様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

# 科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月 ２７ 日現在

機関番号：３７１１２
研究種目：基盤研究(C)（一般）
研究期間：2017～2021
課題番号：１７Ｋ００３５５

研究課題名（和文）カオス真軌道を用いた乱数検定の独立性解析

研究課題名（英文）Individuality analysis of randomness tests using chaotic true orbits

研究代表者
山口　明宏（Akihiro, Yamaguchi）

福岡工業大学・情報工学部・教授

研究者番号：６０２８１７８９

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：本研究では，相関構造を調整可能なカオス真軌道，乱数検定プログラムの高速化，乱数検定の類似性の評価について研究を行った．更に，カオス真軌道計算の高速化や乱数検定の安全性の評価についても研究を行った．乱数検定の類似性については，乱数性の異なる複数の系列の検定結果のp値から構成した特徴ベクトルを構成し，その距離で類似度を評価する方法を提案した．更に乱数検定間の距離の総和を最小化するように乱数検定を選択することで，類似性が低い乱数検定の集合を構成できることを実験的に示した．この結果は，特徴ベクトルの構成に使用する系列に依存すると考えられるため，その依存性の解析は次の課題である．

研究成果の学術的意義や社会的意義
現在の情報基盤の一つである暗号などのセキュリティ技術において擬似乱数は広く用いられており，その乱数性の評価は重要な課題の一つである．本研究の成果の一つである類似性の評価は，乱数検定の独立性を考える上で，検定結果の統計的独立性とは意味での評価指標を与えるものであり，最適な乱数検定集合を議論するための指標として有用であると考えられる．更に，安全性の評価については，現在の乱数検定で広く用いられている２段階の検定において Kolmogorov-Smirnov検定を用いる場合のp値の厳密分布と一様分布のずれの影響を解析しており，検定の安全性の指標として有用であると考えられる．

研究成果の概要（英文）：We studied the chaotic true orbits with flexible correlation structure, the speed-up of randomness tests, and the evaluation of the similarity of randomness tests. We also studied the speed-up of computation time of the chaotic true orbits and the safety of randomness tests. For the similarity between randomness tests, we propose a method to evaluate the similarity by the distance between two feature vectors constructed from the p-values of randomness tests for multiple sequences with different degrees of randomness. Then, we experimentally showed that a set of randomness tests with low similarity could be constructed by selecting randomness tests to minimize the sum of the distances between tests. Since this result depends on the sequences to construct the feature vectors, the analysis of theier dependency is one of our next subjects.

研究分野：非線形力学系の情報学

キーワード：カオス真軌道　乱数検定　類似性　擬似乱数生成　安全性評価

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

擬似乱数は，暗号や数値解析など様々な分野で利用されており，その乱数性の判定は重要な課題の一つである．擬似乱数系列の乱数性の検定としては，NIST SP800-22 が知られており，2010 年に公開された Revision 1a では，15 種類 188 項目の検定の集合として定義されている．NIST 乱数検定では，個々の検定の合否判定は規定されているが，全ての検定結果を総合した最終的な判定については具体的には規定されておらず，個々の乱数検定の間の独立性が非自明であり，188 項目全ての検定を行う必要があるのか否かについても明確でないことが問題点として知られている．これらの問題点を解決し，より合理的な乱数検定を行うためには，個々の乱数検定項目の判定結果の独立性を解析し，独立性が高い乱数検定項目の最小集合をつくることが望まれるが，そのためには，「真の乱数と同等の統計的性質を有する系列」を検定する場合の解析だけでなく「統計的性質が明らかであり，かつ，乱数性が劣る系列」を検定する場合の解析も必要となると考えられる．一方，代数的数を用いた真軌道計算においては，通常の浮動小数点による演算では計算が難しいカオス軌道を厳密に計算することができる．そこで，統計的性質がわかっているカオス力学系について真軌道計算を適用することにより，設計した統計的性質に厳密に従う乱数性が劣る系列を生成でき，乱数検定の独立性の解析に応用できると考えて，本研究を実施した．

２．研究の目的

本研究では，乱数検定の独立性の解析に向けて，課題１）乱数検定アルゴリズムのテストデータとなりうるカオス真軌道の生成系の構成，課題２）乱数検定の並列化と高速乱数検定サーバーの開発，課題３）乱数検定の独立性解析と乱数検定の評価アルゴリズムの開発，の３つの課題に取り組んだ．加えて，研究の過程で，真軌道計算の高速化や，乱数検定の安全性について知見が得られたため，これらについても取り組んだ．課題１については，統計的性質を解析的に導出でき，相関構造を調整できる擬似乱数系列を，カオス真軌道を用いて構成することを目標とした．課題２については，NIST SP800-22 の大規模検定を可能とするために，プログラムの並列化とクラスタ計算機を用いた高速乱数検定サーバーの構築を目標とした．課題３については，課題１で構成した統計的性質を設計可能な系列の検定結果を用いて乱数検定の独立性を解析し乱数検定の集合としての評価を行うことを目標とした．研究の過程で，独立性の高い検定集合を構築するためには，検定結果の統計的独立性の概念だけでなく，乱数検定自体の類似性の概念も重要となることがわかったため，乱数検定の結果に基づく乱数検定間の類似性の評価も目標とした．これらの研究を通して，乱数検定の集合としての独立性の評価を行い，独立性が高い最適な乱数検定の集合を得るための評価指標を構築することを目的とした．

３．研究の方法

課題１については，「真の乱数と同等の統計的性質を有する系列」の生成として，ベルヌーイシフト写像の真軌道を用いて理想的な擬似乱数を生成する．「統計的性質が明らかであり，かつ，乱数性が劣る系列」の生成としては，マルコフ過程に厳密に対応する力学系を区分線形写像で設計し，その真軌道の生成系を構成することで，相関構造を調整できる系列の生成を行う．課題２については，NIST SP800-22 に対応した乱数検定ツールである STS Version 2.1.2 について，MPI を用いて並列化し，Web 経由でクラスタ計算機での並列計算を行うためアプリケーションを開発する．課題３については，課題１で構成した理想的擬似乱数系列，および，乱数性の劣る系列の検定結果を特徴ベクトルとして，特徴ベクトルの距離に基づく類似性の概念を導入することで，類似性が低く独立性が高い乱数検定集合を得るための評価指標を提案する．提案した評価手法については，NIST SP800-22 に含まれる検定に適用し最小集合の構成を試みる．

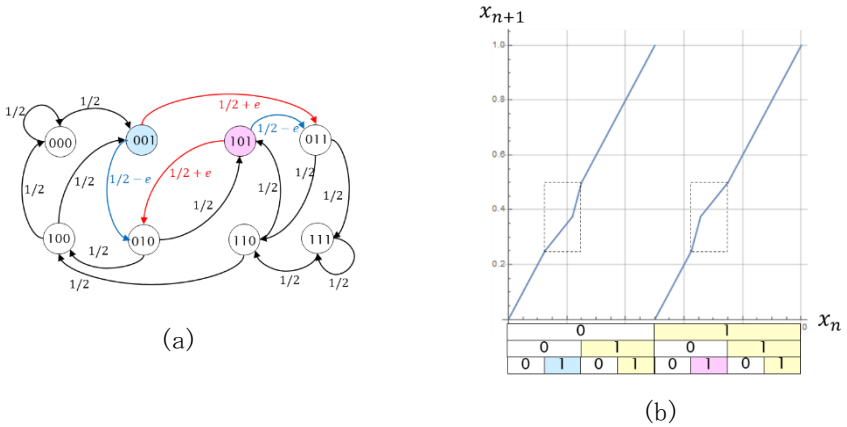
４．研究成果

4.1 乱数検定アルゴリズムのテストデータとしてのカオス真軌道生成系の構成

テストデータとしては，真の乱数と同等の統計的性質を有する系列の生成系と相関構造を調整可能な系列の生成系を構成した．前者については，これまでに実現していたベルヌーイシフト写像の２次代数的整数を用いた真軌道計算による方法に加えて，３次代数的整数を用いた真軌道計算による生成系を構成した．これによって，これまで以上に擬似乱数生成のパラメータの自由度を向上させることができた．生成される系列の乱数性については，NIST SP800-22 だけでなく，DIEHARD や TestU01 でも検定を行い良質な擬似乱数系列を生成できることを示した．

後者の乱数性の劣る系列の生成については，乱数検定の性能評価や特徴付では，乱数性のわずかな違いを検出できるかが課題となるため，統計的性質が保証されていて，相関構造を調整可能な系列が必要となる．そこで，本研究では，アーノルドの猫写像やマルコフ過程に厳密に対応する区分線形写像で与えられる力学系の真軌道による生成系を構成した．マルコフ過程に厳密に対応する区分線形写像による力学系としては，指定した長さ $l$ のビット列 $s$ につづく 0，1 の確率を 1/2 から指定した確率 $e$ だけずらすことで，相関構造（乱数性が劣る度合い）を調整可能な系列を実現することができた．この系列では，長さ $l$ の部分列までは均等に $2^{-l}$ の等確率

で生成され，長さ $l+1$ 以上の部分列については，指定した確率 $e$ に応じて等確率からのずれを生じる．図１は，$l=3$，$e=4^{-1}$ の場合のマルコフ過程(a)と対応する区分線形写像(b)の例であり，部分列 001，101 に続く 0，1 の生成確率を 1/2 からずらしている．なお，長さ $l$ までの部分列を等確率に生成するために，指定した部分列 $s$ の最上位ビットを反転させた部分列についても生成確率をずらす必要がある．4.3 で述べる乱数検定の評価では，$l$，$e$ および $s$ を複数設定して，乱数性の劣る度合いが異なる複数種類のテストデータを生成した．




(a)　　(b)

図１　マルコフ過程に厳密に対応する区分線形写像の例

4.2　乱数検定の並列化と高速乱数検定サーバーの開発

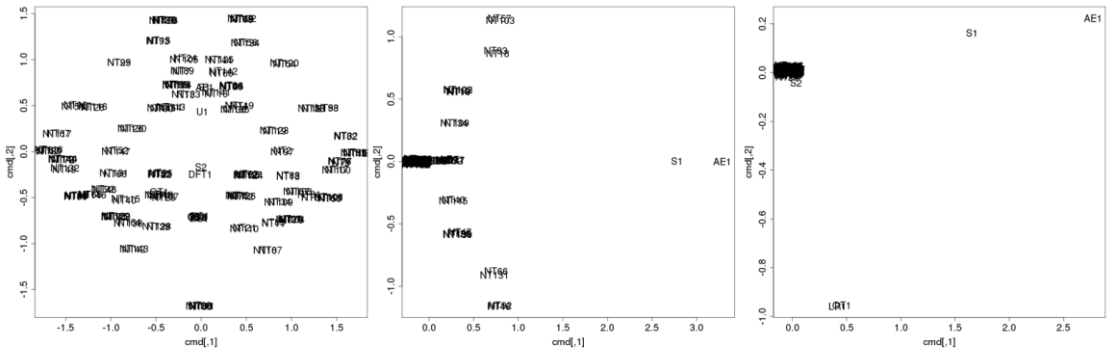
乱数検定の並列化については，NIST SP800-22 に対応した乱数検定ツールである STS Version 2.1.2 について MPI を用いて並列化を行った．加えて，STS は，テキストベースの対話型のプログラムで，乱数検定の設定のために対話入力を必要としたが，クラスタ計算機においてバッチジョブ型で実行できるように拡張した．更に，Web を経由してクラスタ計算機上で乱数検定を実行し結果を閲覧するための Web アプリケーションもあわせて開発した．これらの拡張によって一般的なバッチジョブ型で MPI プログラムを実行できるクラスタ計算機で NIST SP800-22 の乱数検定を高速に実行することが可能となり，操作性も向上させることができた．

4.3 乱数検定の独立性解析と乱数検定の評価アルゴリズムの開発

乱数検定の独立性としては，乱数検定の検定結果の統計的な独立性が考えられるが，個々の検定で独立な異なる系列を対象とすると仮に同じ乱数検定だったとしても検定結果は統計的に独立となる．そのため，統計的な独立性だけでなく，乱数検定の類似性の概念も必要になると考えられる．そこで本研究では，乱数性の劣る度合いが異なる系列の検定結果として得らえる平均 p 値で特徴ベクトルを構成し，乱数検定間の類似度を評価する方法を提案した．以下に類似度評価の手順を示す．

① 4.1 で述べた乱数性の度合いを調整可能な系列を用いて，$l$，$e$ および $s$ のパラメータを複数設定してテストデータを生成する．
② 各乱数検定について以下の手順で特徴ベクトルを構成する．
　(1) 乱数性の度合いの異なる各データストデータに乱数検定を適用する．
　(2) テストデータ毎に検定結果として得られる p 値の平均値を算出する．
　(3) 平均 p 値のベクトルを対象とする乱数検定の特徴ベクトルとする．特徴ベクトルの次元は，乱数性の度合いが異なるテストデータの数となる．
③ 乱数検定毎に構成された特徴ベクトル間の距離を用いて類似度を評価する．本研究では，Euclid 距離を用いており，距離が近いほど類似度が高いとする．

得られた特徴ベクトルに対して，多次元尺度構成法やクラスタ分析を適用して，乱数検定間の類似度の構造を解析した．図２，図３に NIST SP800-22 に含まれる乱数検定について，これらの手法を適用した結果を示す．ここでは，NIST SP800-22 の 188 検定中の Random Excursion 系の検定を除く 162 検定を対象とした．図２は，指定する部分列の長さ $l$ を変えた場合の特徴ベクトルを，多次元尺度構成法を用いて２次元に可視化した例である．$l$ が増えると乱数検定のクラスタ構造が変化してクラスタが集約していくことがわかる．ここで各テキストラベルが１つの乱数検定に対応する．図３，図４は，$l$ とクラスタ数の関係を解析したものであり，k 平均法を用いクラスタ内の距離の二乗和が全体の距離の二乗和の 10%程度となる k をクラスタ数とした．図４では，$l$ が増えるとクラスタの個数が減少していくことがわかる．これは，$l$ が増えると乱数性が劣る度合いが弱くなり，理想的な乱数に近づくため，検出力が弱い検定は他の検定と区別がつかなくなり，クラスタ数が減少したと考えられる．




(a) $l = 4$　　(b) $l = 7$　　(c) $l = 10$

図２　多次元尺度構成法を用いた乱数検定の特徴ベクトルの可視化の例

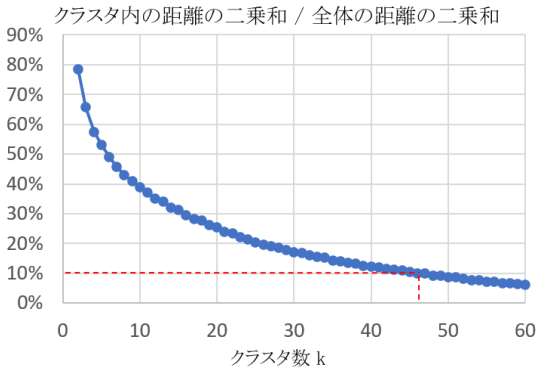



図３　クラスタ数の推定($l = 4$)

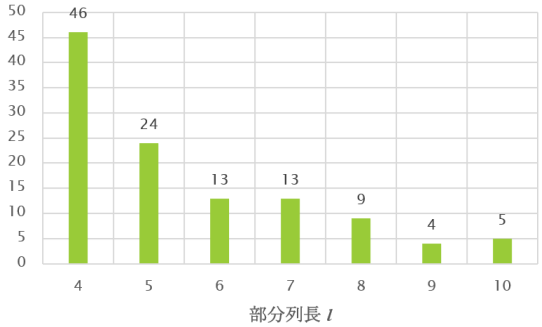



図４　乱数性の度合いとクラスタ数の関係

乱数検定の評価アルゴリズムとしては，乱数検定集合に含まれる乱数検定間の距離の総和を評価指標とすることを提案した．検定数を指定した乱数検定集合について，距離の総和が最大となるように乱数検定を選択することで，指定された検定数において，類似度が低く多様な検定集合を構成できると考えられる．　NIST SP800-22 から Random Excursion 系の検定と Non-overlapping Template Matching 検定を除いた 14 検定について，検定数 2 から 7 までの部分集合について，それぞれ距離の総和を最大化する集合を探索した例を表 1 に示す．ここで，$l$，$e$ および $s$ を変えて，336 種類の乱数性の度合いが異なる系列を生成して特徴ベクトルを構成した．加えて，乱数検定集合としての検出力も算出している．得られた集合は各検定数において，含まれる検定の類似度の低さの意味で最適な集合と考えられ，乱数検定の最小集合の候補になると考えられる．ここで，AE は Approximate Entropy 検定，LC は Linear Complexity 検定，BF は Block Frequency 検定，LR は Longest Run 検定，S1，S2 は Serial 検定，U は Universal 検定である．

検出力の評価では，どの集合も約 85%から 86%の検出力となっており，構成した集合には，検出力が高い検定だけでなく，検出力が低い検定も含まれる傾向が見られた．今回作成したテストデータについては，Approximate Entropy 検定(AE)が高い検出力をもっており，AE 検定を含むことで検定集合の検出力が高くなる傾向がみられた．これは，検出力の意味では，AE 検定単体が最小集合となることを意味しており，最小集合の決定には，集合としての多様性と検出力の高さを両立した評価指標が必要となると考えられる．ここで得られた集合は，類似度の評価において特徴ベクトルの構成に用いたテストデータに依存すると考えられ，その依存性の解析と，乱数検定の目的に応じたテストデータの設計することで目的に応じた最適な検定集合を構成できる可能性があると考えられる．

表１　距離の総和を最大化する検定集合の構成例

| 検定数 | 距離の総和 | 検出力 | 距離の総和を最大化する検定集合 |
|---|---|---|---|
| 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 |

4.4 真軌道計算に基づく擬似乱数生成の高速化と乱数検定の安全性解析

擬似乱数生成の高速化については，4.1 で述べたベルヌーイシフト写像を用いた理想的な乱数性を有する擬似乱数列の真軌道計算による計算の時間計算量は，系列長の２乗のオーダーであり，系列長の長い擬似乱数列の計算には多くの計算時間を必要としていた．ベルヌーイシフト写像の場合は，生成される系列が，初期点に関する整数係数の代数方程式の解の 2 進展開に対応することに着目して，代数方程式を，Newton 法を用いて直接解くことで擬似乱数列を得る方法を考案した．この方法の時間計算量は系列長に対応する桁数の乗算の時間計算量に対応し，高速な乗算アルゴリズムを使用することで飛躍的に計算速度を向上させることに成功した．

NIST SP800-22 においては,検定に用いる系列のサンプル数を増やすと,検定項目によっては，理想的な擬似乱数系列でも，検定に不合格になる傾向があることが知られている．本研究では，乱数検定の第２段階の検定(P 値の一様性の検定)について，Kolmogorov-Smirnov 検定を用いる場合の安全性の解析を行った．結果として，P 値の厳密分布と一様分布のずれの影響が検定統計量に与える影響として，一様分布を参照分布とする場合の検定統計量の期待値のずれの上限を解析的に与えることができた．更に一様分布の代わりにカオス真軌道で生成した理想的な乱数性を有する擬似乱数系列の検定結果の P 値の経験分布を参照分布とする 2 標本 Kolmogorov-Smirnov 検定を行うことで，サンプル数を増やした場合の検定結果が改善することを数値実験で示した．

以上のように，本研究を通してカオス真軌道を用いた乱数検定の独立性の解析について，カオス真軌道を用いた擬似乱数系列の生成系の構成と高速化，乱数検定の並列化による高速化，乱数検定の類似性の評価と最小集合の構成，乱数検定の安全性の解析において，一定の成果を得ることができたと考えている．次の課題としては，乱数検定の最小集合の構成における検定集合の検出力と多様性を両立する評価指標の構成,および,テストデータへの依存性の解析が挙げられる．

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　2件）

| | |
|---|---|
| １．著者名<br>Akihiro Yamaguchi, Asaki Saito | ４．巻<br>14 |
| ２．論文標題<br>Second-level randomness test based on the Kolmogorov-Smirnov test | ５．発行年<br>2022年 |
| ３．雑誌名<br>JSIAM Letters | ６．最初と最後の頁<br>73-76 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.14495/jsiaml.14.73 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>Asaki Saito, Akihiro Yamaguchi | ４．巻<br>28 |
| ２．論文標題<br>Pseudorandom number generator based on the Bernoulli map on cubic algebraic integers | ５．発行年<br>2018年 |
| ３．雑誌名<br>Chaos: An Interdisciplinary Journal of Nonlinear Science | ６．最初と最後の頁<br>103122 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1063/1.5048115 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>斉藤朝輝 | ４．巻<br>172 |
| ２．論文標題<br>テント写像の真軌道計算とその擬似乱数生成への応用 | ５．発行年<br>2018年 |
| ３．雑誌名<br>北海道大学数学講究録 | ６．最初と最後の頁<br>18-23 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>なし | 査読の有無<br>無 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

〔学会発表〕　計19件（うち招待講演　2件／うち国際学会　4件）

| |
|---|
| １．発表者名<br>Akihiro Yamaguchi, Asaki Saito |
| ２．発表標題<br>Characterization of randomness tests by using tests results of weakly correlated chaotic sequences |
| ３．学会等名<br>International Conference on Artificial Life and Robotics 2022（国際学会） |
| ４．発表年<br>2022年 |

１．発表者名
山口明宏，斉藤朝輝

２．発表標題
Bernoulli写像のカオス真軌道を用いた擬似乱数生成法のNewton法による高速化

３．学会等名
日本応用数理学会 2021年 研究部会連合発表会

４．発表年
2021年

１．発表者名
山口 明宏，斉藤 朝輝

２．発表標題
P値の分布とのKolmogorov-Smirnov検定を用いた乱数性判定へのカオス真軌道の応用

３．学会等名
日本応用数理学会 2020年 研究部会連合発表会

４．発表年
2020年

１．発表者名
山口明宏，斉藤朝輝

２．発表標題
P値の厳密分布が一様分布と異なる場合のKolmogorov-Smirnov検定を用いた乱数性の判定について

３．学会等名
日本応用数理学会 2020年度 年会

４．発表年
2020年

１．発表者名
Asaki Saito, Akihiro Yamaguchi

２．発表標題
Generating High-Quality Pseudorandom Sequences Using Chaotic True Orbits on Algebraic Integers

３．学会等名
The 12th International Conference on Monte Carlo Methods and Applications, July 8-12, 2019, Sydney, Australia.（国際学会）

４．発表年
2019年

１．発表者名
山口 明宏，斉藤 朝輝

２．発表標題
乱数性の劣る2値系列を用いた乱数検定の特徴付けと類似性の評価について

３．学会等名
日本応用数理学会 2019年度 年会

４．発表年
2019年

１．発表者名
小森雅弘，柿本侑毅，伴内湧生，田村健太郎，山口明宏

２．発表標題
Arnold の猫写像におけるパラメーター推定の困難さの分類と乱数性向上の試み

３．学会等名
日本応用数理学会 2019年 研究部会連合発表会

４．発表年
2019年

１．発表者名
Asaki Saito

２．発表標題
Algebraic integers and pseudorandom number generation

３．学会等名
Workshop on Fractal Geometry and Related Topics（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
斉藤朝輝，山口明宏

２．発表標題
3次代数的整数上のカオス真軌道を利用した擬似乱数生成

３．学会等名
電子情報通信学会NOLTAソサイエティ大会

４．発表年
2018年

１．発表者名
山口明宏，斉藤朝輝

２．発表標題
カオス真軌道から生成した相関系列を用いた乱数検定の特徴付け

３．学会等名
電子情報通信学会NOLTAソサイエティ大会

４．発表年
2018年

１．発表者名
多久島秀平，田村健太郎，斉藤朝輝，山口明宏

２．発表標題
Arnoldの猫写像のカオス真軌道の生成と乱数性の解析

３．学会等名
日本応用数理学会 2018年度 年会

４．発表年
2018年

１．発表者名
山口明宏，斉藤朝輝

２．発表標題
一様分布との適合度検定を用いた乱数性判定におけるP値の分布の離散性の影響の解析

３．学会等名
日本応用数理学会 2018年度 年会

４．発表年
2018年

１．発表者名
斉藤朝輝

２．発表標題
Finite-state approximation of a pseudorandom number generator using true orbits of the Bernoulli map

３．学会等名
Workshop「数論とエルゴード理論」

４．発表年
2018年

１．発表者名
山口明宏，斉藤朝輝

２．発表標題
乱数性の劣る2値系列を用いた乱数検定の特徴付けについて

３．学会等名
日本応用数理学会 第14回 研究部会連合発表会

４．発表年
2018年

１．発表者名
Asaki Saito

２．発表標題
Pseudorandom number generator based on the binary expansion of algebraic integers and its p-adic analogue

３．学会等名
Prime Numbers and Automatic Sequences: Determinism and Randomness（招待講演）（国際学会）

４．発表年
2017年

１．発表者名
山口明宏，斉藤朝輝

２．発表標題
乱数検定の独立性解析に向けた区分線形写像のカオス真軌道によるマルコフ過程の構成

３．学会等名
日本応用数理学会2017年度年会

４．発表年
2017年

１．発表者名
山口明宏

２．発表標題
NIST検定の検定結果の独立性

３．学会等名
第３回有限体理論とその擬似乱数系列生成への応用ワークショップ

４．発表年
2017年

１．発表者名
斉藤朝輝

２．発表標題
代数的整数上のBernoulli写像による擬似乱数生成

３．学会等名
第３回有限体理論とその擬似乱数系列生成への応用ワークショップ

４．発表年
2017年

１．発表者名
Asaki Saito

２．発表標題
Continued fractions and pseudorandom numbers based on p-adic chaotic maps

３．学会等名
Workshop “Number Theoretical Aspects of Tilings and Dynamics”

４．発表年
2017年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

| | 氏名<br>（ローマ字氏名）<br>（研究者番号） | 所属研究機関・部局・職<br>（機関番号） | 備考 |
|---|---|---|---|
| 研究分担者 | 斉藤　朝輝<br>(Saito Asaki)<br>(60344040) | 公立はこだて未来大学・システム情報科学部・教授<br>(20103) | |

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

| 共同研究相手国 | 相手方研究機関 |
|---|---|