Analysis for binary chaotic sequences generated by cascade chaotic maps

Hyojeong Choi, Daekyeong Kim, Sangwon Chae, Hong-Yeop Song
School of Electrical and Electronic Engineering, Yonsei University
Seoul, Korea

Yundong Lee, Sangung Shin, Hongjun Noh
Tactical Communication Systems Waveform R&D, LIG Nex1
Gyeonggi-do, Korea

2023

ICTC

Contents

Introduction

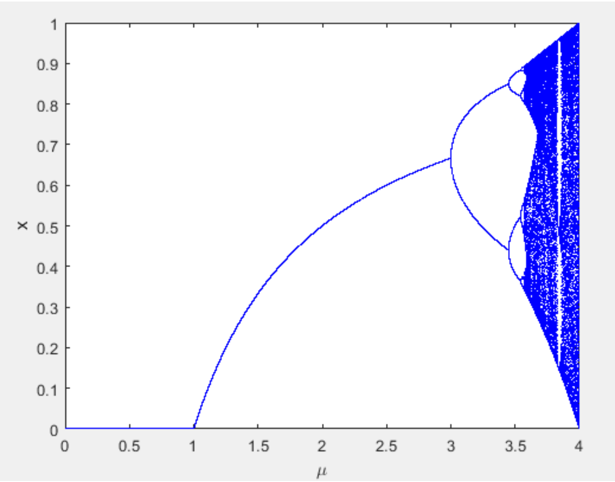
- The chaotic map is a nonlinear function characterized by its sensitivity to initial values, where even slight differences in initial values can lead to completely distinct outcomes.
- Due to this characteristic, it becomes possible to easily generate infinitely different sequences solely by varying the initial values.
- The PN codes used in conventional Direct Sequence Spread Spectrum (DSSS) systems have the fixed period, which limits the size of the sequence set.
- Therefore, the use of chaotic sequences in existing DSSS systems employing PN codes has been studied [3], [8]–[10].
- This paper analyzes the characteristics of sequences generated using cascade chaotic maps employing two or three seed maps.

Traditional Chaotic maps

- In general, a chaos means a state of disorder. These terms are frequently used in dynamic systems and were defined by R. L. Devaney [2],[6].
- The chaotic map is a nonlinear function characterized by its sensitivity to initial values, where even slight differences in initial values can lead to completely distinct outcomes.

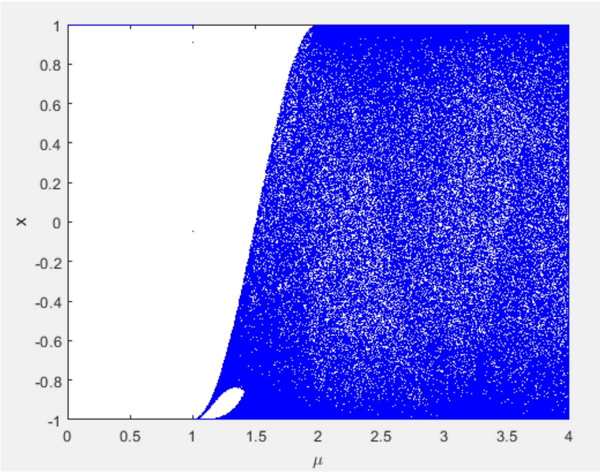
❖ **Logistic map :** $x_{n+1} = \mu x_n(1 - x_n)$

$1 \leq \mu \leq 4, \qquad x_n \in [0,1]$



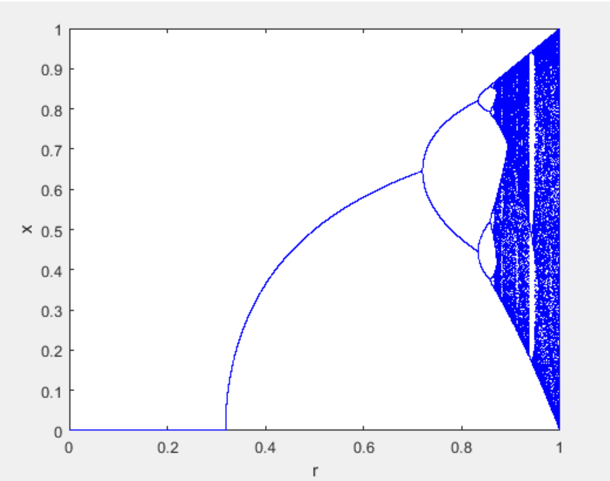
❖ **Chebyshev map :** $x_{n+1} = cos(u \cdot arccos(x_n))$

$0 \leq u \leq 4, \qquad x_n \in [-1,1]$



❖ **Sine map:** $x_{n+1} = r \cdot sin(\pi x_n)$

$0 \leq r \leq 1, \qquad x_n \in [0,1]$



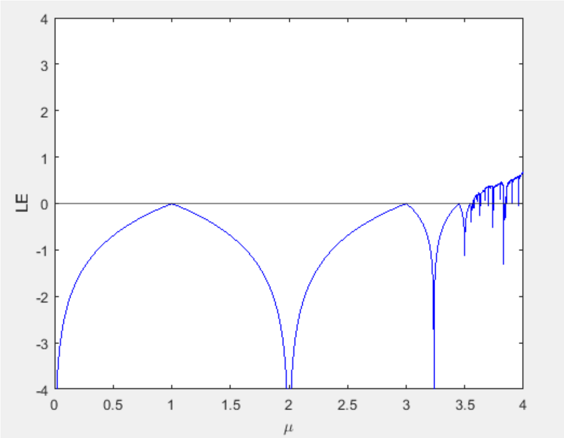
Lyapunov Exponent

- Lyapunov Exponents (LE) can be utilized to explain the chaotic behavior of a chaotic system, as they provide a quantitative description of the variation between two adjacent output values in a dynamic system [7,15].

Lyapunov exponent	$\lambda = \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} \ln\left|\frac{df(x_i)}{dx}\right|$	$\lambda > 0$: Chaotic state

❖ Logistic map : $x_{n+1} = \mu x_n(1 - x_n)$

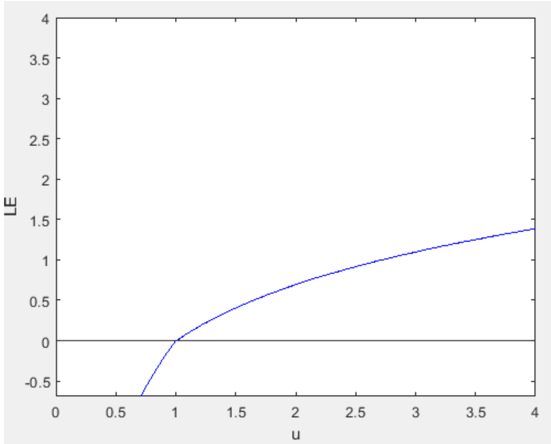
$1 \le \mu \le 4, \quad x_n \in [0,1]$



❖ Chebyshev map :

$x_{n+1} = cos(u \cdot arccos(x_n))$

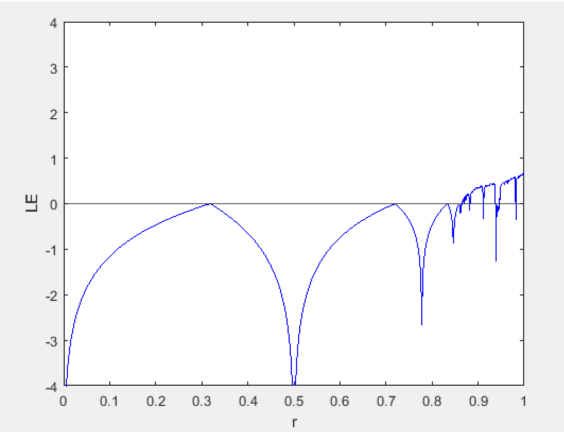
$0 \le u \le 4, \quad x_n \in [-1,1]$



❖ Sine map:

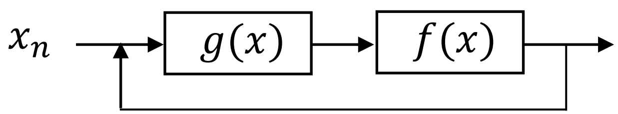
$x_{n+1} = r \cdot sin(\pi x_n)$

$0 \le r \le 1, \quad x_n \in [0,1]$



Cascade chaotic system

[15]



$x_{n+1} = \Gamma(x_n) = f(g(x_n))$

Fig. 1. Structure of CCS

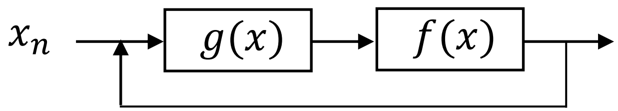
- [15] LE of CCS $\Gamma(x)$

$$\lambda_{\Gamma(x)} = \lim_{N\longrightarrow\infty} \frac{1}{N} \sum_{i=0}^{N-1} \ln \left| \frac{dg(x_i)}{dx} \right| + \lim_{N\longrightarrow\infty} \frac{1}{N} \sum_{i=0}^{N-1} \ln \left| \frac{df(x_i)}{dx} \right|$$

$$\lambda_{\Gamma(x)} = \lambda_{F(x)} + \lambda_{G(x)}.$$

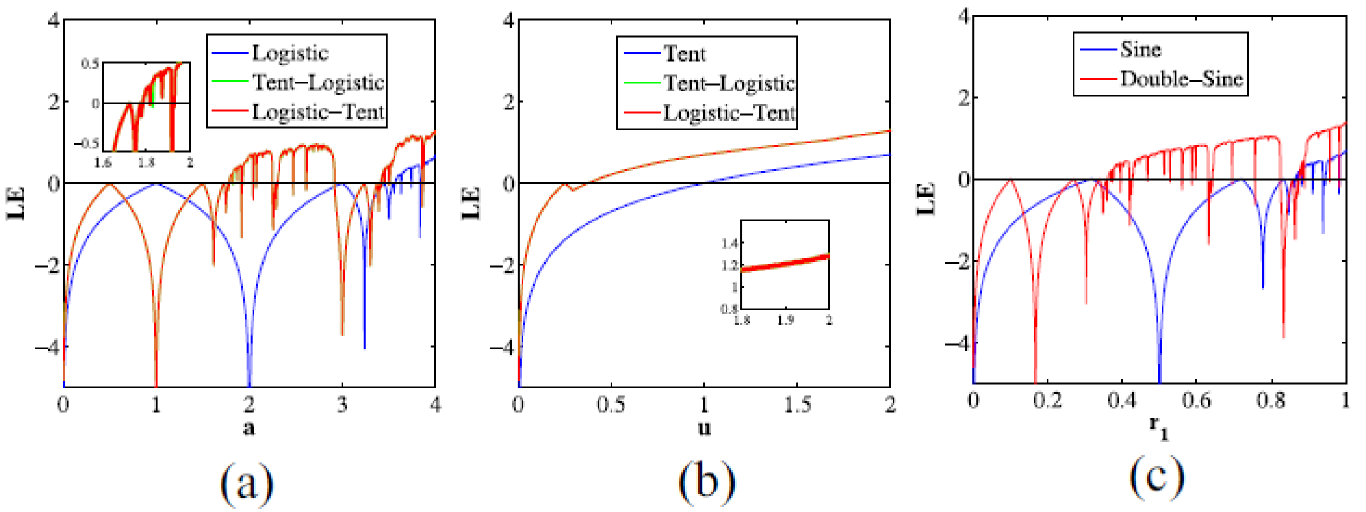
[15] Y. Zhou, Z. Hua, C. M. Pun, and C. L. P. Chen, “Cascade chaotic system with applications,” IEEE Transactions on Cybernetics, vol. 45, no. 9, pp. 2001–2012, Sep. 2015.

Cascade chaotic system



$$x_{n+1} = \Gamma(x_n) = f(g(x_n))$$

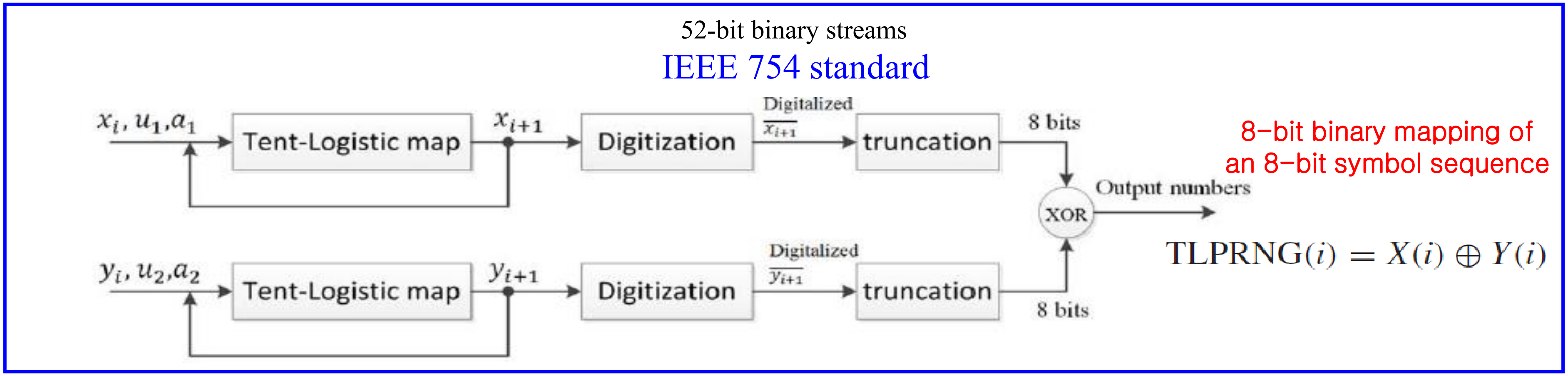
Fig. 1. Structure of CCS



[15] Y. Zhou, Z. Hua, C. M. Pun, and C. L. P. Chen, "Cascade chaotic system with applications," IEEE Transactions on Cybernetics, vol. 45, no. 9, pp. 2001–2012, Sep. 2015.

Pseudo Random Number Generators

1) [15] PRNG (pseudo-random number generators)



2) **Threshold method**

This method involves mapping each x_n value to binary using half of the range of x_n corresponding to each map as a threshold.

ex) $x_n \in [0,1]$ $\quad f(x_n) = \begin{cases} 1, & x_n \geq 0.5 \\ 0, & x_n < 0.5 \end{cases}$

[15] Y. Zhou, Z. Hua, C. M. Pun, and C. L. P. Chen, "Cascade chaotic system with applications," IEEE Transactions on Cybernetics, vol. 45, no. 9, pp. 2001–2012, Sep. 2015.

1. Introduction

2. Preliminary

1) Traditional chaotic maps

2) Lyapunov Exponents (LE)

3) Cascade chaotic system (CCS)

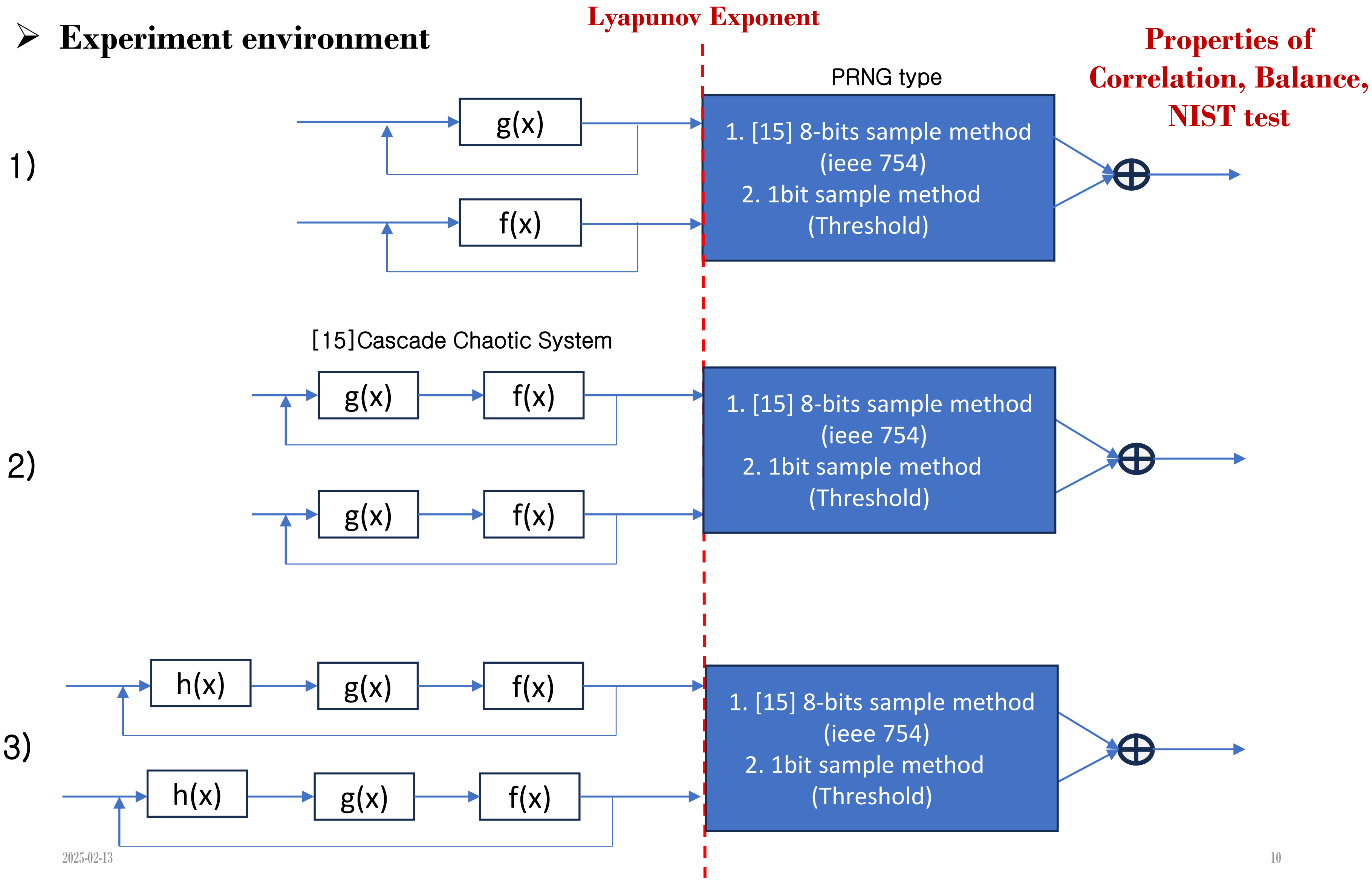
4) Pseudorandom number generators (PRNGs)

3. Properties for binary chaotic sequences generated by cascade chaotic maps (**Main Results**)

4. Concluding Remark

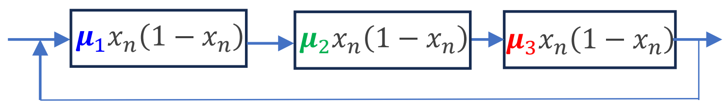
Properties for binary chaotic sequences generated by cascade chaotic maps

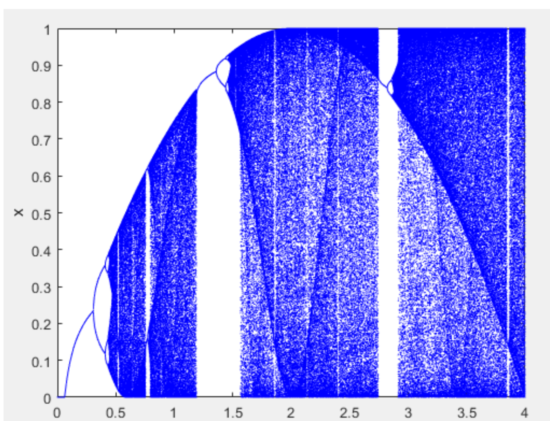
- Experiment environment



Properties for binary chaotic sequences generated by cascade chaotic maps

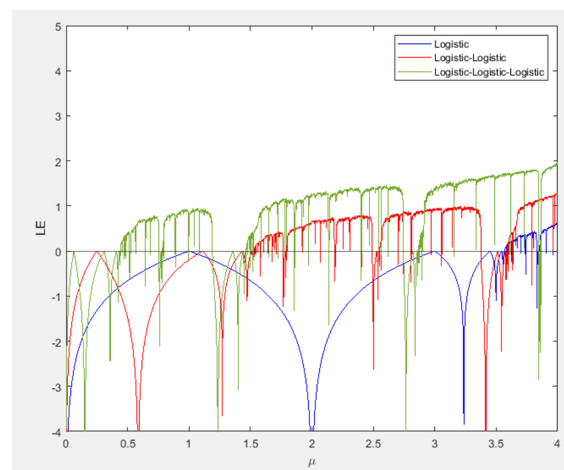
- **Experiment environment**
  - **Triple-Logistic map**





μ_3

Bifurcation diagram

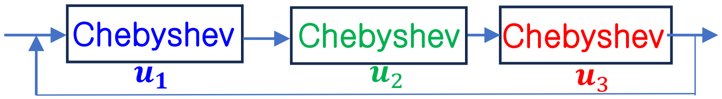


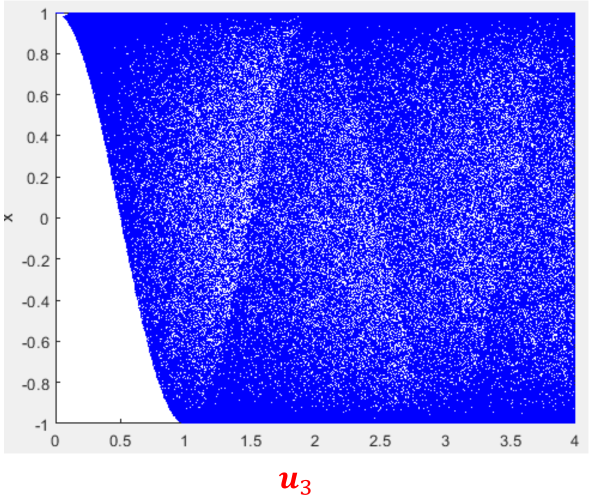
Lyapunov Exponent

Properties for binary chaotic sequences generated by cascade chaotic maps

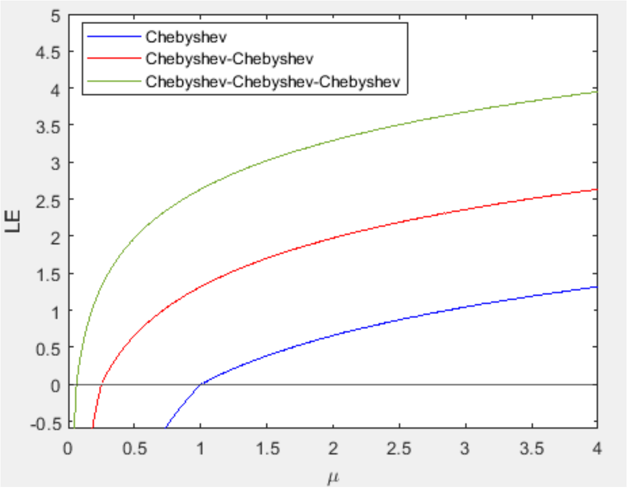
- **Experiment environment**

  - **Triple-Chebyshev map**





Bifurcation diagram

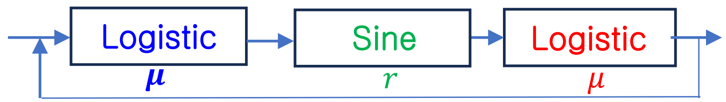


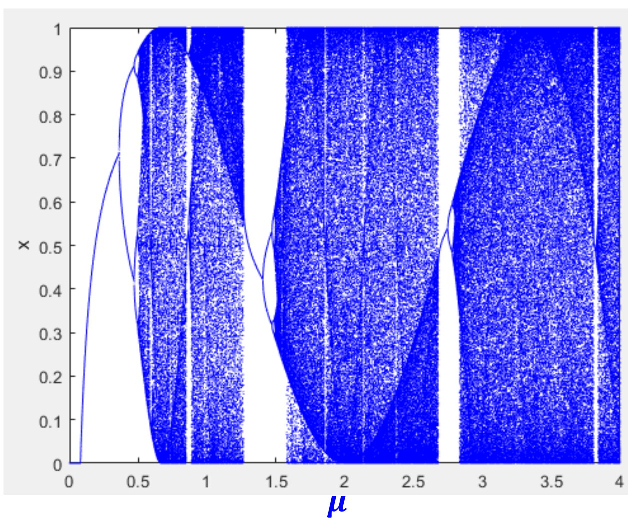
Lyapunov Exponent

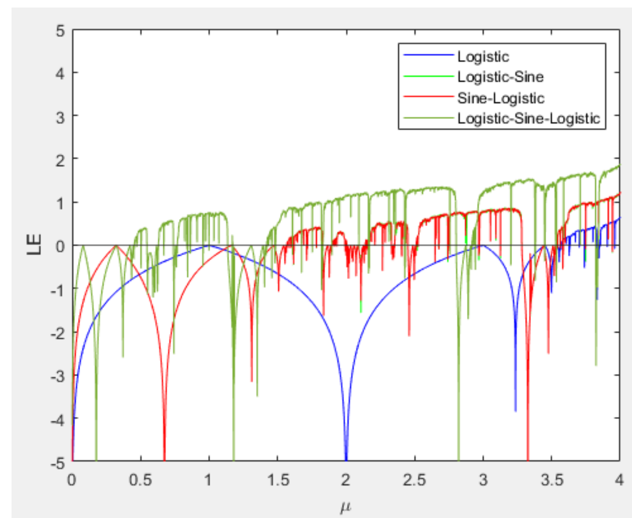
Properties for binary chaotic sequences generated by cascade chaotic maps

➢ **Experiment environment**

- **Logistic-Sine-Logistic map**





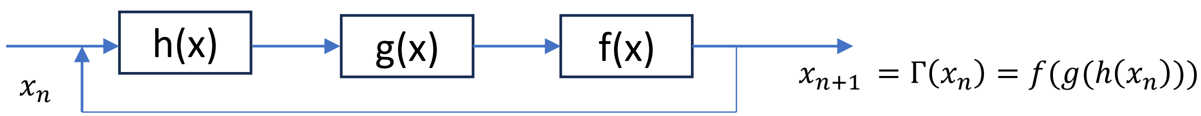


Bifurcation diagram

Lyapunov Exponent

Properties for binary chaotic sequences generated by cascade chaotic maps

➢ Our conjecture



- LE of CCS $\Gamma(x)$

$$\lambda_{\Gamma(x)} = \lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N-1}\ln\left|\frac{dh(x_i)}{dx}\right| + \lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N-1}\ln\left|\frac{dg(x_i)}{dx}\right| + \lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N-1}\ln\left|\frac{df(x_i)}{dx}\right|$$

$$\boxed{\lambda_{\Gamma(x)} = \lambda_{h(x)} + \lambda_{g(x)} + \lambda_{f(x)}}$$

Properties for binary chaotic sequences generated by cascade chaotic maps

➢ Correlation properties

Classification	Length: 10000 Initial value: 0.4001 – 0.4100				Length: 100000 Initial value: 0.4001 – 0.4100			
	Normalized Auto-correlation		Normalized Cross-correlation		Normalized Auto-correlation		Normalized Cross-correlation	
	Average (sidelobe)	Average (sidelobe max)	Average	Max Average	Average (sidelobe)	Average (sidelobe max)	Average	Max Average
Double-Logistic Triple-Logistic Double-Chebyshev Triple-Chebyshev Logisitc-Sine Logisitc-Sine-Logisitc	≈ 0.008 ≈ -21dB	≈ 0.04 ≈ -14dB	≈ 0.008 ≈ -21dB	≈ 0.04 ≈ -14dB	≈ 0.002 ≈ -27dB	≈ 0.01 ≈ -20dB	≈ 0.002 ≈ -27dB	≈ 0.01 ≈ -20dB
m-sequence	≈ 0.006 ≈ -22dB	≈ 0.02 ≈ -16dB	–	–	≈ 0.001 ≈ -28dB	≈ 0.007 ≈ -21dB	–	–

TABLE I. CORRELATION PROPERTIES FOR BINARY CHAOTIC SEQUENCES AND M-SEQUENCE

Properties for binary chaotic sequences generated by cascade chaotic maps

- **Balance properties**

Classification	Length: 10000 Initial value: 0.4001 – 0.4100			
	0 Average Percentage		1 Average Percentage	
	[15] method	Threshold	[15] method	Threshold
Double-Logistic	49.9898	49.9767	50.0102	50.0233
Triple-Logistic	50.0285	50.0581	49.9715	49.9419
Double-Chebyshev	49.9731	49.9442	50.0269	50.0558
Triple-Chebyshev	50.0076	50.0068	49.9924	49.0068
Logisitc-Sine	50.0243	50.2240	49.9757	49.7760
Logisitc-Sine-Logisitc	49.9675	50.0081	50.0325	49.9919

TABLE II. BALANCE PROPERTIES FOR BINARY CHAOTIC SEQUENCES USING TWO DISTINCT BINARY MAPPING METHOD

Properties for binary chaotic sequences generated by cascade chaotic maps

- **NIST test**

Classification		Frequency	Run	Rank	DFT	Linear Comp.	Cusum
Double-Logistic	[15] method	0.739918	0.911413	0.213309	0.534146	0.350485	0.911413
	Threshold	0.534146	0.739918	0.122325	0.017912	0.739918	0.350485
Triple-Logistic	[15] method	0.739918	0.991468	0.534146	0.350485	0.739918	0.534146
	Threshold	0.350485	0.534146	0.739918	0.122325	0.739918	0.350485
Double-Chebyshev	[15] method	0.911413	0.122325	0.122325	0.122325	0.122325	0.213309
	Threshold	0.319084	0.595549	**0.000000**	**0.000320**	0.162606	0.534146
Triple-Chebyshev	[15] method	0.213309	0.739918	0.350485	0.911413	0.350485	0.534146
	Threshold	0.115387	0.181557	**0.002374**	0.213309	0.102526	0.437274
Logisitc-Sine	[15] method	0.534146	0.350485	0.534146	0.213309	0.350485	0.534146
	Threshold	0.213309	0.122325	0.739918	0.534146	0.534146	0.122325
Logisitc-Sine-Logisitc	[15] method	0.739918	0.213309	0.122325	0.911413	0.213309	0.739918
	Threshold	0.066882	0.911413	0.739918	0.213309	0.350485	0.739918
m-sequence		0.262249	0.224821	**0.000000**	**0.000320**	**0.000000**	**0.002559**

TABLE III. RESULTS OF NIST STATISTICAL TEST FOR BINARY CHAOTIC SEQUENCES USING TWO DISTINCT BINARY MAPPING METHOD AND M-SEQUENCE

1. Introduction

2. Preliminary

1) Lyapunov Exponents (LE)

2) Cascade chaotic system (CCS)

3) Pseudorandom number generators (PRNGs)

3. Properties for binary chaotic sequences generated by cascade chaotic maps

4. Concluding Remark

Concluding Remark

In this paper,

- Analyzes the characteristics of sequences generated using cascade chaotic maps employing two or three seed maps.
- Propose a new conjecture for the LE of the cascade chaotic map using three seed maps.
- The real-valued output sequences of CCS are converted to the binary sequences using two binary mapping methods. These binary sequences exhibit good correlation and balance properties.
- As a result of the NIST test, this is acceptable in all tests when using the [15] method, but not in some tests when using the Chebyshev map as the seed map for the threshold method.
- It is expected that the use of chaotic binary sequences can be considered in the existing DSSS system using PN codes.

Thank you for listening