情報処理学会論文誌　数理モデル化と応用　Vol.6　No.1　57–63 (Mar. 2013)

# RMTテストの性能検証—NIST乱数検定との比較

三賀森 悠大[1,a)]　楊 欣[1]　糸井 良太[1]　田中 美栄子[1,b)]

受付日 2012年4月19日，再受付日 2012年6月7日，
採録日 2012年7月27日

**概要**：我々が以前に提案した，RMT との比較による乱数度計測法，すなわち RMT テストの誤差基準を NIST 検定との比較によって再考察した結果を報告する．様々な乱数度の数列を用意するため，完全規則列から出発してそれにシャッフルをかけることにより，異なる乱数度のデータ列を作成し，RMT テストによりその乱数度を測定するとともに，15 種類の検定法を持つ NIST 乱数検定の結果を用いて RMT テストとの比較実験を行った．その結果，NIST 乱数検定で良い乱数と見なせるシャッフル度を持つデータ列では，RMT テストによる誤差が 0.60%以下となり，先に擬似乱数列や物理乱数を用いて作成した乱数度評価基準よりも厳しい基準となる．ただし先の結果は多数のデータのサンプル平均であること，また今回は NIST 乱数検定に掛けるために 2 進列で検証を行っていることや，両テストにおけるデータ列の制限などを考慮すると，矛盾しているとまではいえないが，RMT テストの誤差基準値の選定に対する新たな知見を得たといえる．

**キーワード**：乱数度評価基準，RMT テスト，NIST 乱数検定，RMT 定量評価，モーメント

# Performance Verification of RMT-test — Comparison with the NIST Randomness Test

Yuta Mikamori[1,a)]　Xin Yang[1]　Ryota Itoi[1]　Mieko Tanaka-Yamawaki[1,b)]

Received: April 19, 2012, Revised: June 7, 2012,
Accepted: July 27, 2012

***Abstract:*** In this article, we report a new result of the error limit to be used for the RMT test, which we have proposed earlier in order to measure the randomness of one-dimensional data sequence based on the comparison to the theoretical value derived by the random matrix theory (RMT). This new limit is obtained by comparing the error level of the RMT-test to the result of the NIST test. We prepared data sequences of various levels of randomness by shuffling a regular sequence many times. The result shows that the RMT error must be less than 0.60% in order to satisfy the requirement of the NIST test. This new limit is severer than the limit that we have obtained in the study of pseudo-random sequences. Although we need to consider the fact that the previous limit was the result of averaging over many samples, and the NIST test is applied only binary sequences and the conditions to apply the two tests are not the same, this result suggests us to reconsider the error limit of the RMT test in more detail.

***Keywords:*** evaluation criteria of randomness, RMT-test, NIST randomness test, RMT quantitative test, moment

## 1. 序章

### 1.1 はじめに

乱数度とは，いかに数の並び方の予測や再現が難しいかの具合で，これが高いほど良い乱数とされる．しかし実際にデータ列の乱数度の測定をしようとすると，JIS で推奨

[1] 鳥取大学大学院工学研究科情報エレクトロニクス専攻
Department of Information and Electronics, Graduate School of Engineering, Tottori University, Tottori 680–8552, Japan
[a)] s082053@ike.tottori-u.ac.jp
[b)] mieko@ike.tottori-u.ac.jp

される手法 [1] や，暗号分野で使われる NIST ツール [2] のように，複数の基準を併用するものが多い．さらにデータ形式に対しても，2 進数，整数，実数のいずれかを指定し，データ長も決められていて使いにくいことが多い．

以上のことを改善するため，我々はランダム行列理論（Random Matrix Theory：以下 RMT）を乱数度評価に応用した，RMT テストを提案した [3], [4]．RMT テストは，単一の評価基準であらゆるデータ形式の数列の乱数度を，定量的に測定することができる便利な手法である．問題点としては，第 1 に，データとして非常に長い数列を必要とするが，社会科学や医学の分野に応用する際に，十分なデータ数の確保が困難な場合があることがあげられる．また，第 2 には，定量評価基準を定める際に，乱数度のかなり高いことが自明の，擬似乱数列や物理乱数列を用いたため，乱数度が高いと判定する基準値選定が局所的には非常に小さな値であるが，サンプル平均の誤差のため結果として大きく見えるものであったことがあげられる．

これまでに，擬似乱数列，物理乱数列，およびそれらから作成した対数収益列を用いて検証を行い，乱数度の高い数列とその対数収益列とでは乱数度に大きな違いがあるという結果を得た．しかし，これらの中間にある，擬似乱数列や物理乱数列よりは乱数度が低いが，対数収益列よりは乱数度が高い，という場合の評価があまりよく分からなかった．原因はそのような乱数度を持つデータを入手できなかったことにある．

### 1.2　研究目的

RMT テストによって評価され，本当にランダム性の高い乱数列と見なされているのであれば，その乱数列は様々な種類の検定にかけても合格と判断されるはずである．本研究ではそこに着目し，RMT テスト以外の乱数検定法として，NIST 乱数検定法との比較を行うことで RMT テストの性能検証を行う．NIST 乱数検定は，「NIST Special Publication 800-22（以下 NIST SP 800-22）」という乱数検定ツールを用いる．このツールは暗号分野で広く使われており，含まれている 15 種類の検定すべてに合格すれば，暗号としての使用に適していることになる．比較実験により，NIST が定めた 15 種類の乱数検定（以下 NIST 乱数検定）[2] の基準で乱数度が高くなり始める点を RMT テスト結果から定めることで，RMT テストを多面的に評価することを目的とする．

本稿では，完全規則列にシャッフルをかけることにより，様々な乱数度を持つと予想されるデータを作成する．RMT テストによりその乱数度を測定するとともに，NIST 乱数検定との比較を行い，RMT テストの評価基準値について再考することにしたい．

## 2.　RMT と乱数度評価

### 2.1　RMT の概要

RMT は半世紀以上前から原子核物理学の分野で応用されてきた [5] が，ここでは Laloux ら [6]，Plerou ら [7], [8] などにより株式市場に応用された文脈に基づいて，N 個の等長（長さ L とする）時系列間の相関行列の固有値分布を求め，これを $Q{=}L/N{>}1$ を定数パラメータとして $L \to \infty$，$N \to \infty$ の極限で RMT から導かれた固有値分布の理論式と比較することで，ランダム性を測る．ここに現れるパラメータは

$$Q = \frac{L}{N} \tag{1}$$

のみであり，固有値 $\lambda$ の分布の最大値 $\lambda_+$ と最小値 $\lambda_-$ は

$$\lambda_\pm = 1 + \frac{1}{Q} \pm 2\sqrt{\frac{1}{Q}} \tag{2}$$

を使って，固有値分布は以下の式で表される．

$$P_{RMT}(\lambda) = \frac{Q}{2\pi\lambda}\sqrt{(\lambda_+ - \lambda)(\lambda - \lambda_-)} \tag{3}$$

### 2.2　乱数度評価の手法

#### 2.2.1　乱数データの扱い方

データ長 $L$ の乱数データを $N$ 個用意する．本研究ではあらかじめ 1 つの乱数列を生成しておき，**図 1** のようにデータ長 $L$ で区切って $N$ 分割することにより，相関行列を作成するために必要なデータを得る．行列を作成する際，$i$ 行 $j$ 列要素 $A_{i,j}$ は，数列の $(i{-}1) \times L{+}j$ 番目の数字となる．

#### 2.2.2　相関行列作成

前項で用意した乱数列データを**図 2** のように並べ，$N$ 行 $L$ 列の行列を作成する．

次に，この行列を行ごとに

$$g_{i,j} = \frac{A_{i,j} - \langle A_i \rangle}{\sqrt{\langle {A_i}^2 \rangle - \langle A_i \rangle^2}} \tag{4}$$

によって平均 0，分散 1 となるよう正規化し，$N$ 行 $L$ 列の


**図 1**　乱数列の分割方法
**Fig. 1**　Method of dividing the random number sequence.

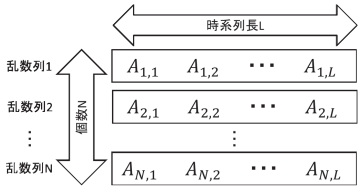



**図 2**　乱数列データの並べ方
**Fig. 2**　Arrangement of the data sequence of random numbers.

データ行列

$$G = \begin{bmatrix} g_{1,1} & \cdots & g_{1,L} \\ \vdots & \ddots & \vdots \\ g_{N,1} & \cdots & g_{N,L} \end{bmatrix} \tag{5}$$

を作成する．相関行列 $C$ は $G$ とその転置行列の積として

$$C = \frac{1}{L} G G^T \tag{6}$$

を使って求められ，$N$ 行 $N$ 列の対称行列となる．

#### 2.2.3　定量評価

長さ 100 万のデータ列を $N$ 本に等分割してそれらの内積から相関行列を作成する．先行研究 [3], [4] により $N$=500 以上であれば十分に RMT 公式が使えることが分かっているので，今回は，$N$=500，$L$=2000 の条件のもとで乱数度評価を行い，モーメントの理論値と実測値との誤差により，乱数度を数値で判定する．以下に乱数度評価の方法を述べる．

最初に，相関行列 $C$ を $k$ 乗し，その対角要素の平均をとることにより

$$m_k = \frac{1}{N}\sum_{i=1}^{N}(C^k)_{i,i} = \frac{1}{N}\sum_{i=1}^{N}{\lambda_i}^k \tag{7}$$

によって $k$ 次モーメントの実測値 $m_k$ を求める．次に，$k$ 次モーメントの理論値を

$$\mu_k = \int_{\lambda_-}^{\lambda_+} \lambda^k P_{RMT}(\lambda) d\lambda \tag{8}$$

によって計算すると，パラメータ $Q$ の関数として以下のように書ける [3], [4].

$$\mu_1 = 1 \tag{9}$$

$$\mu_2 = 1 + \frac{1}{Q} \tag{10}$$

$$\mu_3 = 1 + \frac{3}{Q} + \frac{1}{Q^2} \tag{11}$$

$$\mu_4 = 1 + \frac{6}{Q} + \frac{6}{Q^2} + \frac{1}{Q^3} \tag{12}$$

$$\mu_5 = 1 + \frac{10}{Q} + \frac{20}{Q^2} + \frac{10}{Q^3} + \frac{1}{Q^4} \tag{13}$$

$$\mu_6 = 1 + \frac{15}{Q} + \frac{50}{Q^2} + \frac{50}{Q^3} + \frac{15}{Q^4} + \frac{1}{Q^5} \tag{14}$$

乱数度は

$$\text{誤差 (\%)} = \left(\frac{m_k}{\mu_k} - 1\right) \times 100 \tag{15}$$

により数値化する [3], [4].

## 3.　NIST 乱数検定

RMT テストの客観的評価のため，別手法の結果と比較する．本稿では比較対象として，米国国立標準技術研究所（NIST）で開発された NIST SP 800-22 を使用する．NIST SP 800-22 は，複数の検定法からなる米国標準の統計的乱数検定であるが，1 つの数列を読み込むことで，様々な検定をまとめて行うことができる．NIST のホームページにおいて，ソースコードが提供されている [2]．また，NIST 乱数検定は暗号として使用できるかどうかの検定として広く使用されている．

NIST SP 800-22 では，0 と 1 からなる ASCII 形式の乱数データを対象として，乱数の検定を行う．採用されている検定法は，以下の 15 種類である．

- 1 次元度数検定（Frequency）
- ブロック単位の頻度検定（BlockFrequency）
- 累積和検定（CumulativeSums）
- 連の検定（Runs）
- ブロック単位の最長連検定（LongestRun）
- 2 値行列ランク検定（Rank）
- 離散フーリエ変換検定（FFT）
- 重なりのないテンプレート適合検定（NonOverlappingTemplate）
- 重なりのあるテンプレート適合検定（OverlappingTemplate）
- Maurer のユニバーサル統計検定（Universal）
- 近似エントロピー検定（ApproximateEntropy）
- ランダム偏差検定（RandomExcursions）
- 種々のランダム偏差検定（RandomExcursionsVariant）
- 系列検定（Serial）
- 線形複雑度検定（LinearComplexity）

NIST SP 800-22 によって検定する数列の長さとしては 100 万が推奨されている [9], [10]．また，統計的に有意な結果を得るためには，少なくとも 55 サンプルの数列を用意する必要がある [10]．これは，サンプル数または 1 サンプルあたりのデータ長が過度に少なければ，合否判定が不可能な検定が存在するからである．

## 4.　検証に用いる乱数データ

### 4.1　乱数列生成の目的

NIST 乱数検定により良い乱数と見なされる基準を探るにあたり，RMT テストで求めた乱数度と照合して解析を行うため，様々な乱数度の数列データを用意したい．しかし，擬似乱数などコンピュータによって生成される乱数列は，RMT テストによれば多くのものがランダム性の高い，良い乱数と判断される．また，人間が自分で作成するとしても，検定に使用すべきデータ数が非常に多いために，手間の問題が出るなど，普通では手に入りにくいという問題点がある．

そこで，ランダム性がきわめて低い規則的な数列データをシャッフルさせることにより，徐々に乱数度を高くしつ

つ，2 種類の評価の比較を行う．NIST 乱数検定の条件に合わせるため，本研究で扱うデータとして，全 100 万の数列を 55 サンプル用意する．コンピュータによる生成およびシャッフル作業により，元の規則的な数列から研究の目的に合った乱数列を高速で用意することが可能になる．5.1 節では，RMT テストにより，実際にシャッフル回数に応じて乱数度に変化が生じることを確認する．

### 4.2　シャッフル

シャッフルを行う前のデータ，つまり初期の数列データとして，0 と 1 がそれぞれ 50 個ずつ交互に並べられた数列を用意する．このとき，データ長 100 万，かつ 0 と 1 のそれぞれの度数がすべて均一の規則的な数列が構成される．

数列データにある全 100 万の要素の中から 2 個をそれぞれランダムに選び，お互いの順番を入れ替える．この作業を 1 回としてカウントし，繰り返す．シャッフル作業が一定の回数（$N$ 回とおく）に達すれば，シャッフル $N$ 回分の乱数列として RMT テストおよび NIST 乱数検定で扱う．

データ作成の例として，シャッフル 100 万回，200 万回，300 万回分の乱数列をそれぞれ 1 つずつ作成する場合の手順を以下に示す．

(1) 初期の数列データを 100 万回シャッフルし，終了時点の数列の並びをシャッフル 100 万回分のファイルに出力．
(2) 100 万回シャッフル終了時点の並びの数列をさらに 100 万回シャッフルする．それにより，元の規則的な数列を 200 万回シャッフルしたことになる．終了時点の数列の並びをシャッフル 200 万回分のファイルに出力．
(3) 200 万回シャッフル終了時点の並びの数列をさらに 100 万回シャッフルする．それにより，元の規則的な数列を 300 万回シャッフルしたことになる．終了時点の数列の並びをシャッフル 300 万回分のファイルに出力．

以上のような流れでファイル出力を行うことにより，1 つのサンプルのシャッフルによる乱数度の変遷を考慮した乱数データを入手できる．上記の (1)〜(3) の作業は，必要サンプル数に相当する 55 回分行う．

## 5.　実験

### 5.1　RMT テストによる結果

前章で作成する数列の乱数度を RMT テストで調査することにより，シャッフル回数に応じた乱数度の変化を確認する．

シャッフル回数 100 万〜500 万回での，それぞれの終了時点の乱数列の定量評価結果を**図 3** のグラフにまとめる．ここで，縦軸の数値は式 (15) により求めた誤差の数値（絶対値）であり，55 サンプルの平均値を示す．RMT テストの結果は，誤差の値が 0 に近付くほど乱数度が高いと定義する．以降，RMT テストの結果グラフの縦軸ラベルでは，

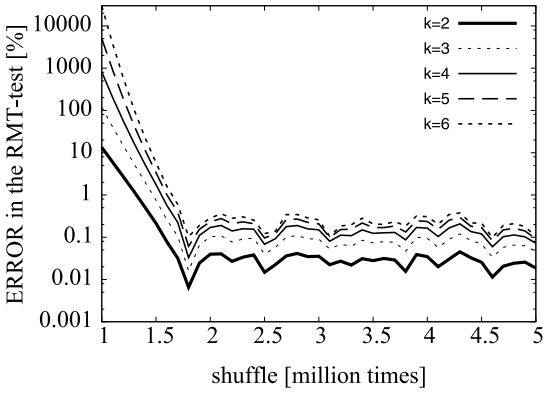



**図 3**　シャッフルによる誤差（k=2〜6）の推移
**Fig. 3**　Changes of ERROR due to shuffling (k=2〜6).

誤差を「ERROR」と表す．

なお，1 次モーメントについては，どのシャッフル回数においても限りなく誤差 0%に近似しているので省略する．

図 3 を見ると，シャッフル回数が少ない場合では，他の回数の場合と比べて誤差が膨大な数値である．しかし，シャッフル回数の増加とともに誤差の絶対値が減少し，一定の誤差以下で遷移していることが分かる．

よって以上のことから，RMT テストを用いて，シャッフル回数の増加に応じて乱数度が高くなっていることが確認できた．

### 5.2　NIST 乱数検定による結果

NIST SP 800-22 では，検定対象は 0 と 1 からなる ASCII 形式の乱数データという制約がある．もし 0 と 1 以外の数値が含まれている場合，出現範囲の中央値を境目にして，乱数データを 0 と 1 のデータに変換して扱う．例として，データがすべて整数で出現範囲が 0〜99 の場合，中央値が 49.5 なので，0〜49 を 0，50〜99 を 1 として変換する．NIST 乱数検定の全検定においては，Proportion 評価を行ったうえで合否を判断する．Proportion 評価とは，乱数列の全サンプル中，その検定に合格したサンプル数の比率を見ることである．比率が一定基準以上であれば，検定に総合的に合格したと判断される．

シャッフル回数 100 万〜500 万回での，それぞれの終了時点の乱数列の検定結果を**表 1** にまとめる．ここで，NIST 乱数検定に用いたデータは，5.1 節の定量評価で使用した乱数列データと同一のものである．

シャッフル回数 170 万回以降を 10 万回区切りで見ると，15 種類すべての検定に合格して Proportion 評価で合格と見なされたものや，特定の検定であと数サンプルだけが検定に合格しなかったため，基準を満たさず Proportion 評価で不合格と見なされたものばかりである．

### 5.3　比較

RMT テストと NIST 乱数検定の結果を比較するため，先

表 1　NIST 乱数検定における結果
**Table 1**　Result in the NIST randomness test.

| シャッフル数（万回） | 合格率 | シャッフル数（万回） | 合格率 |
|---|---|---|---|
| 100 | 5/15 | 310 | 15/15 |
| 110 | 7/15 | 320 | 14/15 |
| 120 | 7/15 | 330 | 14/15 |
| 130 | 7/15 | 340 | 14/15 |
| 140 | 7/15 | 350 | 15/15 |
| 150 | 10/15 | 360 | 14/15 |
| 160 | 13/15 | 370 | 14/15 |
| 170 | 14/15 | 380 | 15/15 |
| 180 | 14/15 | 390 | 15/15 |
| 190 | 15/15 | 400 | 15/15 |
| 200 | 15/15 | 410 | 15/15 |
| 210 | 15/15 | 420 | 15/15 |
| 220 | 14/15 | 430 | 15/15 |
| 230 | 15/15 | 440 | 15/15 |
| 240 | 15/15 | 450 | 15/15 |
| 250 | 14/15 | 460 | 14/15 |
| 260 | 15/15 | 470 | 15/15 |
| 270 | 14/15 | 480 | 15/15 |
| 280 | 15/15 | 490 | 15/15 |
| 290 | 14/15 | 500 | 15/15 |
| 300 | 15/15 | | |

ほどの 5.1 節および 5.2 節での検証結果を**表 2** にまとめる．RMT テストの結果として，$k$=2∼6 の中でも，6 次モーメントを採用する．その理由は，6 次モーメントは $k$=2∼6 の中でも誤差が最も大きくなりやすく，他と比べて特徴が出やすいためである．表 2 の表示の形式としては，図 1 の誤差の絶対値をとってソートし，NIST 乱数検定結果との比較を示している．表中に同じ誤差の値が複数出ることがあるが，シャッフル回数が異なるため，偶然同じ誤差の列が生成されただけで，数列の中の要素は別物である．

表 2 より，NIST 乱数検定の結果が，誤差の絶対値 0.60%（太字）以下のすべての乱数列において合格率 14/15 以上と高いのに対し，誤差が大きい（乱数度が低い）乱数列ほど，合格率が低いことが分かる．

### 5.4　シンボル数による違い

前節では，NIST 乱数検定の検定対象が 0 と 1 から構成されるデータであることから，主に 0 と 1 からなるシンボル数 2 という条件で RMT テストと NIST 乱数検定との比較を行った．さらにここでは，シンボル数の違いによって 2 種類の検定法による結果に差が生じるかどうかについても検証を行う．そのため，初期データとして，0∼99 の 100 個を昇順に並べていき，その数列 1 セットを 1 万個連結させた長さ 100 万のデータに対してもシャッフルを行い，テストデータを作成した．その検証結果を，5.1 節の結果と照合して**図 4** に示す．結果の比較にはそれぞれの 6 次モーメントを使用した．

表 2　RMT テスト（左）と NIST 乱数検定（右）の結果
**Table 2**　Result of RMT-test (left) and NIST randomness test (right).

| RMT テスト 誤差 [%] | NIST 乱数検定 合格率 | RMT テスト 誤差 [%] | NIST 乱数検定 合格率 |
|---|---|---|---|
| 29582.88 | 5/15 | 0.25 | 15/15 |
| 3803.87 | 7/15 | 0.24 | 14/15 |
| 572.09 | 7/15 | 0.22 | 15/15 |
| 101.80 | 7/15 | 0.21 | 15/15 |
| 22.27 | 7/15 | 0.21 | 15/15 |
| 5.79 | 10/15 | 0.21 | 15/15 |
| 1.60 | 13/15 | 0.20 | 15/15 |
| **0.60** | **14/15** | 0.20 | 14/15 |
| 0.38 | 15/15 | 0.20 | 14/15 |
| 0.36 | 15/15 | 0.19 | 15/15 |
| 0.35 | 15/15 | 0.19 | 15/15 |
| 0.34 | 15/15 | 0.18 | 14/15 |
| 0.34 | 14/15 | 0.18 | 15/15 |
| 0.32 | 15/15 | 0.18 | 15/15 |
| 0.31 | 15/15 | 0.14 | 15/15 |
| 0.30 | 15/15 | 0.12 | 14/15 |
| 0.29 | 14/15 | 0.11 | 15/15 |
| 0.28 | 15/15 | 0.10 | 15/15 |
| 0.28 | 14/15 | 0.10 | 14/15 |
| 0.28 | 14/15 | 0.10 | 14/15 |
| 0.26 | 15/15 | | |

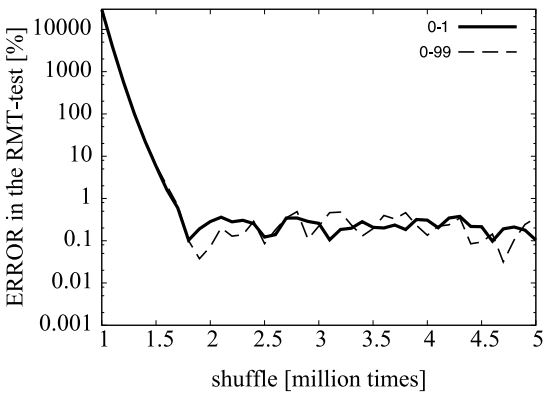



図 4　シャッフルによる誤差の推移（シンボル数 2，100 の場合）
**Fig. 4**　Changes of ERROR due to shuffling (2 and 100 if the number of symbols).

図 4 より，両者とも多少の誤差はあるものの，100 万回から一定回数の間で誤差の単調減少が見られる点，およびシャッフル回数が増えるにつれて誤差が 1%以下で遷移するようになるという点に変化はなかった．

また，0-1 データに関して，初期データを変えた数列に対してもシャッフルを行い，検証した．RMT テストおよび NIST 乱数検定による結果をそれぞれ**図 5**，**図 6** に示す．図 6 の縦軸の数値は，NIST SP 800-22 に含まれる検定全 15 種類のうちの合格検定数を示し，この値が大きいほど乱数度が高いと定義する．合格検定数を，図 6 の縦軸

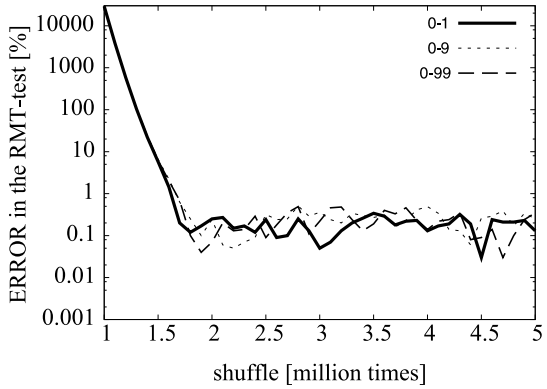



図 5　RMT テストにおける結果
**Fig. 5**　Result in the RMT-test.

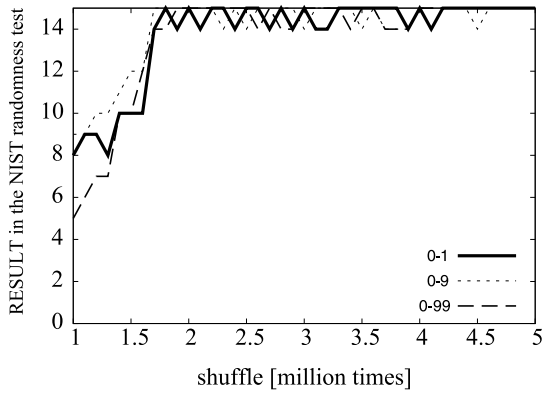



図 6　NIST 乱数検定における結果
**Fig. 6**　Result in the NIST randomness test.

ラベルでは「RESULT」と表す．

シンボル数は 2，10，100 でそれぞれ検証している．初期データは，シンボル数 2 の場合は 0 と 1 が交互に 1 個ずつ並べられた数列，シンボル数 10 の場合は 0〜9 を昇順に並べたものを 10 万個連結させた数列，シンボル数 100 の場合は 0〜99 を昇順に並べたものを 1 万個連結させた数列となっている．

図 5，図 6 においても，RMT テストにより，一定回数までの誤差の単調減少，および 1%以下での誤差の遷移に変化がないことが確認できる．また，NIST 乱数検定により，一定回数までの合格検定数の単調増加，および一定回数以降の結果の安定性に変化がないことが確認できる．

### 5.5　乱数度が高い例・低い例

擬似乱数および物理乱数を用いて検証した例を**表 3** に示す．RMT テストでは 6 次モーメントの誤差を用いる．以下の乱数は先行研究により，乱数度が高いとされている [3], [4].

また，対数収益をとることによって乱数度を低くした数列についても比較を行った．比較結果を**表 4** に示す．

表 3，表 4 を比較すると，対数収益をとった場合の方が，RMT テストから求まる乱数度低下と同時に，NIST 乱数検定における合格率も低下していることが分かる．実際に，5.3 節での比較結果でも同様の傾向が見られる．このことから，NIST 乱数検定の結果は，RMT テストの結果と並行していると考えられる．

表 3　擬似乱数（LCG）および物理乱数 3 種類を用いた比較
**Table 3**　Comparison using Pseudo-random number (LCG) and Three types of physical random number.

| 乱数の種類 | RMT テスト誤差 [%] | NIST 乱数検定合格率 |
|---|---|---|
| LCG による擬似乱数 | −0.2831 | 14/15 |
| 日立製作所製物理乱数 | −0.1597 | 15/15 |
| 東芝製物理乱数 | 0.0026 | 15/15 |
| 東京エレクトロンデバイス製物理乱数 | −0.1194 | 15/15 |

表 4　対数収益をとった数列の比較
**Table 4**　Comparison of log-return sequences.

| 乱数の種類 | RMT テスト誤差 [%] | NIST 乱数検定合格率 |
|---|---|---|
| LCG による擬似乱数 | 99.3042 | 5/15 |
| 日立製作所製物理乱数 | 98.8686 | 5/15 |
| 東芝製物理乱数 | 99.2463 | 5/15 |
| 東京エレクトロンデバイス製物理乱数 | 98.7580 | 5/15 |

## 6.　考察

前章により，RMT テストと NIST 乱数検定の結果の類似性を確認することができた．これにともない，本実験の結果から，「NIST 乱数検定を考慮に入れた場合の良い乱数」の基準に対する知見を得た．

乱数度の向上にもかかわらず，誤差 0.60%以下で合格検定数が 14，15 で遷移していることが表 2 から分かる．調査の結果，シャッフル 170 万回，180 万回の場合は「連の検定」で不合格であったが，それ以降の回数での合格率 14/15 の乱数列すべてにおいて「重なりのないテンプレート適合検定」が不合格と判定されていることが判明した．これより，重なりのないテンプレート適合検定と RMT テストで求めた乱数度との関連性が，NIST 乱数検定の他の検定 14 種類に比べて薄いと考えられる．

先行研究では，RMT テストにより求めた 6 次モーメントと RMT 理論値の誤差の値が 5%を下回れば，良い乱数として判断した．しかし，前の段落で述べたことと，5.3 節の結果が類似していることを考慮すると，RMT テストで求めた誤差の値が 0.60%を下回っていれば，NIST 乱数検定の基準で良い乱数として判断できると考えられる．

また，シャッフル回数を増やして乱数度を向上させた乱数列ほど，NIST が定めた乱数検定で合格しているものが多いことが分かる．実際，NIST が定めた乱数検定は暗号として使用できるかの検定として広く使われており，5.3

節の結果から，検定の合格率が高い数列ほど乱数度が高く，暗号としてふさわしいと考えられる．以上のことを考慮すると，乱数度を示す，6 次モーメントと RMT 理論値の誤差の値が 0.60%以下である乱数列のように，NIST 乱数検定において合格率が 14/15 または 15/15 のものは，「暗号としてふさわしい程度の良い乱数」と判断できると考えられる．

## 7. 終わりに

規則的な数列をシャッフルして作成した乱数データを RMT テストおよび NIST 乱数検定で検証した結果，どちらもシャッフル回数に応じた乱数度の向上を確認できた．このことをふまえて両者の結果を比較したところ，6 次モーメントの誤差 0.60%以下で，NIST 乱数検定において 14/15 以上の合格率を確認できた．RMT テストのより詳細な精度を追求するためには，数列のサンプル数や初期データの様々な場合についても検証する必要がある．その他，今後の課題として，シンボル数および NIST 乱数検定用の 0-1 変換方法の工夫，境界線 0.60%付近の精密化などがある．

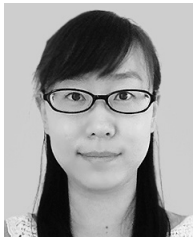
### 参考文献


[1] 日本規格協会：JIS Z 9031 乱数発生及びランダム化の手順，2001 年改正 (2001),
[2] NIST: available from ⟨http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html⟩.
[3] 田中美栄子，糸井良太，楊　欣：ランダム行列理論を用いた乱数度評価法の提案，情報処理学会論文誌　数理モデル化と応用，Vol.5, pp.1–8 (2012).
[4] Yang, X., Itoi, R. and Tanaka-Yamawaki, M.: Testing Randomness by Means of Random Matrix Theory, *Progress of Theoretical Physics, Supplement*, Vol.194, pp.73–83 (2012).
[5] Wigner, E.P.: *Ann. Math.*, Vol.67, pp.325–327 (1958).
[6] Laloux, L., Cizeaux, P., Bouchaud, J. and Potters, M.: Noise Dressing of Financial Correlation Matrices, *Physical Review Letters*, Vol.83, pp.1467–1470 (1998).
[7] Plerou, V., Gopikrishnan, P., Rosenow, B., Amaral, L.A.N. and Stanley, H.E.: *Physical Review Letters*, Vol.83, pp.1471–1474 (1999).
[8] Plerou, V., Gopikrishnan, P., Rosenow, B., Amaral, L.A.N., Guhr, T. and Stanley, H.E.: Random Matrix Approach to Cross Correlation in Financial Data, *Physical Review E*, Vol.65, No.066126, pp.1–18 (2002).
[9] 情報処理振興事業協会セキュリティセンター：電子政府情報セキュリティ技術開発事業擬似乱数検証ツールの調査開発調査報告書，pp.1–45 (Feb. 2003).
[10] Rukhin, A. et al: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, pp.5-1–5-8 (Apr. 2010).



**三賀森 悠大**　（学生会員）

1989 年生．2008 年鳥取大学工学部知能情報工学科入学．2012 年鳥取大学大学院情報エレクトロニクス専攻博士前期課程入学．



**楊 欣**　（学生会員）

1984 年生．2009 年中国吉林大学大学院工学研究科物流工学専攻修士課程修了．2011 年鳥取大学大学院工学研究科情報エレクトロニクス専攻博士後期課程入学．乱数に関する領域に着目し，研究している．

**糸井 良太**　（学生会員）

1989 年生．2007 年鳥取大学工学部知能情報工学科入学．2011 年鳥取大学大学院情報エレクトロニクス専攻博士前期課程入学．

**田中 美栄子**　（正会員）

1950 年生．1974 年京都大学理学部卒業，1979 年名古屋大学大学院満期退学，1983 年 Rochester 大学博士課程修了（Ph.D. in Physics）．CCNY，SUNY，NASC，椙山女学園大学，宮崎大学工学部を経て，現在，鳥取大学大学院工学研究科情報エレクトロニクス専攻知能情報工学講座教授．主たる研究テーマは経済物理学，複雑系科学．日本物理学会，IEEE，応用数理学会各会員．