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　元 年　 ６ 月 ２４ 日現在

機関番号：２０１０３
研究種目：基盤研究(C)（一般）
研究期間：2015～2018
課題番号：１５Ｋ００３４２

研究課題名（和文）真軌道計算の展開：非線形現象の解明と擬似乱数生成への応用

研究課題名（英文）Development of true orbit computation: analysis of nonlinear phenomena and application to pseudorandom number generation

研究代表者

斉藤　朝輝（Saito, Asaki）

公立はこだて未来大学・システム情報科学部・准教授

研究者番号：６０３４４０４０

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）：誤差の入らない新しいシミュレーション法である真軌道計算を使った非線形現象の解明と真軌道計算の擬似乱数生成への応用に関する研究を行った．特に，擬似乱数生成に関しては，初期点（種）を良質な擬似乱数列に変換するアルゴリズムだけでなく，初期点の適切な選択方法についても明らかにした．また関連する連分数の研究（p進連分数アルゴリズムの構築とその周期性の証明）も行った．
なお，研究成果の一部をまとめた論文Saito, Yamaguchi, Chaos 28, 103122 (2018)は，掲載された論文誌のFeatured Articleに選ばれ，また一般向けの紹介記事がAIP Scilightに掲載された．

研究成果の学術的意義や社会的意義
擬似乱数は，モンテカルロ法を使った数値計算や暗号通信で欠かせないのはもちろん，シミュレーションなどでも活用されており，現代社会を支える基盤技術の１つと言える．本研究で得られた真軌道擬似乱数生成器によって，高品質な（非周期性などの性質が理論的に保証され，また統計性も極めて良好な）擬似乱数列を大量に生成できるようになった．
また，真軌道計算は従来のシミュレーション法とは比較にならないほど高精度なシミュレーションを実現する．しかし，提案されてから日が浅く，とりわけ応用に関しては初歩的な段階にとどまっており，発展の余地が大きい．本研究課題によって，特に擬似乱数生成への応用に関しては研究が大きく進展した．

研究成果の概要（英文）：True orbit computation is an errorless simulation method recently proposed by Saito et al. In order to promote its new development, we have conducted two types of researches: (i) Analyses of nonlinear phenomena by using the true orbit computation. (ii) Application of the true orbit computation to pseudorandom number generation. In particular, as for (ii), we have not only proposed algorithms that transform an initial point (seed) into a high-quality pseudorandom sequence but also have established methods for properly selecting initial points. Also, we have conducted related researches on continued fractions (we have constructed several p-adic continued fraction algorithms and also proved their periodicity for all the quadratic elements).

研究分野：非線形科学

キーワード：真軌道計算　カオス　非線形現象　擬似乱数　代数的数　p進数　連分数　Lagrangeの定理

様　式　C－１９、F－１９－１、Z－１９、CK－１９（共通）

１．研究開始当初の背景

(1) 非線形科学や複雑系の分野では，計算機を使ったシミュレーション解析が幅広く行われている．しかし，シミュレーションで通常使われる倍精度浮動小数点数のような固定精度の数表現では，実数は不可避的に丸められ，演算にも誤差が生じうる．非線形系や複雑系は微視的スケールの摂動に対して“デリケート”に応答しうるため，たとえ個々の計算誤差が小さくても，膨大な数の計算を繰り返すこれらの系のシミュレーションにおいては，計算誤差は深刻な問題となりうる．特に，初期値鋭敏性を特徴としてもつカオス系に関しては，そのシミュレーションがどの程度有効と言えるかについて，半世紀近くにわたり議論されてきている．実際に，Open Flow System の空間方向分岐のように，固定精度の数表現の使用によって，シミュレーションで本来再現したかった系の巨視的・定性的振る舞いが壊されてしまい，系に存在しない人工的な挙動が現れる場合もあることがわかっている．

(2) 擬似乱数は，モンテカルロ法を使った数値計算や暗号通信で欠かせないのはもちろん，シミュレーションなどでも活用されており，現代社会を支える基盤技術の１つと言える．乱雑な振る舞いをみせるカオスを擬似乱数生成に応用することは古くから考えられてきている．理論上，擬似ランダムビット列を生成するには，カオス写像の中でも最も単純な単位区間上の Bernoulli 写像 $x \mapsto 2x \bmod 1$ やテント写像 $x \mapsto 1-|2x-1|$ をシミュレートできればよい．しかし，従来のシミュレーション法を使って，これらの写像の典型的軌道（カオス的軌道）を生成するのは困難であるため，これまでのカオス擬似乱数生成にはより複雑な写像を使用せざるをえなかった．

２．研究の目的

我々はあるクラスの力学系（区分的線形写像を含む区分的 1 次分数写像で表現される力学系）の真軌道を計算する新しい方法を構築した．[1,2] この方法は，数として整数ベクトルで表現できる代数的数を採用し，計算機で正確に実行できる整数演算のみを用いて，軌道生成を行う点に特長がある．本研究課題では，この真軌道計算を使った非線形現象の解明と真軌道計算の擬似乱数生成への応用とを目的に研究を行った．

参考文献

[1] A. Saito, S. Ito, Physica D 268 (2014), 100-105.
[2] A. Saito, S. Yasutomi, J. Tamura, S. Ito, Chaos 25 (2015), 063103.

３．研究の方法

本研究の方法の最大の特色は，我々が構築した真軌道生成法を用いる点である．この方法を使えば，極めて高い精度が要求されるシミュレーションでも誤差なしで行うことができ，また，Bernoulli 写像やテント写像を使って擬似乱数を生成することが可能になる（これらは，従来のシミュレーション法では不可能だった）．この真軌道生成法を使って，カオス真軌道を使った擬似乱数生成器の構築と，関連する連分数の研究を主に行った．

４．研究成果

本研究課題では，次の研究を行った．1. 3 次実代数的整数上の Bernoulli 写像の真軌道を使った擬似乱数生成器の構築．2. p=2 進数体の 2 次代数的要素上の Bernoulli 写像の真軌道を使った擬似乱数生成器の構築．3. 1 と 2 それぞれの擬似乱数生成器に関して，以下の意味で極めて良い性質を持つ初期点（seed）集合のクラスの特定．そのクラスに所属する初期点集合 I に関しては，I に含まれる各要素が全て異なる代数体に所属する．その他にも，I は，一様性，一般性，各要素の連分数展開の純周期性という性質をもつ．　4．虚 2 次代数的整数の集合のクラスで，同様の性質をもつものの特定．　5．真軌道を使った擬似乱数生成器を有限状態で近似する擬似乱数生成器の構築．6. p 進数体の要素を連分数展開するためのアルゴリズムをいくつか構成し，それらが 2 次代数的要素に対してだけ周期的展開をあたえることを証明．7．多次元 p 進連分数アルゴリズムの構築．　8．サブスティテューションと Rauzy フラクタルの p 進世界への拡張，など．

これらの成果は，専門誌や国内外の会議で発表済み，もしくは発表準備中である（補助事業期間内には，論文発表を 10 件，学会発表を 47 件行った）．特に，1 と 3 の一部の成果をまとめた論文 A. Saito, A. Yamaguchi, Pseudorandom number generator based on the Bernoulli map on cubic algebraic integers, Chaos 28, 103122 (2018)は，掲載された Chaos 誌の Featured Article に選ばれ，また一般向けの紹介記事が AIP Scilight に掲載された．以下では，この研究について簡単に紹介する．

3 次代数的整数とは，最高次係数 1 の 3 次既約多項式 X^3+bX^2+cX+d（ただし，$b,c,d \in Z$）の根となる複素数のことである．

ここで，2 つの集合 $\overline{S}$ と S，ならびに $\overline{S}$ から S への写像 π を定義する．

- S を，次の条件(i)-(iii)をみたす $(b,c,d) \in Z^3$ の集合とする：(i) $b^2-3c \le 0$，(ii) $d<0$，(iii) $1+b+c+d>0$（図 1）．$(b,c,d) \in \overline{S}$ のとき，多項式 X^3+bX^2+cX+d

はただ一つ実根αを単位開区間$(0,1)$内にもち，さらにαの次数は3である（つまりαは3次代数的整数である）ことがわかる．

- Sを，X^3+bX^2+cX+d（ただし，$(b,c,d)\in\overline{S}$）の根となる$(0,1)$内の3次代数的整数の集合とする．
- πを，$(b,c,d)\in\overline{S}$に対して，X^3+bX^2+cX+dの唯一の実根$\alpha\in S$を対応させる$\overline{S}$からSへの写像とする．πは全単射であることがわかる．

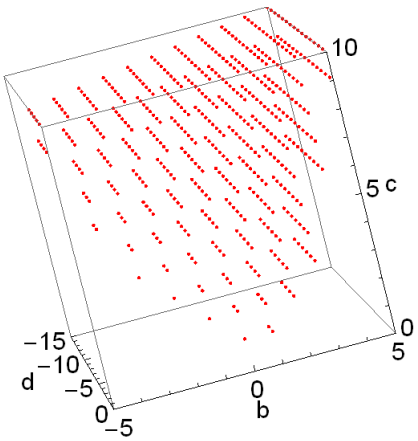

図1　集合$\overline{S}$

Bernoulli 写像$M_B(x)=2x \pmod 1$は，Sの元をSの元にうつすことが示せる．さらに，S上のM_Bに対応する，$\overline{S}$上の変換$\overline{M}_B=\pi^{-1}\circ M_B\circ\pi$が以下で与えられることも示せる．

$1+2b+4c+8d>0$のとき

$$\overline{M}_B:\ \begin{pmatrix}b\\c\\d\end{pmatrix}\mapsto\begin{pmatrix}2&0&0\\0&4&0\\0&0&8\end{pmatrix}\begin{pmatrix}b\\c\\d\end{pmatrix}.$$

$1+2b+4c+8d<0$のとき

$$\overline{M}_B:\ \begin{pmatrix}b\\c\\d\end{pmatrix}\mapsto\begin{pmatrix}2&0&0\\4&4&0\\2&4&8\end{pmatrix}\begin{pmatrix}b\\c\\d\end{pmatrix}+\begin{pmatrix}3\\3\\1\end{pmatrix}.$$

$\overline{M}_B$は整数演算のみを使って計算可能であり，初期点$(b_0,c_0,d_0)\in\overline{S}$に対して$\overline{M}_B$を反復適用することにより$\overline{M}_B$の真軌道$\{(b_n,c_n,d_n)\}_{n=0,1,2,\cdots}$が生成できる．擬似ランダムビット列$\{\varepsilon_n\}_{n=0,1,2,\cdots}$を得るためには，$1+2b_n+4c_n+8d_n>0$のとき$\varepsilon_n=0$，$1+2b_n+4c_n+8d_n<0$のとき$\varepsilon_n=1$とすればよい．

この擬似乱数生成器に関して，初期点（seed）の適切な選択方法についても明らかにした．$\pi(b_0,c_0,d_0)\in S$は有理数ではないため，$\{\varepsilon_n\}_{n=0,1,2,\cdots}$の非周期性は保証される．その意味で，$S$の任意の要素は擬似ランダムビット列を生成するための初期点として使用できる．

複数の擬似ランダムビット列を生成する場合には，初期点の集合$I\subset\overline{S}$を用意する必要がある．ここで，正の整数cに対して定まる$\overline{S}$の部分集合

$$\overline{I}_{0,c}=\left\{(0,c,d)\in\overline{S}\mid d\in\{-1,-2,\ldots,-c\}\right\}$$

を考える．この$\overline{I}_{0,c}$は，初期点集合として以下の良い性質をもつ．

性質1：cが十分大きければ，$I_{0,c}=\pi(\overline{I}_{0,c})$の要素は単位区間内をほぼ一様に分布する．

性質2：$I_{0,c}$の要素はそれぞれ異なる3次体に所属する．

さらに，大規模な検定を行い，生成された擬似乱数列の統計性がよいことも確認した．また，現在最も広く使われている擬似乱数生成器である Mersenne Twister MT19937 との比較を行い，我々の擬似乱数生成器の優位点も明らかにした．

5．主な発表論文等

〔雑誌論文〕（計 10 件）

① Asaki Saito, Jun-ichi Tamura, Shin-ichi Yasutomi, Multidimensional p-adic continued fraction algorithms, Mathematics of Computation, 印刷中，査読有
DOI:10.1090/mcom/3458

② Asaki Saito, Jun-ichi Tamura, Shin-ichi Yasutomi, Continued fraction algorithms and Lagrange's theorem in Q_p, Commentarii Mathematici Universitatis Sancti Pauli 67 (2019)，印刷中，査読有

③ Asaki Saito, Akihiro Yamaguchi, Pseudorandom number generator based on the Bernoulli map on cubic algebraic integers, Chaos 28 (2018), 103122，査読有
DOI: 10.1063/1.5048115

④ 斉藤朝輝，田村純一，安冨真一，p 進数体上の連分数アルゴリズムとその周期性，京都大学数理解析研究所講究録 2092 (2018)，55-62，査読無
http://www.kurims.kyoto-u.ac.jp/~kyodo/kokyuroku/contents/pdf/2092-07.pdf

⑤ 安冨真一，斉藤朝輝，田村純一，Multidimensional p-adic continued fraction algorithms，京都大学数理解析研究所講究録 2092 (2018)，63-74，査読無

http://www.kurims.kyoto-u.ac.jp/~kyodo/kokyuroku/contents/pdf/2092-08.pdf

⑥ 斉藤朝輝，テント写像の真軌道計算とその擬似乱数生成への応用，北海道大学数学講究録 172 (2018)，18-23，査読無
DOI: 10.14943/81533

⑦ Asaki Saito, Akihiro Yamaguchi, Pseudorandom number generation using chaotic true orbits of the Bernoulli map, Chaos 26 (2016), 63122, 査読有
DOI: 10.1063/1.4954023

⑧ Jun-ichi Tamura, Shin-ichi Yasutomi, Dual substitutions over R>0-powered symbols, RIMS Kokyuroku Bessatsu B58 (2016), 231-242, 査読有

⑨ Jun-ichi Tamura, Shin-ichi Yasutomi, Substitutions over C-powered symbols, and Rauzy fractals for imaginary directions, RIMS Kokyuroku Bessatsu B58 (2016), 191-229, 査読有

⑩ Asaki Saito, Shin-ichi Yasutomi, Jun-ichi Tamura, Shunji Ito, True orbit simulation of piecewise linear and linear fractional maps of arbitrary dimension using algebraic numbers, Chaos 25 (2015), 63103, 査読有
DOI: 10.1063/1.4921938

〔学会発表〕(計 47 件)

① 田村純一, An exact formula related to simultaneous approximations of p-adic numbers, Workshop「数論とエルゴード理論」, 2019

② Asaki Saito, Algebraic integers and pseudorandom number generation, Workshop on Fractal Geometry and Related Topics, 2018

③ 斉藤朝輝，山口明宏，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，電子情報通信学会 NOLTA ソサイエティ大会，2018

④ 尾ヶ瀬拓哉，斉藤朝輝，C.elegans の歩行の調節と神経系のダイナミクス，電子情報通信学会 NOLTA ソサイエティ大会，2018

⑤ 斉藤朝輝, Finite-state approximation of a pseudorandom number generator using true orbits of the Bernoulli map, Workshop「数論とエルゴード理論」, 2018

⑥ Jun-ichi Tamura, Foundation of Rauzy fractals in the p-adic world, Workshop on Fractal Geometry and Related Topics, 2018

⑦ Jun-ichi Tamura, Generation of a set of complex numbers satisfying certain Boolean inequality, Workshop on Fractal Geometry and Related Topics, 2018

⑧ 田村純一, Some multi-dimensional continued fractions and the linear independence measure of related values, Workshop「数論とエルゴード理論」, 2018

⑨ 安冨真一, Certain p-adic continued fraction expansion, Workshop「数論とエルゴード理論」, 2018

⑩ Shin-Ichi Yasutomi, Certain multidimension p-adic continued fraction algorithm and cubic numbers, Diophantine Analysis and Related Fields 2018, 2018

⑪ 山口明宏，斉藤朝輝，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，日本応用数理学会第 14 回研究部会連合発表会，2018

⑫ Asaki Saito, Pseudorandom number generator based on the binary expansion of algebraic integers and its p-adic analogue, Prime Numbers and Automatic Sequences: Determinism and Randomness, 2017

⑬ Asaki Saito, Continued fractions and pseudorandom numbers based on p-adic chaotic maps, Workshop “Number Theoretical Aspects of Tilings and Dynamics”, 2017

⑭ 斉藤朝輝，代数的整数上の Bernoulli 写像による擬似乱数生成，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，2017

⑮ Asaki Saito, Continued fraction algorithms and Lagrange's theorem in the p-adic number field, Analytic Number Theory and Related Areas, 2017

⑯ Asaki Saito, Continued fraction algorithms and Lagrange's theorem in Qp, New Advances in Symbolic Dynamics, 2017

⑰ 斉藤朝輝, Algorithms for p-adic continued fractions and Lagrange's theorem, Workshop「数論とエルゴード理論」, 2017

⑱ 斉藤朝輝，真軌道計算とカオス，複雑系数理の新展開，2017

⑲ 斉藤朝輝，山口明宏，Bernoulli 写像のカオス的真軌道を使った擬似乱数生成，日本物理学会第 72 回年次大会，2017

⑳ Jun-Ichi Tamura, Convergence theorems of substitutions and Rauzy fractals in the p-adic world, Prime Numbers and Automatic Sequences: Determinism and Randomness, 2017

㉑ Jun-ichi Tamura, Rauzy fractals in the p-adic world, New Advances in Symbolic Dynamics, 2017

㉒ 田村純一, p-adic substitutions, convergence theorems, and Rauzy fractals, Workshop「数論とエルゴード理論」, 2017

㉓ Shin-Ichi Yasutomi, Multidimensional p-adic continued fraction algorithms and p-reduced matrices, Prime Numbers and Automatic Sequences: Determinism and Randomness, 2017
㉔ Shin-Ichi Yasutomi, On p-reduced lattice and multidimensional p-adic continued fraction algorithms, Analytic Number Theory and Related Areas, 2017
㉕ Shin-Ichi Yasutomi, Multidimensional p-adic continued fraction algorithms and cubic number fields, Workshop “Number Theoretical Aspects of Tilings and Dynamics”, 2017
㉖ 安冨真一, On multidimensional p-adic continued fraction algorithms and p-reduced matrices, Workshop「数論とエルゴード理論」, 2017
㉗ 山口明宏, 斉藤朝輝, 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, 日本応用数理学会 2017 年度年会, 2017
㉘ 山口明宏, NIST 検定の検定結果の独立性, 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, 2017
㉙ Asaki Saito, p-adic continued fractions and Lagrange's theorem, Analysis on Fractals and Graphs Workshop, 2016
㉚ Asaki Saito, Pseudorandom number generator with the Bernoulli map on cubic algebraic integers, Workshop Number Theory and Ergodic Theory 2016, 2016
㉛ Asaki Saito, Pseudorandom number generators using true orbits of the 2x modulo 1 map on algebraic integers, Substitutions and Continued Fractions, 2016
㉜ Jun-ichi Tamura, p-adic substitutions and Rauzy fractals, Analysis on Fractals and Graphs Workshop, 2016
㉝ Jun-ichi Tamura, Fractional calculi of substitutions, Rauzy fractals, and multidimensional complex continued fractions, Workshop Number Theory and Ergodic Theory 2016, 2016
㉞ Jun-ichi Tamura, Fractional calculi of substitutions, Rauzy fractals, and diophantine approximation of complex numbers I, Substitutions and Continued Fractions, 2016
㉟ Jun-ichi Tamura, Fractional calculi of substitutions, Rauzy fractals, and diophantine approximation of complex numbers II, Substitutions and Continued Fractions (satellite), 2016
㊱ 安冨真一, Multidimensional p-adic continued fraction algorithm, 研究集会：エルゴード理論とその周辺, 2016
㊲ Shin-ichi Yasutomi, On multidimensional p-adic continued fraction, Analysis on Fractals and Graphs Workshop, 2016
㊳ Shin-ichi Yasutomi, Generalization of stepped surfaces, Workshop Number Theory and Ergodic Theory 2016, 2016
㊴ Shin-ichi Yasutomi, Generation of stepped surfaces via modified Jacobi-Perron algorithm and cubic numbers, Substitutions and Continued Fractions, 2016
㊵ 山口明宏, 斉藤朝輝, カオス真軌道から構成した相関系列に対する NIST 乱数検定の判定結果の解析, 日本応用数理学会 2016 年度年会, 2016
㊶ Asaki Saito, Pseudorandom number generation using true orbits of the Bernoulli map on algebraic integers, Sino-Japanese Workshop on Dynamical Systems and Fractals, 2015
㊷ Jun-ichi Tamura, Fractional calculus of substitutions, the Kolakoski word, the Minkowski Question - Mark function and continued fractions, Natural Extention of Arithmetic Algorithms and S-adic System, 2015
㊸ Jun-ichi Tamura, Fractional calculus of substitutions and Rauzy fractals for imaginary directions, エルゴード理論とその周辺, 2015
㊹ Jun-ichi Tamura, Fractional calculi of substitutions, Rauzy fractals, and continued fractions, Sino-Japanese Workshop on Dynamical Systems and Fractals, 2015
㊺ Shin-ichi Yasutomi, Certain multidimensional continued fraction algorithm, Natural Extention of Arithmetic Algorithms and S-adic System, 2015
㊻ Shin-ichi Yasutomi, Dual fractional substitutions, Sino-Japanese Workshop on Dynamical Systems and Fractals, 2015
㊼ 山口明宏, 斉藤朝輝, NIST 乱数検定における P 値の一様性に基づく検定結果の判定法について, 日本応用数理学会 2015 年度年会, 2015

６．研究組織

(1)研究分担者

研究分担者氏名：田村　純一

ローマ字氏名：Jun-ichi Tamura

所属研究機関名：津田塾大学
部局名：数学・計算機科学研究所
職名：研究員
研究者番号（8 桁）：90418905

研究分担者氏名：安冨　真一
ローマ字氏名：Shin-ichi Yasutomi
所属研究機関名：東邦大学
部局名：理学部
職名：教授
研究者番号（8 桁）：60230231

研究分担者氏名：山口　明宏
ローマ字氏名：Akihiro Yamaguchi
所属研究機関名：福岡工業大学
部局名：情報工学部
職名：教授
研究者番号（8 桁）：60281789