Vol.2012-MPS-88 No.16
2012/5/17

モーメント分析法によるランダム行列理論を用いた乱数度評価法の改良

楊　欣[1,a)]　糸井　良太[1]　田中　美栄子[1,b)]

概要：先行研究においてランダム行列理論を用いた乱数度評価法（RMT-テスト）を提案した．これは，対象とする数列から作成した相関行列の固有値分布が RMT 公式に一致するか否かで乱数度を判定するものである．本稿では，モーメント法を用いて RMT-テストを定量化し，さらに，乱数度の高いことが既知である擬似乱数の例と，乱数度が低いと予想される対数差数列を用いて評価基準を数値化した上で本手法をハッシュ関数の乱数度評価に応用する．二つの暗号学的ハッシュ関数，MD5 と SHA-1 を比較すると，SHA-1 の出力データの乱数度が一貫して高くなることから，ハッシュ関数の評価にも本手法を使えることが分かった．

キーワード：乱数度評価法，RMT-テスト，ランダム行列理論，モーメント分析法，SHA-1

Moment Approach for Quantitative Evaluation of Randomness by RMT-test

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

Abstract: In this article we develop a quantitative formulation of the randomness-test based on the random matrix theory (RMT-test), in order to compare a subtle difference of randomness between given random sequences. We employ the moment analysis in order to compare the eigenvalue distribution of the cross correlation matrix between pairs of sequences. Namely, we compare the moments of the actual eigenvalue distribution to the corresponding theoretical expression that we derive from the formula theoretically derived by the random matrix theory. According to the test result of five kinds of random data generated by two pseudo-random generators (LCG and MT) and three physical generators which randomness are high, and the derivatives of the sequences, or the initial part of LCG, which randomness are distinctly lower, that we determined the criterion of the quantitative RMT-test. Finally we point out that the RMT-test can distinguish the randomness of digest output by MD5 and SHA-1 successfully.

Keywords: randomness test, RMT-test, random matrix theory, moment analysis, SHA-1

1. はじめに

ランダム行列理論を用いた乱数度評価法（以下：RMT-テスト）は，データ列から作成した相関行列の固有値分布と RMT の理論分布を比較することによって，乱数度を判定する方法であり，代表的な機械乱数である線形合同法とメルセンヌ・ツイスターから生成した乱数列を「可」と判定する一方，乱数列の初期部分や数列の変化率のように乱数度を低下させた数列に対しては，目視だけでも乱数度の低さを検出する [1]．一方，目視で見分けられないような乱数度の高い数列の乱数度を比較するには，乱数度を数値化する必要がある．本稿ではモーメント分析法を用いた定量化手法により，乱数度の高低を決める評価基準を定めると共に，ハッシュ関数の性能評価への応用について述べる．

[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)] yx0709@ike.tottori-u.ac.jp
[b)] mieko@ike.tottori-u.ac.jp

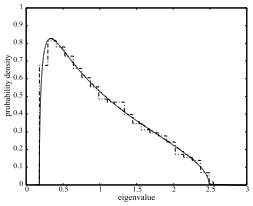

図 1 乱数度が高い場合

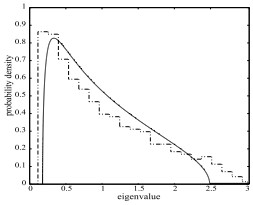

図 2 乱数度が低い場合

Fig. 1 Case of random data **Fig. 2** Case of low random data

2. モーメント分析法と定量評価

2.1 ランダム行列理論

ランダム行列理論はメゾスコピック系の物理学や量子重力，数論，経済物理学，生態学，ワイヤレス通信を含む様々な分野へ広範な応用を持つ大変普遍的な理論である [2][3]．本稿で用いるのは Plerou らにより 2002 年に株式市場の主成分分析に応用された文脈 [4] に基づき，時系列の相関行列の固有値分布をランダム行列理論から導かれる式 (1)

$$P_{RMT}(\lambda) = \frac{Q}{2\pi\lambda}\sqrt{(\lambda_+ - \lambda)(\lambda - \lambda_-)} \tag{1}$$

$$\lambda_\pm = \left(1 \pm \sqrt{\frac{1}{Q}}\right)^2 \tag{2}$$

と比較することにより時系列のランダム性を評価しようとする方法である．以下に手法を概説する．時系列長 L の無作為なデータ N 個の内積を成分とする相関行列を作成し固有値を求める．相関行列の固有値経験分布は，データがランダム列であれば $N \to \infty$，$L \to \infty$ でその統計性によらず $Q = L/N$ のみに依存する簡単な関数となり，式 (1) と (2) で表せる．

2.2 定性評価

先行研究 [1] は，実データの固有値分布のヒストグラムがランダム行列理論の式に一致するかどうかを図示により判断し，乱数度を評価する．このランダム行列理論による特徴を検出する方法を使うことで，実データの固有値分布とランダム行列理論の式の比較結果が一致すればランダム（図 1），逆に一致しなければ規則性が判断し，乱数度が低いと評価する（図 2）．

2.3 モーメント分析法

乱数度の高いデータに対し，その乱数度を比較するには数値化した基準を必要とする．図 1 と図 2 のような固有値分布の形状を数値化するにはその k 次モーメント，即ち，固有値の k 乗の平均値

$$m_k = \frac{1}{N}\sum_{i=1}^{N}\lambda_i^k \tag{3}$$

と，対応する理論値

$$\mu_k = E(\lambda^k) = \int_{\lambda_-}^{\lambda_+}\lambda^k P_{RMT}(\lambda)d\lambda \tag{4}$$

を比較するのが便利である．式（1）の関数に対する低次モーメントは β 関数を用いて簡単に計算できる．ここでは 6 次以下のモーメントを Q の関数として求めた結果 [5] を記しておく．

$$\mu_1 = 1 \tag{5}$$

$$\mu_2 = 1 + \frac{1}{Q} \tag{6}$$

$$\mu_3 = 1 + \frac{3}{Q} + \frac{1}{Q^2} \tag{7}$$

$$\mu_4 = 1 + \frac{6}{Q} + \frac{6}{Q^2} + \frac{1}{Q^3} \tag{8}$$

$$\mu_5 = 1 + \frac{10}{Q} + \frac{20}{Q^2} + \frac{10}{Q^3} + \frac{1}{Q^4} \tag{9}$$

$$\mu_6 = 1 + \frac{15}{Q} + \frac{50}{Q^2} + \frac{50}{Q^3} + \frac{15}{Q^4} + \frac{1}{Q^5} \tag{10}$$

2.4 定量評価

固有値分布のモーメントとその理論値の比較を利用し，「k 次以下のモーメントが理論式に x パーセント以下の誤差で一致すれば乱数度が高い」という基準を定め定量評価基準とする．式（5）ー（10）より計算した理論値からの実測値の誤差は以下のようになる．

$$error = m_k/\mu_k - 1 \tag{11}$$

3. 評価基準の決定

3.1 N と L の範囲の決定

実験パラメータとして使用するデータ長 L とデータ数 N の選択について述べる．式（1）の固有値分布の理論式，P_{RMT} は一個のパラメータ $Q(= L/N)$ のみに依存する．しかし，この式は N と L が無限大の極限という条件で導かれているため，N と L を大きく取る必要があり，また，必要な自由度を確保する必要がある．どのぐらい大きな N が必要かを調べるため文献 4 では一般的に使用頻度の高い線形合同法（LCG）と，周期の長いことで知られるメルセンヌ・ツイスタ（MT）[6] に対して，$N = 200$，300，400，500（$Q = 3$）の場合に式（11）で与えられる誤差を比較した．その結果，いずれの擬似乱数についても N を大きくするに従って誤差は減少し，$N = 500$ で 0.25% 以下になった．すなわち $N = 500$，$L = 1500$（$Q = 3$）で無限大の極限という条件が十分に満たされているものと考え，以下本稿ではこのパラメータを使用する．

表 1 定量化結果：100 サンプルに対する誤差平均値と標準偏差 (Q=3)
Table 1 Average and standard deviation of error(100 samples)

k	LCG	MT	Toshiba	Hitachi	Tokyo
2	-.0004(.0010)	-.0004(.0009)	-.0004(.0010)	-.0004(.0010)	-.0004(.0009)
3	-.0010(.0026)	-.0009(.0024)	-.0011(.0026)	-.0011(.0025)	-.0009(.0025)
4	-.0018(.0047)	-.0014(.0041)	-.0019(.0046)	-.0019(.0044)	-.0015(.0044)
5	-.0027(.0072)	-.0019(.0062)	-.0026(.0070)	-.0028(.0066)	-.0019(.0067)
6	-.0036(.0100)	-.0022(.0085)	-.0033(.0096)	-.0037(.0092)	-.0021(.0093)

表 2 定量化結果：100 サンプルに対する誤差平均値と標準偏差 (Q=6)
Table 2 Average and standard deviation of error(100 samples)

k	LCG	MT	Toshiba	Hitachi	Tokyo
2	-.0003(.0006)	-.0001(.0006)	-.0002(.0006)	-.0002(.0006)	-.0002(.0005)
3	-.0008(.0016)	-.0004(.0015)	-.0005(.0015)	-.0006(.0016)	-.0004(.0014)
4	-.0014(.0028)	-.0006(.0027)	-.0008(.0027)	-.0011(.0028)	-.0007(.0026)
5	-.0020(.0043)	-.0009(.0042)	-.0012(.0042)	-.0016(.0043)	-.0009(.0040)
6	-.0026(.0060)	-.0012(.0058)	-.0015(.0058)	-.0020(.0060)	-.0010(.0056)

3.2 実験

(1) 乱数度が高い場合：擬似乱数，及び物理乱数
二つの擬似乱数，LCG と MT，及び統計数理研究所ホームページ [7] から東芝，日立と東京エレクトロンデバイスの各ボードにより発生する，3 種類の物理乱数のデータを入手し，これら 5 種の乱数発生器で発生した乱数から 100 サンプルを作成し，RMT-テストにより乱数度を測定した．結果を表 1 に示す．また，乱数列長により，乱数度が変化するため，$Q = 3$ の 2 倍長の $Q = 6$ の結果を表 2 に示す．表 1 より，東京エレクトロンデバイス製物理乱数の誤差平均値（$k = 6$）は MT より小さい，しかし，標準偏差から見ると MT より東京エレクトロンデバイス製物理乱数の範囲が大きい（東芝製物理乱数と LCG の比較結果も同じだった）．つまり，$Q = 3$ のときに物理乱数のばらつきは擬似乱数より大きいということが分かった．
また，表 2 より，東京エレクトロンデバイス製物理乱数の誤差平均値（$k = 6$）は MT より小さい，標準偏差から見る東京エレクトロンデバイス製物理乱数の範囲が小さい（東芝製物理乱数と LCG の比較結果も同じだった）．つまり，乱数列が長くなると物理乱数の乱数度は擬似乱数より高くなるという結果が分かった．
他に，4 次モーメントまでの誤差による 5 種類の発生器の差はあまり見えなかったことから，6 次モーメントの誤差によって乱数度を判定するという基準を決めた．又，全サンプルの誤差の絶対値は 2.86% 以下になった． 以上の分析により乱数度を高いとする判定基準としては 6 次モーメントの誤差が 3% から 5% の間と考えて良い．
(2) 乱数度が低い場合
先行研究 [1] で LCG の初期乱数と対数収益を取ったデータを定性評価で評価した．その中 LCG の初期乱数の悪さもはっきりと確認でき．乱数度が低いということが分かった．ここで，それらの定量化結果を示す．表 5 の結果によると，LCG の初期乱数の 6 次モーメントの誤差の絶対値を 5% 以上だった．そこで，定量評価基準を 5% に設定すれば，不合格の乱数列は定性評価でも判断できることになる．

表 3 最初 500 個のみを集めた初期乱数の定量評価
Table 3 Quantitative evaluation of initial parts of LCG and MT

k	LCG(Q=3)	MT(Q=3)	LCG(Q=6)	MT(Q=6)
2	.0045	-.0018	.0057	-.0007
3	.0103	-.0042	.0141	-.0021
4	.0197	-.0064	.0251	-.0041
5	.0352	-.0083	.0392	-.0066
6	.0583	-.0099	.0571	-.0092

表 4 変化率を取って乱数度を下げた場合の評価結果 LCG(左)MT(右)
Table 4 Quantitative evaluation of log-return sequences of LCG and MT

k	LCG(Q=3)	MT(Q=3)	LCG(Q=6)	MT(Q=6)
2	.1047	.1227	.0696	.0702
3	.2578	.3088	.1866	.1892
4	.4445	.5442	.3391	.3450
5	.6596	.8260	.5240	.5342
6	.9092	1.174	.7426	.7579

3.3 定量評価基準の決定とその適応条件

ここまで，$N = 500$ による実験結果を出し，6 次モーメントの誤差の絶対値は 3% 以下であることが分かった．また，乱数列の長度制限を緩和するため，$N = 200$，300，400($Q = 3, \cdots, 10$) の擬似乱数と物理乱数の 6 次モーメントの誤差を調査した．その結果有意水準 $\alpha = 0.05$ の時に $N = 200$（$Q = 3$）の乱数列の 6 次モーメントの誤差の絶

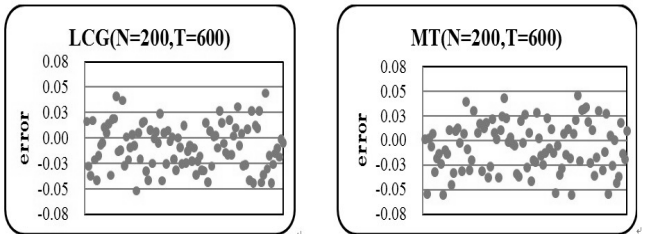

図 3 判定基準が 5% の場合 LCG と MT の乱数列 95% が合格 (N=200)

Fig. 3 More than 95% samples pass the RMT-test for x=0.05 and N=200

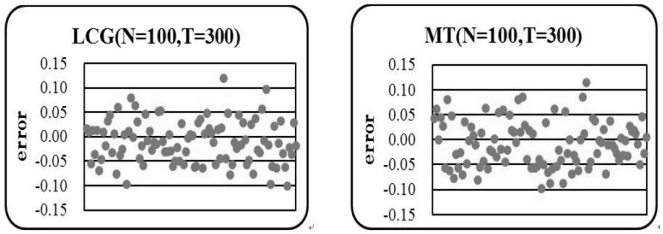

図 4 判定基準が 5% の場合 $N = 100$ に対しては LCG と MT の乱数列いずれも RMT-テストに不合格 (N=100)

Fig. 4 Both LCG and MT failed the RMT-test for x=0.05 and N=100

対値は 5% 以下になった（図 2）．そこで，RMT-テストの定量評価基準は「$k = 6$，$x = 5$」と決定した．つまり，6 次以下のモーメントが理論式に 5 パーセント以下の誤差で一致すれば乱数度が高いと言える．しかし，乱数列の長さは 12 万以下の乱数列はこの基準を適応できない．例えば，$N = 100$（$Q = 3$）の乱数列の 6 次以下のモーメントが理論式に 10 パーセント以下の誤差絶対値だった（図 3）．そこで，提案手法の定量基準の制限条件は乱数列の長さが 12 万以上ということになる．

4. NIST との比較

米国商務省標準局 NIST（National Institute of Standards and Technology）が開発した乱数検定法は，本来，乱数を暗号として使用できるかを判定するためのものであるが，既存手法として確立されているので提案手法との比較を行う．公開当初は 16 方式計 189 の検定項目で構成されていたが，2010 年でマイナーアップデートした「sts-2.1.1」版 [8] 検定法は 15 個テスト項目を用いて，乱数の全体的な様子を見るようになっている．これを用いて提案手法で乱数度の高かった LCG データは，NIST 乱数判定法で評価すると，15 項目全部に合格した．一方，LCG データの対数収益を取ったデータは提案手法で乱数度が低く出たが，これを NIST で評価すると，15 項目中 6 項目に合格した．この結果を表 5 に示す．つまり 4 割しかテスト項目をクリアしなかったことになる．これらの結果から，提案手法と NIST 検定法の結果は矛盾しない．

表 5 対数収益を取ったデータの NIST 乱数評価法での評価結果

Table 5 Result of log-return sequences test by NIST Randomness test

	テスト項目	結果
1	一次元度数検定	pass
2	ブロック単位の度数検定	pass
3	連の検定	fail
4	ブロック単位最長連検定	fail
5	行列ランク検定	pass
6	離散フーリエ変換検定	fail
7	重複無テンプレート適合検定	fail
8	重複有テンプレート適合検定	fail
9	Maurer の統一統計検定	fail
10	線形複雑度検定	pass
11	系列検定	fail
12	近似エントロピー検定	fail
13	累積和検定	pass
14	ランダム偏差検定	fail
15	ランダム偏差分散検定	pass

しかし，NIST の評価法はデータの形式の制限がある，実数を評価できない上，データ長が 100 万以上でなければならないという欠点がある．これに対して，提案手法ではそこまでの強い制限はない．評価基準を 5% とした場合，長さ 12 万以上ならば使用出来る．また，LCG の初期乱数のデータを NIST で評価すると合格してしまうが，提案手法では不合格となることから，NIST より提案手法の検定基準のほうが厳しいと言える．

また，提案手法は定性評価において視覚化の利点がある上に，定量評価も可能である．これに対して他の可視化手法，例えばモアレ縞法等は定量化評価が出来ない．これに対し，本手法は視覚的評価と共に定量的な評価が可能な点において有用性が高いと考えられる．

5. 考察

RMT-テストを考察するために，ここで，既知の乱数列を比較できるかをチェックする．使用した乱数列は暗号学的ハッシュ関数 MD5 と SHA-1 の出力データ．暗号学的ハッシュ関数は多数存在するが，その多くは脆弱性が判明し，使われなくなっている． 2004 年 8 月，当時よく使われていたハッシュ関数（SHA-0，RIPEMD，MD5 など）の弱点が判明した．このことから，これらのハッシュ関数から派生したアルゴリズム，特に SHA-1 と RIPEMD-128 の長期的なセキュリティに疑問が投げかけられた．2009 年現在，最も広く使われている暗号学的ハッシュ関数は MD5

表 6 MD5 と SHA-1 の出力データのランダム性
Table 6 Quantitative evaluation of sequences output by MD5 and SHA-1

k	MD5(Q=3)	SHA-1(Q=3)	MD5(Q=6)	SHA-1(Q=6)
2	-.0012	-.0019	-.0008	-.0013
3	-.0051	-.0032	-.0031	-.0033
4	-.0115	-.0034	-.0065	-.0049
5	-.0194	-.0029	-.0108	-.0058
6	-.0282	-.0020	-.0159	-.0057

と SHA-1 である．しかし，MD5 は既に破られているため [9]，安全性が高いと言えるのは SHA-1[10] である．ここで，MD5 と SHA-1 の出力データのランダム性の視点から両種類の暗号学的ハッシュ関数を比較する．定量評価基準の制限条件により，MD5 と SHA-1 の出力データの長さを 12 万（$N = 200$，$Q = 3$）に設定し考察した．6 次モーメントの誤差の絶対値は両方とも 5% 以下で乱数度が高い（表 6）．また，SHA-1 の各次モーメントの誤差の絶対値は小さく，さらに，5 次と 6 次のモーメントの誤差の絶対値はその増える傾向を抑制できた．従って，MD5 より SHA-1 の出力データのランダム性が良いという結果が分かった．暗号学的ハッシュ関数の出力データはもとファイルのダイジェストから，そのランダム性が高い方はセキュリティ性も高いといえる．そこで，提案手法の有用性をチェックできた．

6. 終わりに

本研究ではモーメント分析法によるランダム行列理論を用いる乱数度評価法（RMT-テスト）の定量評価を提案した．定量基準を決めるため，我々は東芝，日立，東京エレクトロン製の 3 つ物理乱数発生器と 2 つ擬似乱数生成器（LCG と MT）のそれぞれの定量評価結果を出した．これらの実験に基づいて本稿は長さ 12 万以上の乱数列「6 次以下のモーメントが理論式に 5 パーセント以下の誤差絶対値で一致すれば乱数度が高い」という基準を決めた．最後に，現存手法との比較研究と暗号学的ハッシュ関数 MD5 と SHA-1 の出力データの定量化研究により，RMT-テストの有用性をチェックした．

参考文献

[1] Yang, X. and Itoi, R. and Tanaka-Yamawaki, M.: *Testing Randomness by Means of RMT Formula*, IDT, SIST Vol.10, pp.589-596 (2011).
[2] 永尾　太郎：ランダム行列の基礎，東京大学出版会 (2005).
[3] Mehta, M.: *Random Matrices, Third Edition*, Academic Press (2004).
[4] Plerou, V., Gopikrishnan, P., Rosenow, B., Amaral, L.A.N. and Stanley, H.E.: *Random Matrix Approach to Cross Correlation in Fianancial Data*, Physical Review E, Vol.65, no.066126 (2002).
[5] 田中　美栄子，糸井　良太，楊　欣：RMT 公式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).
[6] Matsumoto, M. and Nishimura, T.: *Mersenne Twister: A 623-Dimensionally Equidistributed Uniform Pseudorandom Number Generator*, ACM Transactions on Modeling and Computer Simulation, Vol.8, pp.3-30 (1998).
[7] Tamura, Y.: *Random Number Library* (online), http://random.ism.ac.jp/random/index.php (2010.07.26).
[8] NIST: *A Statistical Test Suite* (online), csrc.nist.gov/groups/ST/toolkit/rng/documentation-software.html (2010.08.13).
[9] Black, J., Cochran, M. and Highland, T.: *A Study of the MD5 Attacks: Insights and Improvements* (online), http://www.cs.colorado.edu/ jrblack/papers/md5e-full.pdf (2008.07.27).
[10] Locktyukhin, M. and Farrel, K.: *Improving the Performance of the Secure Hash Algorithm(SHA-1)* (online), http://software.intel.com/en-us/articles/improving-the-performance-of-the-secure-hash-algorithm-1/ (2010.03.29).