True Random Source from Integratable Chaotic Circuits

Ned Corron

Marko Milosavljevic, Jon Blakely

U.S. Army RDECOM

Aviation and Missile Research, Development and Engineering Center (AMRDEC)

Charles M. Bowden Laboratory

Redstone Arsenal, Alabama, USA

Physical Random Number Generation

- **Large Quantities of Random Numbers**
  - Monte Carlo simulation
  - encryption
- **Pseudo-Random Is Not Good Enough**
  - potential weakness
  - obscurity relies on computational hardness
- **Physical Random Sources**
  - human interaction (stochastic seed)
  - quantum effects (stochastic process)
  - classical mechanics (chaotic process)

Pseudo-Random Numbers:

$$\mathbf{x}_n = F\left(\mathbf{x}_n \mid \lambda\right)$$

$$s_n = P\left(\mathbf{x}_n\right)$$

where

s_n – pseudo-random sample

$\mathbf{x}_n$ – internal state

λ – seed

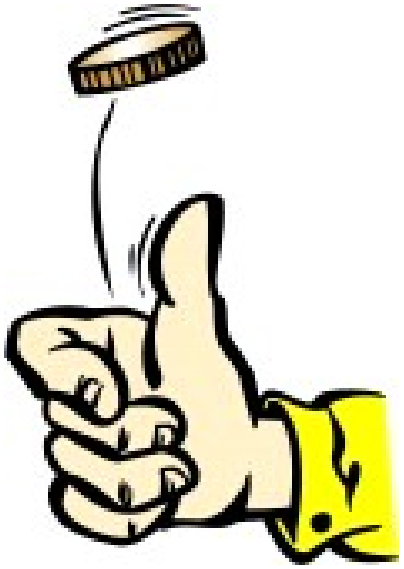
Successive samples are necessarily related

Random Bits for Encryption

- **Ideal Random Process**

$$P(\mathrm{H}) = P(\mathrm{T}) = 1/2$$

H T T H T H H T T T T H T T…



- **Bits**

$$\mathrm{H} \rightarrow 0 \quad \mathrm{T} \rightarrow 1$$

0 1 1 0 1 0 0 1 1 1 1 0 1 1…

Process to generate random bits must be independent and fair.
Otherwise, tendencies can be exploited.

Bias

- **Unfair Coin** $p \neq 1/2$

$$P(\mathrm{H}) = p$$
$$P(\mathrm{T}) = 1-p$$

$$P(\mathrm{HH}) = p^2$$
$$P(\mathrm{HT}) = p(1-p)$$
$$P(\mathrm{TH}) = p(1-p)$$
$$P(\mathrm{TT}) = (1-p)^2$$

von Neumann Bias Corrector:

$$HT \to 0$$
$$TH \to 1$$
$$(HH, TT \to \text{n.s.})$$

… HT TT TT HT TT TH HT TT HH TT TH TT …

… 0 0 1 0 1 …

Correlation

- **Conditional Probability**

$$P\left(\text{next toss}\middle|\text{prior tosses}\right)$$

- **Independent (uncorrelated)**

$$P\left(\text{H}\middle|\text{any sequence}\right)=P\left(\text{H}\right)$$

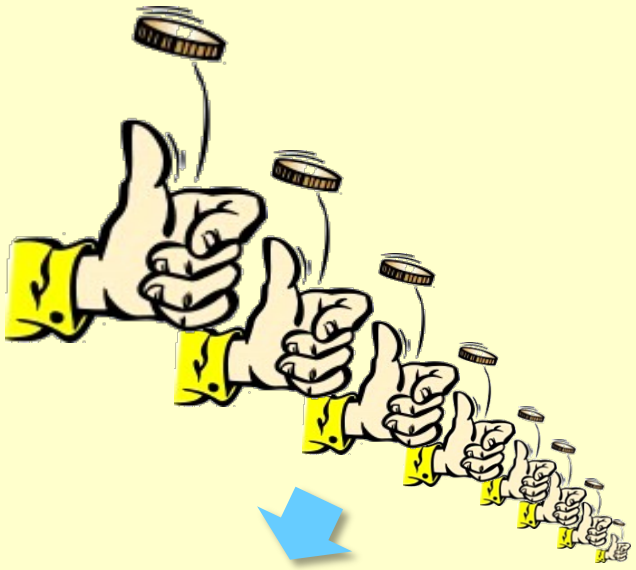
$$P\left(\text{T}\middle|\text{any sequence}\right)=P\left(\text{T}\right)$$

- **Dependent (correlated)**

$$P\left(\text{H}\middle|\ldots\text{H}\ldots\right)\neq P\left(\text{H}\middle|\ldots\text{T}\ldots\right)$$

$$P\left(\text{T}\middle|\ldots\text{H}\ldots\right)\neq P\left(\text{T}\middle|\ldots\text{T}\ldots\right)$$

Random Bit Stream:



H T T H T H H T T …

Lazy sequential tosses could be correlated…

Classical Sources of Randomness

- **Classical Mechanics**
  - motion determined by physical laws and initial conditions

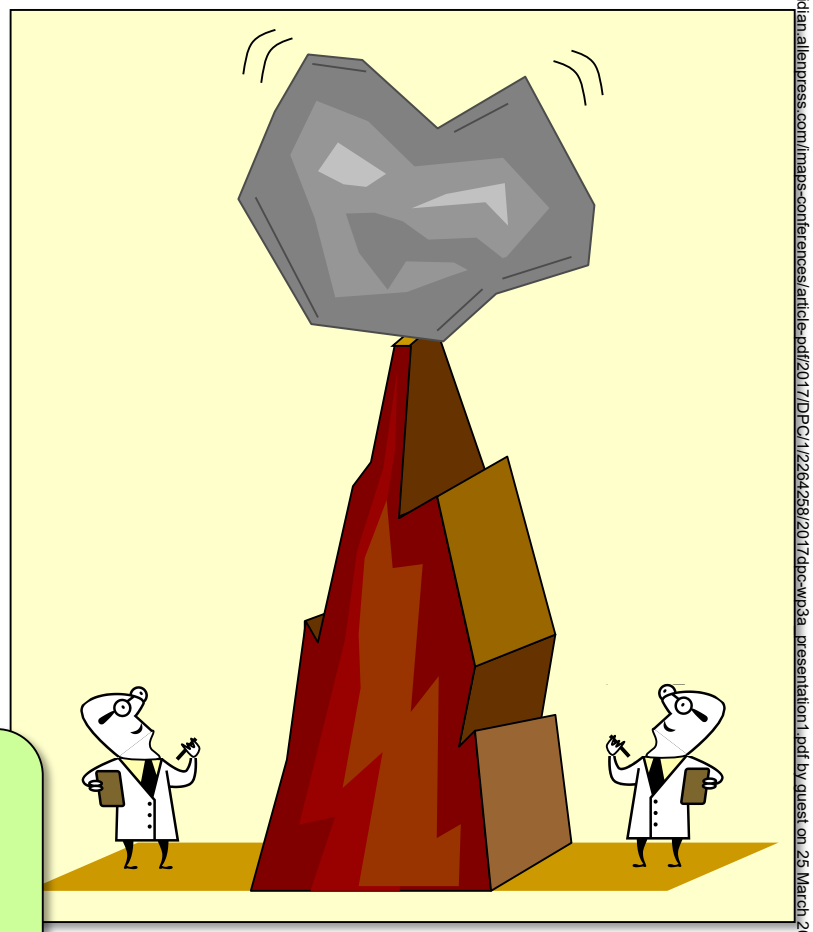
$$F = ma$$

- **Laplace's Demon**
  - if position and velocity of every particle in the universe is precisely known…

Can classical mechanics generate truly random bits?

Determinism and Information

- **No new information comes from deterministic dynamics…**
  - initial conditions
  - system equations
- **… unless your knowledge is incomplete**
  - finite precision
  - model errors
  - unmodeled effects (noise)

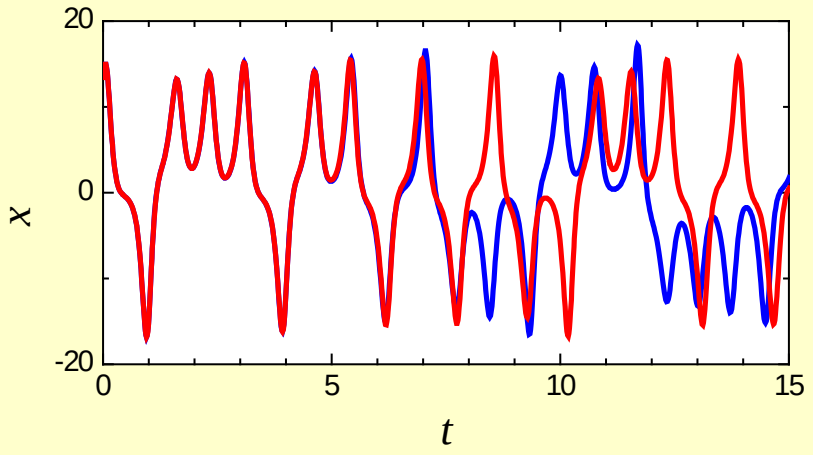


Instability can be an information source when observed with limited precision

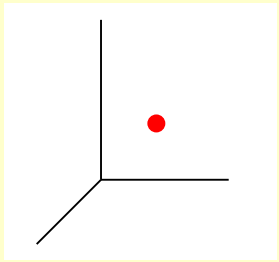
Chaos

- **Dynamic State**
  - aperiodic, bounded oscillations
  - extreme sensitivity to initial conditions
  - deterministic, yet unpredictable
  - continuously unstable

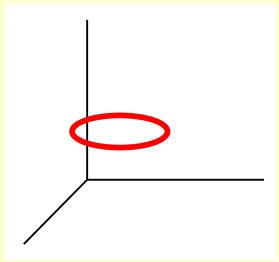
Sensitivity to Initial Conditions



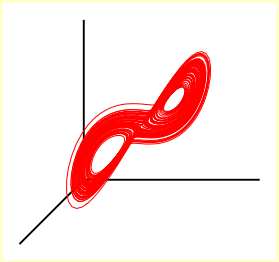
Attractor Hierarchy



equilibrium
(steady state)



limit cycle
(periodic)



strange attractor
(chaos)

Chaos as Information Source

- **Given a chaotic flow**
  - deterministic dynamics

$$\frac{dx}{dt} = f(x)$$

- **Measure state with finite precision**
  - information beyond measurement precision is unknown

$$x(t) \doteq 3.197\_\_\_\_\cdots$$

- **Future state can be predicted**
  - precision lost due to sensitivity to initial conditions

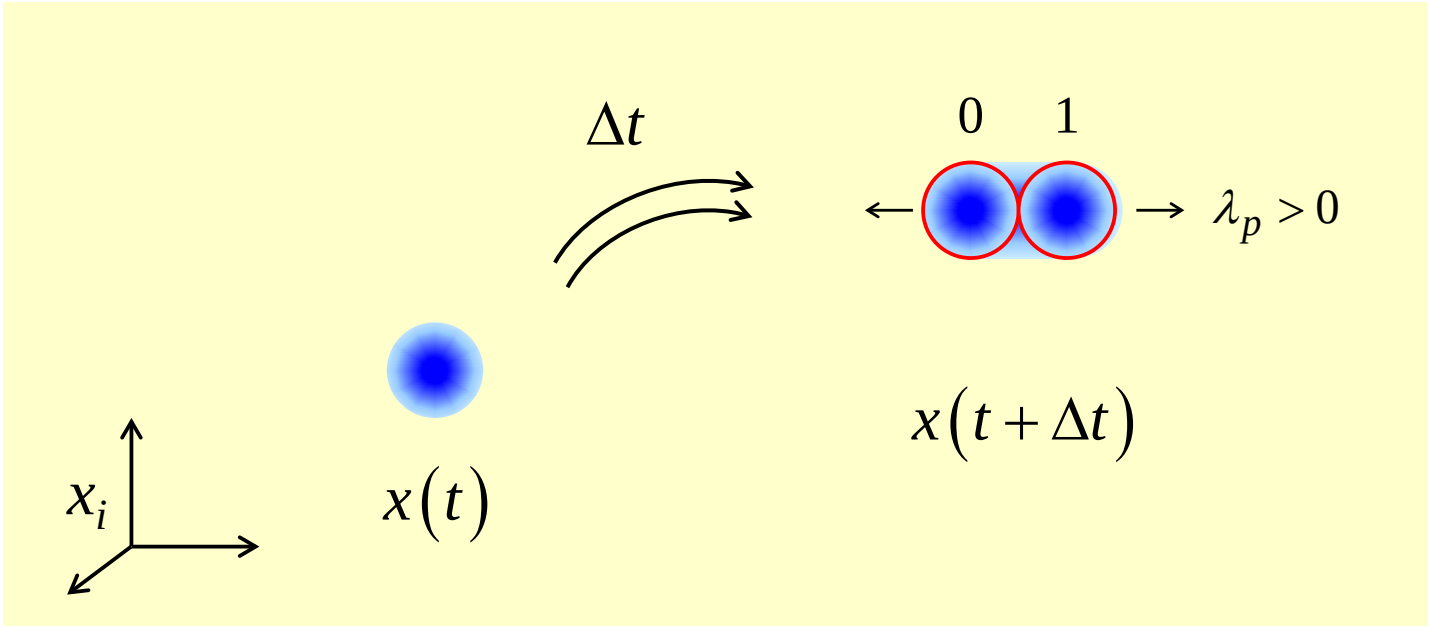
$$x(t+\Delta t) \doteq 1.78?$$

- **Re-measuring state reveals new information**
  - new information derived from previously unresolved digits

$$x(t+\Delta t) \doteq 1.784$$

new information

Entropy Rate in Chaos

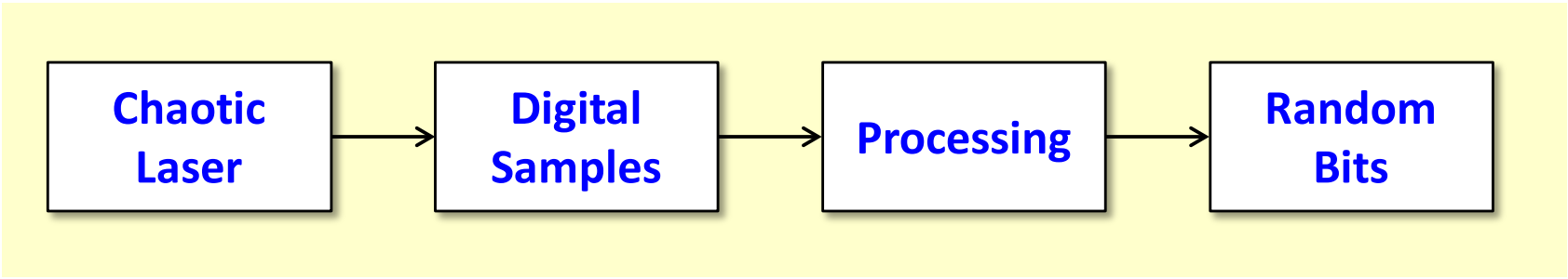


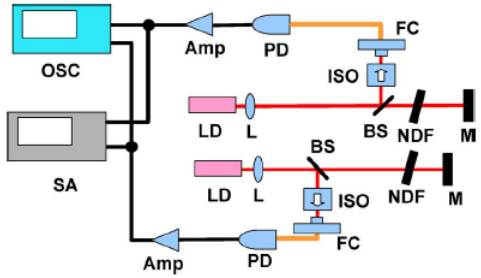
$$\Delta t = \frac{\ln 2}{\lambda_p} \quad \Rightarrow \quad H = \frac{1 \text{ bit}}{\Delta t} = \frac{\lambda_p}{\ln 2}$$

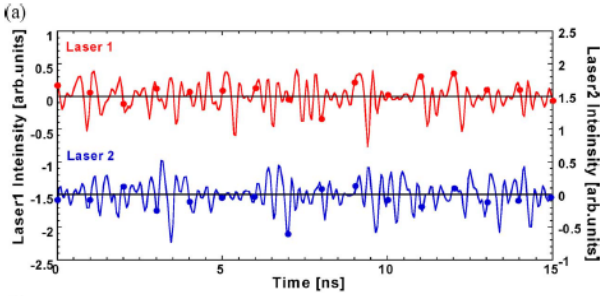
entropy rate

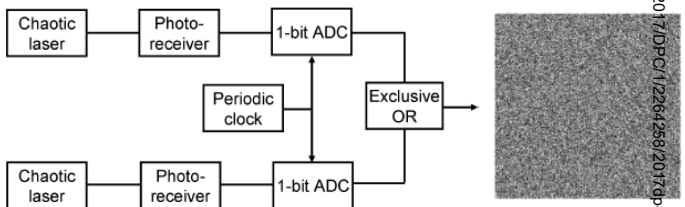
Theoretical Speed Limit for Physical Random Bits

Fast Physical Random Number Generation Using Laser Chaos





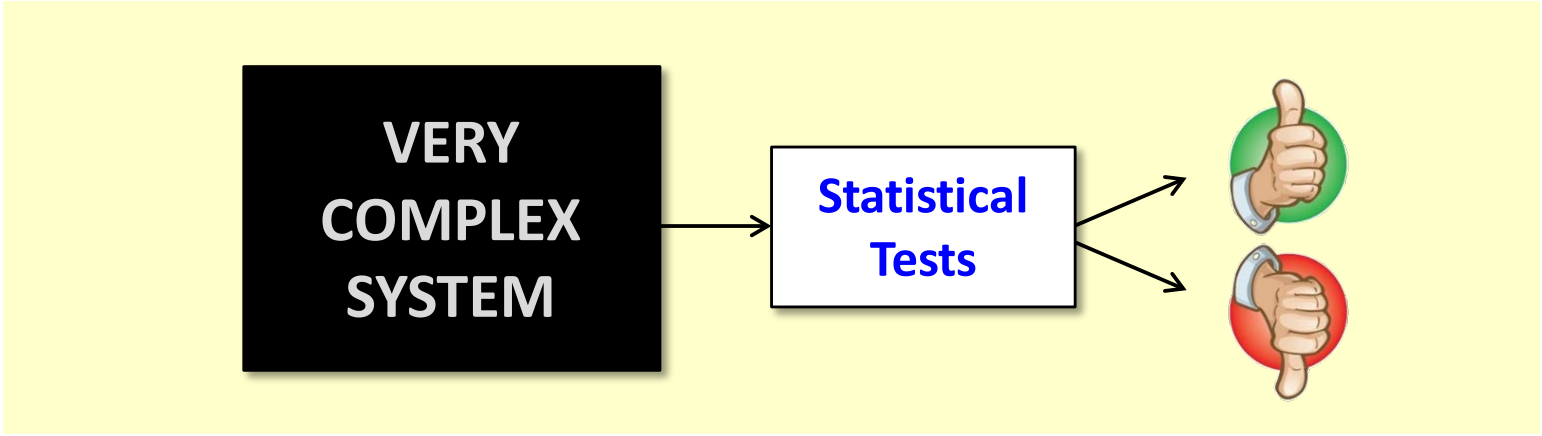




- Uchida et al., *Nature Photonics* (2008), 1.7 Gb/s
- Reidler et al., *Phys. Rev. Lett.* (2009), 12.5 Gb/s
- Argyris et al., *Optics Express* (2010), 140 Gb/s
- Uchida et al., *IEEE Photonics Tech. Lett.* (2012), 400 Gb/s
- Oliver et al., *Optics Lett.* (2013), 480 Gb/s
- Li et al., *Dynamics Days US*, *SPIE* (2014), >1 Tb/s

All passing NIST statistical tests

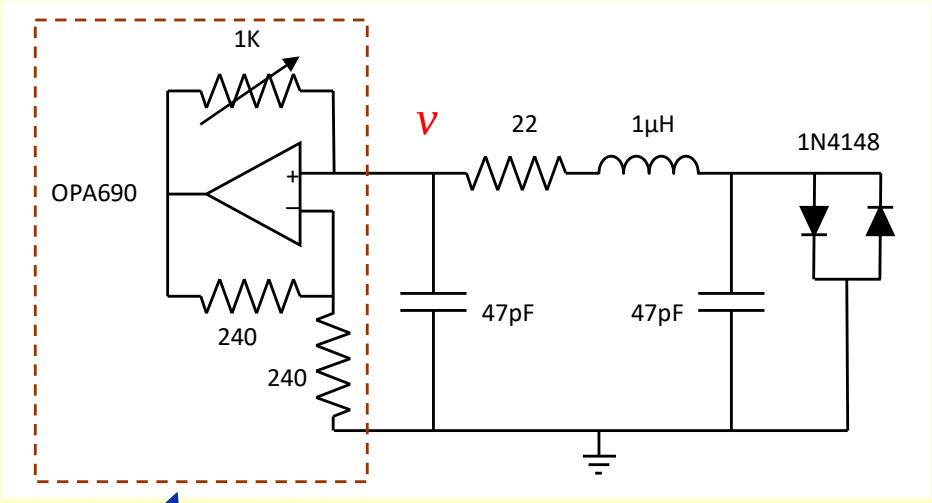
Statistical Testing

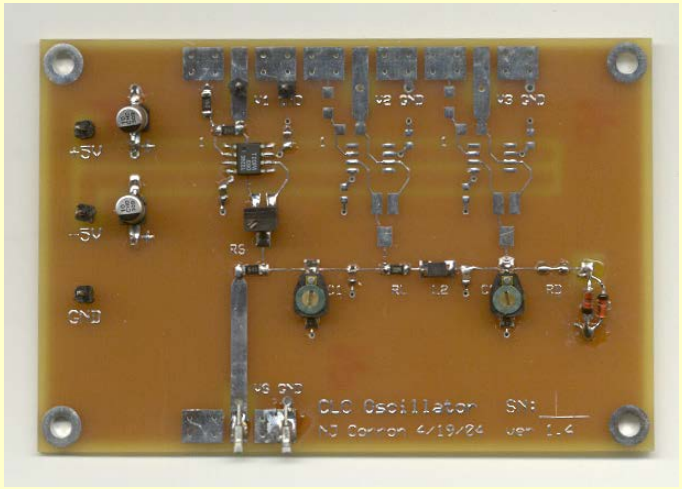


- **Pseudorandom Number Generators**
  - have correlations, yet pass statistical tests
- **Complex Physical System**
  - may also have correlations, yet pass statistical tests

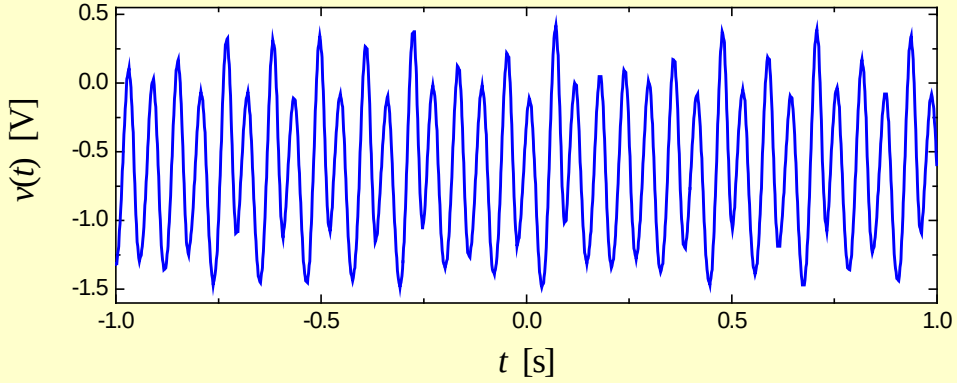
True Random Generators Must be Based on First-Principle Physics

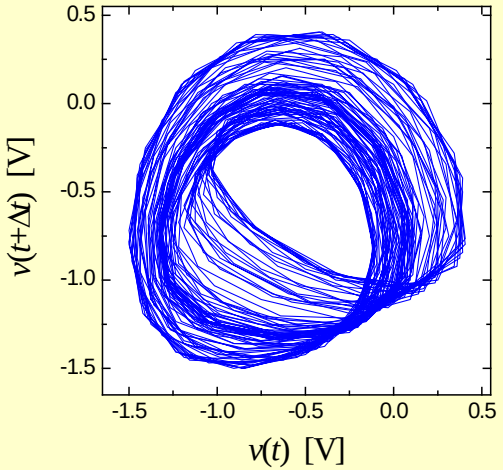
20-MHz Chaotic Oscillator





~20 MHz chaos

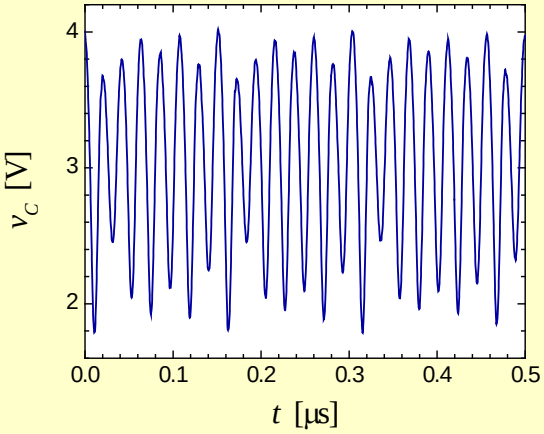


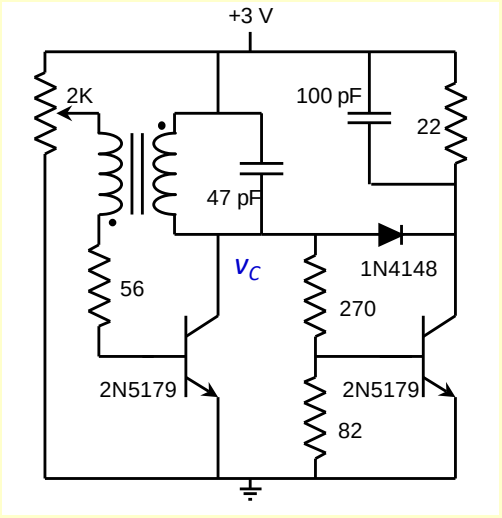


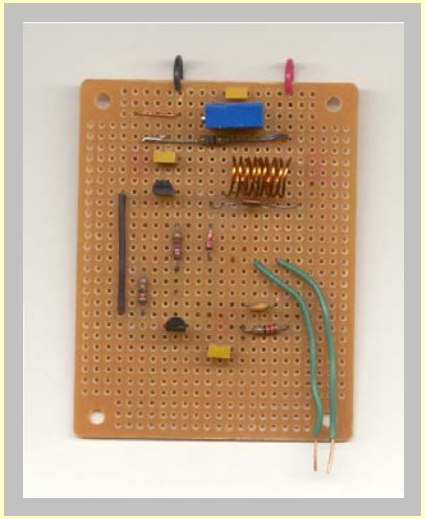
- N. J. Corron, J. N. Blakely, and S. D. Pethel, "Lag and Anticipating Synchronization without Time-Delay Coupling," *Chaos* 15, 023110 (2005)

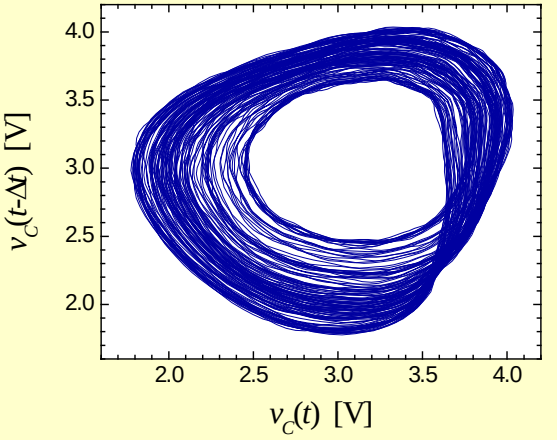
50-MHz Chaotic Transistor Oscillator

- **Two-Transistor RF Oscillator**
  - Modified tuned-collector LC oscillator
  - Exhibits chaotic dynamics
    - nearly sinusoidal waveform
    - peak-to-peak amplitude variations



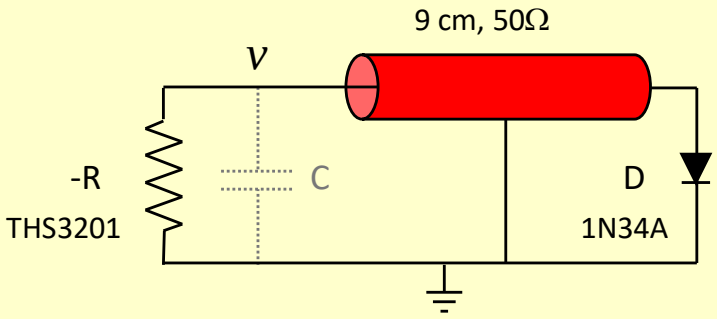


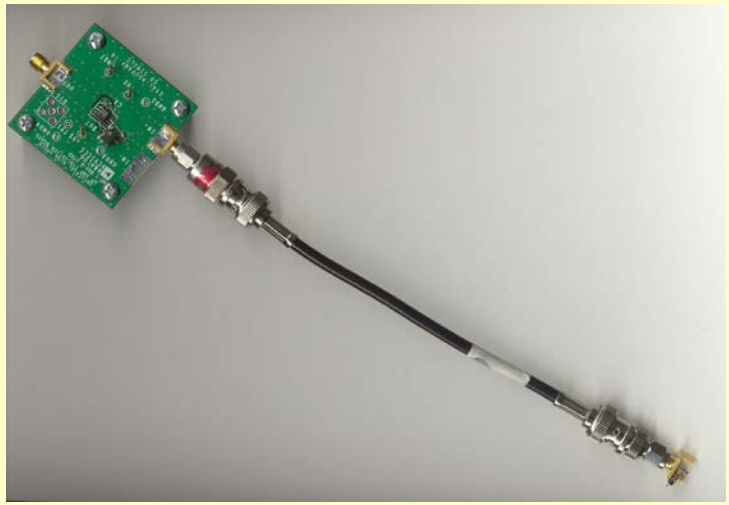


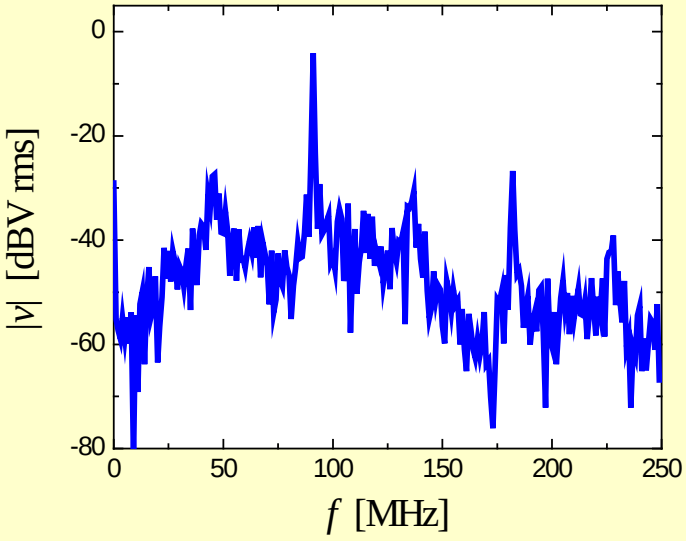


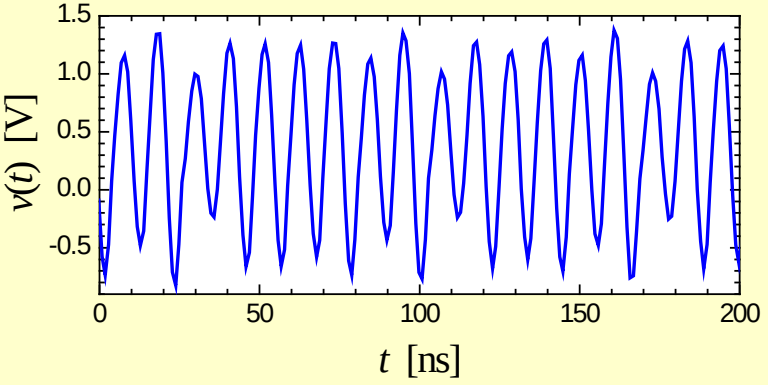
– N. J. Corron, B. A. Hopper, and S. D. Pethel, "Limiter Control of a Chaotic RF Transistor Oscillator," *International Journal of Bifurcation and Chaos* 13, 957 (2003)

90-MHz Chaotic TX-Line Oscillator





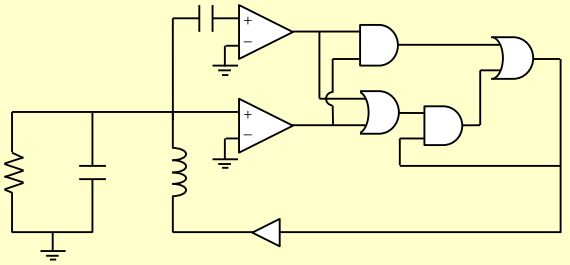




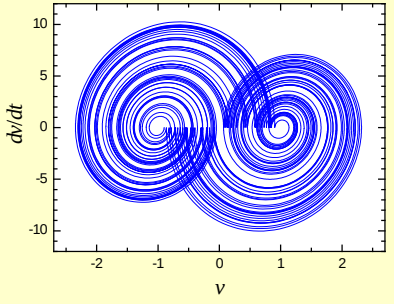
– J. N. Blakely and N. J. Corron, "Experimental Observation of Delay-Induced RF Chaos in a Transmission Line Oscillator," *Chaos* 14, 1035 (2004)

Exactly Solvable Chaos

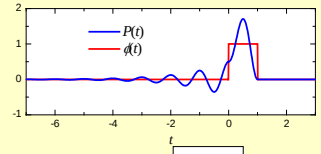
- **Analytically Solvable Nonlinear Systems**
  - piecewise linear dynamics
  - discrete switching events
  - straightforward hybrid circuit realization (analog and digital components)
- **First-Principle Understanding**
  - provably chaotic
  - exact return map
  - generating partition
  - complete symbolic representation
- **Tunable Parameters**
  - Markov partition
  - IID events (possibly biased)

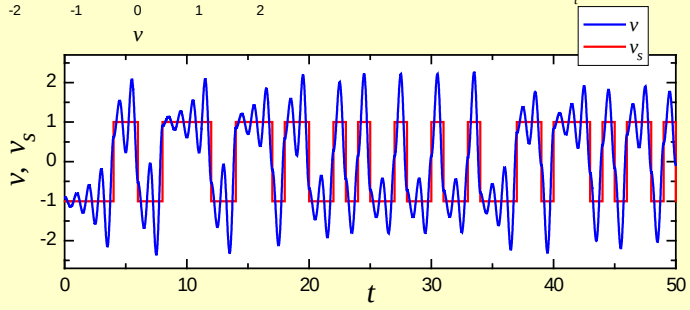


$$\frac{d^2v}{dt^2} - 2\beta\frac{dv}{dt} + \left(\omega^2 + \beta^2\right)\cdot\left(v - v_s\right) = 0$$



$$\frac{dv}{dt} = 0 \quad \Rightarrow \quad v_s = \mathrm{sgn}\left(v\right)$$



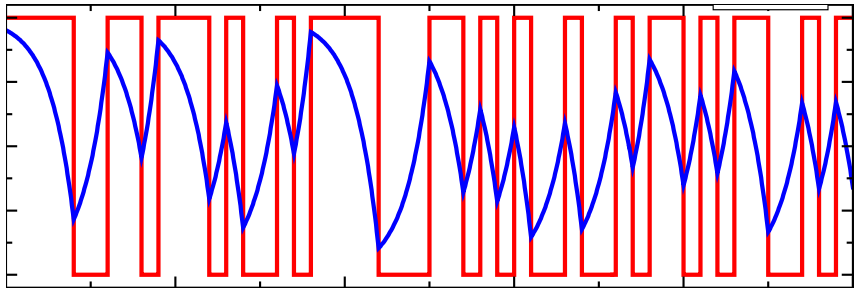


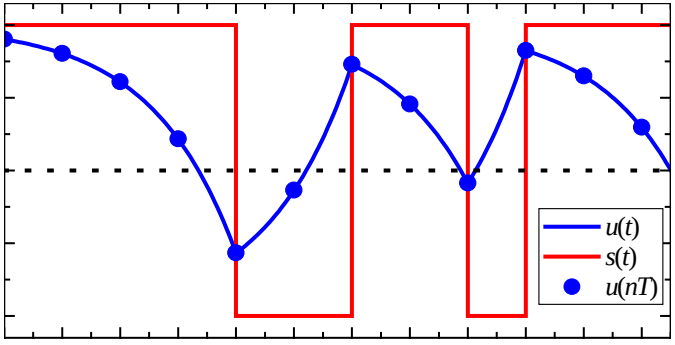
Exactly Solvable First-Order Chaos

- **Dynamical System**

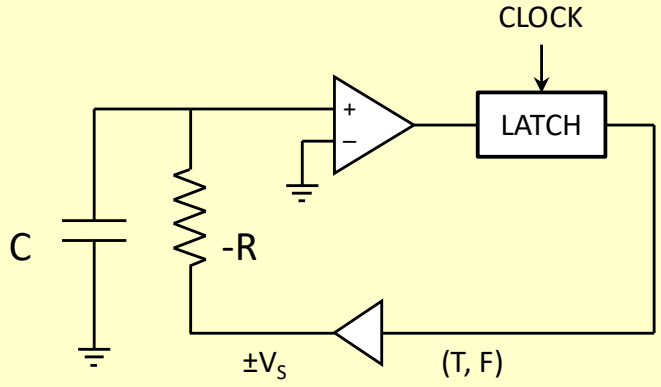
$$\frac{du}{dt} = u - s$$

$$s(nT) = \begin{cases} +1, & u(nT) > 0 \\ -1, & u(nT) \le 0 \end{cases}$$

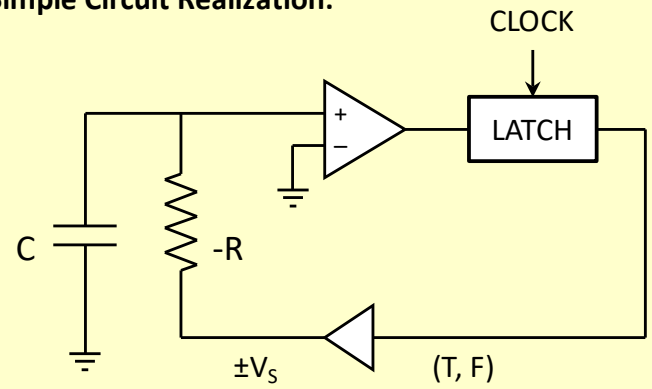


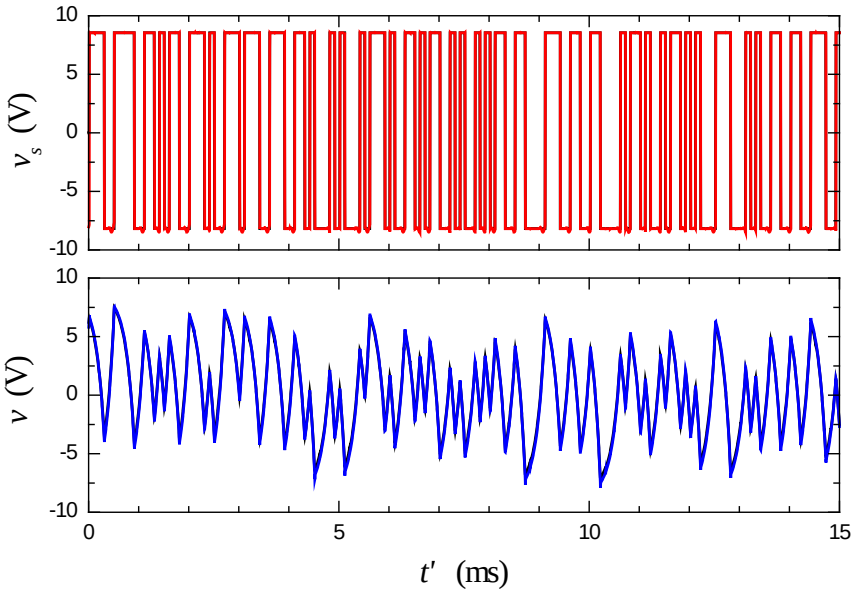


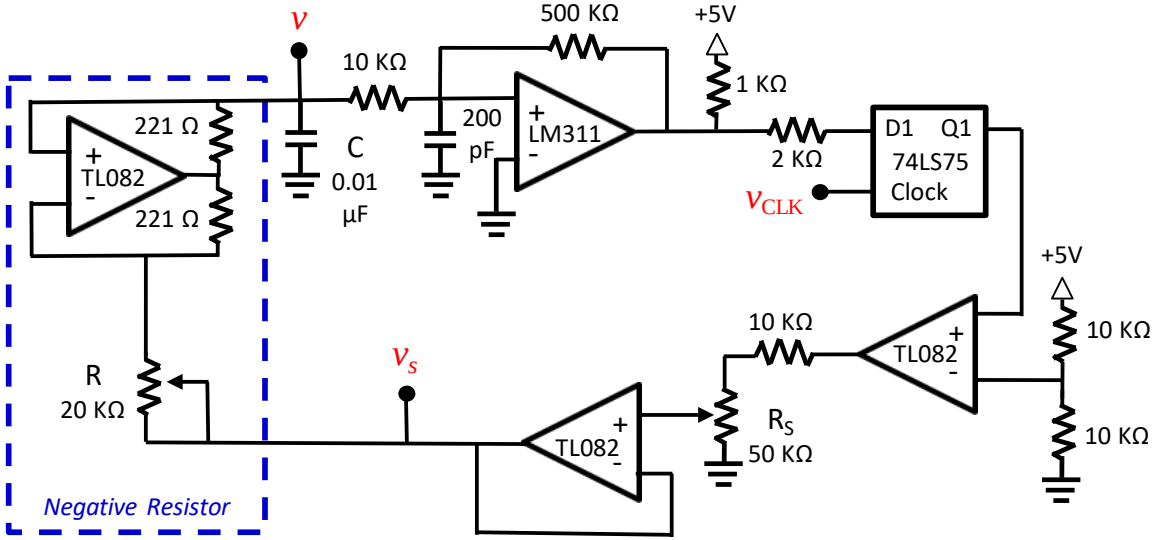
Simple Circuit Realization:

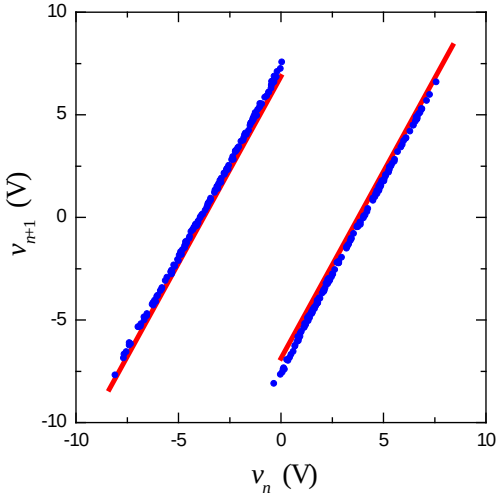


Simple Circuit Realization:









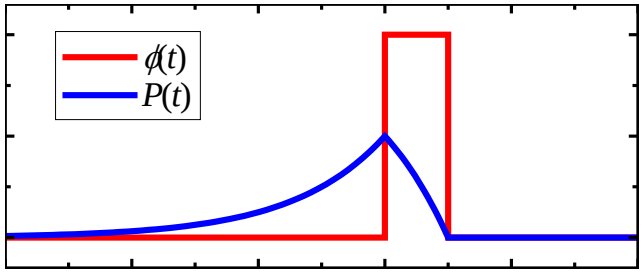
- **Analytic Solution**

$$s(t) = \sum_{n=-\infty}^{\infty} s_n \cdot \phi(t - nT)$$

$$u(t) = \sum_{n=-\infty}^{\infty} s_n \cdot P(t - nT)$$

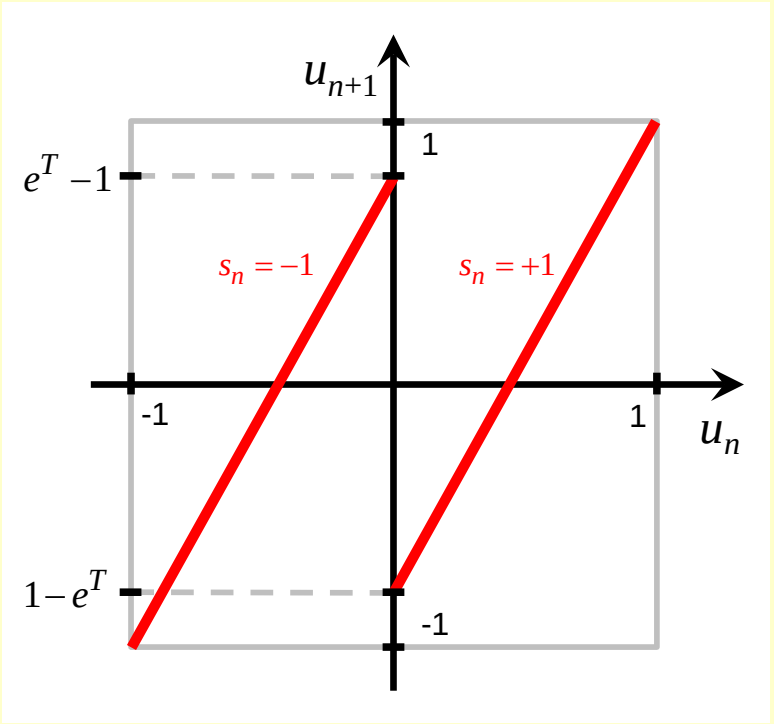
$$\phi(t) = \begin{cases} 1, & 0 \le t < T \\ 0, & \text{otherwise} \end{cases}$$

$$P(t) = \begin{cases} \left(1 - e^{-T}\right) e^{t}, & t < 0 \\ 1 - e^{(t-T)}, & 0 \le t < T \\ 0, & T \le t \end{cases}$$



Return Map:

$$u_{n+1} = s_n + e^{T}\left(u_n - s_n\right)$$



$$t_n = nT$$

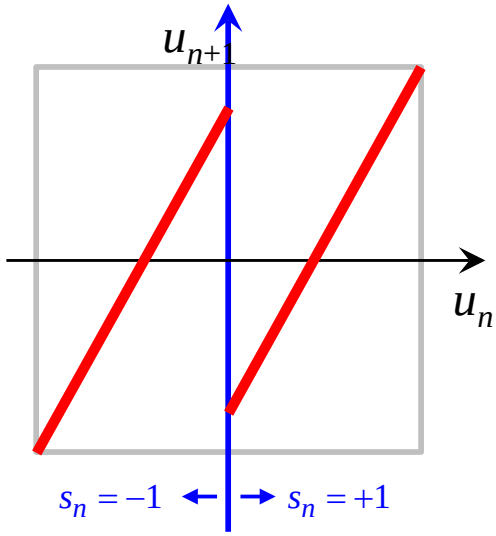
$$u_n = u(t_n) \qquad s_n = s(t_n)$$

Partitioning Random Bits

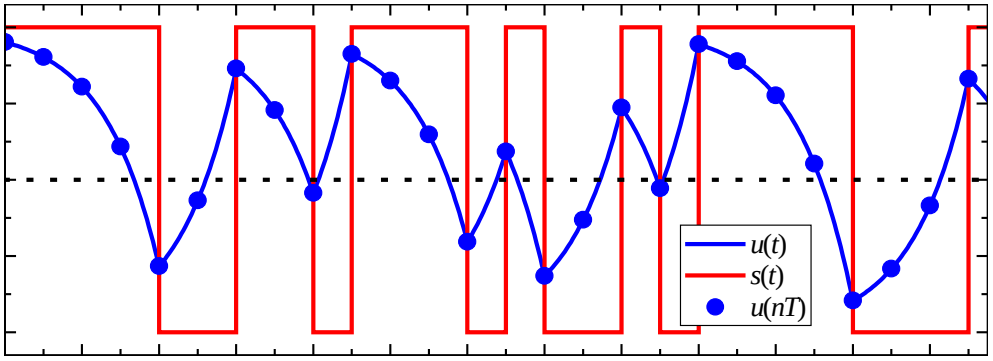
- **Dynamical System**

$$\frac{du}{dt} = u - s$$

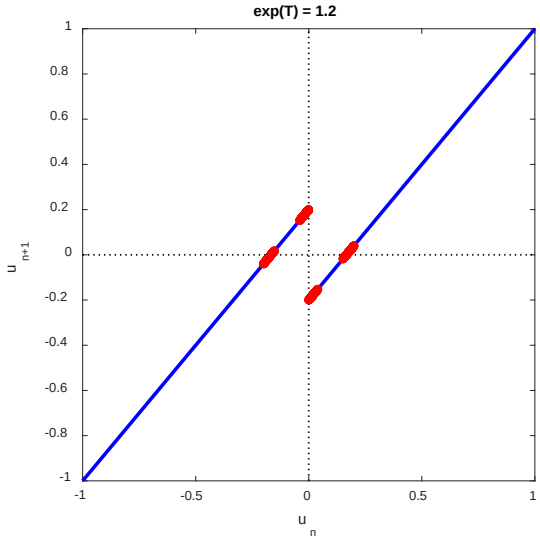
$$s(nT) = \begin{cases} +1, & u(nT) > 0 \\ -1, & u(nT) \le 0 \end{cases}$$

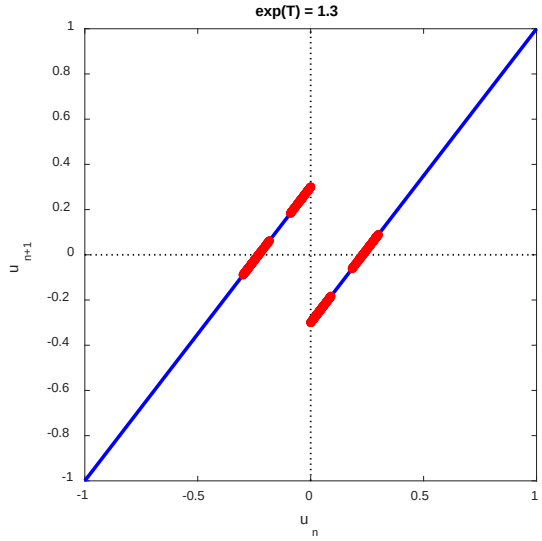


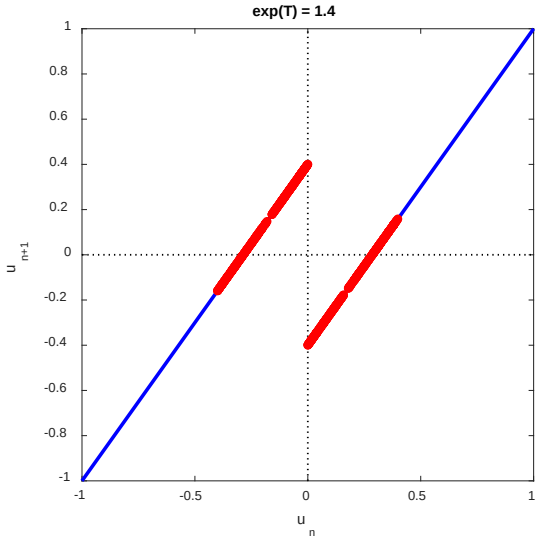
…1111001101111010010111110001…

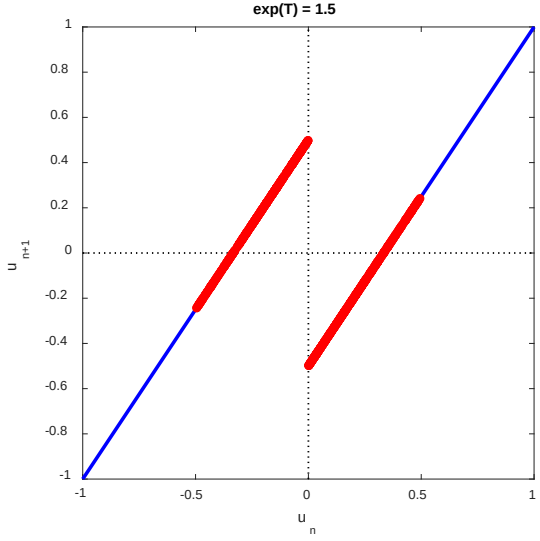


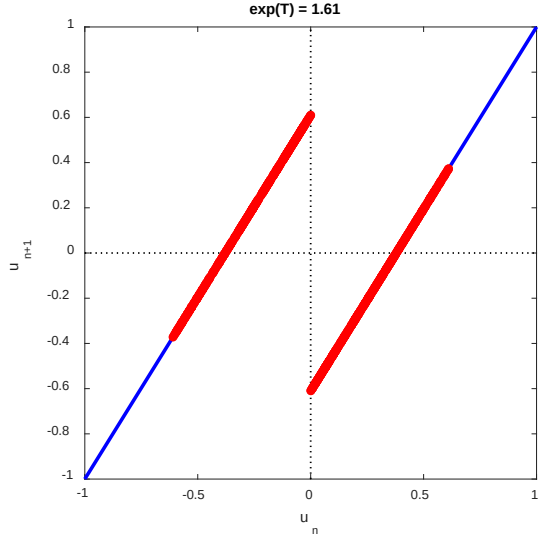
Tunable Return Map

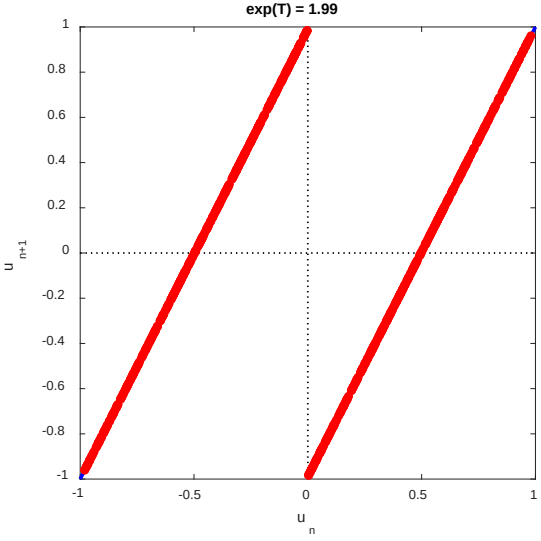






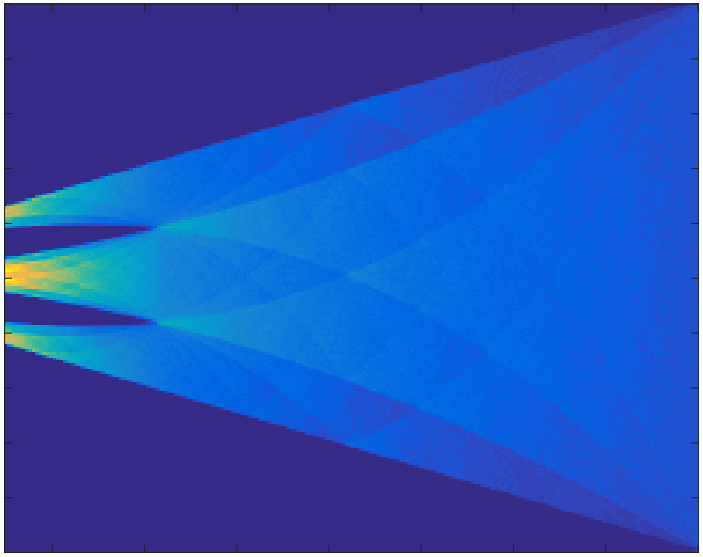


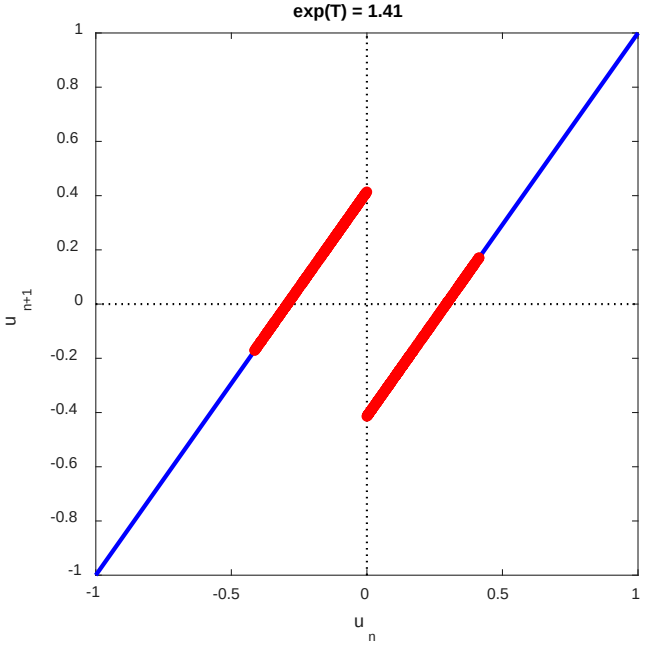




Special Tuning

- **Emergence of Period-1 Orbit**





$$e^T = \sqrt{2}$$

$$u_{n+1} = s_n + \sqrt{2}\left(u_n - s_n\right)$$

$$s_n = \mathrm{sgn}\left(u_n\right)$$

Maximal Sequences

- **Map Function**

$$f(u) = s + \sqrt{2}(u - s)$$

$$s = \operatorname{sgn}(u)$$

- **Closed Set**

$$f\left(1-\sqrt{2}\right) = 2\sqrt{2-3}$$

$$f\left(2\sqrt{2}-3\right) = 3-2\sqrt{2}$$

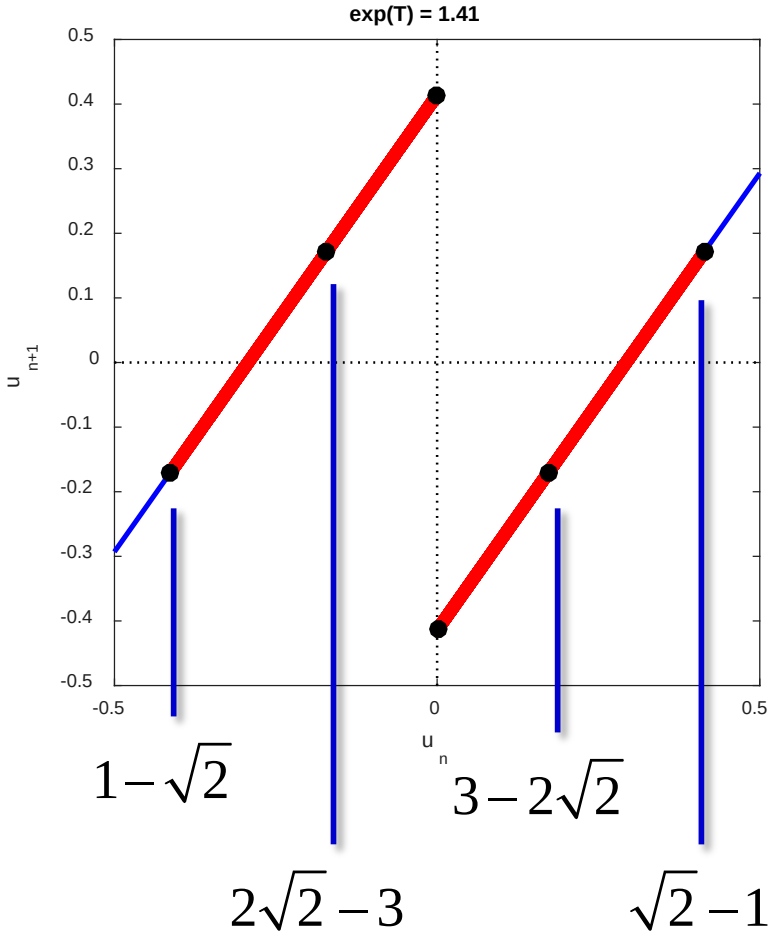
$$f\left(0^{-}\right) = \sqrt{2}-1$$

$$f\left(0^{+}\right) = 1-\sqrt{2}$$

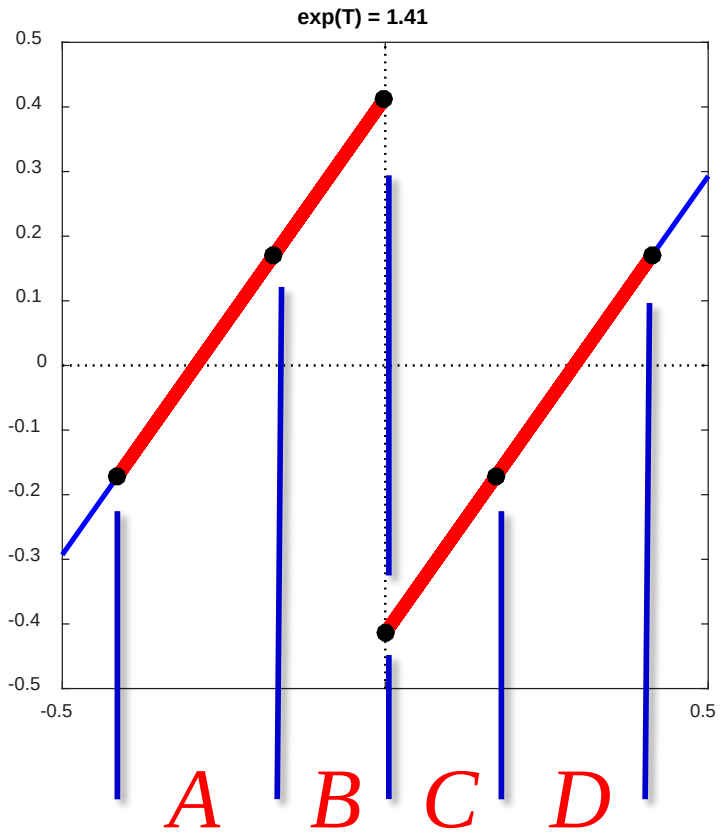
$$f\left(3-2\sqrt{2}\right) = 2\sqrt{2}-3$$

$$f\left(\sqrt{2}-1\right) = 3-2\sqrt{2}$$

$$u_{n+1} = f(u_n)$$

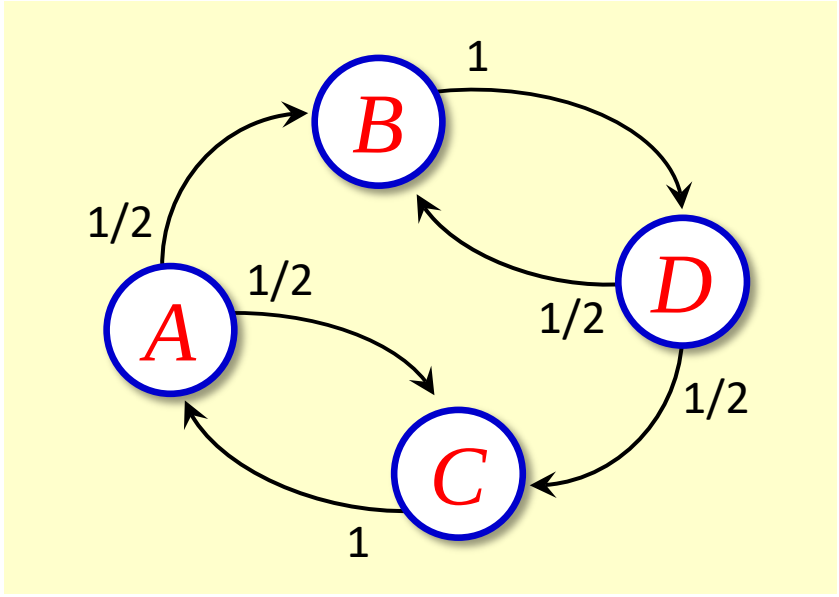


Markov Partition



$$\Phi = \{A, B, C, D\}$$

$$f\left(d\Phi\right) \in d\Phi$$



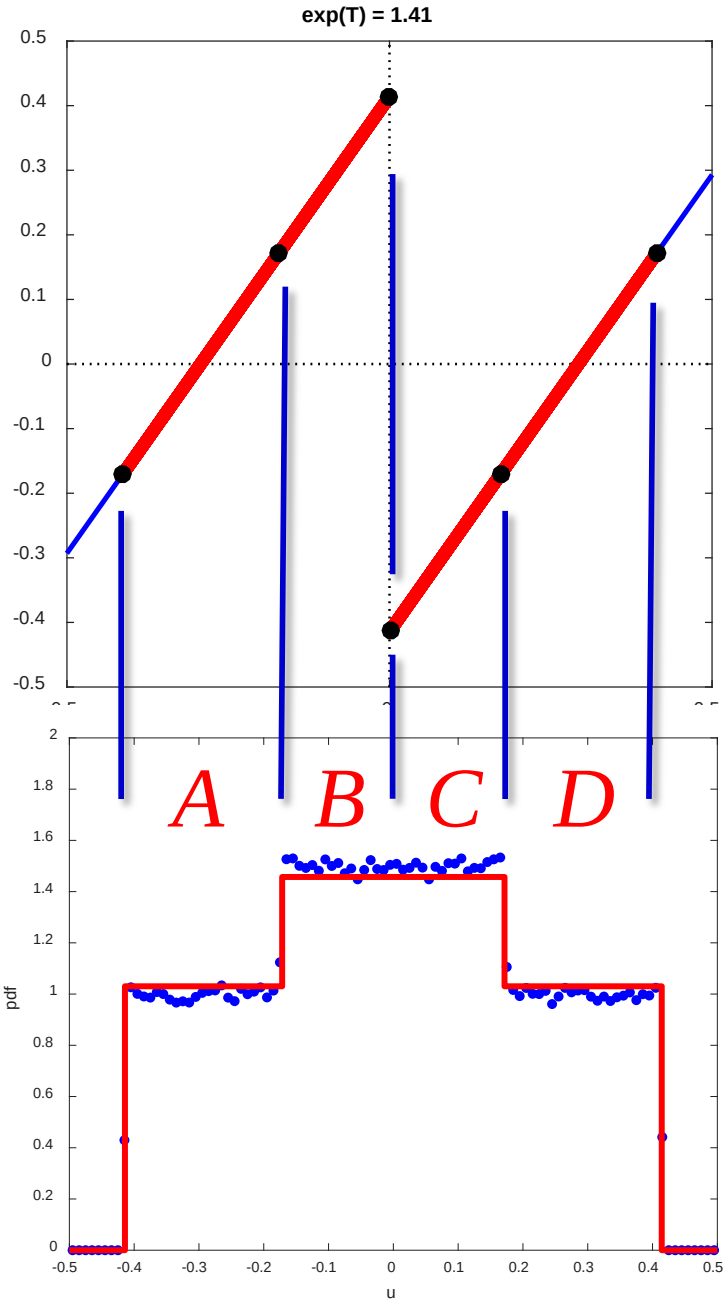
- **Natural Invariant Measure**

$$\mu_I = \sum_{f(J)\subset I} \frac{\mu_J}{\left|f'(J)\right|}$$

$$\begin{pmatrix} \mu_A \\ \mu_B \\ \mu_C \\ \mu_D \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} \mu_A \\ \mu_B \\ \mu_C \\ \mu_D \end{pmatrix}$$

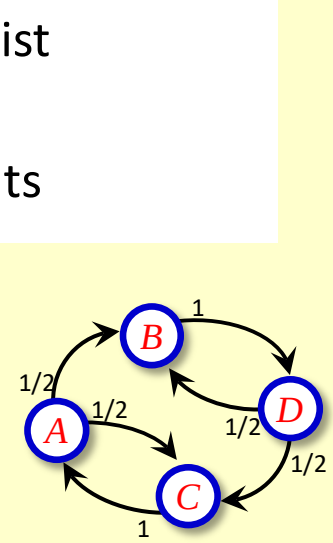
$$\mu_A = \mu_D = \frac{1}{4\left(3\sqrt{2}-4\right)}$$

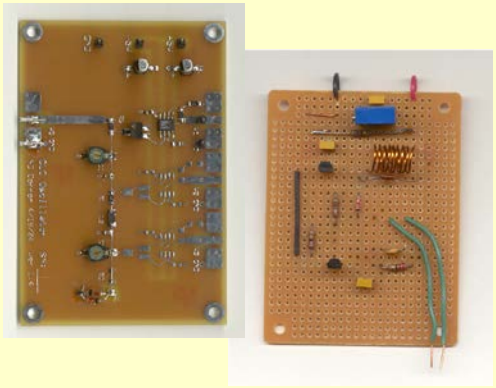
$$\mu_B = \mu_C = \frac{1}{4\left(3-2\sqrt{2}\right)}$$

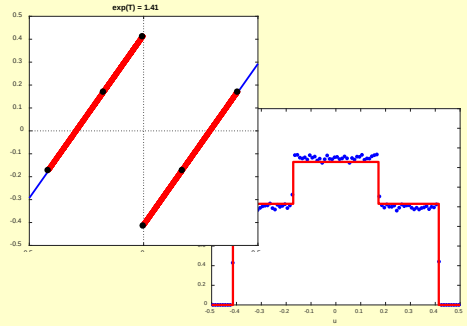


Conclusions

- **Motivation for Physical or True Random Number Generators**
  - it is not enough to be “good enough”
  - 100% assurance no correlations exist
  - transparent path from first-principle physics to random bits
- **Chaotic Electronic Circuits**
  - simple, low-cost devices
  - does not require exotic
- **Complete Analytic Description**
  - natural invariant density
  - independent, identically distributed events
- **Implementation**
  - easily integratable circuits
  - parameter feedback control required







Chaotic Circuit → Random Bits