Vol.2012-MPS-88 No.15
2012/5/17

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)]

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共に，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なった．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に対応するデータ列では，RMT テストによる誤差が 0.69% 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．NIST 検定に掛けるために 2 進列に変換していることや，両テストにおけるデータ列の制限等を考慮すると，矛盾しているとまでは言えないが，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言える．

キーワード：乱数度評価基準，RMT テスト，NIST 乱数検定

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)]

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 RMT-test to the result of 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 0.69% 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 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

1. はじめに

乱数度とは，如何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上，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事が多い．

以前に我々が提案した，乱数度評価のための RMT テスト [3][4] 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測ることができる便利な手法であり，直観性に

[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
Tottori University, Graduate School of Engineering, Department of Information and Electronics
[a)] s082053@ike.tottori-u.ac.jp
[b)] mieko@ike.tottori-u.ac.jp

優れた定性評価 [3] と，客観性に優れた定量評価 [4] を併用することで，様々な種類のデータの乱数度を簡便に測定するツールを提供するものである．問題点としては，第一に，データとして非常に長い数列を必要とし，社会科学や医学の分野に応用する際に十分なデータ数を確保することが必ずしも可能でない場合があること，また，第二には，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の選定に任意性を排除できなかったことがある [4]．すなわち，擬似乱数列や物理乱数列に対しては，局所的には誤差が 1-2% 程度と小さく，データ間のゆらぎを考慮して 100 サンプルの平均をとった場合の誤差の最大値が 5% 以下であれば擬似乱数と同等の乱数度を保証できる，という観察に基づいて「RMT 理論値との誤差 5% 以下なら乱数」という基準を決めた一方で，乱数列から作成した対数収益列のように，明らかに乱数度の低いデータに対しては，RMT 理論値との誤差が 20% 程度となるため，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良く解らなかった．原因はそのようなデータを入手できなかったことにある．

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し，RMT テストによりその乱数度を測定すると共に，NIST 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 テストの概要

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 1998 年 ~2002 年にかけて文献 [6][7][8] により株式市場に応用された文脈に基づいて提案された RMT 乱数度評価法 [3][4] を用いる．

相関行列の固有値分布の理論は，データ長 L，乱数列の個数 N，理論の最大固有値及び最小固有値 (λ_+ 及び λ_-) を用いて，

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

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

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

で表される．

この時，固有値分布の理論は式 (1) のみに依存する関数となる．条件として，$L \to \infty$，$N \to \infty$ で，かつ $L/N > 1$ となるように行列を作成する．

乱数から行列を構成する為に，予め一つの長い乱数列を生成しておき，図 1 のようにデータ長 L で区切る．この作業を N 回繰り返すことにより，相関行列を作成していくのに必要なデータを得ることができる．行列を作成する際，i 行 j 列目の要素 $A_{i,j}$ は，数列の（$i \times L + j$）番目の数字となる．

図 1　乱数列の分割方法
Fig. 1　How to divide the random number sequence

相関行列作成の過程として，まず 2.2.1 節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．

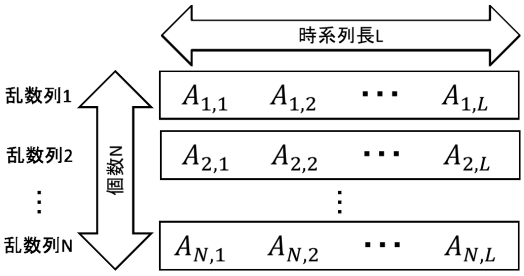

図 2　乱数列データの並べ方
Fig. 2　Arrangement of the data sequence of random numbers

次に，この行列を列ごとに平均 0，分散 1 で正規化する．正規化する際には次の式 (4) を使い，求めた数値を正規化行列 G に代入する（式 (5)）．

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

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

さらに，式 (6) のように正規化行列 G とその転置行列 G^T の積をとることにより，相関行列 C を求める．

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

乱数度の評価方法は，モーメント法によって固有値の k 次モーメントを求め，その理論値で割って数値化することにより，乱数度をより細かく分析できる定量評価を用いる．1 つのサンプル（データ長 100 万）から $N \times L$ を決定して相関行列を作成する．今回は，N=500，L=2000 の条件のもとで乱数度評価を行っている．その後，定量評価を行うことにより，乱数度を数値で判定する．

最初に，式 (6) で求めた相関行列 C から対角要素の平均をとることにより，次式を用いて k 次モーメントの実測

値 m_k を求める．

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

k に対応する理論値は次式により計算する．

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

さらに，求めた k 次モーメント m_k を，その k に対する RMT 理論値 μ_k で割ることによって，誤差を数値で表す．誤差を表す数値は，

$$\text{誤差 (\%)} = (\tfrac{m_k}{\mu_k} - 1) \times 100 \tag{9}$$

で求める．これは，RMT が完全にランダムと見なす理論からどの程度ずれているかを表すもので，誤差の値が大きいものほど乱数度が低く，逆に誤差が 0% に近いものほど乱数度が高いと判断する．

3. NIST 乱数検定の概要

様々な視点で検定を行うことで，乱数の良し悪しをより細かく調査することができる．その為，今回は乱数検定の道具として，米国国立標準技術研究所（NIST）で開発された， NIST SP 800-22 を使用した．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り，1 つの数列を読み込むことで，様々な検定をまとめて素早く行うことができる．NIST のホームページにて，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おり，合格と判断された検定の数が多いほど乱数度は高くなり，その数列は「暗号に相応しい程度の良い乱数」として判断できる．

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全部で 15 種類である．

文献 [9][10] によると，NIST SP 800-22 によって検定する数列の対象として，長さ 100 万の数列が推奨されている．また，統計的に有意な結果を得る為には，少なくとも 55 サンプルの数列を用意する必要がある．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. 検証に用いた乱数データの作成方法

NIST 乱数検定により良い乱数として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なっていく為，様々な乱数度の数列データを用意したい． そこで，ランダム性が極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なっていく．NIST 乱数検定の条件に合わせる為，本研究で扱うデータとして，全要素数 100 万の数列を 55 サンプル用意する．元の規則的な数列の生成及びシャッフル作業は全てコンピュータによって行われる為，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である．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．

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，0〜99 の 100 個を昇順に並べていき，その数列 1 セットを 1 万個連結させることでデータ長 100 万，かつ 0〜99 のそれぞれの度数が全て均一の規則的な数列を構成する．

シャッフルは，数列データにある全要素数 100 万の要素の中から 2 要素をそれぞれランダムに選び，お互いの順番を入れ替えるというアルゴリズムで行う．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 テスト及び NIST 乱数検定で扱う．

5. 実験

5.1 RMT テストによる結果

まず，RMT テストを用いて，規則的な数列をシャッフルしたものの乱数度を調査することにより，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．

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 (9) 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．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．

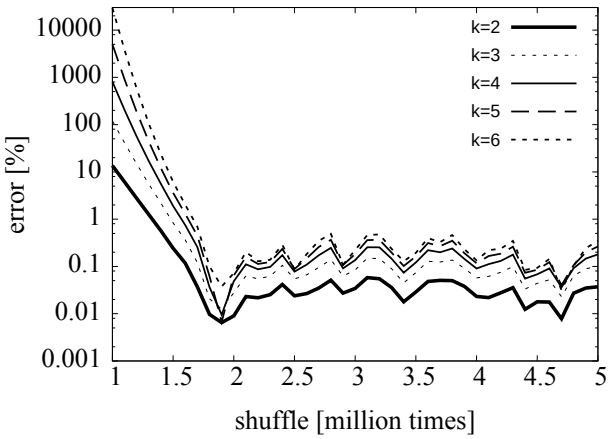

図 3 シャッフルによる誤差 (k=2〜6) の推移
Fig. 3 Changes in error due to shuffle(k=2〜6)

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為，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，データが全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 評価を行った上で合否を判断する．

※ Proportion 評価

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ている．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．

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	6/15	320	15/15
120	7/15	330	15/15
130	7/15	340	14/15
140	10/15	350	15/15
150	10/15	360	15/15
160	12/15	370	14/15
170	14/15	380	14/15
180	14/15	390	14/15
190	15/15	400	15/15
200	15/15	410	15/15
210	15/15	420	15/15
220	15/15	430	15/15
230	15/15	440	15/15
240	15/15	450	15/15
250	15/15	460	15/15
260	14/15	470	15/15
270	15/15	480	15/15
280	14/15	490	15/15
290	14/15	500	15/15
300	15/15		

シャッフル回数 170 万回以降を 10 万回区切りで見ると，15 種類全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為，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 RMT テストと NIST 乱数検定の比較

RMT テストと NIST 乱数検定の結果を比較する為，先程の 5.1 節及び 5.2 節での検証結果を表 2 にまとめる．RMT による乱数度評価の結果は k=2~6 の中でも，6 次モーメントを扱う．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．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為，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　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
29359.22	5/15	0.23	14/15
3801.86	6/15	0.22	15/15
574.22	7/15	0.22	15/15
104.59	7/15	0.20	15/15
23.36	10/15	0.19	15/15
6.16	10/15	0.18	14/15
2.02	12/15	0.14	15/15
0.69	**14/15**	0.14	15/15
0.49	14/15	0.14	15/15
0.48	15/15	0.13	15/15
0.46	15/15	0.13	14/15
0.46	14/15	0.11	14/15
0.40	15/15	0.10	15/15
0.35	15/15	0.10	14/15
0.35	15/15	0.09	15/15
0.35	15/15	0.09	15/15
0.33	14/15	0.08	15/15
0.29	15/15	0.07	15/15
0.24	15/15	0.04	15/15
0.24	15/15	0.03	15/15
0.24	15/15		

表 2 より，NIST 乱数検定の結果が，誤差の絶対値 0.69%（太字）以下の全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 乱数度が高い例・低い例

擬似乱数及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．

表 3　擬似乱数 (LCG) 及び物理乱数 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

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 4　対数収益をとることにより乱数度を下げた数列に対する結果
Table 4　Results for the sequences which were reduced there level of randomness by log-return

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

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．

6. 考察

乱数度の向上にも関わらず，誤差 0.69% 以下で合格検定数が 14，15 で遷移しているが，調査の結果，合格率 14/15 の乱数列全てにおいて「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分かる．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，以上のことと，5.3 節の比較結果が安定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 0.69% 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，検定の合格率が高い数列ほど，暗号として相応しいとされている．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 0.69% 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，「暗号として相応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 テスト及び 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．このことを踏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 0.69% 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為には，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．また，NIST 乱数検定に使用できる数列の種類に制限があることを考慮すると，0-1 データに関しても RMT テストで検証することで，より詳しい分析が可能であると考えられる．

その他，今後の課題として，シンボル数及び NIST 乱数検定用の 0-1 変換方法の工夫，境界線 0.69% 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．
[2] NIST: `http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html`
[3] 楊欣，田中美栄子，“ランダム行列理論を用いた乱数度評価法の提案”，情報処理学会研究報告，Vol.2011-MPS-83 No.2(2011 年 5 月 17 日)．
[4] X. Yang, R.Itoi, M. Tanaka-Yamawaki, “Testing Randomness by Means of Random Matrix Theory”, Progress of Theoretical Physics, Supplement, 2012, accepted.
[5] E. P. Wigner, Ann. Math., Vol. 67, pp. 325-327, 1958.
[6] L. Laloux, P. Cizeaux, J. Bouchaud, M. Potters, ”Noise Dressing of Financial Correlation Matrices”, Physical Review Letters, Vol.83 , pp.1467-1470, 1998.
[7] V. Plerou, P. Gopikrishnan, B. Rosenow, L. A. N. Amaral, H. E. Stanley, Physical Review Letters, Vol. 83, pp. 1471-1474, 1999.
[8] V. Plerou, P. Gopikrishnan, B. Rosenow, L. Amaral, H. Stanley, ”Random Matrix Approach to Cross Correlation in Financial Data”, Physical Review E, Vol. 65 no.066126, 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，(平成 15 年 2 月)
[10] Andrew Rukhin 他，“A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications” ，pp. 5-1 ～ 5-8，(April 2010)