Electronic gene networks as true random number generators

R. Edwards[1], E. Farcot[2], S. Best[3], P. Gill[3], I. Belgacem[1]

[1]University of Victoria
[2]University of Nottingham
and [3]Rambus, Inc., California

SIAM, 9 July 2018

Table of contents

How current TRNGs work

- Essentially, use ring oscillators (a ring of logic gates that produces an oscillation, acting as a negative feedback loop) in which the thermal noise of the circuit causes random phase shifts.
- Output from two or more of these are often combined through an XOR gate or a binary tree of XOR gates to increase the density in time of the phase shifts.

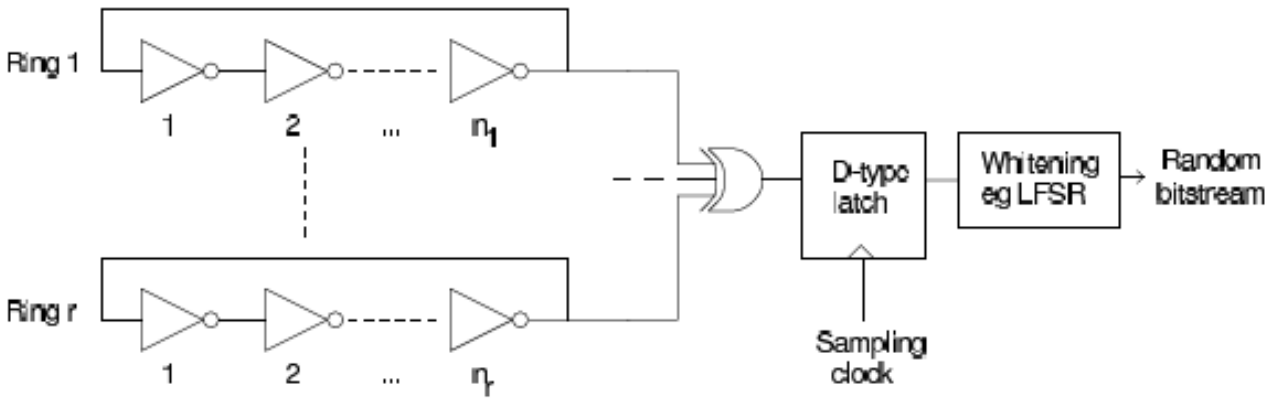


Fig. 2. Outline of the basic ring oscillator TRNG.

Markettos and Moore, 2009 (Cryptographic Hardware and Embedded Systems)

How current TRNGs work - and how they are hacked

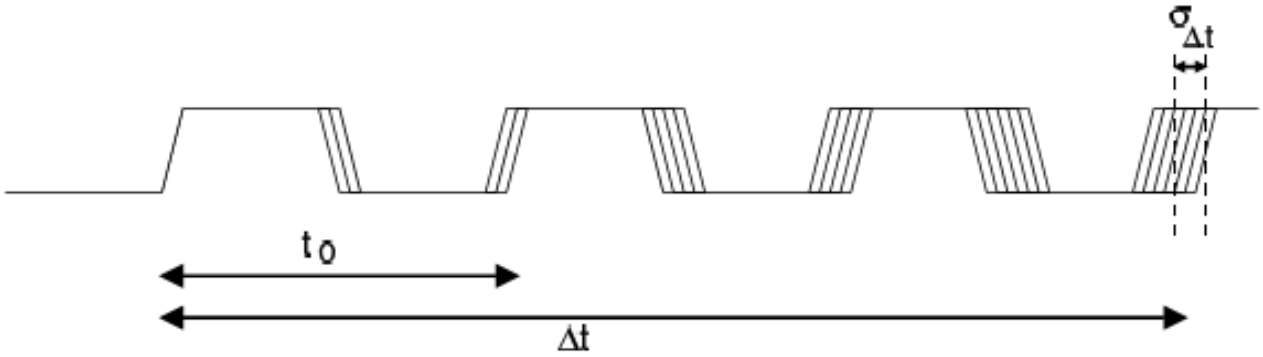


Fig. 3. Jitter in the time domain causes increasing uncertainty in the timing of transitions.

Markettos and Moore, 2009 (Cryptographic Hardware and Embedded Systems)

- The result is sampled at a non-commensurate frequency, to produce a sequence of bits with positive entropy.
- Injection of a signal at an appropriate frequency can eliminate much of the phase shifting, rendering the signal more predictable.
- Idea: An intrinsically chaotic circuit may be more robust to hacking.

How current TRNGs work - and how they are hacked

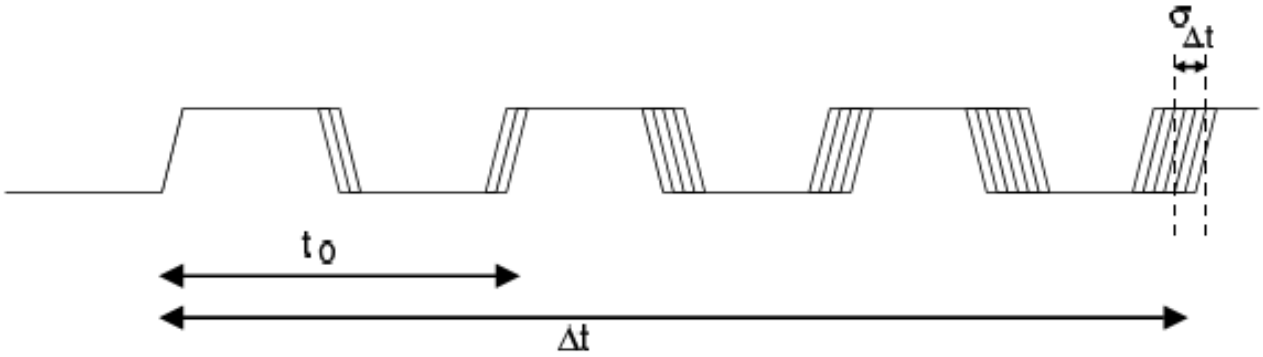


Fig. 3. Jitter in the time domain causes increasing uncertainty in the timing of transitions.

Markettos and Moore, 2009 (Cryptographic Hardware and Embedded Systems)

- The result is sampled at a non-commensurate frequency, to produce a sequence of bits with positive entropy.
- Injection of a signal at an appropriate frequency can eliminate much of the phase shifting, rendering the signal more predictable.
- Idea: An intrinsically chaotic circuit may be more robust to hacking.

2. Rambus circuit

The idea

- Scott Best, of Rambus, Inc. (California), proposed a design that would have an inherently broader power spectrum and should thus be more resistant to hacking.
- The idea is to use a circuit that is intrinsically chaotic, even before considering the thermal noise that is always present. Thus, the circuit without noise should already have a positive Lyapunov exponent.
- The Rambus circuit is still based on the ring oscillator idea, but with local feedback and feedforward connections to mimic the logic of CA Rule 30 (the 30th of Wolfram's Elementary Cellular Automata).
- Rule 30 produces irregular ('chaotic') behaviour in Cellular Automata.

The idea

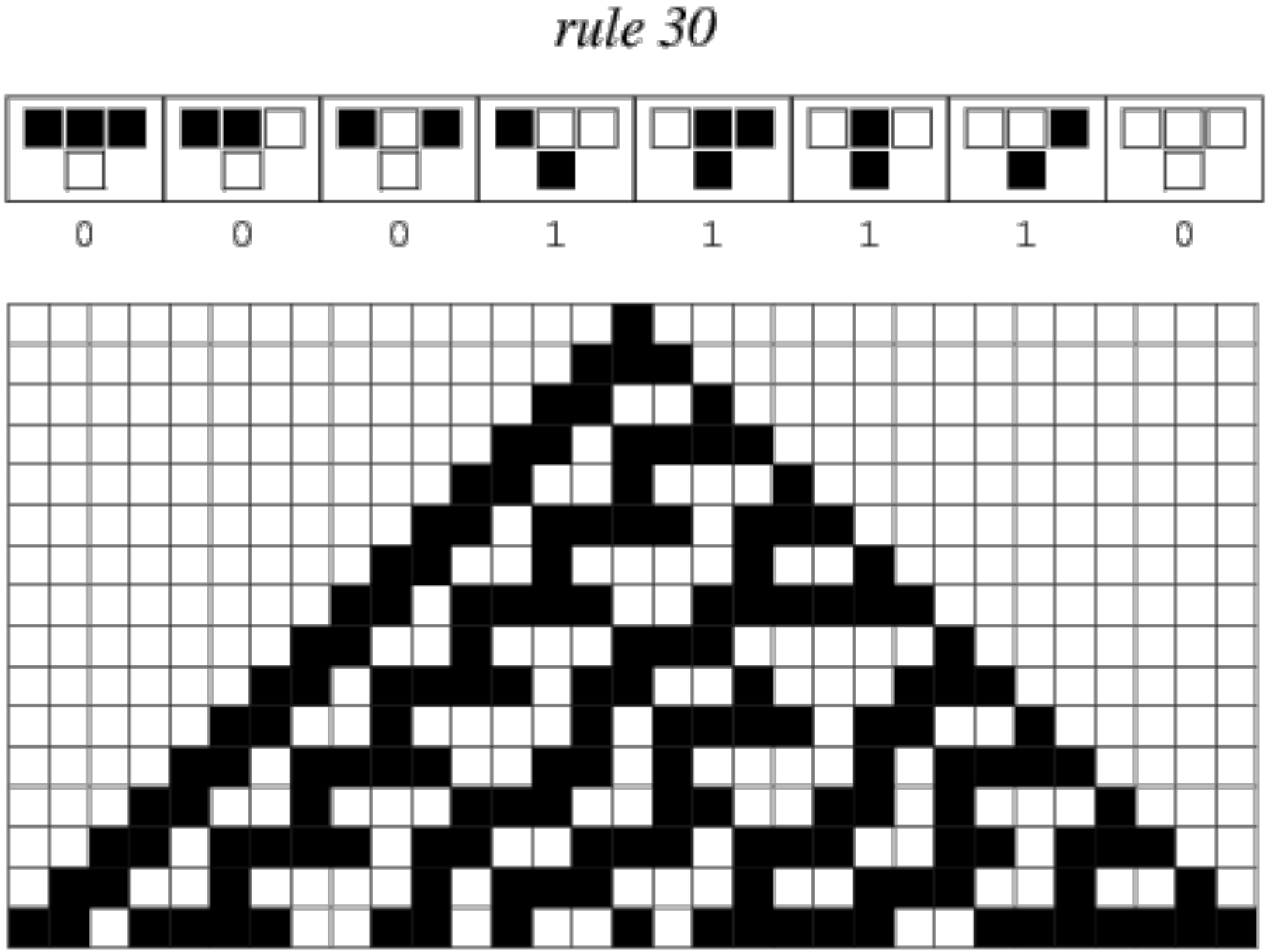
- Scott Best, of Rambus, Inc. (California), proposed a design that would have an inherently broader power spectrum and should thus be more resistant to hacking.
- The idea is to use a circuit that is intrinsically chaotic, even before considering the thermal noise that is always present. Thus, the circuit without noise should already have a positive Lyapunov exponent.
- The Rambus circuit is still based on the ring oscillator idea, but with local feedback and feedforward connections to mimic the logic of CA Rule 30 (the 30th of Wolfram's Elementary Cellular Automata).
- Rule 30 produces irregular ('chaotic') behaviour in Cellular Automata.

CA Rule 30

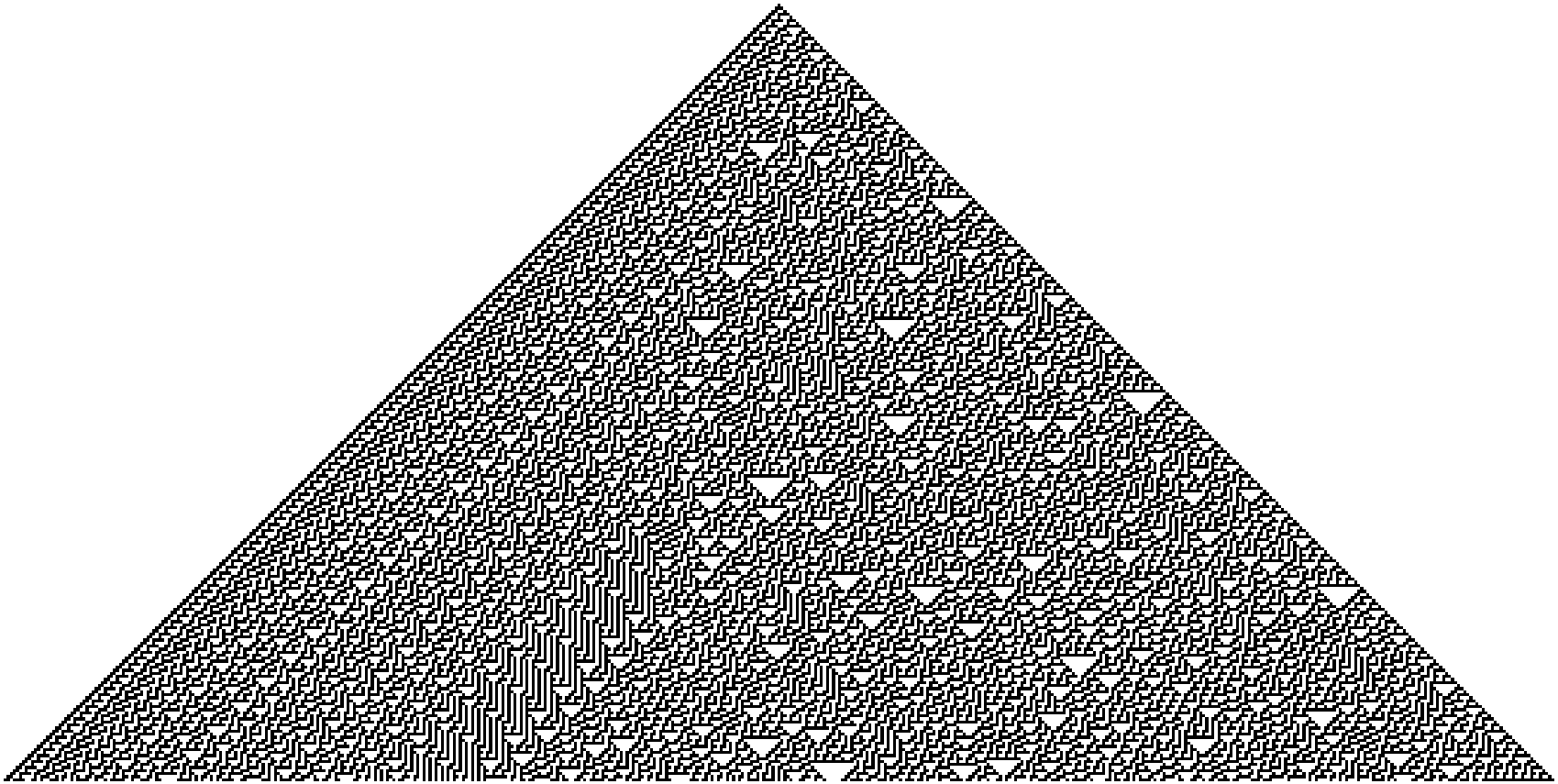
Rule 30: $x_i^{(t+1)} \leftarrow (x_i^{(t)} \text{ OR } x_{i+1}^{(t)}) \text{ XOR } x_{i-1}^{(t)}$

$x_{i-1}^{(t)}, x_i^{(t)}, x_{i+1}^{(t)}$	$x_i^{(t+1)}$
000	0
001	1
010	1
011	1
100	1
101	0
110	0
111	0

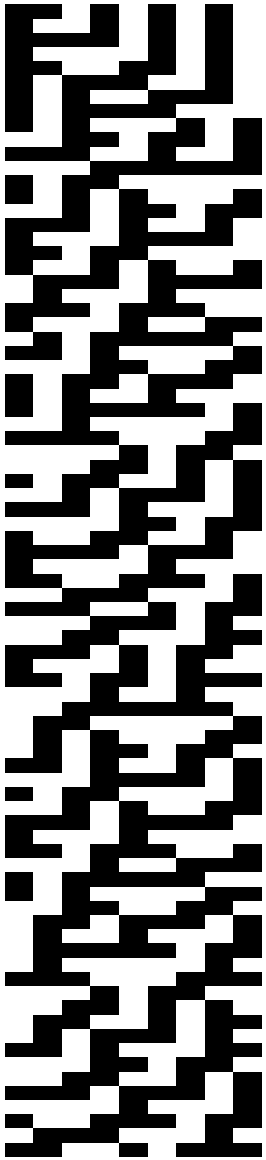
CA Rule 30



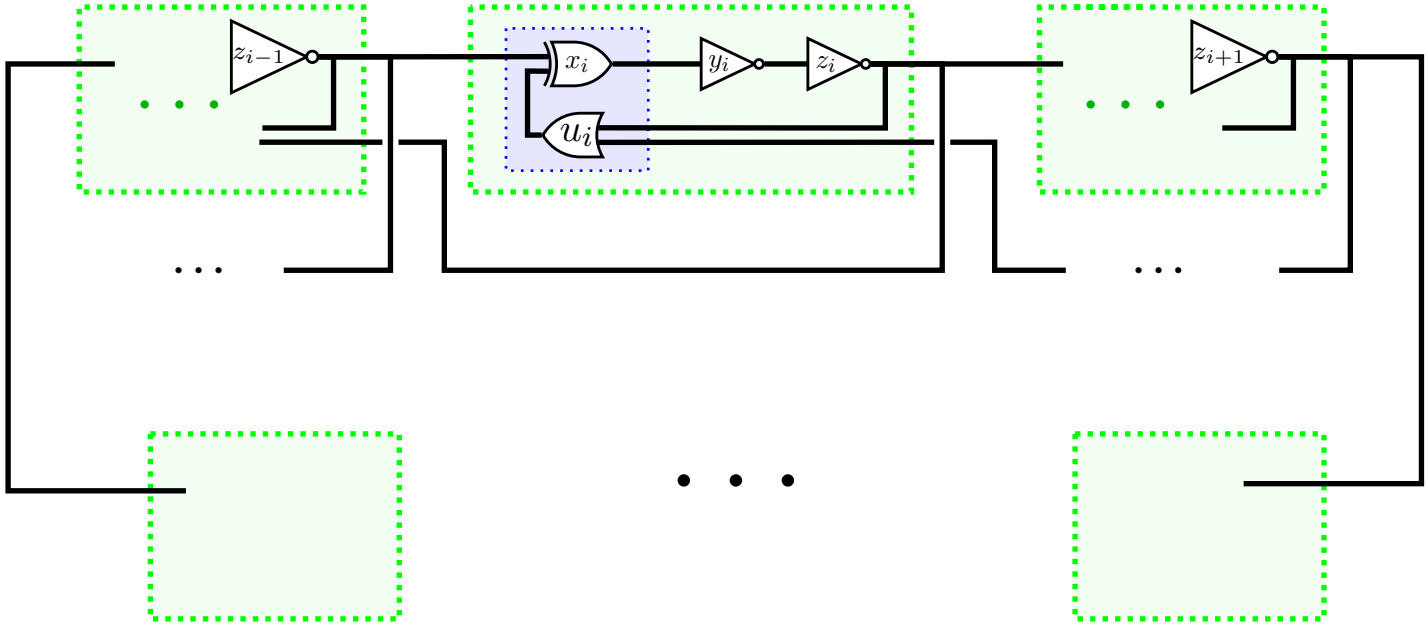
CA Rule 30 - infinite number of cells



CA Rule 30 - 9 cell ring



The Rambus circuit



$$
\begin{aligned}
u_i &\leftarrow z_i \text{ OR } z_{i+1} \\
x_i &\leftarrow u_i \text{ XOR } z_{i-1} \\
y_i &\leftarrow \text{NOT } x_i \\
z_i &\leftarrow \text{NOT } y_i
\end{aligned}
$$

Rambus circuit equations ($4n$-dimensional model)

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

where

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

and κ_{x_i}, γ_{x_i}, etc., and θ are positive constants.

Rambus circuit equations ($3n$-dimensional model)

More simply, if we take the OR gate (u_i) to be instantaneous,

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

where

$$f(z_{i-1}, z_i, z_{i+1}) = s^-(z_{i-1})\left(1 - s^-(z_i)s^-(z_{i+1})\right) + s^+(z_{i-1})s^-(z_i)s^-(z_{i+1}),$$

s^+ and s^- are as before, and the constants are adjusted appropriately.

Rambus circuit equations (n-dimensional model)

Since the inverters are thought to be quicker in practice, we could obtain a lower-dimensional model by eliminating y_i or z_i or both, or even reduce the logic of each unit to a single equation:

$$\frac{dx_i}{dt} = \kappa_{x_i} f(x_{i-1}, x_i, x_{i+1}) - \gamma_{x_i} x_i$$

where

$$f(x_{i-1}, x_i, x_{i+1}) = s^-(x_{i-1})\left(1 - s^-(x_i)s^-(x_{i+1})\right) + s^+(x_{i-1})s^-(x_i)s^-(x_{i+1}),$$

s^+ and s^- are as before, and the constants are adjusted appropriately.

All of these equations are in the form of Glass networks, as used to model gene regulation!

Rambus circuit equations (n-dimensional model)

Since the inverters are thought to be quicker in practice, we could obtain a lower-dimensional model by eliminating y_i or z_i or both, or even reduce the logic of each unit to a single equation:

$$\frac{dx_i}{dt} = \kappa_{x_i} f(x_{i-1}, x_i, x_{i+1}) - \gamma_{x_i} x_i$$

where

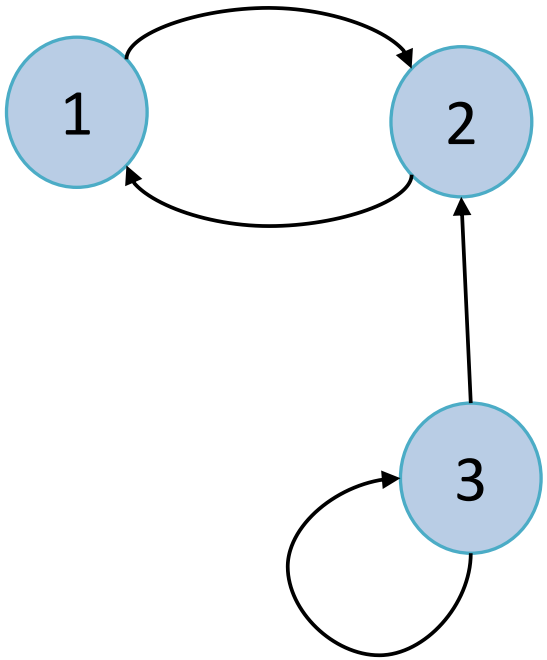
$$f(x_{i-1}, x_i, x_{i+1}) = s^-(x_{i-1})\left(1 - s^-(x_i)s^-(x_{i+1})\right) + s^+(x_{i-1})s^-(x_i)s^-(x_{i+1}),$$

s^+ and s^- are as before, and the constants are adjusted appropriately.

All of these equations are in the form of Glass networks, as used to model gene regulation!

3. Qualitative gene network modelling

Modeling gene regulation by Glass networks



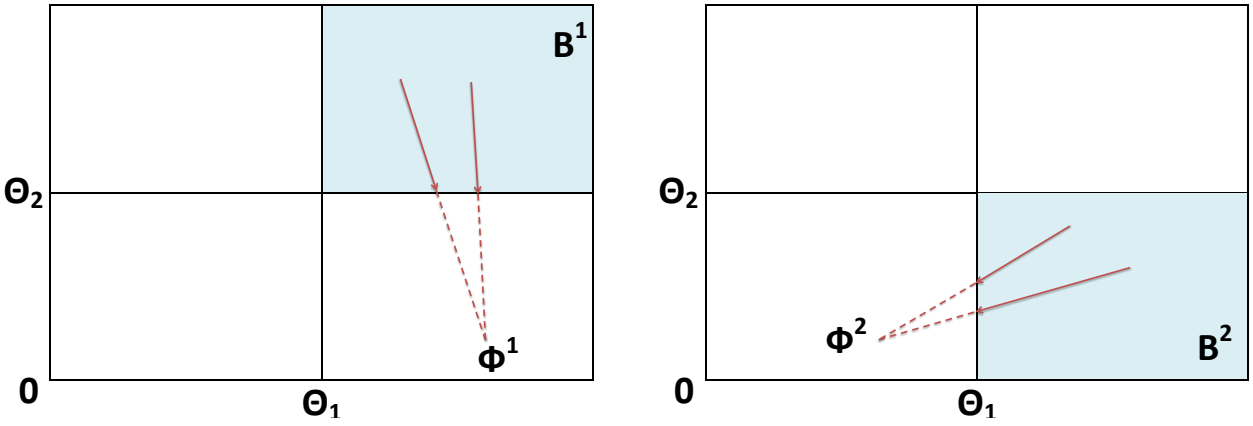
$$\dot{x}_1 = \kappa_1 s^+(x_2) - \gamma_1 x_1$$
$$\dot{x}_2 = \kappa_2 s^-(x_1) s^+(x_3) - \gamma_2 x_2$$
$$\dot{x}_3 = \kappa_3 s^-(x_3) - \gamma_3 x_3$$

Behaviour of the dynamical system

2-D example:

$$\dot{x}_1 = s^+(x_1)s^+(x_2) + s^-(x_1)s^-(x_2) - \gamma_1 x_1,$$
$$\dot{x}_2 = s^-(x_1) - \gamma_2 x_2$$

$$1/\gamma_1 > \theta_1, \quad 1/\gamma_2 > \theta_2$$

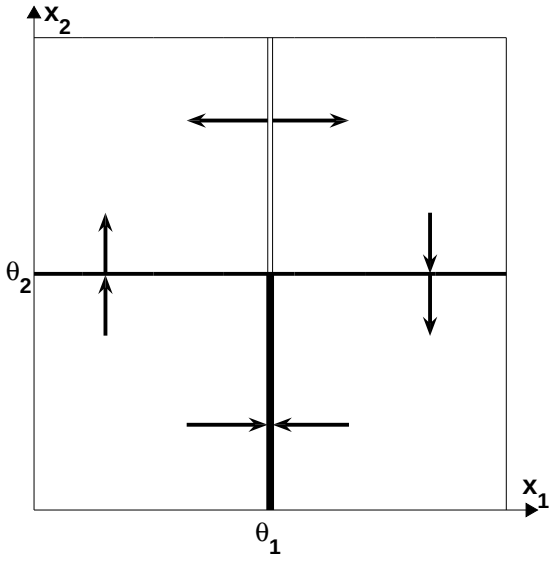


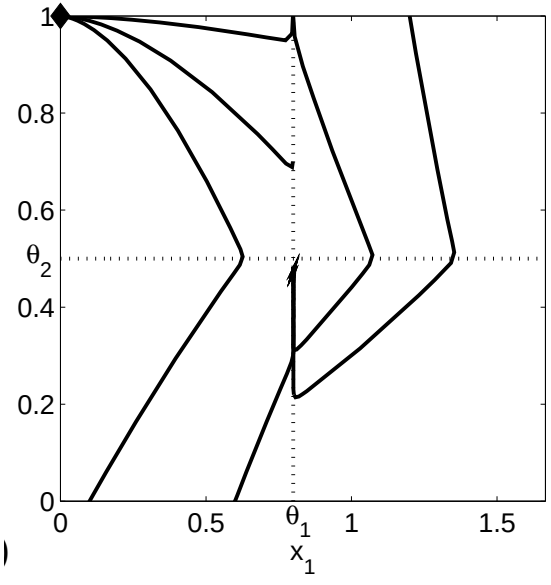
$$\dot{x}_i = \alpha_i - \gamma_i x, \quad x_i \in \mathrm{B}^{\mathrm{i}}, \quad so \quad x_i \to \frac{\alpha_i}{\gamma_i}$$

Behaviour of the dynamical system

2-D example:

$$\dot{x}_1 = s^+(x_1)s^+(x_2) + s^-(x_1)s^-(x_2) - \gamma_1 x_1,$$
$$\dot{x}_2 = s^-(x_1) - \gamma_2 x_2$$





What happens when $x_1 = \theta_1$?
What happens at $x_1 = \theta_1, x_2 = \theta_2$?

Use Filippov analysis or singular perturbation.

4. Rambus circuit - behaviour analysis

Steady states

n-dimensional model:

- all-off state (00000) is locally stable, but basin of attraction is only the all-off box
- all-on state (11111) is unstable in all directions (all units try to turn off)
- if n is even, alternating state (010101 or 101010) is stable.
- if n is odd, sequences of alternating units are locally stable but perturbations of the alternating pattern must exist, and propagate (e.g. 110101010 can't persist)

Similar for higher-dimensional versions of the model.

Perturbed alternating sequences

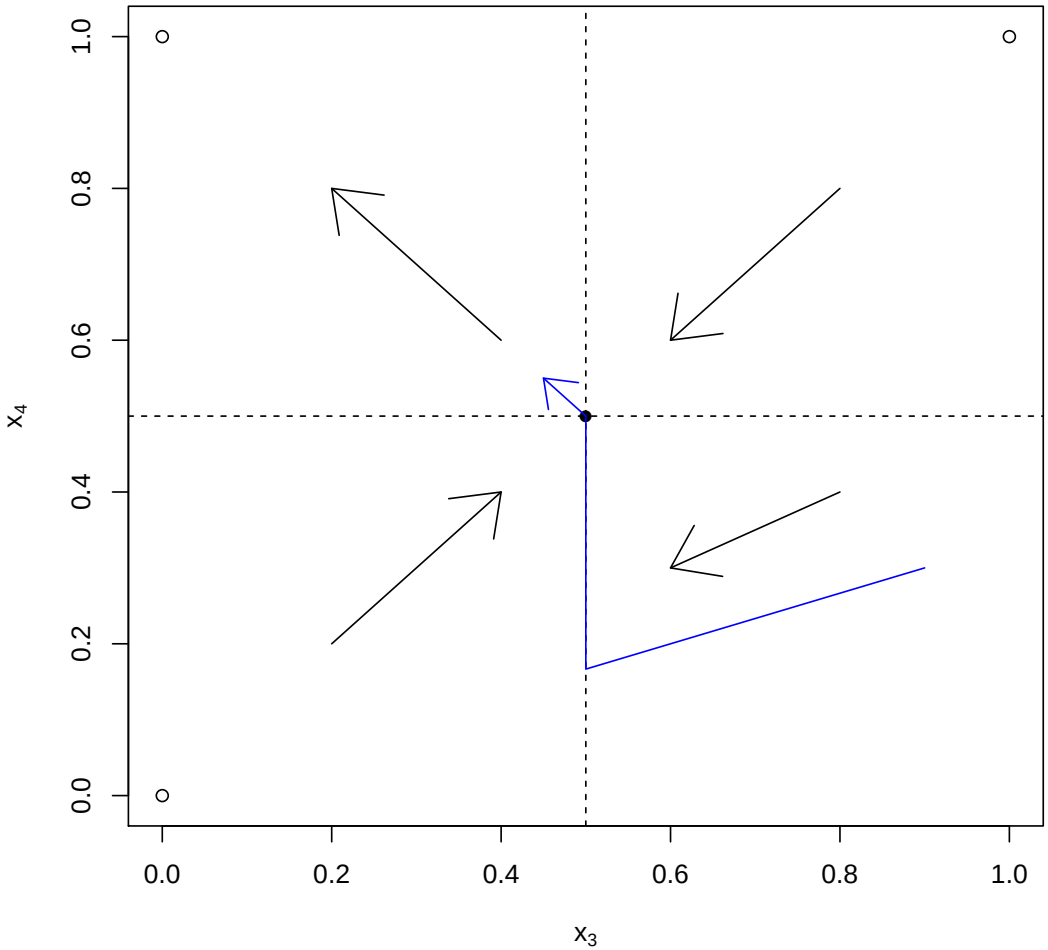
Still considering the n-dimensional model:

$$0110101010 \to 01\theta 010101 \to 01\theta\theta 10101 \to 0101110101$$

so 11 propagates to the right two units at a time.

Call the corresponding variables $x_1, x_2, x_3, x_4, \ldots$.

Sliding solution



Flow in the black wall is towards the focal point for the sliding motion: *i.e.*, the threshold intersection, if units are identical.

Singular perturbation analysis shows that flow from the threshold intersection is into the 01 box.

Singular perturbation analysis of threshold intersection

For identical unit parameters, WLOG take $\kappa_i = \gamma_i = 1$ and $\theta = 0.5$.

Approximate the step functions by sigmoids:

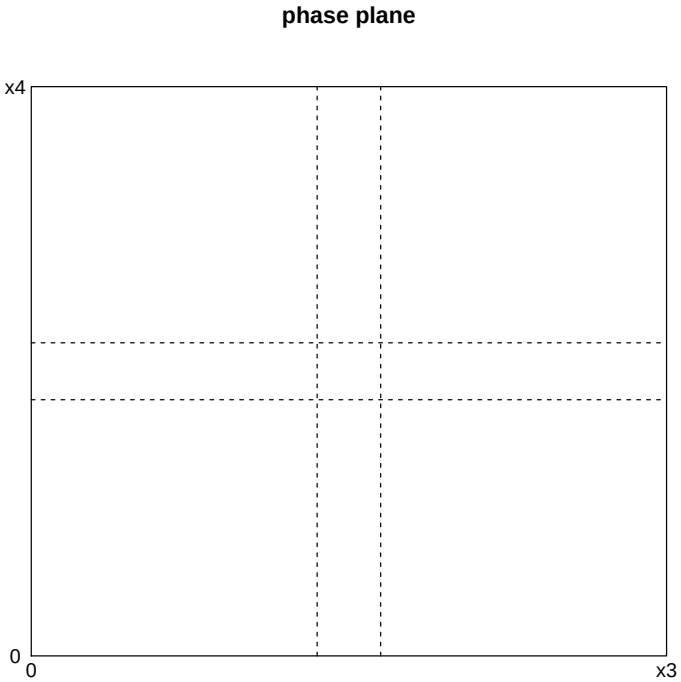
$$Z_i = H(x_i) = \frac{x_i^{1/q}}{\theta^{1/q} + x_i^{1/q}} \approx s^+(x_i), \qquad \lim_{q \to 0} H(x_i) = s^+(x_i)$$

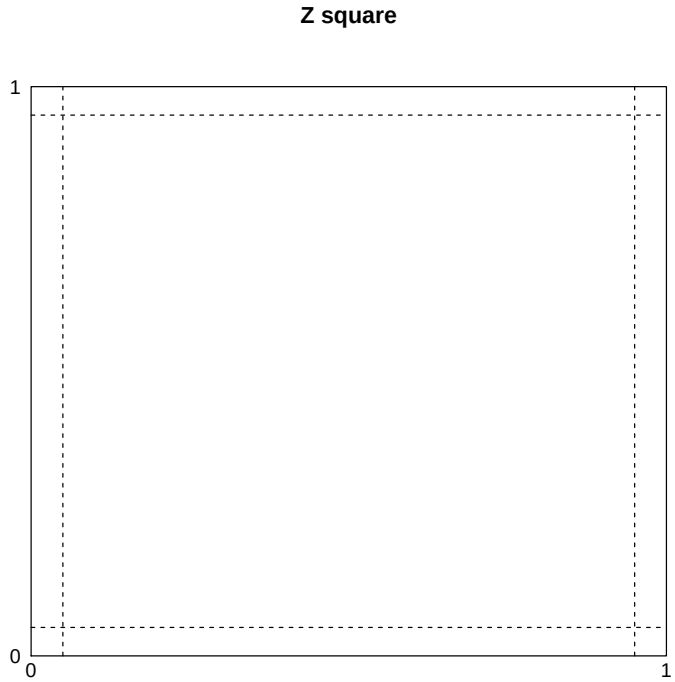
Blow up the threshold intersection by translating from x_3, x_4 to Z_3, Z_4 and $\tau = t/q$:

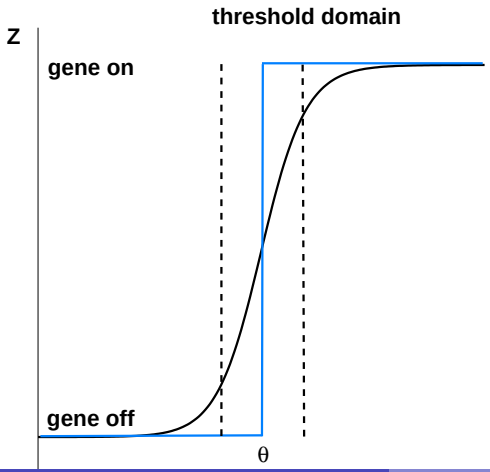
$$\begin{aligned} Z_3' &= \frac{Z_3(1 - Z_3)}{0.5} \left((1 - Z_3)(1 - Z_4) - 0.5 \right) \\ Z_4' &= \frac{Z_4(1 - Z_4)}{0.5} \left(1 - Z_3 - 0.5 \right) \end{aligned}$$

...and determine the flow of these 'boundary layer' equations.

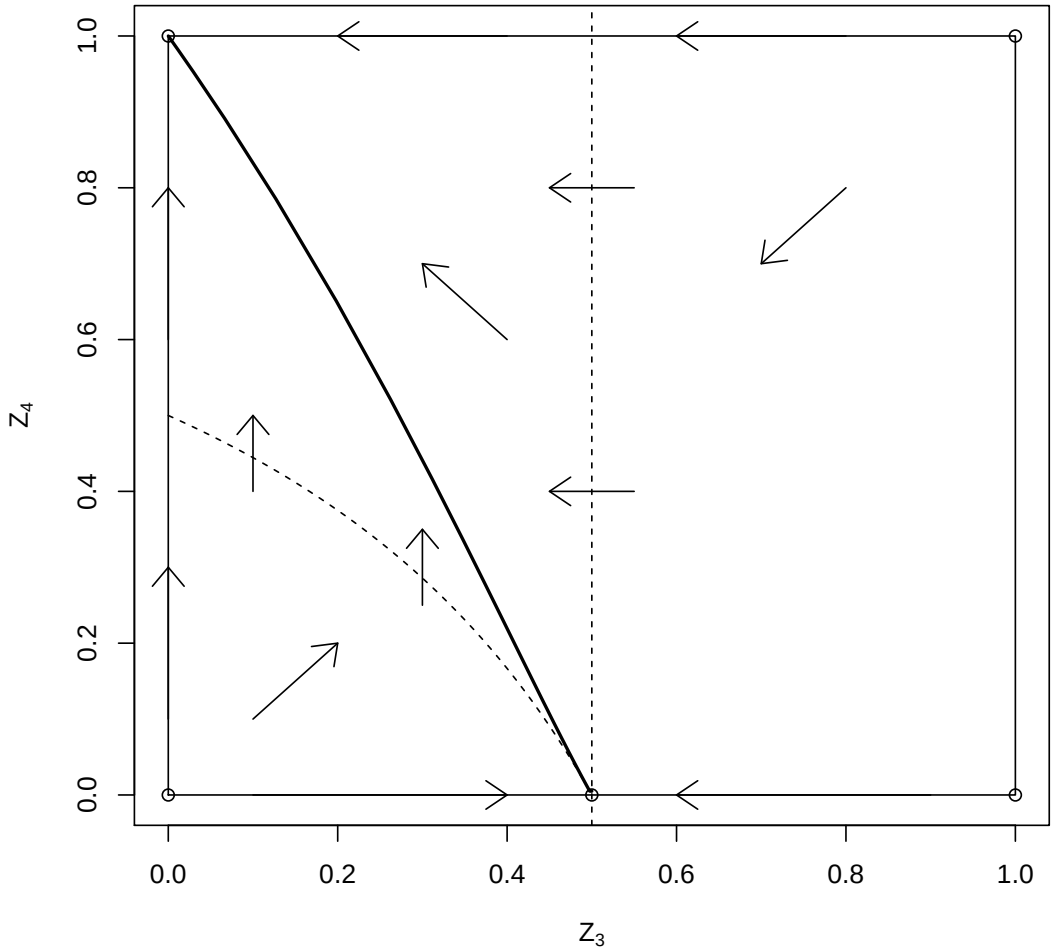
Singular perturbation analysis of threshold intersection





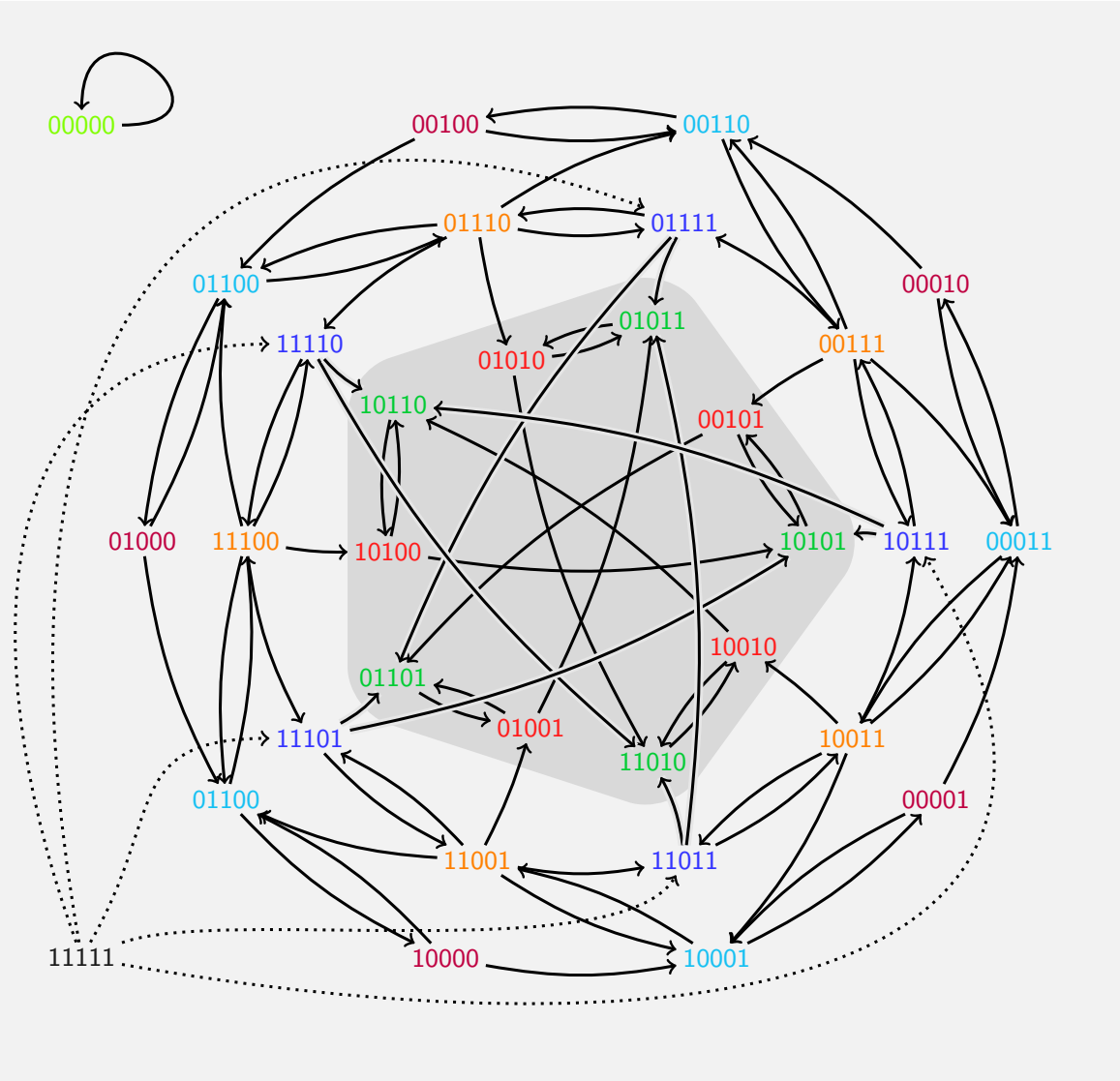


Singular perturbation analysis of threshold intersection



In the black wall, $x_4 < \theta \Leftrightarrow Z_4 = 0$ and $Z_3 = 0.5$ during sliding, so we start at $(Z_3, Z_4) = (0.5, 0)$, which has eigenvalues $\lambda_1 < 0, \lambda_2 = 0$. Once $Z_4 > 0$, all solutions go to $(0, 1)$, which corresponds to $x_3 < \theta$, $x_4 > \theta$.

State space diagram ($n = 5$)



The shaded region is attracting.

Global dynamics

However, it takes an infinite time for the sliding approach to the threshold intersection on the black wall (when units are identical).

Thus, globally, there is a heteroclinic cycle in which the double 1 propagates to the right around the ring twice.

When there are other variables oscillating (instead of sliding), as in the $3n$ or $4n$ models,

- the flow is able to pass the threshold intersections,
- but with irregular timing,
- and intermittent triggering of the next pair of units,
- so more than one pair of units can be transitioning at the same time.

This leads to very complex switching sequences, and (we conjecture) chaos.

Global dynamics

However, it takes an infinite time for the sliding approach to the threshold intersection on the black wall (when units are identical).

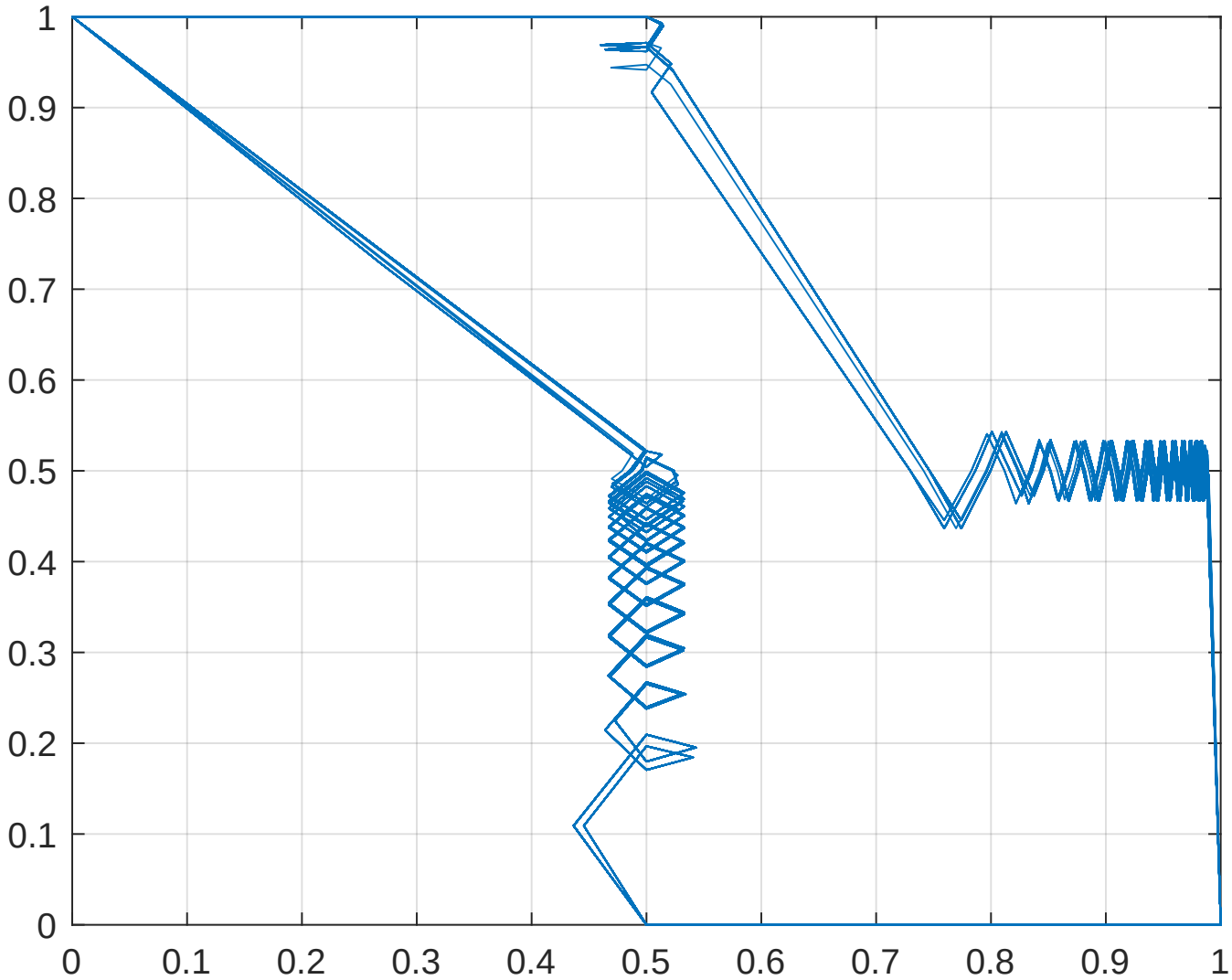
Thus, globally, there is a heteroclinic cycle in which the double 1 propagates to the right around the ring twice.

When there are other variables oscillating (instead of sliding), as in the $3n$ or $4n$ models,

- the flow is able to pass the threshold intersections,
- but with irregular timing,
- and intermittent triggering of the next pair of units,
- so more than one pair of units can be transitioning at the same time.

This leads to very complex switching sequences, and (we conjecture) chaos.

$2n$ model, fast OR gate - 2 unit transition

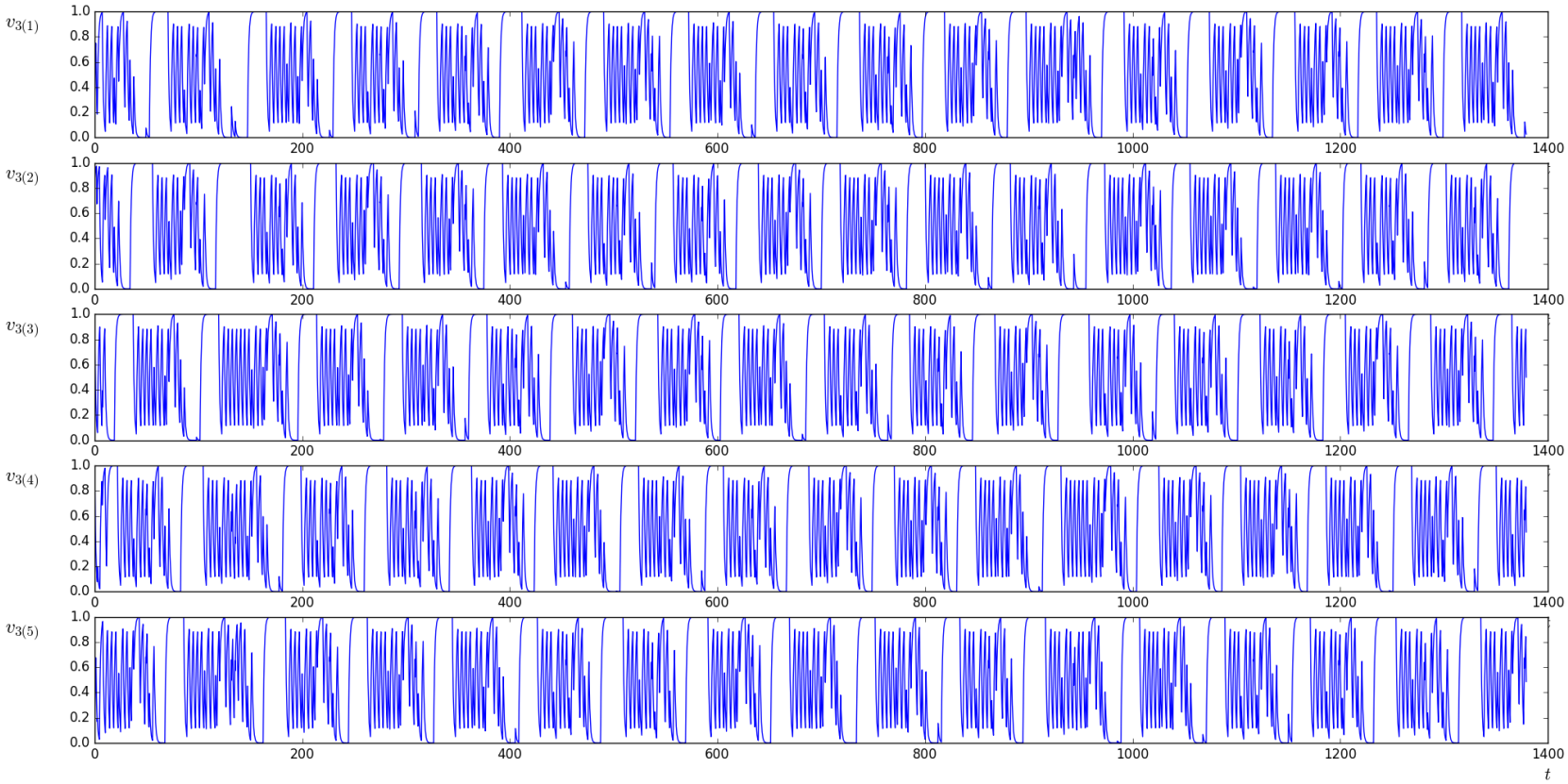


5. Rambus circuit - Numerical simulations

Numerics for the $3n$-dimensional model

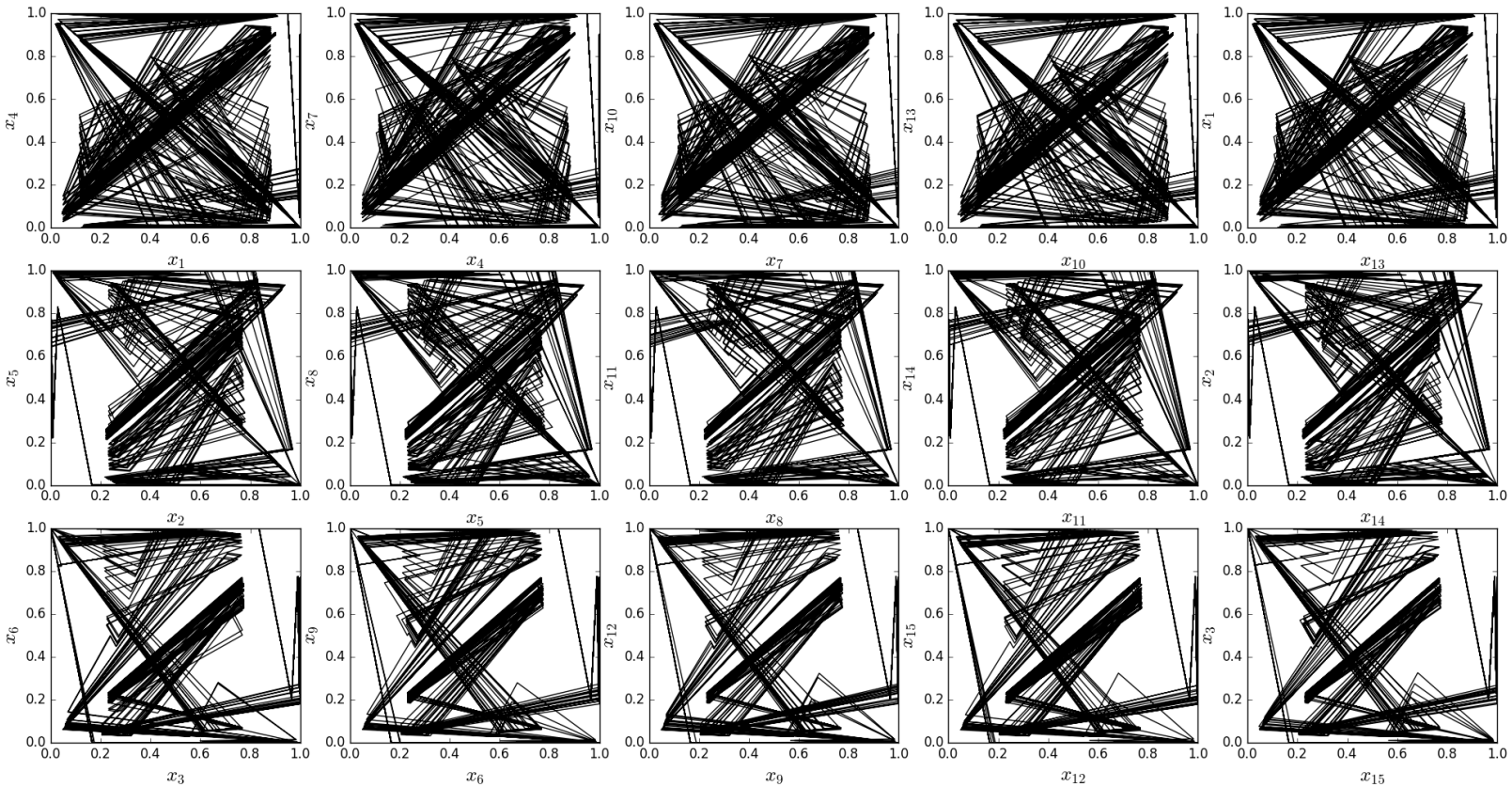
- We take $\kappa_{x_i} = \gamma_{x_i} = \mu$ and $\kappa_{y_1} = \kappa_{z_i} = \gamma_{y_i} = \gamma_{z_i} = \nu$.
- After rescaling time, the dynamics is controlled by a single parameter $\frac{\mu}{\nu}$ or its inverse.

Time series (x_i variables only)



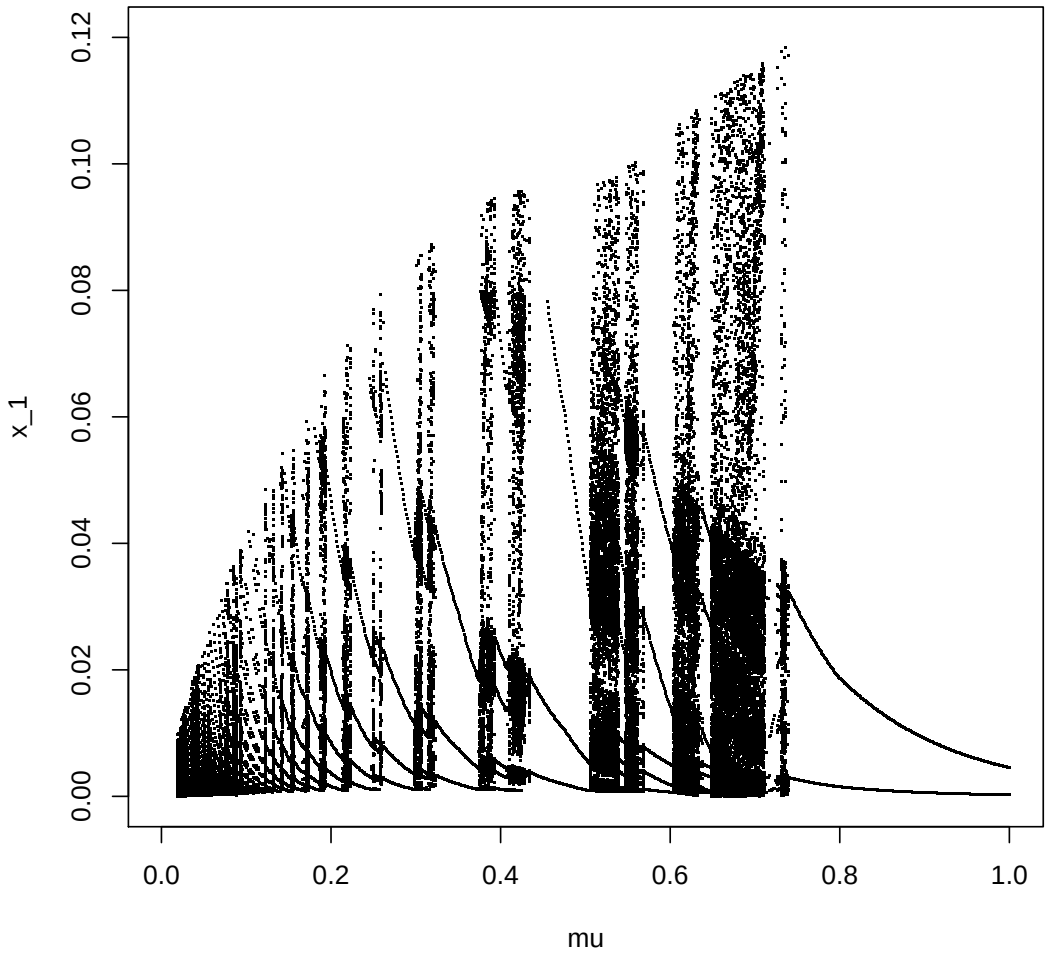
$n = 5$, $\mu = 1$, $\nu = 0.6$, random initial condition.

Phase space projections



$n = 5$, $\mu = 1$, $\nu = 0.6$, random initial condition.

Bifurcation diagram, varying μ

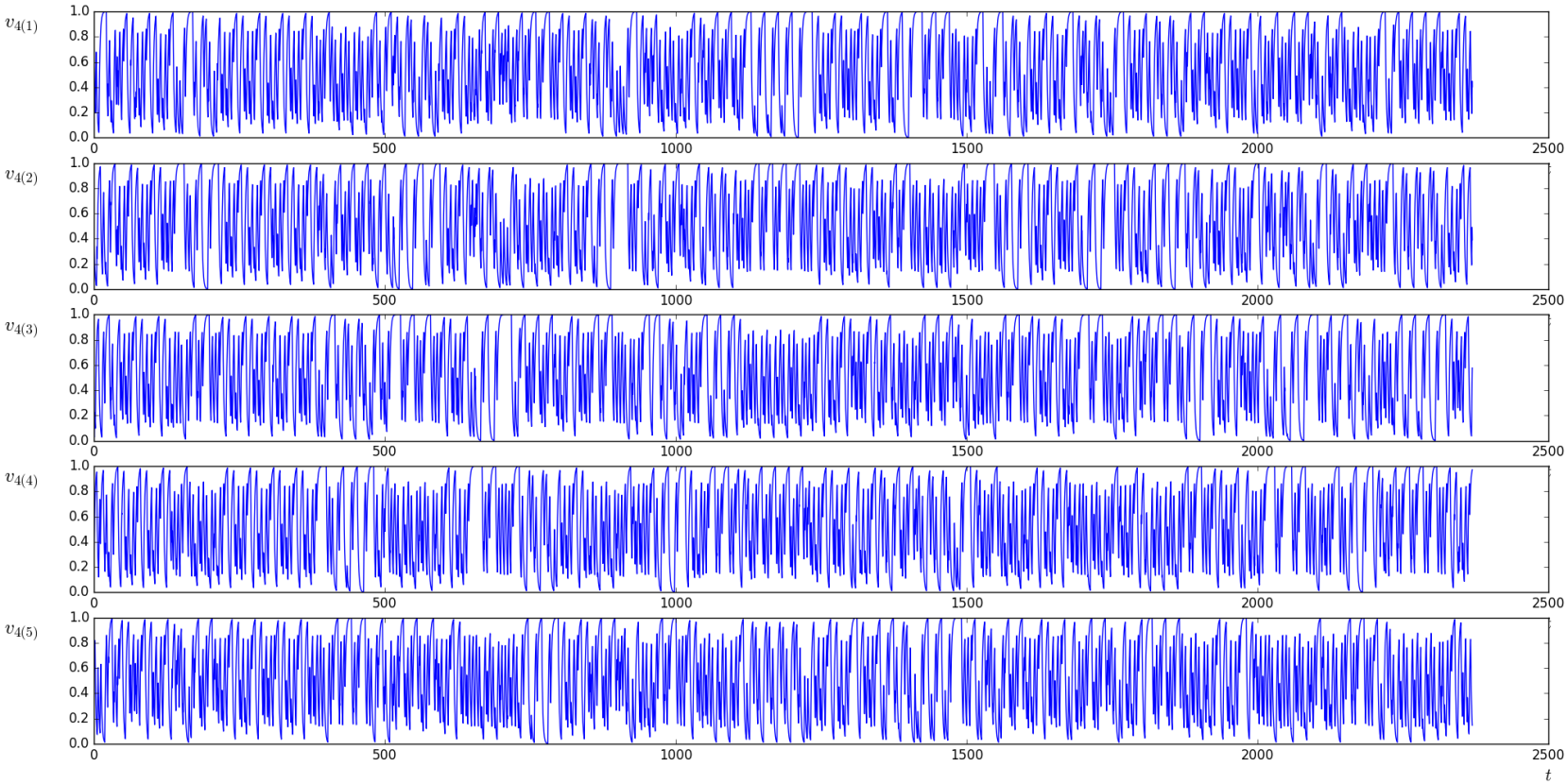


$n = 5$, $\nu = 1$. For each μ, 5000 successive values of $x_1 - \theta$ are plotted on a Poincaré section where $x_2 = \theta$: $(101, \theta 01, 101, 010, 101)$

Estimating Lyapunov exponents

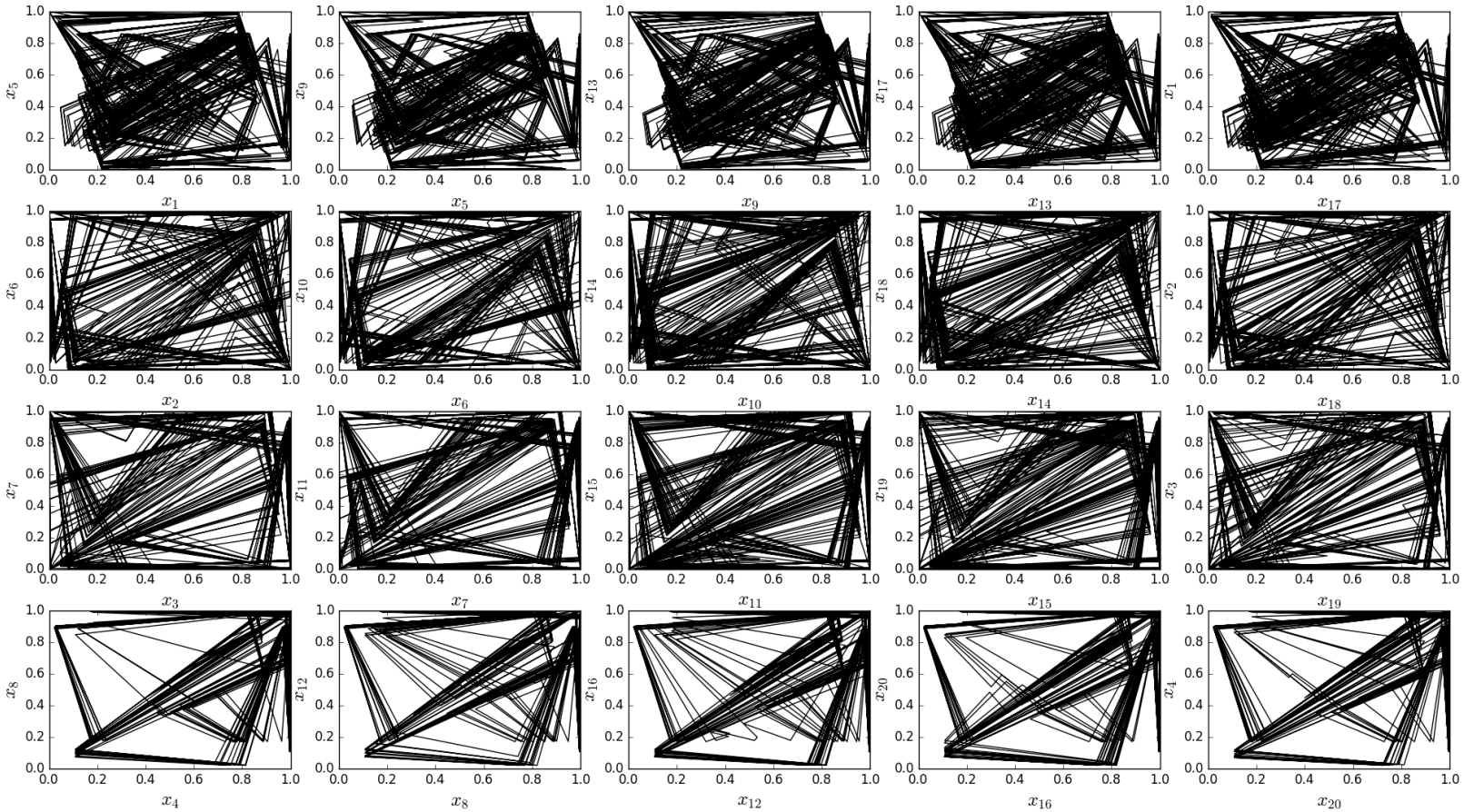
- Method: compute in parallel a numerical solution of both the original model, $\dot{v} = f(v)$, and its associated variational equation $\dot{Y} = Df(v(t))Y, \qquad Y(0) = \mathrm{Id}$
- Y is an $N \times N$ matrix and the Jacobian Df is evaluated along the solution to the ODE $\dot{v} = f(v)$
- The 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 achieve this, a QR decomposition of the approximate solution Y is performed at regular time intervals, amounting to an orthonormalization of the column space of Y.

Time series (x_i variables only) - $4n$-dimensional model



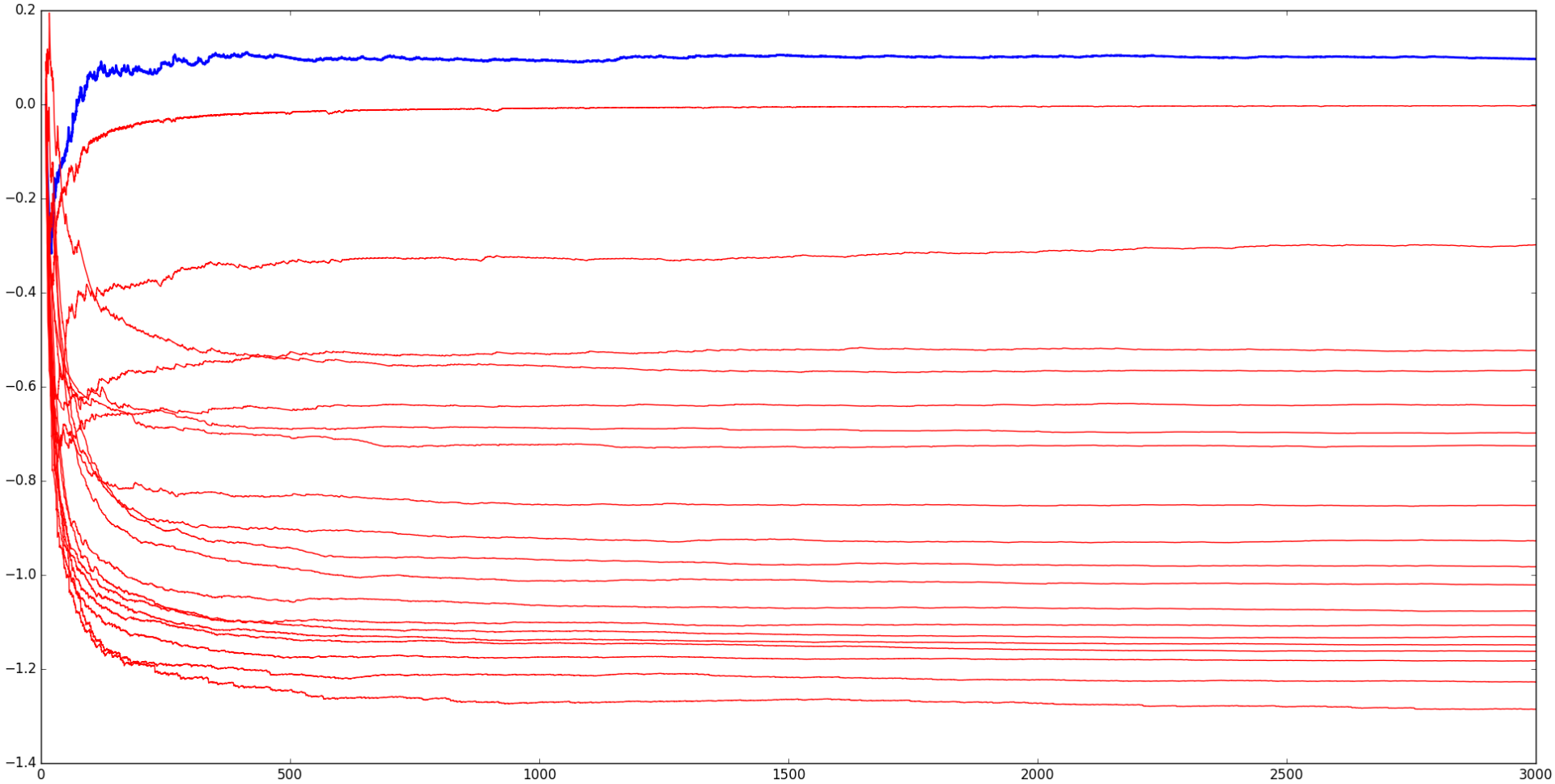
$n = 5$, $\mu = 0.6$, $\nu = 1$, $\lambda = 0.7$, random initial condition.

Phase space projections



$n = 5$, $\mu = 0.6$, $\nu = 1$, $\lambda = 0.7$, random initial condition.

Lyapunov exponents - $4n$ system (smooth version)



7. Conclusions

Conclusions

- There is convincing evidence that the Rambus circuit is intrinsically chaotic for intervals of parameter values and $n \geq 5$ odd, especially if we use the $4n$-dimensional model, but probably for the $3n$-dimensional model too.
- Rambus has applied for a patent, and is currently seeking certification.
- Robustness to hacking still needs to be demonstrated.
- Earlier work on the gene network models suggests that other chaotic designs are possible, not based on the ring-oscillator concept and, thus, even further from anything with a dominant intrinsic frequency.
- It is possible that such designs could either produce entropy at a higher rate, or be even more robust to hacking, or both.