Chaotic Behavior
of
Integer Sequences
from
Linear Feedback Shift Registers

Hong-Yeop Song
Channel Coding Lab., Yonsei University

KICS-NA WORKSHOP 2026

Contents

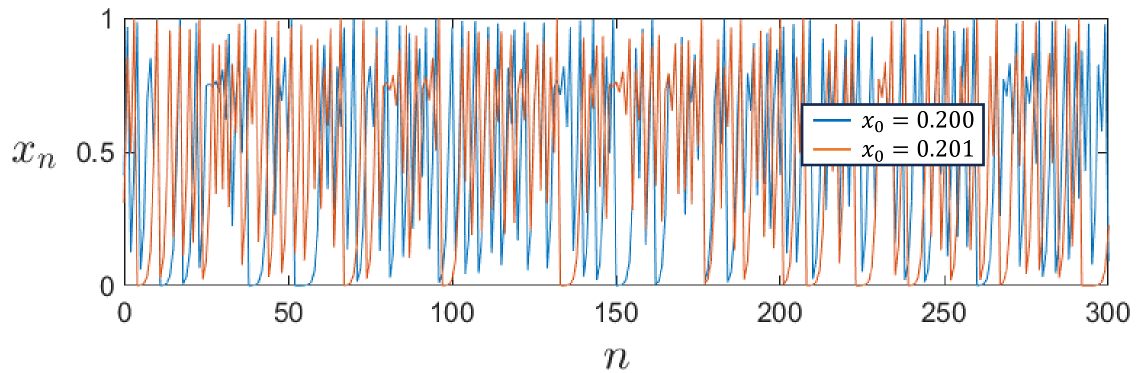
- **Introduction**
  - What is chaotic behavior?
  - Problems in Discrete Chaos
  - Discrete Lyapunov Exponent of Discrete Chaos
- **Main Contribution**
  - Chaotic behavior of integer sequences from LFSRs
  - Main Theorem and Proof
- **Conclusion**

What is chaotic behavior?

- **Chaotic behavior** : aperiodic and highly unpredictable dynamics

- **Chaotic maps** are nonlinear functions that are **extremely sensitive** to initial values, where even small differences can produce **completely different** sequences.

e.g., Logistic maps



- **Applications:**

CRYPTOGRAPHY,
DIGITAL WATERMARKING,
SPREAD-SPECTRUM COMMUNICATION,
RANDOM NUMBER GENERATION,… … … ……

Examples ? from WIKIPEDIA

List of chaotic maps

Map	Time domain	Space domain	Number of space dimensions	Number of parameters
2D Lorenz system[1]	discrete	real	2	1
2D Rational chaotic map[2]	discrete	rational	2	2
3-cells CNN system	continuous	real	3	
ACT chaotic attractor [3]	continuous	real	3	
Aizawa chaotic attractor[4]	continuous	real	3	5
Arneodo chaotic system[5]	continuous	real	3	
Arnold's cat map	discrete	real	2	0
Baker's map	discrete	real	2	0
Basin chaotic map[6]	discrete	real	2	1
Beta Chaotic Map[7]				12
Bogdanov map	discrete	real	2	3
Brusselator	continuous	real	3	
Burke-Shaw chaotic attractor[8]	continuous	real	3	2
Chen chaotic attractor[9]	continuous	real	3	3
Chen-Celikovsky system[10]	continuous	real	3	
Chen-LU system[11]	continuous	real	3	3
Chen-Lee system	continuous	real	3	
Chialvo map	discrete	discrete		3
Chossat-Golubitsky symmetry map				
Chua circuit[12]	continuous	real	3	3
Circle map	discrete	real	1	2
Complex quadratic map	discrete	complex	1	1
Complex squaring map	discrete	complex	1	0
Complex cubic map	discrete	complex	1	2
Clifford fractal map[13]	discrete	real	2	4
Degenerate Double Rotor map				
De Jong fractal map[14]	discrete	real	2	4
Delayed-Logistic system[15]	discrete	real	2	1
Discretized circular Van der Pol system[16]	discrete	real	2	1
Discretized Van der Pol system[17]	discrete	real	2	2
Double rotor map				
Duffing map	discrete	real	2	2

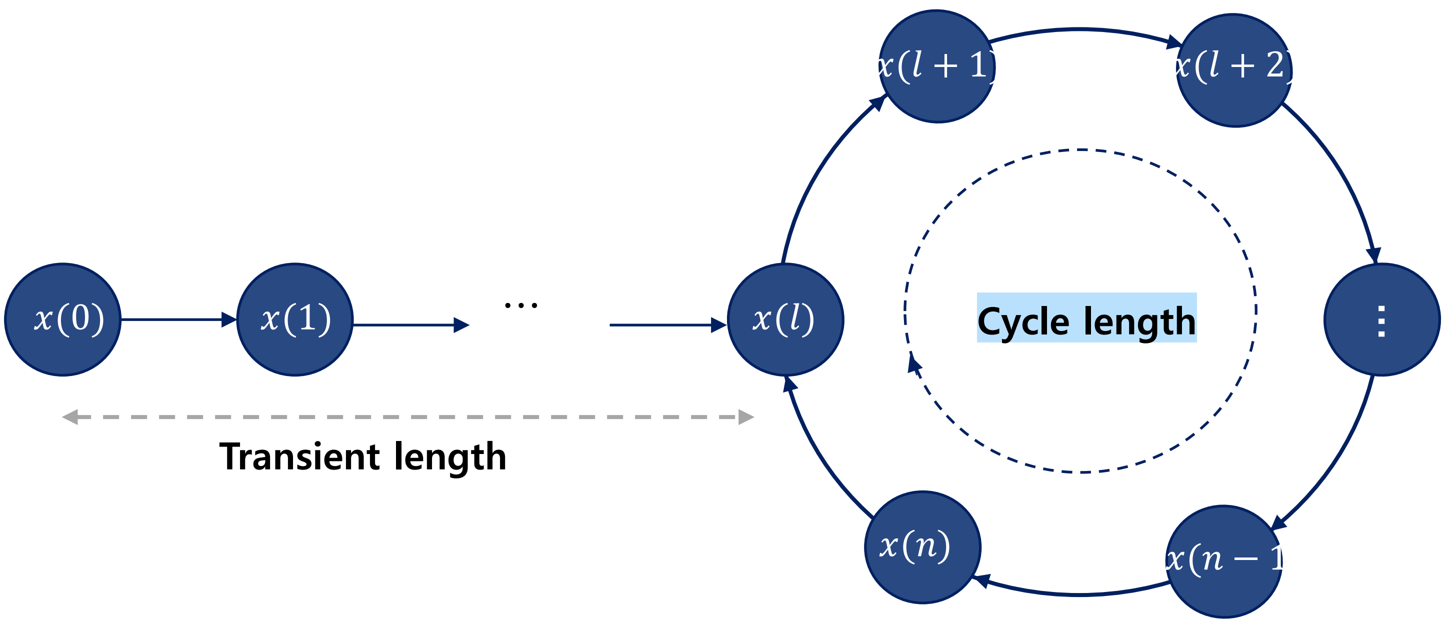
Problems in Discrete Chaos

When **implemented** in digital systems,
any (real field) chaotic map will suffer from some serious

dynamic degradation

due to **finite-precision** effects:

shorter periods, convergence to fixed values, and
other problems from rounding-off and quantization



Typical orbit of discrete chaotic maps

Discrete Lyapunov Exponent of Discrete chaos

- **Discrete Lyapunov Exponent (DLE) [10,11]**

  quantifies **the average rate of divergence** between ***neighboring elements*** of a permutation ***F*** in the discrete domain

$$\boldsymbol{S} := \{1, 2, 3, \dots, M-1, M\}$$

neighbors

DLE $\boldsymbol{\lambda_F}$ of a **permutation** $\boldsymbol{F}$ on the set $\boldsymbol{S}$:

$$\lambda_{\mathrm{F}} = \frac{1}{M} \sum_{i=1}^{M} ln|\boldsymbol{F}(\boldsymbol{z}_i) - \boldsymbol{F}(\boldsymbol{z}_{i+1})|$$

where $z_i = i$ for $i \in \boldsymbol{S}$ and $z_{M+1} = M - 1$ [11].

[10] L. Kocarev and J. Szczepanski, "Finite-space Lyapunov exponents and pseudochaos," ***Phys. Rev. Lett***., vol. 93, p. 234101, **2004**.

[11] L. Kocarev, J. Szczepanski, J.M.Amigo, and I. Tomovski, "Discrete chaos-I: Theory," ***IEEE Trans. Circuits Syst. I, Reg. Papers***, vol. 53, no.6, pp.1300–1309, **2006**.

Discrete Lyapunov Exponent of Discrete chaos

➢ Discrete Lyapunov Exponent (DLE) [10,11]

A **permutation** F on a discrete domain **{1,2,…,*M*}** is said to be ***discretely chaotic***

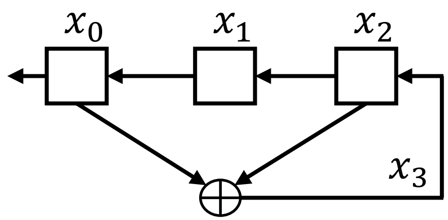
if its DLE λ_F satisfies

$$\lim_{M \to \infty} \lambda_F > 0$$

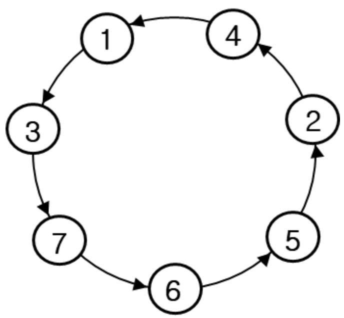
[10] L. Kocarev and J. Szczepanski, "Finite-space Lyapunov exponents and pseudochaos," ***Phys. Rev. Lett***., vol. 93, p. 234101, **2004**.
[11] L. Kocarev, J. Szczepanski, J.M.Amigo, and I. Tomovski, "Discrete chaos-I: Theory," ***IEEE Trans. Circuits Syst. I, Reg. Papers***, vol. 53, no.6, pp.1300–1309, **2006**.

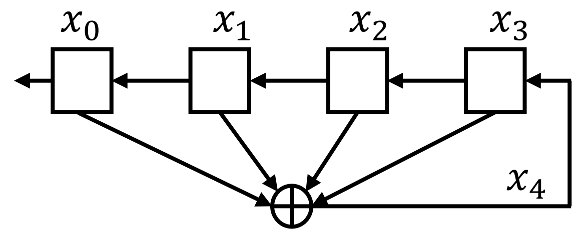
Contents

Permutation from the integer sequences of LFSRs

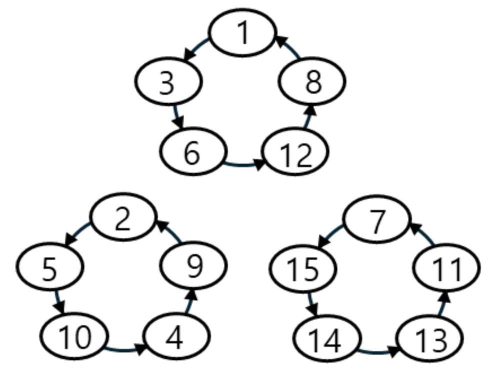


Primitive *Connection Polynomial* :
$x^3 + x^2 + 1$





Non-primitive but irreducible
Connection Polynomial :
$x^4 + x^3 + x^2 + x + 1$



The resulting integer sequences partition
the set $\{1, 2, \ldots, 2^L - 1\}$ into **disjoint cycles** and induce
a permutation on the set $\{1, 2, \ldots, 2^L - 1\}$

Is this a **discrete Chaos** ?
Can we calculate its **dLE** ?

Main Theorem

Theorem 1

The **discrete Lyapunov Exponent** λ_F of F satisfies the following:

$$\boldsymbol{ln(\sqrt{3})} \leq \lim_{L\to\infty} \lambda_F \leq \boldsymbol{ln(2)},$$

where F is the **induced integer permutation** from an L-stage LFSR with **irreducible connection polynomial** and **a non-zero initial state**.

Satisfies the definition of discrete chaos !

DLE λ_F of a permutation F on the set S:

$$\lambda_F = \frac{1}{M}\sum_{i=1}^{M} \ln\left|F(z_i) - F(z_{i+1})\right|$$

where $z_i = i$ for $i \in S$ and $z_{M+1} = M-1$ [11].

$S := \{1, 2, 3, \ldots, M-1, M\}$

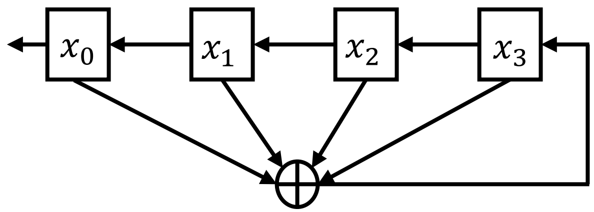
neighbors

$S := \{1, 2, \ldots, 2^L - 1\}$

$F: S \rightarrow S$

	z ($x_0\,x_1\,x_2\,x_3$)	$F(z)$ ($x_0\,x_1\,x_2\,x_3$)
1 =	0 0 0 1	0 0 1 1
2 =	0 0 1 0	0 1 0 1
3 =	0 0 1 1	0 1 1 0
	0 1 0 0	1 0 0 1
⋮	0 1 0 1	1 0 1 0
	0 1 1 0	1 1 0 0
$2^{L-1}-1$ =	0 1 1 1	1 1 1 1
2^{L-1} =	1 0 0 0	0 0 0 1
	1 0 0 1	0 0 1 0
⋮	1 0 1 0	0 1 0 0
	1 0 1 1	0 1 1 1
	1 1 0 0	1 0 0 0
	1 1 0 1	1 0 1 1
	1 1 1 0	1 1 0 1
$2^L - 1$ =	1 1 1 1	1 1 1 0

We will use this running example and prove the result in general



irreducible $x^4 + x^3 + x^2 + x + 1$

We divide $S := \{1, 2, \ldots, 2^L - 1\}$ into **three cases**:

Case 1) $z \in D := S \setminus \{2^{L-1}-1, 2^{L-1}, 2^L - 1\}$

Case 2) $z = 2^{L-1} - 1$

Case 3) $z \in \{2^{L-1}, \ 2^L - 1\}$

Sketch of Proof

$$\lambda_{\mathrm{F}} = \frac{1}{M}\sum_{i=1}^{M} ln\,|F(z_{i+1}) - F(z_i)|$$

$\boldsymbol{S} \coloneqq \{\mathbf{1}, \mathbf{2}, \ldots, \mathbf{2}^{\boldsymbol{L}} - \mathbf{1}\}$

$\boldsymbol{F}\colon \boldsymbol{S} \to \boldsymbol{S}$

	z	$F(z)$
	$x_0\,x_1\,x_2\,x_3$	$x_0\,x_1\,x_2\,x_3$
1 =	0 0 0 1	
2 =	0 0 1 0	
3 =	0 0 1 1	
	0 1 0 0	
⋮	0 1 0 1	
	0 1 1 0	
$\mathbf{2}^{\boldsymbol{L}-\mathbf{1}} - \mathbf{1}$ =	0 1 1 1	
$\mathbf{2}^{\boldsymbol{L}-\mathbf{1}}$ =	1 0 0 0	
	1 0 0 1	
⋮	1 0 1 0	
	1 0 1 1	
	1 1 0 0	
	1 1 0 1	
	1 1 1 0	
$\mathbf{2}^{\boldsymbol{L}} - \mathbf{1}$ =	1 1 1 1	

$\mathbf{2}\boldsymbol{z}$

or

$\mathbf{2}\boldsymbol{z} + \mathbf{1}$

Case 1) $D := S \setminus \{2^{L-1} - 1, 2^{L-1}, 2^{L} - 1\}$

Claim 1-(1) For all $\boldsymbol{z} \in \boldsymbol{D}$

$$|\boldsymbol{F}(\boldsymbol{z} + \mathbf{1}) - \boldsymbol{F}(\boldsymbol{z})| \in \{1, 2, 3\}.$$

Update rule:

when the feedback is 0	when the feedback is 1
$\boldsymbol{F}(\boldsymbol{z}) = \mathbf{2}\boldsymbol{z}$	$\boldsymbol{F}(\boldsymbol{z}) = \mathbf{2}\boldsymbol{z} + \mathbf{1}$
$\boldsymbol{F}(\boldsymbol{z} + \mathbf{1}) = \mathbf{2}(\boldsymbol{z} + \mathbf{1})$	$\boldsymbol{F}(\boldsymbol{z} + \mathbf{1}) = \mathbf{2}(\boldsymbol{z} + \mathbf{1}) + \mathbf{1}$

Therefore,

$$|\boldsymbol{F}(\boldsymbol{z} + \mathbf{1}) - \boldsymbol{F}(\boldsymbol{z})| = \begin{cases} |2(z+1) - 2z| = 2 \\ |(2(z+1)+1) - 2z| = 3 \\ |2(z+1) - (2z+1)| = 1 \\ |(2(z+1)+1) - (2z+1)| = 2 \end{cases}$$

Sketch of Proof

$$\lambda_{\mathrm{F}} = \frac{1}{M}\sum_{i=1}^{M} ln\, |F(z_{i+1}) - F(z_i)|$$

Case 1) $D := S \setminus \{2^{L-1}-1, 2^{L-1}, 2^L - 1\}$

Claim 1-(2) For all $z \in D$

$$|\{z \in D|\ |F(z+1) - F(z)| = 3\}|$$
$$= |\{z \in D|\ |F(z+1) - F(z)| = 1\}|$$

$$S \coloneqq \{1, 2, \ldots, 2^L - 1\}$$

$$F: S \to S$$

	z: x_0	$x_1\, x_2\, x_3$	$F(z)$: $x_0\, x_1\, x_2\, x_3$	
$1 =$	0	0 0 1	0 0 1 1	
$2 =$	0	0 1 0	0 1 0 1	2
$3 =$	0	0 1 1	0 1 1 0	1
always not	0	1 0 0	1 0 0 1	3
⋮	0	1 0 1	1 0 1 0	1
	0	1 1 0	1 1 0 0	2
$2^{L-1} - 1 =$	0	1 1 1	1 1 1 1	
$2^{L-1} =$	1	0 0 0	0 0 0 1	
	1	0 0 1	0 0 1 0	
⋮	1	0 1 0	0 1 0 0	2
always	1	0 1 1	0 1 1 1	3
contribute	1	1 0 0	1 0 0 0	1
to the	1	1 0 1	1 0 1 1	3
feedback	1	1 1 0	1 1 0 1	2
$2^L - 1 =$	1	1 1 1	1 1 1 0	

For $z \in [1, 2^{L-1} - 1]$,

- $|F(z+1) - F(z)| = 3 \Leftrightarrow$
  $|F(z + 2^{L-1} + 1) - F(z + 2^{L-1})| = 1$

- $|F(z+1) - F(z)| = 1 \Leftrightarrow$
  $|F(z + 2^{L-1} + 1) - F(z + 2^{L-1})| = 3$

Sketch of Proof

$$\lambda_{\mathrm{F}} = \frac{1}{M}\sum_{i=1}^{M} ln\,|F(z_{i+1}) - F(z_i)|$$

$\boldsymbol{S} \coloneqq \{\mathbf{1}, \mathbf{2}, \ldots, \mathbf{2}^{L} - \mathbf{1}\}$

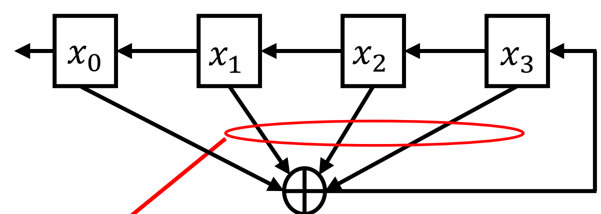
$\boldsymbol{F}\colon \boldsymbol{S} \rightarrow \boldsymbol{S}$

	z	$F(z)$	
	$x_0\,x_1\,x_2\,x_3$	$x_0\,x_1\,x_2\,x_3$	
1 =	0 0 0 1	0 0 1 1	
2 =	0 0 1 0	0 1 0 1	
3 =	0 0 1 1	0 1 1 0	
	0 1 0 0	1 0 0 1	
⋮	0 1 0 1	1 0 1 0	
	0 1 1 0	1 1 0 0	
$2^{L-1} - 1$ =	0 1 1 1	1 1 1 1	$= \mathbf{2}^{L} - \mathbf{1}$
2^{L-1} =	1 0 0 0	0 0 0 1	$= \mathbf{1}$
	1 0 0 1	0 0 1 0	
⋮	1 0 1 0	0 1 0 0	
	1 0 1 1	0 1 1 1	
	1 1 0 0	1 0 0 0	
	1 1 0 1	1 0 1 1	
	1 1 1 0	1 1 0 1	
$2^{L} - 1$ =	1 1 1 1	1 1 1 0	

Case 2) For $\boldsymbol{z = 2^{L-1} - 1}$,

Claim 2: $\left|\boldsymbol{F}\left(\mathbf{2}^{L-1}\right) - \boldsymbol{F}\left(\mathbf{2}^{L-1} - \mathbf{1}\right)\right| = \mathbf{2}^{L} - \mathbf{2}$

An irreducible polynomial has an **odd number of terms** including x^L and x^0.



odd number of terms

(except for the first and the last)

contribute to the feedback

FOR ANY IRRED. POLYNOMIAL

Sketch of Proof

$$\lambda_{\mathrm{F}} = \frac{1}{M}\sum_{i=1}^{M} ln\,|F(z_{i+1}) - F(z_i)|$$

$S := \{1, 2, \ldots, 2^L - 1\}$

$F: S \rightarrow S$

z		$F(z)$
	$x_0 x_1 x_2 x_3$	$x_0 x_1 x_2 x_3$
1 =	0 0 0 1	
2 =	0 0 1 0	
3 =	0 0 1 1	
	0 1 0 0	
⋮	0 1 0 1	
	0 1 1 0	
$2^{L-1} - 1$ =	0 1 1 1	
2^{L-1} =	1 0 0 0	→ 0 0 0 1 = 1
	1 0 0 1	→ 0 0 1 x
⋮	1 0 1 0	
	1 0 1 1	
	1 1 0 0	
	1 1 0 1	
	1 1 1 0	1 1 0 x
$2^L - 1$ =	1 1 1 1	1 1 1 0

similarly

Case 3) for $z = 2^{L-1}$ or $z = 2^L - 1$.

Claim 3: Depending on whether the term x^{L-1} appears **or not** in the polynomial, we have,

$$|F(z+1) - F(z)| \in \{1, 2\}.$$

when x^{L-1} appears in the conn. poly.

0 0 1 x = 0 0 1 0 = 2

$\Rightarrow |F(z+1) - F(z)| = 1$

when x^{L-1} DOES NOT appear in the conn. poly.

0 0 1 x = 0 0 1 1 = 3

$\Rightarrow |F(z+1) - F(z)| = 2$

Sketch of Proof

$$\lambda_{\mathrm{F}} = \frac{1}{M}\sum_{i=1}^{M} ln \left|\underbrace{F(z_{i+1}) - F(z_i)}_{diff}\right|$$

As a summary,

when x^{L-1} appears in the conn. poly.

$|\{z \in S \mid diff = 2\}| = \beta \quad \rightarrow \beta \ln 2$

$|\{z \in S \mid diff = 3\}| = \alpha \quad \rightarrow \alpha \ln 3$

$|\{z \in S \mid diff = 1\} = \alpha + 2 \quad \rightarrow 0$

$|\{z \in S \mid diff = 2^L - 2\} = 1 \quad \rightarrow 1 \ln(2^L - 2)$

$(2^L - 1)\ \lambda_{\mathrm{F}}$

	z ($x_0 x_1 x_2 x_3$)	$F(z)$ ($x_0 x_1 x_2 x_3$)
1 =	0 0 0 1	0 0 1 1
2 =	0 0 1 0	0 1 0 1
3 =	0 0 1 1	0 1 1 0
	0 1 0 0	1 0 0 1
⋮	0 1 0 1	1 0 1 0
	0 1 1 0	1 1 0 0
$2^{L-1} - 1$ =	0 1 1 1	1 1 1 1
2^{L-1} =	1 0 0 0	0 0 0 1
	1 0 0 1	0 0 1 0
⋮	1 0 1 0	0 1 0 0
	1 0 1 1	0 1 1 1
	1 1 0 0	1 0 0 0
	1 1 0 1	1 0 1 1
	1 1 1 0	1 1 0 1
$2^L - 1$ =	1 1 1 1	1 1 1 0

(claim 1)
1 or 2 or 3

(claim 2) $2^L - 2$

(claim 3) 1 or 2

when x^{L-1} **DOES NOT** appear in the conn. poly.
similar calculation follows.

Sketch of Proof

$$\lambda_{\mathrm{F}} = \frac{1}{M}\sum_{i=1}^{M} ln\left|\boldsymbol{F}(\boldsymbol{z}_{i+1}) - \boldsymbol{F}(\boldsymbol{z}_i)\right|$$

$$\lambda_{\mathrm{F}} = \frac{\alpha\ ln3 + \beta\ ln2 + ln(2^L - 2)}{2^L - 1} = \frac{ln\left(3^\alpha 2^\beta\right) + ln(2^L - 2)}{2^L - 1}$$

We use $\sqrt{\mathbf{3}} < 2$ for **lower bound** and $3 < \mathbf{2^2}$ for **upper bound**:

$$\frac{ln\left(3^\alpha \mathbf{3^{\beta/2}}\right) + ln(2^L - 2)}{2^L - 1} < \frac{ln\left(3^\alpha 2^\beta\right) + ln(2^L - 2)}{2^L - 1} < \frac{ln\left(\mathbf{2^{2\alpha}} 2^\beta\right) + ln(2^L - 2)}{2^L - 1}$$

Or

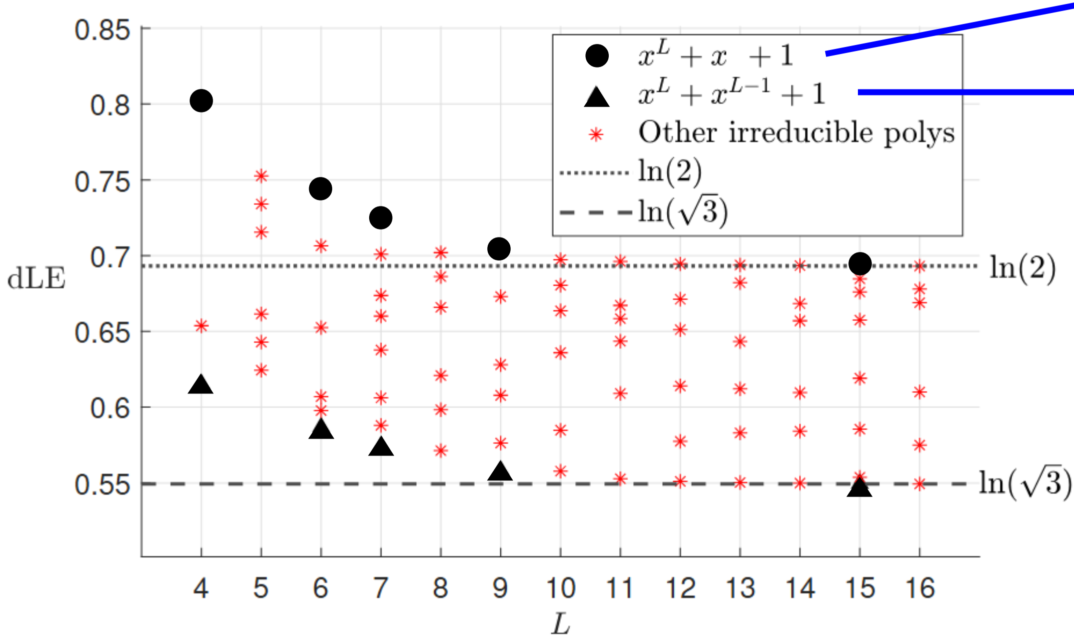
$$\frac{(\mathbf{2}\boldsymbol{\alpha} + \boldsymbol{\beta})\ \boldsymbol{ln}\left(\sqrt{\mathbf{3}}\right) + ln(2^L - 2)}{\mathbf{2}^{\boldsymbol{L}} - \mathbf{1}} < \lambda_F < \frac{(\mathbf{2}\boldsymbol{\alpha} + \boldsymbol{\beta})\ \boldsymbol{ln}(\mathbf{2}) + ln(2^L - 2)}{\mathbf{2}^{\boldsymbol{L}} - \mathbf{1}}$$

We use finally $\mathbf{2}\boldsymbol{\alpha} + \boldsymbol{\beta} + \mathbf{3} = \mathbf{2}^{\boldsymbol{L}} - \mathbf{1}$ and $\boldsymbol{L} \to \infty$

$$\boldsymbol{ln}\left(\sqrt{\mathbf{3}}\ \right) \leq \lim_{\boldsymbol{L}\to\infty} \boldsymbol{\lambda_F} \leq \boldsymbol{ln}(\mathbf{2})$$

Theorem 1.

$$\boldsymbol{ln(\sqrt{3}) \leq \lim_{L\to\infty} \lambda_F \leq ln(2)}$$



$\lim_{L\to\infty} \lambda_F = \boldsymbol{ln(2)}$

$\lim_{L\to\infty} \lambda_F = \boldsymbol{ln(\sqrt{3})}$

Some Computations for
$4 \leq L \leq 16$

Conclusion

- Studied the **chaotic nature** of **the integer sequences** from L-stage ***irreducible*** LFSRs
- Derived the **discrete Lyapunov Exponent** of the integer permutation and showed that it is **lower bound by** $\sqrt{3}$ as the register length L **increases indefinitely.**