

연접 혼돈 맵으로 생성된 이진 수열에 대한 분석

최효정, 송홍엽

연세대학교

{hjchoi3022, hysong}@yonsei.ac.kr,

Analysis of binary sequences generated by cascade chaotic maps

Hyojeong Choi and Hong-Yeop Song

Yonsei Univ.

요약

본 논문은 세 개의 시드맵 (seed maps)을 사용하여 생성된 이진 수열들의 여러 특성들을 분석한다. 먼저, 세 개의 시드맵을 사용한 연접 혼돈 시스템들의 리아푸노프 지수(Lyapunov Exponent)를 비교한다. 그리고 이들의 출력 실수 수열은 두 가지 서로 다른 이진 맵핑 방법을 사용하여 이진 수열로 변환하여 상관 및 균형 특성을 m -수열과 비교하고 NIST 테스트를 통해 통계적으로 랜덤 특성을 검증한다.

I. 서론

혼돈 맵(Chaotic map)은 미세한 초기 값의 차이만으로도 완전히 다른 실수 값이 도출되는 비선형 함수이다. 이러한 특성으로 인해 서로 다른 무한한 수열을 쉽게 생성할 수 있으므로 의사 잡음 코드(PN code)를 사용하는 기존의 직접 수열 대역 확산 (Direct Sequence Spread Spectrum, DSSS) 시스템에서 혼돈 수열의 사용이 연구되어왔다[1,2].

혼돈 맵의 혼돈 성능은 직접적으로 증명하는 것이 매우 어렵기 때문에, 두 인접한 초기 값으로 생성된 혼돈 맵의 출력 수열 간의 변동을 정량화한 파라미터인 리아푸노프 지수(Lyapunov Exponent, LE)로 혼돈 성능을 판단한다[3-5]. 단일 혼돈 맵은 비교적 낮은 리아푸노프 지수를 갖기 때문에 최근 암호학 연구에서 리아푸노프 지수를 향상시키기 위한 연구가 진행되어왔다. [4]에서는 두 개의 단일 맵을 연결하여 더 나은 혼돈 성능을 갖는 연접 혼돈 시스템(Cascade Chaotic System, CCS)을 소개하였고, 두 개의 단일맵을 연결하였을 때의 리아푸노프 지수는 두 단일 맵의 각각의 리아푸노프 지수의 합이 되는 것을 증명했다.

본 논문에서는 세 개의 단일 맵을 사용한 연접 혼돈 시스템을 고려한다. 먼저, 이들의 리아푸노프 지수를 비교하고, 이러한 연접 혼돈 시스템의 출력 실수 수열을 [4]에서 제안한 이진 맵핑 방식과 임계값 이진 맵핑 방식을 적용하여 이진 수열로 변환하여 이들의 상관 및 균형 특성, 그리고 NIST test 결과를 m -수열과 비교한다.

II. 본론

A. 단일 혼돈 맵

본 논문에서는 혼돈 맵으로 Logistic map, Chebyshev map, 그리고 Sine map을 고려한다. Logistic map은 다음 식 (1)로 정의되는 함수이다.

$$x_{n+1} = \mu x_n (1 - x_n) \quad (1)$$

여기서 $1 \leq \mu \leq 4$ 이고 $x_n \in (0,1)$ 이다. 이 함수는 $3.5699 < \mu \leq 4$

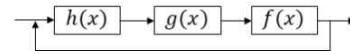


그림 1. 연접 혼돈 시스템

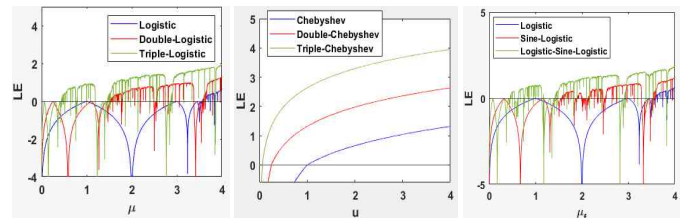


그림 2. 연접 혼돈 시스템의 리아푸노프 지수

일 때 혼돈 상태가 된다. Chebyshev map은 다음 식 (2)로 정의되는 함수이다.

$$x_{n+1} = \cos(u \cdot \arccos(x_n)) \quad (2)$$

여기서 $0 \leq u \leq 4$ 이고 $x_n \in [-1,1]$ 이다. 이 함수는 $\mu \geq 2$ 일 때 혼돈 상태가 된다. Sine map은 다음 식 (3)으로 정의되는 함수이다.

$$x_{n+1} = r \cdot \sin(\pi \cdot x_n) \quad (3)$$

여기서 $0 \leq r \leq 1$ 이고 $x_n \in (0,1)$ 이다. 이 함수는 $0.867 < r \leq 1$ 일 때 혼돈 상태가 된다.

B. 연접 혼돈 시스템

본 논문에서는 그림 1과 같이 세 개의 단일 맵을 결합하여 다음과 같이 정의되는 연접 혼돈 시스템을 고려한다.

$$x_{n+1} = \Gamma(x_n) = f(g(h(x_n))) \quad (4)$$

본 논문에서는 서로 다른 fractal 파라미터를 갖는 세 개의 Logistic map을 연접시킨 Triple-Logistic map과 세 개의 Chebyshev map을 연접시킨

분류	길이: 10000 초기값: 0.4001-0.4100				길이: 100000 초기값: 0.4001-0.4100			
	정규화된 자기상관		정규화된 상호상관		정규화된 자기상관		정규화된 상호상관	
	sidelobe 평균	sidelobe max 평균	평균	max 평균	sidelobe 평균	sidelobe max 평균	평균	max 평균
Triple-Logistic	≈ 0.008	≈ 0.04	≈ 0.008	≈ 0.04	≈ 0.002	≈ 0.01	≈ 0.002	≈ 0.01
Triple-Cheby.	$\approx -21\text{dB}$	$\approx -14\text{dB}$	$\approx -21\text{dB}$	$\approx -14\text{dB}$	$\approx -27\text{dB}$	$\approx -20\text{dB}$	$\approx -27\text{dB}$	$\approx -20\text{dB}$
Logi.-Sine-Logi.								
m -수열	≈ 0.006 $\approx -22\text{dB}$	≈ 0.02 $\approx -16\text{dB}$	-	-	≈ 0.001 $\approx -28\text{dB}$	≈ 0.007 $\approx -21\text{dB}$	-	-

표 1. 이진 혼돈 수열과 m -수열의 상관 특성

분류	길이: 10000 초기값: 0.4001-0.4100			
	0 평균 비율		1 평균 비율	
	[4] 방식	임계값 방식	[4] 방식	임계값 방식
Triple-Logi.	50.0285	50.0581	49.9715	49.9419
Triple-Cheby.	50.0076	50.0068	49.9924	49.0068
Logi.-Sine-Logi.	49.9675	50.0081	50.0325	49.9919

표 2. 두 가지 이진 맵핑 방식에 대한 이진 혼돈 수열의 균형 특성

분류		Freq.	Run	Rank	DFT
Triple-Logi.	[4]방식	0.73991	0.99146	0.53414	0.35048
	임계값 방식	0.35048	0.5314	0.73391	0.12232
Triple-Cheby.	[4]방식	0.21330	0.73991	0.35048	0.91141
	임계값 방식	0.11538	0.18155	0.00237	0.21330
Logi.-Sine-Logi.	[4]방식	0.73991	0.21330	0.12232	0.91141
	임계값 방식	0.06688	0.91141	0.73991	0.23309
m -수열		0.26224	0.22482	0.00000	0.00032

표 3. 이진 혼돈 수열의 NIST test 결과

Triple-Chebyshev map, 그리고 Logistic map, Sine map, Logistic map을 차례로 연결시킨 Logistic-Sine-Logistic map을 고려한다. 그림 2는 이들의 리아푸노프 지수를 보여준다. 그림에서 볼 수 있듯이 두 개의 단일 맵을 연결시킨 경우보다 향상된 리아푸노프 지수를 갖는 것을 확인했다.

C. 이진 혼돈 수열의 특성 분석

본 논문에서는 연결 혼돈 시스템의 출력 실수 수열을 [4]에서 제안한 이진 맵핑 방식과 임계값 이진 맵핑 방식을 사용하여 이진 수열로 변환한다. [4]에서 제안하는 이진 맵핑 방식은 각 실수 출력을 IEEE 754 표준을 기반으로 52비트 이진 수열로 변환한 뒤 이를 8비트로 잘라서 한번의 반 복에 대해 8비트 이진 수열이 출력된다. 자세한 방법은 [4]의 Section VI에 설명되어있다. 임계값 이진 맵핑 방식은 해당 혼돈 수열의 도메인의 중간값을 임계값으로 설정하여 임계값보다 크면 1로, 작으면 0으로 맵핑하는 방식이다.

표 1에서는 연결 혼돈 수열을 두 가지 이진 맵핑 방식으로 생성된 길이 10000과 100000인 이진수열의 상관 특성과 m -수열의 상관 특성을 보여 준다. 우리가 고려하고 있는 두가지 이진 맵핑 방식에 대한 결과가 매우 유사하여 따로 분류하지 않았다. 표 1에서 볼 수 있듯이 연결 혼돈 수열보다 m -수열의 자기 상관 특성이 약 1dB정도 좋은 성능을 보이며, 길이가

10배 증가 함에 따라 전체적으로 약 6dB정도 좋은 상관특성을 갖는다. 표 2는 두가지 이진 맵핑 방식에 대한 이진 혼돈 수열의 균형 특성을 보여 준다. 실험결과, 모두 좋은 균형 특성을 갖는 것을 확인했다. 표 3은 두가지 이진 맵핑 방식에 대한 이진 혼돈 수열과 m -수열의 NIST test 결과를 보여준다. NIST test의 15개 test 중 Frequency, Run, Rank, DFT test를 선택하여 실험을 진행하였다. 실험 결과, Triple-Chebyshev map은 Rank test를 통과하지 못했으며, m -수열은 Frequency, Run test를 제외한 나머지 test를 통과하지 못했다. 즉, 본 결과에 따르면, Triple-Logistic map과 Logistic-Sine-Logistic map을 이진 맵핑한 이진 수열은 랜덤 수열로 간주 될 수 있다.

III. 결론

본 논문에서는 세 개의 단일 맵을 결합한 연결 혼돈 시스템으로부터 생성된 실수 수열을 두 가지 이진 맵핑 방식을 사용하여 이진 수열로 변환하고 이들의 상관특성을 m -수열과 비교하고, 균형 특성을 분석했다. 또한 NIST test를 통해 연결 혼돈 시스템으로부터 생성된 이진 수열이 m -수열보다 좋은 랜덤 특성을 갖는 것을 확인하였다.

ACKNOWLEDGMENT

이 (성과)는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.RS-2023-00209000).

참 고 문 헌

[1] A. Michaels, “Digital Chaotic Communications,” Georgia Institute of Technology Ph.D dissertation, 2009.

[2] G. Heidari-Bateni, C.D. McGillem, “A chaotic direct sequence spread-spectrum communication system,” *IEEE Trans. Commun.* vol. 42, pp.1524 - 1527, 1994.

[3] G. Ablay, “Lyapunov Exponent Enhancement in Chaotic Maps with Uniform Distribution Modulo One Transformation,” *Chaos Theory Appl.*, vol 4, pp. 45 - 58, 2022.

[4] Y. Zhou, Z. Hua, C. M. Pun, and C. L. P. Chen, “Cascade chaotic system with applications,” *IEEE Trans. Cybern.*, vol. 45, no. 9, pp. 2001 - 2012, Sep. 2015.

[5] Z. Hua, B. Zhou, and Y. Zhou, “Sine chaotification model for enhancing chaos and its hardware implementation,” *IEEE Trans. Ind. Electron.*, vol. 66, no. 2, pp. 1273 - 1284, Feb. 2019.