(19)日本国特許庁（ＪＰ）　(12)特　許　公　報（Ｂ２）　(11)特許番号
特許第3455748号
(P3455748)
(45)発行日　平成15年10月14日(2003.10.14)　(24)登録日　平成15年８月１日(2003.8.1)

(51)Int.Cl.⁷	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６５０	Ｇ０９Ｃ　1/00	６５０Ｂ
Ｇ０６Ｆ　7/58		Ｇ０６Ｆ　7/58	Ａ

請求項の数18(全 12 頁)

(21)出願番号　特願平11－362203
(22)出願日　平成11年12月21日(1999.12.21)
(65)公開番号　特開2001－175168(P2001－175168A)
(43)公開日　平成13年６月29日(2001.6.29)
審査請求日　平成11年12月21日(1999.12.21)

(73)特許権者　301022471
独立行政法人通信総合研究所
東京都小金井市貫井北町４－２－１
(73)特許権者　597044841
梅野　健
東京都小金井市貫井北町４－２－１　独立行政法人通信総合研究所内
(72)発明者　梅野　健
東京都小金井市貫井北町４丁目２番１号　郵政省通信総合研究所内
(74)代理人　100095407
弁理士　木村　満　（外１名）

審査官　石山　信行

(56)参考文献　特開2000－276331（ＪＰ，Ａ）
特開　平10－283344（ＪＰ，Ａ）

最終頁に続く

(54)【発明の名称】　ベクトル列の出力装置、出力方法、および、情報記録媒体

(57)【特許請求の範囲】
【請求項１】以下を備えることを特徴とするベクトル列の出力装置。
（ａ）１次元以上のベクトルxを記憶する第１の記憶部と、
（ｂ）前記第１の記憶部に記憶されたベクトルxに第１の有理ベクトル写像fを適用した結果のベクトルx'=f(x)を計算する第１の計算部と、
（ｃ）１次元以上のベクトルyを記憶する第２の記憶部と、
（ｄ）前記第１の記憶部に記憶されたベクトルxと、前記第２の記憶部に記憶された１次元以上のベクトルyとに、第２の有理ベクトル写像gを適用した結果のベクトルy'=g(x,y)を計算する第２の計算部と、
（ｅ）前記第１の計算部により計算された結果のベクトルx'と前記第２の計算部により計算された結果のベクトルy'とを結合したベクトルz'を出力する出力部と、
（ｆ）前記第１の計算部により計算された結果のベクトルx'を前記第１の記憶部に記憶させて更新する第１の更新部と、
（ｇ）前記第２の計算部により計算された結果のベクトルy'を前記第２の記憶部に記憶させて更新する第２の更新部。ただし、有理ベクトル写像とは、有理数の成分からなる１次元以上のベクトルを有理数の成分からなる１次元以上のベクトルへと変換する写像をいう。
【請求項２】前記第１の有理ベクトル写像fを１次元以上のベクトルxに０回以上適用して得られるベクトル列
x，f(x)，f(f(x))，f(f(f(x)))，…
の極限分布の密度関数は解析的な関数であり、
前記第２の有理ベクトル写像gにパラメータとして１次

元以上のベクトルλを与えた写像g(λ,・)を１次元以上のベクトルyに０回以上適用して得られるベクトル列
y, g(λ,y), g(λ,g(λ,y)), g(λ,g(λ,g(λ,y))), …
の極限分布の密度関数は当該パラメータλを有する解析的な関数であることを特徴とする請求項１に記載の出力装置。

【請求項３】前記第１の有理ベクトル写像fは、楕円関数の加法定理より導かれる有理写像、特に、ウラム＝フォン・ノイマン写像、キュービック写像、クインティック写像、又は、カツラ＝フクダ写像、一般化ウラム＝フォン・ノイマン写像、一般化キュービック写像、もしくは一般化チェビシェフ写像に所定のパラメータを与えたもののいずれかであることを特徴とする請求項２に記載の出力装置。

【請求項４】前記第２の有理ベクトル写像gは、楕円関数の加法定理より導かれる有理写像、特に、カツラ＝フクダ写像、一般化ウラム＝フォン・ノイマン写像、一般化キュービック写像、一般化チェビシェフ写像のいずれかであることを特徴とする請求項２に記載の出力装置。

【請求項５】以下を備えることを特徴とするベクトル列の出力装置。

（ａ）２次元以上のベクトルζを受け付けて、これから１次元以上のベクトルξと１次元以上のベクトルηとを生成する生成部と、

（ｂ）前記生成部により生成されたベクトルξを受け付けて、第１の有理ベクトル写像fを用いた漸化式
x[0] = ζ
x[i+1] = f(x[i])　（ただしi≧0）
により得られるベクトル列x[i]を出力する第１の出力部と、

（ｃ）前記生成部により生成されたベクトルηと、前記第１の出力部により出力されるベクトル列x[i]とを受け付けて、第２の有理ベクトル写像gを用いた漸化式
y[0] = η
y[i+1] = g(x[i],y[i])　（ただしi≧0）
により得られるベクトル列y[i]を出力する第２の出力部と、

（ｄ）前記第１の出力部により出力されるベクトル列x[i]と、前記第２の出力部により出力されるベクトル列y[i]とを結合して得られるベクトル列z[i]を結果として出力する第３の出力部。

【請求項６】前記第１の有理ベクトル写像fを１次元以上のベクトルxに０回以上適用して得られるベクトル列
x, f(x), f(f(x)), f(f(f(x))), …
の極限分布の密度関数は解析的な関数であり、
前記第２の有理ベクトル写像gにパラメータとして１次元以上のベクトルλを与えた写像g(λ,・)を１次元以上のベクトルyに０回以上適用して得られるベクトル列
y, g(λ,y), g(λ,g(λ,y)), g(λ,g(λ,g(λ,y))), …
の極限分布の密度関数は当該パラメータλを有する解析的な関数であることを特徴とする請求項５に記載の出力装置。

【請求項７】前記第１の有理ベクトル写像fは、楕円関数の加法定理より導かれる有理写像、特に、ウラム＝フォン・ノイマン写像、キュービック写像、クインティック写像、または、カツラ＝フクダ写像、一般化ウラム＝フォン・ノイマン写像、一般化キュービック写像もしくは一般化チェビシェフ写像に所定のパラメータを与えたもののいずれかであることを特徴とする請求項６に記載の出力装置。

【請求項８】前記第２の有理ベクトル写像gは、楕円関数の加法定理より導かれる有理写像、特に、カツラ＝フクダ写像、一般化ウラム＝フォン・ノイマン写像、一般化キュービック写像、一般化チェビシェフ写像のいずれかであることを特徴とする請求項６に記載の出力装置。

【請求項９】前記第１の出力部もまた請求項５に記載の出力装置であることを特徴とする請求項５に記載の出力装置。

【請求項１０】以下のステップを備えることを特徴とするベクトル列の出力方法。

（ａ）第１の記憶部に記憶された１次元以上のベクトルxに第１の有理ベクトル写像fを適用した結果のベクトルx'=f(x)を計算する第１の計算ステップと、

（ｂ）前記第１の記憶部に記憶されたベクトルxと、第２の記憶部に記憶された１次元以上のベクトルyとに第２の有理ベクトル写像gを適用した結果のベクトルy'=g(x,y)を計算する第２の計算ステップと、

（ｃ）前記第１の計算ステップにおいて計算された結果のベクトルx'と、前記第２の計算ステップにおいて計算された結果のベクトルy'とを結合したベクトルz'を出力する出力ステップと、

（ｄ）前記第１の計算ステップにおいて計算された結果のベクトルx'を前記第１の記憶部に記憶させて更新する第１の更新ステップと、

（ｅ）前記第２の計算ステップにおいて計算された結果のベクトルy'を前記第２の記憶部に記憶させて更新する第２の更新ステップ。

【請求項１１】前記第１の有理ベクトル写像fを１次元以上のベクトルxに０回以上適用して得られるベクトル列
x, f(x), f(f(x)), f(f(f(x))), …
の極限分布の密度関数は解析的な関数であり、
前記第２の有理ベクトル写像gにパラメータとして１次元以上のベクトルλを与えた写像g(λ,・)を１次元以上のベクトルyに０回以上適用して得られるベクトル列
y, g(λ,y), g(λ,g(λ,y)), g(λ,g(λ,g(λ,y))), …
の極限分布の密度関数は当該パラメータλを有する解析的な関数であることを特徴とする請求項１０に記載の出力方法。

【請求項１２】前記第１の有理ベクトル写像fは、楕円

関数の加法定理より導かれる有理写像、特に、ウラム＝フォン・ノイマン写像、キュービック写像、クインティック写像、又はカツラ＝フクダ写像、一般化ウラム＝フォン・ノイマン写像、一般化キュービック写像もしくは一般化チェビシェフ写像に所定のパラメータを与えたもののいずれかであることを特徴とする請求項１１に記載の出力方法。

【請求項１３】前記第２の有理ベクトル写像gは、カツラ＝フクダ写像、一般化ウラム＝フォン・ノイマン写像、一般化キュービック写像、一般化チェビシェフ写像のいずれかであることを特徴とする請求項１１に記載の出力方法。

【請求項１４】以下のステップを備えることを特徴とするプログラムを記録した情報記録媒体。

（ａ）第１の記憶部に記憶された１次元以上のベクトルxに第１の有理ベクトル写像fを適用した結果のベクトルx'=f(x)を計算する第１の計算ステップと、

（ｂ）前記第１の記憶部に記憶されたベクトルxと、第２の記憶部に記憶された１次元以上のベクトルyとに第２の有理ベクトル写像gを適用した結果のベクトルy'=g(x,y)を計算する第２の計算ステップと、

（ｃ）前記第１の計算ステップにおいて計算された結果のベクトルx'と、前記第２の計算ステップにおいて計算された結果のベクトルy'とを結合したベクトルz'を出力する出力ステップと、

（ｄ）前記第１の計算ステップにおいて計算された結果のベクトルx'を前記第１の記憶部に記憶させて更新する第１の更新ステップと、

（ｅ）前記第２の計算ステップにおいて計算された結果のベクトルy'を前記第２の記憶部に記憶させて更新する第２の更新ステップ。

【請求項１５】前記第１の有理ベクトル写像fを１次元以上のベクトルxに０回以上適用して得られるベクトル列

x, f(x), f(f(x)), f(f(f(x))), …

の極限分布の密度関数は解析的な関数であり、

前記第２の有理ベクトル写像gにパラメータとして１次元以上のベクトルλを与えた写像g(λ,・)を１次元以上のベクトルyに０回以上適用して得られるベクトル列

y, g(λ,y), g(λ,g(λ,y)), g(λ,g(λ,g(λ,y))), …

の極限分布の密度関数は当該パラメータλを有する解析的な関数であることを特徴とする請求項１４に記載の情報記録媒体。

【請求項１６】前記第１の有理ベクトル写像fは、楕円関数の加法定理より導かれる有理写像、特に、ウラム＝フォン・ノイマン写像、キュービック写像、クインティック写像、又は、カツラ＝フクダ写像、一般化ウラム＝フォン・ノイマン写像、一般化キュービック写像もしくは一般化チェビシェフ写像に所定のパラメータを与えたもののいずれかであることを特徴とする請求項１５に記載の情報記録媒体。

【請求項１７】前記第２の有理ベクトル写像gは、楕円関数の加法定理より導かれる有理写像、特に、カツラ＝フクダ写像、一般化ウラム＝フォン・ノイマン写像、一般化キュービック写像、一般化チェビシェフ写像のいずれかであることを特徴とする請求項１５に記載の情報記録媒体。

【請求項１８】前記情報記録媒体は、コンパクトディスク、フロッピーディスク、ハードディスク、光磁気ディスク、ディジタルビデオディスク、磁気テープ、または、半導体メモリであることを特徴とする請求項１４から１７に記載の情報記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ベクトル列の出力装置、出力方法、および、情報記録媒体に関する。

【０００２】特に、出力されるランダムなベクトル列の分布の密度関数が既知の解析的な関数であるようなベクトル列の生成手法が２つあるときに、これらを結び付けて、より高次元のランダムなベクトル列であって、その分布の密度関数が解析的な関数として得られるものを出力するベクトル列の出力装置、出力方法、および、これらを実現するプログラムを記録した情報記録媒体に関する。

【０００３】

【従来の技術】従来から、漸化式を用いた乱数の生成手法が多数知られている。物理学や工学などの模擬実験を行うモンテカルロ法では、このようにして生成された乱数を用いる。

【０００４】また、移動体電話で用いられるＣＤＭＡ（Code Division Multiple Access）法では、限られた電波帯域を多数のユーザが有効に利用できるようにするため、乱数から得られるＰＮ（Pseudo Noise）コードを各ユーザに割り当てている。

【０００５】このほか、インターネットなどの通信技術の発達により、通信の秘密保持の必要性がますます大きくなってきており、公開鍵暗号という手法を用いて秘密保持を行うことが一般的になりつつある。この手法においても、公開鍵を生成するために乱数が用いられている。

【０００６】このような乱数を得るために、従来から、漸化式を用いた手法が広く利用されている。古くから知られる乗算による漸化式では乱数の周期が問題となっていた。しかし、近年、カオス理論の発展により、楕円関数（三角関数を含む）の加法定理から導かれる有理写像を漸化式に用いて得られる乱数には、以下のような有利な性質があることが判明しており、その重要性はますます高まってきている。

【０００７】（１）出力される乱数列には周期がないため、繰り返し同じ列が出力されることがない。

7

（２）乱数の種（漸化式に与える初期値）として有理数を与えると、得られる乱数列に含まれる数がいずれも有理数になる。

（３）乱数の分布を表す密度関数が既知の解析的関数である。

【０００８】このような有理写像としては、ウラム＝フォン・ノイマン写像［数１］、キュービック写像［数２］、クインティック写像［数３］などが知られている。

【０００９】

【数１】

$$f(x) = 4x(1-x)$$

【００１０】

【数２】

$$f(x) = x(3-4x)^2$$

【００１１】

【数３】

$$f(x) = x(5-20x+16x^2)^2$$

【００１６】たとえば、一般化ウラム＝フォン・ノイマン写像［数５］を用いて上記の漸化式により乱数列を得た場合、その分布も同じパラメータを有する密度関数

$$f(l,m,x) - \frac{4(1-x)(1-lx)(1-mx)}{1 \quad Ax^2 \mid Bx^2 \mid Cx^4}$$

ただし

$$A - 2(l \mid m \mid lm)$$

$$B \cdot \ 8lm$$

$$C - l^2 + m^2 - 2lm - 2l^2m - 2lm^2 + l^2m^2$$

［数６］で表現される。

【００１７】

【数６】

$$\frac{1}{K(l,m)\sqrt{x(1-x)(1-lx)(1-mx)}}$$

ただし

$$K(l,m) - \int_0^1 \frac{du}{\sqrt{(1-u^2)(1-lu^2)(1-mu^2)}}$$

【００１８】なお、カツラ＝フクダ写像は、一般化ウラム＝フォン・ノイマン写像［数５］において、m=0とおいたものである。

【００１９】これらの有理写像を用いた乱数を生成する手法については、本願の発明者らによる出願に係る特開平１０－２８３３４４号公報に開示されている。また、その理論的背景については以下の文献に開示されている。

S. M. Ulam and J. von Neumann, Bull. Math. Soc. 53 (1947) pp.1120.

8

【００１２】これらの有理写像のいずれを選んだ場合であっても、適当な初期値ξ　(0＜ξ＜1)を与え、以下の漸化式により乱数列x[i]を得た場合、この乱数列x[i]の分布を表す密度関数は、［数４］で表現される。

x[0] = ξ

x[i+1] = f(x[i])　(i≧0)

【００１３】

【数４】

$$\rho(x) = \frac{1}{\pi\sqrt{x(1-x)}}$$

【００１４】また、パラメータを有する有理写像も漸化式として用いることができ、このような有理写像としてカツラ＝フクダ写像、一般化ウラム＝フォン・ノイマン写像［数５］、一般化キュービック写像、一般化チェビシェフ写像などがある。

【００１５】

【数５】

R. L. Adler and T. J. Rivlin, Proc. Am. Math. Soc. 15 (1964) pp.794.

K. Umeno, Method of constructing exactly solvable chaos, Phys. Rev. E(1997) Vol.55 pp.5280-5284.

【００２０】従来、このような乱数生成手法では、乱数の種としてスカラー値（１次元のベクトル）を与えることにより、乱数列（ランダムな１次元のベクトル列）を得ることができた。

【００２１】

【発明が解決しようとする課題】しかしながら、従来の

乱数発生の手法においては、以下のような問題があった。

【００２２】すなわち、２次元以上の空間におけるモンテカルロ法では、２次元以上のベクトルのランダムな列が必要である。しかし、従来の乱数発生の手法においては、得られる乱数列はスカラー値の列（１次元のベクトル列）であり、たとえば、３次元空間の模擬実験を行う際に、この列の先頭から順に３個ずつ値を必要な数だけ選択するのでは、乱数分布に偏りが発生し、収束性が悪化してしまうという問題が生じていた。

【００２３】また、公開鍵暗号を生成する場合には、２つの整数の対からなる乱数を得る必要があるが、従来の乱数発生の手法においては、この対を同時に生成することができないため、悪意のある暗号解読者に対する防御が十分でなくなってしまうという問題が生じていた。

【００２４】このように、複数個の乱数の組が同時に１つのベクトルとして生成され、これを列として、ランダムなベクトル列を出力でき、なおかつ、これらのベクトル列の分布の密度関数が解析的に得られるような出力装置や出力方法に対する要望は、極めて大きい。

【００２５】本発明は、以上のような問題を解決するためになされたもので、出力されるランダムなベクトル列の分布の密度関数が既知の解析的な関数であるようなベクトル列の生成手法が２つあるときに、これらを結び付けて、より高次元のランダムなベクトル列であって、その分布の密度関数が解析的な関数として得られるものを出力するベクトル列の出力装置、出力方法、および、これらを実現するプログラムを記録した情報記録媒体を提供することを目的とする。

【００２６】

【課題を解決するための手段】以上の目的を達成するため、本発明の原理にしたがって、下記の発明を開示する。

【００２７】図１に示すように、本発明のベクトル列の出力装置１００は、第１の記憶部１０１と、第１の計算部１０２と、第２の記憶部１０３と、第２の計算部１０４と、出力部１０５と、第１の更新部１０６と、第２の更新部１０７とを備え、（ａ）第１の記憶部１０１は、１次元以上のベクトルxを記憶し、（ｂ）第１の計算部１０２は、第１の記憶部１０１に記憶されたベクトルxに第１の有理ベクトル写像fを適用した結果のベクトルx'=f(x)を計算し、

【００２８】（ｃ）第２の記憶部１０３は、１次元以上のベクトルyを記憶し、（ｄ）第２の計算部１０４は、第１の記憶部１０１に記憶されたベクトルxと、第２の記憶部１０３に記憶された１次元以上のベクトルyとに、第２の有理ベクトル写像gを適用した結果のベクトルy'=g(x,y)を計算し、

【００２９】（ｅ）出力部１０５は、第１の計算部１０２により計算された結果のベクトルx'と第２の計算部１０４により計算された結果のベクトルy'とを結合したベクトルz'を出力し、（ｆ）第１の更新部１０６は、第１の計算部１０２により計算された結果のベクトルx'を第１の記憶部１０１に記憶させて更新し、（ｇ）第２の更新部１０７は、第２の計算部１０４により計算された結果のベクトルy'を第２の記憶部１０３に記憶させて更新する。

【００３０】ここで、有理ベクトル写像fおよびgとしては、後述するカオス理論に基づく写像のほか、乱数を生成する漸化式に用いられる任意の写像を用いることができる。たとえば、巨大な素数を乗算して剰余を求める写像などを利用することが可能である。

【００３１】また、本発明のベクトル列の出力装置において、第１の有理ベクトル写像fを１次元以上のベクトルxに０回以上適用して得られるベクトル列

x, f(x), f(f(x)), f(f(f(x))), …

の極限分布の密度関数は解析的な関数であり、

【００３２】第２の有理ベクトル写像gにパラメータとして１次元以上のベクトルλを与えた写像g(λ,・)を１次元以上のベクトルyに０回以上適用して得られるベクトル列

y, g(λ,y), g(λ,g(λ,y)), g(λ,g(λ,g(λ,y))), …

の極限分布の密度関数は当該パラメータλを有する解析的な関数であるように構成することができる。

【００３３】また、本発明のベクトル列の出力装置の第１の有理ベクトル写像fは、楕円関数の加法定理より導かれる有理写像、特に、ウラム＝フォン・ノイマン写像、キュービック写像、クインティック写像、又は、カツラ＝フクダ写像、一般化ウラム＝フォン・ノイマン写像、一般化キュービック写像、もしくは一般化チェビシェフ写像に所定のパラメータを与えたもののいずれかとすることができる。

【００３４】また、本発明の第２の有理ベクトル写像gは、楕円関数の加法定理より導かれる有理写像、特に、カツラ＝フクダ写像、一般化ウラム＝フォン・ノイマン写像、一般化キュービック写像、一般化チェビシェフ写像のいずれかとすることができる。

【００３５】第１の有理ベクトル写像fと、第２の有理ベクトル写像gとして上記のような楕円関数の加法定理より導かれる有理写像を選択すると、出力部１０５が順次出力するベクトルの列の分布の密度関数をこれらの写像から得られる乱数列の密度関数から得ることができる。

【００３６】図２に示すように、本発明のベクトル列の出力装置２００は、生成部２０１と、第１の出力部２０２と、第２の出力部２０３と、第３の出力部２０４とを備え、（ａ）生成部２０１は、２次元以上のベクトルζを受け付けて、これから１次元以上のベクトルξと１次元以上のベクトルηとを生成し、

【００３７】（ｂ）第１の出力部２０２は、生成部２０

１により生成されたベクトルξを受け付けて、第１の有理ベクトル写像fを用いた漸化式
x[0] = ζ
x[i+1] = f(x[i])　（ただしi≧0）
により得られるベクトル列x[i]を出力し、

【００３８】（ｃ）第２の出力部２０３は、生成部２０１により生成されたベクトルηと、第１の出力部２０２により出力されるベクトル列x[i]とを受け付けて、第２の有理ベクトル写像gを用いた漸化式
y[0] = η
y[i+1] = g(x[i],y[i])　（ただしi≧0）
により得られるベクトル列y[i]を出力し、

【００３９】（ｄ）第３の出力部２０４は、第１の出力部２０２により出力されるベクトル列x[i]と、第２の出力部２０３により出力されるベクトル列y[i]とを結合して得られるベクトル列z[i]を結果として出力する。

【００４０】また、本発明のベクトル列の出力装置において、第１の有理ベクトル写像fを１次元以上のベクトルxに０回以上適用して得られるベクトル列
x, f(x), f(f(x)), f(f(f(x))), …
の極限分布の密度関数は解析的な関数であり、

【００４１】第２の有理ベクトル写像gにパラメータとして１次元以上のベクトルλを与えた写像g(λ,・)を１次元以上のベクトルyに０回以上適用して得られるベクトル列
y, g(λ,y), g(λ,g(λ,y)), g(λ,g(λ,g(λ,y))), …
の極限分布の密度関数は当該パラメータλを有する解析的な関数であるように構成することができる。

【００４２】また、本発明のベクトル列の出力装置の第１の有理ベクトル写像fは、楕円関数の加法定理より導かれる有理写像、特に、ウラム＝フォン・ノイマン写像、キュービック写像、クインティック写像、または、カツラ＝フクダ写像、一般化ウラム＝フォン・ノイマン写像、一般化キュービック写像もしくは一般化チェビシェフ写像に所定のパラメータを与えたもののいずれかとすることができる。

【００４３】また、本発明のベクトル列の出力装置の第２の有理ベクトル写像gは、楕円関数の加法定理より導かれる有理写像、特に、カツラ＝フクダ写像、一般化ウラム＝フォン・ノイマン写像、一般化キュービック写像、一般化チェビシェフ写像のいずれかとすることができる。

【００４４】この場合も、有理ベクトル写像fとgとから、出力されるベクトル列の分布の密度関数を解析的に得ることができる。

【００４５】また、本発明のベクトル列の出力装置の第１の出力部２０２もまた、本発明のベクトル列の出力装置とすることができる。すなわち、

（１）まず、ある有理ベクトル写像fとパラメータを有する有理ベクトル写像gとからベクトル列の出力装置Ｘを構成する。

【００４６】（２）次に、当該出力装置Ｘをある有理ベクトル写像f'に対応させ、これとパラメータを有する有理ベクトル写像g'とから、同じように新たなベクトル列の出力装置Ｙを構成する。出力装置Ｙが出力するベクトル列のベクトルの次元は、出力装置Ｘが出力するベクトル列のベクトルの次元よりも大きい。

【００４７】（３）これを繰り返すことにより、ランダムな任意の次元のベクトル列の出力装置を構成することができる。

【００４８】本発明のベクトル列の出力方法は、以下のステップを備える。

（ａ）第１の記憶部に記憶された１次元以上のベクトルxを取得する第１の取得ステップと、（ｂ）第１の取得ステップにおいて取得されたベクトルxに第１の有理ベクトル写像fを適用した結果のベクトルx'=f(x)を計算する第１の計算ステップと、

【００４９】（ｃ）第２の記憶部に記憶された１次元以上のベクトルyを取得する第２の取得ステップと、

（ｄ）第１の記憶部に記憶されたベクトルxと、第２の取得ステップにおいて取得されたベクトルyとに第２の有理ベクトル写像gを適用した結果のベクトルy'=g(x,y)を計算する第２の計算ステップと、

【００５０】（ｅ）第１の計算ステップにおいて計算された結果のベクトルx'と、第２の計算ステップにおいて計算された結果のベクトルy'とを結合したベクトルz'を出力する出力ステップと、

【００５１】（ｆ）第１の計算ステップにおいて計算された結果のベクトルx'を第１の記憶部に記憶させて更新する第１の更新ステップと、（ｇ）第２の計算ステップにおいて計算された結果のベクトルy'を第２の記憶部に記憶させて更新する第２の更新ステップ。

【００５２】また、本発明のベクトル列の出力方法において、第１の有理ベクトル写像fを１次元以上のベクトルxに０回以上適用して得られるベクトル列
x, f(x), f(f(x)), f(f(f(x))), …
の極限分布の密度関数は解析的な関数であり、

【００５３】第２の有理ベクトル写像gにパラメータとして１次元以上のベクトルλを与えた写像g(λ,・)を１次元以上のベクトルyに０回以上適用して得られるベクトル列
y, g(λ,y), g(λ,g(λ,y)), g(λ,g(λ,g(λ,y))), …
の極限分布の密度関数は当該パラメータλを有する解析的な関数であるように構成することができる。

【００５４】また、本発明のベクトル列の出力方法において、第１の有理ベクトル写像fは、楕円関数の加法定理より導かれる有理写像、特に、ウラム＝フォン・ノイマン写像、キュービック写像、クインティック写像、又はカツラ＝フクダ写像一般化ウラム＝フォン・ノイマン写像、一般化キュービック写像もしくは一般化チェビシ

ェフ写像に所定のパラメータを与えたもののいずれかとすることができる。

【００５５】また、本発明のベクトル列の出力方法において、第２の有理ベクトル写像gは、カツラ＝フクダ写像、一般化ウラム＝フォン・ノイマン写像、一般化キュービック写像、一般化チェビシェフ写像のいずれかとすることができる。

【００５６】この場合も、有理ベクトル写像fとgとから、出力されるベクトル列の分布の密度関数を解析的に得ることができる。

【００５７】本発明のベクトル列を出力する出力装置と、出力方法とを実現するプログラムをコンパクトディスク、フロッピーディスク、ハードディスク、光磁気ディスク、ディジタルビデオディスク、磁気テープ、半導体メモリなどの情報記録媒体に記録することができる。

【００５８】本発明の情報記録媒体に記録されたプログラムを、記憶装置、計算装置、出力装置などを備える情報処理装置、たとえば汎用コンピュータ、ゲーム装置、携帯情報端末、移動体電話で実行することにより、上記のベクトル列を出力する出力装置と、出力方法とを実現することができる。

【００５９】また、情報処理装置とは独立して、本発明のプログラムを記録した情報記録媒体を配布、販売することができる。

【００６０】

【発明の実施の形態】以下に本発明の一実施形態を説明する。なお、以下に説明する実施形態は説明のためのものであり、本願発明の範囲を制限するものではない。したがって、当業者であればこれらの各要素もしくは全要素をこれと均等なものに置換した実施形態を採用することが可能であるが、これらの実施形態も本願発明の範囲に含まれる。

【００６１】（第１実施例）図３は、本発明のベクトル列の出力装置を汎用コンピュータなどの情報処理装置において実現する実施例の、当該情報処理装置のブロック構成図である。

【００６２】情報処理装置３０１は、ＣＰＵ（Central Processing Unit；中央処理ユニット）３０２により制御され、ＲＡＭ（Random Access Memory；ランダム・アクセス・メモリ）などの主記憶装置３０３には一時的なデータなどを記憶し、ハードディスク、フロッピーディスク、ＣＤ－ＲＯＭ（Compact Disk Read Only Memory）、磁気テープ、光磁気ディスクなどの外部記憶装置３０４にはＣＰＵ　３０２が実行するプログラムが記憶される。

【００６３】情報処理装置３０１に電源が投入されると、ＣＰＵ　３０２は、まず、ＲＯＭ（Read Only Memory；読出専用メモリ）３０８に記憶されている初期プログラムローダと呼ばれるプログラムを実行し、しかる後に外部記憶装置３０４などからオペレーティングシステムのプログラムやアプリケーションのプログラムなどを主記憶装置３０３にロードして実行する。

【００６４】実行した結果は、外部記憶装置３０４にファイルとして記憶したり、ＣＲＴ（Cathode Ray Tube）や液晶ディスプレイなどの表示装置３０５に表示することができる。情報処理装置のユーザは、マウスやキーボードなどの入力装置３０６を用いて情報処理装置に対する指示を与える。

【００６５】ここで、情報処理装置３０１が図１に示すベクトル列の出力装置１００として機能する場合、主記憶装置３０３は、第１の記憶部１０１、第２の記憶部１０３として機能し、ＣＰＵ　３０２は、第１の計算部１０２、第２の計算部１０４、第１の更新部１０６、第２の更新部１０７として機能し、外部記憶装置３０４は、結果をファイルとして出力する場合は出力部１０５として機能し、表示装置３０５は、結果を表示して出力する場合は出力部１０５として機能し、主記憶装置３０３は、結果をほかのプログラムで利用する場合は出力部１０５として機能する。

【００６６】また、情報処理装置３０１が、図２に示すベクトル列の出力装置２００として機能する場合は、ＣＰＵ　３０２は、主記憶装置３０３や、必要に応じて外部記憶装置３０４、表示装置３０５と共働して、生成部２０１、第１の出力部２０２、第２の出力部２０３、第３の出力部２０４として機能する。

【００６７】また、主記憶装置３０３、外部記憶装置３０４は、本発明の情報記録媒体として機能する。また、ＲＯＭ　３０８を本発明の情報記録媒体として機能させることもできる。

【００６８】以下、図４を参照して、本発明のベクトル列の出力装置の処理を説明する。図４は、本発明の処理の流れを示すフローチャートである。

【００６９】なお、以下では説明の都合上、有理写像fとしてウラム＝フォン・ノイマン写像［数１］を、有理写像gとしてカツラ＝フクダ写像を、それぞれ採用するが、これ以外の写像を利用することも当業者には容易であり、これらの実施形態も本発明の範囲に含まれる。

【００７０】まず、ＣＰＵ　３０２は、現在の時刻などから乱数の種を取得する（ステップＳ４０１）。この場合、有理写像fはスカラー値（１次元のベクトル）に対して適用され、有理写像gは、スカラー値（１次元のベクトル）のパラメータとともにスカラー値（１次元のベクトル）に対して適用されるので、スカラー値の種が２つ必要である。見方を変えれば、２次元のベクトルを乱数の種として取得することになる。

【００７１】なお、乱数の種は、ユーザが入力装置３０６から入力することも可能であり、これと時刻などの数値を組み合わせてもよい。これらは、公開鍵を生成する場合に有用である。

【００７２】次に、ＣＰＵ　３０２は、取得した種をそ

15

れぞれ主記憶装置３０３内の第１の記憶部１０１と、第２の記憶部１０３とに記憶する（ステップＳ４０２）。これにより、乱数を生成するための初期値が設定される。

【００７３】なお、ステップＳ４０１からステップＳ４０２の処理は、図２に示すランダムなベクトル列を出力する装置２００の生成部２０１が実行する処理に相当する。

【００７４】ついで、ＣＰＵ　３０２は、第１の記憶部１０１に記憶された値xと、第２の記憶部１０３に記憶された値yとを取得し（ステップＳ４０３）、これらを用いて値y'=g(x,y)を計算し（ステップＳ４０４）、計算された値y'を第２の記憶部１０３に記憶させて更新する（ステップＳ４０５）。

【００７５】すなわち、ステップＳ４０４において、ＣＰＵ　３０２は、第２の計算部１０４として機能することになる。

【００７６】さらに、ＣＰＵ　３０２は、第１の記憶部１０１に記憶された値xを取得し（ステップＳ４０６）、これを用いて値x'=f(x)を計算し（ステップＳ４０７）、計算された値x'を第１の記憶部１０１に記憶させて更新する（ステップＳ４０８）。

【００７７】すなわち、ステップＳ４０７において、ＣＰＵ　３０２は、第１の計算部１０２として機能することになる。

【００７８】最後に、ＣＰＵ　３０２は、第１の記憶部１０１に記憶された更新後の値x'と、第２の記憶部１０３に記憶された更新後の値y'とを結合して、外部記憶装置３０４などに出力し（ステップＳ４０９）、ステップＳ４０３に戻る。

【００７９】なお、あるｎ次元のベクトルと別のｍ次元のベクトルとを結合した結果は（ｎ＋ｍ）次元のベクトルであり、その要素は、まずｎ次元のベクトルの要素を並べ、ついでｍ次元のベクトルの要素を並べたものである。図２に示すベクトル列の出力装置２００の生成部２０１の処理は、ベクトルの結合の逆演算を行うことにより実現することができる。

【００８０】この繰り返しを行うことにより、ランダムな２次元ベクトルの列が外部記憶装置３０４に出力されることになる。

【００８１】なお、図２に示すベクトル列の出力装置２００の第１の出力部２０２が実行する処理はステップＳ４０６～ステップＳ４０８に、第２の出力部２０３が実行する処理はステップＳ４０３～ステップＳ４０５に、第３の出力部２０４が実行する処理はステップＳ４０６により、それぞれ実現されている。

【００８２】なお、本実施例では、上述の通り、有理写像fとして一般化ウラム＝フォン・ノイマン写像［数１］を採用するが、これを漸化式に使用した場合に得られる乱数の分布の密度関数を図５に示す。図５に示す通り、これは0≦x≦1の範囲で定義される非一様な密度関数であり、x=0およびx=1で無限大となり、0＜x＜1の範囲で下に凸な関数である。

16

【００８３】また、本実施例では、上述の通り、有理写像gとしてカツラ＝フクダ関数［数７］を採用するが、パラメータx'を固定して漸化式に使用した場合に得られる乱数の分布もまた、［数８］のように解析的に得ることができる。

【００８４】

【数７】

$$g(x',y)-\frac{4y(1-y)(1-x'y)}{(1\quad x'y^2)^2}$$

【００８５】

【数８】

$$\nu(x,y)-\frac{1}{K(x)\sqrt{y(1-y)(1-xy)}}$$

ただし

$$K(x)-\int_0^1\frac{du}{\sqrt{(1-u^2)(1-xu^2)}}$$

【００８６】図６には、ステップＳ４０９において出力される２次元ベクトルを座標値として、順次プロットしたものを示し、図７には、ステップＳ４０９において出力される２次元ベクトルを座標値として、これをヒストグラムとしたものを示す。また、図８には、図７に示すヒストグラムをある断面で切った場合の様子を示す。

【００８７】発明者は、「一般に密度関数ρ(x)を有する有理写像fと、xというパラメータを持ち密度関数ν(x,y)を有する有理写像g(x,・)とを本発明の漸化式を用いる手法により結合した場合、出力されるベクトル列の分布の密度関数はν(x,y)ρ(x)となる」ことを数学的に証明している。したがって、分布の密度関数が既知の解析的な関数である場合には、これらを組み合わせた場合、分布の密度関数は、もとの分布の密度関数の積として、解析的に得ることができる。

【００８８】図８に示すグラフの形状が図５に示すグラフの形状とほぼ同じ形状をしていることからも、この結論が正しいことがわかる。また、従来の手法で問題となっていた乱数の偏りも少ないことがわかっている。

【００８９】なお、適宜各ステップの順序を変更したり、同じ処理を行うステップを別途実行することにより、上記実施例における制御の流れと同等の処理を実現することができるが、そのような実施形態も本発明の範囲に含まれる。

【００９０】（第２実施例）本発明の第２実施例は、汎用コンピュータなどの情報処理装置によりベクトル列の出力装置を構成するものではなく、電子回路により構成

するものである。

【００９１】すなわち、図１に示すベクトル列の出力装置１００の第１の記憶部１０１と第２の記憶部１０３とは、いずれも、フリップフロップなどを基本とする記憶回路で構成することができる。

【００９２】第１の計算部１０２と第２の計算部１０４とは、いずれも、加算回路と乗算回路の組み合わせで構成することができる。

【００９３】出力部１０５は、第２の計算部１０４を構成する回路の出力線により構成することができる。

【００９４】第１の更新部１０６と第２の更新部１０７とは、第１の計算部１０２と第２の計算部１０４とを構成する回路の出力線を、一定のクロック遅延をもってそれぞれ第１の記憶部１０１と第２の記憶部１０３とに帰還させて記憶させることにより構成することができる。

【００９５】このように、専用の電子回路により本発明のベクトル列の出力装置を構成することにより、たとえば携帯情報端末や移動体電話など、少ない電力消費と簡単で省スペースな構成が必要とされる機器に本発明を適用することができる。

【００９６】（第３実施例）上記実施例では、有理写像として楕円関数の加法定理より導かれる有理写像を用いているが、楕円積分、超楕円積分、あるいは、これらを変形したものから導かれる写像にも、類似した性質を有するものがあり、そのような写像を利用してもよい。また、従来から用いられている乱数の発生手法の漸化式を表す写像を利用することもできる。

【００９７】（第４実施例）本発明で得られるランダムなベクトル列の密度関数は解析的に得られるので、フォン・ノイマンの逆関数法により、本発明で得られた任意次元のランダムなベクトル列から、一様分布を持つランダムなベクトル列を発生させることができる。

【００９８】（第５実施例）本発明は、ＵＮＩＸなどのオペレーティング・システムやｐｒｏｌｏｇ、ＧＨＣなどの論理型言語やＬｉｓｐ、Ｈａｓｋｅｌｌなどの関数型言語などで多用されるストリーム処理により実現することができる。すなわち、上述のような有理ベクトル写像fとgについて、以下のベクトル列x[i]のデータストリームを生成するプロセス（プログラミング言語上は、述語、関数、手続などで表現される）Ａと、

x[0], x[1], x[2], x[3], …

x[0] = ζ

x[i+1] = f(x[i])　（ただしi≧0）

このプロセスＡが出力するデータストリームx[i]を順に受け付けて、以下のベクトル列y[i]のデータストリームを生成するプロセスＢとを用意することにより、

y[0], y[1], y[2], y[3], …

y[0] = η

y[i+1] = g(x[i],y[i])　（ただしi≧0）

本発明を実現することができる。

【００９９】プロセスＡとプロセスＢとの通信は、いわゆる製造者＝消費者モデルにより記述でき、要求駆動による生成、データストリームのバッファリングなどの公知の技法を利用することができる。

【０１００】

【発明の効果】以上説明したように、本発明によれば、以下の効果を奏する。

【０１０１】出力されるランダムなベクトル列の分布の密度関数が既知の解析的な関数であるようなベクトル列の生成手法が２つあるときに、これらを結び付けて、より高次元のランダムなベクトル列であって、その分布の密度関数が解析的な関数として得られるものを出力するベクトル列の出力装置、出力方法を提供することができる。

【０１０２】本発明では、既知のベクトル列の生成手法の分布の密度関数の積がより高次元のランダムなベクトル列の分布の密度関数となるため、容易に分布の特徴を得ることができ、さまざまな応用に資することができる。特に、生成手法として有理写像を採用した場合には、得られるベクトル列の各要素もすべて有理数となるという特徴を有し、計算機上の計算精度を厳密に保存しうるという利点を有する。

【０１０３】このようなランダムなベクトル列は、モンテカルロ法、移動体通信や光通信におけるＣＤＭＡ、インターネットなどの通信における公開鍵暗号などで利用することができる。

【０１０４】さらに、プログラムを記録した情報記録媒体をソフトウェア商品として、情報処理装置のハードウェアと独立して容易に配布したり販売したりすることができるようになる。本発明の情報記録媒体に記録されたプログラムを汎用コンピュータなどの情報処理装置で実行すれば、上記の発明に係るベクトル列の出力装置、出力方法が実現できる。

【図面の簡単な説明】

【図１】本発明のベクトル列の出力装置の構成を示すブロック構成図である。

【図２】本発明のベクトル列の出力装置の構成を示すブロック構成図である。

【図３】本発明のランダムなベクトル列の出力装置を汎用コンピュータなどの情報処理装置において実現する実施例の、当該情報処理装置のブロック構成図である。

【図４】本発明の処理の流れを示すフローチャートである。

【図５】一般化ウラム＝フォン・ノイマン写像を漸化式に使用した場合に得られる乱数の分布の密度関数を示すグラフである。

【図６】図４に示すフローチャートのステップＳ４０９において出力される２次元ベクトルを座標値として、順次プロットした説明図である。

【図７】図４に示すフローチャートのステップＳ４０９

19

において出力される２次元ベクトルを座標値としたヒストグラムである。

【図８】図７に示すヒストグラムをある断面で切断した場合のグラフである。

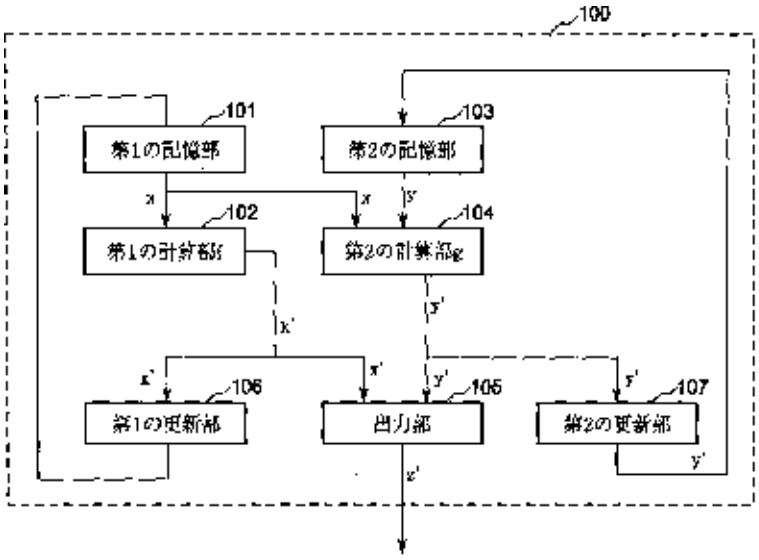
【符号の説明】

１００　ベクトル列の出力装置
１０１　第１の記憶部
１０２　第１の計算部
１０３　第２の記憶部
１０４　第２の計算部
１０５　出力部
１０６　第１の更新部
１０７　第２の更新部

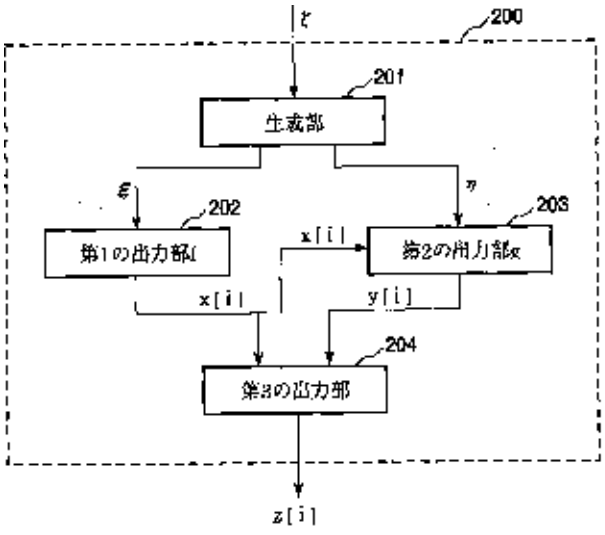
20

２００　ベクトル列の出力装置
２０１　生成部
２０２　第１の出力部
２０３　第２の出力部
２０４　第３の出力部
３０１　情報処理装置
３０２　ＣＰＵ
３０３　主記憶装置
３０４　外部記憶装置
３０５　表示装置
３０６　入力装置
３０８　ＲＯＭ

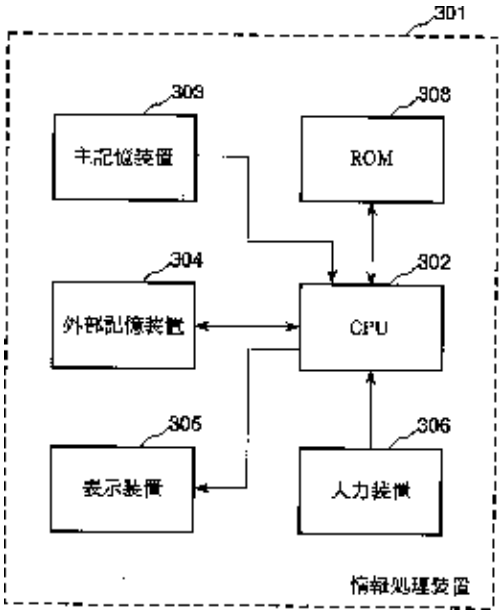
【図１】



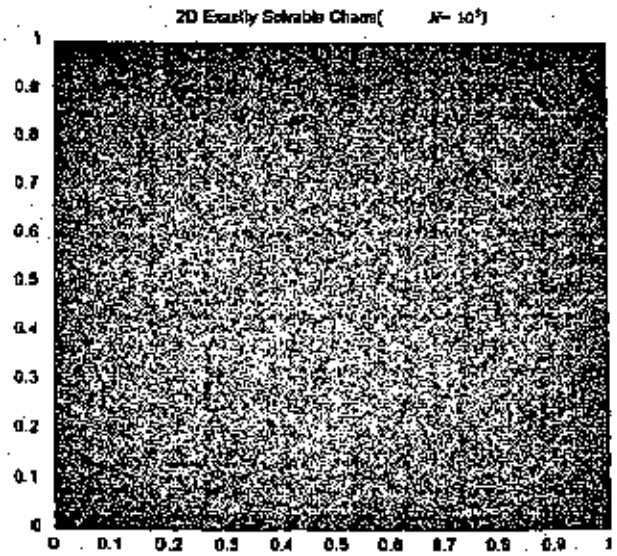
【図２】



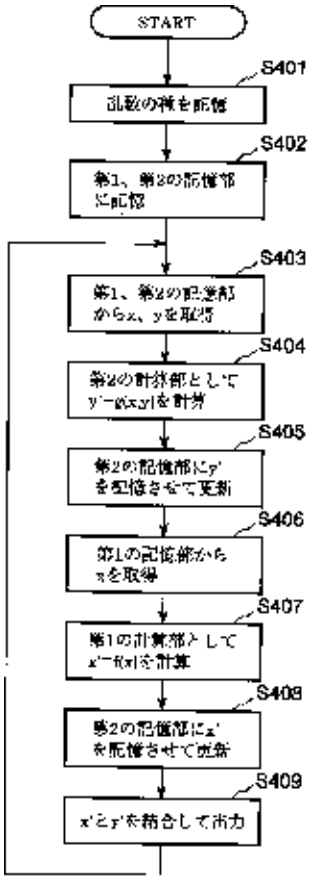
【図３】



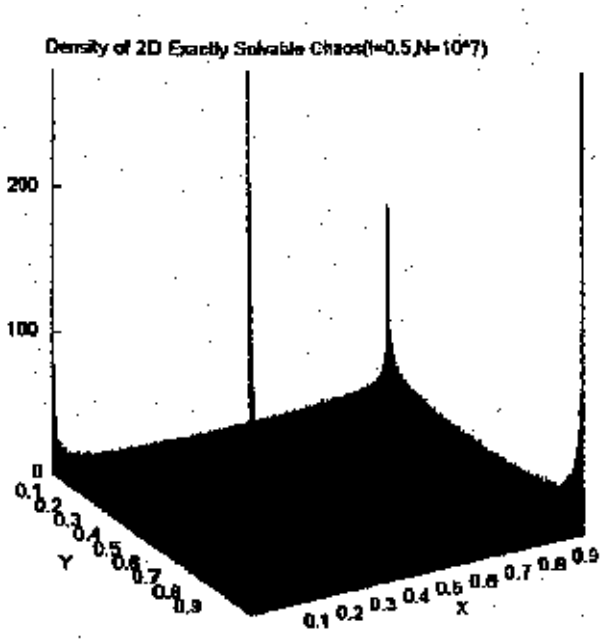
【図６】



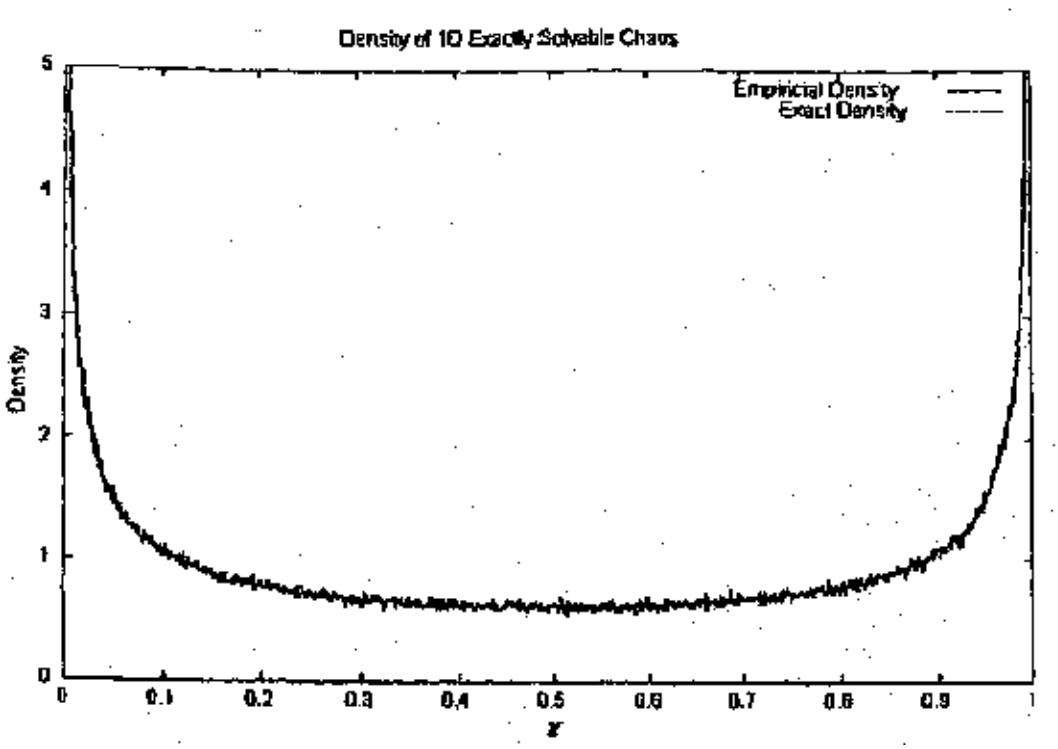
【図４】


START
S401
乱数の種を記憶
S402
第1、第2の記憶部に記憶
S403
第1、第2の記憶部からx、yを取得
S404
第2の計算部としてy'=φ(x,y)を計算
S405
第2の記憶部にy'を記憶させて更新
S406
第1の記憶部からxを取得
S407
第1の計算部Aとしてx'=f(x)を計算
S408
第2の記憶部にx'を記憶させて出力
S409
x'とy'を結合して出力

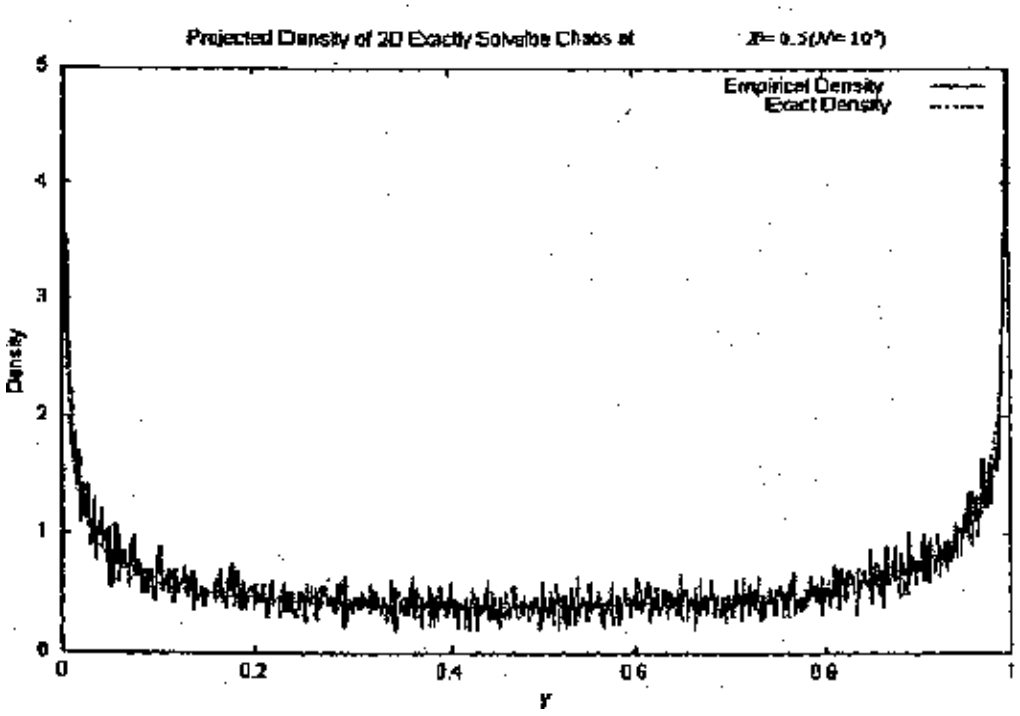
【図７】


Density of 2D Exactly Solvable Chaos(l=0.5,N=10^7)
200
100
0
Y
X

【図５】


Density of 1D Exactly Solvable Chaos
Empirical Density
Exact Density
Density
x

【図８】



フロントページの続き

(58)調査した分野(Int.Cl.[7]，ＤＢ名)

G09C　1/00　650

G06F　7/58