Chaos in a ring circuit

Cite as: Chaos **29**, 043103 (2019); https://doi.org/10.1063/1.5079941
Submitted: 05 November 2018 . Accepted: 05 March 2019 . Published Online: 05 April 2019

E. Farcot, S. Best, R. Edwards, I. Belgacem, X. Xu, and P. Gill

Chaos ARTICLE scitation.org/journal/cha

Chaos in a ring circuit

Cite as: Chaos **29**, 043103 (2019); doi: 10.1063/1.5079941
Submitted: 5 November 2018 · Accepted: 5 March 2019 ·
Published Online: 5 April 2019

E. Farcot,[1,a)] S. Best,[2,b)] R. Edwards,[3,c)] I. Belgacem,[3,d)] X. Xu,[4,e)] and P. Gill[5,f)]

AFFILIATIONS

[1]School of Mathematical Sciences, University of Nottingham, United Kingdom
[2]Rambus Inc., Sunnyvale, California, USA
[3]Department of Mathematics and Statistics, University of Victoria, British Columbia, Canada
[4]Electrical and Computer Engineering, University of Illinois at Chicago, Chicago, Illinois, USA
[5]Sunnyvale, California 94085, USA

[a)]**Electronic mail:** etienne.farcot@nottingham.ac.uk
[b)]**Electronic mail:** sbest@rambus.com
[c)]**Electronic mail:** edwards@uvic.ca
[d)]**Electronic mail:** ismailbelgacem@uvic.ca
[e)]**Electronic mail:** xiaolin8@uic.edu
[f)]**Electronic mail:** patrick.robert.gill@gmail.com

ABSTRACT

A ring-shaped logic circuit is proposed here as a robust design for a True Random Number Generator (TRNG). Most existing TRNGs rely on physical noise as a source of randomness, where the underlying idealized deterministic system is simply oscillatory. The design proposed here is based on chaotic dynamics and therefore intrinsically displays random behavior, even in the ideal noise-free situation. The paper presents several mathematical models for the circuit having different levels of detail. They take the form of differential equations using steep sigmoid terms for the transfer functions of logic gates. A large part of the analysis is concerned with the hard step-function limit, leading to a model known in mathematical biology as a Glass network. In this framework, an underlying discrete structure (a state space diagram) is used to describe the likely structure of the global attractor for this system. The latter takes the form of intertwined periodic paths, along which trajectories alternate unpredictably. It is also invariant under the action of the cyclic group. A combination of analytical results and numerical investigations confirms the occurrence of symmetric chaos in this system, which when implemented in (noisy) hardware, should therefore serve as a robust TRNG.

Random number generators (RNGs) are an essential element of most cryptographic systems. Many RGN designs rely on an oscillating ring circuit structure, in which physical noise is leveraged to generate random alterations of the periodic behavior. This paper discusses an alternative approach, where a ring circuit is intrinsically able to generate chaos rather than periodic oscillations. We introduce and analyze several models of this circuit. The analysis aims to show that these models present chaotic dynamics, which provides the circuit with inherent unpredictability, even before considering the noise inherent in the physical circuit. To achieve this, we use a combination of analytical and numerical approaches.

I. INTRODUCTION

RNGs are an essential element of most cryptographic systems.[1] The unpredictable values they generate are useful for many applications, including secret-key generation and challenge generation for challenge/response authentication. Yet, the design complexity of a high-performance True Random Number Generator (TRNG)—one in which the entropy is derived from a truly random physical characteristic that is difficult to measure and predict (e.g., thermal noise, metastability)—can be incompatible with low cost. Most proposed TRNGs leveraging such random physical features require special-purpose analog circuits, which limit their applicability to a low-cost design. Therefore, for low-cost chip applications, an all-digital circuit implementation is preferred, one in which every circuit element in the TRNG is a simple logic gate that can be instantiated directly from the design's standard-cell library. Moreover, to ensure low cost and low risk, it is important that such an all-digital circuit be fully compatible with a standard VLSI design methodology, including synthesized RTL (Register Transfer Language) and auto-place-and-route circuit blocks, with minimum design constraints and no need for hands-on fine-tuning of critical

signaling paths. But even for large SoCs (Systems on a Chip) and high-performance processors that can afford the higher design cost of complex analog TRNG circuits, a highly portable all-digital RNG can provide benefit, as its outputs can be mixed together with the other on-die TRNG subsystems, thereby providing some entropy even in the case when an adversary successfully mitigates one of the TRNG elements.

The simplest and most well-known way to construct an all-digital TRNG is by sampling the error (jitter) between phases in ring oscillators. Such TRNGs are built from at least two free running oscillators, each of which is usually built by chaining an odd number of inverters in a feedback loop.[2–5] To sample the jitter, a detector is required for the phase differences between the outputs of ring oscillators, which can be implemented using XOR gates. A problem with true random number generators based on the sampling phase jitter in ring oscillators is that the phase can be locked with a frequency injection attack, which destroys or diminishes the randomness of their combined output, even in the case where the ring oscillators comprising the TRNG have different intrinsic frequencies.[6–9] This suggests that a TRNG with an intrinsic behavior that is more complex than a simple oscillator could be more robust to frequency injection attack.

In order to make a TRNG more robust against attack, we propose using a circuit that is inherently chaotic, also having the advantage of portability that comes from an all-digital design. S.B. designed a ring oscillator modified by feedforward and feedback between units in a way that implements the logic of Wolfram's Cellular Automaton Rule 30, as described in Sec. II and analyzed in the rest of this paper. Other analog electronic networks displaying complex, even chaotic, behavior have been proposed before. The most well known is probably Chua's circuit,[10] shown by Galias[11] to be chaotic, and studied quite extensively since (e.g., by Kuznetsov *et al.*[12,13]). Closer to the current idea are the ring oscillator-based circuits proposed by Hosokawa and Nishio[14] and by Dhanuskodi *et al.*[15] These designs, however, are less portable than the one proposed here, because they are not all-digital. The circuit of the current paper will be analyzed by methods derived from the theory of Glass networks, as used in qualitative modeling of gene regulation. Glass and colleagues have previously pointed out that standard electronic circuits are governed by essentially the same class of equations, and electronic implementations of Glass networks were built and studied.[16] Other researchers have used Glass network equations to study ring oscillators without identifying them as such (e.g., Srivastava and Roychowdhury[17]). Chaotic dynamics in electronic circuit implementations of Glass networks have also been studied.[18] Various alternative designs for chaotic Glass networks (Ref. 38) might also be investigated in future as potential TRNGs.

The paper is constructed as follows. After describing the circuit's architecture in Sec. II, we present a differential equation model of its dynamics, which in the limit of step response functions is exactly a Glass network. Simplified variants of the model with aggregated variables are also presented. We then proceed to study these models using both analytical observations and extensive numerical results. A final section (Sec. V) describes a discrete approximate model often used for Glass networks, allowing us to deduce some global properties of the structure of trajectories and attractors for the different models. A conclusion reviews the main findings of the paper.

II. THE CIRCUIT

This article is concerned with the the dynamical behavior of a circuit consisting of a ring of identical units, as depicted in Fig. 1.

Each unit (green box in Fig. 1) is composed of a logical function with three inputs

$$f(a, b, c) = a \oplus (b \vee c), \tag{1}$$

where $\oplus$ and $\vee$, respectively, denote the XOR and OR functions. The unit is followed by two inverters wired in series. The logical function, described using XOR and OR gates in the figure, corresponds to cellular automaton rule 30 in Wolfram's nomenclature.[19] A physical implementation of this circuit displays some highly irregular dynamical behavior and suggests that it could be used as a true random number generator (TRNG).

More specifically, the assumption is that this circuit displays chaotic dynamics, so that even in an ideal situation where all circuit's components have perfectly known characteristics, the slightest perturbations on the voltage fed to the circuit are amplified and lead to unpredictable changes in the long-term dynamics. In other words, the occurrence of chaos entails that the system is able to generate entropy on its own, even in the absence of any noise.

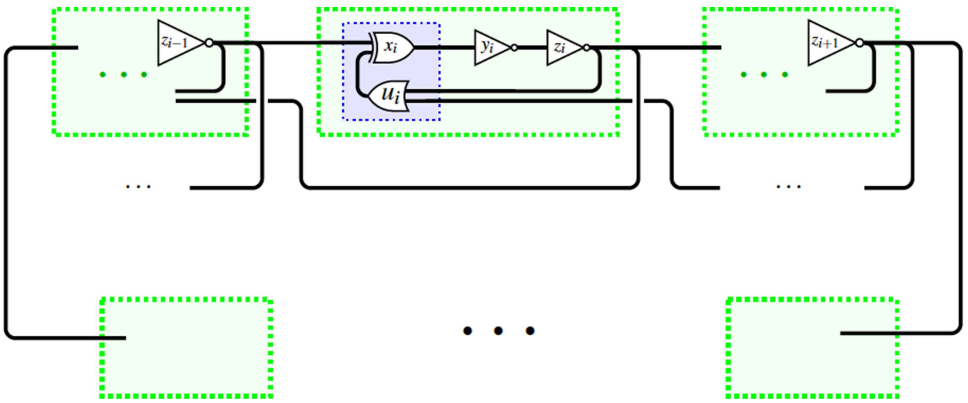


FIG. 1. The basic unit (within the green rectangle) receives input from the second inverter of both the previous and next units. Besides two inverters, each unit comprises a logical gate (blue rectangle) coding for the Boolean function $f(z_{i-1}, z_i, z_{i+1})$, see (1). The overall structure is periodic: $i \in \{1, \ldots, n\}$ and i is considered modulo n.

III. MODEL DEFINITION

One key assumption underlying the proposed mathematical models is that all logical gates involved in the circuit have a very steep response curve, almost step-like. Furthermore, the dynamics of interest must be robust to changes of parameters to avoid any dynamical property that would be sensitive to parameter choices, as any physical implementation of the circuit will have some imprecision in its quantitative characteristics.

To capture our assumption in a parameter insensitive way, we represent logical gates using a basic sigmoid response curve, which we allow to vary within a range of plausible choices. Specifically, we define

$$h^+(x) = \frac{1+\tanh[\beta(x-\theta)]}{2} \quad \text{or} \quad \frac{x^\beta}{\theta^\beta + x^\beta} \tag{2}$$

as two possible *sigmoid* shaped response curves, with β a steepness parameter and θ a threshold parameter. We also define

$$h^-(x) = 1 - h^+(x)$$

as the decreasing counterpart, which will be used to model inverter gates. Both the above functions will be considered and the notation $h^\pm$ may be used hereafter without further specification when discussing a property that is valid for both forms, usually under a condition that $\beta \gg 1$.

In fact, since the steepness parameter β is typically expected to be high, the limit $\beta \to \infty$ will also be considered, using the step functions

$$s^+(x) = \begin{cases} 0 & \text{if} \quad x < \theta, \\ 1 & \text{if} \quad x > \theta, \end{cases} \qquad \text{and} \quad s^-(x) = 1 - s^+(x).$$

The threshold value is left unspecified at this stage. The advantage of introducing step functions is that they lead to the models taking the form of piecewise-linear (PL) differential equations, for which analytical results can be obtained, unlike the case of smooth sigmoids. In addition, it is known that for β large enough, the phase portraits of a system with a sigmoid and a system with its PL limit are qualitatively similar in a large range of situations, and exceptions have been partly characterized.[20]

Unless stated otherwise, we use the step functions $s^\pm$ as a main model, as they allow for analytical developments to an extent that is not possible with their smooth counterpart. We proceed to define models with different levels of approximation, starting with the most realistic form. Subsequent models are obtained by lumping variables present in the initial formulation, which results in lower dimensional models.

As a generic notation, we denote the total number of variables by N in the following, where N will equal $4n$, $3n$, or n, for n units on the ring depending on the particular model as detailed in Secs. III A and III B.

A. "Full" 4*n*-dimensional model

Following the scheme in Fig. 1, we describe the system with the following system of differential equations:

$$\begin{aligned} \frac{dx_i}{dt} &= \kappa_{x_i}\left[s^+(z_{i-1})s^-(u_i) + s^-(z_{i-1})s^+(u_i)\right] - \gamma_{x_i}x_i, \\ \frac{dy_i}{dt} &= \kappa_{y_i}s^-(x_i) - \gamma_{y_i}y_i, \\ \frac{dz_i}{dt} &= \kappa_{z_i}s^-(y_i) - \gamma_{z_i}z_i, \\ \frac{du_i}{dt} &= \kappa_{u_i}\left[1 - s^-(z_i)s^-(z_{i+1})\right] - \gamma_{u_i}u_i, \end{aligned} \tag{3}$$

where x_i, y_i, z_i, and u_i represent the voltage measured at the output point of the corresponding gates in Fig. 1, and $i \in \{1, \ldots, n\}$ is taken modulo n. The parameters κ and γ, respectively, represent the maximum voltage and characteristic times (or RC constant, or delay) of the different gates. In each case, we suppose that the threshold is in the range allowing the variable to switch: e.g., $s^+(z_{i-1})$ has a threshold θ satisfying $0 < \theta < \frac{\kappa_{z_{i-1}}}{\gamma_{z_{i-1}}}$.

In this first formulation, all the logical gates are represented individually. Even with a fairly low number of units, the number of variables and parameters to consider is quickly high and even the dynamics of a single unit of the network is hard to depict graphically. This leads us to consider the lower dimensional models described in Sec. III B.

B. Lower dimensional models

Simplified models can be obtained by aggregating pairs of variables x_i and u_i, or y_i and z_i. This could be interpreted by saying that the discarded variables evolve fast, so that they are approximated by their steady state value, given exactly by the logical term in their right-hand side. Alternatively, this can be understood as a description of a related circuit having less logical gates, where, for instance, the two inverters are replaced by one non-inverting buffer, or two XOR and OR elements are replaced by a single, more complex gate. Either choice gives a $3n$-dimensional model [as opposed to $4n$ in (3)]. Note that the inverter element is the fastest (e.g., around 20 ps in a modern process node), the OR gate is the next fastest (around 30 ps), and the XOR gate is about the same as the non-inverting buffer (around 40 ps).[21] By grouping x_i and u_i (still denoted x_i for simplicity), i.e., considering the overall logic function performed in the blue area in Fig. 1 as a single gate with three inputs, Eq. (5), one obtains a model with only two distinct types of gate, and therefore two distinct decay parameters[22]

$$\begin{aligned} \frac{dx_i}{dt} &= \kappa_{x_i}g(z_{i-1}, z_i, z_{i+1}) - \gamma_{x_i}x_i, \\ \frac{dy_i}{dt} &= \kappa_{y_i}s^-(x_i) - \gamma_{y_i}y_i, \\ \frac{dz_i}{dt} &= \kappa_{z_i}s^-(y_i) - \gamma_{z_i}z_i, \end{aligned} \tag{4}$$

where $\kappa_{y_i} = \kappa_{z_i}, \gamma_{y_i} = \gamma_{z_i}$, and

$$\begin{aligned} g(z_{i-1}, z_i, z_{i+1}) &= f[s^+(z_{i-1}), s^+(z_i), s^+(z_{i+1})] \\ &= s^-(z_{i-1})\left[1 - s^-(z_i)s^-(z_{i+1})\right] \\ &\quad + s^+(z_{i-1})s^-(z_i)s^-(z_{i+1}) \end{aligned} \tag{5}$$

is the continuous version of the Boolean function f.

Finally, we could also consider an even simpler version, where all the variable aggregations discussed above are applied. As a result, each unit is described by a single variable x_i, whose dynamics is given by

$$\frac{dx_i}{dt} = \kappa_{x_i} g(x_{i-1}, x_i, x_{i+1}) - \gamma_{x_i} x_i. \tag{6}$$

Note that all model equations have some symmetry when parameters are identical between units; as a directed ring of n units, the circuit's group of symmetry is the cyclic group $\mathbb{Z}_n$, which is generated by the "shift" σ, where $\sigma(i) = i + 1 \mod n$. $\mathbb{Z}_n$ acts on the model's variables as $(\sigma x)_i = x_{\sigma^{-1}(i)}$.

In general, a system of differential equations $\dot{x} = F(x)$ is symmetric (or *equivariant*) if $\sigma F(x) = F(\sigma x)$ for all x (see, e.g., the standard text of Golubitsky and Stewart[23]). For the n-dimensional model (6), this clearly applies (when units are identical): $\sigma g(x) = g(\sigma x)$ since $\sigma^{-1}(i \pm 1) = \sigma^{-1}(i) \pm 1$. This extends to the higher dimensional models for the same reason, provided we let σ act on variables x, y, z, u separately

$$\sigma\left[(x_i, y_i, z_i, u_i)_{1 \leqslant i \leqslant n}\right] = [x_{\sigma^{-1}(i)}, y_{\sigma^{-1}(i)}, z_{\sigma^{-1}(i)}, u_{\sigma^{-1}(i)}]_{1 \leqslant i \leqslant n}.$$

All of the above applies for any rotation in $\mathbb{Z}_n$, which is always of the form $\rho = \sigma^k$ for some $1 \leqslant k \leqslant n$, i.e., $\rho(i) = i + k \mod n$. This symmetry entails the existence of invariant subspaces in $\mathbb{R}^N$, which amounts to a dimensionality reduction when studying the system. It also has implications in terms of the bifurcations that can occur.[23]

IV. MODEL ANALYSIS

Bearing in mind that (3) is a more realistic description, we focus on the system (4) in this section. Both analytical and numeric results can be obtained to describe the dynamical behavior of the system. For the latter, though, it will be useful to make additional hypotheses on the parameters, so that the overall parameter space is reduced. We discuss this normalization in Sec. IV A, before presenting some analysis of the phase space structure of this system.

A. Normalization

To simplify the analysis, we make the following assumptions:

- The maximum voltage of each gate is considered in normalized units, so that any non-zero steady state value is equal to 1. This is ensured by setting $\kappa_i = \gamma_i$ for each $i \in \{1, \ldots, N\}$, as discussed also in Sec. V A.
- The steepness β is supposed to be identical for each component and very high, well approximated by the limit $\beta \to \infty$.
- With all variables normalized to belong to the interval $[0, 1]$, we set a default threshold value, identical for all units: unless specified explicitly, we always have $\theta = 0.5$ in the following.
- Identical units are supposed to have strictly identical characteristics. In particular, we denote

$$\mu = \gamma_{x_i} = \kappa_{x_i}, \quad \nu = \gamma_{y_i} = \kappa_{Y_i} = \gamma_{z_i} = \kappa_{z_i}, \quad 1 \leqslant i \leqslant n.$$

Thanks to these assumptions, the parameter space becomes essentially two dimensional, with the pair μ, ν varying in a range of positive values. Finally, a change of time scale $\tau = \mu t$ or $\tau = \nu t$ allows to reduce even further, to a single control parameter (ν/μ or μ/ν, respectively).

For the $N = 4n$ model, a third delay parameter λ is required for u_i variables. Like in the $N = 3n$ case, a change of time units can in fact reduce the parameter space to a two-dimensional domain.

B. The core heteroclinic cycle (the fast inverter, or no inverter, limit)

1. Perturbed alternating sequences

Consider the n-dimensional model with identical units (so we can take $\kappa_i = \gamma_i = \kappa = \gamma$ and we will also take $\theta = 0.5$). This can be thought of as the $3n$-dimensional model, Eq. (4), in the limit of infinitely fast inverters, or simply with no inverters present, or the $4n$-dimensional model in which the OR gate is also infinitely fast. The closest we can get to a purely alternating state is one in which there is a single consecutive pair of units that are "on" (11) or a single consecutive pair that are "off" (00), and all others alternate. Other states, apart from the all 0 state, converge to the attractor consisting of such states, as shown later in Proposition 5. Consider what happens to a state with 0110 embedded in an otherwise alternating sequence, with n odd and sufficiently large ($n \geq 5$). Call the corresponding variables x_1, x_2, x_3, x_4 and the Boolean values b_1, b_2, b_3, b_4.

The two 0's (b_1 and b_4) have 1's on either side and so remain 0 (i.e., x_1 and x_4 are driven to a low value and are already below the threshold). The first 1 (b_2) remains 1 since $011 \to 1$ [i.e., $f(0, 1, 1) = 1$; so x_2 is driven to a high value and is already above the threshold]. The second 1 (b_3) is driven to a low value since $110 \to 0$ (x_3 decreases from a value above the threshold). Thus, the only significant event that can occur initially is for x_3 to decrease until it hits its threshold.

Now, $x_3 = \theta$, with $x_4 < \theta$ is a black wall, since $100 \to 1$. Thus, when x_3 reaches its threshold, sliding occurs, i.e., x_3 remains fixed at its threshold value, while other variables evolve. Furthermore, in the box 0100, x_4 is driven up since $001 \to 1$, while in 0110, x_4 is driven down as discussed above. The balance between the vector fields on either side of the black wall determines the sliding motion in the wall, by applying Filippov's method, a mathematical method to define solutions of differential equations with discontinuities in set-valued terms.[24,39] Equivalently in this setting, a singular perturbation analysis can be used, in which the step functions are perturbed as steep sigmoids (typically Hill functions);[20] see Sec. IV B 2.

With identical units, the Filippov method determines that the focal point of the sliding motion is at the threshold intersection $(x_3, x_4) = (\theta, \theta)$. With unequal unit parameters, the focal point may be below the threshold intersection, in which case it becomes a stable equilibrium point and the flow stops there, or above the threshold intersection, in which case the solution enters the threshold intersection with a positive velocity. At that point, a singular perturbation

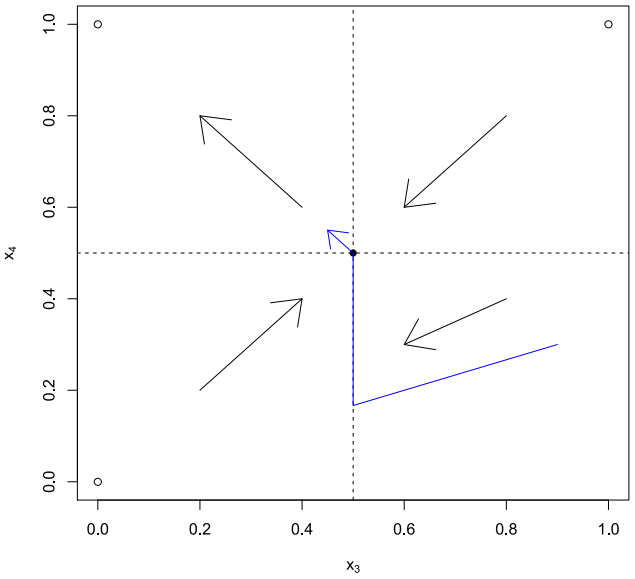


FIG. 2. Flow in x_3 and x_4 including sliding motion in the black wall, when units have identical parameters, and $\theta = 0.5$.

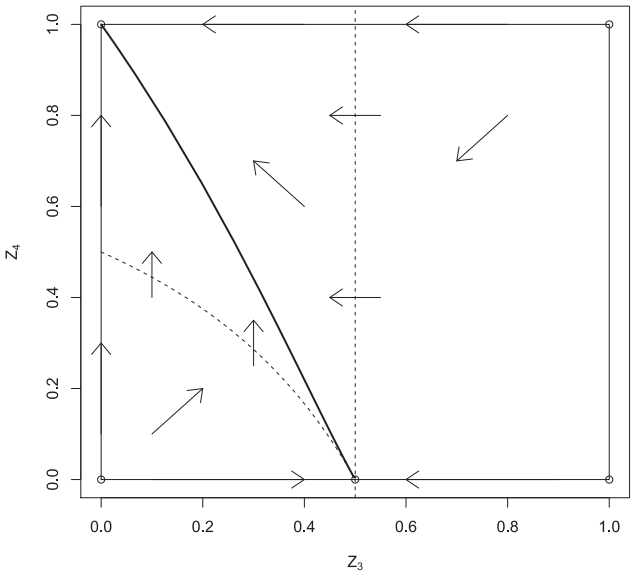


FIG. 3. Flow in Z_3 and Z_4 in the blowup of the threshold intersection. Dotted lines are the nullclines. Arrows show the approximate direction of the flow. The bold line is the solution from $(0.5, 0)$ to $(0, 1)$.

analysis shows that the flow continues into the box in which $x_3 < \theta$ and $x_4 > \theta$, i.e., $b_3 = 0, b_4 = 1$.

In the case of identical unit parameters, the same singular perturbation analysis (see below) shows that the flow from the threshold intersection is into the $b_3 = 0, b_4 = 1$ box, but in this case the sliding approach to the threshold intersection takes an infinite amount of time. The flow in the x_3, x_4 projection of the phase space is shown in Fig. 2.

2. Singular perturbation analysis of the threshold intersection

The singular perturbation analysis proceeds as follows.[20] First, approximate the step functions by sigmoids

$$Z_i = \frac{x_i^{1/q}}{\theta^{1/q} + x_i^{1/q}} \approx s^+(x_i).$$

Note that Z_i above and in the remainder of this section is distinct from the one used in table (12).

Now, blow up the threshold intersection by translating from x_3, x_4 to Z_3, Z_4 and rescaling time by $\tau = t/q$. The system becomes[20]

$$Z_3' = \frac{Z_3(1 - Z_3)}{0.5}\,[(1 - Z_3)(1 - Z_4) - 0.5],$$

$$Z_4' = \frac{Z_4(1 - Z_4)}{0.5}\,(1 - Z_3 - 0.5),$$

where the derivatives are with respect to τ. Then, consider the limit $q \to 0$. The phase plane for this system is shown in Fig. 3.

Note that $(0.5, 0)$ is an equilibrium point with a negative eigenvalue corresponding to the flow along the edge $Z_4 = 0$ and a zero eigenvalue corresponding to the flow into the interior of the square [the eigenvector is $(-1, 2)$]. It is easy to show that once in the interior of the square, all solutions flow to $(0, 1)$. Thus, in the original x variables, smooth systems with sufficiently steep sigmoids flow into the box $x_3 < \theta, x_4 > \theta$.

3. Global behavior of the n-dimensional system

Once in the box $b_3 = 0, b_4 = 1$, we have the state 0101 for b_1, b_2, b_3, b_4, but since $b_5 = 1$ and $b_6 = 0$ by our assumption of an essentially alternating initial state, the state of the first 6 variables has gone from 011010 initially to 010110 and it is clear that the pair of sequential 1's has propagated two units to the right, leaving an otherwise alternating state everywhere else. By symmetry, this process can now be repeated and the pattern 11 will propagate two units at a time twice around the ring (since n is odd), to arrive back at the initial state, following the cyclic attractor described in Sec. V B.

However, in the step-function limit, we know that the approach to the threshold intersection on the black wall is only asymptotic in time (this is an interpretation of the 0 eigenvalue in the Z system). Thus, we have a heteroclinic cycle with fixed points (actually singular stationary points) at each threshold intersection of consecutive pairs of variables.

If the parameters are not identical between units, then some of the focal points of the sliding motions will lie above the threshold, and some below, so some threshold intersections will be passed through, but trajectories will stop before reaching others.

However, if we introduce relatively fast additional variables (as in the $3n$ or $4n$ models here) we can develop an intuitive sense of how complex behavior can arise. Sliding in the black wall will be replaced by oscillations in the additional variables, so the heteroclinic cycle for the identical unit system will break down and solutions will

tend to be nudged past the threshold intersections, but not without some potentially complex oscillations as these transitions occur. Introducing small amplitude noise would have a similar effect. Even if units have non-uniform parameters, if the noise or oscillations are large enough, solutions may always be pushed far enough to pass the threshold intersections.

Thus, we expect that the higher dimensional systems or the systems with noise will have complex oscillations near these transition points that are nevertheless built around an underlying heteroclinic cycle. In fact, the perturbations can in this case go farther from the simple situation where only a single pair of variables are transitioning at a time, since during the oscillations around the threshold intersection, the time that a pair of units spends in the "final" state (01) can trigger the next pair of units to start transitioning, even while the first pair is still oscillating back and forth.

For example, Fig. 4(a) shows a projection onto the x_2, x_3-plane of a trajectory of the n-dimensional model with $n = 9$ and steep sigmoids (Hill functions) with exponent 50, while Fig. 4(b) shows the corresponding trajectory in the $4n$-dimensional model, where only the XOR gates are slow, and the additional variables are all fast. Similar to Fig. 2, these plots show the transition of this pair of units from box 10 (the lower right corner of the plot) to box 01 (the top left corner of the plot) by going to the wall between the 00 and 10 boxes, and then moving up to the vicinity of the threshold intersection before escaping into the 01 box. Even in the n-dimensional case, when the step functions are replaced by steep sigmoids, the heteroclinic point at the threshold intersection is avoided and the cycle becomes a periodic orbit. In the $4n$-dimensional case, trajectories oscillate around the black wall, rather than sliding in it, because of the delay caused by the fast variables y_2, z_2, u_2, until the region around the threshold intersection is reached, at which point, the trajectory escapes and goes into the 10 box toward the point $(1, 0)$. The rest of the trajectory occurs later, when x_2 becomes the second of the transitioning pair x_1, x_2, and then x_3 becomes the first of the transitioning pair x_3, x_4, after which the trajectory returns, in this projection, close to $(1, 0)$.

C. Cellular automaton behavior (the many inverter limit)

The core heteroclinic cycle can be thought of as the behavior of the $3n$-dimensional system (4) with identical units in the limit of infinitely fast inverters, or equivalently, with the inverters removed. In the opposite limit of infinitely many inverters, we converge to the cellular automaton behavior, at least when initial conditions are such that all variables that can switch from the initial state do so simultaneously. Each x_i then has time to converge (almost) to 0 or 1 before the inverters can react and initiate a new set of changes. If the initial state has all variables at 0 or 1 and units are identical then those that flip state do so at the same instant, and all inverters react at the same time, so the simultaneous switchings of the cellular automaton are also simultaneous in the continuous model.

The cellular automaton Rule 30 is known to produce irregular behavior on an infinite domain. However, here we have a fixed number, n, of units, and so the state space of the cellular automaton is finite and its behavior ultimately is periodic, even if the cycle is long, as discussed by Wolfram.[25] An example with $n = 9$ cells and 80 iterations from an initial sequence corresponding to the perturbed cycle of Sec. IV B 3 is shown in Fig. 5(a). For comparison, 200 iterations from a perturbed cycle on 81 units are shown in Fig. 5(b).

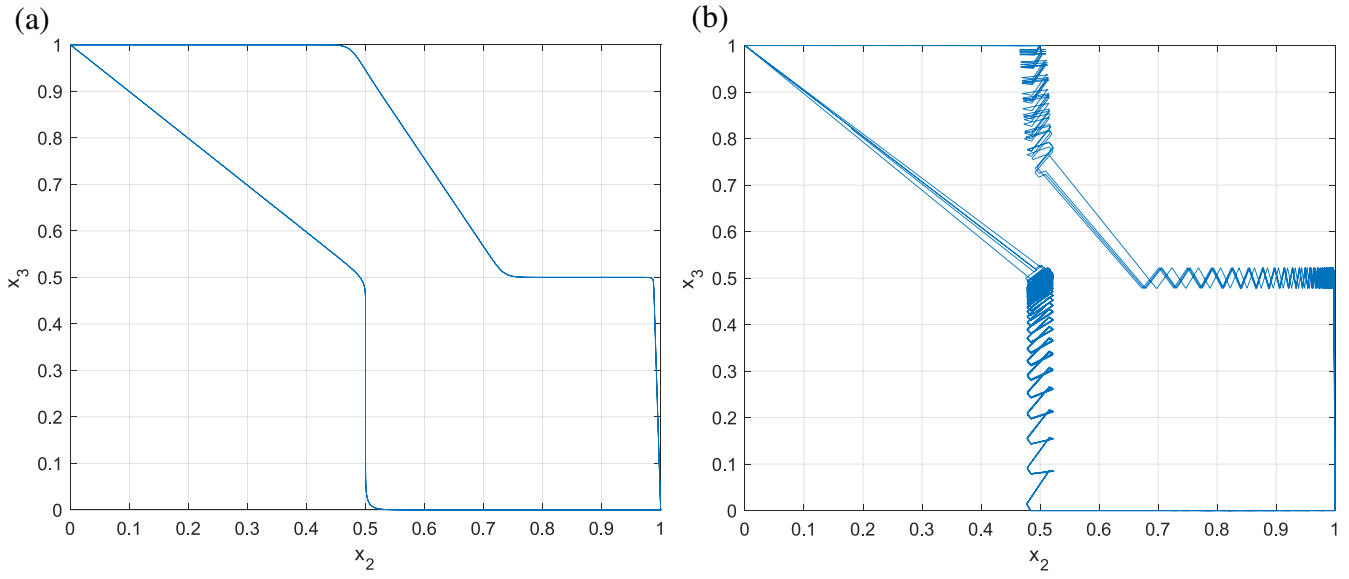
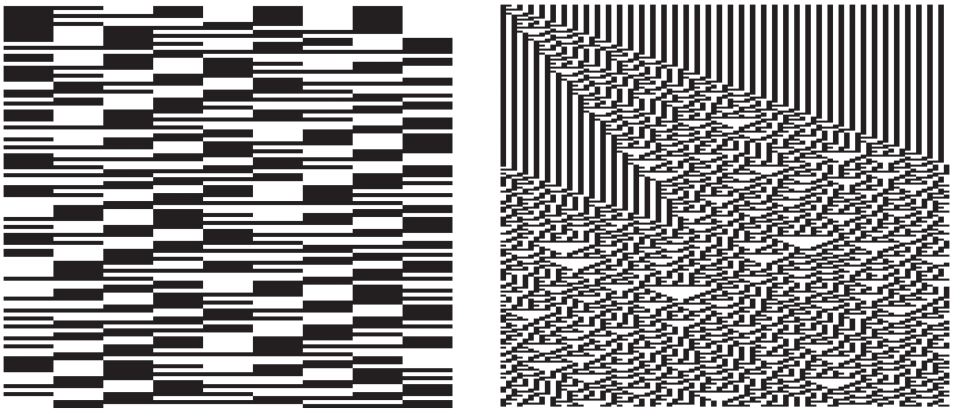


FIG. 4. Dynamics of a circuit with $n = 9$ units and sigmoids with slope parameter $\beta = 50$, projected onto the x_2, x_3-plane. (a) n-dimensional model, with parameter values $\kappa_{x_i} = \gamma_{x_i} = 1, \theta = 0.5$. Note that with the steep Hill function, the heteroclinic points are avoided and the trajectory becomes a periodic orbit. (b) $4n$-dimensional model, with parameters $\kappa_{x_i} = \gamma_{x_i} = 1, \kappa_{y_i} = \gamma_{y_i} = \kappa_{z_i} = \gamma_{z_i} = \kappa_{u_i} = \gamma_{u_i} = 50, \theta = 0.5$. Note that on different circuits, trajectories are slightly different. Thus, the additional fast variables introduce complexity.



(a) (b)

FIG. 5. (a) Behavior of the cellular automaton with Rule 30 on a finite domain of 9 cells. A continuous network similar to the 3*n* network (4) approaches this behavior in the limit of infinitely many inverters, when initial conditions are binary valued. Although the initial sequence is a perturbed alternation pattern, the alternation is quickly lost. Note that after 11 iterations, a pattern of six successive 1s and three successive 0s appears, which reappears 19 iterations later, but shifted 4 cells to the right. Thus, the period of the periodic orbit is $19 \times 9 = 171$ iterations. (b) 200 iterations from a perturbed alternation pattern on 81 cells.

Neither limiting behavior (no inverters or infinitely many inverters) produces chaotic dynamics. They do provide some intuition, however, about the nature of the dynamics when additional inverters are present, but only somewhat fast in relation to the main logic gate(s), where chaotic behavior may occur.

D. Numerical results

1. Simulations

The definition of trajectories "box by box" leads to a natural algorithm to solve ordinary differential equations (ODEs) of the form (3) or (4): the time to exit each box is calculated explicitly from (9) (see Sec. V) and, together with (9) itself, allows one to write an explicit map defined on the boundaries of boxes. The details can be found elsewhere,[26] but trajectories calculated using this algorithm will be shown in the following. In addition, standard ODE solvers will be used for models with smooth sigmoids.

Given the structure of the discrete transition graph described in Proposition 5 (see Sec. V B), odd values of n are more favorable to the occurrence of complex trajectories. This is confirmed by simulations using arbitrary parameters and initial conditions, which often tend to one of the regular steady states when n is even. Therefore, we restrict the following to cases where n is odd.

We first discuss numerical simulations of the $N = 3n$ model (4). As discussed earlier, up to a rescaling of time the model has a unique parameter, chosen here to be μ (i.e., $\nu = 1$ and the time unit is given by the inverters' intrinsic delay). We calculated some trajectories of the PL version of (4) for various arbitrarily chosen values of μ and random initial conditions, for n taking the odd values $3, 5, 7, 9$. From this exploration, it appears that very complex periodic orbits appear in the system, corresponding to periodic paths comprising many hundreds of nodes in the transition graph. Besides, for $n \geqslant 5$, some aperiodic trajectories are observed: for tens of thousands of successive boxes, no periodic pattern is found. Some graphical representations of such orbits are shown in Fig. 6.

As $n = 5$ seems to be the minimal number of units allowing for aperiodic dynamics, we performed a more systematic parameter exploration: fixing the inverter delay $\nu = 1$ we varied μ in the interval $[0, 1]$. For each tested value of μ, a trajectory through 50 000 boxes was started from a random initial condition and a periodic pattern was sought in the sequence of boxes. If no period was found, the period was recorded as a fixed, large number. The results are reported in Fig. 7.

As shown in Fig. 7, the period of limit cycles seems to be inversely proportional to the parameter μ. The same holds when considering the number of boxes crossed by a limit cycle, the "cycle length," rather than the actual period. Since fixing μ to 1 and varying ν instead would amount to varying the inverse of μ, we infer that the period of limit cycles (either expressed in time units or number of boxes) is bounded from below by a constant when varying ν. This claim is confirmed numerically, see Fig. 8. In other words, this seems to suggest that it is the time the main unit takes to react that determines the lower bound on the period, and it is almost completely insensitive to the time the inverters take to react.

Though the lower bound on cycle periods described in the legends of Figs. 7 and 8 is intriguing, the main feature shown in these plots is the presence of seemingly full intervals of parameter values for which the system behaves aperiodically. A bifurcation diagram, shown in Fig. 9 confirms this observation: some branches are strongly suggestive of the existence of a fixed point for the Poincaré return map (i.e., a limit cycle), whereas dense intervals of points indicate chaotic dynamics.

2. Lyapunov exponents

All the above results show that the system's dynamics is aperiodic for various intervals of parameter values. However, to fully confirm the occurrence of chaos, we estimated the Lyapunov exponents (LEs) of the system numerically. Indeed, the existence of a positive LE is a well-known characteristic of chaotic dynamics. Furthermore, as far as the random number generation is concerned, one must verify that the system has the ability to generate a positive entropy. The existence of a positive LE is sufficient to confirm the positive entropy, as the Kolmogorov-Sinai entropy of a dynamical system is equal to the sum of positive LEs according to Pesin's theorem.[27] To estimate these exponents, we implemented a discrete QR algorithm.[27,28] The principle of this algorithm is to compute in parallel a numerical solution of both the original model, written

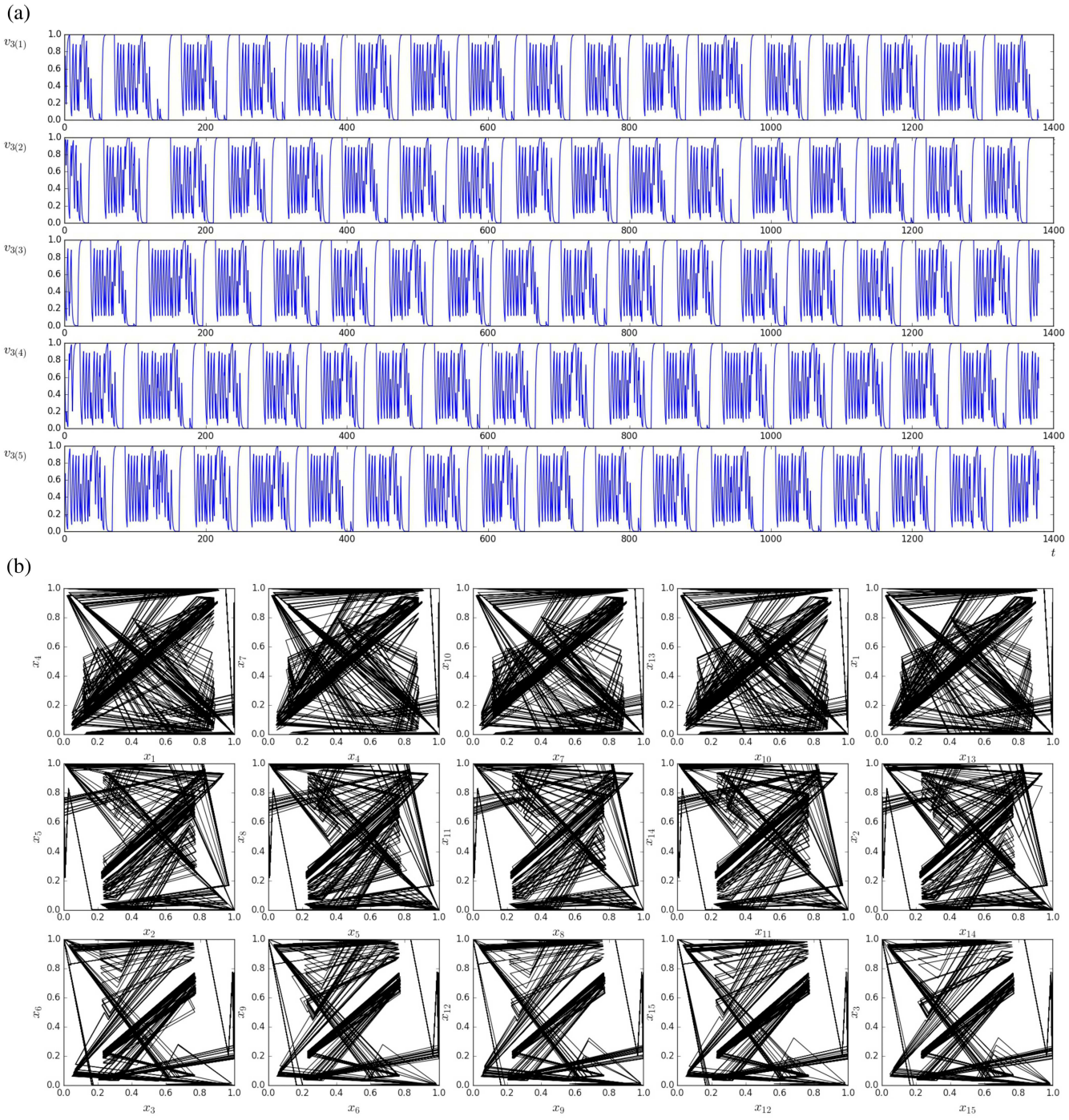


FIG. 6. Numerical simulation of a trajectory for the model (4) with $n = 5$ units, $\mu = 1$ and $\nu = 0.6$ and a random initial condition. No periodic pattern is found out of 200 000 successive boxes. (a) Time courses; only the variables x_i are shown for clarity. (b) Projections of the trajectory on different planes (x_j, x_{j+3}) as indicated. Though not perfectly identical, the plots along each row present some strong similarities, reflecting the symmetry of the system.

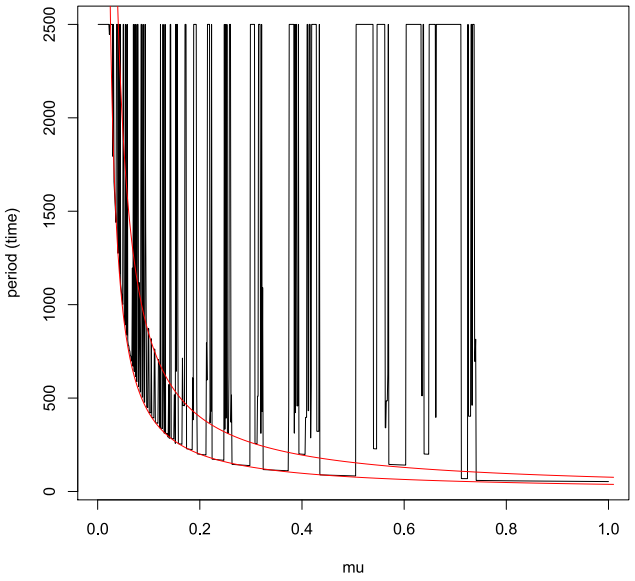


FIG. 7. Period of trajectories calculated for varying values of μ and fixed $\nu = 1$. A period of 2500 indicates that no period was actually found. In red, the curves' period $= 38/(\mu - 0.01)$ and period $= 76/(\mu - 0.01)$ are shown.

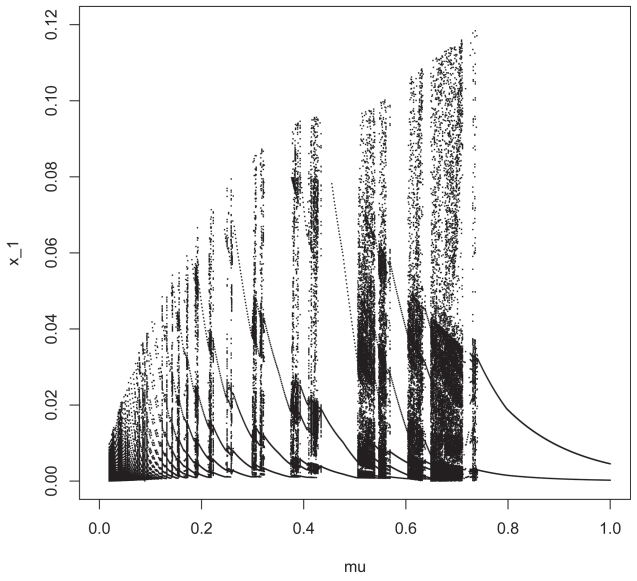


FIG. 9. In the same run as Fig. 7, a sequence of 5000 successive values (after the transient) of the first variable x_1 were recorded, at each time that the trajectory satisfied $x_2 = \theta$ (the threshold is translated to 0 in the figure), and the other variables in a particular pattern of above and below the threshold (so this is a Poincaré section) corresponding to the box $b = (101, \theta 01, 101, 010, 101)$. The first unit is "on," the second unit is transitioning from or to the "on" state with the main unit at the threshold and the other two where they should be if the main unit was "on," the third unit "on," the fourth "off," and the fifth "on."

compactly as

$$\dot{\nu} = f(\nu)$$

and its associated variational equation

$$\dot{Y} = Df[\nu(t)]Y, \quad Y(0) = \mathrm{Id},$$

where the unknown Y is an $N \times N$ matrix and the Jacobian Df is evaluated along the solution to the ODE $\dot{\nu} = f(\nu)$. The eigenvalues of the solution to the variational equation can in theory be used to calculate Lyapunov exponents, but in practice the existence of a positive exponent entails that all columns of Y become (numerically) linearly dependent. To overcome this issue, a QR decomposition of the approximate solution Y is performed at regular time intervals, amounting to an orthonormalization of the column space of Y. The details of the algorithm can be found in the references given above.

Because the existing algorithms are defined only for smooth ODEs, we performed our estimation on a version of the model that uses tanh sigmoids [with a high steepness coefficient $\beta \geqslant 58$, see

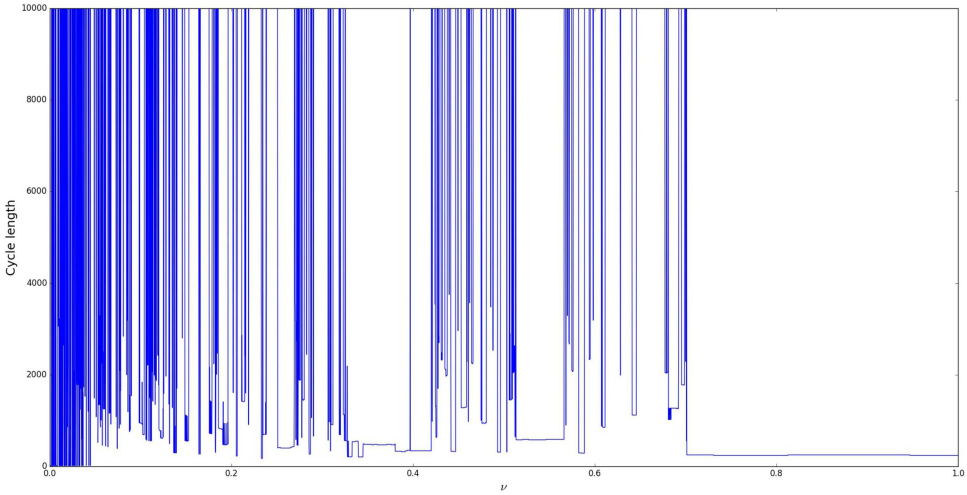


FIG. 8. Length (number of boxes) of periodic trajectories calculated for varying values of ν and fixed $\mu = 1$. A period of 10 000 indicates that no period was actually found. The values found for low values of ν are not reliable as very long cycles exist in this region, involving repeated patterns of shorter length which can be mistakenly taken for periodic patterns in our implementation.

Eq. (2)] rather than step functions. The implementation was made in Python, using the solver odeint for both the original ODE model and its associated variational equation. The code was tested on the Lorenz system and returned values agreeing with published estimates.

A first exploration, using values of parameters where the previously presented bifurcation diagrams displayed aperiodic dynamics, did not lead to a clearly positive LE: though nearly an order of magnitude higher than the second LE (in absolute value), the leading LE was close to zero, making conclusions uncertain. Additional calculations for various values of the delay constants did not allow us to find a clearly positive LE. However, the computational time (15 to 70 min to calculate a set of LE estimates) only allowed for a very limited exploration.

This led to considering the more realistic model (3) with $4n$ variables. In that case, a positive LE was found, as shown in Fig. 10. To confirm at least visually that the dynamics is chaotic, trajectories calculated for the same parameter values as the Lyapunov exponents are shown in Fig. 11. The main features observed in the $N = 3n$ case are still present (complex aperiodic orbits, presenting some approximate symmetries).

Since the LEs were estimated using a smooth version of the model, we also calculated trajectories for this version of the model. In Fig. 12, it appears as expected that trajectories of the smooth and step-function versions initially agree, but diverge after a short time due to the system's sensitivity to perturbations. The overall time courses have similar features.

3. Effect of noise

An unrealistic feature of our simulations so far is their complete determinism, as solutions of a system of differential equations. It is possible to compute LEs for stochastic models in a similar way to differential equations.[27] We took advantage of this feature and implemented different forms of noise in the model, aiming at approximate

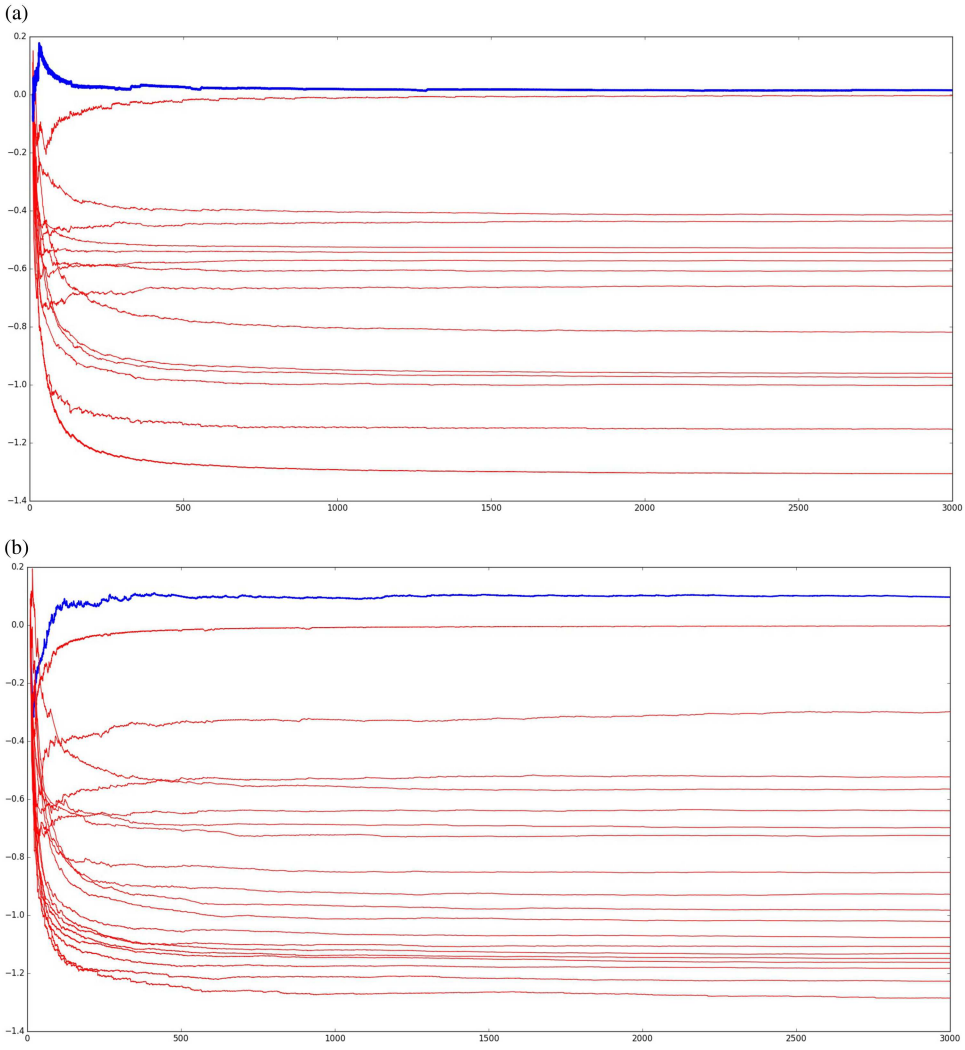


FIG. 10. Lyapunov exponent estimates: the leading exponent is shown in bold and blue, all remaining exponents are in red. Abscissa is time. (a) The $3n$ model, with $n = 5$ and $(\mu, \nu) = (1, 0.5)$. Though positive, the leading exponent is very small and numerical inaccuracies do not allow one to conclude with high confidence that the leading exponent is positive (final values ≈ 0.015 and -0.004). (b) The $4n$ model, with $n = 5$ and $(\mu, \nu, \lambda) = (0.6, 1, 0.7)$. The leading exponent is significantly higher than the second exponent, which is very close to zero as expected (final values ≈ 0.097 and -0.004).

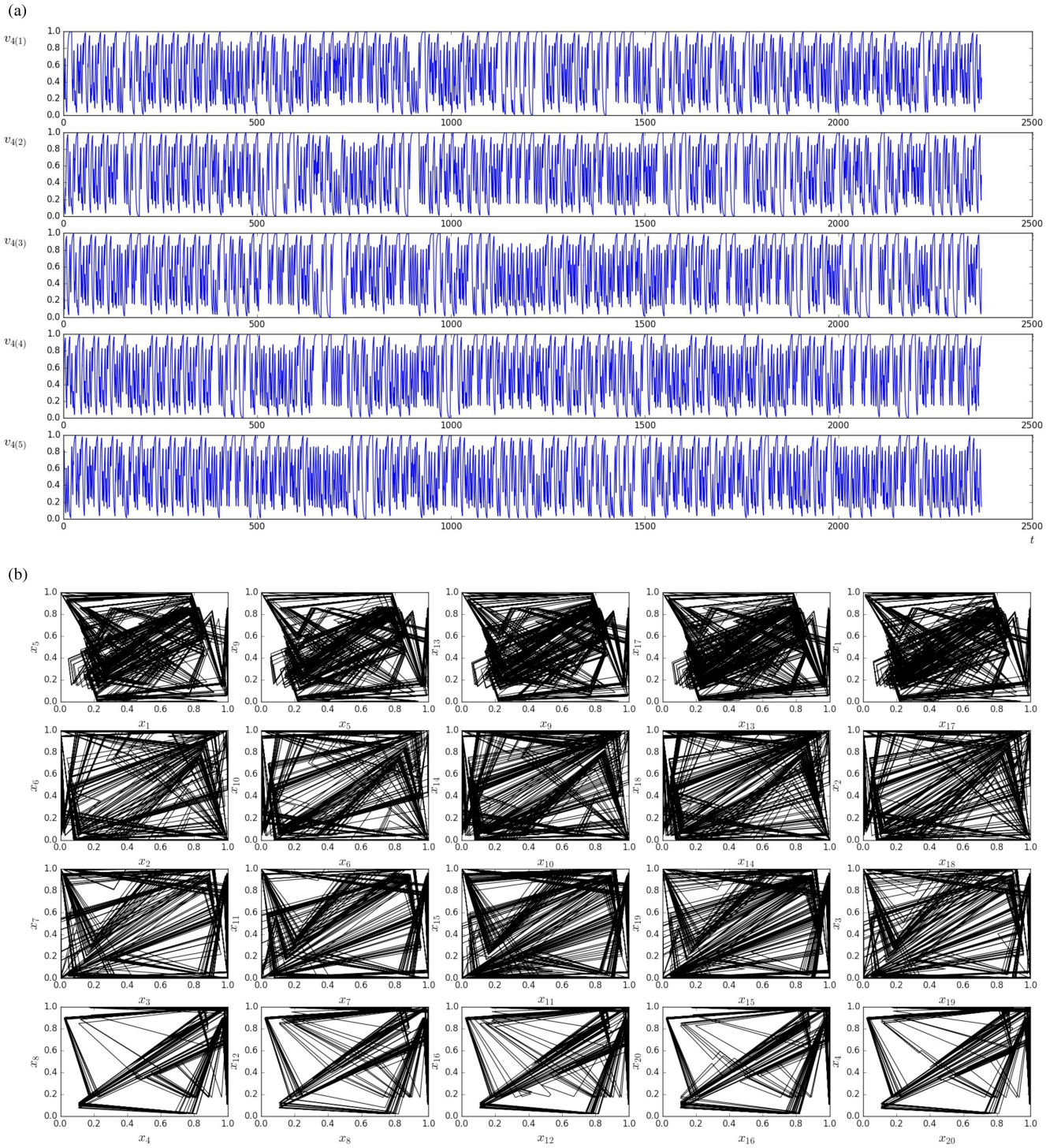


FIG. 11. Numerical simulation of a trajectory for the $N = 4n$ model with $n = 5$ units, $\mu = 0.6$, $\nu = 1$ and $\lambda = 0.7$ and a random initial condition. No periodic pattern is found out of 200 000 successive boxes. (a) Time courses, only the variables x_i are shown for clarity. (b) Projections of the trajectory on different planes (x_j, x_{j+4}) as indicated.

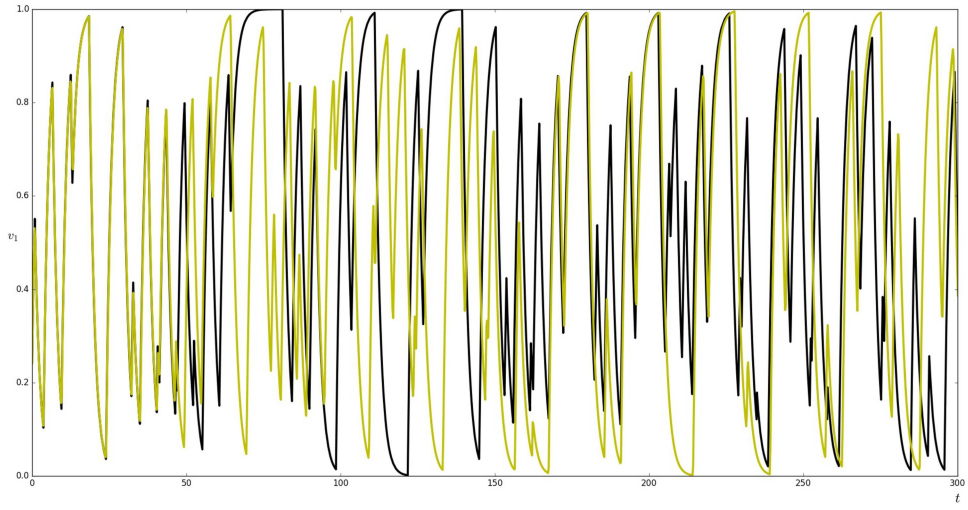


FIG. 12. Initial time course for the first variable of the model used for Fig. 11 (dark), along with a smooth version using the tanh form in (2) with a steepness coefficient $\beta = 58$ (light).

descriptions of the natural jitter occurring in any real-life circuit. More specifically, we implemented three different models, described below.

As detailed by Hajimiri *et al.*,[29] the standard deviation of the timing uncertainty due to jitter is expected to be proportional to the square root of the gates' typical delay. Denoting this relation by $k\sqrt{\tau}$, the constant k for a modern transistor at room temperature would be typically $k \approx 15 \times 10^{-9}$, and since the delays used in our models were all close to one, we use this value of k as the standard deviation in our simulations. More specifically:

- *noise 1:* the model includes a multiplicative noise term (normally distributed with mean 1 and standard deviation k) in the delay parameters γ_i. The model is therefore a stochastic differential equation and is solved using the Euler-Maruyama algorithm.
- *noise 2:* the deterministic model is solved as in the noise-free situation, but a perturbation of the voltage is introduced at regular time intervals [in our simulations, every $\Delta t = 0.1$ unit of time the voltage $v(t + \Delta t)$ is perturbed by adding a normally distributed term with mean 0 and standard deviation $k\sqrt{\Delta t}v(t)$].
- *noise 3:* is as noise 2, but with the perturbations introduced at random times (the implementation is as in *noise 2* but with Δt being modified by an additive term taken as the maximum of 0 and a normally distributed variable of mean 0 and standard deviation k).

Overall, none of the noise models seem to induce any major shift of the Lyapunov spectrum (Fig. 13). The lowest positive exponents are found for the first noise model, but this is most likely explained by the sensitivity of the integration algorithm to the size of time steps. Larger time steps led to lower LEs, to the point of getting close to zero. On the other hand, reducing the time step further comes at a high computational cost.

The three models are clearly simplified approximations. Furthermore, by their very nature stochastic models would require a more statistical investigation, for wide ranges of initial conditions and parameters (such as noise distribution). However, such a survey would carry us out of the scope of this paper and come at very high computational cost. The main point made at this stage is that for reasonable ranges and qualitative forms of noise, the measure of entropy provided by the LE remains within the chaotic range.

4. Entropy and time series analysis

In Secs. IV D 2 and IV D 3, the complexity estimates are based on the model, and, in particular, even though analytical results can only be obtained for the PL model, LE's have to be calculated for a smooth version of the model, perhaps with the addition of noise. To confirm the robustness of the claim of chaos, we also used an empirical measure of complexity, which is solely based on time series. One advantage of such approaches is that they can be used with the PL model, for which the generation of time series is computationally less expensive. Another is that ultimately, in the implementation of the TRNG, a sequence of bits will be extracted that should have a positive entropy. We chose the notion of sample entropy.[30] $\mathrm{SampEn}(m, r, N)$ is defined as the negative natural logarithm of the conditional probability that two sequences of length N similar (i.e., within a distance r of each other) for m points remain similar at the next point, ignoring self-matches.[30]

We generated various trajectories of various lengths (up to 5×10^7 time steps) of the $4n$-dimensional model for 9 units and extracted the Boolean trace, i.e., the position of variables above or below the threshold over time. With 9 units, the parameters used for 5 units and reported in Fig. 10 led to periodic trajectories. Instead, we observed that using slightly different decay rates for the same gate in different units (e.g., adding a small noise term) seemed to be required for aperiodic behavior to occur. In the remainder of this section, the following is used (but other choices with close values led to similar results):

$$\begin{aligned}(\gamma_{x_1}, \ldots, \gamma_{u_9}) = (&0.6, 1, 1, 0.7,\ 0.6, 1, 1, 0.7,\ 0.5, 1, 1, 0.7,\\ &0.6, 1, 1, 0.6,\ 0.6, 1, 1, 0.7, 0.6, 1, 1, 0.7,\\ &0.7, 1, 1, 0.8,\ 0.6, 1, 1, 0.6,\ 0.6, 1, 1, 0.7).\end{aligned} \tag{7}$$

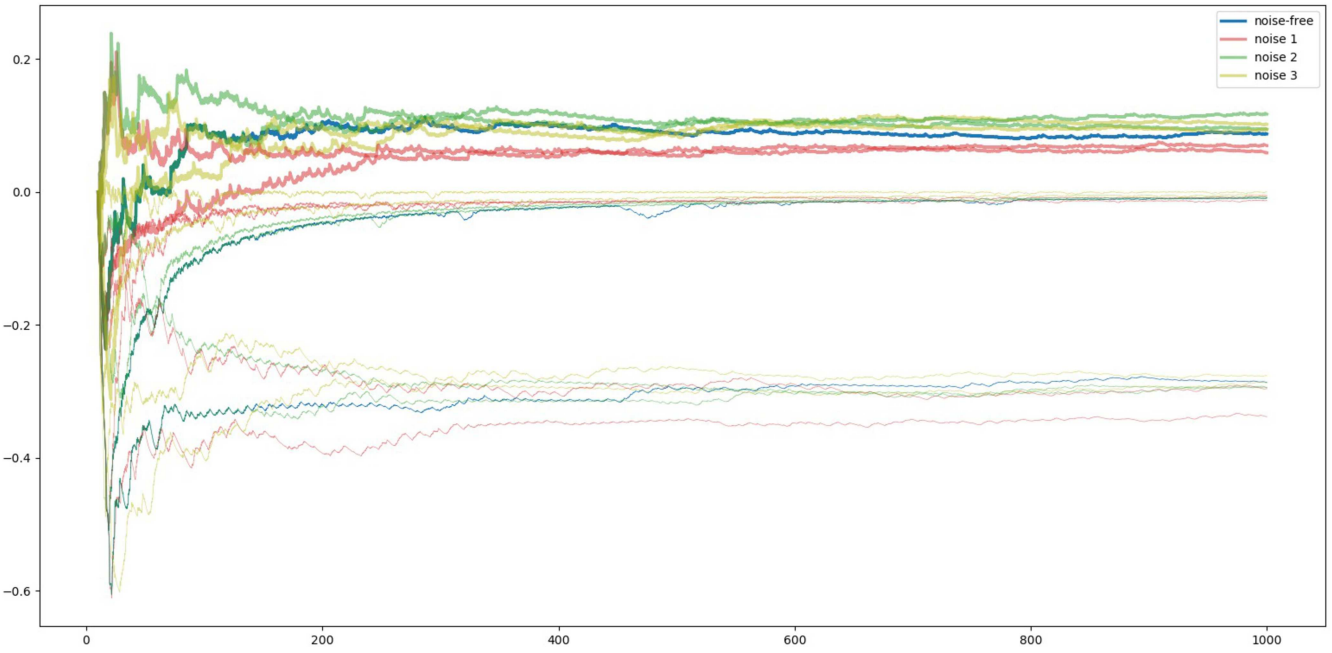


FIG. 13. Lyapunov exponent estimates with noise terms, see the text for a description of the three noise models. Abscissa is time. The $4n$-dimensional model is used, with $n = 5$ units, $\mu = 0.6$, $\nu = 1$ and $\lambda = 0.7$. For each model, two different initial conditions are chosen at random. Only the three leading LEs are plotted for clarity, with thicker lines for the leading exponent.

From this discretized time series, we extracted the state of the second inverter gate for all but the last unit, therefore creating a series of 8-bit Boolean vectors. The latter can be represented as integers taking values between 0 and $2^8 - 1 = 255$. We calculated SampEn for various lengths of these integer sequences, consistently finding an entropy ≈ 0.2. For example, Fig. 14 reports values as a function of the length of a sample extracted from a long simulation (1×10^6 time steps). In addition to considering different lengths of subsequences, we considered increasing the embedding dimension [the tolerance r was set to a standard 0.2 std(data)], without much effect for $m \leqslant 7$ (most applications use $m = 2, 3$). We conclude that SampEn robustly indicates a significant level of unpredictability, with a positive SampEn ≈ 0.2.

Note that the notion of time step in this context is not a constant: as mentioned in Sec. IV D, the integration of piecewise-linear equations proceeds "box by box" and each time step corresponds to the occurrence of a threshold crossing event (i.e., the switch of one variable). This can take a variable amount of "physical time" depending on how close the non-switching variables are to their threshold values.

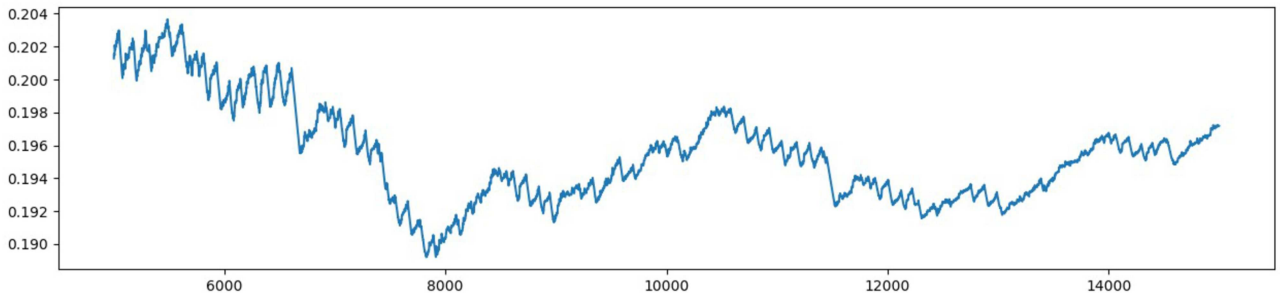


FIG. 14. Sample entropy on a sequence of 8-bit integers (second inverter output of a 9 unit $4n$-dimensional model). The sequences correspond to the k last time steps of a long time series, as described in the main text. The abscissa denotes the length k of the sub-sequence being analyzed. Parameters are as in (7).

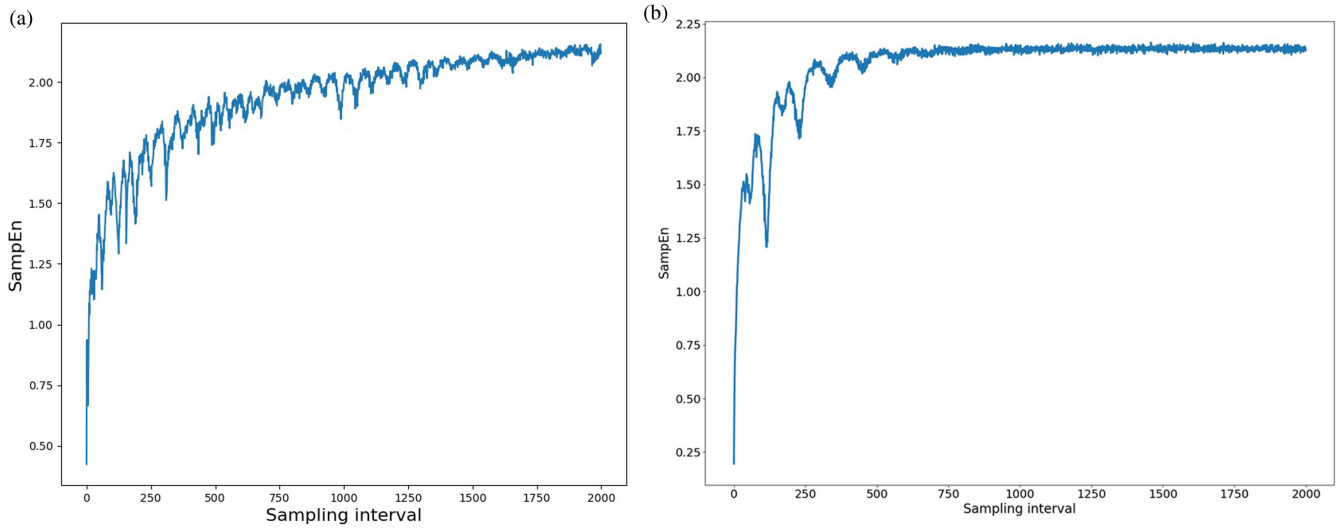


FIG. 15. A sequence X of 5×10^7 digits was generated. Then, for each sampling value k, the last 10 000 values (taken every k time steps) of X are used to calculate SampEn. Using this method, SampEn is reported above as a function of the sampling rate k (in number of time steps; see the main text) for (a) a sequence of 5-bit integers generated using the second inverter of each unit in a $3n$-dimensional model ($\mu = 1$ $\nu = 0.5$), (b) a sequence of 8-bit integers generated using the second inverter outputs of 8 out of 9 units in a $4n$-dimensional model [parameters as in (7)].

Furthermore in practice, the sequence of Boolean values generated by the circuit is sampled at time intervals that are significantly longer than the typical switching time between variables. Typically, the sampling occurs at 1/100th of the inverter gate's update rate. In the model, the latter is the time unit, therefore a similar sampling would correspond to 50 (physical) time units. Based on a long simulation, there are typically $\approx$ 1900 switches (with standard deviation $\approx$ 13) switches (i.e., time steps in the numerical integration) occurring over 50 actual time units.

Following this discussion, to assess the effect of sampling we also calculated SampEn of sequences extracted every k time steps, for k varying between 0 and 2000 (chosen larger than the value 1900 mentioned above). The result is shown in Fig. 15. Interestingly, it appears that the values $\approx$ 0.2 found above give a lower bound when considering the effect of sampling. Indeed, one sees in Fig. 15 an increase of SampEn as a function of the sampling interval. For values of $k \geqslant$ 700, the entropy reaches a plateau approximately equal to 2.1. This also indicates that the sampling rate of 1/100th is somewhat optimal: it is in the plateau, and any faster rate might lead to lower entropy rates (though of course, this would depend on the actual parameters of the different gates). The figure also illustrates that this property is not restricted to the $4n$-dimensional model but also applies for $3n$.

Given the local analysis reported in Sec. IV B, it seems reasonable to speculate that the cause of the increase in SampEn with the sampling interval is that there are sequences of repeated patterns occurring on smaller time scales (corresponding to the 2-cycles within the attractor of the discrete model TG^n introduced in Sec. V, see Figs. 16–18).

E. NIST suite assessment of a physical circuit implementation

Strictly speaking, the numerical results presented so far are only valid for the proposed models, rather than an actual physical device. However, for practical use, an actual chip implementing the circuit

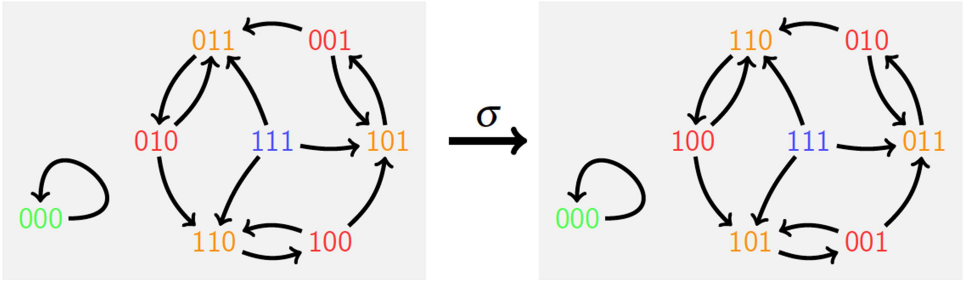


FIG. 16. The graph TG^3 and its image under the action of the shift on vertices. Colors represent the orbits of $\mathbb{Z}_3$'s action. Clearly, the two graphs are identical. The attractors are $\{000\}$ and $\{0, 1\}^n \setminus \{000, 111\}$.

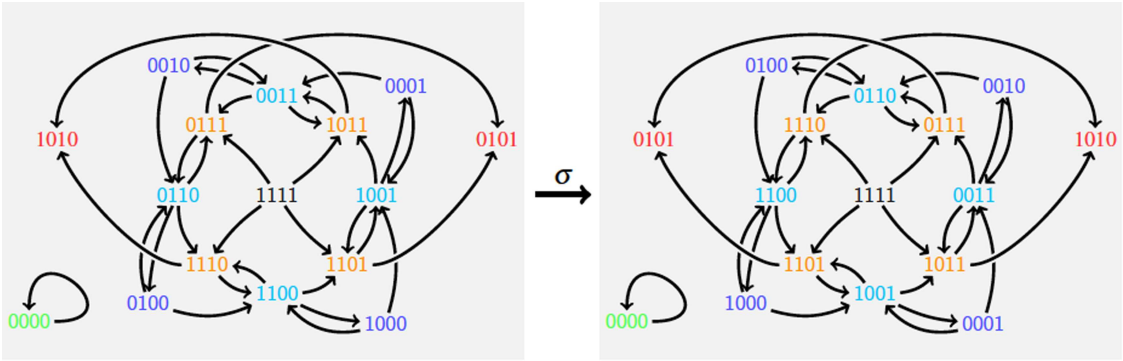


FIG. 17. The graph TG^4 and its image under the action of the shift on vertices. Colors represent the orbits of $\mathbb{Z}_4$'s action. Clearly, the two graphs are identical. The only attractors are the fixed points 0000, 1010, and 0101.

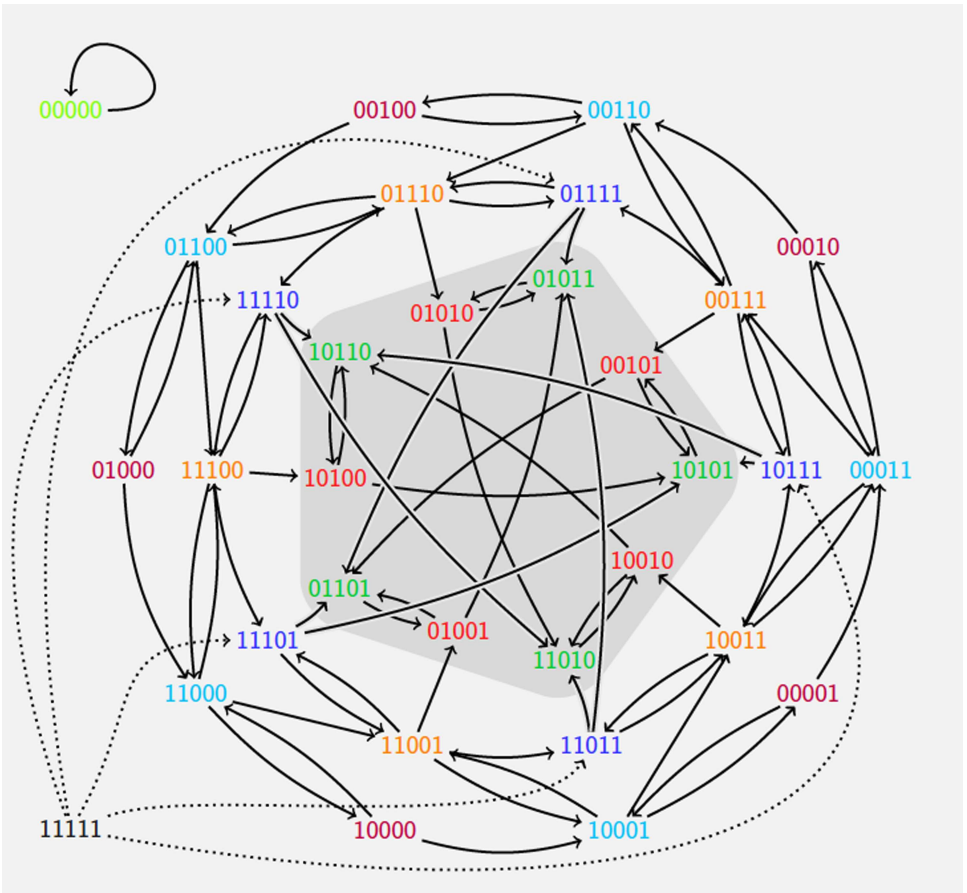


FIG. 18. The graph TG^5. Colors represent the orbits of $\mathbb{Z}_5$'s action. The only attractors are the fixed point 00000 and the shaded nodes at the center, corresponding to the $\mathbb{Z}_5$ orbits of 10101 and 00101. Dotted lines from the "source" node 11111 are used to improve visibility only.

design from Fig. 1 should be analyzed. Though a complete characterization of the physical circuit is to be reported elsewhere, we include some statistical assessment of the bit-streams generated from test chips fabricated in a testchip utilizing TSMC 40 nm technology.

Specifically, these bit-streams were assessed using two of the most widely used test suites for TRNGs or pseudo-random number generators. Both suites have been released by the National Institute of Standards and Technology (NIST) in special publication SP800-22[31] and the more recent draft publication SP800-90B,[32] respectively.

100 test sequences comprising 1M bytes were collected from the test chips. These test sequences were applied to all the 15 tests; the overall pass rate and smallest P-value across all 100 test sequences are provided in Table I. It was found that all the tests of NIST SP800-22 passed with a high pass rate.

Similarly, Table II reports results for some of the SP800-90B tests, specifically, tests assessing if the bit-streams are plausibly independent and identically distributed (iid) random numbers. As seen in the table, the test sequences passed all tests with a minimum entropy of 7.07026, which is considered random and iid.[32]

V. PHASE PORTRAIT DESCRIPTION: THE DISCRETE LEVEL

The switching nature of the equations introduced so far leads to a natural discretisation of the models, whereby only the ON/OFF status of each variable is recorded. Although this point of view does not lead to a proof of chaos it provides a framework, valid for any choice of parameter values, in which to interpret the continuous dynamics discussed in Secs. III and IV. It also allows for mathematical proofs in support of the main statements, as opposed to the more experimental nature inherent in any numerical investigation.

A. Transition graph

This section reviews some general properties of PL systems of ODEs of the form (3)–(6). More detailed discussions can be found in earlier publications.[26,33]

Each right-hand side equation is composed of a negative linear term (a "decay") and a piecewise constant term, which is fixed in rectangular regions of the state space $\mathbb{R}^N$. Since the piecewise constant terms can always take exactly two values, 0 and κ_i, all the models (of dimension $N = n, \dots, 4n$) considered in this paper can be written in the generic form

$$\frac{dv_i}{dt} = \kappa_i \phi_i[B(v)] - \gamma_i v_i, \quad 1 \leqslant i \leqslant N,$$

where v is the N-dimensional vector describing the whole system, $\phi_i \in \{0,1\}$, or after the simple change of variable $v_i \leftarrow \frac{\gamma_i}{\kappa_i} v_i$, reducing the number of parameters by half

$$\frac{dv_i}{dt} = \gamma_i \left\{\phi_i[B(v)] - v_i\right\}, \quad 1 \leqslant i \leqslant N. \tag{8}$$

Note that this rescaling also implies that each threshold θ_i has been rescaled to $\frac{\kappa_i \theta_i}{\gamma_i}$, though we keep the notation θ_i in the sequel for simplicity, and that now each $\theta_i \in (0,1)$ to ensure that each variable can switch. Also note that, in this rescaling, $[0,1]^N$ is an invariant region, since $\phi_i \in \{0,1\}$ in Eq. (8).

The position of state variables relative to their threshold can naturally be coded using a Boolean vector $B = B(v) \in \{0,1\}^N$, where B is a map defined by

$$B_i(v) = s^+(v_i).$$

The domain of B is the set of points where no variable is equal to its threshold value and will be called the *regular set* hereafter and denoted $R = \prod_{i=1}^N ([0,1] \setminus \{\theta_i\})$. Its complement will be referred to as the *singular set* $S = [0,1]^N \setminus R$.

For any Boolean vector $b \in \{0,1\}^N$, $B^{-1}(b)$ is a rectangular region in $\mathbb{R}^N$, i.e., a product of intervals of the form $[0,\theta_i)$ or $(\theta_i,1]$. We will call *boxes* the regions of the form $B^{-1}(b)$, often referring to "the box b" by abuse of notation, or denoting $v \in b$ for $v \in B^{-1}(b)$, i.e., $B(v) = b$.

Let us also denote $\overline{b_i} = 1 - b_i$ and $\overline{b} = (\overline{b_i})_{1 \leqslant i \leqslant N}$, and $\overline{b}^i = (b_1, \dots, b_{i-1}, \overline{b_i}, b_{i+1}, \dots, b_N)$.

The map $\phi : \{0,1\}^N \to \{0,1\}^N$ is a purely Boolean map, hereafter referred to as the underlying *focal point* map of the system. This terminology stems from the explicit solution to (8), valid in a given box b

$$\forall i \in \{1, \dots, N\}, \quad v_i(t) = [v_i(0) - \phi_i(b)]\, e^{-\gamma_i t} + \phi_i(b), \tag{9}$$

so that $\phi(b)$ is attracting all trajectories originating from the box b. Depending on the position of $\phi(b)$ in the state space $[0,1]^N$, two main cases can be distinguished, listed below. Note that because $\phi(b)$ is Boolean, it is exactly equal to the label of the box in which it lies, i.e., $\phi(b) = B[\phi(b)]$.

1. $\phi(b) = b$. In this case, $\phi(b)$ is an asymptotically stable steady state for the system and no trajectory can leave the box b. Indeed, it is clear from (9) that $v_i(t) \to \phi_i(b)$ for all i, in a monotonic way so that no threshold is crossed (the definitions imply that $v_i(0)$ and ϕ_i are all on the same side of any threshold).
2. $\phi(b) \neq b$. In this case, all trajectories exit b in finite time, entering a neighboring box b' in which they will tend to the new focal point $\phi(b')$, as detailed further below.

In summary, the function ϕ captures the dynamics of (3)–(6) at the level of boxes: for any box b, $\phi(b)$ provides the direction in which all trajectories tend. This informal description can be made more precise by introducing the notion of a *transition graph*, denoted TG: it is a directed graph with node set $\{0,1\}^N$ and edges $b \to b'$ between any pairs of boxes such that an open set of trajectories can leave box b to enter b'. The openness condition implies that b and b' are adjacent through an $N-1$-dimensional face (hereafter referred to as a "wall"), of the form ($c\ell$ denotes the closure)

$$c\ell(b) \cap cl(b') \subset [0,1]^{i-1} \times \{\theta_i\} \times [0,1]^{N-i}$$

i.e., any v in this intersection satisfies $v_i = \theta_i$ and $B_j(v) = b_j = b'_j$ for all $j \neq i$. Following the above discussion, this happens exactly when the boxes containing $\phi(b)$ and b differ in direction i, which can be

written as

$$\phi_i(b) = \overline{b_i}.$$

Defining the exit directions of the box b as

$$I(b) = \{i \,|\, \phi_i(b) \neq b_i\} = \{i \,|\, \phi_i(b) = \overline{b_i}\},$$

edges in the transition graph are thus all pairs of the form

$$(b, \overline{b}^i) \quad \text{for } i \in I(b).$$

The main point of defining TG is that it provides an intuitive and convenient "coarse grained" description of the dynamics of the system: by construction, any sequence of boxes that are intersected by a solution of (8) is exactly a path in TG. In particular, any attractor of the original dynamics lies within a strongly connected component (scc) of TG. The term "attractor" is also used for TG, referring to the terminal[34] scc's. In this discrete setting, an attractor that is not a fixed point will be termed a *cyclic attractor*.[35,36]

Remark 1. *In general, a non-terminal scc in the* TG *may contain an attractor of the PL differential equations for some parameter values. For a terminal scc, corresponding to a compact invariant region for the dynamics, there is necessarily always an attractor for any choice of parameters, see, e.g., the earlier publications*[26,33] *for related discussions. It is important to keep in mind that in general some paths in the* TG *may not be the code of any trajectory (even within a scc).*

B. Transition graphs for the *n*-dimensional model

To begin with, the transition graph for the simplest, n-dimensional, model (6) is constructed and analyzed. We denote this graph by TG^n. Higher dimensional models will then be compared to this simpler version. From (6), we readily deduce the following expression for the focal point map ϕ:

$$\phi_i(b) = f(b_{i-1}, b_i, b_{i+1}) = b_{i-1} \oplus (b_i \vee b_{i+1}), \quad 1 \leqslant i \leqslant n,$$

where as before subscripts are understood modulo n.

To describe TG^n, we can take advantage of the circuit's symmetry under the action of the cyclic group $\mathbb{Z}_n$, discussed earlier. For a directed graph $G = (V, E)$, symmetry occurs if G is left invariant by the action of a group of graph isomorphisms, i.e., bijections $h : V \to V$ such that $(i, j) \in E \iff (h(i), h(j)) \in E$. In the case of TG^n, $V = \{0, 1\}^n$ and $\sigma \in \mathbb{Z}_n$ (or its iterates) acts on V as discussed earlier: $\sigma\, b = \sigma\,(b_1, \ldots, b_n) = [b_{\sigma^{-1}(1)}, \ldots, b_{\sigma^{-1}(n)}]$.

Now, edges in TG^n are of the form $(b, \overline{b}^i)$ for i such that $\phi_i(b) \neq b_i$. The discussion after Eq. (6) entails that

$$\begin{aligned}\phi_i(\sigma^k b) &= f[b_{\sigma^{-k}(i-1)}, b_{\sigma^{-k}(i)}, b_{\sigma^{-k}(i+1)}] \\ &= f[b_{\sigma^{-k}(i)-1}, b_{\sigma^{-k}(i)}, b_{\sigma^{-k}(i)+1}] \\ &= \phi_{\sigma^{-k}(i)}(b) = \left(\sigma^k \phi\right)_i (b),\end{aligned}$$

in other words ϕ is $\mathbb{Z}_n$-equivariant

$$\sigma^k \phi(b) = \phi(\sigma^k b) \quad \text{for any } k \text{ and } b \in \{0, 1\}^n. \tag{10}$$

In words, the coordinates b_i and $\phi_i(b)$ are shifted identically by σ^k and therefore $b_i \neq \phi_i(b) \iff b_{\sigma^k(i)} \neq \phi_{\sigma^k(i)}(b)$. This means that σ^k's action is a digraph homomorphism, and edges are identical in TG^n and its image under σ^k, i.e., the graph is symmetric under the action of $\mathbb{Z}_n$. This induces a natural decomposition of TG^n into the *orbits* of $\mathbb{Z}_n$'s action, i.e., sets of nodes that are equivalent up to a circular permutation of subscripts. We denote by $\mathbb{Z}_n b \subset \{0, 1\}^n$ the $\mathbb{Z}_n$-orbit of $b \in \{0, 1\}^n$.

We shall consider examples for small values of n to visualize TG^n and its invariance under the shift σ; see Figs. 16–18.

Besides the purely visual aspect, Figs. 16–18 illustrate how symmetries constrain the possible attractors in TG^n. Indeed, an attractor A being a terminal scc, it must be a *trapping domain*, i.e., $b \in A \implies b' \in A$ for any (b, b'). On the other hand, since TG^n is invariant under the action of σ, if a node b belongs to A, all other nodes in the orbit $\mathbb{Z}_n b$ must also be in A. In other words, an attractor must be composed of a union of $\mathbb{Z}_n$-orbits. Yet, single $\mathbb{Z}_n$-orbits are never invariant, unless they are composed of fixed points:

Proposition 1. *For any $b \in \{0, 1\}^n$, either:*

- *b is a fixed point, in which case any $b' \in \mathbb{Z}_n b$ is also a fixed point, or*
- *any successor of b in TG^n belongs to $\{0, 1\}^n \setminus \mathbb{Z}_n b$, i.e., an orbit other than that of b. In particular, any cyclic attractor must be composed of at least two orbits.*

Proof. The first case follows directly from the fact that F is $\mathbb{Z}_n$-equivariant (10). Indeed, if b is a fixed point, i.e., $b = \phi(b)$, one deduces

$$\phi(\sigma^k b) = \sigma^k \phi(b) = \sigma^k b,$$

i.e., any $\sigma^k b$ is also a fixed point, and therefore the orbit $\mathbb{Z}_n b$ consists entirely of fixed points.

Now, let $b \neq \phi(b)$, i.e., it has one or several successors of the form $\overline{b}^i$ in TG^n. Then b and any successor $\overline{b}^i$ have a different number of coordinates equal to 1 (or 0), since the ith differ. On the other hand, any cyclic permutation σ^k clearly preserves the number of 1's (and 0's), from which the claimed property follows. □

Other attractors in TG can be characterized in terms of $\mathbb{Z}_n$-orbits as well. The set of $\mathbb{Z}_n$-orbits can be enumerated and is well known in combinatorics as the set of n-bead necklaces with two colors. In particular, an explicit formula is known for the number of orbits.[37]

$$\frac{1}{n} \sum_{d|n} \varphi(d) 2^{n/d} = \frac{1}{n} \sum_{k=1}^{n} 2^{\gcd(k,n)},$$

where φ is Euler's totient function (number of smaller coprime integers). This formula is in fact an application of Burnside's Lemma, where the sum counts the number of fixed points of different permutations in $\mathbb{Z}_n$. Though not directly of use here, this formula is indicative of the structure of the set of orbits and its relation to the divisors of n. In intuitive terms, one can think of Boolean vectors in terms of blocks of consecutive 0's or 1's. If a pattern of such blocks has a length d that divides n, repeating this block gives a vector whose orbit size is smaller than n (it equals d). For example, when n is even, one retrieves the two fixed points 0101 . . . 01 and 1010 . . . 10, which form a complete orbit of size 2.

A successor of $b \in \{0, 1\}^n$ is of the form $\overline{b}^i$ for some $1 \leqslant i \leqslant n$ such that $f_i \doteq f(b_{i-1}, b_i, b_{i+1}) \neq b_i$. One can list all possible values of f_i in the truth table below, where ↑ marks cases where $f_i \neq b_i$, i.e., $\overline{b}^i$

is a successor of b in TG,

b_{i-1}	0	0	0	0	1	1	1	1
b_i	0	0	1	1	0	0	1	1
b_{i+1}	0	1	0	1	0	1	0	1
f_i	0	1	1	1	1	0	0	0
		↑			↑		↑	↑

. (11)

This table can be expressed as rules, which summarize possible transitions in TG^n at a local level.

Proposition 2. *$\overline{b^i}$ is a successor of b if and only if*

$R0 : b_i = 0$ *and* $b_{i-1} \neq b_{i+1}$, *or*
$R1 : b_i = 1$ *and* $b_{i-1} = 1$,

where i is taken modulo n.

Note that this could have been derived directly from the definition of f.

From the rules above, we can deduce how blocks of successive 0's or 1's always admit successors in TG^n with a different pattern. First, for blocks of 0's:

Proposition 3. *Consider $b \in \{0,1\}^n$ containing a block of at least 2 and at most $n-1$ successive 0's. Then, there is a path in TG^n from b to b', where b' is as b with all but one of the 0's replaced by 1's in the aforementioned block.*

Proof. Let $2 \leqslant p \leqslant n-1$ denote the length of the block of 0's. By repeatedly applying rule R0 in Proposition 2, any block of 0's preceded (respectively, followed by) a 1 can be replaced by a block of 1's, switching each 0 starting from the leftmost (respectively, rightmost). After $p-1$ iterations, a single 0 is left and since it must be surrounded by two 1's R0 cannot be applied any more. □

So, we have that any state containing repeated 0's can reach another state where these are replaced by 1's and only leave isolated 0's. If a state contains several blocks of 0's, this can clearly be applied to all of them (in any order). The next result shows that a state with blocks of three or more repeated 1's (e.g., reached from a state with blocks of 0's) can reach a state with alternating values.

Proposition 4. *Consider $b \in \{0,1\}^n$ containing a block of at least 2 successive 1's. Then, there is a path in TG^n from b to b', defined by substituting 1010 . . . for the block of 1's occurring in b, resulting in no repetitions of 1 within the original block position in b, except in the special case where $b = 111\ldots1$ and n is odd, which leads to a single repeat of the form 11.*

Proof. The rule R1 in 2 states that the following transitions can occur: $11 \to 10$. The result directly follows from repeatedly applying the same rule. If the block is of even length this results in 10 . . . 10 and if it is of odd length in 10 . . . 101. In the latter case, if the block was the whole of b, the first and last digits are neighbors and this leads to a single repeat 11. □

We can now deduce a complete description of attractors in TG^n.

Proposition 5. *The state 00 . . . 0 is always a fixed point in TG^n. In addition,*

- *If n is even, the only other attractors in TG^n are the fixed points 0101 . . . 01 and 1010 . . . 10.*
- *If n is odd, the only other attractor is a cyclic attractor composed of the two orbits*

$$\mathbb{Z}_n\{1010\ldots101\} \quad \textit{and} \quad \mathbb{Z}_n\{0010\ldots101\},$$

where . . . denotes repeats of the block 10.

The basin of attraction of the non-zero attractors contains any state different from 00 . . . 00.

The proof is given in Appendix C. Note that the paths to the attractor(s) described in the proof above are non-unique, as appears in Figs. 16–18.

C. Transition graphs for the higher dimensional models

Section V B completely characterizes the global dynamics of the n-dimensional model at the discrete level of the transition graph. The underlying continuous dynamics was discussed in more detail in Sec. IV, but from the structure of the attractor (Proposition 5 or Figs. 16–18), one can anticipate the occurrence of length-2 cycles, which correspond to singular walls attracting trajectories from both sides (known as "black walls"). In this section, we describe how the higher dimensional models do not have black walls, but instead higher dimensional regular cycles in a way which can be put in systematic correspondence with the n-dimensional model.

Consider the $3n$-dimensional model (4). Since each unit has now three variables, an analog to the truth table (11) would contain $8^3 = 512$ columns and would be difficult to interpret. Note however that the variables of unit i only depend on neighboring units through their variables $x_{i\pm1}$, regardless of $y_{i\pm1}$ and $z_{i\pm1}$. To keep the subscripts simple, let us use the redundant notation for Boolean variables

$$V_i = (X_i, Y_i, Z_i) = (b_{3i-2}, b_{3i-1}, b_{3i}).$$

Then, a box will be described by a Boolean vector of the form $(V_i)_{1\leqslant i\leqslant n}$ and one can write the successor relation as

$$\left(X_i^{t+1}, Y_i^{t+1}, Z_i^{t+1}\right) = \left[f\left(Z_{i-1}^t, Z_i^t, Z_{i+1}^t\right), \overline{X_i}^t, \overline{Y_i}^t\right].$$

Leaving Z_{i-1} and Z_{i+1} as variables, one can write the truth table in a compact form, using a primed notation $'$ to denote successors

X_i	Y_i	Z_i	X_i'	Y_i'	Z_i'
0	0	0	$Z_{i-1} \oplus Z_{i+1}$	1	1
0	0	1	$\overline{Z_{i-1}}$	1	1
0	1	0	$Z_{i-1} \oplus Z_{i+1}$	1	0
0	1	1	$\overline{Z_{i-1}}$	1	0
1	0	0	$Z_{i-1} \oplus Z_{i+1}$	0	1
1	0	1	$\overline{Z_{i-1}}$	0	1
1	1	0	$Z_{i-1} \oplus Z_{i+1}$	0	0
1	1	1	$\overline{Z_{i-1}}$	0	0

. (12)

It is apparent from the truth table that the two Boolean values $Z_{i-1} \oplus Z_{i+1}$ and Z_{i-1} completely determine this graph. The relation between

these values and $Z_{i\pm1}$ themselves is summarized in the following table:

$\overline{Z_{i-1}}, Z_{i-1} \oplus Z_{i+1}$	00	01	10	11
Z_{i-1}, Z_{i+1}	11	10	00	01

from which we see, in particular, that all the 4 possible combinations of $Z_{i\pm1}$ lead to a distinct table.

By considering single digit (i.e., asynchronous) updates, one can build a "local" transition graph on the 8 nodes above, for each of the 4 possible values taken by the pair of neighboring inputs Z_{i-1} and Z_{i+1}, see Fig. 19 (the analogous graph for the n-dimensional model is also included for comparison). One can note that the neighborhoods 00 (respectively, 10) give rise to a white wall (respectively, black wall) in the n-dimensional model, with an unstable (respectively, stable) periodic sequence as analog in the $3n$-dimensional model.

There is an apparent similarity in Fig. 19 between the n and $3n$-dimensional models. In particular, the rules from Proposition 2 can be extended.

The manifestation of R0 in Fig. 19 is that for both neighborhoods 01 and 10, all configurations of unit i having at least one 0 are unstable, whereas $00Z$ is stable when $Z_{i-1} = Z_{i+1} = Y$, for $Z \in \{0, 1\}$. The two states 000 and 001 take the role of a single 0 for the n-dimensional model.

The manifestation of R1 in Fig. 19 is that for both neighborhoods 10 and 11, all configurations of unit i having either $X_i = 1$ or $Y_i = 1$ are unstable, whereas 111 is stable whenever $Y_{i-1} = 0$. The state 111 is now the $3n$ analog of a single 1 in the n-dimensional model.

Importantly, these main qualitative features extend to the $4n$-dimensional model, which is the most accurate. The local transitions, though less readable, are shown in Appendix B:

- the state 1011 is analogous to a "1" and stable if and only if the preceding input is 0,
- the states 0101 and 0100 are analogous to a "0," stable when both neighbors are equal,
- the neighborhood 10 leads to a stable cyclic sequence,
- the neighborhood 00 leads to an unstable cyclic sequence. Unlike the n-dimensional model, this sequence has branching points, which has the potential to generate entropy (cf. Sec. IV D 4).

In summary, higher dimensional models are expected to present qualitatively similar sequences of states to the n-dimensional version, but with additional steps corresponding to variable updates taking place sequentially within individual units on the ring. For instance, the one step changes described by Proposition 2 are still possible, but require several transitions in TG, with perhaps several alternative paths possible. Alternations of "0" and "1" still have some level of persistence (and lead to fixed points with an even number of units) and the full zero state is fixed, but "0" now corresponds to a different internal state.

As for the attractors, the combinatorial explosion of possible paths makes any visual representation impossible. The analogies at the local level lead us to expect a similar global structure as described in Proposition 5, albeit each $\mathbb{Z}_n$-orbit increases exponentially (with the number $2, 3, 4$ or internal variables) in size, and may include internal transitions (notably cycles which could be repeated an arbitrary number of times and therefore contribute to the generation of entropy). As noted in Remark 1, the transition graphs only offer an over-approximation of the dynamics and for a more accurate description one needs to return to the continuous model.

VI. CONCLUSION

In summary, the main practical result of this investigation is that the system modeled in this paper does exhibit chaotic dynamics, as measured by a positive LE, and therefore is able to spontaneously generate a positive entropy (in the sense of Kolmogorov-Sinai as well as for the more empirical SampEn).

The amplitude of LEs seemed relatively small (especially for the $3n$ model). Of the reasons that could explain this is the strong restriction on parameter exploration that was imposed by the computational cost of evaluating LEs. In particular, it is expected that real circuits will not have strictly identical decays for all units of the same types, i.e., the parameters μ, ν, λ should be considered with small perturbation terms accounting for hardware variability. Furthermore, the number of units n, certainly impact the dynamics, but only the case $n = 5$ has been considered here when estimating LEs, and $n = 9$ in estimating SampEn. The more empirical results obtained using Sample Entropy suggest that the sampling rate plays an important role in the generation of entropy: sampling too fast may result in lesser unpredictability.

On the more theoretical side, the construction of a simplified n-dimensional model has allowed us to completely characterize the global dynamics of the model at the discrete level. It is known that the discrete transition graph underlying a Glass network typically has a higher entropy than the continuous system itself.[26] This upper bound at least shows that a positive entropy cannot be ruled out (indeed the attractors described in Proposition 5 have a positive topological entropy).

Beyond this point, the n-dimensional model can be related to its higher dimensional counterparts quite clearly. The main intuitive bridge between these models is that black/white walls occurring in the n-dimensional model (which appear as 2-cycles in Figs. 16–18) give rise to cycles in the transition graphs of the higher dimensional models. An outstanding question which we leave for future work is the following: when it is chaotic, is the continuous dynamics always restricted to (the higher dimensional analog of) the global attractor of the n-dimensional model, or can it remain in other parts of state space? Reasoning in terms of limits of infinitely fast, slow or many inverters as we have started in Sec. IV D might provide a good entry point to address this problem.

In any case, whatever the ultimate source of the chaotic behavior, the complexity of the dynamics of this circuit, combined with the portability implied by its design using standard logic gates, make it an excellent candidate for a TRNG.

ACKNOWLEDGMENTS

R. Edwards was partially supported by the Natural Sciences and Engineering Research Council (NSERC) of Canada.

APPENDIX A: NIST TEST SUITES RESULTS

TABLE I. Results for 100 MB samples under NIST SP800-22 test suite.

Test	Byte/sequence (M)	Test sequences	Smallest P-value	Pass rate	Overall
Frequency	1	100	0.494392	100/100	Pass
Block frequency	1	100	0.002374	97/100	Pass
Cumulative sums	1	100	0.108791	99/100	Pass
Runs	1	100	0.108791	99/100	Pass
Longest run	1	100	0.419021	100/100	Pass
Rank	1	100	0.964295	100/100	Pass
FFT	1	100	0.574903	96/100	Pass
Non-overlapping template	1	100	0.002559	100/100	Pass
Overlapping template	1	100	0.145326	98/100	Pass
Universal	1	100	0.401199	98/100	Pass
Approximate entropy	1	100	0.090936	97/100	Pass
Random excursions	1	100	0.155209	98/100	Pass
Random excursions variant	1	100	0.005166	97/100	Pass
Serial	1	100	0.401199	99/100	Pass
Linear complexity	1	100	0.289667	99/100	Pass

TABLE II. The IID test results of 100 MB TRNG samples against NIST SP800-90B test suite.

Tests			Results		
			$C_{i,0}$	$C_{i,1}$	IID
Permutation test	Excursion		4882	0	Pass
	Number of directional runs		6088	7	Pass
	Length of directional runs		3952	5993	Pass
	Number of increases and decreases		485	4	Pass
	Number of runs based on the median		4396	8	Pass
	Length of runs based on median		6110	2407	Pass
	Average collision test statistic		136	0	Pass
	Maximum collision test statistic		1995	790	Pass
	Compression test statistic		8229	4	Pass
	Periodicity test statistic	Periodicity(1)	7436	52	Pass
		Periodicity(2)	4492	64	Pass
		Periodicity(8)	7075	57	Pass
		Periodicity(16)	9849	4	Pass
		Periodicity(32)	6990	54	Pass
	Covariance test statistic	Covariance(1)	6073	0	Pass
		Covariance(2)	4253	0	Pass
		Covariance(8)	4101	0	Pass
		Covariance(16)	8045	0	Pass
		Covariance(32)	2546	0	Pass
Chi-square independence			Pass		
Chi-square goodness-of-fit			Pass		
Length of the longest repeated substring test			Pass		
Restart tests			Pass		
Min-entropy			7.07026		

APPENDIX B: 4*n*-DIMENSIONAL MODEL: LOCAL TRANSITIONS

For the model (3), the truth table below describes transitions. As before the primed notation X' is used a shorthand for X^{t+1}

X_i	Y_i	Z_i	U_i	X_i'	Y_i'	Z_i'	U_i'
0	0	0	0	Z_{i-1}	1	1	Z_{i+1}
0	0	0	1	$\overline{Z_{i-1}}$	1	1	Z_{i+1}
0	0	1	0	Z_{i-1}	1	1	1
0	0	1	1	$\overline{Z_{i-1}}$	1	1	1
0	1	0	0	Z_{i-1}	1	0	Z_{i+1}
0	1	0	1	$\overline{Z_{i-1}}$	1	0	Z_{i+1}
0	1	1	0	Z_{i-1}	1	0	1
0	1	1	1	$\overline{Z_{i-1}}$	1	0	1

X_i	Y_i	Z_i	U_i	X_i'	Y_i'	Z_i'	U_i'
1	0	0	0	Z_{i-1}	0	1	Z_{i+1}
1	0	0	1	$\overline{Z_{i-1}}$	0	1	Z_{i+1}
1	0	1	0	Z_{i-1}	0	1	1
1	0	1	1	$\overline{Z_{i-1}}$	0	1	1
1	1	0	0	Z_{i-1}	0	0	Z_{i+1}
1	1	0	1	$\overline{Z_{i-1}}$	0	0	Z_{i+1}
1	1	1	0	Z_{i-1}	0	0	1
1	1	1	1	$\overline{Z_{i-1}}$	0	0	1

We deduce local transition graphs, similar to Fig. 19, see Figs. 20 and 21.

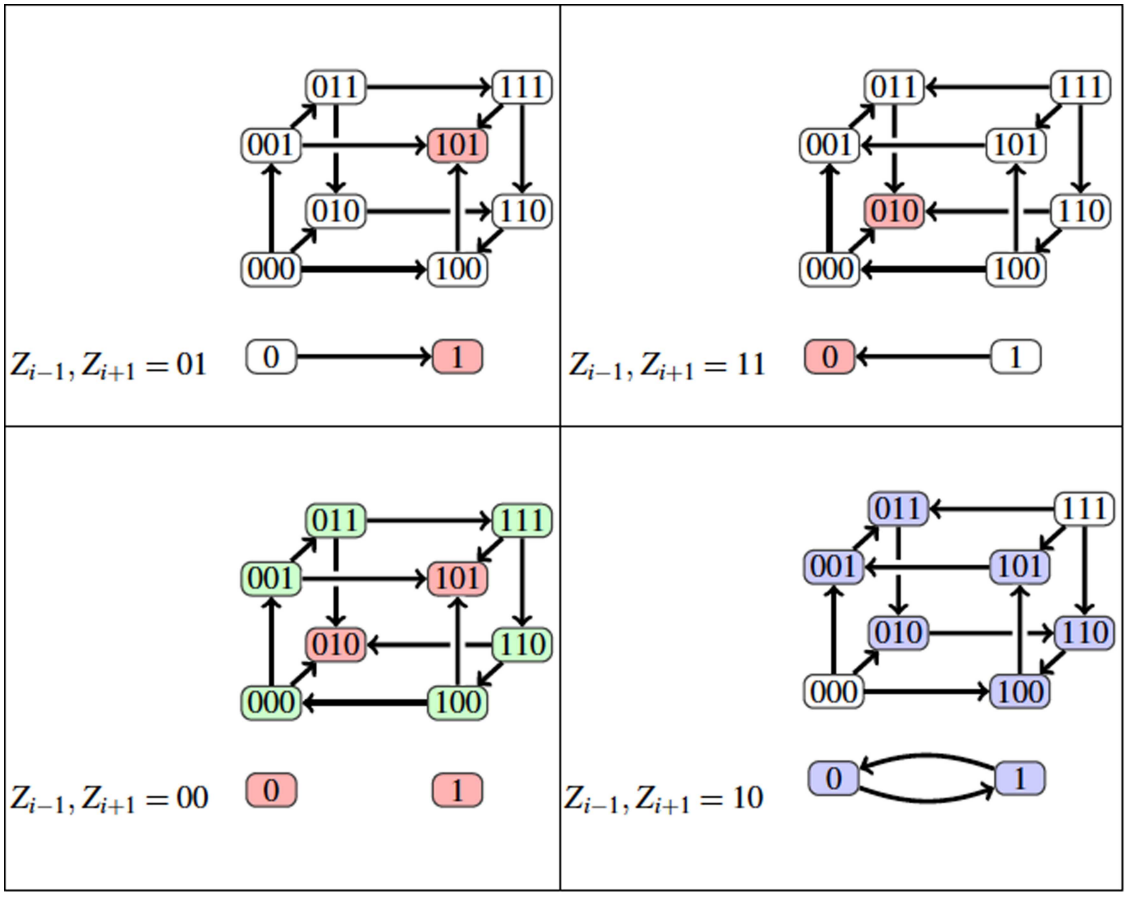


FIG. 19. The possible transitions in a single unit on the ring, assuming all other units remain unchanged, for the 3*n*- and *n*- dimensional models (top and bottom graphs, respectively), for all 4 possible values of the neighboring inputs (denoted $Z_{i\pm1}$ generically). Fixed points in red, stable cycles in blue, unstable cycles in green.

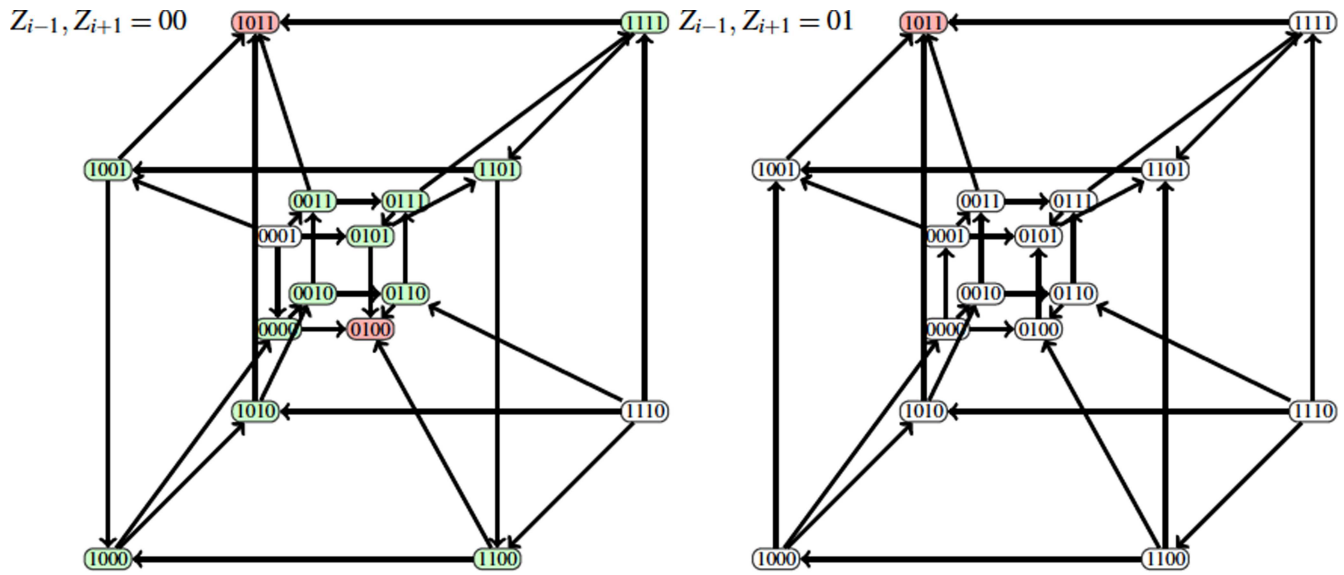


FIG. 20. The local transition graphs, similar to Fig. 19, for the 4*n*-dimensional model, for 0 left neighbors.

APPENDIX C: PROOF OF PROPOSITION 5

Proof. That $00\ldots0$ is a fixed point can be directly verified, for instance using the truth table (11).

• Suppose n is even and let $b = \phi(b) \neq (00\ldots0)$ be a fixed point. $b \neq (11\ldots1)$ either, since the latter is not fixed. Hence, there must be a pair 10, which one may assume by symmetry to be $b_1 = 1$ and $b_2 = 0$. From Proposition 2 (rule R1), b cannot be fixed if $b_n = 1$, so it must be 0. Then, because of rule R1, b_{n-1} must be 1 since otherwise b is not fixed, and by induction, one readily deduces that $b = 1010\ldots10$ is the only possible fixed point with $b_1 = 1$ and $b_2 = 0$, which can only occur for n even. Then, from Proposition 1 one gets $0101\ldots01$ as only other point in the same orbit, which must be fixed by symmetry.

• Let now n be an odd integer. We shall prove first that the two orbits do indeed form an attractor. In words, the two orbits are

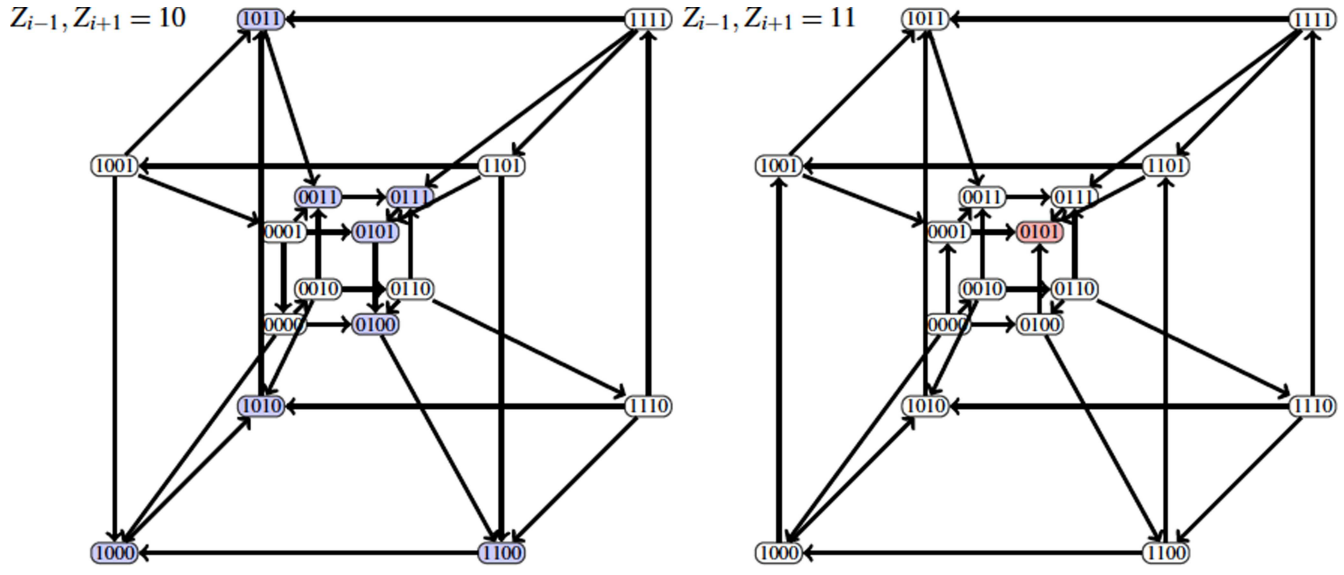


FIG. 21. The local transition graphs, similar to Fig. 19, for the 4*n*-dimensional model, for 1 left neighbors.

composed of repeats of the pair 10, with a single repeated block of the form 00 or 11, respectively. We denote $a = 1010\ldots01$ and $c = 0010\ldots01$ the two orbit representatives appearing in the proposition. From the rules in Proposition 2, one deduces that the only coordinate susceptible of change in a is $a_1 = 1$. Indeed, its predecessor $a_n = 1$, and all other 1's are preceded by a 0, and all 0's are surrounded by two 1's. Therefore, the only successor of a in TG^n is $\bar{a}^1 = 0010\ldots101 = c$. Now, the coordinates susceptible of change in c are c_1 and c_2, as the only 0's surrounded by a pair of different values and given the absence of repeated 1's. Therefore, c has exactly two successors in TG^n, namely a itself (switching back c_1) and $\bar{c}^2 = 0110\ldots101$. One sees that $\bar{c}^2 = \sigma^2 a \in \mathbb{Z}_n a$, so that the two orbits $\mathbb{Z}_n a$ and $\mathbb{Z}_n c$ do indeed form a trapping domain in TG^n, which from Proposition 1 is minimal and therefore an attractor.

It remains to prove that non-zero attractors have all nonzero states in their basin of attraction. Let $b \in \{0,1\}^n$, assumed nonzero and not in either orbits $\mathbb{Z}_n a$ or $\mathbb{Z}_n c$ for n odd or not one of the fixed points if n is even. It follows that b must contain either

(i) at least one block of $\geqslant 3$ consecutive 0's or at least two blocks of $\geqslant 2$ consecutive 0's,
(ii) at least one block of $\geqslant 3$ consecutive 1's
(iii) at least two blocks of 2 consecutive 1's.

From Proposition 3, case (i) reduces to (ii) and (iii). From Proposition 4, in case (ii) all blocks of 1's can be replaced by alternations of 10. The same proposition also shows that if a block is of full length, i.e., $b = 11\ldots1$, there is a path to the attractors described above. So, assume that the blocks are of length $p \leqslant n-1$. Then they must be preceded and followed by a 0 (which can be the same if the block length is $n-1$). From Proposition 4, one has that the block and its 0 neighbors can follow a path in TG^n of the form

$$0\overbrace{11\ldots1}^{1's}0 \longrightarrow 0\overbrace{10\ldots10}^{10's}0 \qquad \text{if } p \text{ is even,}$$

$$0\overbrace{11\ldots1}^{1's}0 \longrightarrow 0\overbrace{10\ldots10}^{10's}10 \qquad \text{if } p \text{ is odd.}$$

For p even the final 00 can switch to 10 by applying R0 to the penultimate digit. This gives a length-2 block 11, while p odd leads to no repeats at all. Overall, applying the above to all blocks of length $\geqslant 3$ shows that case (ii) reduces to case (iii).

Case (iii) is treated by relying on the observation that 11 blocks can be shifted two coordinates to the right along an alternating sequence

$$1101 \xrightarrow{\text{R1}} 1001 \xrightarrow{\text{R0}} 1011 \qquad (\sigma^2)$$

all other coordinates of b remaining unchanged. Now, if two 11 blocks occur from (i) and (ii) above, it can be assumed that the sequence in-between is an alternation of $0101\ldots0$ and therefore there is an odd number of coordinates between the two blocks, say $p = 2q+1$. The overall form is $11\,0101\ldots010\,11$. The shifting described above gives after q iterations

$$11\,0101\ldots010\,11 \xrightarrow{\sigma^{2q}} 10\,1010\ldots110\,11.$$

Then, the final five digits can follow the sequence:

$$11011 \xrightarrow{\text{R1}} 10011 \xrightarrow{\text{R0}} 10111 \xrightarrow{\text{R1}} 10101.$$

Therefore, pairs of 11 blocks can cancel out. To conclude, once all repeats other than 11 have vanished as per (i) and (ii), one has

- For even n, there must be an even number of 11, and the cancellation of pairs above eventually reaches one of the two fixed points.
- For odd n, there must be an odd number of 11, and the cancellation of pairs leaves a single block 11, corresponding to the attractor. □

REFERENCES

[1] V. Fischer, "Random number generators for cryptography, design and evaluation," in *Summer School on Design and Security of Cryptographic Algorithms and Devices* (2014).
[2] B. Jun and P. Kocher, "The intel random number generator," Technical Report (Cryptography Research Inc. white paper, 1999).
[3] P. Kohlbrenner and K. Gaj, "An embedded true random number generator for fpgas," in *Proceedings of the 2004 ACM/SIGDA 12th International Symposium on Field Programmable Gate Arrays* (ACM, 2004), pp. 71–78.
[4] S. Robson, B. Leung, and G. Gong, "Truly random number generator based on a ring oscillator utilizing last passage time," IEEE Trans. Circuits Syst. II Express Briefs **61**, 937–941 (2014).
[5] B. Sunar, W. J. Martin, and D. R. Stinson, "A provably secure true random number generator with built-in tolerance to active attacks," IEEE Trans. Comput. **56**, 109–119 (2007).
[6] R. Adler, "A study of locking phenomena in oscillators," in *Proceedings of the IRE* (IEEE, 1946), Vol. 34, pp. 351–357.
[7] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, B. Robisson, and P. Maurine, "Contactless electromagnetic active attack on ring oscillator based true random number generator," in *International Workshop on Constructive Side-Channel Analysis and Secure Design* (Springer, 2012), pp. 151–166.
[8] A. T. Markettos and S. W. Moore, "The frequency injection attack on ring-oscillator-based true random number generators," in *International Workshop on Cryptographic Hardware and Embedded Systems* (Springer, 2009), pp. 317–331.
[9] H. Martin, T. Korak, E. S. Millán, and M. Hutter, "Fault attacks on strngs: Impact of glitches, temperature, and underpowering on randomness," IEEE Trans. Inf. Forensics Secur. **10**, 266–277 (2015).
[10] T. Matsumoto, "A chaotic attractor from Chua's circuit," IEEE Trans. Circuits Syst. **31**, 1055–1058 (1984).
[11] Z. Galias, "Positive topological entropy of Chua's circuit: A computer assisted proof," Int. J. Bifurc. Chaos **7**, 331–349 (1997).
[12] N. Kuznetsov, O. Kuznetsova, G. Leonov, and V. Vagaytsev, "Hidden attractor in Chua's circuit," in *Proceedings of the 8th International Conference on Informatics in Control, Automation and Robotics* (Scitepress, 2011), Vol. 1, pp. 279–283.
[13] N. Kuznetsov, O. Kuznetsova, G. Leonov, T. Mokaev, and N. Stankevich, "Hidden attractors localization in Chua circuit via the describing function method," IFAC Papers Online **50**, 2651–2656 (2017).
[14] Y. Hosokawa and Y. Nishio, "Simple chaotic circuit using cmos ring oscillators," Int. J. Bifurcation Chaos **14**, 2513–2524 (2004).
[15] S. N. Dhanuskodi, A. Vijayakumar, and S. Kundu, "A chaotic ring oscillator based random number generator," in *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)* (IEEE, 2014), pp. 160–165.
[16] J. Mason, P. Linsay, J. Collins, and L. Glass, "Evolving complex dynamics in electronic models of genetic networks," Chaos **14**, 707–715 (2004).
[17] S. Srivastava and J. Roychowdhury, "Analytical equations for nonlinear phase errors and jitter in ring oscillators," IEEE Trans. Circuits Syst. I **54**, 2321–2329 (2007).
[18] L. Glass, T. Perkins, J. Mason, H. Siegelmann, and R. Edwards, "Chaotic dynamics in an electronic model of a genetic network," J. Stat. Phys. **121**, 969–994 (2005).

[19]S. Wolfram, *A New Kind of Science* (Wolfram Media, 2002).
[20]E. Plahte and S. Kjøglum, "Analysis and generic properties of gene regulatory networks with graded response functions," Physica D **201**, 150–176 (2005).
[21]All of these numbers have at least around ±15% variation.
[22]In an idealized situation where the ±15% variation is ignored.
[23]M. Golubitsky and I. Stewart, *The Symmetry Perspective: From Equilibrium to Chaos in Phase Space and Physical Space* (Birkhäuser, 2002).
[24]A. Filippov, *Differential Equations with Discontinuous Righthand Sides* (Springer, 1988).
[25]S. Wolfram, "Random sequence generation by cellular automata," Adv. Appl. Math. **7**, 123–169 (1986).
[26]E. Farcot, "Geometric properties of piecewise affine biological network models," J. Math. Biol. **52**, 373–418 (2006).
[27]A. Pikovsky and A. Politi, *Lyapunov Exponents: A Tool to Explore Complex Dynamics* (Cambridge University Press, 2016).
[28]L. Dieci, R. Russell, and E. V. Vleck, "On the computation of lyapunov exponents for continuous dynamical systems," SIAM J. Numer. Anal. **34**, 402–423 (1997).
[29]A. Hajimiri, S. Limotyrakis, and T. Lee, "Jitter and phase noise in ring oscillators," IEEE J. Solid-State Circuits **34**, 790–804 (1999).
[30]J. Richman and J. Moorman, "Physiological time-series analysis using approximate entropy and sample entropy," Am. J. Physiol. Heart Circ. Physiol. **278**, 2039–2049 (2000).
[31]A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, A statistical test suite for random and pseudorandom number generators for cryptographic applications, Technical Report (Booz-Allen and Hamilton Inc Mclean Va, 2001).
[32]M. Turan, E. Barker, J. Kelsey, K. McKay, M. Baish, and M. Boyle, Nist special publication 800-90b: Recommendation for the entropy sources used for random bit generation, US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD (2018).
[33]R. Edwards, "Analysis of continuous-time switching networks," Physica D **146**, 165–199 (2000).
[34]A strongly connected component S is *terminal*, if there is no edge having its origin in S and its end out of S.
[35]L. Glass, "Global analysis of nonlinear chemical kinetics," in *Statistical Mechanics, Part B: Time-Dependent Processes*, edited by B. J. Berne (Plenum, New York, 1977), pp. 311–349.
[36]L. Glass, "Combinatorial aspects of dynamics in biological system," in *Statistical Mechanics and Statistical Methods in Theory and Application*, edited by U. Landman (Plenum, New York, 1977), pp. 585–611.
[37]See http://oeis.org/A000031 for the terms up to $n = 10$ are $1, 2, 3, 4, 6, 8, 14, 20, 36, 60$.
[38]R. Edwards, E. Farcot, and E. Foxall, "Explicit construction of chaotic attractors in glass networks," Chaos Solitons Fractals **45**, 666–680 (2012).
[39]J. Gouzé and T. Sari, "A class of piecewise linear differential equations arising in biological models," Dyn. Syst. **17**, 299–316 (2003).