

(19) 日本国特許庁 (J P)

(12) 特 許 公 報 (B 1)

(11) 特許番号

特許第3030341号
(P3030341)

(45) 発行日 平成12年4月10日(2000.4.10)

(24) 登録日 平成12年2月10日(2000.2.10)

(51) Int.Cl. ⁷	識別記号	F I
G 0 6 F 7/58		G 0 6 F 7/58 B
G 0 9 C 1/00	6 5 0	G 0 9 C 1/00 6 5 0 B
H 0 4 L 9/22		H 0 4 L 9/00 6 5 5

請求項の数18(全 13 頁)

(21) 出願番号 特願平11-85744

(22) 出願日 平成11年3月29日(1999.3.29)

審査請求日 平成11年3月29日(1999.3.29)

(73) 特許権者 391027413

郵政省通信総合研究所長

東京都小金井市貫井北町4丁目2番1号

(73) 特許権者 598156561

梅野 健

東京都小金井市貫井北町4-2-1 郵

政省通信総合研究所内

(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 100101764

弁理士 川和 高穂

審査官 石田 信行

最終頁に続く

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

1

(57) 【特許請求の範囲】

【請求項1】以下の手段を備えることを特徴とするランダムな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の記憶手段と、

(b) 前記第1の記憶手段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の計算手段と、

(d) 1次元以上のベクトル y を記憶する第2の記憶手段と、

(e) 前記第1の計算手段により計算された結果のベクトル x' と、前記第2の記憶手段に記憶された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の計算手段と、

2

(f) 前記第1の計算手段により計算された結果のベクトル x' と前記第2の計算手段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' を出力する出力手段と、

(g) 前記第1の計算手段により計算された結果のベクトル x' を前記第1の記憶手段に記憶させて更新する第1の更新手段と、

(h) 前記第2の計算手段により計算された結果のベクトル y' を前記第2の記憶手段に記憶させて更新する第2の更新手段。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 $x, f(x), f(f(x)), f(f(f(x))), \dots$

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 y を与えた写像 $g(\cdot, y)$ を 1 次元以上のベクトル列 $y, g(\cdot, y), g(\cdot, g(\cdot, y)), g(\cdot, g(\cdot, g(\cdot, y))), \dots$ の極限分布の密度関数は当該パラメータ y 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 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、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 2 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 記載の出力装置。

【請求項 5】以下の手段を備えることを特徴とするランダムなベクトル列の出力装置。

(a) 2 次元以上のベクトル x を受け付けて、これから 1 次元以上のベクトル x' と 1 次元以上のベクトル y とを生成する生成手段と、

(b) 前記生成手段により生成されたベクトル x' 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 $x[0] =$

$$x[i+1] = f(x[i]) \quad (\text{ただし } i \geq 0)$$

により得られるベクトル列 $x[i]$ を出力する第 1 の出力手段と、

(c) 前記生成手段により生成されたベクトル x' と、前記第 1 の出力手段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 $y[0] =$

$$y[i+1] = g(x[i+1], y[i]) \quad (\text{ただし } i \geq 0)$$

により得られるベクトル列 $y[i]$ を出力する第 2 の出力手段と、

(d) 前記第 1 の出力手段により出力されるベクトル列 $x[i]$ と、前記第 2 の出力手段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 の出力手段。

【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 $x, f(x), f(f(x)), f(f(f(x))), \dots$

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 y を与えた写像 $g(\cdot, y)$ を 1 次元以上のベクトル列 $y, g(\cdot, y), g(\cdot, g(\cdot, y)), g(\cdot, g(\cdot, g(\cdot, y))), \dots$

の極限分布の密度関数は当該パラメータ y 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 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 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 記載の出力装置。

【請求項 9】前記第 1 の出力手段もまた請求項 5 記載の出力装置であることを特徴とする請求項 5 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ランダムなベクトル列の出力方法。

(a) 第 1 の記憶手段に記憶された 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) 前記第 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、

(c) 第 2 の記憶手段に記憶された 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) 前記第 1 の計算ステップにおいて計算されたベクトル x' と、前記第 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、

(e) 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、

(f) 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 の記憶手段に記憶させて更新する第 1 の更新ステップと、

(g) 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 の記憶手段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

$$x, f(x), f(f(x)), f(f(f(x))), \dots$$

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 $g(\cdot, \cdot)$ を 1 次元以上のベクトル列 $y, g(\cdot, y), g(\cdot, g(\cdot, y)), g(\cdot, g(\cdot, g(\cdot, y))), \dots$ の極限分布の密度関数は当該パラメータ g 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 0 記載の出力方法。

【請求項 1 2】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エ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 1 1 記載の出力方法。

【請求項 1 3】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、一般化チェビシエフ写像のいずれかであることを特徴とする請求項 1 1 記載の出力方法。

【請求項 1 4】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 の記憶手段に記憶された 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) 前記第 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、

(c) 第 2 の記憶手段に記憶された 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) 前記第 1 の計算ステップにおいて計算されたベクトル x' と、前記第 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、

(e) 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、

(f) 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 の記憶手段に記憶させて更新する第 1 の更新ステップと、

(g) 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 の記憶手段に記憶させて更新する第 2 の更新ステップ。

【請求項 1 5】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列 $x, f(x), f(f(x)), f(f(f(x))), \dots$

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 $g(\cdot, \cdot)$ を 1 次元以上

のベクトル列 $y, g(\cdot, y), g(\cdot, g(\cdot, y)), g(\cdot, g(\cdot, g(\cdot, y))), \dots$ の極限分布の密度関数は当該パラメータ g 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 4 記載の情報記録媒体。

【請求項 1 6】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エ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 1 5 記載の情報記録媒体。

【請求項 1 7】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、一般化チェビシエフ写像のいずれかであることを特徴とする請求項 1 5 記載の情報記録媒体。

【請求項 1 8】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 1 4 から 1 7 記載の情報記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】本発明は、ランダムな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。

【0 0 0 2】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ランダムな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。

【0 0 0 3】

【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。

【0 0 0 4】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。

【0 0 0 5】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。

【 0 0 0 6 】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。

【 0 0 0 7 】（ 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。

（ 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。

【 0 0 0 8 】このような有理写像には、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。

【 0 0 0 9 】

【 数 1 】

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

【 0 0 1 0 】

【 数 2 】

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

【 0 0 1 1 】

【 数 3 】

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

【 0 0 1 2 】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 (0 < x < 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。

$$x[0] =$$

$$x[i+1] = f(x[i]) \quad (i \geq 0)$$

【 0 0 1 3 】

【 数 4 】

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

【 0 0 1 4 】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。

【 0 0 1 5 】

【 数 5 】

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

ただし

$$A = 2(l + m + lm)$$

$$B = 8lm$$

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

【 0 0 1 6 】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 [数 6] で表現される。

【 0 0 1 7 】

【 数 6 】

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

ただし

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

【 0 0 1 8 】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。

【 0 0 1 9 】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 1 0 - 2 8 3 3 4 4 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) 1120.

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

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

【 0 0 2 0 】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。

【 0 0 2 1 】

【発明が解決しようとする課題】しかしながら、従来の乱数発生的手法においては、以下のような問題があった。

50 【 0 0 2 2 】すなわち、2次元以上の空間におけるモン

テカル口法では、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、従来の乱数発生的手法においては、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、従来の乱数発生的手法においては、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、これらを選び付けて、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ランダムな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、本発明のランダムなベクトル列の出力装置100は、第1の記憶手段101と、第1の計算手段102と、第2の記憶手段103と、第2の計算手段104と、出力手段105と、第1の更新手段106と、第2の更新手段107とを備え、(a)第1の記憶手段101は、1次元以上のベクトル x を記憶し、(b)第1の計算手段102は、第1の記憶手段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の記憶手段103は、1次元以上のベクトル y を記憶し、(d)第2の計算手段104は、第1の計算手段102により計算された結果のベクトル x' と、第2の記憶手段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)出力手段105は、第1の計算手段102により計算された結果のベクトル x' と第2の計算手段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の更新手段106

は、第1の計算手段102により計算された結果のベクトル x' を第1の記憶手段101に記憶させて更新し、(g)第2の更新手段107は、第2の計算手段104により計算された結果のベクトル y' を第2の記憶手段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、本発明のランダムな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 $x, f(x), f(f(x)), f(f(f(x))), \dots$

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を与えた写像 $g(\cdot, \cdot)$ 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

$y, g(\cdot, y), g(\cdot, g(\cdot, y)), g(\cdot, g(\cdot, g(\cdot, y))), \dots$ の極限分布の密度関数は当該パラメータ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、本発明のランダムな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。

【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、出力手段105が順次出力するベクトル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、本発明のランダムなベクトル列の出力装置200は、生成手段201と、第1の出力手段202と、第2の出力手段203と、第3の出力手段204とを備え、(a)生成手段201は、2次元以上のベクトルを受け付けて、これから1次元以上のベクトルと1次元以上のベクトルとを生成し、

【0037】(b)第1の出力手段202は、生成手段201により生成されたベクトルを受け付けて、第1の有理ベクトル写像 f を用いた漸化式

$x[0] =$

$x[i+1] = f(x[i])$ (ただし $i \geq 0$)

により得られるベクトル列 $x[i]$ を出力し、

【0038】(c)第2の出力手段203は、生成手段201により生成されたベクトル と、第1の出力手段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

$y[0] =$

$y[i+1] = g(x[i+1], y[i])$ (ただし $i \geq 0$)

により得られるベクトル列 $y[i]$ を出力し、

【0039】(d)第3の出力手段204は、第1の出力手段202により出力されるベクトル列 $x[i]$ と、第2の出力手段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、本発明のランダムな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 $x, f(x), f(f(x)), f(f(f(x))), \dots$

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 を与えた写像 $g(\cdot, \cdot)$ 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

$y, g(\cdot, y), g(\cdot, g(\cdot, y)), g(\cdot, g(\cdot, g(\cdot, y))), \dots$

の極限分布の密度関数は当該パラメータ 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、本発明のランダムな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エフ写像に所定のパラメータを与えたものいずれかとすることができる。

【0043】また、本発明のランダムな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、一般化チェビシエフ写像のいずれかとする 40

【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、本発明のランダムなベクトル列の出力装置の第1の出力手段もまた、本発明のランダムな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 とからランダムな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、同じように新たなランダムなベクトル列の出力装置 Y を構成する。 Y が出力するベクトル列のベクトルの次元は、 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。

10 【0048】本発明のランダムな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の記憶手段に記憶された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の記憶手段に記憶された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の計算ステップにおいて計算されたベクトル 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の記憶手段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の記憶手段に記憶させて更新する第2の更新ステップ。

【0052】また、本発明のランダムな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 $x, f(x), f(f(x)), f(f(f(x))), \dots$

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 を与えた写像 $g(\cdot, \cdot)$ 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

$y, g(\cdot, y), g(\cdot, g(\cdot, y)), g(\cdot, g(\cdot, g(\cdot, y))), \dots$

の極限分布の密度関数は当該パラメータ 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、本発明のランダムな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、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エフ写像に所定のパラメータを与えたもの 50

のいずれかとすることができる。

【 0 0 5 5 】また、本発明のランダムな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。

【 0 0 5 6 】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。

【 0 0 5 7 】本発明のランダムな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。

【 0 0 5 8 】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、上記のランダムな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。

【 0 0 5 9 】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。

【 0 0 6 0 】

【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。

【 0 0 6 1 】(第 1 実施例) 図 3 は、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。

【 0 0 6 2 】情報処理装置 3 0 1 は、CPU (Central Processing Unit) 3 0 2 により制御され、RAM (Random Access Memory) などの主記憶装置 3 0 3 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 3 0 4 には CPU 3 0 2 が実行するプログラムが記憶される。

【 0 0 6 3 】情報処理装置 3 0 1 に電源が投入されると、CPU 3 0 2 は、まず、ROM (Read Only Memory) 3 0 8 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 3 0 4 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 3 0 3

にロードして実行する。

【 0 0 6 4 】実行した結果は、外部記憶装置 3 0 4 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 3 0 5 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 3 0 6 を用いて情報処理装置に対する指示を与える。

【 0 0 6 5 】ここで、情報処理装置 3 0 1 が図 1 に示すランダムなベクトル列の出力装置 1 0 0 として機能する場合、主記憶装置 3 0 3 は、第 1 の記憶手段 1 0 1、第 2 の記憶手段 1 0 3 として機能し、CPU 3 0 2 は、第 1 の計算手段 1 0 2、第 2 の計算手段 1 0 4、第 1 の更新手段 1 0 6、第 2 の更新手段 1 0 7 として機能し、外部記憶装置 3 0 4 は、結果をファイルとして出力する場合は出力手段 1 0 5 として機能し、表示装置 3 0 5 は、結果を表示して出力する場合は出力手段 1 0 5 として機能し、主記憶装置 3 0 3 は、結果をほかのプログラムで利用する場合は出力手段 1 0 5 として機能する。

【 0 0 6 6 】また、情報処理装置 3 0 1 が、図 2 に示すランダムなベクトル列の出力装置 2 0 0 として機能する場合は、CPU 3 0 2 は、主記憶装置 3 0 3 や、必要に応じて外部記憶装置 3 0 4、表示装置 3 0 5 と共働して、生成手段 2 0 1、第 1 の出力手段 2 0 2、第 2 の出力手段 2 0 3、第 3 の出力手段 2 0 4 として機能する。

【 0 0 6 7 】また、主記憶装置 3 0 3、外部記憶装置 3 0 4 は、本発明の情報記録媒体として機能する。また、ROM 3 0 8 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。

【 0 0 6 8 】以下、図 4 を参照して、本発明のランダムな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。

【 0 0 6 9 】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。

【 0 0 7 0 】まず、CPU 3 0 2 は、現在の時刻などから乱数の種を取得する (ステップ S 4 0 1)。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。

【 0 0 7 1 】なお、乱数の種は、ユーザが入力装置 3 0 6 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。

【 0 0 7 2 】次に、CPU 3 0 2 は、取得した種をそれぞれ主記憶装置 3 0 3 内の第 1 の記憶手段 1 0 1 と、

第 2 の記憶手段 1 0 3 とに記憶する (ステップ S 4 0 2) 。これにより、乱数を生成するための初期値が設定される。

【 0 0 7 3 】なお、ステップ S 4 0 1 からステップ S 4 0 2 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 2 0 0 の生成手段 2 0 1 が実行する処理に相当する。

【 0 0 7 4 】さらに、CPU 3 0 2 は、第 1 の記憶手段 1 0 1 に記憶された値 x を取得し (ステップ S 4 0 3) 、これを用いて値 $x' = f(x)$ を計算し (ステップ S 4 0 4) 、計算された値 x' を第 1 の記憶手段 1 0 1 に記憶させて更新する (ステップ S 4 0 5) 。

【 0 0 7 5 】すなわち、ステップ S 4 0 4 において、CPU 3 0 2 は、第 1 の計算手段として機能することになる。

【 0 0 7 6 】ついで、CPU 3 0 2 は、第 1 の記憶手段 1 0 1 に記憶された更新後の値 x' と、第 2 の記憶手段 1 0 3 に記憶された値 y とを取得し (ステップ S 4 0 6) 、これらを用いて値 $y' = g(x', y)$ を計算し (ステップ S 4 0 7) 、計算された値 y' を第 2 の記憶手段 1 0 3 に記憶させて更新する (ステップ S 4 0 8) 。

【 0 0 7 7 】すなわち、ステップ S 4 0 7 において、CPU 3 0 2 は、第 2 の計算手段として機能することになる。

【 0 0 7 8 】最後に、CPU 3 0 2 は、第 1 の記憶手段 1 0 1 に記憶された更新後の値 x' と、第 2 の記憶手段 1 0 3 に記憶された更新後の値 y' とを結合して、外部記憶装置 3 0 4 などに出力し (ステップ S 4 0 9) 、ステップ S 4 0 3 に戻る。

【 0 0 7 9 】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 に示すランダムなベクトル列の出力装置 2 0 0 の生成手段 2 0 1 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。

【 0 0 8 0 】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 3 0 4 に出力されることになる。

【 0 0 8 1 】なお、図 2 に示すランダムなベクトル列の出力装置 2 0 0 の第 1 の出力手段 2 0 2 が実行する処理はステップ S 4 0 3 ~ ステップ S 4 0 5 に、第 2 の出力手段 2 0 3 が実行する処理はステップ S 4 0 6 ~ ステップ S 4 0 8 に、第 3 の出力手段 2 0 4 が実行する処理はステップ S 4 0 6 により、それぞれ実現されている。

【 0 0 8 2 】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。

【 0 0 8 3 】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。

【 0 0 8 4 】

【 数 7 】

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

【 0 0 8 5 】

【 数 8 】

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

ただし

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

【 0 0 8 6 】図 6 には、ステップ S 4 0 9 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 S 4 0 9 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。

【 0 0 8 7 】発明者は、「一般に密度関数 (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 (x, y) を有する有理写像 $g(x, \cdot)$ 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 (x, y) (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。

【 0 0 8 8 】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、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。

【 0 0 8 9 】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。

【 0 0 9 0 】(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ランダムな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に示すランダムなベクトル列の出力装置100の第1の記憶手段101と第2の記憶手段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の計算手段102と第2の計算手段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】出力手段105は、第2の計算手段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の更新手段106と第2の更新手段107とは、第1の計算手段102と第2の計算手段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の記憶手段101と第2の記憶手段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ランダムな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に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、手順などで表現される) A と、

$x[0], x[1], x[2], x[3], \dots$

$x[0] =$

$x[i+1] = f(x[i])$ (ただし $i \geq 0$)

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、

$y[0], y[1], y[2], y[3], \dots$

$y[0] =$

$y[i+1] = g(x[i+1], y[i])$ (ただし $i \geq 0$)

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ランダムな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す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、上記の発明に係るランダムな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】本発明のランダムな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】本発明のランダムな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

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】

- 1 0 0 ランダムなベクトル列の出力装置
- 1 0 1 第 1 の記憶手段
- 1 0 2 第 1 の計算手段
- 1 0 3 第 2 の記憶手段
- 1 0 4 第 2 の計算手段
- 1 0 5 出力手段
- 1 0 6 第 1 の更新手段
- 1 0 7 第 2 の更新手段
- 2 0 0 ランダムなベクトル列の出力装置
- 2 0 1 生成手段
- 2 0 2 第 1 の出力手段
- 2 0 3 第 2 の出力手段
- 2 0 4 第 3 の出力手段
- 3 0 1 情報処理装置
- 3 0 2 CPU
- 3 0 3 主記憶装置

- 3 0 4 外部記憶装置
- 3 0 5 表示装置
- 3 0 6 入力装置
- 3 0 8 ROM

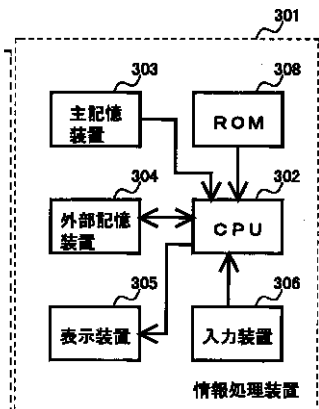
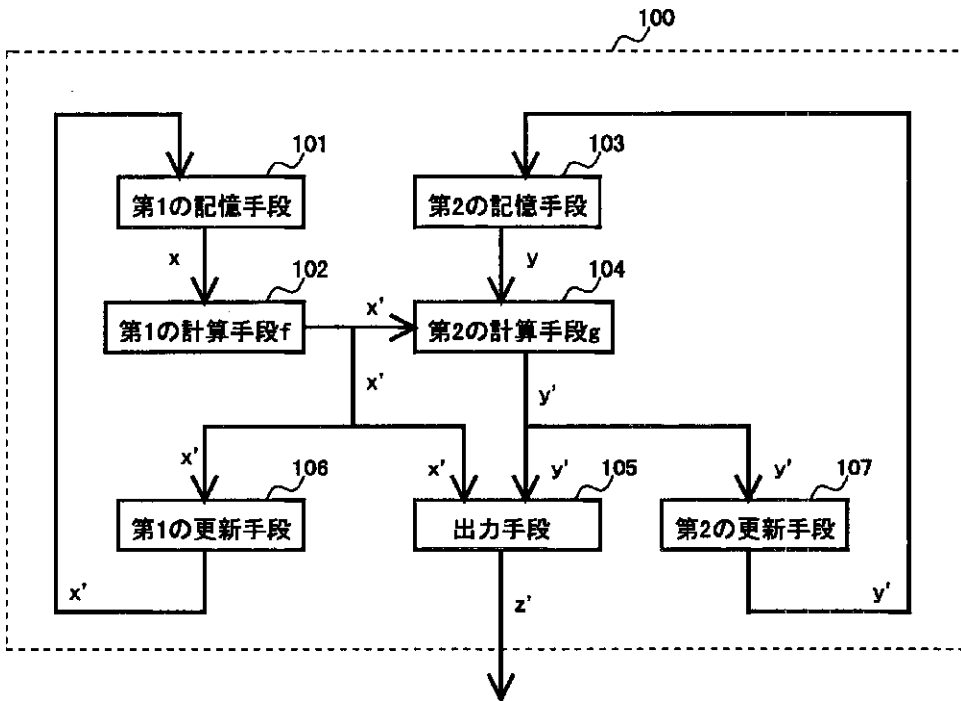
【要約】

【課題】 ランダムなベクトル列の出力装置、出力方法、および、情報記録媒体を提供する。

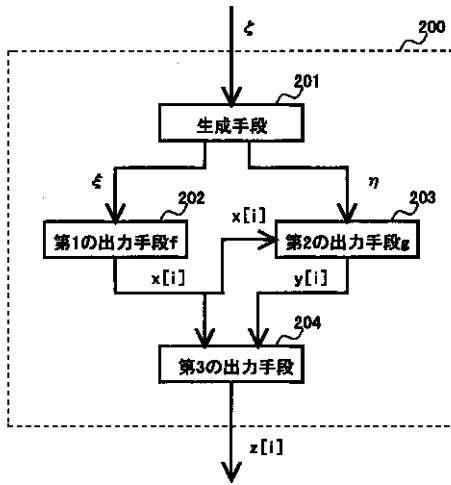
【解決手段】 ベクトル列の出力装置 1 0 0 の第 1 の記憶手段 1 0 1 は、1 次元以上のベクトル x を記憶し、第 1 の計算手段 1 0 2 は、記憶されたベクトル x に第 1 の有理ベクトル写像 f を適用した結果のベクトル $x' = f(x)$ を計算し、第 2 の記憶手段 1 0 3 は、1 次元以上のベクトル y を記憶し、第 2 の計算手段 1 0 4 は、結果のベクトル x' と、記憶されたベクトル y とに第 2 の有理ベクトル写像 g を適用した結果のベクトル $y' = g(x', y)$ を計算し、出力手段 1 0 5 は、結果のベクトル x' と結果のベクトル y' とを結合したベクトル z' を出力し、第 1 の更新手段 1 0 6 と第 2 の更新手段 1 0 7 とは、結果のベクトル x' を第 1 の記憶手段 1 0 1 に記憶させ、結果のベクトル y' を第 2 の記憶手段 1 0 3 に記憶させて更新する。

【図 1】

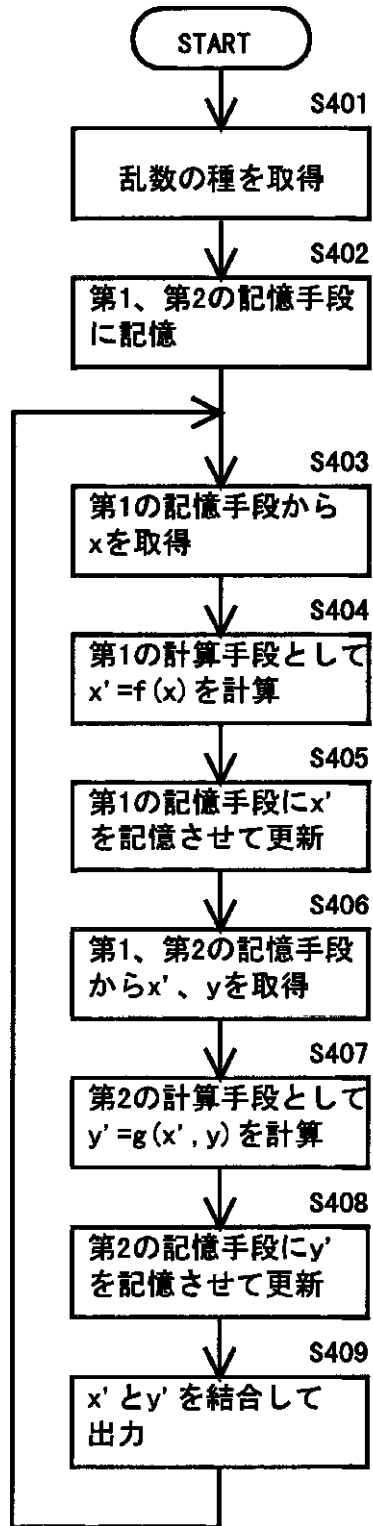
【図 3】



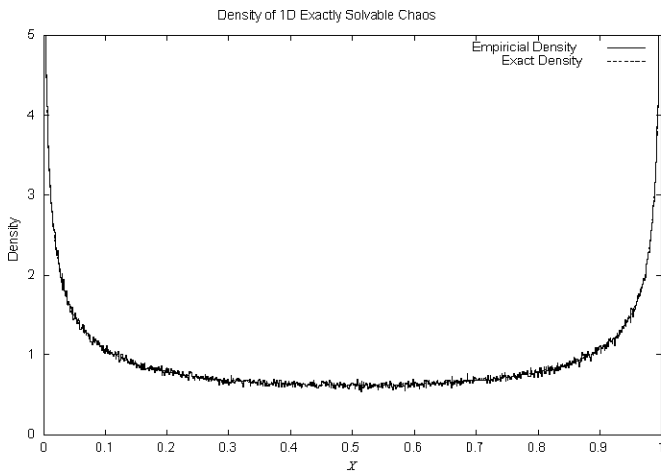
【 図 2 】



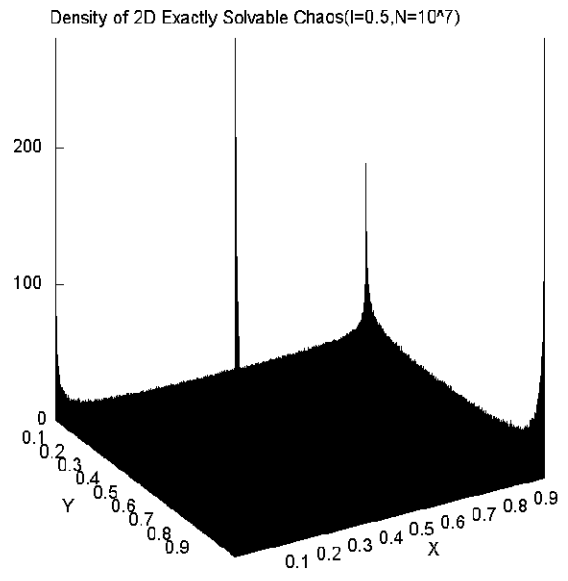
【 図 4 】



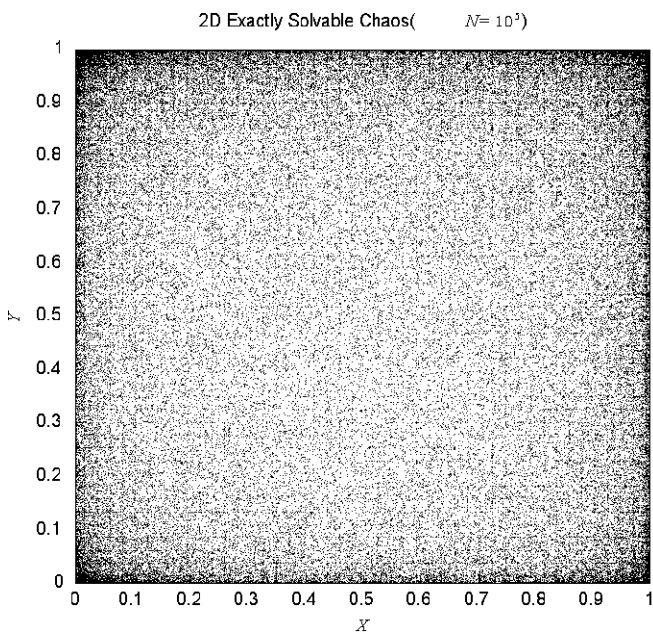
【 図 5 】



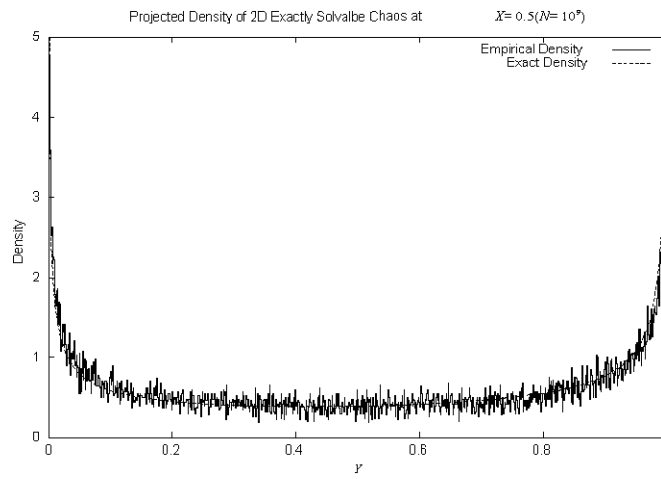
【 図 7 】



【 図 6 】



【 図 8 】



フロントページの続き

- (56) 参考文献 特開 平10 - 333569 (J P , A)
- 特開 平10 - 283344 (J P , A)
- 特開 平 7 - 311675 (J P , A)

(58) 調査した分野(Int.Cl.⁷, D B 名)

- G06F 7/58
- G09C 1/00 650
- H04L 9/22