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　６ 年　 ６ 月　 ４ 日現在

機関番号：１７４０１
研究種目：基盤研究(C)（一般）
研究期間：2019～2023
課題番号：１９Ｋ１２１５８

研究課題名（和文）カオス理論を活用したランダム技術に関する基礎研究

研究課題名（英文）Fundamental Study on Random Techniques Using Chaos Theory

研究代表者
常田　明夫（Tsuneda, Akio）

熊本大学・大学院先端科学研究部（工）・教授

研究者番号：４０２７４４９３

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：本研究では、一次元非線形カオス写像に基づいて様々な自己相関特性をもつカオス乱数を理論的に設計し、それらをモンテカルロ積分、機械学習、ステガノグラフィ、可視光CDMA通信、ストカスティックコンピューティングなど、ランダム性を利用する技術（ランダム技術）へ応用し、その性能を評価した。その結果、各応用において、適切な自己相関特性をもつカオス乱数を用いた場合に性能向上が可能であることを明らかにした。

研究成果の学術的意義や社会的意義
乱数（ランダム性）は、様々な技術で利用されているが、どのような性質の乱数が有効であるかの議論はあまりなされてこなかった。本研究では、まず一次元非線形写像のカオス理論に基づいて様々な自己相関特性をもつ乱数の生成が可能であることを示した。そして、このカオス理論に基づいた乱数の自己相関特性の「可制御性」を利用して、様々な特性の乱数をいくつかのランダム技術へ応用し、適切な自己相関の選択によって性能向上が可能であることが示された。今後、さらなる性能向上や他の技術への応用などが期待できる。

研究成果の概要（英文）：In this research, we theoretically design chaotic random numbers with various auto-correlation properties based on one-dimensional chaotic maps. The chaos-based random numbers are applied to Monte-Carlo integration, machine learning, steganography, visible-light CDMA communication, and stochastic computing, which utilize randomness. It has been shown that chaos-based random numbers with appropriate auto-correlation properties can enhance the performance of these applications.

研究分野：非線形理論、情報通信

キーワード：カオス理論　ランダム技術　乱数　自己相関

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

カオスとは、単純な決定論的システムからランダムな現象を生じるもので、その現象自体を興味の対象とした研究の他、乱数生成やランダム符号生成、カオスニューラルネットワーク、暗号など、特に情報・通信分野での応用の試みが多くなされてきた。これらの応用は、何らかの「ランダム性」を必要とするもので、本報告書では「ランダム技術」と総称する。カオスがもつランダム性は、これらのランダム技術へ利用できることが期待できる。しかしながら、「ランダム性」には、様々な種類の性質があり、いかなる「ランダム性」が有効であるかは、各々のランダム技術に依存する。

例えば、暗号用乱数への応用に関しては、予測不可能性が求められるため、相関のない乱数の利用が望ましい。一方、非同期 CDMA（符号分割多元接続）通信において用いるスペクトル拡散符号（擬似ランダム符号）としては、ある適切な負の自己相関をもつものが、無相関な符号よりもビット誤り率を低減できることが知られている。また、モンテカルロ積分と呼ばれる乱数を用いた数値積分においても、負の自己相関をもつ乱数を用いることで、真の積分値への収束を速くできることも明らかにされている。また、確率的現象を乱数で模倣して行うモンテカルロシミュレーションにおいては、対象とする確率的現象の確率モデルに近い乱数を用いることが、シミュレーション精度の向上へつながる。

非同期 CDMA 通信で有用な負の自己相関については、最適特性が理論的に明らかにされるとともに、その最適特性に近いスペクトル拡散符号がカオス理論により設計・実現され、その有用性が明らかにされたが、その他の応用に関しては、求められる「ランダム性」に違いがあるにも関わらず、この点にあまり注意が払われていなかった。したがって、本研究においては、カオス理論をランダム技術へ応用する場合に、「カオスのいかなる『ランダム性』を活用するのか？」という学術的問いを核心として位置づける。

２．研究の目的

本研究は、カオス理論に基づいた乱数や符号系列を種々のランダム技術（モンテカルロ積分、機械学習、ステガノグラフィ、CDMA 通信、ストカスティックコンピューティングなど）へ応用し、既存技術の性能向上やカオス理論の新しい応用の創成を目指すものである。

カオスは、単純な決定論的システムから生じるランダム現象で、用いる決定論的システムに依存して様々な性質のカオス時系列（確率変数列の一種）が生成可能である。中でも、あるクラスの一次元非線形カオス写像を用いると、不変密度と呼ばれる確率密度関数が理論的に与えられ、これに基づいて、生成されるカオス時系列の統計的性質の理論的評価が可能であり、また所望の特性をもつカオス時系列の設計を行うことも可能である。

前述したように、各ランダム技術において有用な「ランダム性」が異なるため、求められる「ランダム性」に応じて、カオス時系列を設計することが非常に重要となる。本研究代表者は，独自のアイディアにより，無相関・正相関・負相関など種々の統計的性質を有するカオス系列の簡単な設計法を理論的に与えている。その中で、カオス写像として有名なベルヌイ写像を用いた手法においては、従来の擬似乱数生成器である線形フィードバックシフトレジスタ（LFSR）およびその一般形である非線形フィードバックシフトレジスタ（NFSR）に基づいた実現が可能であり，従来符号とカオス理論を組み合わせた応用を可能にした。また、既存の乱数に対して、LFSR/NFSR を用いた後処理を施すことにより、所望の特性をもつ乱数へ変換することが可能であることも示している。

このように、本研究代表者がもつ独自の「カオス設計技術」は、様々な性質（ランダム性）をもつカオス時系列（乱数）の生成を可能にしており、各ランダム技術で求められる「ランダム性」に適応させることで、その性能向上が期待される。さらに、従来、「ランダム性」が必要とされてなかった技術にもランダム性を導入することで、新たな応用技術の創成を目指す。

３．研究の方法

主として、以下の(1)～(6)のテーマについて検討を行った。

(1) カオス理論に基づいた乱数生成

ベルヌイ写像やテント写像および様々な 2 値関数用いて生成したカオス 2 値系列の自己相関特性を理論的に評価する。また、2 つのカオス 2 値系列を組み合わせて新しい 2 値系列を生成し、その自己相関特性を調べる。

(2) モンテカルロ積分

様々な自己相関特性のカオス乱数を用いてモンテカルロ積分を行い、自己相関特性と解の収束の速さの関係について検討する。また、カオス２値系列を用いて生成した有限ビットの一様な実数乱数を用いた場合についても検討する。

(3) 機械学習への応用
MNIST データの深層学習において、雑音を付加した場合や重みの初期分布を変えた場合の正答率の変化について検討する。

(4) ステガノグラフィへの応用
非線形フィードバックシフトレジスタ系列に基づいた２値直交行列による直交変換（ドブルイン変換）を用いたステガノグラフィについて検討する。

(5) 可視光 CDMA 通信
カメラ通信を想定した CDMA 通信のシミュレーションを行い、どのようなスペクトル拡散符号が有効であるかを検討する。

(6) ストカスティックコンピューティング
カオス２値系列のストカスティックコンピューティングへの応用を試みる。

４．研究成果
(1) カオス理論に基づいた乱数生成
ベルヌイ写像／テント写像および Walsh 関数を用いることで互いに直交する独立同分布（i.i.d.）のカオス２値系列が生成できることを理論的に明らかにした。次に、様々な自己相関特性をもつ乱数の実現のために、２つのマルコフ２値系列を組み合わせた新たな２値乱数の生成法を提案した。その結果、マルコフ情報源の様々な組み合わせで、結合後の２値乱数の自己相関特性は多様な特徴をもつことが明らかになった。また、２つのカオス 2 値系列を組み合わせて新たな 2 値系列を生成する方法を提案し、その自己相関特性を調査した。その結果、単一のカオス写像と単一の 2 値関数の組合せでは実現できない様々な自己相関特性をもつ 2 値系列が生成可能であることを明らかにした。

(2) モンテカルロ積分
理論上 i.i.d.であるカオス２値系列を用いて有限ビットの一様な実数乱数を生成し、これを用いていくつかの被積分関数に対してモンテカルロ積分を行い、真値との 2 乗誤差の挙動を確認した。その結果、16 ビットまたは 32 ビットのカオス乱数の場合は，標準 C ライブラリの random()関数による乱数を用いたものと同じような収束の挙動を示すことが明らかになった。また、モンテカルロ積分は用いる乱数の自己相関特性によって収束の速さが変化するため、乱数の自己相関特性を容易に制御できるカオス乱数の利用を試みた。ここで一様分布のカオス乱数を生成するテント写像を用い、そのパラメータを変えて様々な自己相関特性のカオス乱数を生成し、これを用いてモンテカルロ積分を行った。その結果、パラメータによってモンテカルロ積分の精度が変化することが明らかになった。また、積分区間を分割することで解の精度が向上することも明らかにした。

(3) 機械学習への応用
MNIST データの深層学習において、雑音を付加した場合の正答率の変化について検討した。雑音として、テント写像から生成されるカオス系列を用い、意図的に相関性を変えて、正答率への影響を調査した。その結果、雑音の相関性が正答率にある程度影響していることを確認した。また、ネットワークに与える重みの初期分布として、ガウス分布および一様分布を与え、一様分布については相関性も変えて、深層学習にどのような影響を及ぼすかについて検討した。その結果、重みの初期分布の与え方や相関性を変えると学習に影響があることが確認できた。

(4) ステガノグラフィへの応用
非線形フィードバックシフトレジスタ系列に基づいた２値直交行列による直交変換（ドブルイン変換）を用いたステガノグラフィについて、よく知られている直交変換のアダマール変換との組み合わせも含め、いくつかの方法を検討した。その結果、画像の埋め込み方によっては、アダマール変換と組み合わせることで、性能が向上することを確認した。また、これらの直交変換を利用した場合に、係数行列のビット反転が原画像にどのような影響を与えるかについて検討した。その結果、直交変換によって、ビット反転の影響が異なっていることが分かった。

(5) 可視光 CDMA 通信
カメラ通信を想定した CDMA 通信のシミュレーションを行い、負相関スペクトル拡散符号や NFSR 直交符号が有効であることを確認した。

(6) ストカスティックコンピューティング
カオス２値系列のストカスティックコンピューティングへの応用を試みた。AND ゲートによる乗算について、入力するカオス２値系列の自己相関特性が演算結果の収束特性に影響を与えることを明らかにした。

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　4件／うち国際共著　0件／うちオープンアクセス　3件）

１．著者名 Tsuneda Akio	４．巻 4
２．論文標題 Auto-Correlation Functions of Chaotic Binary Sequences Obtained by Alternating Two Binary Functions	５．発行年 2024年
３．雑誌名 Dynamics	６．最初と最後の頁 272～286
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/dynamics4020016	査読の有無 有
オープンアクセス 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 －

１．著者名 TSUNEDA Akio	４．巻 E104.A
２．論文標題 Orthogonal Chaotic Binary Sequences Based on Tent Map and Walsh Functions	５．発行年 2021年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1349～1352
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020EAL2119	査読の有無 有
オープンアクセス 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 －

１．著者名 Tsuneda Akio	４．巻 23
２．論文標題 Various Auto-Correlation Functions of m-Bit Random Numbers Generated from Chaotic Binary Sequences	５．発行年 2021年
３．雑誌名 Entropy	６．最初と最後の頁 1295～1295
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/e23101295	査読の有無 有
オープンアクセス 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 －

１．著者名 Akio Tsuneda	４．巻 Vol.21, No.10
２．論文標題 Orthogonal Chaotic Binary Sequences Based on Bernoulli Map and Walsh Functions	５．発行年 2019年
３．雑誌名 Entropy	６．最初と最後の頁 930
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/e21100930	査読の有無 有
オープンアクセス 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 －

〔学会発表〕　計19件（うち招待講演　1件／うち国際学会　3件）

1．発表者名
Muhammad Ahmad Abdulfattah, Akio Tsuneda

2．発表標題
A Study on Generating Correlated Random Numbers with Gaussian Distribution

3．学会等名
電子情報通信学会総合大会

4．発表年
2024年

1．発表者名
Akio Tsuneda, Masato Uetani

2．発表標題
A Study on Monte-Carlo Integration with Divided Interval Using Chaotic Sequences

3．学会等名
European Conference on Circuit Theory and Design（国際学会）

4．発表年
2023年

1．発表者名
Akio Tsuneda, Masahiro Fujikawa

2．発表標題
Auto-Correlation Properties of Binary Sequences Obtained by Switching Two Bernoulli Chaotic Binary Sequences

3．学会等名
International Conference on ICT Convergence（国際学会）

4．発表年
2023年

1．発表者名
常田明夫，藤川雅浩

2．発表標題
2つのカオス2値系列を組み合わせた2値系列の自己相関について

3．学会等名
電子情報通信学会ソサイエティ大会

4．発表年
2023年

１．発表者名
常田明夫，上谷真人

２．発表標題
区間を分割したモンテカルロ積分についての一検討

３．学会等名
電気・情報関係学会九州支部連合大会

４．発表年
2023年

１．発表者名
奥野修造，常田明夫

２．発表標題
2つのマルコフ2値系列を組み合わせた乱数の自己相関特性について

３．学会等名
電子情報通信学会非線形問題研究会

４．発表年
2022年

１．発表者名
黒木優作，常田明夫

２．発表標題
MNISTの深層学習における重みの初期分布の影響について

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
2022年

１．発表者名
小森琢巳，常田明夫

２．発表標題
2値直交行列を用いた2次元直交変換対におけるビット反転の影響

３．学会等名
第30回電子情報通信学会九州支部学生会講演会

４．発表年
2022年

１．発表者名
織田裕也，常田明夫

２．発表標題
カメラ通信を想定した光CDMA方式に関する基礎検討

３．学会等名
第30回電子情報通信学会九州支部学生会講演会

４．発表年
2022年

１．発表者名
辻 尭英，常田明夫

２．発表標題
カオス2値系列を用いた有限ビット乱数によるモンテカルロ積分の一検討

３．学会等名
第30回電子情報通信学会九州支部学生会講演会

４．発表年
2022年

１．発表者名
阿部 楓，常田明夫

２．発表標題
CDMA方式とドブルイン系列を用いた圧縮センシングの一検討

３．学会等名
電子情報通信学会非線形問題研究会

４．発表年
2022年

１．発表者名
多賀舜哉，常田明夫

２．発表標題
カオス2値系列を用いたStochastic Computing の一検討

３．学会等名
電子情報通信学会非線形問題研究会

４．発表年
2022年

１．発表者名
常田明夫

２．発表標題
カオス理論に基づいた乱数生成～種々の自己相関の実現～

３．学会等名
電子情報通信学会スマートインフォメディアシステム研究会（招待講演）

４．発表年
2022年

１．発表者名
常田明夫，前田成輝

２．発表標題
非線形シフトレジスタに基づいた後処理によるマルコフ２値乱数の生成

３．学会等名
電子情報通信学会非線形問題研究会

４．発表年
2021年

１．発表者名
常田明夫

２．発表標題
テント写像とWalsh 関数に基づいた直交カオス２値系列について

３．学会等名
2019年電子情報通信学会ソサイエティ大会

４．発表年
2019年

１．発表者名
木村公康，常田明夫

２．発表標題
カオス理論に基づく乱数を用いたモンテカルロ積分の基礎検討

３．学会等名
第27回電子情報通信学会九州支部学生会講演会

４．発表年
2019年

１．発表者名
平井大智，常田明夫

２．発表標題
テント型NFSRを用いたブロック暗号システムの一検討

３．学会等名
第27回電子情報通信学会九州支部学生会講演会

４．発表年
2019年

１．発表者名
阿部優志，常田明夫

２．発表標題
SIK方式光CDMA通信におけるSS符号の平衡性の影響

３．学会等名
第27回電子情報通信学会九州支部学生会講演会

４．発表年
2019年

１．発表者名
Akio Tsuneda, Hiroki Shiraishi

２．発表標題
A Study on Auto-Correlation Functions of Quaternary Random Sequences Generated from Chaotic Binary Sequences

３．学会等名
2019 International Symposium on Nonlinear Theory and its Applications（国際学会）

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

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