11 March 2002

PHYSICS LETTERS A

ELSEVIER

Physics Letters A 295 (2002) 25–34

www.elsevier.com/locate/pla

A mechanism for randomness

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

[a] *Centro de Física, Instituto Venezolano de Investigaciones Científicas, Apartado Postal 21827, Caracas 1020-A, Venezuela*
[b] *The Abdus Salam International Centre for Theoretical Physics, Strada Costiera 11, 34100 Trieste, Italy*
[c] *Departamento de Física, Universidad Simón Bolívar, Apartado Postal 89000, Caracas 1080-A, Venezuela*

Received 29 August 2001; received in revised form 18 January 2002; accepted 18 January 2002

Communicated by C.R. Doering

Abstract

We investigate explicit functions that can produce truly random numbers. We use the analytical properties of the explicit functions to show that certain class of autonomous dynamical systems can generate random dynamics. This dynamics presents fundamental differences with the known chaotic systems. We present real physical systems that can produce this kind of random time-series. We report the results of real experiments with nonlinear circuits containing direct evidence for this new phenomenon. In particular, we show that a Josephson junction coupled to a chaotic circuit can generate unpredictable dynamics. Some applications are discussed. © 2002 Elsevier Science B.V. All rights reserved.

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

Keywords: Chaotic systems; Random systems; Experimental chaos

1. Introduction

Over the last three decades or so, a revolution has happened in the development of science. We are talking about Chaos theory [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 sen-

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

PII: S0375-9601(02)00101-9

sitive 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

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

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

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

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.

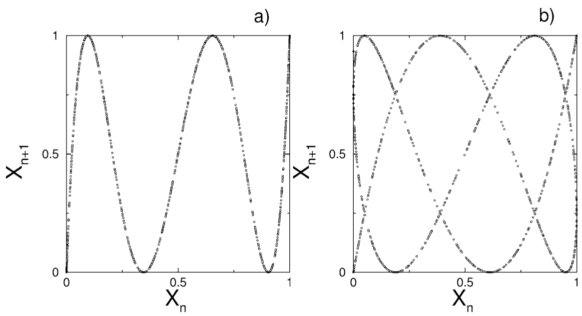

Fig. 1. First-return maps produced by function (1): (a) $z = 5$; (b) $z = 7/3$.

2. Random functions

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): $X_0, X_1, X_2, X_3, \dots, X_m$ (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:

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

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

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

for all $n \leqslant m$. Note that the number $kp^n q^{(m-n)}$ 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 $X_0, X_1, X_2, X_3, \dots, X_m$, 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 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.

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)).

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.

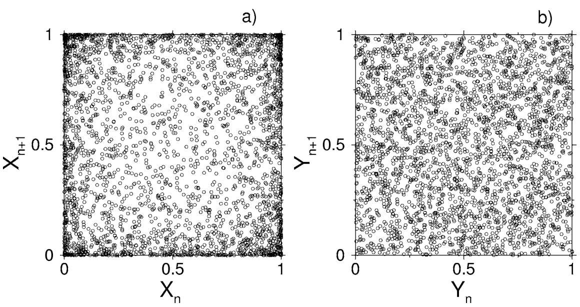

Fig. 2. First-return maps produced by function (1): (a) $z = e$ (irrational); (b) $z = e$, $Y_n = (2/\pi)\arcsin(X_n^{1/2})$.

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 careful 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

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

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:

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

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

However, a more deep analysis shows that (to produce complex behavior) the function $f(n)$ 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.

3. Autonomous dynamical systems

The following autonomous dynamical system can produce truly random dynamics:

$$X_{n+1} = \begin{cases} aX_n, & \text{if } X_n < Q, \\ bY_n, & \text{if } X_n > Q, \end{cases} \tag{8}$$

$$Y_{n+1} = cZ_n, \tag{9}$$

$$Z_{n+1} = \sin^2(\pi X_n). \tag{10}$$

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. (9) 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 (8)–(10) is shown in Fig. 3. 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 (8)–(10), the prediction error is independent of the time-steps into the future, as in the case of a random sequence. Other very strong methods [15], which allow to distinguish between chaos and random noise, produce the same result.

Here we should make an important remark. Mathematical models can be of different types. For instance, natural phenomena can be described by differential equations, difference equations, cellular automata, neural networks, etc.

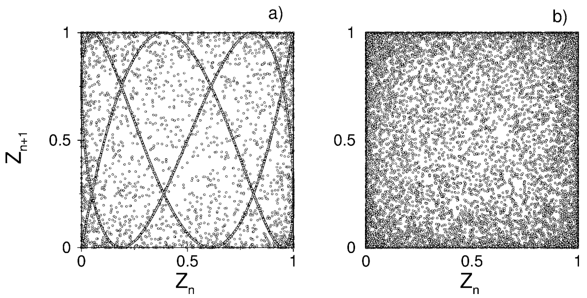

Fig. 3. First-return maps produced by the dynamics of the dynamical system (8)–(10). (a) $a = 7/3$, $b = 171$, $c = 1.5$, $Q = 1000/a$; (b) $a = e$ (irrational), $b = 171$, $c = 1.5$, $Q = 1000/a$.

Even explicit functions can be mathematical models. If we consider function (1) as the mathematical model of some dynamical process, then this process can be completely random. If all we know is the series of outcomes $X_0, X_1, X_2, \ldots$, then it does not matter how many values we already have, the next value is unpredictable. However, this is because from the observation of the values $X_0, X_1, X_2, \ldots, X_m$, it is impossible to determine the "variable" $Y_n = \theta \pi z^n$. This could be considered as a "hidden variable". Of course, we cannot say that this is just a problem of hidden variables, because not for any hidden variable Y_n, the function $X_n = \sin^2(Y_n)$ is a random system. Here we have obtained necessary conditions for this phenomenon to occur.

Let us extend this analysis to the dynamical system (8)–(10). In this case the completely random variable is Z_n. The role of "hidden variable" is played by X_n. If one could observe the series X_n, then the complete randomness of the data set is lost. We could say that some projection of the complete set of variables onto a proper subset is necessary for the effect.

It is important to notice that the dynamical system (8)–(10) is a well-posed set of difference equations with unique forward time evolution. Given the initial conditions (X_0, Y_0, Z_0), the future evolution of the dynamics is fully determined. However, if the only observable is Z_n, then this variable will behave as a completely random time-series. How can one reconcile the unique forward time evolution with this randomness? The answer is related to the fact that only a subset of the variables are observed.

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

4. Pseudorandom number generators

There is a large literature dedicated to pseudorandom number generators (see, e.g., [16–38] and references therein). A very fine 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 [17], 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 [17,18,24–26,33].

D'Souza et al. [24] 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

$$X_{n+1} = f(X_n, X_{n-1}, \dots, X_{n-r+1}). \tag{11}$$

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

Multiplicative linear congruential generators [16, 17] are defined by the following equation:

$$X_{n+1} = (aX_n + c) \bmod m. \tag{12}$$

Some famous values for these parameters are the following: $a = 23$, $m = 10^8 + 1$, $c = 0$; $a = 65539$, $m = 2^{29}$, $c = 0$; $a = 69069$, $m = 2^{32}$, $c = 1$; $a = 16807$, $m = 2^{31} - 1$, $c = 0$; $a = 1664525$, $m = 2^{32}$, $c = 0$ (this is the best generator for $m = 2^{32}$, according to the criteria of Knuth [20]).

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

$$X_{n+1} = (X_{n-p} \odot X_{n-q}) \bmod m, \tag{13}$$

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:

$$X_{n+1} = (aX_n + bX_{n-1} + c) \bmod m. \tag{14}$$

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

$$X_{n+1} = (X_{n-r} \pm X_{n-s} \pm c) \bmod m. \tag{15}$$

Among the high quality generators investigated in the famous paper [16] are the following:

$$X_{n+1} = (16807X_n) \bmod \bigl(2^{31} - 1\bigr), \tag{16}$$

$$X_{n+1} = (X_{n-103}.XOR.X_{n-250}), \tag{17}$$

$$X_{n+1} = (X_{n-1063}.XOR.X_{n-1279}), \tag{18}$$

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

$$X_n = (X_{n-22} - X_{n-43} - c), \tag{19}$$

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

All known generators (in some specific physical calculations) give rise to incorrect results because they deviate from randomness [16,24,25].

The problem is that these algorithms are predictable.

An example of this can be found in the work of Ferrenberg et al. [16]. 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 [16] related the errors in the simulations to the dependence in the generated numbers. Indeed, they are all based on maps of type (11).

In the present Letter we have shown that both the sequence of numbers X_n defined by function (1) and the sequence of numbers Z_n defined by the dynamical system (8)–(10) cannot be expressed as a map of type (11). In fact, these numbers are unpredictable and the next value cannot be determined as a function of the previous values.

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 [16], ballistic deposition [24], and random walks [25].

Nogués et al. [25] 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).

D'Souza et al. [24] 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 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 $\langle d^2 \rangle \sim N$.

The present Letter is not about random number generators. In the present Letter 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 Letter 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 the pseudorandom-number-generator algorithms (11)–(19) and the systems described in the present Letter.

5. Experiments

When the input is a normal chaotic signal and the system is an electronic circuit with the I–V characteristics shown in Figs. 4 and 5, then the output will be a very complex signal.

In Ref. [39] a theory of nonlinear circuits is presented. There we can find different methods to construct circuits with these I–V characteristic curves.

The scheme of this composed system is shown in Fig. 6. A set of equations describing this dynamical system is the following:

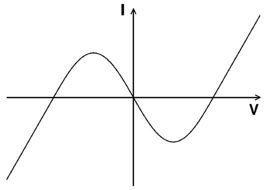

Fig. 4. Noninvertible I–V characteristic. Two extrema.

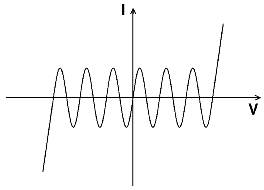

Fig. 5. Noninvertible I–V characteristic. Many extrema.

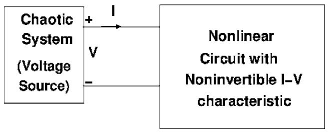

Fig. 6. Scheme of a nonlinear system where a chaotic voltage source is used as the input signal for a nonlinear circuit with a noninvertible I–V characteristic.

$$X_{n+1} = F_1(X_n, Y_n), \tag{20}$$

$$Y_{n+1} = F_2(X_n, Y_n), \tag{21}$$

$$Z_{n+1} = g(X_n), \tag{22}$$

where Eqs. (20) and (21) 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. 5.

Figs. 7(a) and (b) show nonlinear circuits that can be used as the nonlinear system shown on the right of the scheme of Fig. 6.

The system on the left of the scheme can be a chaotic circuit, e.g., the Chua's circuit [40].

We have constructed a circuit similar to the one shown in Fig. 7(a). We produced chaotic time-series using a common nonlinear map and then we transformed them into analog signals using a converter. These analog signals were introduced as the voltage-input to the circuit shown in Fig. 7(a). Similar results are obtained when we take the input signal from a chaotic electronic circuit.

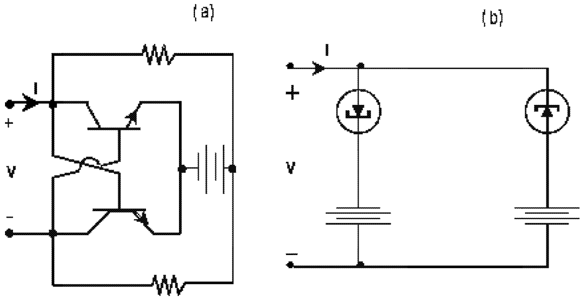

Fig. 7. Nonlinear circuits with noninvertible I–V characteristics. (a) The resistors possess $R = 2.2$ kΩ, the source voltage in the battery is 10 V and the twin transistors are $2N2222$ with $\beta = 140$). The I–V characteristic of this circuit is shown in Fig. 4. (b) Another circuit with a similar I–V characteristic.

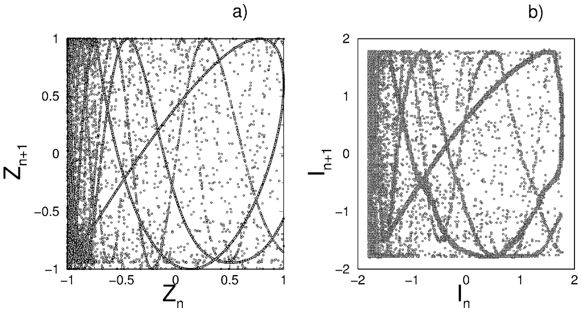

Fig. 8. Modelling versus experiment. (a) Numerical simulation of the dynamical system (23)–(25); (b) first-return map produced with the real data (current measurements) from experiments using the scheme of Fig. 6, where the circuit of the right is the one of Fig. 7(a).

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

$$X_{n+1} = aX_n\big[1 - \Theta(X_n - q)\big] + bY_n\Theta(X_n - q), \tag{23}$$

$$Y_{n+1} = \sin^2\big[d \arcsin\sqrt{Y_n}\,\big], \tag{24}$$

$$Z_{n+1} = 4W_n^3 - 3W_n, \tag{25}$$

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 (23)–(25) and the experimental time-series produced by the nonlinear system of Figs. 6 and 7(a) are shown in Figs. 8(a) and (b).

When the nonlinear circuit has an I–V characteristic with many more maxima and minima, e.g., Fig. 5 (and this can be done in practice, see Ref. [39]), we can produce a much more complex dynamics.

Nonlinear chaotic circuits can be described successfully by discrete maps as Eqs. (20)–(22) (see, e.g., [41]).

However, in some cases it can be very helpful to have a physical situation with a model based on a set of well-posed ordinary differential equations.

In Ref. [42] we can find several models for chaotic circuits as the following:

$$\frac{dX}{dt} = \alpha\big[f(x) - Y\big], \tag{26}$$

$$\frac{dY}{dt} = Y - X - Z, \tag{27}$$

$$\frac{dZ}{dt} = \beta Y + \gamma Z, \tag{28}$$

$$\frac{dW}{dt} = g(X), \tag{29}$$

where $f(x) = -X^3 + cX$, $g(X) = \sum_{i=1}^{N} a_i x^i$.

A comparison of different time-series is shown in Fig. 9. The fixed parameter values are $\alpha = 285.714$, $\beta = 1499.25$, $c = 0.144$, $\gamma = -0.51325$. Note that when the I–V characteristic of the circuit shown on the right of Fig. 6 is a function with many extrema, the produced time-series is more complex (see Fig. 9(b)).

Using our theoretical results we can make a very important prediction here. A nonlinear physical system constructed with chaotic circuits and a Josephson junction [43] 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

$$I = I_c \sin\phi, \tag{30}$$

where

$$\frac{d\phi}{dt} = kV. \tag{31}$$

Here ϕ is the phase 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

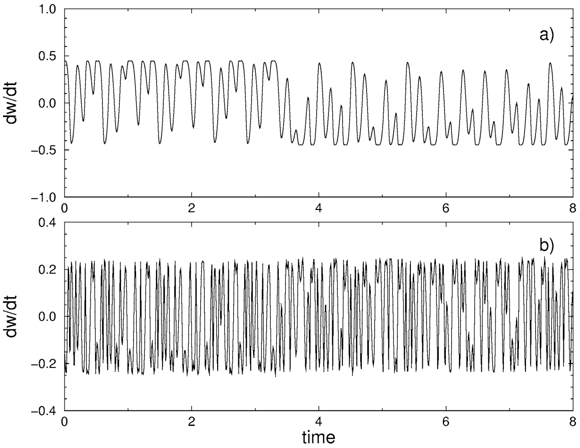

Fig. 9. Time-series generated by the dynamical system (26)–(29): (a) $g(x) = 4X^3 - 3X$; (b) $g(x) = (1/256)(88179X^{11} - 230945 \times X^9 + 218790X^7 - 90090X^5 + 15015X^3 - 693X)$.

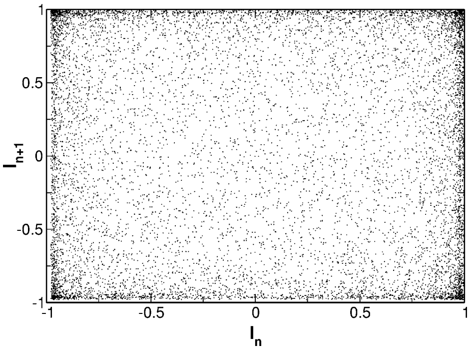

Fig. 10. First-return map of the time-series generated with real data from an experiment with an analog Josephson junction coupled to the Chua's circuit.

the creation of electronic analogs that can simulate the Josephson junction [45–48]. In that case k can be a parameter with different numerical values.

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

In our experiments we have used the Josephson junction analog constructed by Magerlein [48]. 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 [48].

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 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 10000.

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 [40]. For this, we have implemented the Chua's circuit following the recipe of Ref. [44].

The scheme of the Chua's circuit constructed by us can be found in Fig. 1 of Ref. [44].

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 [44].

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 differential equations that describe our experimental system are the following:

$$\frac{dV_1}{dt} = 6.3(V_2 - V_1) - 9f(V_1), \tag{32}$$

$$\frac{dV_2}{dt} = 0.7(V_1 - V_2) + I_L, \tag{33}$$

$$\frac{dI_L}{dt} = -7V_2, \tag{34}$$

$$\frac{d\phi}{dt} = kV_1, \tag{35}$$

$$\frac{dQ}{dt} = \sin\phi, \tag{36}$$

where $f(V_1) = -0.5[V_1 + 0.3(|V_1 + 1| - |V_1 - 1|)]$ and $k = 10^4$. Notice that this system has been rewritten using adimensional variables (see Ref. [44]).

The results of the experiments are shown in Fig. 10 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. Fig. 11 shows the results of the simulation of dynamical system (32)–(36).

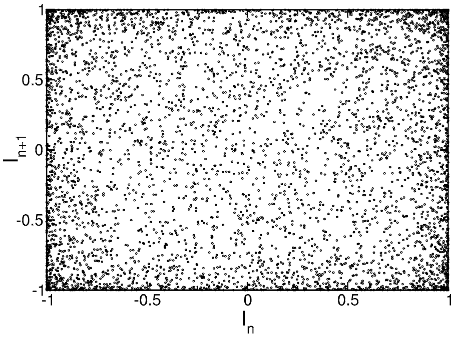

Fig. 11. First-return map of the time-series generated by the dynamical system (32)–(36). Here $I = dQ/dt$.

6. 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 [49]. In this context, the most important application of our systems is masking messages using random signals [50]. 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 Letter "deterministic randomness". The words "deterministic randomness" have been used (metaphorically) in the past as a name for chaos. However, the known chaotic systems are not random. So we think this is a good name for the present phenomenon.

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

Deterministic randomness 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, deterministic randomness 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 (20)–(22), 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 type (8)–(10) or (20)–(22). In these cases, some prediction is possible.

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, 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) 13583.
[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. Bifurc. Chaos 10 (2000) 1867;
J.A. González, L.I. Reyes, L.E. Guerrero, Chaos 11 (2001) 1.
[15] P. Grassberger, I. Proccacia, Physica D 9 (1983) 189;
Wolf, J.B. Swift, H.L. Swinney, J.A. Vastano, Physica D 16 (1985) 285.
[16] A.M. Ferrenberg, D.P. Landau, Y.J. Wong, Phys. Rev. Lett. 69 (1992) 3382.
[17] F. James, Comput. Phys. Commun. 60 (1990) 329.
[18] F. James, Chaos Solitons Fractals 6 (1995) 221.
[19] J.J. Collins, M. Fanciulli, R.G. Hohlfeld, D.C. Finch, G.v.H. Sandri, E.S. Shtatland, Comput. Phys. 6 (1992) 630.
[20] D.E. Knuth, Seminumerical Algorithms, The Art of Computer Programming, Vol. 2, Addison-Wesley, Reading, MA, 1981.
[21] S. Park, K. Miller, Commun. Am. Chem. Soc. 31 (1988) 1192.
[22] J.L. Doob, Stochastic Processes, Wiley, New York, 1991.
[23] L.M. Berliner, Statist. Sci. 7 (1992) 69.
[24] R.M. D'Souza, Y. Bar-Yam, M. Kardar, Phys. Rev. E 57 (1998) 5044.
[25] J. Nogués, J.L. Costa-Krämer, K.V. Rao, Physica A 250 (1998) 327.
[26] M.E. Fisher, Physica A 263 (1999) 554.
[27] G. Marsaglia, Proc. Natl. Acad. Sci. 61 (1968) 25.
[28] G. Marsaglia, in: L. Billard (Ed.), Computer Science and Statistics: The Interface, Elsevier, Amsterdam, 1985.
[29] G. Marsaglia, B. Narasimhan, A. Zaman, Comput. Phys. Commun. 60 (1990) 345.
[30] I. Vattulainen, T. Ala-Nissila, K. Kankaala, Phys. Rev. Lett. 73 (1994) 2513.
[31] L.N. Shchur, J.R. Heringa, H.W.J. Blöte, Physica A 241 (1997) 579.
[32] T.Y. Li, J.A. Yorke, Nonlinear Anal. Theory Methods Appl. 2 (1978) 473.
[33] S.C. Phatak, S.S. Rao, Phys. Rev. E 51 (1995) 3670.
[34] R.L. Kautz, J. Appl. Phys. 86 (1999) 5794.
[35] A. Proykova, Comput. Phys. Commun. 124 (2000) 125.
[36] T. Stojanovski, L. Kocarev, IEEE Trans. Circuits Syst. I 48 (2001) 281.
[37] T. Stojanovski, L. Kocarev, IEEE Trans. Circuits Syst. I 48 (2001) 382.
[38] R. Bernardini, G. Cortelazzo, IEEE Trans. Circuits Syst. I 48 (2001) 552.
[39] L.O. Chua, C.A. Desoer, E.S. Kuh, Linear and Nonlinear Circuits, McGraw-Hill, New York, 1987.
[40] T. Matsumoto, L.O. Chua, M. Komoro, IEEE Trans. Circuits Syst. CAS-32 (1985) 797;
T. Matsumoto, L.O. Chua, M. Komoro, Physica D 24 (1987) 97.
[41] A. Rodríguez-Vásquez, J.L. Huertas, A. Rueda, B. Pérez-Verdú, L.O. Chua, Proc. IEEE 75 (1987) 1090.
[42] A.S. Huang, L. Pirka, M. Franz, Int. J. Bifurc. Chaos 6 (1996) 2175.
[43] 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, New York, 1986.
[44] M.P. Kennedy, Frequenz 46 (1992) 66.
[45] N.R. Werthamer, S. Shapiro, Phys. Rev. 164 (1967) 523.
[46] C.A. Hamilton, Rev. Sci. Instrum. 43 (1972) 445.
[47] C.K. Bak, N.F. Pedersen, Appl. Phys. Lett. 22 (1973) 149.
[48] J.H. Magerlein, Rev. Sci. Instrum. 49 (1978) 486.
[49] 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.
[50] R. Brown, L.O. Chua, Int. J. Bifurc. Chaos 6 (1996) 219;
Y.Y. Chen, Europhys. Lett. 34 (1996) 24.