-mail address: jorge@pion.ivic.ve (J.A. González).

0378-4371/02/$ - see front matter
PII: S0378-4371(02)01031-2

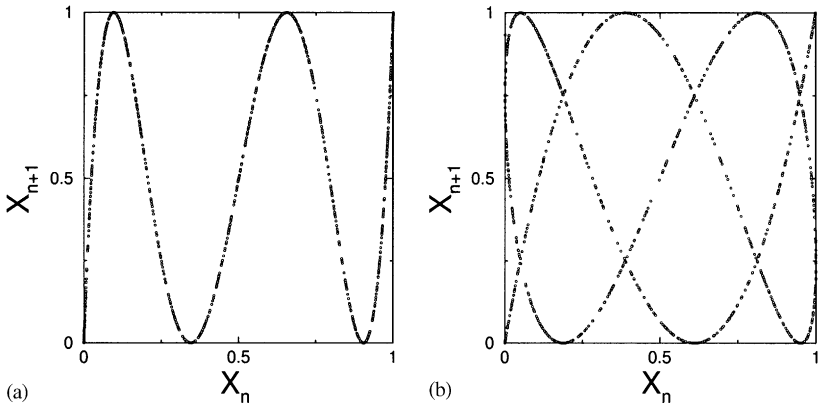


Fig. 1. First-return maps produced by function (1): (a) $z = 5$; (b) $z = 7/3$.

contemporary science [1–10]. In the chaotic regime, the behavior of a deterministic system appears random. This finding has forced many experimentalists to re-examine their data to determine whether some of the random behaviors attributed to noise are due to deterministic chaos instead.

Chaos theory has been successfully applied to many scientific and practical situations [1–10].

In the philosophical realm, however, the importance of this development was that chaos theory seemed to offer scientists the hope that almost "any" random behavior observed in Nature could be described using low-dimensional chaotic systems. Random-looking information gathered in the past (and shelved because it was assumed to be too complicated) perhaps could now be explained in terms of simple laws.

The known chaotic systems are not random [11]. If the previous values of a time-series determine the future values, then even if the dynamical behavior is chaotic, the future may, to some extent, be predicted from the behavior of past values that are similar to those of the present. The so-called "unpredictability" in the known chaotic systems is the result of the sensitive dependence on initial conditions. It is not an absolute unpredictability.

Truly random systems are different from the chaotic ones. Past sequences of values of a random dynamical variable that are similar to present ones tell as much or little about the next value as about the next hundredth value. The so-called nonlinear forecasting methods for distinguishing chaos from random time-series are based on these ideas [11].

Recently, we have introduced explicit functions that produce truly random sequences [12–14]. For instance, let us define the function:

$$X_n = \sin^2(\theta \pi z^n), \tag{1}$$

where z is a real number and θ is a parameter.

For an integer $z > 1$, this is the solution to some chaotic maps [12–14] (see Fig. 1(a)). For a noninteger z, function (1) can produce truly unpredictable random sequences whose values are independent.

Functions (1) with noninteger z cannot be expressed as a map of type

$$X_{n+1} = f(X_n, X_{n-1}, \ldots, X_{n-r+1}) . \tag{2}$$

In the present letter we address the following question: can an autonomous dynamical system with several variables produce a random dynamics similar to that of function (1)? We will present several dynamical systems with this kind of behavior. We will report the results of real experiments with nonlinear circuits, which contain direct evidence for this new phenomenon. We discuss some applications.

2. Random sequences

Let us discuss first some properties of function (1). We will present here a short proof of the fact that the sequences generated by functions (1) are unpredictable from the previous values. This proof is presented here for the first time. However, a more detailed discussion of the properties of these functions (including statistical tests) can be found in Refs. [12–14].

Let z be a rational number expressed as $z = p/q$, where p and q are relative prime numbers.

We are going to show that if we have $m+1$ numbers generated by function (1): X_0, X_1, X_2, $X_3, \ldots, X_m$ (m can be as large as we wish), then the next value X_{m+1} is still unpredictable. This is valid for any string of $m+1$ numbers.

Let us define the following family of sequences:

$$X_n^{(k,m)} = \sin^2\left[\pi(\theta_0 + q^m k)\left(\frac{p}{q}\right)^n\right] , \tag{3}$$

where k is an integer. The parameter k distinguishes the different sequences. For all sequences parametrized by k, the first $m+1$ values are the same. This is so because

$$X_n^{(k,m)} = \sin^2\left[\pi\theta_0\left(\frac{p}{q}\right)^n + \pi k p^n q^{(m-n)}\right] = \sin^2\left[\pi\theta_0\left(\frac{p}{q}\right)^n\right] , \tag{4}$$

for all $n \leqslant m$. Note that the number $k p^n q^{(m-n)}$ is an integer for $n \leqslant m$. So we can have infinite sequences with the same first $m+1$ values.

Nevertheless, the next value

$$X_{m+1}^{(k,m)} = \sin^2\left[\pi\theta_0\left(\frac{p}{q}\right)^{m+1} + \frac{\pi k p^{m+1}}{q}\right] \tag{5}$$

is uncertain.

In general, $X_{m+1}^{(k,m)}$ can take q different values. These q values can be as different as 0, $1/2$, $\sqrt{2}/2$, $1/e$, $1/\pi$, or 1. From the observation of the previous values X_0, X_1, X_1, X_2, $X_3, \ldots, X_m$, there is no method for determining the next value.

This result shows that for a given set of initial conditions, there exists always an infinite number of values of θ that satisfy those initial conditions. The time-series produced for different values of θ satisfying the initial conditions is different in most of the cases. Even if the initial conditions are exactly the same, the following values

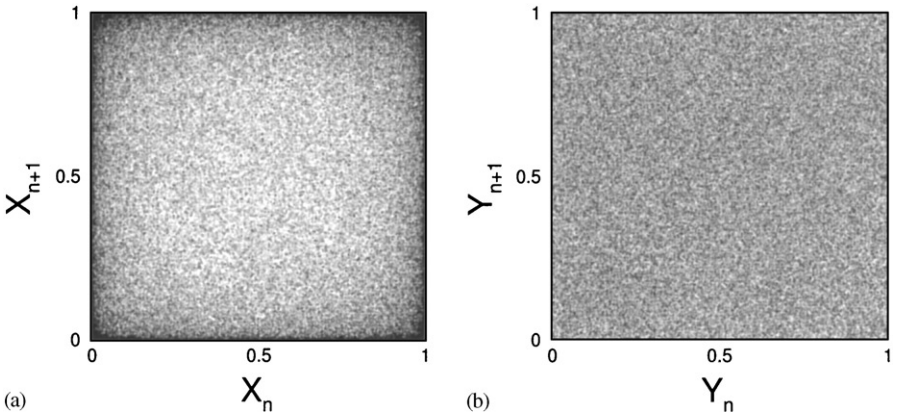


Fig. 2. First-return maps produced by function (1): (a) $z = e$ (irrational); (b) $z = e$, $Y_n = (2/\pi)\arcsin(X_n^{1/2})$.

Table 1
Representation of matrix $X_n^{(k,m)}$ given by Eq. (3) with m fixed ($m = 3$, $p/q = 4/3$, $\theta_0 = 1.581$)

	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$
X_0	0.9366	0.9366	0.9366	0.9366	0.9366	0.9366	0.9366
X_1	0.1107	0.1107	0.1107	0.1107	0.1107	0.1107	0.1107
X_2	0.3139	0.3139	0.3139	0.3139	0.3139	0.3139	0.3139
X_3	0.5076	0.5076	0.5076	0.5076	0.5076	0.5076	0.5076
X_4	0.0001	0.7410	0.7588	0.0001	0.7410	0.7588	0.0001
X_5	0.7617	0.9650	0.3997	0.0001	0.4266	0.9743	0.7380
X_6	0.1289	0.9274	0.6258	0.0003	0.6607	0.9074	0.1055

Note that, in each column, the first values are the same. However, the next values can be different. X_4 can take three different values.

are completely different. This property is, in part, related to the fact that the equation $\sin^2\theta = \alpha$, where $0 \leqslant \alpha \leqslant 1$, possesses infinite solutions for θ.

We should stress that from the observation of a string of values X_0, X_1, X_2, $X_3,\ldots$, X_m generated by function (1) it is impossible to determine which value of θ was used.

Figs. 1(a) and (b) show the first-return maps for $z = 5$ and $z = 7/3$.

For z irrational (we exclude the numbers of type $z = m^{1/k}$), the numbers generated by function (1) are completely independent (see Fig. 2(a) that shows the first-return map for $z = e$). After any string of $m + 1$ numbers X_0, X_1, X_2, $X_3,\ldots,X_m$, the next outcome X_{m+1} can take infinite different values.

Some of the results presented in this section can be illustrated using Tables 1–4. These tables are finite representations of the infinite matrices $X_n^{(k,m)}$ (defined by Eq. (3)) for m fixed. The columns are the sequences X_0, X_1, $X_2,\ldots,X_n,\ldots$ for a given $\theta = \theta_0 + q^m k$. Parameter θ can be changed when we change k. The parameter θ has been defined in such a way that for different k we have a family of sequences X_n with the same first $m + 1$ values.

Table 2
Representation of matrix $X_n^{(k,m)}$ given by Eq. (3) with m fixed ($m=5,\ p/q=4/3,\ \theta_0=1.581$)

	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$
X_0	0.9366	0.9366	0.9366	0.9366	0.9366	0.9366	0.9366
X_1	0.1107	0.1107	0.1107	0.1107	0.1107	0.1107	0.1107
X_2	0.3139	0.3139	0.3139	0.3139	0.3139	0.3139	0.3139
X_3	0.5076	0.5076	0.5076	0.5076	0.5076	0.5076	0.5076
X_4	0.0001	0.0001	0.0001	0.0001	0.0001	0.0001	0.0001
X_5	0.7617	0.7617	0.7617	0.7617	0.7617	0.7617	0.7617
X_6	0.1289	0.3953	0.9757	0.1289	0.3953	0.9757	0.1289
X_7	0.2212	0.6199	0.5532	0.2799	0.8603	0.0428	0.9988
X_8	0.3690	0.0258	0.6860	0.9524	0.2613	0.0752	0.7880

Note that, in each column, the first values are the same. However, the next value X_6 can be as different as $0.1289\ldots, 0.3953\ldots$, or $0.9757\ldots$. If we increase m, we can have strings of any length, and still, the next value is unpredictable.

Table 3
Representation of matrix $X_n^{(k,m)}$ given by Eq. (3) with m fixed ($m=4,\ p/q=7/5,\ \theta_0=1.581$)

	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$
X_0	0.9366	0.9366	0.9366	0.9366	0.9366	0.9366	0.9366
X_1	0.3860	0.3860	0.3860	0.3860	0.3860	0.3860	0.3860
X_2	0.0932	0.0932	0.0932	0.0932	0.0932	0.0932	0.0932
X_3	0.7632	0.7632	0.7632	0.7632	0.7632	0.7632	0.7632
X_4	0.0524	0.0524	0.0524	0.0524	0.0524	0.0524	0.0524
X_5	0.9999	0.0900	0.6634	0.6455	0.1010	0.9999	0.0900
X_6	0.0878	0.1712	0.2752	0.3933	0.5182	0.6419	0.7566
X_7	0.7521	0.0009	0.8036	0.6608	0.0172	0.8768	0.5630

Note that, in all columns, the first 5 values are the same. However, the next outcome X_5 can take five different values.

Table 4
Representation of matrix $X_n^{(k,m)}$ given by Eq. (3) with m fixed ($m=6,\ p/q=7/5,\ \theta_0=1.581$)

	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$
X_0	0.9366	0.9366	0.9366	0.9366	0.9366	0.9366	0.9366
X_1	0.3860	0.3860	0.3860	0.3860	0.3860	0.3860	0.3860
X_2	0.0932	0.0932	0.0932	0.0932	0.0932	0.0932	0.0932
X_3	0.7632	0.7632	0.7632	0.7632	0.7632	0.7632	0.7632
X_4	0.0524	0.0524	0.0524	0.0524	0.0524	0.0524	0.0524
X_5	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999
X_6	0.0878	0.0878	0.0878	0.0878	0.0878	0.0878	0.0878
X_7	0.7521	0.5497	0.1672	0.9885	0.0422	0.7521	0.5497
X_8	0.7469	0.8473	0.9258	0.9776	0.9994	0.9897	0.9493
X_9	0.7542	0.9956	0.8582	0.4470	0.0763	0.0294	0.3421

Note that, in all columns, the first 7 values are the same. However, the next outcome X_7 can take five different values. In fact, for any string of length $m+1$, produced by function (3), with given $z=p/q$ and θ, there are infinite other strings with the same $m+1$ values. However, the next value X_{m+1} can take q different values. From the observation of the previous values, it is impossible to predict the next one.

In Table 1 ($p/q=4/3$, $m=3$), we see that all the column-sequences possess exactly the same first 4 values. However, the next values can be different. It can take 3 different values.

In Table 2 ($p/q=4/3$, $m=5$), all the column-sequences possess exactly the same first 6 values. Nevertheless, the next values are uncertain. Again there are three different possible values.

In Table 3 ($p/q=7/5$, $m=4$) and Table 4 ($p/q=7/5$, $m=6$), the same phenomenon can be observed. In this case, there are always 5 possible values. Knowing only the previous values, it is impossible to say which the next is.

For any given string of sequence-values X_0, X_1, $X_2,\ldots,X_m$, we can always find infinite values of θ such that the corresponding sequences can possess this same string of $m+1$ values, but the next values can be different.

The numbers produced by function (1) are random but are not distributed uniformly. The probability density behaves as $P(X) \sim 1/\sqrt{X(1-X)}$. If we need uniformly distributed random numbers, we should make the following transformation $Y_n = 2/\pi \arcsin\sqrt{X_n}$. In this case $P(Y) = \text{const}$ (see Fig. 2(b)).

3. Generalized random functions

It is important to mention here that the argument of function (1) does not need to be exponential all the time, for $n \to \infty$. In fact, a set of finite sequences (where each element-sequence is unpredictable, and the law for producing a new element-sequence cannot be obtained from the observations) can form an infinite unpredictable sequence. See the discussion in the following paragraph.

So if we wish to produce random sequences of very long length, we can determine a new value of parameter θ after a finite number N of values of X_n. This procedure can be repeated the desired number of times. It is important to have a nonperiodic method for generating the new value of θ. For example, we can use the following method in order to change the parameter θ after each set of N sequence values. Let us define $\theta_s = AW_s$, where W_s is produced by a chaotic map of the form $W_{s+1} = f(W_s)$; s is the order number of θ in a way that $s=1$ corresponds to the θ used for the first set of N values of X_n, $s=2$ for the second set, etc. The inequality $A > 1$ should hold to ensure the absolute unpredictability. In this case, from the observation of the values X_n, it is impossible to determine the real value of θ.

After a carefully analysis of functions (1), we arrive at the preliminary conclusion that (to produce unpredictable dynamics) the main characteristics for any functions are the following: the function should be able to be re-written in the form

$$X_n = h\,(f(n))\,, \tag{6}$$

where the argument function $f(n)$ grows exponentially and the function $h(y)$ should be finite and periodic. This result allows us to generalize this behavior to other functions as the following

$$X_n = P\,(\theta z^n)\,, \tag{7}$$

where $P(t)$ is a periodic function.

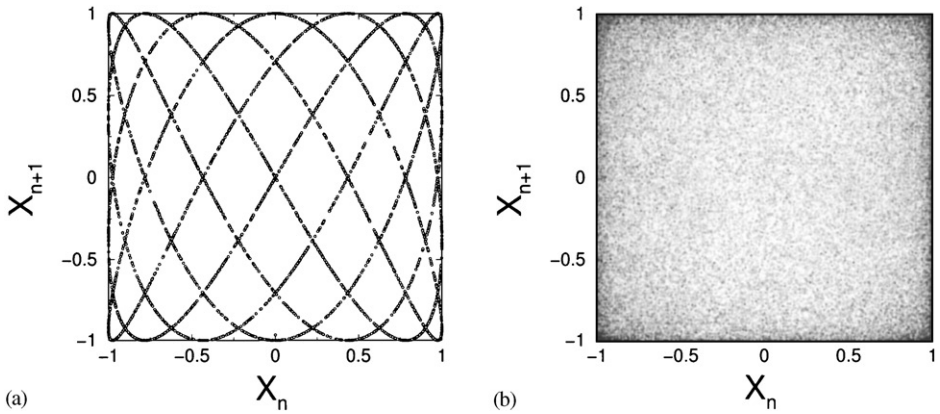


Fig. 3. First-return maps produced by function (8): (a) $z = 7/4$; (b) $z = e$.

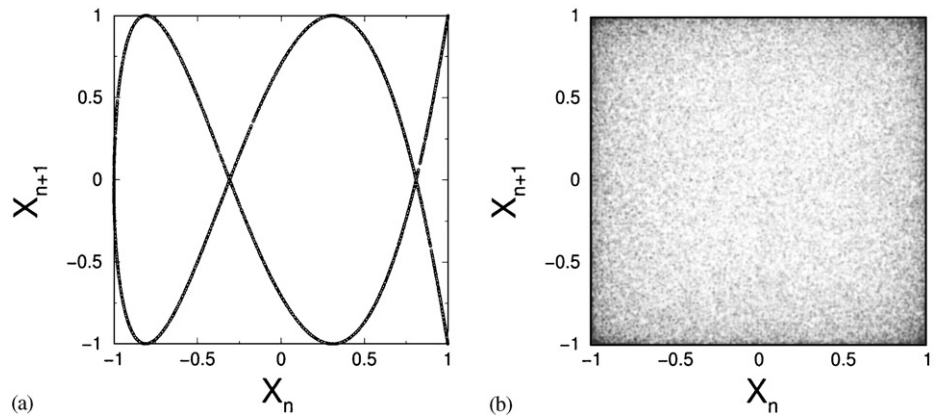


Fig. 4. First-return maps produced by function (9): (a) $z = 5/2$; (b) $z = \pi/2$.

So there is nothing special in function $X_n = \sin^2(\theta\pi z^n)$.

Let us see some examples of functions of type $X_n = P(\theta z^n)$.

The first-return maps produced by function

$$X_n = \sin(2\theta\pi z^n) \tag{8}$$

is shown in Fig. 3.

Note that in this case (if $z = p/q$) for a given X_n, we have $2q$ possible values for X_{n+1}; and for a given X_{n+1}, we have $2p$ possible values of X_n.

A different first-return map (see Fig. 4) can be generated by function

$$X_n = \cos(2\theta\pi z^n)\,. \tag{9}$$

The distribution functions of Eqs. (3) and (4) are peaked at points $X_n = 0$ and $X_n = 1$.

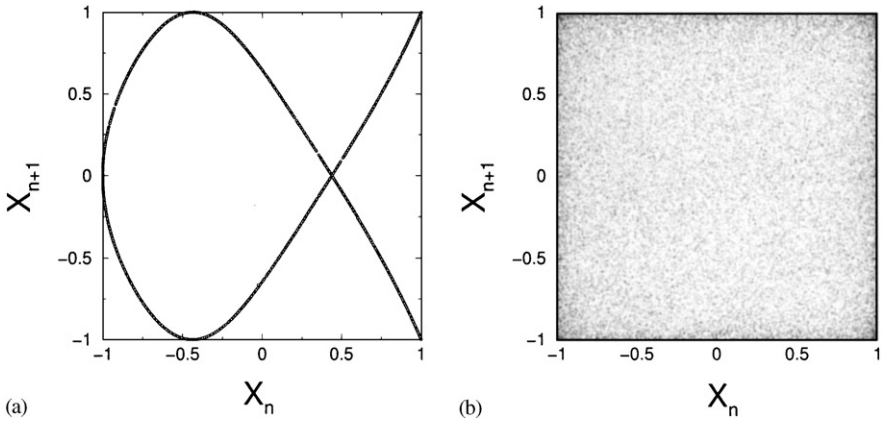


Fig. 5. First-return maps produced by function (10) ($k = 0.5$): (a) $z = 3/2$; (b) $z = \pi/3$.

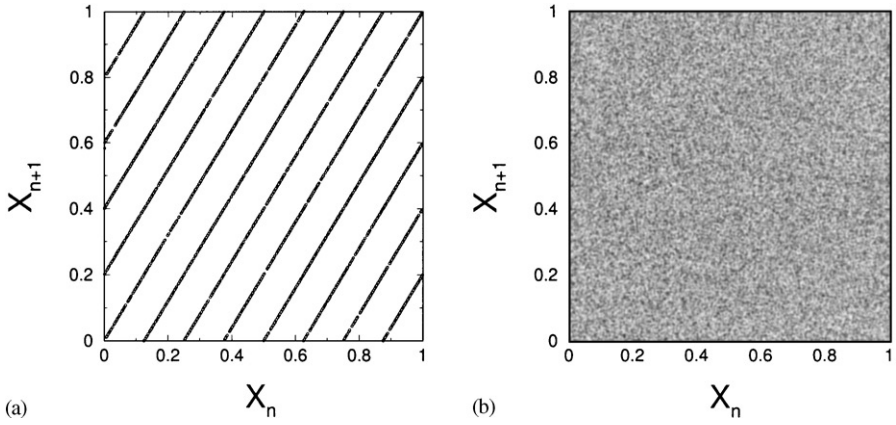


Fig. 6. First-return maps produced by function (11): (a) $z = 8/5$; (b) $z = e/2$.

A generalization of the trigonometric functions (elliptic functions)

$$X_n = cn(\theta z^n, k)\,. \tag{10}$$

is also good for the construction of stochastic functions (see Fig. 5).

These functions can be used for many algebraic manipulations that can lead to the solution of different stochastic problems.

A very special stochastic function is the following:

$$X_n = \theta z^n \,(\mathrm{mod}\, 1)\,. \tag{11}$$

In Fig. 6 we can find the first-return maps.

Function (11) can produce uniformly distributed random numbers.

Interesting first-return maps can be generated by a superposition of several periodic functions $P_1(t)$, $P_2(t)$, ... with the argument function $t = \theta z^n$. See, for instance, the

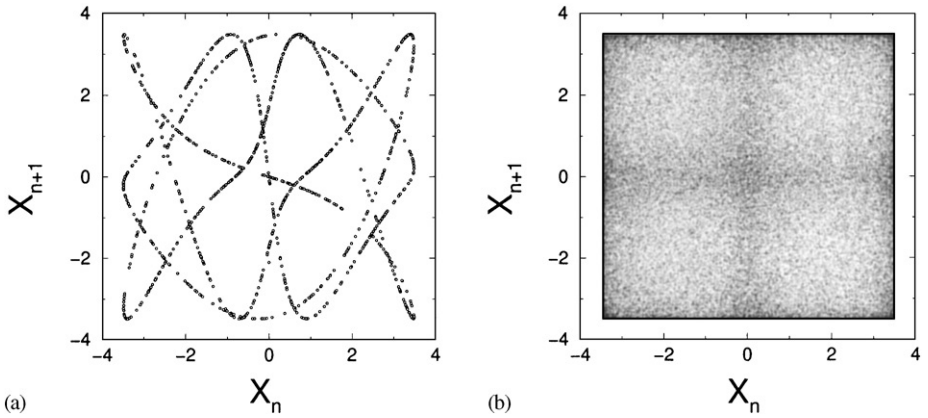


Fig. 7. First-return maps produced by function (12): ($a = 1,\ b = c = 3;\ d = 3/2$): (a) $z = 5/3$; (b) $z = \pi/3$.

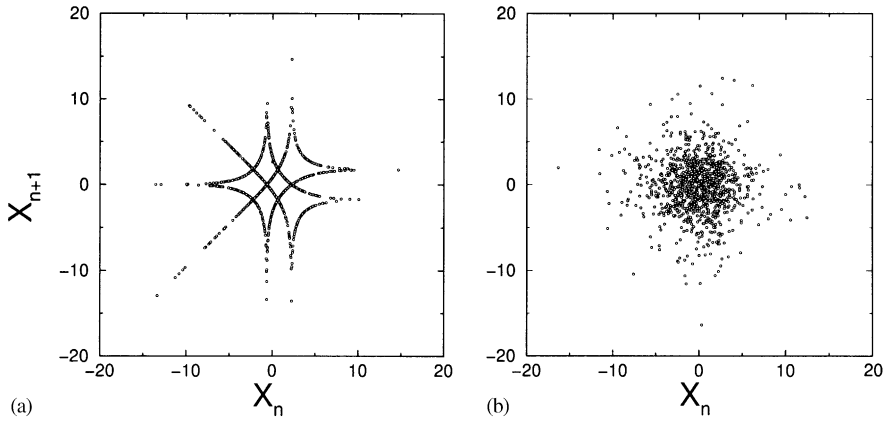


Fig. 8. First-return maps produced by function (13): (a) $z = 5/4$; (b) $z = e$.

maps generated by function

$$X_n = a \sin\,(c\theta\pi z^n) + b \sin(\mathrm{d}\theta\ \pi z^n)\,, \tag{12}$$

in Fig. 7.

Note that in all these cases, even if for rational z we can have some structure in the first-return maps, for irrational z the dynamics is structureless.

Another very important stochastic function is the following:

$$X_n = \ln\,[\tan^2(\theta\pi z^n)]\,. \tag{13}$$

The outcomes produced by this function are distributed following a Gaussian-like law (this can be obtained analytically).

It is interesting that the distribution of the sequences shown in Figs. 8 (a) and (b) are the same. However, the actual dynamics is very different. In the case $z = e$, this

dynamics is very similar to Gaussian white noise. In the case $z=5/4$, when X_n is close to the point $X_n=0$, we can say that, for any string of values X_k, X_{k+1}, $X_{k+2},\ldots,X_{k+m}$, there are always 4 different possible next values. However, unlike the case $z=e$, for $z=5/4$, we can know these possible 4 values for each X_n (although, before the outcome, we will not know which of the 4 values will be produced). Even more interesting is this: although the distribution is symmetric (the mean value is $X=0$), the dynamics is not symmetric. For large values of X_n (say $X_n>10$), we can say that there are two possible next values.

In this case, the uncertainty is less than in a neighborhood of $X_n=0$. However, for $X_n<-10$, there are always three possible values. And these three values diverge for $X_n\to\infty$.

We will see in Sections 6 and 7 that physical systems can be constructed such that the dynamics of these functions can be realized in practice. In some cases this can be done when we have a many-component chaotic system and some of the chaotic dynamical variables are transformed by the nonlinear dynamics of other variables. Using different nonlinearities, different dynamical behaviors can be produced. For instance we can obtain some of the dynamics shown in Figs. 3–7.

This theory can help to predict the general behavior of some nonlinear systems. Moreover, in special cases some random systems can be more predictable than others.

We should say that a more deep analysis shows that (to produce complex behavior) the function $f(n)$ in Eq. (6) does not have to be exponential all the time, and function $h(y)$ does not have to be periodic. In fact, it is sufficient for function $f(n)$ to be a finite nonperiodic oscillating function which possesses repeating intervals with finite exponential behavior. For instance, this can be a chaotic function. On the other hand, function $h(y)$ should be noninvertible. In other words, it should have different maxima and minima in such a way that equation $h(y)=\alpha$ (for some specific interval of α, $\alpha_1<\alpha<\alpha_2$) possesses several solutions for y.

To conclude this section we will present a random function of type (7) constructed with a nonperiodic function $P(t)$, where the argument t is defined as $t=\theta z^n$.

Let us define $P(t)$ as:

$$P(t)=\sin\{B_1\sinh[a_1\cos(\omega_1 t)+a_2\cos(\omega_2 t)]+B_2\cosh[a_3\cos(\omega_3 t)+a_4\cos(\omega_4 t)]\}, \tag{14}$$

where $B_1=20$, $B_2=30$, $a_1=10$, $a_2=15$, $a_3=10$, $a_4=15$, $\omega_1=1$, $\omega_2=\pi$, $\omega_3=\sqrt{2}$, $\omega_4=e$.

Although this function is composed of quasiperiodic functions, its behavior can be very complicated (see Fig. 9).

Fig. 10 shows the dynamics of function $P(\theta z^n)$, where $P(t)$ is given by Eq. (14).

4. Pseudorandom number generators

There is a large literature dedicated to pseudorandom number generators and their applications (see e.g. Refs. [15–38,43–50] and references quoted therein). A very fine

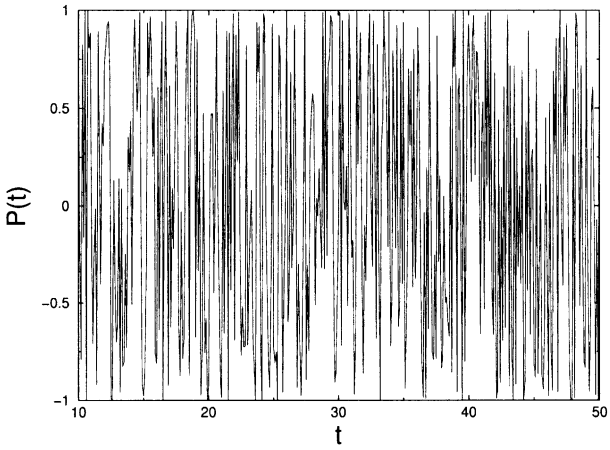


Fig. 9. The function (14) can appear very complex.

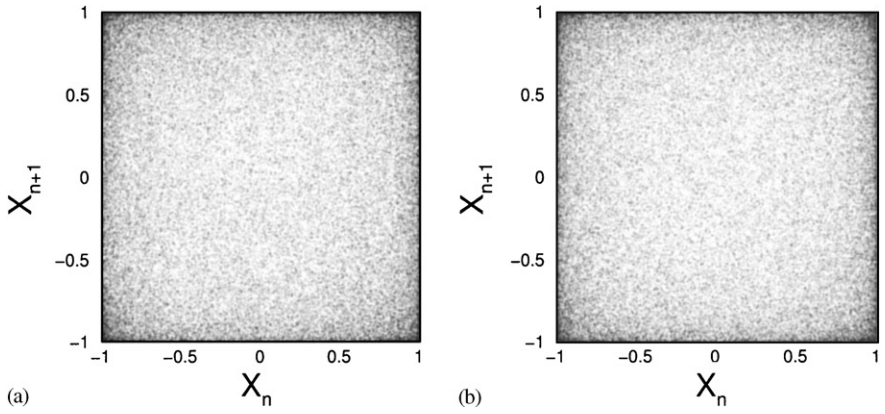


Fig. 10. First-return maps produced by function $X_n = P(\theta z^n)$, where $P(t)$ is the function given by Eq. (14): (a) $z = \pi$; (b) $z = 7/5$. Note that the dynamics is structureless in both cases.

theory has been developed in this area and this theory has produced many important results.

However, we should say here that the known pseudorandom number generators are not supposed to generate truly random numbers.

In his important review article [21], James says: "Truly random numbers are unpredictable in advance and must be produced by a random physical process, such as radioactive decay".

In fact, pseudorandom numbers are produced using recurrence relations, and are therefore not truly random [21,22,28–30,37].

D'Souza et al. [28] say in their paper: "Pseudorandom number generators are at best a practical substitute, and should be generally tested for the absence of undesired correlations".

Many known pseudorandom number generators are based on maps of type:

$$X_{n+1} = f(X_n, X_{n-1}, \ldots, X_{n-r+1}) . \tag{15}$$

Now we will present the maps behind some of the most famous and best pseudorandom number generators.

Multiplicative linear congruential generators [15,21] are defined by the following equation:

$$X_{n+1} = (aX_n + c) \bmod m . \tag{16}$$

Some famous values for these parameters are the following: $a = 23, m = 10^8 + 1, c = 0; a = 65,539, m = 2^{29}, c = 0; a = 69,069, m = 2^{32}, c = 1; a = 16,807, m = 2^{31} - 1, c = 0; a = 1,664,525, m = 2^{32}, c = 0$ (this is the best generator for $m = 2^{32}$, according to the criteria of Knuth [24]).

The *Fibonacci-like generators* obey the following equation:

$$X_{n+1} = (X_{n-p} \odot X_n - q) \bmod m , \tag{17}$$

where $\odot$ is some binary or logical operation. For instance, $\odot$ can be addition, subtraction or exclusive-or.

Other *extended algorithms* use equations as the following:

$$X_{n+1} = (aX_n + bX_{n-1} + c) \bmod m . \tag{18}$$

The *add-and-carry generators* are defined as

$$X_{n+1} = (X_{n-r} \pm X_{n-s} \pm c) \bmod m . \tag{19}$$

Among the high quality generators investigated in the famous paper [15] are the following:

$$X_{n+1} = (16807X_n) \bmod (2^{31} - 1) , \tag{20}$$

$$X_{n+1} = (X_{n-103} .XOR. X_{n-250}) , \tag{21}$$

$$X_{n+1} = (X_{n-1063} .XOR. X_{n-1279}) , \tag{22}$$

where *.XOR.* is the bitwise exclusive OR operator,

$$X_n = (X_{n-22} - X_{n-43} - c) , \tag{23}$$

here for $X_n \geqslant 0$, $c = 0$, and for $X_n < 0$, $X_n = X_n + (2^{32} - 5)$, $c = 1$.

We should say here that many of these generators are used or investigated in some very good and very recent papers about pseudorandom number generators [16,20,34,35, 39–42].

All known generators (in some specific physical calculations) give rise to incorrect results because they deviate from randomness [15,28,29,16,20,34].

The problem is that these algorithms are predictable.

An example of this can be found in the work of Ferrenberg et al. [15]. They found that high quality pseudorandom number generators can yield incorrect answers due to subtle correlations between the generated numbers.

Suppose we have an ideal generator for truly random numbers. In this case, no matter how many numbers we have generated, the value of the next number will be still unknown. That is, there is no way to write down a formula that will give the value of the next number in terms of the previous numbers, no matter how many numbers have been already generated.

The authors of paper [15] related the errors in the simulations to the dependence in the generated numbers. Indeed, they are all based on maps of type (15).

Recently, new methods for pseudorandom number generation have been developed [22,23,37,43–48]. Many of them are based on chaotic systems. These generators can also be a source of systematic errors when some physical calculations are performed.

In Ref. [47], it is shown that although the Marsaglia–Zaman generator is chaotic, that is not enough, because the Lyapunov exponent is not big enough to eliminate all correlations. In fact, it can be shown that even if the Lyapunov exponent is very large, there will always exist correlations between the generated values.

A sequence of pseudorandom numbers with significantly better statistical properties is obtained by keeping only a fraction of the full sequence of numbers produced by Marsaglia–Zaman algorithm (the improved generator is described in Refs. [47–49]).

In Ref. [37] a similar procedure is applied to a generator based on the logistic map.

We should say that, using this method it is possible to produce a map with a very large Lyapunov exponent. However, it is still a map of type $X_{n+1} = f(X_n, X_{n-1}, \ldots, X_{n-r+1})$. Thus, the future values are defined by the past values in a deterministic way.

In the present paper, we have shown that the sequence of numbers Y_n defined by function (1) after transformation $Y_n = 2/\pi \arcsin \sqrt{X_n}$ and the sequence of numbers X_n defined by the function (11) cannot be expressed as a map of type (15) and are uniformly distributed. In fact, these numbers are unpredictable and the next value cannot be determined as a function of the previous values.

Now we will resort to two important measures that recently have been used successfully for the characterization of stochastic sequences and pseudorandom number generators [51–57,38].

First, we should explain how we produced the numbers that we are going to investigate.

The numbers are produced using the equation

$$X_n = \theta_0 z^n \,(\mathrm{mod}\, 1)\,, \tag{24}$$

where $z = \pi$. A given number N of values of X_n is generated in this way. Then, a new value for θ is produced through the formula $\theta_1 = AX_1$, where $A > 1$, and X_1 had been obtained from Eq. (24). Using again Eq. (24) with this new $\theta = \theta_1$, a new string of N values is generated. After that, new values for θ are produced following the formula $\theta_k = AX_k$, and new strings of N values for X_n are generated.

Mutual information I is a measure of the interdependence between two variables [51]. I is more general than a correlation function because the latter can characterize only linear dependence between the variables. Suppose we have two time-series in the form

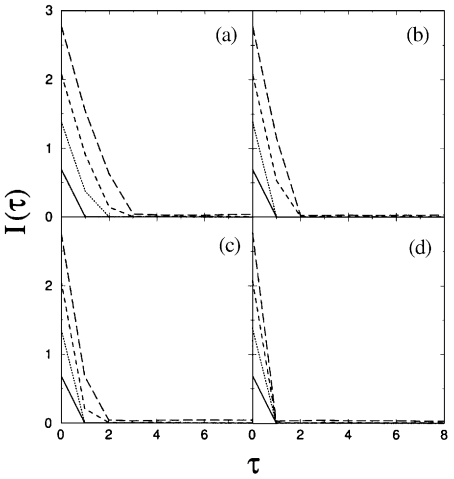


Fig. 11. Mutual information $I(\tau)$ for sequences produced by function (24) using different values of z. For each z, I is shown for different values of b. (a) $z = 3/2$, (b) $z = 4/3$, (c) $z = 7/6$, (d) $z = \pi$. In all these figures: solid line is for $b = 2$, dotted line is for $b = 4$, dashed line is for $b = 8$, and long-dashed line is for $b = 16$.

$s_1, s_2, \ldots, s_N$, and $q_1, q_2, \ldots, q_N$, then the mutual information between the observations s_i and q_j is defined as follows:

$$I_{s,q}(s_i, q_j) = \log_2 \left[\frac{P_{s,q}(s_i, q_j)}{P_s(s_i)\, P_q(q_j)} \right] , \tag{25}$$

where $P_{s,q}(s_i, q_j)$ is the joint probability density of s and q evaluated at (s_i, q_j), $P_s(s_i)$ and $P_q(q_j)$ are the marginal probabilities of s and q evaluated at s_i and q_j, respectively.

The average mutual information is then defined:

$$\bar{I}_{s,q}(s_i, q_j) = -\sum_{ij} P_{s,q}(s_i, q_j) \log_2 \left[\frac{P_{s,q}(s_i, q_j)}{P_s(s_i) P_q(q_j)} \right] . \tag{26}$$

If we wish to characterize one time-series, then the relevant measure is

$$I(\tau) = -\sum_{i,j} p_{ij}(\tau) \ln \frac{p_{ij}(\tau)}{p_i\, p_j} , \tag{27}$$

where, for a given partition of real numbers, p_i is the probability of finding a value of the time-series in the ith interval, and $p_{ij}(\tau)$ is the joint probability of finding an observation in the ith interval and (at time τ in the future) finding an observation in the jth interval.

Fig. 11 shows $I(\tau)$ calculated using different interval partitions (e.g. $b = 4$ implies that the interval has been divided in 4 parts) for time-series generated by function $X_n = \theta z^n \pmod 1$.

Results are shown for $z = 3/2$, $z = 4/3$, $z = 7/6$ and $z = \pi$. Note that when $z = \pi$, for any interval partition, $I(\tau = 1) = 0$. This is a test for the absence of correlations between the values of the sequence.

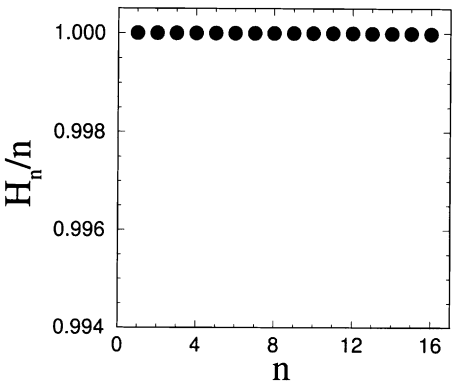


Fig. 12. H_n/n is calculated for sequences produced by function (24) with $z = \pi$.

Another important measure is the so-called "block entropy" H_n. Given a sequence of symbols in an alphabet of m characters, we define sequences considering blocks of size n, where $n = 1, 2, \ldots$. Then we calculate the probability p_b of occurrence of any of the m^n possible blocks. The mathematical formula for H_n is

$$H_n = -\sum p_b \log_m p_b \, . \tag{28}$$

In the case of a uniformly distributed random sequence, where all the possible blocks should be observed with equal probability, $H_n = n$ [56,57].

This test has been used very recently [56,57] to characterize pseudorandom number generators. If we plot H_n/n vs. n for a uniformly distributed random sequence we should get $H_n/n = 1$. Fig. 1 of Ref. [56] shows H_n/n for sequences produced by a currently accepted "very good" pseudorandom number generator [48]. Such figure shows that H_n/n decays after $n = 10$. After that, H_n/n is a rapidly decaying function.

In Fig. 12, we show the calculation of H_n/n using our random numbers. We should say that the calculation depends on the number of values in the sequences. In order to keep $H_n/n \approx 1$, we should increase the length of the sequences. With our generator this process works, because for any length the sequence is still random. For any other generator, if we try to increase the length of the sequence, the correlations will be stronger. So this process will not help in providing a better performance for function H_n/n.

Recently, simulations of different physical systems have become the "strongest" tests for pseudorandom number generators. Among these systems are the following: the two-dimensional Ising model [15], ballistic deposition [28], random walks [29], and percolation [50].

Nogués et al. [29] have found that using common pseudorandom number generators, the produced random walks present symmetries, meaning that the generated numbers are not independent.

On the other hand, the logarithmic plot of the mean distance versus the number of steps N is not a straight line (as expected theoretically) after $N > 10^5$ (in fact, it is a rapidly decaying function).

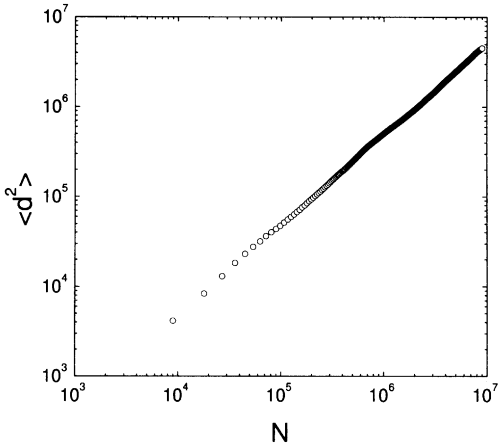


Fig. 13. Mean distance vs. number of steps for a random walk generated with the random numbers $Y_n = (2/\pi)$ arcsin $(X_n^{1/2})$, where X_n is given by function $X_n = \sin^2(\theta\pi z^n)$.

D'Souza et al. [28] use ballistic deposition to test the randomness of pseudorandom number generators. They found correlations in the pseudorandom numbers and strong coupling between the model and the generators (even very recently invented generators that pass extensive statistical tests).

One consequence of the Kardar–Parisi–Zhang theory is that the steady-state behavior for the interface fluctuations (in ballistic deposition in one dimension) should resemble a random walk. Thus, a random walk again serves as a good test for pseudorandom numbers.

We have produced random walks using the numbers generated by our systems. The produced random walks possess the correct properties, including the mean distance behavior $\langle d^2 \rangle \sim N$ (see Fig. 13).

The present paper is not about random number generators. In the present paper we discuss a new phenomenon: the fact that unperturbed physical systems can produce truly random dynamics.

Of course, one of the applications of this phenomenon is random number generation.

The art of random number generation requires more than the randomness of the generated numbers. It requires good programming skills and techniques to obtain the desired distributions for the numbers.

The functions and systems described in this paper can be used to create very good random number generators. Algorithms designed for this purpose along with the statistical tests will be published elsewhere.

In this section we only wished to present a theoretical comparison between the sequences produced by some well-known pseudorandom number generator algorithms and the systems described in the present paper.

5. Random dynamics generated by an autonomous dynamical system

The following autonomous dynamical system can produce truly random dynamics:

$$X_{n+1} = \begin{cases} aX_n & \text{if } X_n < Q, \\ bY_n & \text{if } X_n > Q, \end{cases} \tag{29}$$

$$Y_{n+1} = cZ_n, \tag{30}$$

$$Z_{n+1} = \sin^2(\pi X_n)\,. \tag{31}$$

Here $a > 1$ can be an irrational number, $b > 1, c > 1$. We can note that for $0 < X_n < Q$, the behavior of function Z_n is exactly like that of function (1).

For $X_n > Q$ the dynamics is re-injected to the region $0 < X_n < Q$ with a new initial condition. While X_n is in the interval $0 < X_n < Q$, the dynamics of Z_n is unpredictable as it is function (1). Thus, the process of producing a new initial condition through Eq. (30) is random.

If the only observable is Z_n, then it is impossible to predict the next values of this sequence using only the knowledge of the past values.

An example of the dynamics produced by the dynamical system (29)–(31) is shown in Fig. 14. If we apply the nonlinear forecasting method analysis to a common chaotic system, then the prediction error increases with the number of time-steps into the future. On the other hand, when we apply this method to the time-series produced by system (29)–(31), the prediction error is independent of the time-steps into the future, as in the case of a random sequence. Other very strong methods [58], which allows to distinguish between chaos and random noise, produce the same result.

With this result we are uncovering a new mechanism for generating random dynamics. This is a fundamental result because it is very important to understand different

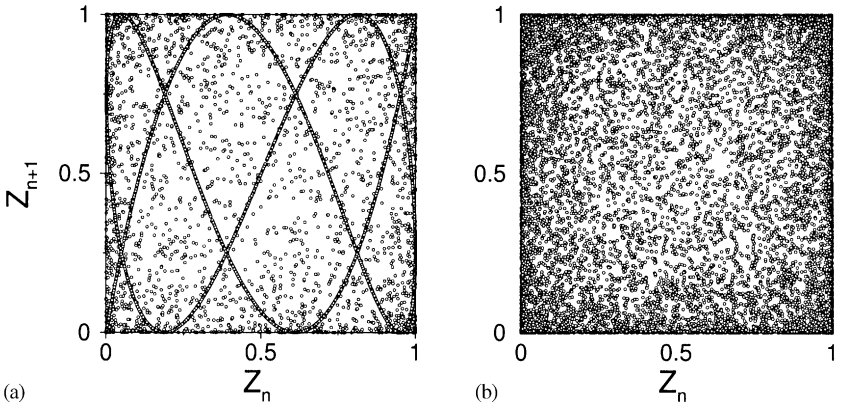


Fig. 14. First-return maps produced by the dynamics of the dynamical system (29)–(31). (a) $a = 7/3, b = 171, c = 1.5, Q = 1000/a$; (b) $a = e$ (irrational), $b = 171, c = 1.5, Q = 1000/a$.

mechanisms by which the natural systems can produce truly random (not only chaotic) dynamics.

6. Other dynamical systems

In the present section we will discuss different dynamical systems, whose dynamics is similar to that of random functions (1).

In the previous section we studied a dynamical system where the re-injection of variable X_n to the interval $0 < X_n < Q$ was defined using the random variable Z_n. Here we present a dynamical system:

$$X_{n+1} = \begin{cases} aX_n & \text{if } X_n < Q, \\ bY_n & \text{if } X_n > Q, \end{cases} \tag{32}$$

$$Y_{n+1} = f(Y_n)\,, \tag{33}$$

$$Z_{n+1} = \sin^2(\pi X_n)\,, \tag{34}$$

where the mentioned re-injection is produced through a chaotic system (in this case this is the map $Y_{n+1} = f(Y_n) \equiv \sin^2[c \arcsin\sqrt{Y_n}]$.

Fig. 15 shows two different examples of the dynamics of this system.

In order to produce this kind of dynamics we do not need to use the sine function in Eq. (34). We can use a polynomial function:

$$X_{n+1} = \begin{cases} aX_n & \text{if } X_n < Q, \\ bY_n & \text{if } X_n > Q, \end{cases} \tag{35}$$

$$Y_{n+1} = \sin^2[c \arcsin \sqrt{Y_n}]\,, \tag{36}$$

$$Z_{n+1} = h(X_n)\,. \tag{37}$$

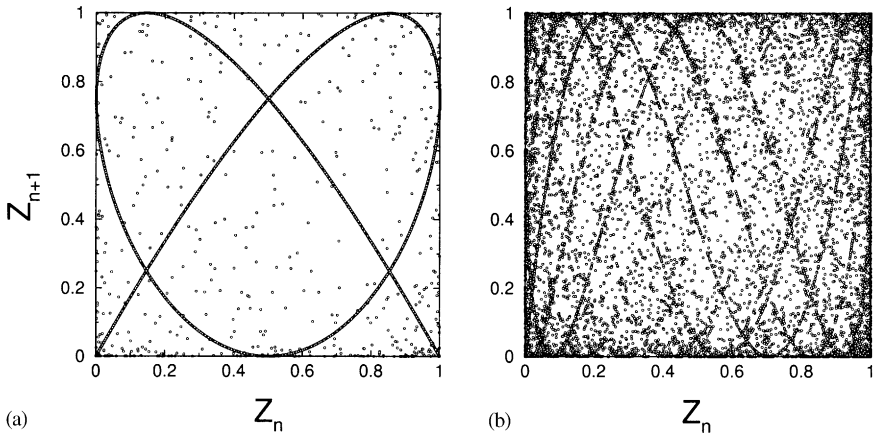


Fig. 15. The map (Z_n, Z_{n+1}), where the dynamics Z_n is produced by the dynamical system (32)–(34): (a) $a = 4/3, b = 2, c = 3, Q = 100$; (b) $a = \pi, b = 2, c = 3, Q = 100$.

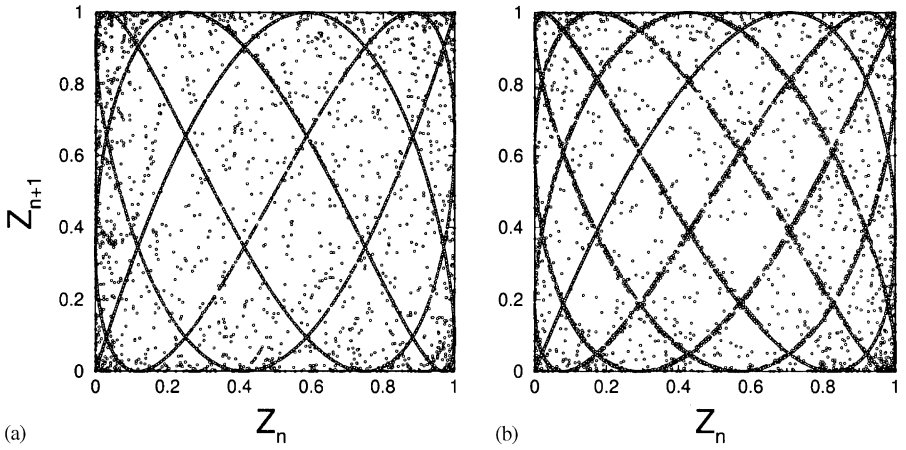


Fig. 16. The map (Z_n, Z_{n+1}), where the dynamics Z_n is produced by the dynamical system (35)–(37), $b = 2.49, c = 3, Q = 63, h(x) = [\sum_{i=1}^{m}(-1)^i(\pi x)^i/i]^2, m = 90$: (a) $a = 9/5$; (b) $a = 1.5707963$.

It is important that the function X_n behaves as truncated exponential "inside" function $h(X_n)$. And function $h(X_n)$ should make several "oscillations" in the interval that coincides with the range of function X_n (i.e., the image of function X_n). For a set of fixed parameters, the number of "oscillations" of function $h(X_n)$ is proportional to the "complexity" of the dynamics. An example of this dynamics can be observed in Fig. 16.

Another way to re-inject the dynamics of function X_n into region $0 < X_n < Q$ is the following:

$$X_{n+1} = \begin{cases} a_1 X_n & \text{if } X_n < Q_1, \\ b_1 W_n & \text{if } X_n > Q_1, \end{cases} \tag{38}$$

$$Y_{n+1} = \sin^2[\pi X_n]\,, \tag{39}$$

$$V_{n+1} = \begin{cases} a_2 V_n & \text{if } V_n < Q_2, \\ b_2 Y_n & \text{if } V_n > Q_2, \end{cases} \tag{40}$$

$$W_{n+1} = \sin^2[\pi V_n]\,. \tag{41}$$

In this case, we are using the random dynamics produced in a second system to generate the new "initial" conditions for the variable X_n.

See Figs. 17–19 with some examples of the behavior of system (38)–(41).

If, due to some physical constraints, the dynamics of a simple chaotic system as Eq. (36) can become a little "repetitive", then the system (38)–(41) is a good way to avoid predictability.

Moreover, we could use a completely independent dynamical system as the one explained in Section 4, to produce the re-injection:

$$X_{n+1} = \begin{cases} a_1 X_n & \text{if } X_n < Q_1, \\ b_1 W_n & \text{if } X_n > Q_1, \end{cases} \tag{42}$$

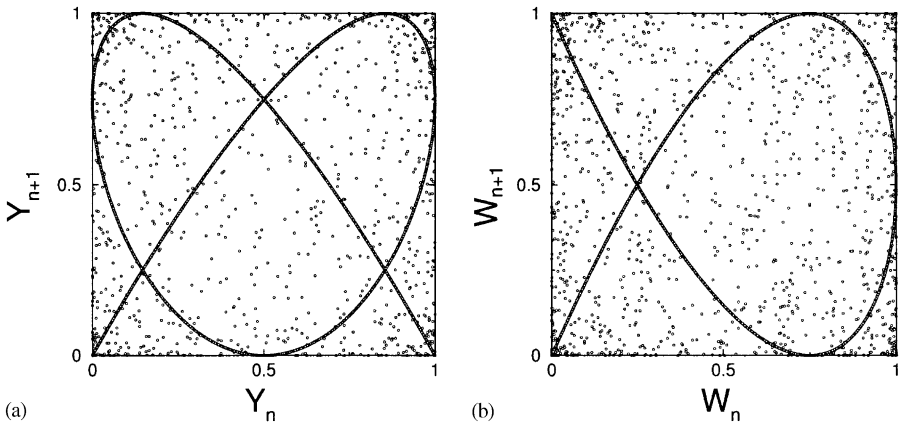


Fig. 17. First-return maps produced by dynamical system (38)–(41), $a_1 = 4/3, a_2 = 3/2, Q_1 = Q_2 = 950, b_1 = b_2 = 249$: (a) map (Y_n, Y_{n+1}); map (W_n, W_{n+1}).

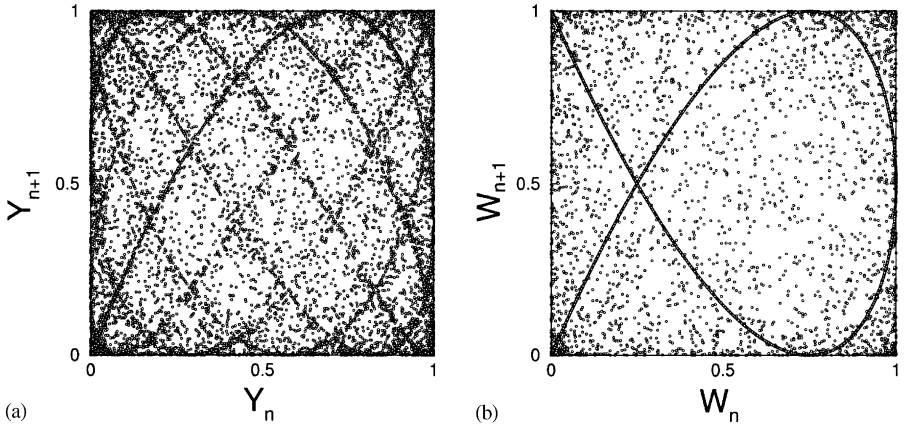


Fig. 18. First-return maps produced by dynamical system (38)–(41), $a_1 = 1.5707963, a_2 = 3/2$, $b_1 = 3, b_2 = 249, Q_1 = 95, Q_2 = 950$: (a) map (Y_n, Y_{n+1}); map (W_n, W_{n+1}).

$$Y_{n+1} = \sin^2[\pi X_n]\,, \tag{43}$$

$$V_{n+1} = \begin{cases} a_2 V_n & \text{if } V_n < Q_2, \\ b_2 W_n & \text{if } V_n > Q_2, \end{cases} \tag{44}$$

$$W_{n+1} = \sin^2[\pi V_n]\,. \tag{45}$$

Note that Eqs. (44) and (45) are completely independent of Eqs. (42) and (43). Using the same mechanism as that explained in Section 4, the dynamics of variable W_n is very complex. This dynamics is used in Eq. (42) to produce the new "initial" conditions for X_n.

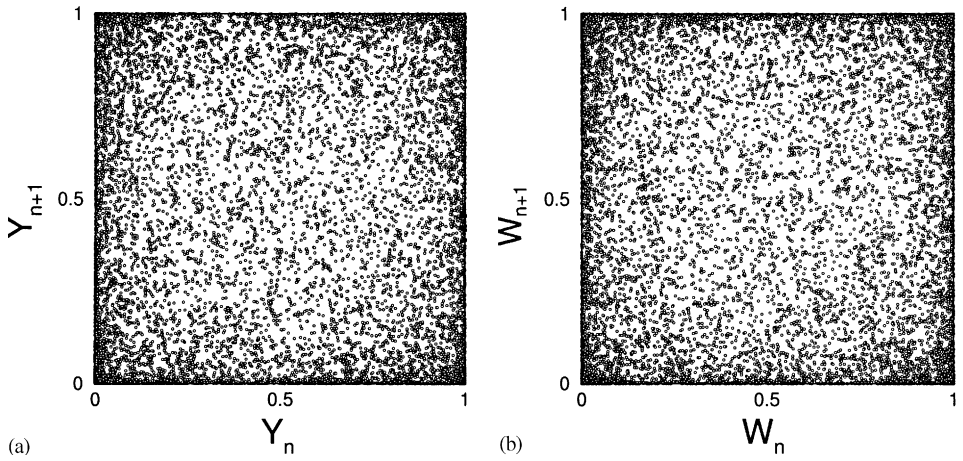


Fig. 19. First-return maps produced by dynamical system (38)–(41), $a_1 = 2\pi, a_2 = 2e, b_1 = 29$, $b_2 = 24, Q_1 = Q_2 = 99$: (a) map (Y_n, Y_{n+1}); map (W_n, W_{n+1}).

Now we would like to discuss the role of noninvertibility in the creation of complex dynamics.

Let us study dynamical systems of the type:

$$X_{n+1} = f(X_n, Y_n)\,, \tag{46}$$

$$Y_{n+1} = g(X_n, Y_n)\,, \tag{47}$$

$$Z_{n+1} = \sin^2(\pi v X_n)\,. \tag{48}$$

Suppose Eqs. (46) and (47) produce chaotic dynamics where there is intermittent finite exponential behavior.

Note that in the argument of the sine function in Eq. (48), there is a new parameter v. Using this parameter we can change the number of oscillations of the sine function in a given interval of possible values of variable X_n.

If Eqs. (46) and (47) conform a dynamical system of types (32) and (33), where there exists a parameter Q, which defines approximately the maximum value of variable X_n, then we can increase this value at our will, and it is not difficult to produce complex dynamics.

In any case, parameter v can help to produce even more complex dynamics (see Fig. 20).

However, suppose the dynamical systems (46) and (47) can produce a chaotic (but predictable) dynamics limited to the interval $0 < X_n < 1$ like the logistic map. Can we obtain very complex dynamics in Eq. (48)?

In Fig. 21, we can observe the consequences of increasing parameter v.

Thus, in a chaotic system as the following:

$$X_{n+1} = f(X_n, Y_n), \tag{49}$$

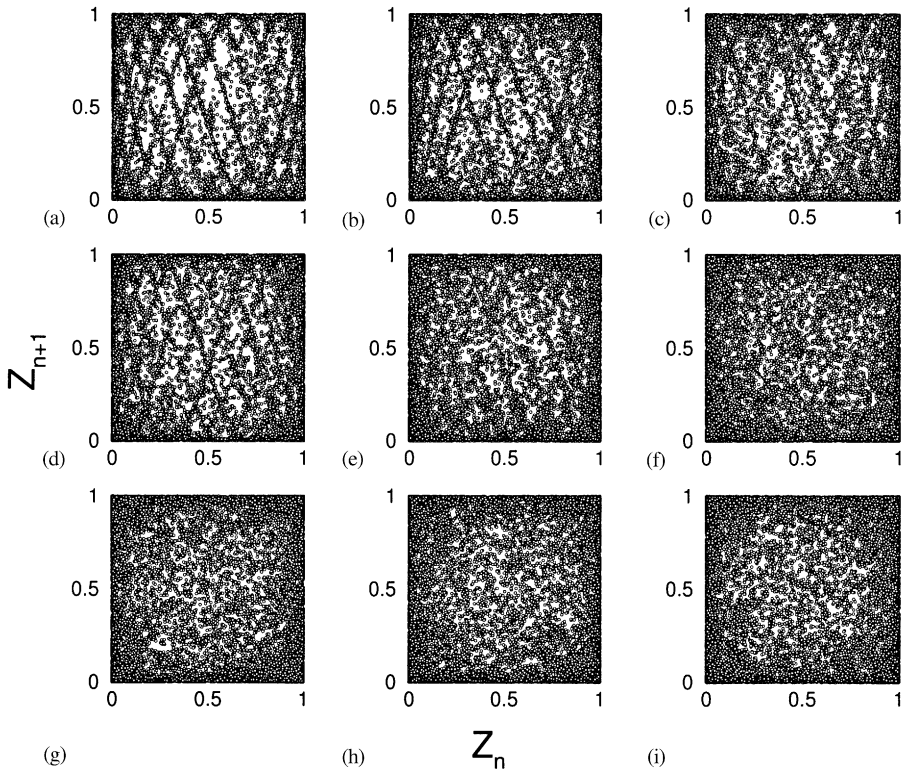


Fig. 20. Maps (Z_n, Z_{n+1}) produced by the dynamical system (46)–(48) (see discussion in the main text): (a) $v = 0.5$; (b) $v = 1$; (c) $v = 1.5$; (d) $v = 2$; (e) $v = 5$; (f) $v = 20$; (g) $v = 50$; (h) $v = 500$; (i) $v = 5000$. Note that the complexity increases with v.

$$Y_{n+1} = g(X_n, Y_n), \tag{50}$$

$$Z_{n+1} = h(X_n), \tag{51}$$

the number of "oscillations" of function $h(X_n)$ in the interval of possible values of the chaotic variable X_n, is crucial for producing complexity.

7. Nonlinear circuits

When the input is a normal chaotic signal and the system is an electronic circuit with the I–V characteristics shown in Figs. 22 and 23, then the output will be a very complex signal.

In Ref. [59] a theory of nonlinear circuits is presented. There we can find different methods to construct circuits with these I–V characteristic curves.

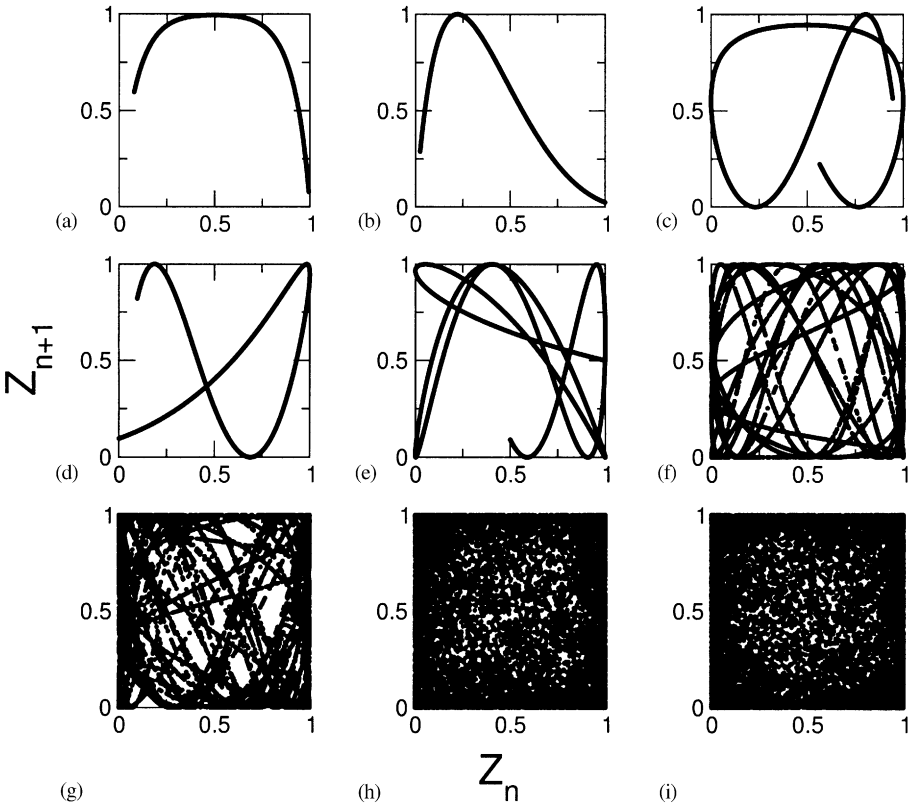


Fig. 21. Maps (Z_n, Z_{n+1}) produced by the dynamical system, (46)–(48) (see discussion in the main text): (a) $v = 0.5$; (b) $v = 1$; (c) $v = 1.5$; (d) $v = 2$; (e) $v = 5$; (f) $v = 20$; (g) $v = 50$; (h) $v = 500$; (i) $v = 5000$. Note that in this case the dynamics produced by Eqs. (46) and (47) is very simple (predictable) chaotic signal, limited to the interval $0 < X_n < 1$. Even in this case, increasing parameter v, the complexity can be increased to unimaginable values.

The scheme of this composed system is shown in Fig. 24. A set of equations describing this dynamical system is the following:

$$X_{n+1} = F_1(X_n, Y_n)\,, \tag{52}$$

$$Y_{n+1} = F_2(X_n, Y_n)\,, \tag{53}$$

$$Z_{n+1} = g(X_n)\,, \tag{54}$$

where Eqs. (52) and (53) describe a normal chaotic dynamics where the variable X_n presents intermittent intervals with a truncated exponential behavior and $g(X_n)$ is a function with several maxima and minima as that shown in Fig. 23.

Figs. 25 (a) and (b) show nonlinear circuits that can be used as the nonlinear system shown on the right of the scheme of Fig. 24.

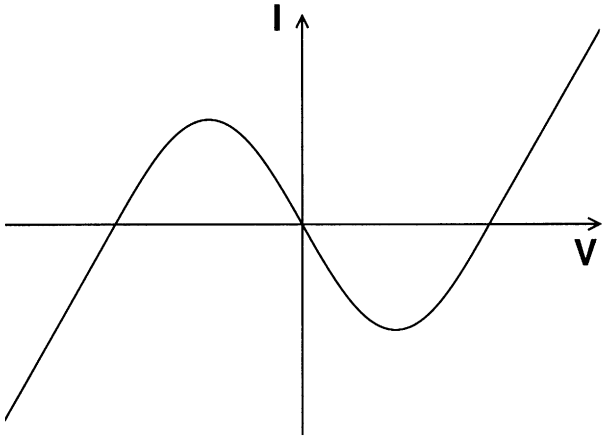


Fig. 22. Noninvertible I–V characteristic. Two extrema.

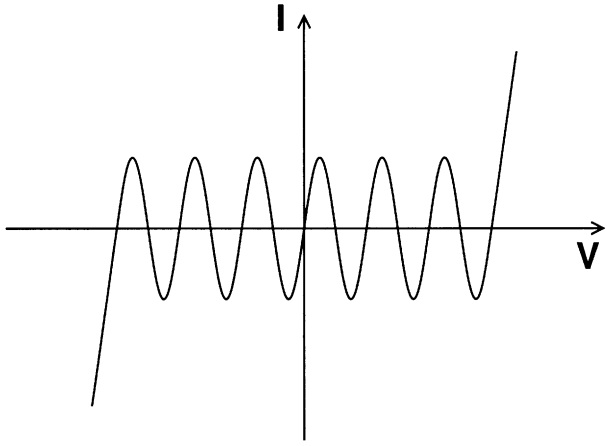


Fig. 23. Noninvertible I–V characteristic. Many extrema.

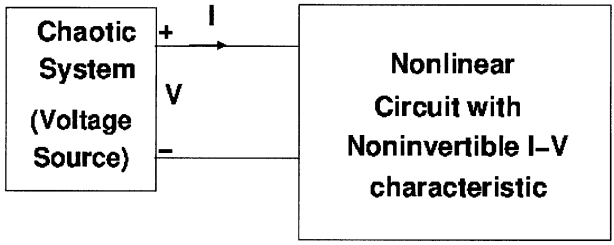
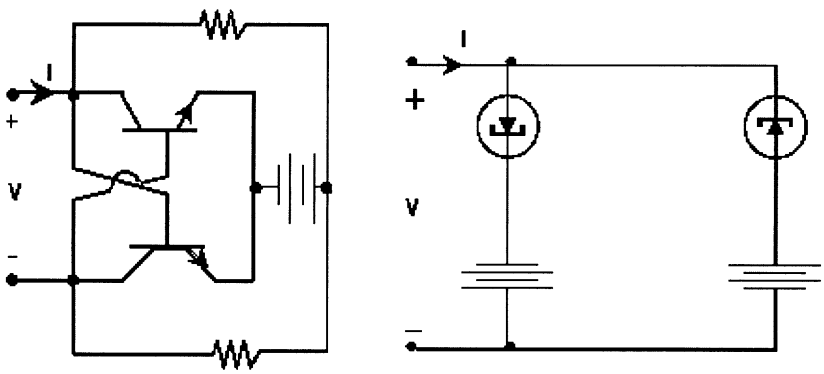


Fig. 24. Scheme of a nonlinear system where a chaotic voltage source is used as the input signal for a nonlinear circuit with a noninvertible I–V characteristic.



(a) (b)

Fig. 25. Nonlinear circuits with noninvertible I–V characteristics: (a) The resistors possess $R = 2.2\,\mathrm{k}\Omega$, the source voltage in the battery is 10 V and the twin transistors are $2N2222$ with $\beta = 140$). The I–V characteristic of this circuit is shown in Fig. 4. (b) Another circuit with a similar I–V characteristic.

The system on the left of the scheme can be a chaotic circuit, e.g., the Chua's circuit [60].

We have constructed a circuit similar to the one shown in Fig. 25 (a). We produced chaotic time-series using a common nonlinear map and then we transformed them into analog signals using a converter. This analog signals were introduced as the voltage-input to the circuit shown in Fig. 25 (a). Similar results are obtained when we take the input signal from a chaotic electronic circuit.

The set of equations that describes one of our experimental situations is the following:

$$X_{n+1} = aX_n[1 - \Theta(X_n - q)] + bY_n\,\Theta(X_n - q)\,, \tag{55}$$

$$Y_{n+1} = \sin^2[d\,\arcsin\sqrt{Y_n}]\,, \tag{56}$$

$$Z_{n+1} = 4W_n^3 - 3W_n\,, \tag{57}$$

where $W_n = 2X_n/s - 1, q = s/a, s = 10, b = 7, a = \pi/2, d = 3, \Theta(x)$ is the Heaviside function.

The first-return maps of the sequence Z_n produced by the theoretical model (55)–(57) and the experimental time-series produced by the nonlinear system of Figs. 24 and 25 (a) are shown in Figs. 26 (a) and (b).

When the nonlinear circuit has an I–V characteristic with many more maxima and minima, e.g. Fig. 23 (and this can be done in practice, see Ref. [59]), we can produce a much more complex dynamics.

8. Josephson junction

Using our theoretical results we can make a very important prediction here. A nonlinear physical system constructed with chaotic circuits and a Josephson junction [61]

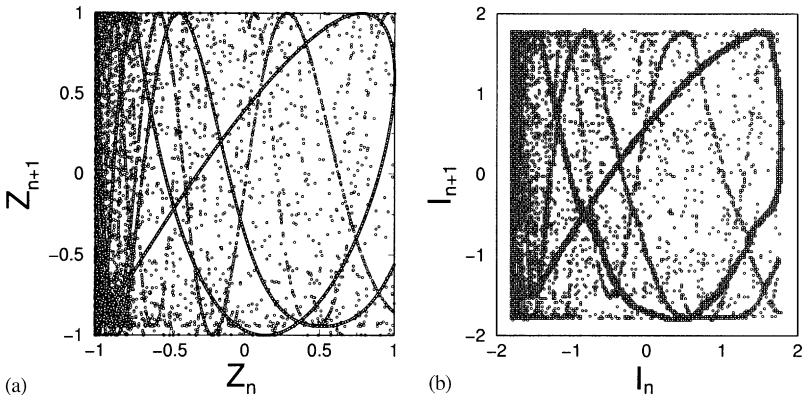


Fig. 26. Modelling vs. experiment: (a) numerical simulation of the dynamical system (55)–(57); (b) first-return map produced with the real data (current measurements) from experiments using the scheme of Fig. 24, where the circuit of the right is the one of Fig. 25 (a).

can be an ideal experimental setup for the random dynamics that we are presenting here.

It is well-known that the current in a Josephson junction may be written as

$$I = I_c \sin\phi\,, \tag{58}$$

where

$$\frac{\mathrm{d}\phi}{\mathrm{d}t} = kV\,. \tag{59}$$

Here ϕ is the phase difference of the superconducting order parameter between each side of the barrier and V is the voltage across the junction. Note that nature has provided us with a phenomenon where the sine-function is intrinsic. Although we have already explained that other noninvertible functions can produce similar results, it is remarkable that we can use this very important physical system to investigate the real consequences of our results with function (1). In a superconducting Josephson junction k is defined through the fundamental constants $k = 2e/\hbar$. However, in the last decades there have been a wealth of experimental work dedicated to the creation of electronic analogs that can simulate the Josephson junction [63–66]. In that case k can be a parameter with different numerical values.

We have performed real experiments with a nonlinear chaotic circuit coupled to a Josephson junction analog.

In our experiments we have used the Josephson junction analog constructed by Magerlein [66]. This is a very accurate device that has been found very useful in many experiments for studying junction behavior in different circuits. The junction voltage is integrated using appropriate resetting circuitry to calculate the phase ϕ, and a current proportional to $\sin\phi$ can be generated. The circuit diagram can be found in Ref. [66].

The parameter k is related to certain integrator time constant RC in the circuit. So we can change its value. This is important for our experiments. We need large values

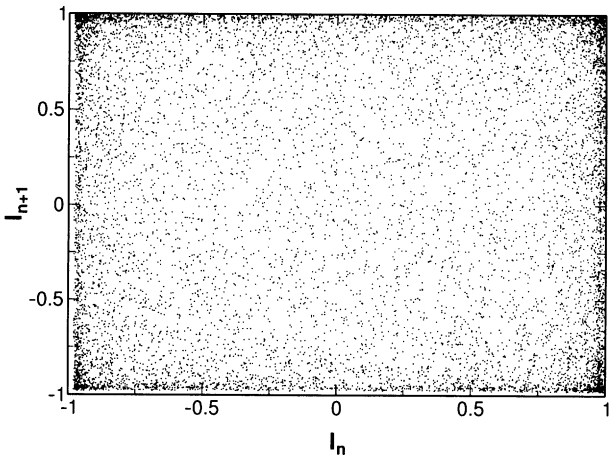


Fig. 27. First-return map of the time-series generated with real data from an experiment with an analog Josephson junction coupled to the Chua's circuit.

of k in order to increase the effective domain of the sine function. In other words, we need the argument of the sine function to take large values in a truncated exponential fashion. This allows us to have a very complex output signal. In our case the value of k is 10,000.

The voltage $V(t)$ across the junction is not taken constant. This voltage will be produced by a chaotic system. In our case we selected the Chua's circuit [60]. For this, we have implemented the Chua's circuit following the recipe of Ref. [62]. Fig. 27

The scheme of the Chua's circuit constructed by us can be found in Fig. 1 of Ref. [62].

The following components were used: $C_1 = 10$ nF, $C_2 = 100$ nF, $L = 19$ mH, and R is a 2.0 kΩ trimpot.

Chua's diode was built using a two-operational-amplifier configuration suggested in Ref. [62].

In our experiment, the voltage in C_1 was used as the driving signal for the Josephson junction. We were interested in the famous double scroll attractor attained with $R \approx 1880\ \Omega$.

The results of the experiments are shown in (27) which is the first-return map of the time-series data produced by direct measurements of the junction current. The time-intervals between measurements was 10 ms. This system can produce unpredictable dynamics.

9. Discussion and conclusions

In conclusion, we have shown that functions of type $X_n = P(\theta z^n)$, where $P(t)$ is a periodic function and z is a noninteger number, can produce completely random numbers.

Certain class of autonomous dynamical systems can generate a similar dynamics. This dynamics presents fundamental differences with the known chaotic systems. We have presented real nonlinear systems that can produce this kind of random time-series. We have reported the results of real experiments with nonlinear circuits containing direct evidence supporting this phenomenon.

Besides the fundamental importance of these findings, these systems possess many practical applications. For instance, game theory tells us that in certain competitive situations the optimal strategy is a random behavior. Specifically, it is necessary to limit the competition's ability to predict our decisions. We can produce randomness using the discussed systems. Another example is secure communications [67]. In this context, the most important application of our systems is masking messages using random signals [68]. In some cases, when we use the usual chaotic systems, the messages can be cracked because the time-series are not truly unpredictable.

Now we will analyze very general ideas.

Just to facilitate our discussion (because it is always important to have a name), we will call the phenomenon studied in this paper "random chaos".

Random chaos imposes fundamental limits on prediction, but it also suggests that there could exist causal relationships where none were previously suspected.

Random chaos demonstrates that a system can have the most complicated behavior that emerges as a consequence of simple, nonlinear interaction of only a few effective degrees of freedom.

On one hand, random chaos implies that if there is a phenomenon in the world (whose mechanism from first principles is not known) described by a dynamical system of type [8–10] or [11–13], and the only observable is a physical variable as Z_n, then the law of this phenomenon cannot be learnt from the experimental data, or the observations. And, situations in which the fundamental law should be inferred from the observations alone have not been uncommon in physics.

On the other hand, the fact that this random dynamics is produced by a relatively simple, well-defined autonomous dynamical system implies that many random phenomena could be more predictable than have been thought.

Suppose there is a system thought to be completely random. From the observation of some single variable, scientists cannot obtain the generation law. However, suppose that in some cases, studying the deep connections of the phenomenon, we can deduce a dynamical system of types [8–10] or [11–13]. In these cases, some prediction is possible. Earthquakes and stock price dynamics have eluded prediction theorists until now. Who knows if these phenomena could be examples of random chaos.

In any case, what is certain at this point is that some dynamical systems can generate randomness on their own without the need for any external random input.

References

[1] E.N. Lorenz, J. Atmos. Sci. 20 (1963) 130.
[2] T.Y. Li, J.A. Yorke, Am. Math. Mon. 82 (1975) 985.
[3] M.J. Feigenbaum, J. Stat. Phys. 19 (1978) 25.
[4] R.M. May, Nature 261 (1976) 459.

[5] J. Ford, Phys. Today 36 (1983) 40.
[6] J.P. Crutchfield, J.D. Farmer, N.H. Packard, R.S. Shaw, Sci. Am. 254 (1986) 46.
[7] C. Grebogi, E. Ott, J.A. Yorke, Science 238 (1987) 632.
[8] E. Ott, M. Spano, Phys. Today 48 (1995) 34.
[9] F. Takens, in: D.A. Rand, L.S. Young (Eds.), Lecture Notes in Mathematics, Vol. 894, Springer, Berlin, 1981.
[10] D. Ruelle, Turbulence, Strange Attractors and Chaos, World Scientific, New Jersey, 1995.
[11] J.D. Farmer, J.J. Sidorovich, Phys. Rev. Lett. 59 (1987) 845;
G. Sugihara, R.M. May, Nature 344 (1990) 734;
D.J. Wales, Nature 350 (1991) 485;
A.A. Tsonis, J.B. Elsner, Nature 358 (1992) 217.
[12] J.A. González, L.B. Carvalho, Mod. Phys. Lett. B 11 (1997) 521.
[13] H.N. Nazareno, J.A. González, I. Costa, Phys. Rev. B 57 (1998) 13 583.
[14] J.A. González, R. Pino, Comput. Phys. Commun. 120 (1999) 109;
J.A. González, R. Pino, Physica A 276 (2000) 425;
J.A. González, M. Martín-Landrove, L. Trujillo, Int. J. Bifurcation Chaos 10 (2000) 1867;
J.A. González, L.I. Reyes, L.E. Guerrero, Chaos 11 (2001) 1.
[15] A.M. Ferrenberg, D.P. Landau, Y.J. Wong, Phys. Rev. Lett. 69 (1992) 3382.
[16] I. Vattulainen, T. Ala-Nissila, K. Kankaala, Phys. Rev. E 52 (1995) 3205.
[17] A. Compagner, Phys. Rev. E 52 (1995) 5634.
[18] L.N. Shchur, H.W.J. Blöte, Phys. Rev. E 55 (1997) R4905.
[19] B.M. Gammel, Phys. Rev. E 58 (1998) 2586.
[20] I. Vattulainen, Phys. Rev. E 59 (1999) 7200.
[21] F. James, Comput. Phys. Commun. 60 (1990) 329.
[22] F. James, Chaos Solitons Fractals 6 (1995) 221.
[23] J.J. Collins, M. Fanciulli, R.G. Hohlfeld, D.C. Finch, G.V.H. Sandri, E.S. Shtatland, Comput. Phys. 6 (1992) 630.
[24] D.E. Knuth, Seminumerical Algorithms, The Art of Computer Programming, Vol. 2, Addison-Wesley, Reading, MA, 1981.
[25] S. Park, K. Miller, Commun. ACM 31 (1988) 1192.
[26] J.L. Doob, Stochastic Processes, Wiley, New York, 1991.
[27] L. Mark Berliner, Statist. Sci. 7 (1992) 69.
[28] R.M. D'Souza, Y. Bar-Yam, M. Kardar, Phys. Rev. E 57 (1998) 5044.
[29] J. Nogués, J.L, Costa-Krämer, K.V. Rao, Physica A 250 (1998) 327.
[30] M.E. Fisher, Physica A 263 (1999) 554.
[31] G. Marsaglia, Proc. Natl. Acad. Sci. 61 (1968) 25.
[32] G. Marsaglia, in: L. Billard (Ed.), Computer Science and Statistics: The Interface, Elsevier, Amsterdam, 1985.
[33] G. Marsaglia, B. Narasimhan, A. Zaman, Comput. Phys. Commun. 60 (1990) 345.
[34] I. Vattulainen, T. Ala-Nissila, K. Kankaala, Phys. Rev. Lett. 73 (1994) 2513.
[35] L.N. Shchur, J.R. Heringa, H.W.J. Blöte, Physica A 241 (1997) 579.
[36] T.Y. Li, J.A. Yorke, Nonlinear Anal. Theory Methods Appl. 2 (1978) 473.
[37] S.C. Phatak, S.S. Rao, Phys. Rev. E 51 (1995) 3670.
[38] R.L. Kautz, J. Appl. Phys. 86 (1999) 5794.
[39] L.N. Shchur, P. Butera, Int. J. Mod. Phys. C 9 (1998) 607.
[40] L.N. Shchur, Comput. Phys. Commun. 121–122 (1999) 83.
[41] D. Stauffer, Int. J. Mod. Phys. C 10 (1999) 807.
[42] A. Srinivasan, D.M. Ceperley, M. Mascagni, Adv. Chem. Phys. 105 (1999) 13.
[43] A. Proykova, Comput. Phys. Commun. 124 (2000) 125.
[44] T. Stojanovski, L. Kocarev, IEEE Trans. Circuits Systems I 48 (2001) 281.
[45] T. Stojanovski, L. Kocarev, IEEE Trans. Circuits Systems I 48 (2001) 382.
[46] R. Bernardini, G. Cortelazzo, IEEE Trans. Circuits Systems I 48 (2001) 552.
[47] M. Lüscher, Comput. Phys. Commun. 79 (1994) 100.
[48] L'Ecuyer, Oper. Res. 47 (1999) 159.

[49] F. James, Comput. Phys. Commun. 79 (1994) 111.
[50] D. Tiggemann, Int. J. Mod. Phys. C 12 (2001) 871.
[51] A.M. Fraser, H.L. Swinney, Phys. Rev. A 33 (1986) 1134.
[52] C.E. Shannon, Bell System Tech. J. 27 (1948) 379,623.
[53] Y. Moon, B. Rajagopalan, U. Lall, Phys. Rev. E 52 (1995) 2318.
[54] A.R. Bulsara, A. Zador, Phys. Rev. E 54 (1996) 2185.
[55] I. Grosse, H. Herzel, S.V. Buldyrev, H.E. Stanley, Phys. Rev. E 61 (2000) 5624.
[56] P.M. Binder, J.A. Plazas, Phys. Rev. E 63 (2001) 065 203.
[57] J.P. Crutchfield, D.P. Feldman, unpublished.
[58] P. Grassberger, I. Proccacia, Physica D 9 (1983) 189;
Wolf, J.B. Swift, H.L. Swinney, J.A. Vastano, Physica D 16 (1985) 285.
[59] L.O. Chua, C.A. Desoer, E.S. Kuh, Linear and Nonlinear Circuits, McGraw-Hill, New York, 1987.
[60] T. Matsumoto, L.O. Chua, M. Komoro, IEEE Trans. Circuits Systems CAS-32 (1985) 797;
T. Matsumoto, L.O. Chua, M. Komoro, Physica D 24 (1987) 97.
[61] A. Barone, G. Paterno, Physics and Applications of the Josephson Effect, Wiley-Interscience, New York, 1982;
K.K. Likharev, Dynamics of Josephson Junctions and Circuits, Gordon and Breach Science Publishers, New York, 1986.
[62] M.P. Kennedy, Frequenz 46 (1992) 66.
[63] N.R. Werthamer, S. Shapiro, Phys. Rev. 164 (1967) 523.
[64] C.A. Hamilton, Rev. Sci. Instr. 43 (1972) 445.
[65] C.K. Bak, N.F. Pedersen, Appl. Phys. Lett. 22 (1973) 149.
[66] J.H. Magerlein, Rev. Sci. Instr. 49 (1978) 486.
[67] L.M. Pecora, T.L. Carroll, Phys. Rev. Lett. 64 (1990) 821;
T.L. Carroll, L.M. Pecora, Physica D 67 (1993) 126;
K. Cuomo, A.V. Oppenheim, Phys. Rev. Lett. 71 (1993) 65.
[68] R. Brown, L.O. Chua, Int. J. Bifurcation Chaos 6 (1996) 219;
Y.Y. Chen, Europhys. Lett. 34 (1996) 24.