Chaotic Behavior of Integer Sequences from Linear Feedback Shift Registers



Hyojeong Choi, Gangsan Kim, **Hong-Yeop Song**
Channel Coding Lab., Yonsei University

and

Hongjun Noh*
*department of C4I R&D Center, LIG Nex1

IWSDA 2025

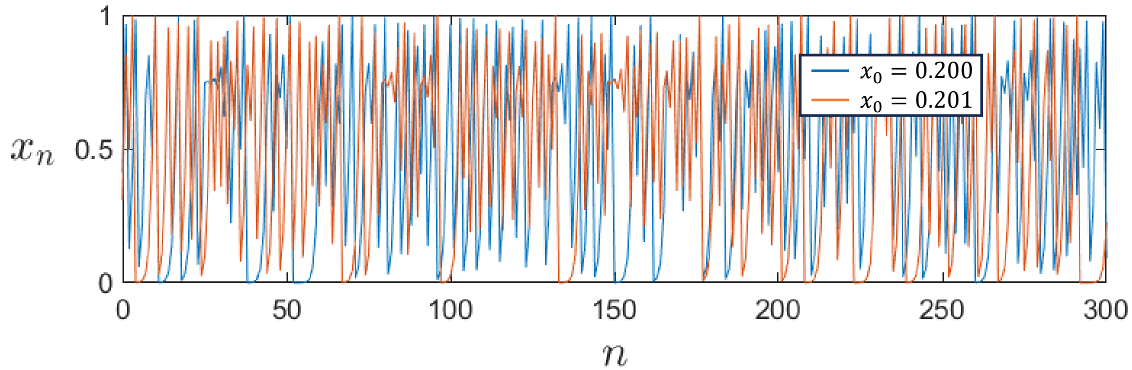
Contents

- **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

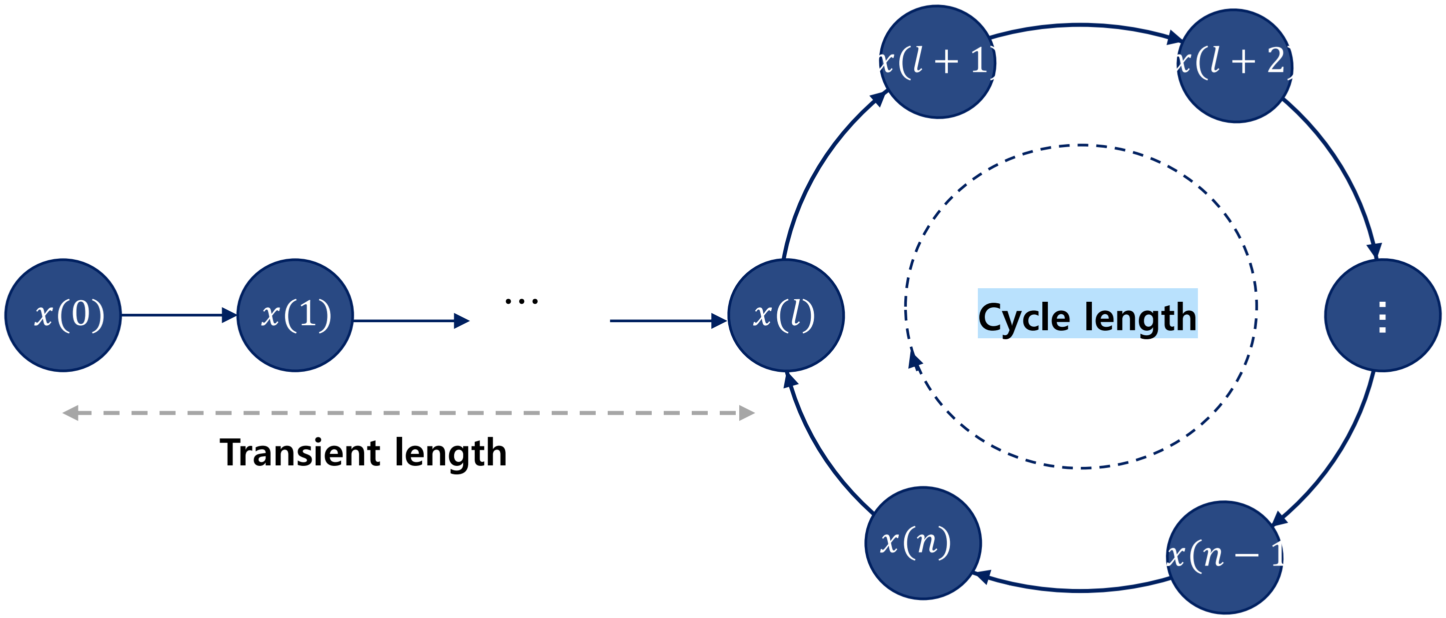


- **Applications:** cryptography, digital watermarking, spread-spectrum communication, random number generation,…

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

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

neighbors

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

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

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** $\boldsymbol{F}$ is said to be ***discretely chaotic***

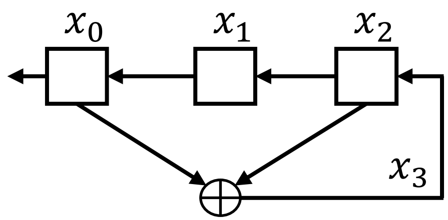
if its DLE satisfies [10,11]

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

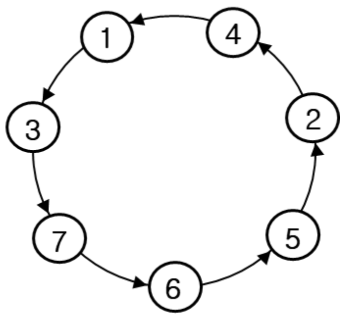
Contents

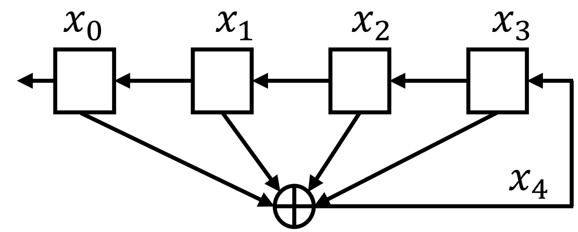
- **Introduction**
  - What is chaotic behavior?
  - Problems in Discrete Chaos
  - Discrete Lyapunov Exponent of Discrete Chaos
- **Main Contribution**
  - Chaotic behavior of integer sequences from LFSRs
  - Main Theorem and Proof
- **Conclusion**

Permutation from the integer sequences of LFSRs

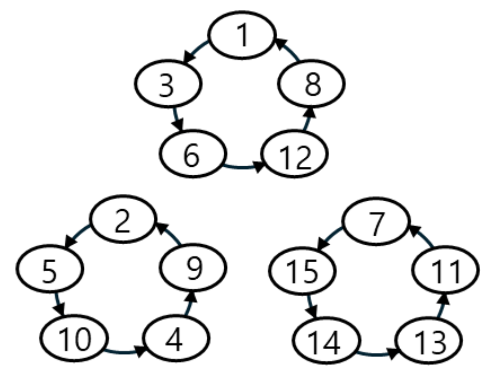


Primitive *Connection Polynomial* :
$x^3 + x^2 + 1$





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



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

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:

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

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:

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

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

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

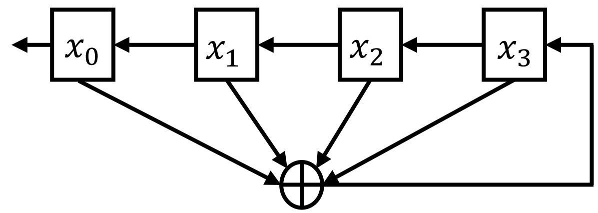
neighbors

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

$F: S \to S$

	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
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

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

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

$$F: S \to S$$

	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	$2z$
	0 1 1 0	
$2^{L-1} - 1$ =	0 1 1 1	or
2^{L-1} =	1 0 0 0	
	1 0 0 1	
⋮	1 0 1 0	$2z + 1$
	1 0 1 1	
	1 1 0 0	
	1 1 0 1	
	1 1 1 0	
$2^L - 1$ =	1 1 1 1	

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

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

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

Update rule:

when the feedback is 0	when the feedback is 1
$F(z) = 2z$	$F(z) = 2z + 1$
$F(z+1) = 2(z+1)$	$F(z+1) = 2(z+1) + 1$

Therefore,

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

Sketch of Proof

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

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

$F\colon S \to S$

	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	

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

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

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

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

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

Sketch of Proof

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

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

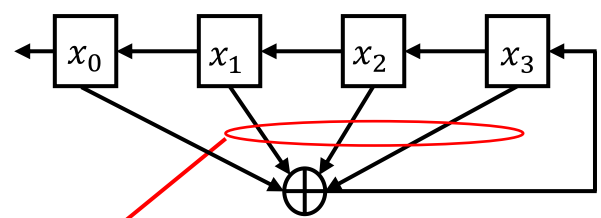
$$F: S \to S$$

	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	
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	$= 2^L - 1$
2^{L-1} =	1 0 0 0	0 0 0 1	$= 1$
	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 $z = 2^{L-1} - 1$,

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

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

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

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,

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

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

$$F: S \to S$$

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

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

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

similarly

Sketch of Proof

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

$diff$

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	$F(z)$
	$x_0 x_1 x_2 x_3$	$x_0 x_1 x_2 x_3$
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
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

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

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

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

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

Or

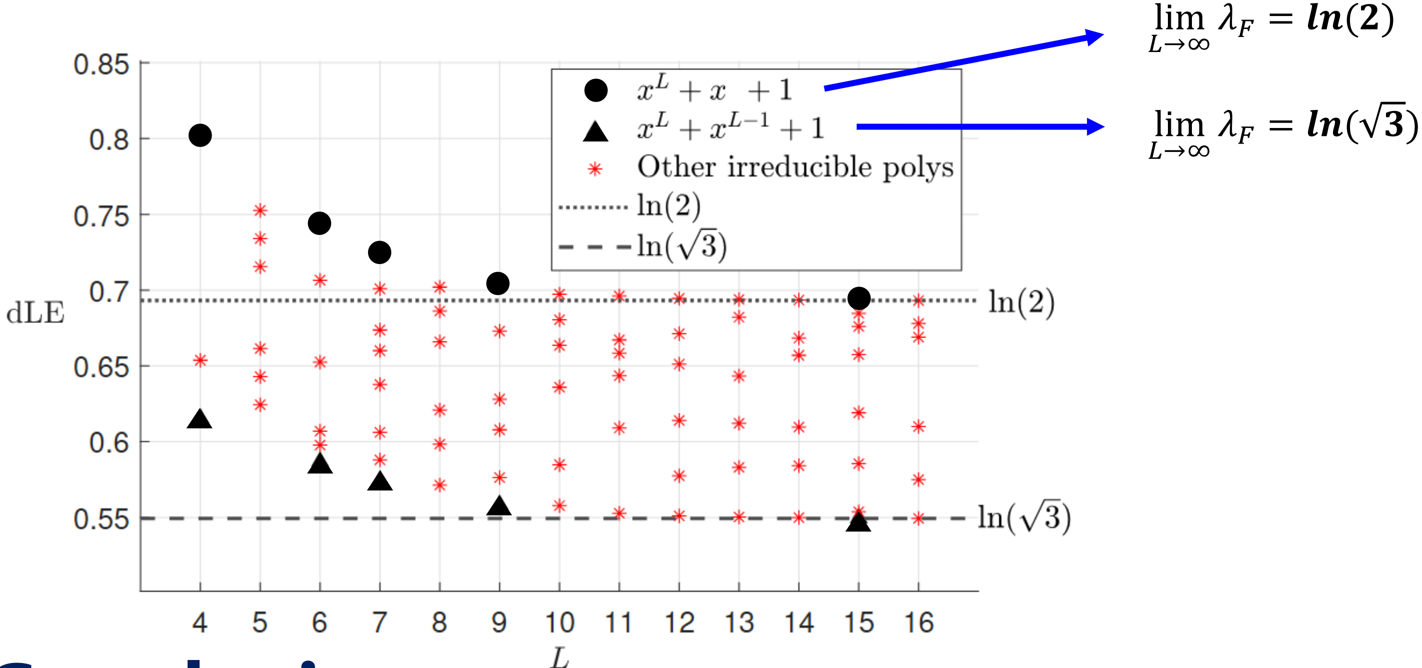
$$\frac{(2\alpha + \beta)\, ln(\sqrt{3}) + \ln(2^L - 2)}{2^L - 1} < \lambda_F < \frac{(2\alpha + \beta)\, ln(2) + \ln(2^L - 2)}{2^L - 1}$$

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

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

Theorem 1.

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



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