（様式７）

学 位 論 文 審 査 結 果 の 要 旨

氏　　名	楊　欣
審 査 委 員	委 員 長　田中　美栄子　印 委　　員　石井　晃　印 委　　員　谷本　圭志　印 委　　員　清水　忠昭　印
論 文 題 目	ランダム行列理論を用いた乱数度測定法の開発とその実データへの応用

審 査 結 果 の 要 旨

乱数は暗号通信を始めとするセキュリティ分野のみならずゲームその他に於いても重要な役割を果たし，我々の生活のあらゆる場面で重要な役割を演じている．この乱数の良し悪しを測る尺度である乱数度の測定方法に対し，単に合格・不合格の判定をするだけでなく，与えられたデータ列の並び方の乱雑さを簡便に数値化できる手法を探究した結果，ランダム行列理論により導出された相関行列の固有値分布とデータから求めた分布とを比較することによってデータの乱数度を数値化する「RMT テスト」を開発し，応用を示したことが本学位論文の主眼である．

本手法の理論的基礎となる，ランダム行列理論(Random Matrix Theory: RMT と略)を用いた主成分分析法(Principal Component Analysis: PCA と略)，すなわち RMT-PCA は，近年の急速なデジタル化に伴い世界中で蓄積されつつある大容量データを様々な目的に則して解析するための有効な手法として多方面で注目を集めている．

申請者である楊欣は，RMT-PCA の手法を応用することにより，数値データ列の乱数度を計測する手法としての，「RMT テスト」の研究を詳細に行いその有効性を明らかにした．

従来の乱数度検定法と比較して，RMT テストの利点は４点ある．

１点目は可視化手法であること，即ち，乱数度が低い数列に対しては，RMT テストの定性評価を用いることで，直感的に見てすぐ検定ができることである．

２点目は，多くの他の検定法が複数手法を併用しており，個々の手法同士の相対的重要性がわかりにくいのに対し，本手法は理論的基礎付けの明快な単一手法に基づくものであることである．

３点目は適用可能なデータ型を問わないことであり，従来の乱数度検定アルゴリズム，米国の NIST などのように，対象とするデータの長さやデータ型に強い制限がなく，実数・整数・二進数などに同一のアルゴリズムを用いることができることである．

４点目は本手法が単なる検定法ではなく，RMT テストの定量評価を用いることで，データの乱数度を数値化して比較することができるため，乱数度の必ずしも高くない，広範囲の実データに対して同一の基準で乱数度を計測できることである．

審 査 結 果 の 要 旨(続)

本論文ではまず，乱数度の高いことが知られている２種の擬似乱数，すなわち，線形合同法(LCG)とメルセンヌ・ツイスタ(MT)，および３種の物理乱数を資料として，実数列や 01 数列などを含む大量のデータの乱数度を RMT テストにより可視化することにより，RMT テストの定性評価に合格することを示し，また，乱数度の低いことが予想される２種の乱数データを資料としてその乱数度の低さを RMT テストの定性評価を用いて検出できることを示した.

しかし定性評価では，乱数度の高いデータ間の乱数度の僅かな差異は検出できないので，これを行うために，RMT テストの定量評価手法を開発した．定性評価では理論式と実験式の差異を目視によって判断したが，定量評価法は分布をモ―メントとして数値化した上で，理論式のモーメントと実験式のそれとの誤差（の逆数）を乱数度と定義する．この目的のためにモーメントの理論式を 6 次まで解析的に求める必要があった．こうして作成した定量評価により，MT と LCG の疑似乱数生成器２種とスーパーコンピュータに組み込まれた物理乱数発生器による物理乱数３種の計 5 種の乱数データを比較した．局所的な乱数度の比較のみならず，100 サンプルの平均±2σまでを考慮して，これら 5 種類の乱数生成器全てが合格する乱数判定基準として
「データ長が12万以上の場合，6 次モーメントが理論式に5%以下の誤差で一致すれば乱数度が高い」
を乱数の判定基準と定めた.

また「RMT テスト」をハッシュ関数，および株の高頻度価格データに適用し,有用な知見を得た.

まず，ハッシュ値の無規則性や予測不可性はランダム性が高いほど上がると考え RMT テストを用いて, よく使われる暗号学的ハッシュ関数 MD5 と SHA1 のランダム性を比較検定し, SHA1 の方が MD5 に比べてランダム性が高く，その意味で安全性が高いことを確認した.

次に株価への適用は，各株価の高頻度時系列の乱数度を RMT テストの定量評価で計算した結果とと，その株価のその後のパフォーマンスとの関連を調べた結果，一定の関連性を見出した．それは，「乱数度の高い株の方が収益性が高い」という経験則で表現できる．これは実験で使った 2007 年から 2009 年にかけて東証株価が下がり相場であったという特殊な条件にのみ適用できるものである可能性もあるが，少なくとも株式市場が下がり相場になる際は，乱数度が高い株に投資すると収益が高いことをデータが示していると言える．この仮説は今後多くのデータを用いて検証することにより，株選定の指標として乱数度を利用できる可能性を開く端緒になると考えられる.

以上により楊欣は，２年半の在学期間に研究室内での共同研究はもとより，多くの国際会議や国内研究会における講演や論文誌投稿を通じて，他大学の研究者とも意見交換をしつつ RMT テストの手法の完成と，乱数データを用いた検証，および実データへの応用など多くの成果を出しながら研究者として成長しており，博士（工学）の資格として充分と判断できる.