Statistical Tests of Some Binary Chaotic and Pseudorandom Sequences

Hyunwoo Cho[1], Hyojeong Choi[1], Daekyung Kim[1], Jae Min Ahn[2], and Hong-Yeop Song[1]
Yonsei University, Seoul, South Korea[1]
Chungnam National University, Daejeon, South Korea[2]

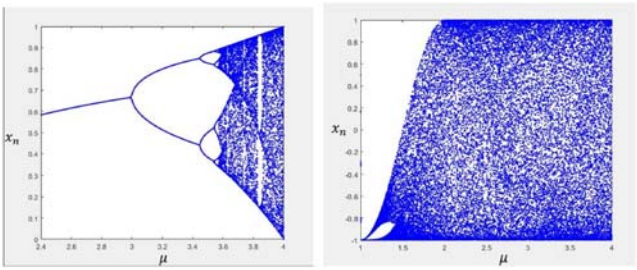
European Navigation Conference 2023

ABSTRACT

Research on generating highly secure PRN sequences in a DSSS systems has been actively conducted. Since the center frequency of a satellite system is public, it is vulnerable to attack. Therefore, research on applying the characteristics of chaos signals is being proposed, in order to compensate for the anti-jamming/spoofing, and robustness to a various noise.

This paper briefly describes some chaotic maps and binary chaotic sequences for GNSS/RNSS in order to improve anti-spoofing ability. We use conventional chaotic maps and two variations maps. We show the results of statistically validating these sequences by NIST SP 800-22.

CLASSIFICATION OF CHAOTIC MAPS



(a) Logistic map (b) Chebyshev map

Chaotic signals generated by nonlinear dynamical systems are non-periodic and pseudo-random like signals. The nonlinear dynamical system consists of a set V of possible states, together with a rule that uniquely determines the next state x_{n+1} in terms of present states x_n.

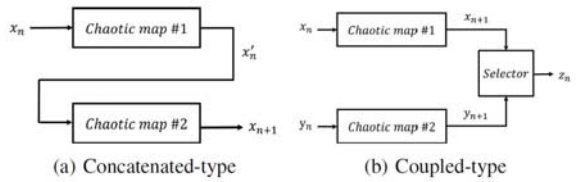
A. Conventional chaotic maps

(a) Logistic map
- $x_{n+1} = \mu x_n(1 - x_n)$
- $1 \le \mu \le 4, x_n \in (0,1)$
- when $\mu \in [3.5699,4]$, the map is chaotic

(b) Chebyshev map
- $x_{n+1} = \cos(\mu \cos^{-1}(x_n))$
- $0 \le \mu \le 4, x_n \in [-1,1]$
- when $\mu \ge 2$, the map is chaotic

(c) Chen's map
- $\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x - xz - cy \\ \dot{z} = xy - bz \end{cases}$
- when $a = 35, b = 3, c = 28$, the map is chaotic

B. Modified chaotic maps



(a) Concatenated-type (b) Coupled-type

Various modified chaotic maps have been proposed to improve based on the vulnerability of one-dimensional chaotic maps, such as implicit-ness, low complexity, and week randomness. The modified chaotic map we investigated was generated by two or more one-dimensional chaotic maps.

NIST STATISTICAL TEST

NIST statistical tests (called NIST SP 800-22) are based on testing hypotheses. That test involves determining whether a particular sequence is random (null hypothesis). For each test, the theoretical reference distribution is determined by mathematical methods and a corresponding probability value (P-value) is calculated that summarizes the strength of evidence for the null hypothesis. A P-value calculated for each test greater than 0.01 means that the test is satisfied with 99% confidence.

STATISTICAL TEST RESULTS

TABLE I: Binary chaotic sequences for NIST statistical testing

Classification	Initial values	Threshold
Logistic Map	$\mu = 4, x_0 = 0.4$	$\theta = 0.5$
Chebyshev Map	$\mu = 4, x_0 = 0.4$	$\theta = 0.0$
Chen's Map	$x_0 = -3, y_0 = 2, z_0 = 20$	-
Concatenated [12]	$\mu = 4, a = 0.4997, x_0 = 0.4$	$\theta = 0.5$
Coupled [13]	$\mu = 4, x_0 = 0.4, x_1 = 0.3$	$\theta = 0.0$

In this paper, chaotic sequences are generated with the initial values shown in TABLE I, and a binary chaotic sequences are generated by binarizing the generated sequence based on the threshold value θ. The number of bitstreams required for the test is set to 10, and the length of the bitstream is set to 10230 (the length of PRN codes in QZSS LEX).

TABLE II: Results of NIST statistical testing (P-value)

Classification	Frequency	Runs	Rank	DFT	Linear Complexity	Cusum(foward)
Logistic Map	0.534146	0.066882	0.350485	0.350485	0.035174	0.350485
Chebyshev Map	0.739918	0.911413	0.122325	0.739918	0.350485	0.739918
Chen's Map	0.350485	0.004301	0.350485	0.534146	0.534146	0.350485
Concatenated-type [12]	0.911413	0.534146	0.534146	0.350485	0.350485	0.122325
Coupled-type [13]	0.213309	0.122325	0.534146	0.350485	0.350485	0.739918
QZSS Kasami	0.350485	0.350485	0.000000	0.000000	0.000000	0.017912

TABLE II shows the NIST SP 800-22 results of the binary chaos sequences generated by the chaos map described above and the Kasami codes used in QZSS LEX. In the case of Kasami codes, randomness is not acceptable for Rank, DFT, and Linear complexity test. It seems to the characteristics of Kasami codes generated by simple LFSR. In the case of Chen's map, it shows that randomness for Runs test is not acceptable. This assumes that analysis for selecting an appropriate threshold is required in the binarization.

CONCLUSION

In this paper, a well-known chaotic maps are briefly summarized, and a binary chaotic sequences of length 10230 are generated and statistically tested using NIST SP 800-22. According to the test results, it was confirmed that the results of the randomness were not acceptable to the Kasami codes used in the existing satellite navigation system.

When this sequence, which is sensitive to the initial value, is applied to the satellite navigation system, high security and tremendous PRN ID are expected. In the future, we plan to study binary chaotic sequences in consideration of highly secure PRN codes in DSSS system based on these results.