International Journal of Bifurcation and Chaos, Vol. 30, No. 8 (2020) 2050116 (8 pages)

DOI: 10.1142/S0218127420501163

A Chaotic Circuit for Producing Gaussian Random Numbers

J. C. Sprott
Department of Physics, University of Wisconsin–Madison, Madison, Wisconsin 53706, USA
sprott@physics.wisc.edu

W. J. Thio
Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, Michigan 48109, USA
thio@umich.edu

Received July 29, 2019; Revised October 14, 2019

One of the main applications for chaotic circuits is the production of aperiodic signals with many of the characteristics of noise for secure communications and similar uses. However, the probability distribution function (pdf) of such signals is usually far from Gaussian. This paper describes a new chaotic circuit based on the recently proposed signum thermostat that produces signals whose pdf is accurately Gaussian. Data from the constructed circuit are analyzed and shown to be in agreement with the theoretical prediction.

Keywords: Chaos; harmonic oscillator; thermostat; ergodicity; Gaussian distribution.

1. Introduction

Random numbers have a wide variety of applications including Monte-Carlo simulations [Binder & Heermann, 2002] and cryptography [Stinson, 2006]. Since the dawn of the computer age, computer algorithms have been developed to meet this need [Knuth, 1981]. These digital "pseudorandom number generators" have the virtues of reproducibility and portability, but they are inherently flawed as a consequence of their deterministic basis, although they can be made to pass all conventional tests for randomness [Press *et al.*, 2007]. As a consequence, hardware-based random number generators have been developed, usually based on some quantum process such as radioactive decay or on thermal noise [Dube, 2008]. The more recent development of chaotic electrical circuits has now provided a deterministic alternative based on Lyapunov instability [Kocarev & Lian, 2011].

Chaotic systems share many of the properties of random systems, but they rarely produce signals whose probability distribution function is even approximately Gaussian. For many years, there has been a concerted effort by molecular dynamicists to devise simple mathematical models with such a property, most of which are only approximate. Such a system would model the fluctuations in the energy of a harmonic oscillator in thermal equilibrium with a heat bath at constant temperature.

One of the earliest such attempts was the *Nosé–Hoover oscillator* [Nosé, 1984; Hoover, 1985],

$$\dot{x} = y, \quad \dot{y} = -x - zy, \quad \dot{z} = y^2 - T. \tag{1}$$

With $T = 1$, this system is also known in the literature as the *Sprott A system* [Sprott, 1994] since it was independently discovered in a systematic search for three-dimensional chaotic flows with only five terms and two quadratic nonlinearities. It is

somewhat unusual because it lacks any equilibrium points provided $T > 0$.

Absent the zy term, this system would be a simple harmonic oscillator with angular frequency $\omega = 1$. The zy term represents a nonlinear damping of the oscillator [Sprott & Hoover, 2017] that removes energy when z is positive and adds energy when z is negative, with z averaging exactly to zero, $\langle z \rangle = 0$. The z variable provides negative feedback to the energy and thus acts like a "thermostat," maintaining the time-averaged energy of the oscillator $\langle E \rangle = \frac{1}{2}\langle x^2 \rangle + \frac{1}{2}\langle y^2 \rangle$ equal to T which can be considered as a dimensionless temperature, but with large fluctuations about the average. Equation (1) is sometimes written with different or additional parameters, but it is inherently a one-parameter system through an appropriate transformation of the variables, and so the use of T as the parameter is convenient but arbitrary.

The resulting system shares many of the properties of a Hamiltonian system except that the energy is allowed to fluctuate in time rather than being rigidly fixed. Such systems are said to be *isothermal* rather than *isoenergetic* and to be *nonuniformly conservative* [Heidel & Zhang, 1999]. As with other conservative systems, Eq. (1) is time-reversible since the transformation $(x, y, z, t) \rightarrow (x, -y, -z, -t)$ leaves the equations unchanged. This three-dimensional modification of the simple harmonic oscillator has chaotic solutions as required for the orbit to visit all points in (x, y) phase space as expected for a physical oscillator in contact with a real heat bath.

A perfect molecular model would have its energy $E = \frac{1}{2}x^2 + \frac{1}{2}y^2$ distributed according to a *Boltzmann factor* $P(E) = e^{-E/T}/T$ with a Gaussian distribution of $P_x = e^{-x^2/2T}/\sqrt{2\pi T}$ and $P_y = e^{-y^2/2T}/\sqrt{2\pi T}$. In fact, a distribution of that form is preserved (constant in time) by Eq. (1) provided P_z is equal to $e^{-z^2/2T}/\sqrt{2\pi T}$ as one can verify by calculating the time derivative of $P(x, v, z) = P_x P_y P_z$ at a fixed position in state space which is given by

$$\dot{P} \equiv \frac{\partial(P\dot{x})}{\partial x} + \frac{\partial(P\dot{y})}{\partial y} + \frac{\partial(P\dot{z})}{\partial z} = 0. \qquad (2)$$

This is a necessary but not a sufficient condition for producing a Gaussian probability distribution of $P(x, v, z)$.

In fact, Eq. (1) fails to generate the entire canonical distribution, but rather it traces out only a small part of it depending on the initial values of (x, y, z). For initial conditions chosen randomly from a Gaussian measure with $T = 1$, 94% of the orbits are quasiperiodic and lie on two-dimensional tori that surround an infinite number of stable one-dimensional periodic orbits. The remaining 6% of the initial conditions lie in a surrounding three-dimensional chaotic sea [Hoover & Hoover, 2018]. Trajectories within the sea eventually come arbitrarily close to any point within it. Thus the Nosé–Hoover system is not *ergodic*.

2. Signum Thermostat

A simple modification of the Nosé–Hoover system recently proposed by Sprott [2018] that exactly satisfies the desired conditions is the *signum thermostat* given by

$$\dot{x} = y, \quad \dot{y} = -x - a\,\mathrm{sgn}(z)y, \quad \dot{z} = y^2 - T \qquad (3)$$

for $a > 1.7$. Smaller values of a allow initial conditions that lie on tori and give quasiperiodic orbits. These tori shrink in size until the last one that passes near the points $(\pm\pi, 0, 0)$ vanishes when a exceeds 1.7. Equation (3) can be viewed as a limiting case of a recently proposed *logistic thermostat* [Tapias *et al.*, 2017] with which it shares many properties.

This system is ergodic in the sense that for any initial conditions (except along the line $x = y = 0$), it will eventually come arbitrarily close to every point in (x, y, z) space. Hence it does not have an attractor, but rather the chaotic sea fills all of space. The damping term $-a\,\mathrm{sgn}(z)y$ averages to zero over a sufficiently long time. Because $\mathrm{sgn}(z)$ abruptly switches between $+1$ and -1 when z crosses zero, it is called a *bang-bang controller*. The furnace turns on and off abruptly and fully, but the heat flow to or from the oscillator is controlled by the parameter a, which arguably better models a real thermostat than does the *proportional controller* in Eq. (1).

Furthermore, the probability distribution of x and y is Gaussian, while the probability P_z is governed by $T\frac{dP_z}{dz} = -aP_z\,\mathrm{sgn}(z)$, whose normalized solution is exponential and given by $P_z = (a/2T)e^{-a|z|/T}$. The Gaussian probability P_x and P_y are independent of a with a width that depends only on T.

Finally, unlike Eq. (1), Eq. (3) has the nice property that the $\dot{x}$ and $\dot{y}$ equations are linear except at $z = 0$, and so the dynamics is independent

of the amplitude of the oscillation. Said differently, T is an *amplitude parameter* [Li & Sprott, 2013] that only affects the magnitude of the variables and thus can be taken as unity without loss of generality. If the system is ergodic and Gaussian for *any* temperature, it is ergodic and Gaussian for *every* temperature, and it has only a single bifurcation parameter a, which facilitates analysis of the system, especially because the system is two-dimensional and linear for $z \neq 0$. Since our interest is in ergodic solutions, we will hereafter take $a = 2$, which is comfortably in excess of 1.7.

3. Numerical Solutions

The parameters $a = 2$ and $T = 1$ give the predicted chaotic orbit in Fig. 1. The colors indicate the value of the local largest Lyapunov exponent with red positive and blue negative. Since the chaotic sea fills the whole of space, initial conditions are arbitrary and are taken as $(x_0, y_0, z_0) = (1, 1, 1)$ here and elsewhere. Calculations are done using a fourth-order Runge–Kutta integrator with adaptive step size and stringent error control.

The time series for $x(t)$ is shown in Fig. 2. As expected for a nonlinearly damped harmonic oscillator, there is a dominant frequency ($\omega \approx 1$ for this case), but with a broad-band power spectral density as is characteristic of a chaotic system.

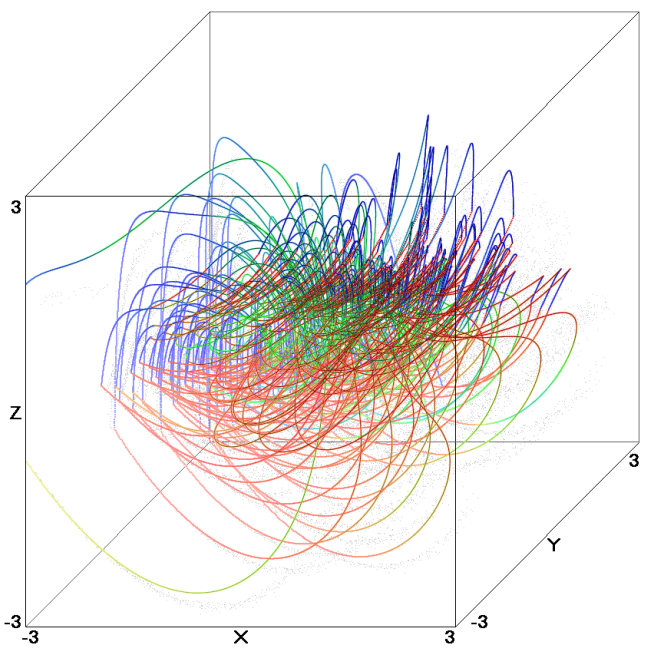


Fig. 1. Numerical solution of Eq. (3) with $a = 2$ and $T = 1$. The colors indicate the value of the local largest Lyapunov exponent with red positive and blue negative.

The time series for $y(t)$ is similar. The Lyapunov exponents are $(0.3032, 0, -0.3032)$ and sum to zero as they must for a conservative system, with a Kaplan–Yorke dimension [Kaplan & Yorke, 1979] of $D_{\mathrm{KY}} = 3$, as expected for an orbit that visits every point in the three-dimensional state space.

The main evidence that the system is ergodic comes from the cross-section of the flow in Fig. 3 showing 10^8 crossings of the $z = 0$ plane. Regions of quasiperiodicity would have appeared as "holes" in the chaotic sea, and none are evident. The two horizontal stripes at $y = \pm 1$ are the z-nullclines, where $\dot{z} = 0$ and the flow is tangent to the $z = 0$ plane. As before, the colors indicate the value of the local largest Lyapunov exponent. Although the colors show considerable spatial structure, the measure (local probability distribution) is perfectly smooth.

The evidence that the distributions are Gaussian comes from the histograms in Fig. 4 showing 6×10^8 values of the three variables along with the theoretical predictions and the even moments of the distributions. The odd moments are negligibly small. The mth even moments agree to within statistical uncertainty with the theoretical predictions of P_x and P_y given by $\langle x^m \rangle = \langle y^m \rangle = (m-1)!! = \{0, 1, 3, 15, 105, 945, \ldots\}$, and P_z given by $\langle z^m \rangle = m!/a^m = \{0, 0.5, 1.5, 11.25, 157.5, 3543.75, \ldots\}$ for $a = 2$.

Although the distributions are accurately Gaussian, successive values are not independent since they come from a deterministic flow, making the values not truly random and hence not suitable for some purposes. However, since the system is chaotic, information about the initial condition is destroyed at an exponential rate given by the largest Lyapunov exponent ($\lambda_1 = 0.3032$ in this case). Hence we would expect successive values separated in time by $\Delta t \gg 1/\lambda_1 \approx 3$ to be independent. More precisely, if it is required for the most significant d digits of the values to be independent, the sample interval should exceed approximately $\Delta t \approx d \ln(10)/\lambda_1 \approx 8d$. Thus to obtain values with four digits of independence requires $\Delta t \approx 32$.

One way to illustrate the effect of serial correlation is to plot each value of $x(t)$ versus the value of $x(t - \Delta t)$ as shown in Fig. 5 for 10^5 points with four values of Δt. Recall that the dominant frequency of oscillation is $\omega \approx 1$, so that $\Delta t = 1$ represents only one radian (≈ 57 degrees) so that successive values have a strong positive correlation. On the other hand, $\Delta t = 3$ represents about 172 degrees, and

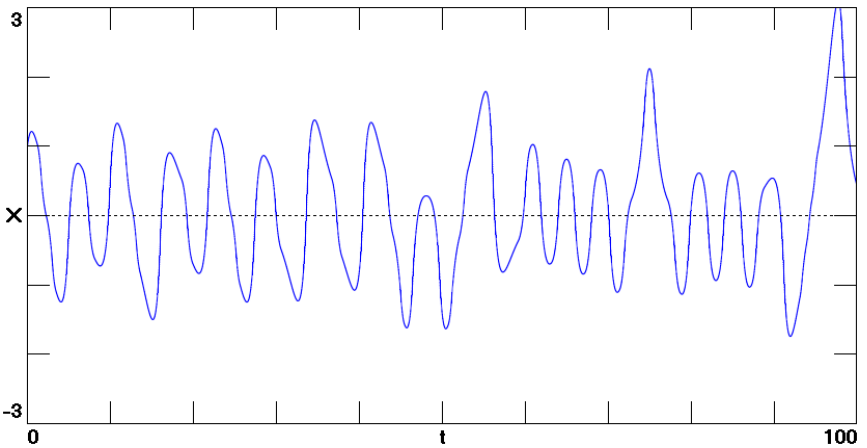


Fig. 2. Numerical waveform for $x(t)$ from Eq. (3) with $a = 2$ and $T = 1$. The $y(t)$ waveform is similar.

there is a strong negative correlation shown in the figure as a 90° rotation of the plot. The correlation decreases with increasing Δt, becoming undetectable in the figure for $\Delta t = 30$ as expected. Similar results occur for the other variables.

Another way to view the decay of the serial correlation is by plotting the *time-lag correlation function* between two variables such as x and y given by

$$C_{xy}(\Delta t) = \frac{\langle x(t)y(t-\Delta t)\rangle}{\sqrt{\langle x^2(t)\rangle\langle y^2(t)\rangle}} \qquad (4)$$

versus Δt, where the angular brackets denote the time average, or in this case the average over many successive samples of the variables. Figure 6 shows the correlation function for the different variables with 4×10^6 points at each of the 400 values of Δt. The *autocorrelation function* C_{xx} shown in Fig. 6(a) is the Fourier transform of the power spectral density of the x variable, and the relatively narrow peak in the former implies a relatively broad peak in the latter as desired for a chaotic signal that emulates noise. As expected, the autocorrelation function is near zero for $\Delta t = \pm 30$. Note that the

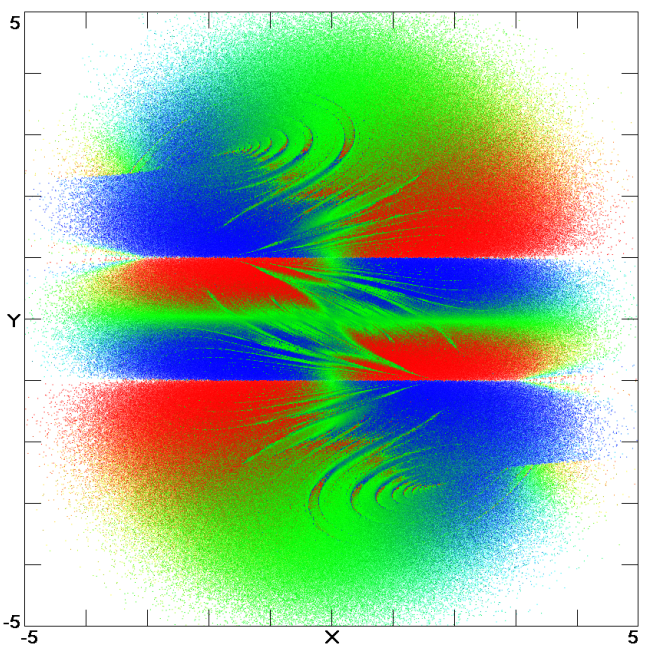


Fig. 3. Cross-section for the flow in Eq. (3) at $z = 0$ for $a = 2$ and $T = 1$. The colors indicate the value of the local largest Lyapunov exponent with red positive and blue negative.

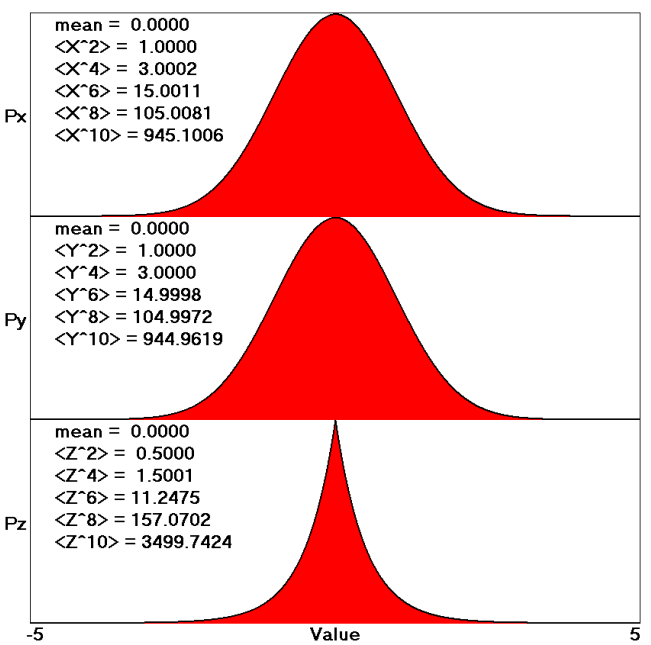


Fig. 4. Probability distributions and their even moments for the three variables of Eq. (3) with $a = 2$ and $T = 1$. The expected distributions are shown as black lines at the edge of the red regions.

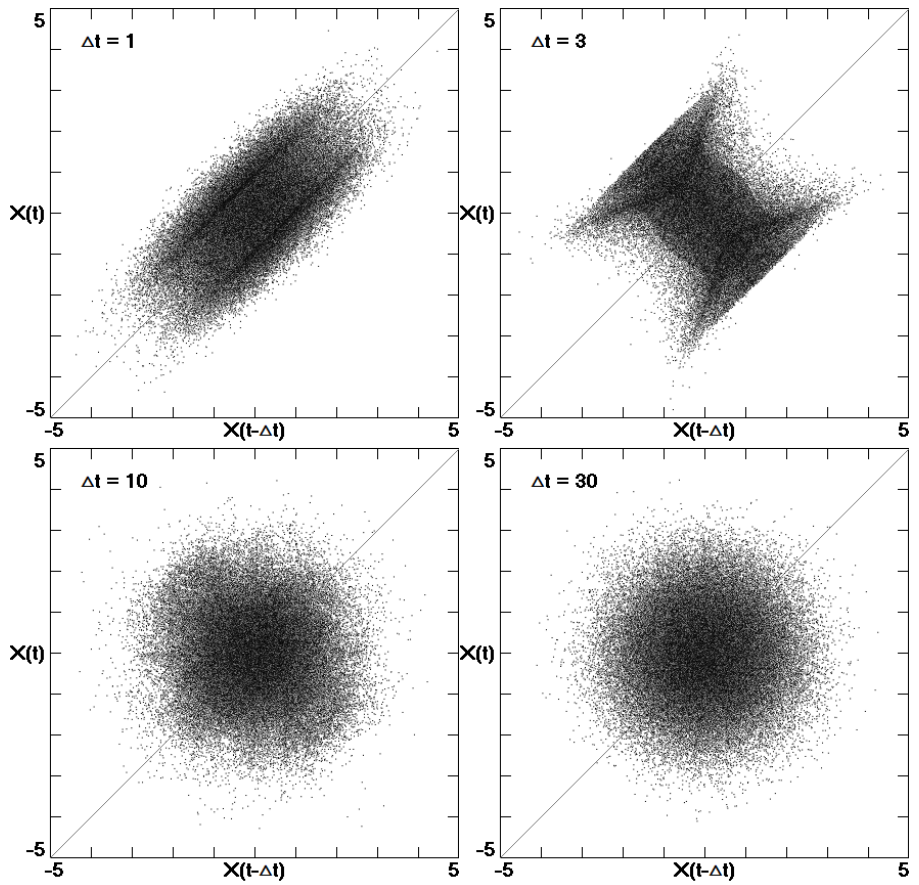
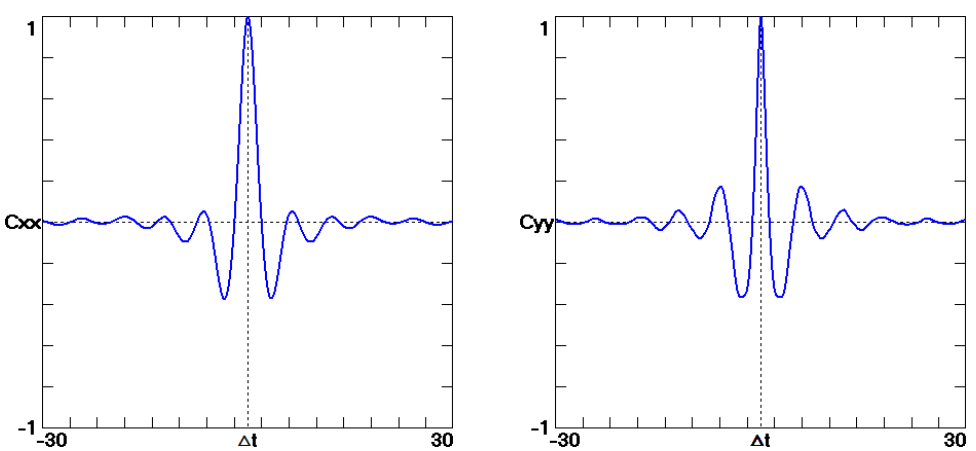
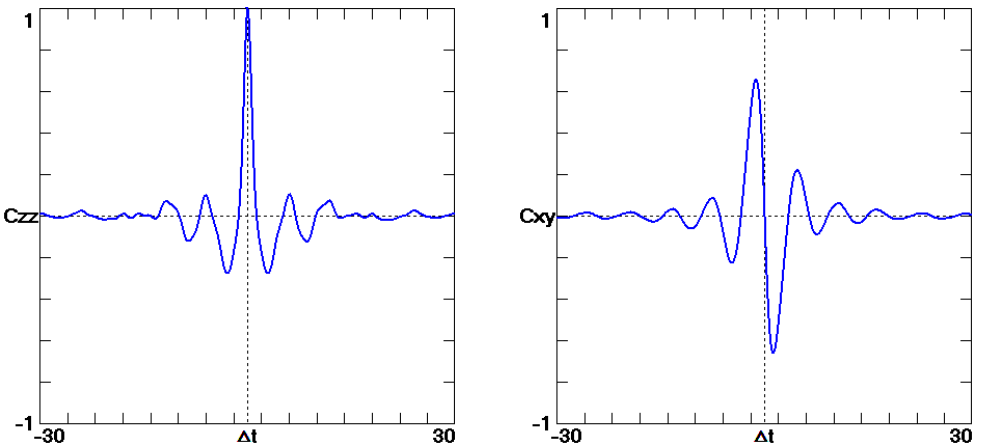


Fig. 5. Return map for the x variable of Eq. (3) with $a = 2$ and $T = 1$ for increasing time lags Δt.



(a) (b)

Fig. 6. Time-lag correlation function for the different variables of Eq. (3) with $a = 2$ and $T = 1$ as a function of the time lag Δt.



(c) (d)

Fig. 6. (*Continued*)

cross-correlation function C_{xy} in Fig. 6(d) is zero at $\Delta t = 0$, which means that Eq. (3) can produce two independent Gaussian random numbers x and y if sampled at the same instant. The correlation functions C_{xz} and C_{yz} are zero within statistical error for all values of the time lag and hence are not shown.

4. Circuit Implementation

It is straightforward to construct an electrical circuit whose voltages correspond to the variables in Eq. (3) with $a = 2$ and $T = 1$ as shown in Fig. 7. The component values are $R_3 = 7.5\,\mathrm{k\Omega}$, $R_6 = R_9 = 1\,\mathrm{k\Omega}$, $R_7 = 150\,\mathrm{k\Omega}$, $R_8 = 1000\,\mathrm{k\Omega}$, and $R_{10} = 2\,\mathrm{k\Omega}$, with the other resistors equal to $10\,\mathrm{k\Omega}$, $C_1 = C_2 = C_3 = 1\,\mu\mathrm{F}$, $C_4 = 0.001\,\mu\mathrm{F}$, and $V_5 = V_6 = 15\,\mathrm{V}$, which corresponds to the parameter $T = 1$ in Eq. (3) and sets the magnitude for all the voltages and currents in the circuit. The AD633 analog multiplier has a factor of ten attenuation to prevent saturation. It is useful to use a high-speed amplifier such as an LT1226 for the comparator to ensure accurate implementation of the signum function. The circuit as designed runs at a relatively low frequency of ~ 100 radians per second ($\sim 16\,\mathrm{Hz}$), but can be rescaled to run at any rate determined by limitations of the amplifiers and multipliers.

To use the circuit to produce Gaussian random numbers, it is only necessary to sample the instantaneous value of V_1 or V_2 (they both have a Gaussian distribution with the same variance) whenever a new value is desired. If the interval between samples is sufficiently large (much larger than the Lyapunov time), successive samples are uncorrelated through

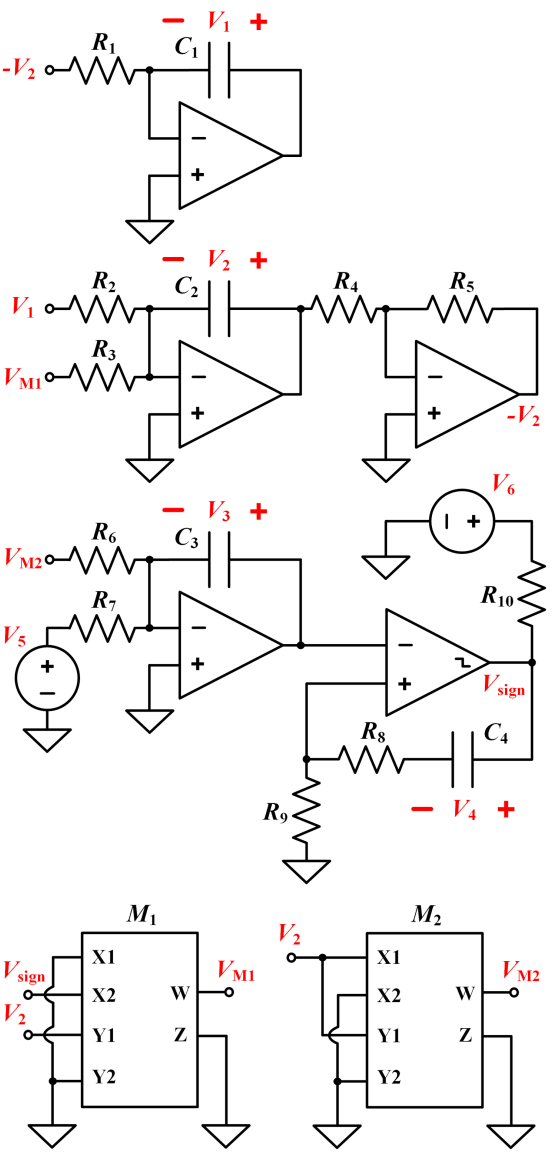


Fig. 7. Electrical circuit for the implementation of Eq. (3).

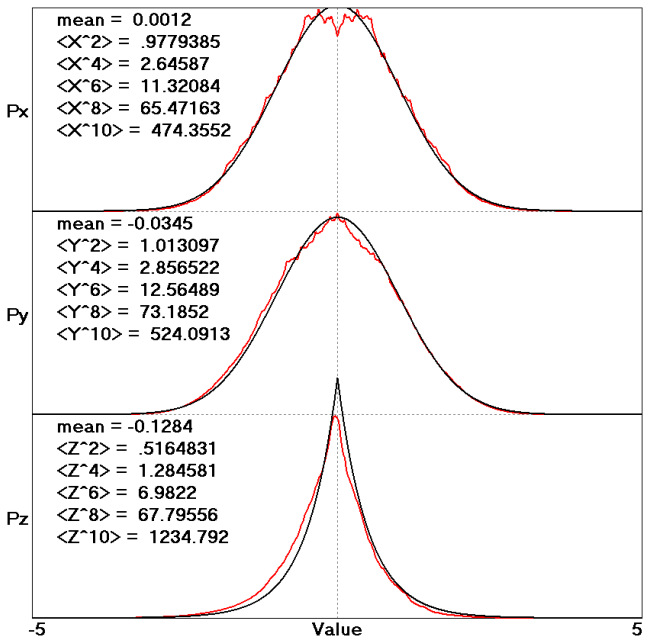


Fig. 8. Probability distributions (in red) and their even moments for ten million samples of the voltages V_1, V_2, and V_3 (resp., P_x, P_y, and P_z) in Fig. 7. The expected distributions are shown as black lines.

Lyapunov instability, although that may not be necessary for some applications. The result of such a process in which ten million samples were taken at a sample rate of 100 Hz (10^5 s or about 28 h) is shown in Fig. 8 and confirms that the distributions for V_1 and V_2 (resp., P_x and P_y) are Gaussian as predicted. The distribution function for V_3 is expected to be given by $P_z = e^{-2|z|}$ in good agreement with the measurement.

The notch near $P_x = 0$ and the asymmetry in P_z in Fig. 8 are attributed to hysteresis in the comparator. This hysteresis makes the comparator switch at values close to zero rather than exactly at zero. Most comparators are designed to have hysteresis to prevent signal noise from causing premature or erratic switching when the signal is small, which can cause errors in timing circuits such as a digital clock. The notch and asymmetry occur when the hysteresis exceeds approximately ± 1 mV.

The comparator can be further modified to have adjustable hysteresis threshold limits by adding an external circuit that provides positive feedback. This circuit is also known as a *Schmitt trigger*. Here C_4, R_8, and R_9 set a hysteresis threshold that decays with time, allowing the comparator to switch exactly at zero while preventing oscillation. C_4 is set to a small value to allow this threshold to quickly decay, and its voltage V_4 is not a part of the dynamical equations. R_{10} is a pullup resistor that should be connected to the +15 V source (represented as V_6) to allow the comparator to saturate quickly.

The small hysteresis limits of the notch and asymmetry in the probability distribution also suggests a sensitivity to noise within ± 1 mV, which can be reduced through low-noise operational amplifiers and 0.1 μF bypass capacitors to remove power supply noise. Additionally, pins 5 and 6 of the LM311 comparator should be connected together since these unused pins can pick up noise. These techniques improve the probability distribution, but do not completely remove the notch and asymmetry. Further work on this circuit could investigate methods to reduce the noise below ± 1 mV.

Normally, it would be difficult or impossible to construct an electrical circuit for a conservative dynamical system because even the slightest damping or anti-damping would cause the oscillations to decay or grow without limit until something in the circuit saturates. However, this nonuniformly conservative system uses negative feedback to control the average energy of the oscillation, and thus it is highly robust. Since it lacks equilibrium points and the chaotic sea fills the whole of state space, initial conditions are arbitrary, and the circuit cannot fail to oscillate for any choice of the parameters or of the corresponding circuit components.

5. Summary and Conclusions

The signum thermostat applied to the simple harmonic oscillator gives a particularly simple three-dimensional dynamical system whose solution is ergodic (the orbit eventually comes arbitrarily close to every point in the space) and whose variables have an exact Gaussian probability distribution function. The equations lead directly to a simple electrical circuit whose chaotic oscillations have the same property.

Although the circuit as described is inherently slow, producing just a few dozen independent and identically distributed random numbers per second, much faster versions are possible in principle, limited only by the speed of the circuit components. Furthermore, the quality of the random numbers is ensured by the Lyapunov instability of the underlying chaotic system. Such a circuit has potential application wherever Gaussian random numbers are required, and the successive values are independent

for a sufficient, well-prescribed interval between samples.

References

Binder, K. & Heermann, D. W. [2002] *Monte Carlo Simulation in Statistical Physics*: *An Introduction*, 4th edition (Springer, Berlin).

Dube, R. R. [2008] *Hardware-Based Computer Security Techniques to Defeat Hackers*: *From Biometrics to Quantum Cryptography* (Wiley, NY).

Heidel, J. & Zhang, F. [1999] "Nonchaotic behavior in three-dimensional quadratic systems II: The conservative case," *Nonlinearity* **12**, 617–633.

Hoover, W. G. [1985] "Canonical dynamics: Equilibrium phase-space distributions," *Phys. Rev. A* **31**, 1695–1697.

Hoover, W. G. & Hoover, C. G. [2018] *Microscopic and Macroscopic Simulation Techniques — The Kharagpur Lectures* (World Scientific, Singapore).

Kaplan, J. & Yorke, J. [1979] "Chaotic behavior of multidimensional difference equations," *Functional Differential Equations and Approximation of Fixed Points*, Lecture Notes in Mathematics, Vol. 730, eds. Peitgen, H.-O. & Walther, H.-O. (Springer, Berlin, Heidelberg), pp. 477–482.

Knuth, D. E. [1981] *The Art of Computer Programming*, Seminumerical Algorithms, Vol. 2, 2nd edition (Addison-Wesley, Reading, MA).

Kocarev, L. & Lian, S. (eds.) [2011] *Chaos-Based Cryptography*: *Theory, Algorithms and Applications* (Springer, Berlin).

Li, C. & Sprott, J. C. [2013] "Amplitude control approach for chaotic signals," *Nonlin. Dyn.* **73**, 1335–1341.

Nosé, S. [1984] "A unified formulation of the constant temperature molecular dynamics methods," *J. Chem. Phys.* **81**, 511–519.

Press, W. H., Flannery, B. P., Teukolsky, S. A. & Vetterling, W. T. [2007] *Numerical Recipes*: *The Art of Scientific Computing*, 3rd edition (Cambridge University Press, Cambridge).

Sprott, J. C. [1994] "Some simple chaotic flows," *Phys. Rev. E* **50**, R647–R650.

Sprott, J. C. & Hoover, W. G. [2017] "Harmonic oscillators with nonlinear damping," *Int. J. Bifurcation and Chaos* **27**, 1730037-1–19.

Sprott, J. C. [2018] "Ergodicity of one-dimensional oscillators with a signum thermostat," *Comput. Meth. Sci. Technol.* **24**, 169–176.

Stinson, D. R. [2006] *Cryptography*: *Theory and Practice*, 3rd edition (CRC Press, Boca Raton).

Tapias, D., Bravetti, A. & Sanders, D. P. [2017] "Ergodicity of one-dimensional systems coupled to the logistic thermostat," *Comput. Meth. Sci. Technol.* **23**, 11–18.