



Logistic 맵으로 생성된 이진 수열에 대한 분석

최효정, 조현우, 송홍엽
연세대학교 채널코딩연구실



목차



1. 서론
2. Logistic 맵
3. NIST test, 상관특성, 균형특성 분석
4. 결론

- 기존 직접 수열 대역 확산(Direct Sequence Spread Spectrum, DSSS)시스템에 사용하는 PN 코드는 일정한 주기를 가지므로 수열 집합의 크기가 제한적임
- Chaotic 맵은 미세한 초기값의 차이만으로 완전히 다른 실수 값이 도출되는 비선형 함수임
 - 초기값의 변화만으로 주기가 없는 서로 다른 무한한 수열 생성 가능
 - 따라서 DSSS 시스템에서 Chaotic 수열의 사용이 연구되어옴 [1-4]
- 본 논문은 Chaotic 맵 중 하나인 Logistic 맵이 Chaotic 상태일때 출력된 수열의 이진변환을 통해 NIST test, 상관특성 및 균형특성을 분석함

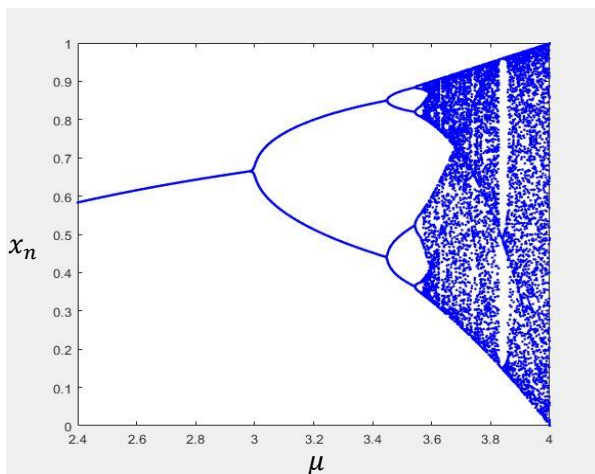
Logistic 맵

❖ Logistic map $x_{i+1} = \mu x_i(1 - x_i)$

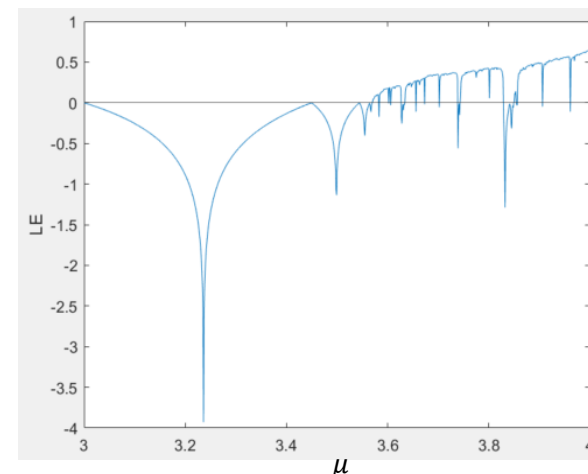
- $1 \leq \mu \leq 4, x_n \in (0, 1)$
- Chaotic map의 초기값에 민감한 정도를 판단하기 위해 Lyapunov Exponent(LE)가 사용되며 다음과 같이 정의됨[7]

$$\lambda = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^N \ln |f'(x_i)|$$

- LE가 양수일때 Chaotic 상태이며, Logistic map은 $3.5699 \leq \mu \leq 4$ 일 때 Chaotic 상태 [5-6]
- Logistic map은 $3.5699 \leq \mu \leq 4$ 구간에 LE가 음수가 되는 일부 "island of stability"가 존재

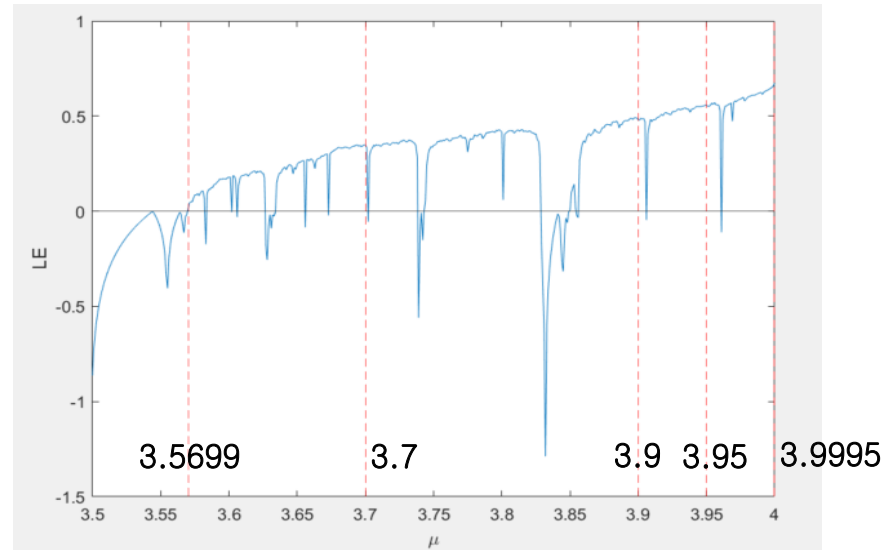


Logistic map의 fractal 파라미터와 x_n 의 관계



fractal 파라미터에 따른 Lyapunov Exponent

❖ 실험환경



- Logistic 맵이 Chaotic 상태인 $\mu = 3.5699, 3.7, 3.9, 3.95, 3.9995, 4$ 고려
- (0,1) 범위의 출력 수열을 0.5를 임계값으로 하여 이진 수열로 변환
- 길이 10230
- 상관특성 및 균형특성 : 초기값 0.40001-0.41까지의 1000개 수열 고려
- NIST test : Frequency, Run, Rank, DFT, Linear Complexity test 고려

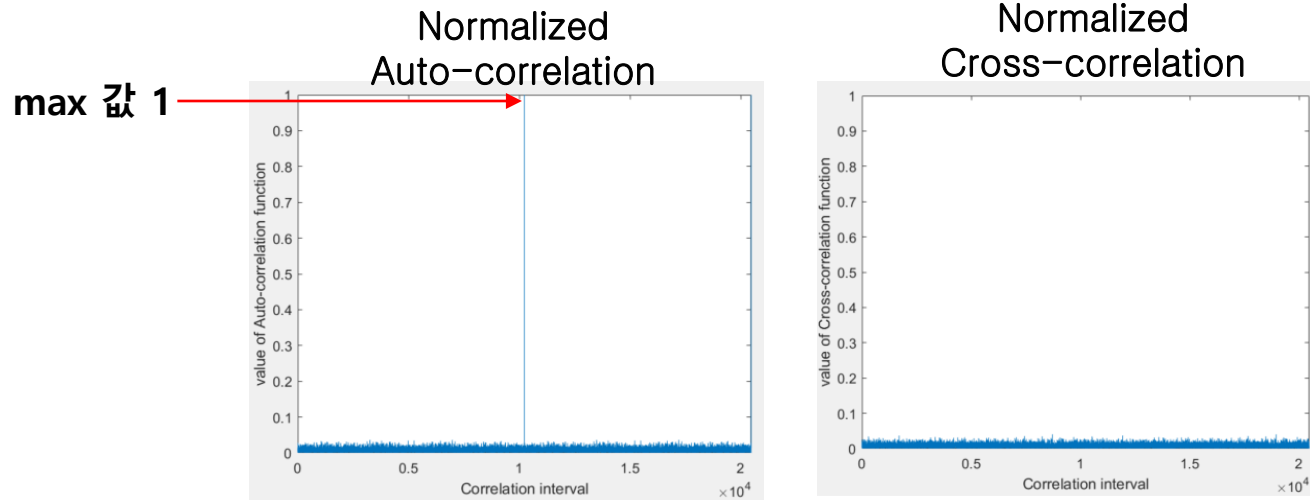
- 모든 test는 수열이 랜덤이라는 귀무가설 하에 P-value(귀무가설에 대한 증거의 강도를 의미)를 계산하여 유의수준 $\alpha = 0.01$ 보다 작다면 랜덤이 아닐 확률이 크다는 것을 의미
- P-value > 0.01이면, 테스트가 99% 신뢰도로 만족됨을 의미

- **Frequency test** : 입력 이진 수열이 랜덤 수열에서 예상되는 '0'과 '1'의 비율과 적절히 일치하는지 판단
- **Run test** : 0-run과 1-run의 수가 랜덤 수열에 대한 기댓값과 유사 여부를 판단
- **Rank test** : 입력 수열 내의 특정 길이의 부분 수열 간 선형 종속성을 판단
- **DFT test** : 랜덤 수열에 벗어나는 주기적 특징이 존재하는지 판단
- **Linear Complexity test** : 랜덤 수열로 간주 될 만큼 충분히 복잡한지 여부를 판단

- 귀무가설 : "입력 수열이 랜덤하다"
- $P\text{-value} < 0.01 \Rightarrow$ 귀무가설 기각

μ	Frequency	Run	Rank	DFT	Linear Complexity
3.5699	0.000000	0.000000	0.000000	0.000000	0.000000
3.7	0.000000	0.000000	0.739918	0.000000	0.213309
3.9	0.000000	0.000000	0.911413	0.000000	0.534146
3.95	0.000000	0.000000	0.739918	0.035174	0.911413
3.9995	0.002043	0.066882	0.350485	0.350485	0.739918
4	0.739918	0.739918	0.534146	0.739918	0.739918

Logistic map의 μ 값 변화에 따른 NIST test 결과



$$\mu = 4$$

μ	초기값 : 0.40001 ~ 0.41			
	Normalized Auto-correlation		Normalized Cross-correlation	
	평균 sidelobe	sidelobe max 평균	평균값	max값 평균
3.5699	0.4313	0.9951	0.4313	0.9988
3.7	0.3061	0.4868	0.3062	0.3421
3.9	0.0201	0.3194	0.0203	0.0636
3.95	0.0452	0.1598	0.0452	0.0846
3.9995	0.0079	0.0385	0.0079	0.0399
4	0.0079	0.0383	0.0079	0.0398

Logistic map의 μ 값 변화에 따른 상관특성

μ	길이 : 10230 초기값 : 0.40001 ~ 0.41	
	0평균 비율	1평균 비율
3.5699	32.77%	67.23%
3.7	22.27%	77.73%
3.9	42.92%	57.08%
3.95	39.41%	60.59%
3.9995	49.40%	50.60%
4	50.09%	49.91%

Logistic map의 μ 값 변화에 따른 균형특성

$\mu = 3.7 \rightarrow 3.5699 \rightarrow 3.95 \rightarrow 3.5 \rightarrow 3.9995 \rightarrow 4$ 순으로 균형특성 우수

- 본 논문은 Chaotic 맵 중 하나인 Logistic 맵이 Chaotic 상태일때 출력된 수열의 이진변환을 통해 NIST 테스트, 상관특성 및 균형특성을 분석함
- 실험 결과
 - NIST test : $\mu = 4$ 인 경우에만 Frequency, Run, Rank, DFT, Linear Complexity test에서 모두 랜덤 수열이라고 판단
 - 상관특성 : $3.95 \leq \mu \leq 4$ 인 경우, μ 값이 클 수록 좋은 상관특성을 가짐
 - 균형특성 : μ 값이 4일 때 가장 좋은 균형특성을 가짐
- Logistic 맵은 $\mu = 4$ 일때 랜덤수열과 유사하며 좋은 상관특성과 균형특성을 갖는 무한한 이진 수열을 생성 할 수 있음



- [1] H. Jiang and C. Fu, "A chaos-based high quality PN sequence generator," International Conference on Intelligent Computation Technology and Automation, pp. 60-64, 20–22 October 2008.
- [2] L. LiHua, HuLi Shi, and GuanYi Ma. "CAPS satellite spread spectrum communication blind multi-user detecting system based on chaotic sequences." Science in China Series G: Physics, Mechanics and Astronomy pp. 339-345, vol. 52, no. 3, 2009.
- [3] A. Michaels, "Digital Chaotic Communications," Georgia Institute of Technology Ph.D dissertation, 2009.
- [4] G. Heidari-Bateni, C.D. McGillem, "A chaotic direct sequence spread-spectrum communication system," IEEE Trans. Commun. vol. 42, pp.1524–1527, 1994.
- [5] 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.
- [6] L. Wang and H. Cheng, "Pseudo-random number generator based on logistic chaotic system," Entropy, vol. 21, no. 10, pp. 960, 2019.
- [7] T. Miyazaki, C. Miyazaki, S. Araki, and S. Uehara, "A Study on the Lyapunov Exponents of Sequences Generated by the Logistic Map over Integers," Proc. of The Sixth International Workshop on Signal Design and its Application in Communications (IWSDA2013), 2013.