Characterization of randomness tests by using tests results of weakly correlated chaotic sequences

Akihiro Yamaguchi
Department of Information and Systems Engineering, Fukuoka Institute of Technology,
3-30-1 Wajiro-higashi, Higashi-ku, Fukuoka, 811-0295, JAPAN

Asaki Saito
Department of Complex and Intelligent Systems, Future University Hakodate
116-2 Kamedanakano-cho, Hakodate, Hokkaido 041-8655, JAPAN
E-mail: aki@fit.ac.jp, saito@fun.ac.jp

Abstract

For the test suite of randomness, a characterization method of the individual tests is proposed. The proposed method is based on the clustering of the results of individual tests for the alternative hypothesis constructed by the weakly correlated chaotic sequences. These sequences are generated by the chaotic true orbit of the piecewise linear chaotic map corresponding to the Markov process. Then we apply our proposed method to the test suite of NIST SP800-22 and try to construct an optimal subset in terms of the distance among tests.

Keywords: randomness test, NIST SP800-22, chaotic true orbit, piecewise linear chaotic map

1. Introduction

High quality pseudo-random number sequences are required in various fields of engineering, and the statistical test of randomness is one of the important subjects. A typical test suite of randomness, e. g. NIST SP800-22[1], is defined as a set of several different kinds of randomness tests. One problem here is that the similarity between the individual tests included in the test suite is not obvious, and it is difficult to make an argument for the optimality of a set of randomness tests. For this problem, Doganaksoy et al. and Sulak et al. studied the independency among tests and the construction of optimal subset of tests based on the experimental results[2,3]. Iwasaki theoretically proved the equivalency among some tests[4]. These studies based on the null hypothesis. To analyze the effectivity of test subsets, the analysis of the statistical power to detect the alternative hypothesis is also necessary.

In this study, we propose a characterization method of randomness tests based on the test results of weakly correlated binary sequences that corresponds to the alternative hypothesis. Theses weakly correlated binary sequences are generated by the piecewise linear chaotic map and its chaotic true orbits[5-8] to guarantee their stochastic properties, exactly[9]. We apply our proposed method to characterize randomness tests included in the test suite of NIST SP800-22 and try to construct the optimal subsets in terms of the distance among tests based on the test results of the alternative hypothesis.

2. Randomness Tests and Definitions

Let the target randomness test suite Γ_{ts} consist of N tests

$$\Gamma_{ts} = \{T_1, T_2, \cdots, T_N\}. \quad (1)$$

For example, the randomness test suite NIST SP800-22 consists of 15 kinds of 188 random number tests.

The null hypothesis H_0 of each randomness test is that the target sequence has the ideal statistical properties of the random number. Let the target sequences of the randomness test be the m binary sequences with length n. In the randomness test $T_i \in \Gamma_{ts}$, each target sequence is tested, and the p-value is obtained from its test statistic.

The p-value corresponds to the probability that the test statistic is equal to or more extreme (farther from H_0) than the test statistic calculated from the target sequence when the null hypothesis H_0 is true. If the p-value is less than the significance level α, H_0 is rejected, otherwise H_0 is accepted, which means the target sequence is judged to be random. As results, we obtain m p-values and decisions of randomness for each test $T_i \in \Gamma_{ts}$.

2.1. *Feature Vector and Distance Matrix*

To characterize the randomness test, we consider the set of different M alternative hypotheses

$$\Lambda_{alt} = \{H_1, H_2, \cdots, H_M\}. \tag{2}$$

For each alternative hypothesis $H_a \in \Lambda_{alt}$, m target sequences that obeys H_a are generated and tested for each $T_i \in \Gamma_{ts}$. Let the obtained p-value of the k-th tested sequence be $p_{T_i}(k; H_a)$ and the mean p-value be $\bar{p}_{T_i}(H_a)$. The feature vector of the randomness test T_i is defined as

$$\bar{v}(T_i; \Lambda_{alt}) = \{\bar{p}_{T_i}(H_1), \bar{p}_{T_i}(H_2), \cdots, \bar{p}_{T_i}(H_M)\}. \tag{3}$$

Then we construct the distance matrix such as

$$D(\Gamma_{ts}; \Lambda_{alt}) = \begin{pmatrix} d_{1,1} & \cdots & d_{1,N} \\ \vdots & & \vdots \\ d_{N,1} & \cdots & d_{N,N} \end{pmatrix}, \tag{4}$$

where $d_{i,j}$ is the distance between two feature vectors,

$$d_{i,j} = \left|\bar{v}(T_i) - \bar{v}(T_j)\right| \tag{5}$$

and $|\cdot|$ denotes the Euclidean norm. Furthermore, we define the total distance of the tests set $\Gamma \subseteq \Gamma_{ts}$ such as

$$td(\Gamma) = \sum_{T_i, T_j \in \Gamma} d_{i,j}. \tag{6}$$

We propose this distance (Eq. (5)) as a measure of the similarity between two tests and the total distance (Eq. (6)) as a measure of the variety of the tests set.

2.2. *Empirical Power of Multiple Testing*

The power of the test $T_i \in \Gamma_{ts}$with the significance level α for the alternative hypothesis $H_a \in \Lambda_{alt}$ is defined as

$$Pw(T_i; H_a, \alpha) = \frac{1}{m}\#\left(\left\{\, k \mid p_{T_i}(k; H_a) < \alpha \right\}\right), \tag{7}$$

where $\#(\cdot)$ denotes the number of elements. The power of the multiple testing with the K tests

$$\Gamma_K = \{T_{i1}, T_{i2}, \cdots, T_{iK}\} \subseteq \Gamma_{ts} \tag{8}$$

with the significance level α for the alternative hypothesis $H_a \in \Lambda_{alt}$ is defined as

$$\begin{aligned} &Pw(\Gamma_K; H_a, \alpha) \\ &\quad = \frac{1}{m}\#\left(\left\{\, k \,\middle|\, \exists T_i \in \Gamma_K : p_{T_i}(k; H_a) < \frac{\alpha}{K} \right\}\right). \end{aligned} \tag{9}$$

Here, the Bonferroni correction is applied to the significance level of each test as α/K to maintain the significance level of the multiple testing that are rejected if even one of the tests in Γ_K is rejected. The Bonferroni correction, however, assumed the independency between tests. Since the some of the tests included in NIST SP800-22 are not independent, the actual significance level is expected to be smaller than α.

3. Construction of Alternative Hypotheses

In this study, we construct alternative hypotheses using weakly correlated chaotic sequences[9]. As an alternative hypothesis, we consider the weakly correlated sequences that has the following stochastic properties. (i) The probability of the length l subsequences are equal to 2^{-l}. (ii) The conditional probability of 0 and 1 following the specified length l subsequences

$$s = 0s_2 \cdots s_l, \qquad s' = 1s_2 \cdots s_l \qquad (s_i \in \{0,1\}) \tag{10}$$

is given as

$$\begin{cases} P(0|s) = P(1|s') = 1/2 + e \\ P(1|s) = P(0|s') = 1/2 - e \end{cases}, \tag{11}$$

where $-1/2 < e < 1/2$. This binary sequence can be generated using the chaotic dynamical system that exactly corresponds to the Markov process. This chaotic dynamical system

$$x_{i+1} = g(x_i) \quad \left(x_i \in [0,1)\right) \tag{12}$$

is given by the piecewise linear map

$$g(x) = \begin{cases} \xi_+ \cdot (x + 2he\Delta) & (x \in I_1\ ) \\ \xi_- \cdot (x - 2(h+1)e\Delta) & (x \in I_2)\ ) \\ 2x & (x \in I_0 \cup I_3) \\ \xi_- \cdot (x - 2^{-1} - 2he\Delta) & (x \in I_5) \\ \xi_+ \cdot (x - 2^{-1} + 2(h+1)e\Delta) & (x \in I_6\ ) \\ 2x - 1 & (x \in I_4 \cup I_7\ ) \end{cases}, \tag{13}$$

where $h = 0,1,\cdots,2^{l-1} - 1$ is a number that corresponds to the subsequence s as binary number, $\xi_{\pm} = 2/(1 \pm 2e)$, $\Delta = 2^{-l}$, $I_i = [a_i, a_{i+1})$, $a_0 = 0$, $a_1 = h\Delta$, $a_2 = (h + \xi_{+}^{-1})\Delta$, $a_3 = (h+1)\Delta$, $a_4 = 2^{-1}$, $a_5 = 2^{-1} + h\Delta$, $a_6 = 2^{-1} + (h + \xi_{-}^{-1})\Delta$, $a_7 = 2^{-1} + (h + 1)\Delta$, and $a_8 = 1$. The example of $g(x)$ is shown in Fig. 1. The shape of $g(x)$ is a partly modified form of the Bernoulli map that generate the ideal random sequences. This dynamical system corresponds to the Markov process shown in Fig. 1(b).

By using the dynamical system (Eq. (12)), we can obtain the binary sequence $s_1 s_2 \cdots s_n$ such as

$$s_i = \begin{cases} 0 & (0 \leq x_i < 1/2) \\ 1 & (1/2 \leq x_i < 1) \end{cases}, \tag{14}$$

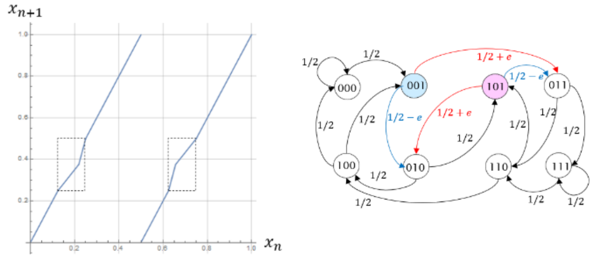
for the given initial point x_0. This binary sequence obeys the stochastic properties (i) and (ii), exactly. In this study, we calculate exact chaotic true orbit[5-8] of the dynamical system (Eq. (12)) and generate binary sequences that obey the alternative hypothesis.

4. Numerical Experiments

In this study, we try to characterize 14 randomness tests included in the NIST SP800-22 test suite. The target randomness tests Γ_{ts} are listed in Table 1. The non-overlapping template matching test and the random excursions, and its variant were excepted.

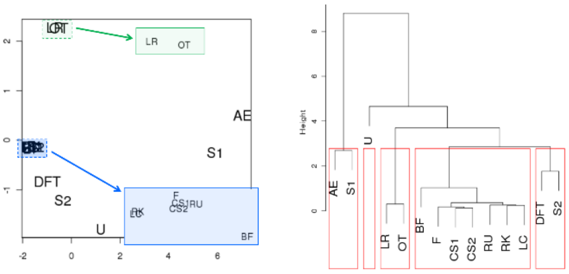
We generated $m = 10^3$ binary sequences with length $n = 10^6$ using Eq. (12) and (14), where $l = 4, \cdots 10$, $e = \pm 4^{-1}, \pm 8^{-1}, \pm 16^{-1}$, and 8 different patterns of s and s' for each l. Totally, $M = 336$ alternative hypotheses were constructed as Λ_{alt}. For the generated binary sequences, we applied the target 14 randomness tests in Γ_{ts} and calculated the p-value for each test and sequence. Then, we obtained the feature vectors (Eq. (3)) and the distance matrix (Eq. (4)). Examples of the cluster analysis based on the feature vector and the distance matrix are shown in Fig. 2. Fig. 2(a) is an example of the two-dimensional representation of the distance relation in $D(\Gamma_{ts}; \Lambda_{alt})$. This figure indicates the similarity among tests, e. g., AE and S1, LR and OT, DFT and S2, and the others except U. These similarities are also confirmed by the results of hierarchical cluster analysis shown in Fig. 2(b). These cluster analyses were performed using R.

The mean power of each test for Λ_{alt} is shown in Table 1. As a result, AE and S1 have high power to detect Λ_{alt}. On the other hand, F, BF, CS, RU, RK and LC could not detect Λ_{alt}. Then, we constructed the optimal subset and the worst subset in terms of the maximization of the total distance (Eq. (6)) with respect to the size of subset $K = 2, \cdots, 7$. Results are shown in Table 2 and Table 3, respectively. Here, $Pw(\Gamma_K)$ is the mean power of the multiple testing Γ_K (Eq. (8)) for Λ_{alt}. For the case of $K = 2$, the most distant pair AE and LC is optimal and the closest pair CS1 and CS2 is worst. The obtained optimal subsets are consistent with the results of the cluster analysis shown in Fig. 2. These results suggest that our method can construct the optimal subset with low similarity. However, our method cannot distinguish several tests that have low sensitivity to the proposed alternative hypothesis. To improve this problem, a more varied set of alternative hypotheses is necessary.



(a) (b)

Fig. 1. (a) An example of the piecewise linear chaotic map and (b) corresponding Markov process for the case that $l = 3$, $h = 1$ $(s = 001)$, and $e = 1/4$. The rectangular part of (a) is modified from Bernoulli map.



(a) (b)

Fig. 2. Examples of the cluster analysis based on the distance matrix $D(\Gamma_{ts})$. (a) A two-dimensional representation of $D(\Gamma_{ts})$ using the classical multidimensional scaling. Rectangular are magnifications of dense areas. (b) A cluster tree obtained by the hierarchical cluster analysis.

5. Conclusion

In this study, we proposed the characterization method of randomness tests and applied to 14 randomness tests in NIST SP800-22. As results, we obtained the optimal subsets in terms of the maximization of the total distance among tests. The characterization of all tests in NIST

Table 1. The mean power of randomness tests in Γ_{ts} for the constructed alternative hypotheses Λ_{alt}.

Target tests Γ_{ts} and abbreviations		$Pw(T_i)$
Frequency Test	F	0.010
Block Frequency Test	BF	0.012
Cumulative Sums Test	CS1	0.010
	CS2	0.010
Runs Test	RU	0.010
Longest Run Test	LR	0.122
Matrix Rank Test	RK	0.010
DFT Test	DFT	0.041
Overlapping Template Matching Test	OT	0.124
Universal Test	U	0.198
Approximate Entropy Test	AE	0.878
Serial Test	S1	0.628
	S2	0.090
Linear Complexity Test	LC	0.010

SP800-22 and the construction of other types of alternative hypothesis are our next future works.

Acknowledgements

This work was supported by JSPS KAKENHI Grant Numbers 16KK0005, 17K00355. The computation was carried out using the computer resources offered under the category of General Projects by the Research Institute for Information Technology, Kyushu University.

References

1. L. E. Bassham et al., NIST SP800-22 Rev. 1a: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST CSRC, 2010.
2. A. Doganaksoy, et al., Mutual correlation of NIST statistical randomness tests and comparison of their sensitivities on transformed sequences, Turkish Journal of Electrical Engineering & Computer Sciences, 25, pp. 655-665, 2017.
3. F. Sulak, et al., On the independence of statistical randomness tests included in the NIST test suite, Turkish Journal of Electrical Engineering & Computer Sciences, 25, pp. 3673-3683, 2017.
4. A. Iwasaki, Study of the relationships among some tests in NIST SP800-22 (in Japanese), Proc. of the 2020 JSIAM Annual Meeting, pp.46-47, JSIAM, 2020.
5. A. Saito and S. Ito, Computation of true chaotic orbits using cubic irrationals, Physica D, 268, pp. 100–105, 2014.
6. A. Saito, et al., True orbit simulation of piecewise linear and linear fractional maps of arbitrary dimension using algebraic numbers, Chaos 25, 063103, 2015.

Table 2. The optimal subset that maximizes the total distance.

K	$td(\Gamma_K)$	$Pw(\Gamma_K)$	Γ_K that maximize the total distance $td(\Gamma_K)$.
2	8.8	0.865	AE, LC
3	20.3	0.864	BF, LR, AE
4	37.9	0.860	BF, LR, AE, S1
5	59.4	0.857	BF, LR, U, AE, S1
6	84.4	0.854	BF, LR, U, AE, S1, LC
7	111.2	0.852	BF, LR, U, AE, S1, S2, LC

Table 3. The worst subset that minimizes the total distance.

K	$td(\Gamma_K)$	$Pw(\Gamma_K)$	Γ_K that minimize the total distance $td(\Gamma_K)$.
2	0.1	0.007	CS1, CS2
3	0.5	0.005	F, CS1, CS2
4	1.4	0.006	F, CS1, CS2, RK
5	2.6	0.007	F, CS1, CS2, RU, RK
6	4.2	0.008	F, CS1, CS2, RU, RK, LC
7	9.6	0.009	F, BF, CS1, CS2, RU, RK, LC

7. A. Saito and A. Yamaguchi, Pseudorandom Number Generation using Chaotic True Orbits of the Bernoulli Map, Chaos, 26, 063112, 2016.
8. A. Saito and A. Yamaguchi, Pseudorandom Number Generator based on the Bernoulli Map on Cubic Algebraic Integers, Chaos, 28, 103122, 2018.
9. A. Yamaguchi and A. Saito, Construction of the Markov process by using chaotic true orbit of piecewise linear map toward the independence analysis of randomness tests (in Japanese), Proc. of the 2017 JSIAM Annual Meeting, pp.255–256, JSIAM, 2017.

Authors Introduction

Dr. Akihiro Yamaguchi

He is a Professor of the Department of Information and Systems Engineering at Fukuoka Institute of Technology. He received his doctor degree in Science from Hokkaido University in 1997. His research interest includes neural networks and applications of chaotic systems.

Dr. Asaki Saito

He is a Professor of Department of Complex and Intelligent Systems at Future University Hakodate in Japan. He received his Ph.D. from University of Tokyo in 1999. His research interest includes true orbit computation of dynamical systems and learning dynamics.