

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関  
国際事務局



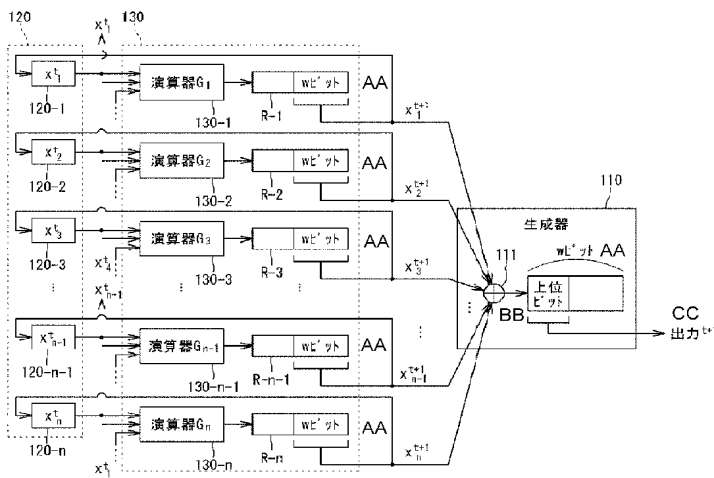
(43) 国際公開日  
2017年9月8日(08.09.2017)

(10) 国際公開番号  
WO 2017/150672 A1

- (51) 国際特許分類:  
G06F 7/58 (2006.01) G09C 1/00 (2006.01)
  - (21) 国際出願番号: PCT/JP2017/008294
  - (22) 国際出願日: 2017年3月2日(02.03.2017)
  - (25) 国際出願の言語: 日本語
  - (26) 国際公開の言語: 日本語
  - (30) 優先権データ:  
特願 2016-041564 2016年3月3日(03.03.2016) JP
  - (71) 出願人: 国立大学法人京都大学(KYOTO UNIVERSITY) [JP/JP]; 〒6068501 京都府京都市左京区吉田本町3番地1 Kyoto (JP).
  - (72) 発明者: 岩▲崎▼ 淳 (IWASAKI, Atsushi); 〒6068501 京都府京都市左京区吉田本町3番地1 国立大学法人京都大学内 Kyoto (JP). 梅野健(UMENO, Ken); 〒6068501 京都府京都市左京区吉田本町3番地1 国立大学法人京都大学内 Kyoto (JP).
  - (74) 代理人: 特許業務法人サンクレスト国際特許事務所(SUNCREST PATENT AND TRADEMARK ATTORNEYS); 〒6500023 兵庫県神戸市中央区栄町通四丁目1番11号 Hyogo (JP).
  - (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
  - (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーロピア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).
- 添付公開書類:  
— 国際調査報告 (条約第 21 条(3))

(54) Title: RANDOM NUMBER GENERATION DEVICE, RANDOM NUMBER GENERATION METHOD, AND COMPUTER PROGRAM

(54) 発明の名称: 乱数発生装置、乱数発生方法及びコンピュータプログラム



110 Generator  
130-1, 130-2, 130-3, 130-n-1, 130-n Calculator  
AA w bit  
BB Higher-order bits  
CC Output

(57) Abstract: A random number generation device 100 equipped with: a storage unit 120 storing multiple variables; a calculation unit 130 that performs multiple update formula calculations for updating each of the multiple variables, and outputs updated values for the multiple variables to the storage unit 120; and a generator 110 that generates a random number on the basis of one or more of the multiple variables. The update formula includes a permutation polynomial expression for the subject variable updated by the update formula, and another variable among the multiple variables other than the subject variable, and the periodicity when the subject variable updated by the update formula is repeatedly updated is a unicursal periodicity.

(57) 要約: 乱数発生装置 100 は、複数の変数を記憶する記憶部 120 と、複数の変数それぞれを更新する複数の更新式の演算を実行し、複数の変数の更新値を記憶部 120 へ出力する演算部 130 と、複数の変数の少なくともいずれか一つの変数に基づいて、乱数を生成する生成器 110 と、を備える。更新式は、更新式によって更新される対象変数の置換多項式と、複数の変数に含まれる対象変数以外の他の変数と、を含み、更新式によって対象変数を繰り返し更新したときの周期性が、一筆書き周期性で

ある。

WO 2017/150672 A1

## 明 細 書

発明の名称：

乱数発生装置、乱数発生方法及びコンピュータプログラム

技術分野

[0001] 本発明は、乱数発生装置等に関するものである。

背景技術

[0002] 特許文献1は、置換多項式を用いた乱数発生装置を開示している。

先行技術文献

特許文献

[0003] 特許文献1：特許第3806762号公報

発明の概要

[0004] 一般に、乱数には、高い乱数性が望まれる。置換多項式の値を用いて生成される乱数の乱数性を高くするための一つのアプローチは、置換多項式の次数を大きくすることである。しかし、置換多項式の次数が大きくなると、演算器による演算時間の増大を招き易い。

[0005] このため、次数を大きくするのは別のアプローチで、高い乱数性を容易に得ることが望まれる。

[0006] 一の観点からみた本発明は、乱数発生装置である。乱数発生装置は、複数の変数それぞれを更新する複数の更新式の演算を実行する。更新式は、更新式によって更新される対象変数の置換多項式と、複数の変数に含まれる対象変数以外の他の変数と、を含む。更新式は、更対象変数を繰り返し更新したときの周期性が、一筆書き周期性である。本発明によれば、一筆書き多項式と同様の長周期が得られ、高い乱数性が容易に得られる。

[0007] 他の観点からみた本発明は、乱数を生成する方法である。他の観点からみた本発明は、コンピュータを乱数発生装置として機能させるためのコンピュータプログラムである。コンピュータプログラムは、コンピュータ読み取り可能な記録媒体に記憶される。

## 図面の簡単な説明

[0008] [図1]置換多項式の軌道を示す図である。

[図2]一筆書き多項式の軌道を示す図である。

[図3]乱数発生装置のブロック図である。

## 発明を実施するための形態

[0009] [1. 用語]

[0010] [1. 1 置換多項式]

置換多項式  $F(X)$  は、有限集合上で  $X$  の置換を与える多項式である。置換多項式は、有限集合において全単射を与える。置換多項式による変数  $X$  の値の変化を示す軌道は、必ず、周期軌道になる。すなわち、置換多項式による変数  $X$  の値の変化は、周期性を持つ。

[0011] [1. 2 2 冪剰余環]

2 冪剰余環は、以下のように表される有限集合である。本明細書では、以下のように表される 2 冪剰余環を、「冪指数  $w$  の 2 冪剰余環」というものとする。 $w$  は、任意の非負整数である。

[数1]

$$\mathbb{Z}/2^w\mathbb{Z} = \{0, 1, 2, \dots, 2^w - 1\}$$

なお、計算途中で値が集合の範囲外に出たら、“ $\text{mod } 2^w$ ” をとる。 $\text{mod}$  は、剰余演算子である。

[0012] [1. 3 2 冪剰余環上置換多項式]

2 冪剰余環上置換多項式は、2 冪剰余環上で置換を与える置換多項式である。2 冪剰余環上置換多項式は、整数係数多項式である。すなわち、2 冪剰余環上置換多項式  $F(X)$  は、 $F(X) \text{ mod } 2^w$  が、冪指数  $w$  の 2 冪剰余環上で全単射を与える整数係数多項式であり、以下のようにも定義される。

[数2]

$$F(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0$$

$$\{F(\bar{X}) \bmod 2^w \mid \bar{X} \in \mathbb{Z}/2^w \mathbb{Z}\} = \mathbb{Z}/2^w \mathbb{Z}$$

[0013] 例えば、冪指数3の2冪剰余環上における、置換多項式  $F_a(X) = 2X^2 + X + 1$  の軌道は、図1(a)に示すように、周期軌道になる。すなわち、 $F_a(0) \bmod 2^3 = 1$  であり、 $F_a(1) \bmod 2^3 = 4$  であり、 $F_a(4) \bmod 2^3 = 5$  であり、 $F_a(5) \bmod 2^3 = 0$  である。

[0014] また、置換多項式  $F_a(X) = 2X^2 + X + 1$  は、図1(b)に示す別の周期軌道も持つ。すなわち、 $F_a(2) \bmod 2^3 = 3$  であり、 $F_a(3) \bmod 2^3 = 6$  であり、 $F_a(6) \bmod 2^3 = 7$  であり、 $F_a(7) \bmod 2^3 = 2$  である。

[0015] [1.4 一筆書き周期性と一筆書き多項式]

一筆書き周期性とは、多項式  $F(X)$  が成す1本の軌道(1周期の軌道)が、2冪剰余環のすべての要素をめぐることをいう。軌道が一筆書き周期性を持つ多項式を、一筆書き多項式という。一筆書き多項式は、以下のように定義される。

[数3]

$$\forall w \in \mathbb{N} \cup \{0\}, \forall \bar{X} \in \mathbb{Z}/2^w \mathbb{Z}, \{F^i(\bar{X}) \bmod 2^w \mid i \in \mathbb{Z}/2^w \mathbb{Z}\} = \mathbb{Z}/2^w \mathbb{Z}$$

[0016] 図2は、冪指数3の2冪剰余環  $= \{0, 1, 2, 3, 4, 5, 6, 7\}$  上における、一筆書き多項式  $F_b(X) = 4X^2 + X + 1$  の軌道を示している。図2に示す軌道は、周期軌道であり、1周期の軌道が、 $\{0, 1, 2, 3, 4, 5, 6, 7\}$  のすべての要素を1回ずつ通過している。したがって、 $F_b(X)$  による2冪剰余環上の軌道は、一筆書き周期性を持ち、 $F_b(X)$  は一筆書き多項式である。図1と図2との対比からも明らかのように、一筆書き周期性がある場合、軌道の周期は最大となり、周期長は  $2^w$  となる。長い周期は、乱数発生において有利である。

[0017] 置換多項式  $F(X)$  が、一筆書き多項式である必要十分条件は、

[数4]

$$a_0 \equiv 1 \pmod{2},$$

$$a_1 \equiv 1 \pmod{2},$$

$$(a_1 + a_2 + a_3 + \dots) \equiv 1 \pmod{4},$$

$$(a_3 + a_5 + a_7 + \dots) \equiv 2a_2 \pmod{4}$$

がすべて成り立つことである。上記の必要十分条件は、

係数  $a_0$  と 1 とは法 2 に関して合同であり、

係数  $a_1$  と 1 とは法 2 に関して合同であり、

添え字が 1 以上であるすべての係数  $a_1, a_2, a_3, \dots$  の和と 1 とは、法 4 に関して合同であり、

添え字が 3 以上の奇数であるすべての係数  $a_3, a_5, a_7, \dots$  の和と  $2a_2$  とは、法 4 に関して合同であることを示す。

[0018] 一筆書き多項式は、長周期であるという観点では乱数の生成に有利であるが、時間発展（変数  $X$  の時間的变化）が単純となり、十分な乱数性を得るのが困難な場合がある。したがって、単なる一筆書き多項式単体は、乱数の生成に不利な面も有する。

[0019] [2. 実施形態の概要]

[0020] [第1項]

実施形態に係る乱数発生装置は、

複数の変数を記憶する記憶部と、

複数の前記変数それぞれを更新する複数の更新式の演算を実行し、複数の前記変数の更新値を前記記憶部へ出力する演算部と、

複数の前記変数の少なくともいずれか一つの変数に基づいて、乱数を生成する生成器と、

を備える。

前記更新式は、

前記更新式によって更新される対象変数の置換多項式と、複数の前記変数に含まれる前記対象変数以外の他の変数と、を含み、

前記更新式によって前記対象変数を繰り返し更新したときの周期性が、一筆書き周期性である。

[0021] 第1項の乱数発生装置によれば、乱数の生成に用いられる変数を更新する更新式は、更新式によって更新される対象変数以外の他の変数も含むので、対象変数の置換多項式の次数を大きくしなくても、乱数性を高くすることができる。しかも、更新式は一筆書き周期性を持つので、長い周期を得ることができる。

[0022] [第2項]

前記更新式は、前記対象変数の前記置換多項式と、前記他の変数と、の和を含むことができる。

[0023] [第3項]

前記対象変数の前記置換多項式は、前記対象変数に乘じられる係数部分であって、多項式で表される前記係数部分を含み、前記他の変数は、前記係数部分に含まれていてもよい。

[0024] [第4項]

前記置換多項式は、一筆書き多項式であるのが好ましい。

[0025] [第5項]

実施形態に係る方法は、

演算部が、記憶部に記憶された複数の変数それぞれを更新する複数の更新式の演算を実行すること、

前記演算部が、複数の前記変数の更新値を記憶部へ出力すること、

生成器が、複数の前記変数の少なくともいずれか一つの変数に基づいて、乱数を生成すること、

を含む。

前記更新式は、

前記更新式によって更新される対象変数の置換多項式と、複数の前記変数に含まれる前記対象変数以外の他の変数と、を含み、

前記更新式によって前記対象変数を繰り返し更新したときの周期性が、

一筆書き周期性である。

[0026] [第6項]

実施形態に係るコンピュータプログラムは、

コンピュータを、

複数の変数を記憶する記憶部、

複数の前記変数それぞれを更新する複数の更新式の演算を実行し、複数の前記変数の更新値を前記記憶部へ出力する演算部、及び

複数の前記変数の少なくともいずれか一つの変数に基づいて、乱数を生成する生成器

として機能させるためのコンピュータプログラムである。

前記更新式は、

前記更新式によって更新される対象変数の置換多項式と、複数の前記変数に含まれる前記対象変数以外の他の変数と、を含み、

前記更新式によって前記対象変数を繰り返し更新したときの周期性が、一筆書き周期性である。

[0027] [3. 実施形態の詳細]

[0028] [3. 1 乱数発生装置の構成]

図3は、実施形態に係る乱数発生装置100を示している。乱数発生装置100は、例えば、乱数を発生させるための演算を実行する演算回路を備えたハードウェアによって構成されている。乱数発生装置100は、乱数発生コンピュータプログラムがインストールされたコンピュータであってもよい。コンピュータは、乱数発生コンピュータプログラムを実行することによって、乱数発生装置100として機能する。

[0029] 乱数発生装置100は、乱数を生成する生成器110を備えている。生成器110は、変数 $x$ から乱数を生成する。実施形態に係る生成器110は、 $n$ 個（ $n$ は2以上の整数）の変数 $x_1, \dots, x_n$ に基づいて、乱数を生成する。ここで、変数 $x_1, \dots, x_n$ は、それぞれ、 $w$ ビットの符号なし変数である。 $w$ は、任意の非負整数であり、例えば64である。以下では、変

数  $x$  の時間発展を表す  $x^t$  の表記を用いることもある。  $x^t$  は、時刻  $t$  における変数  $x$  の値を示す。

- [0030] 乱数発生装置 100 は、  $n$  個の変数を記憶する記憶部 120 と、  $n$  個の変数を更新する演算を実行する演算部 130 と、を備える。記憶部 120 は、  $n$  個の変数を記憶するための  $n$  個の記憶領域 120-1,  $\dots$ , 120- $n$  を有する。各記憶領域 120-1,  $\dots$ , 120- $n$  の大きさは、  $w$  ビットである。
- [0031] 演算部 130 は、  $n$  個の記憶領域 120-1,  $\dots$ , 120- $n$  に対応する、  $n$  個の演算器 130-1,  $\dots$ , 130- $n$  を有している。各演算器 130-1,  $\dots$ , 130- $n$  は、対応する記憶領域 120-1,  $\dots$ , 120- $n$  に記憶された変数  $x_1, \dots, x_n$  を更新するため更新式本体  $G_1, \dots, G_n$  の演算を実行する。更新式本体  $G_1, \dots, G_n$  は、後述する更新式から “ $\text{mod } 2^w$ ” を除いた部分をいう。
- [0032] 各演算器 130-1,  $\dots$ , 130- $n$  が演算の対象とする変数  $x$  を、対象変数とよぶ。例えば、演算器 130-1 にとっての対象変数は、変数  $x_1$  であり、演算器 130- $n$  にとっての対象変数は、変数  $x_n$  である。
- [0033] 各演算器 130-1,  $\dots$ , 130- $n$  は、対象変数の更新のため、記憶部 120 から対象変数を取得する。例えば、演算器 130-1 は、記憶領域 120-1 から変数  $x_1$  を対象変数として取得し、演算器 130- $n$  は、記憶領域 120- $n$  から変数  $x_n$  を対象変数として取得する。
- [0034] 各演算器 130-1,  $\dots$ , 130- $n$  は、対象変数だけでなく、記憶部 120 から他の変数も取得する。他の変数は、複数の変数  $x_1, \dots, x_n$  に含まれる変数であって、対象変数以外の変数である。他の変数は、1 つであってもよいし、複数であってもよい。各演算器 130 は、複数の変数  $x_1, \dots, x_n$  すべてを取得してもよい。例えば、演算器 130-1 は、記憶領域 120-2 から変数  $x_2$  などを他の変数として取得し、演算器 130- $n$  は、記憶領域 120-1 から変数  $x_1$  などを他の変数として取得する。
- [0035] 各演算器 130-1,  $\dots$ , 130- $n$  が取得した他の変数は、対象変



数とともに、対象変数の更新に用いられる。すなわち、更新式は、対象変数と他の変数とを含む式である。更新式の例については後述する。

[0036] 各演算器 130-1, ..., 130-n は、更新式本体  $G_1, \dots, G_n$  の演算結果  $R-1, \dots, R-n$  を出力する。演算結果  $R-1, \dots, R-n$  のビット数は、 $w$  ビットを超えることがある。各演算結果  $R-1, \dots, R-n$  の下位  $w$  ビットが、変数  $x_1^t, \dots, x_n^t$  の更新値  $x_1^{t+1}, \dots, x_n^{t+1}$  となる。各演算結果  $R-1, \dots, R-n$  から、それらの下位  $w$  ビットを取り出すことは、数学的には、各演算結果  $R-1, \dots, R-n$  に対して、" $\text{mod } 2^w$ " の演算を行うことと等価である。本実施形態では、剰余演算を行う必要がないため、演算を高速化できる。

[0037] 更新値  $x_1^{t+1}, \dots, x_n^{t+1}$  は、演算部 130 から記憶部 120 へ出力される。更新値  $x_1^{t+1}, \dots, x_n^{t+1}$  は、記憶領域 120-1, ..., 120-n に上書きされる。

[0038] 本実施形態では、生成器 110 は、時刻  $t+1$  において演算部 130 から出力された 1 又は複数の変数  $x^{t+1}$  から、乱数発生に用いられる出力系列  $t+1$  を生成し、その出力系列  $t+1$  から時刻  $t+1$  における乱数  $t+1$  を生成する。生成器 110 の構成は、1 又は複数の変数  $x$  から乱数を生成する所定の演算を行うものであれば、特に限定されない。生成器 110 が変数から乱数を生成する演算は、複数の変数  $x$  全部又は一部を如何様に組み合わせた演算であってもよいし、複数の変数  $x$  のうちの 1 つの変数だけを用いた演算であってもよい。なお、生成器 110 は、変数  $x$  の更新値が記憶部 120 に上書きされてから、変数  $x$  を記憶部 120 から読み出して乱数を生成してもよい。

[0039] 実施形態に係る生成器 110 は、排他的論理和演算部 111 を備える。排他的論理和演算部 111 は、 $n$  個の変数  $x_1, \dots, x_n$  の排他的論理演算を行う。排他的論理和演算部 111 の出力の所定上位ビット（例えば、上位 16 ビット）が、出力系列  $t+1$  となる。生成器 110 は、出力系列  $t+1$  を用いて乱数  $t+1$  を生成し、生成された乱数  $t+1$  を出力する。なお、排他的論理和演算部 111 は、 $N$  個の変数  $x_1, \dots, x_n$  それぞれの上位ビットに対す

る排他的論理和演算を行っても良い。また、生成器 1 1 0 は、出力系列を乱数として出力してもよい。

[0040] [3. 2 更新式の第 1 例]

$n$  個の変数  $x_1, \dots, x_n$  それぞれ更新する  $n$  個の更新式の第 1 例は、以下のとおりである。

[数5]

$$\begin{aligned} x_1^{(i+1)} &= F_1(x_1^{(i)}) + c_{1,1}x_1^{(i)} + c_{1,2}x_2^{(i)} + c_{1,3}x_3^{(i)} + \dots + c_{1,n}x_n^{(i)} \pmod{2^w} \\ x_2^{(i+1)} &= F_2(x_2^{(i)}) + c_{2,1}x_1^{(i)} + c_{2,2}x_2^{(i)} + c_{2,3}x_3^{(i)} + \dots + c_{2,n}x_n^{(i)} \pmod{2^w} \\ x_3^{(i+1)} &= F_3(x_3^{(i)}) + c_{3,1}x_1^{(i)} + c_{3,2}x_2^{(i)} + c_{3,3}x_3^{(i)} + \dots + c_{3,n}x_n^{(i)} \pmod{2^w} \\ &\vdots \\ x_n^{(i+1)} &= F_n(x_n^{(i)}) + c_{n,1}x_1^{(i)} + c_{n,2}x_2^{(i)} + c_{n,3}x_3^{(i)} + \dots + c_{n,n}x_n^{(i)} \pmod{2^w} \end{aligned}$$

ここで、

- $F_1(X), F_2(X), \dots, F_n(X)$  : 一筆書き多項式
- $x_1, x_2, \dots, x_n$  :  $w$  ビットの符号なし変数

また、任意の変数  $a$  に対して、 $a^{(i)}$  で時刻  $i$  での変数  $a$  の値を表すものとする

[0041] 各更新式の右辺は、“ $\pmod{2^w}$ ”の部分と、“ $\pmod{2^w}$ ”以外の部分である更新式本体と、を有する。例えば、変数  $x_1$  の更新式の更新式本体  $G_1$  は、変数  $x_1$  の更新式のうち、“ $\pmod{2^w}$ ”以外の部分である“ $F_1(x_1^{(i)}) + c_{1,1}x_1^{(i)} + c_{1,2}x_2^{(i)} + c_{1,3}x_3^{(i)} + \dots + c_{1,n}x_n^{(i)}$ ”の部分である。他の変数  $x_2, \dots, x_n$  についても同様である。

[0042] 更新式本体は、対応する演算器によって演算される。例えば、更新式本体  $G_1$  は、演算器 1 3 0 - 1 によって演算される。更新式本体  $G_1$  は、対象変数  $x_1$  の置換多項式としての一筆書き多項式  $F_1(x_1^{(i)})$ 、と、付加多項式  $c_{1,1}x_1^{(i)} + c_{1,2}x_2^{(i)} + c_{1,3}x_3^{(i)} + \dots + c_{1,n}x_n^{(i)}$  と、の和として表される。付加多項式は、少なくとも一つの変数（対象変数  $x_1$  以外の変数） $x_2, \dots, x_n$  を含む。付加多項式は、対象変数  $x_1$  を含んでも良

い。第1例において、付加多項式は、付加多項式に含まれる複数の変数  $x$  に関して、 $c_{k, l}$  を係数とした線形結合となっている。なお、本明細書において、多項式は、単項式を含む。以上の更新式本体  $G_1$  についての説明は、他の変数  $x_2, \dots, x_n$  についての更新式本体  $G_2, \dots, G_n$  においても同様である。

[0043] 更新式の第1例では、各一筆書き多項式に付加多項式が付加されているが、各更新式全体における一筆書き周期性が維持されている。

[0044] 更新式の第1例において、一筆書き周期性を持つための条件は、以下のとおりである。

- ・係数  $c_{k, l}$  ( $k = 1, 2, \dots, n, l = 1, 2, \dots, n$ ) はすべて偶数（偶数は0を含む、以下同様）である。

- ・任意の  $k$  に対して、 $c_{k, 1}, c_{k, 2}, \dots, c_{k, n}$  のうち、4で割り切れないものの個数は偶数である。

[0045] なお、付加多項式中の”+”、及び、付加多項式と置換多項式（一筆書き多項式）との和をとるための”+”は、算術和演算である必要はなく、排他的論理和演算であってもよい。また、複数の”+”に対応する演算として、算術和演算と排他的論理和演算とが混在してもよい。算術和演算と排他的論理和演算とが混在する場合には、両演算の優先順位を適宜決めればよい。

[0046] 更新式の第1例は、以下の点で有用である。まず、各更新式は一筆書き周期性を持つため、各変数の周期は、 $2^w$  という長周期になることが保証される。すなわち、以下が成り立つ。

[数6]

$$\forall m, x_m^{(a)} \neq x_m^{(0)} \quad (0 < a < 2^w), \quad x_m^{(2^w)} = x_m^{(0)}.$$

なお、長周期性は、疑似乱数発生器やストリーム暗号において重要な性質である。

[0047] 更新式の第1例の時間発展は、単なる一筆書き多項式単体の時間発展より複雑な挙動となるため有利である。更新式の第1例では、各更新式の次数は

2に抑えられているが、次数を高くしなくても、時間発展の複雑な挙動が得られる。次数の増加は、演算負荷が大きい乗算の増加を招くが、更新式の第1例では、各更新式の次数を低く抑えられて有利である。

[0048] また、更新式の第1例は、一筆多項式に付加多項式が付加されているが、一筆書き多項式と同様に、実質的に除算を行う必要がない。つまり、剰余算はデジタルコンピュータ上では無視できるという一筆書き多項式の優れた点が維持されている。

[0049]  $n$ 個の更新式を並列に演算することで、すなわち、各演算器  $130-1$ ,  $\dots$ ,  $130-n$ が並列に演算することで、変数の数が増加しても演算時間の増加を抑えることができる。

[0050] 係数  $c_{k,i}$ の値として、2の冪乗のものを選択すると、更新式中では乗算として表現されている  $c_{k,i} \times x_{k,i}$ を、変数  $x_{k,i}$ のビットシフト操作で実現できるため、より高速化が可能である。また、係数  $c_{k,i}$ の値としては、上記の条件を満たす限り、様々な値を採用できる。したがって、乱数発生装置としての設計の自由度が高くなる。

[0051] [3.3 更新式の第1例の評価]

更新式の第1例の乱数性を評価するため、以下の  $n$ 個の更新式を用いた。

[数7]

$$\begin{array}{l}
 \text{更新式本体} \\
 \overline{x_1^{(i+1)} = [2\{x_1^{(i)}\}^2 + a_1x_1^{(i)} + b_1] + 4x_2^{(i)} \pmod{2^{64}} \\
 x_2^{(i+1)} = [2\{x_2^{(i)}\}^2 + a_2x_2^{(i)} + b_2] + 4x_3^{(i)} \pmod{2^{64}} \\
 x_3^{(i+1)} = [2\{x_3^{(i)}\}^2 + a_3x_3^{(i)} + b_3] + 4x_4^{(i)} \pmod{2^{64}} \\
 x_4^{(i+1)} = [2\{x_4^{(i)}\}^2 + a_4x_4^{(i)} + b_4] + 4x_5^{(i)} \pmod{2^{64}} \\
 x_5^{(i+1)} = [2\{x_5^{(i)}\}^2 + a_5x_5^{(i)} + b_5] + 4x_6^{(i)} \pmod{2^{64}} \\
 x_6^{(i+1)} = [2\{x_6^{(i)}\}^2 + a_6x_6^{(i)} + b_6] + 4x_1^{(i)} \pmod{2^{64}} \\
 \underbrace{\hspace{10em}}_{\text{一筆書き多項式}} \quad \underbrace{\hspace{2em}}_{\text{付加多項式}}
 \end{array}$$

ただし、 $x_1, x_2, x_3, x_4, x_5, x_6, a_1, a_2, a_3, a_4, a_5, a_6, b_1, b_2, b_3, b_4, b_5, b_6$  は 64bit 符号なし整数で、

$$a_1, a_2, \dots, a_6 \equiv 3 \pmod{4}, \quad b_1, b_2, \dots, b_6 \equiv 1 \pmod{2}$$

を満たす。

[0052] 評価は、図1の乱数発生装置における演算部130が上記のn個の更新式を演算するようにコンピュータを機能させるプログラムを、コンピュータに実行させて行った。乱数発生装置として機能させたコンピュータのプロセッサは、1.3GHz Intel Core i5である。なお、評価は、n個の更新式の演算を並列化せずに行った。

[0053] 評価において、生成部110は、演算部130が出力した変数 $x_1, x_2, x_3, x_4, x_5, x_6$ の排他的論理和をとり、その結果を、48ビット右シフトさせた16ビットの値（出力系列）を評価系列として生成する。すなわち、生成部110は、以下の演算を行う。

[数8]

$$(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6) \gg 48$$

[0054] 乱数性の評価は、以下を1セットとして40セット行った。

1.  $x_1, x_2, x_3, x_4, x_5, x_6, a_1, a_2, a_3, a_4, a_5, a_6, b_1, b_2, b_3, b_4, b_5, b_6$ の値をランダムに決める。
2. 「1.」で決めた値をセットした乱数発生装置を実行させ、生成された評価系列から $10^9$ ビットの乱数を生成する。
3. 得られた乱数 $10^9$ ビットの乱数を、 $10^6$ ビットの乱数1000本とする。1000本の乱数を、米国商務省標準技術局（NIST）SP 800-22で定義される乱数検定にかける。

[0055] 表1は、乱数検定結果を示している。

[表1]

合格したテスト項目数	セット数
188	26
187	12
186	1
185	0
184	1

[0056] NIST SP 800-22は、188項目のテストで構成されている。188項目すべてについて合格したのは、40セット中26セットであった。理想的な乱数の場合に、188項目すべてをクリアするセット数の理論値は、標準偏差の範囲で、40セット中21セットから27セットである。また、すべての項目に合格しなかった14セットについても、理想的な乱数が十分にとり得る成績である。よって、乱数性に関し良好な結果が得られていることがわかる。

[0057] また、評価では、3 Gbps以上の実行速度が得られており、実行速度の観点からも良好な結果が得られた。

[0058] [3.4 更新式の第2例]

N個の変数 $x_1, \dots, x_N$ それぞれ更新するN個の更新式の第2例は、以下のとおりである。

[数9]

$$\begin{aligned}
 x_1^{(t+1)} &= \sum_j \left[ a_{1,j} + \sum_{k,l} C_{1,j,k,l} \{x_k^{(t)}\}^l \right] \{x_1^{(t)}\}^j \bmod 2^w, \\
 x_2^{(t+1)} &= \sum_j \left[ a_{2,j} + \sum_{k,l} C_{2,j,k,l} \{x_k^{(t)}\}^l \right] \{x_2^{(t)}\}^j \bmod 2^w, \\
 &\vdots \\
 x_N^{(t+1)} &= \sum_j \left[ a_{N,j} + \sum_{k,l} C_{N,j,k,l} \{x_k^{(t)}\}^l \right] \{x_N^{(t)}\}^j \bmod 2^w,
 \end{aligned}$$

ここで

- ・  $j$  は 0 以上の整数を、 $k, l$  は 1 以上の整数を動く。ただし、有限の範囲。
- ・ 各  $l$  について  $F_l(X) = \sum_j a_{i,j} X^j$  : 筆書き多項式
- ・  $x_1, x_2, \dots, x_N$  :  $w$  ビットの符号なし整数型変数
- ・  $j = 0$  の場合を除く、任意の  $(j, k, l)$  について  $C_{i,j,k,l}$  は 4 で割り切れる。
- ・ 任意の  $(i, k, l)$  について、 $C_{i,0,k,l}$  は 2 で割り切れる。
- ・ 任意の  $i$  について、 $\sum_{k,l} C_{i,0,k,l}$  は 4 で割り切れる。(言い換えると、 $i$  を固定したとき  $\{C_{i,0,k,l}\}$  のうち 4 で割り切れないものの個数は偶数)
- ・ 任意の変数  $b$  に対して、 $b^{(t)}$  で時刻  $t$  での変数  $b$  の値を表すものとする
- ・ 任意の  $i$  について、 $\sum_{k=1}^K \sum_l C_{i,0,k,l} \equiv 0 \pmod{4}$  ( $l$  は 3 以上の奇数)

[0059] なお、第 2 例中の ” + ” も、算術和演算である必要はなく、排他的論理和演算であってもよい。また、複数の ” + ” に対応する演算として、算術和演算と排他的論理和演算とが混在してもよい。算術和演算と排他的論理和演算とが混在する場合には、両演算の優先順位を適宜決めればよい。

[0060] 更新式の第 2 例は、第 1 例を包含する形式で定義されている。つまり、全係数  $c_{i,j,k,l}$  のうち、添え字  $j$  が 0 かつ添え字  $l$  が 1 (他の添え字  $i, k$  は、0 でもよいし 0 でなくてよい) である係数  $c_{i,0,k,1}$  以外のものすべてを 0 にすると、

[数10]

$$x_i^{(t+1)} = F_i(x_i^{(t)}) + \sum_k C_{i,0,k,1} x_k^{(t)}$$

となり、第1例に対応する。

[0061] 第2例においても、各変数  $x_1, \dots, x_N$  の更新式は、一筆書き周期性を有する。第2例においても、各更新式の右辺は、” mod  $2^w$ ” の部分と、” mod  $2^w$ ” 以外の部分である更新式本体と、を有する。第2例でも、更新式本体は、対象変数の置換多項式（一筆書き多項式）と、付加多項式としての和として表されるが、第2例では、付加多項式が含まれていなくても良い。第2例では、置換多項式の係数部分（対象変数に乘じられる部分）が、対象変数以外の他の変数を含む多項式で表される。

[0062] 以下は、第2例の具体例を示している。

[数11]

一筆書き多項式

$$\begin{aligned}
 x_1^{(t+1)} &= 2\{x_1^{(t)}\}^2 + \{4x_3^{(t)} + 3\}x_1^{(t)} + 4x_2^{(t)} + 1 \bmod 2^{64} \\
 x_2^{(t+1)} &= 2\{x_1^{(t)}\}^2 + \{4x_4^{(t)} + 3\}x_2^{(t)} + 4x_3^{(t)} + 1 \bmod 2^{64} \\
 x_3^{(t+1)} &= 2\{x_3^{(t)}\}^2 + \{4x_5^{(t)} + 3\}x_3^{(t)} + 4x_4^{(t)} + 1 \bmod 2^{64} \\
 x_4^{(t+1)} &= 2\{x_4^{(t)}\}^2 + \{4x_6^{(t)} + 3\}x_4^{(t)} + 4x_5^{(t)} + 1 \bmod 2^{64} \\
 x_5^{(t+1)} &= 2\{x_5^{(t)}\}^2 + \{4x_7^{(t)} + 3\}x_5^{(t)} + 4x_6^{(t)} + 1 \bmod 2^{64} \\
 x_6^{(t+1)} &= 2\{x_6^{(t)}\}^2 + \{4x_8^{(t)} + 3\}x_6^{(t)} + 4x_7^{(t)} + 1 \bmod 2^{64} \\
 x_7^{(t+1)} &= 2\{x_7^{(t)}\}^2 + \{4x_1^{(t)} + 3\}x_7^{(t)} + 4x_8^{(t)} + 1 \bmod 2^{64} \\
 x_8^{(t+1)} &= 2\{x_8^{(t)}\}^2 + \{4x_2^{(t)} + 3\}x_8^{(t)} + 4x_1^{(t)} + 1 \bmod 2^{64}
 \end{aligned}$$

/ 係数
付加多項式

他の変数

[0063] 例えば、変数  $x_1$  の更新式は、” mod  $2^{64}$ ” 以外の更新式本体  $G_1$  を有している。更新式本体  $G_1$  において、対象変数  $x_1$  のための一筆書き多項式に相当するのは、”  $2\{x_1^{(t)}\}^2 + \{4x_3^{(t)} + 3\}x_1^{(t)} + 1$ ” の部分であり、付加多項式に相当するのが、”  $4x_2^{(t)}$ ” の部分である。更新式本体  $G_1$



の付加多項式は、他の変数として  $x_2^{(t)}$  を有する。

[0064] 更新式本体  $G_1$  の一筆書き多項式においては、 $x_1^{(t)}$  の係数が、定数ではなく、他の変数  $x_3^{(t)}$  を含んでいる。したがって、一筆書き多項式の係数が時間的に変化し、更新式の時間発展が、第1例よりも複雑になる。他の変数  $x_2 \sim x_8$  の更新式についても同様である。

[0065] また、第2例は、第1例を包含しており、第1例と同様の有用性が得られる。さらに、第2例では、置換多項式（一筆書き多項式）の係数部分を他の変数によって変化させることができるため、係数部分が、時間的に値が変化しない定数を含んでいてもその値は小さくてよい。したがって、値が変化しない定数に大きなメモリを割り当てなくても良くなり、メモリ効率が向上する。

[0066] [3. 5 更新式の第2例の評価]

更新式の第2例の乱数性の評価を、上記の具体例として示した  $n$  個の更新式を用いて行った。

[0067] 評価の方法は、第1例の評価方法とほぼ同様である。第2例では、52セットについて評価した。また、第2例では、各変数が64ビットであり、各変数の上位32ビットを出力系列生成に用いた。

[0068] 第2例の場合、実行速度の最高値は、4936.824780Mbpsとなり、暗号化速度に換算すると、2.16cycle/Byteとなり、非常に高い速度が得られている。

[0069] 第2例の場合、NIST SP 800-22で定義される乱数検定の結果は、52セット中、40セットが、188項目すべてについて合格した。第2例においても良好な乱数性が確認された。

[0070] 本発明は、上記実施形態に限定されるものではなく、様々な変形が可能である。

## 符号の説明

[0071] 100 乱数発生装置

110 生成器

1 2 0 記憶部

1 3 0 演算部

## 請求の範囲

- [請求項1] 複数の変数を記憶する記憶部と、  
複数の前記変数それぞれを更新する複数の更新式の演算を実行し、  
複数の前記変数の更新値を前記記憶部へ出力する演算部と、  
複数の前記変数の少なくともいずれか一つの変数に基づいて、乱数を生成する生成器と、  
を備え、  
前記更新式は、  
前記更新式によって更新される対象変数の置換多項式と、複数の前記変数に含まれる前記対象変数以外の他の変数と、を含み、  
前記更新式によって前記対象変数を繰り返し更新したときの周期性が、一筆書き周期性である  
乱数発生装置。
- [請求項2] 前記更新式は、前記対象変数の前記置換多項式と、前記他の変数と、  
の和を含む  
請求項1記載の乱数発生装置。
- [請求項3] 前記対象変数の前記置換多項式は、前記対象変数に乘じられる係数部分であって、多項式で表される前記係数部分を含み、前記他の変数は、前記係数部分に含まれる  
請求項1又は2に記載の乱数発生装置。
- [請求項4] 前記置換多項式は、一筆書き多項式である  
請求項1～3のいずれか1項に記載の乱数発生装置。
- [請求項5] 演算部が、記憶部に記憶された複数の変数それぞれを更新する複数の更新式の演算を実行すること、  
前記演算部が、複数の前記変数の更新値を記憶部へ出力すること、  
生成器が、複数の前記変数の少なくともいずれか一つの変数に基づいて、乱数を生成すること、  
を含み、

前記更新式は、

前記更新式によって更新される対象変数の置換多項式と、複数の前記変数に含まれる前記対象変数以外の他の変数と、を含み、

前記更新式によって前記対象変数を繰り返し更新したときの周期性が、一筆書き周期性である

乱数発生方法。

[請求項6]

コンピュータを、

複数の変数を記憶する記憶部、

複数の前記変数それぞれを更新する複数の更新式の演算を実行し、複数の前記変数の更新値を前記記憶部へ出力する演算部、及び

複数の前記変数の少なくともいずれか一つの変数に基づいて、乱数を生成する生成器

として機能させるためのコンピュータプログラムであって、

前記更新式は、

前記更新式によって更新される対象変数の置換多項式と、複数の前記変数に含まれる前記対象変数以外の他の変数と、を含み、

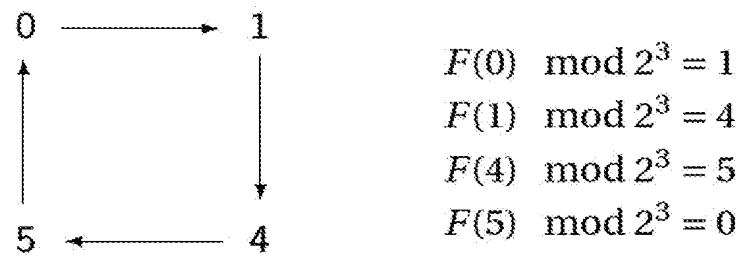
前記更新式によって前記対象変数を繰り返し更新したときの周期性が、一筆書き周期性である

コンピュータプログラム。

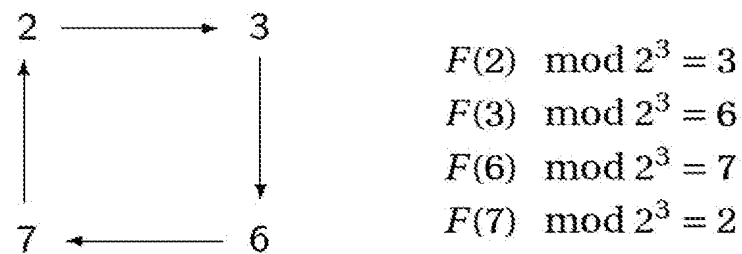
[図1]

(a)

$F_1(X) = 2X^2 + X + 1$  による  $\mathbb{Z}/2^3\mathbb{Z}$  上の軌道

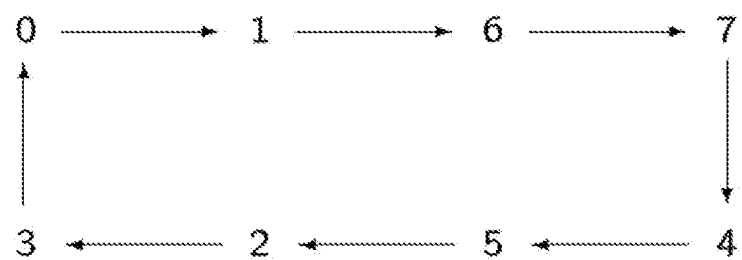


(b)

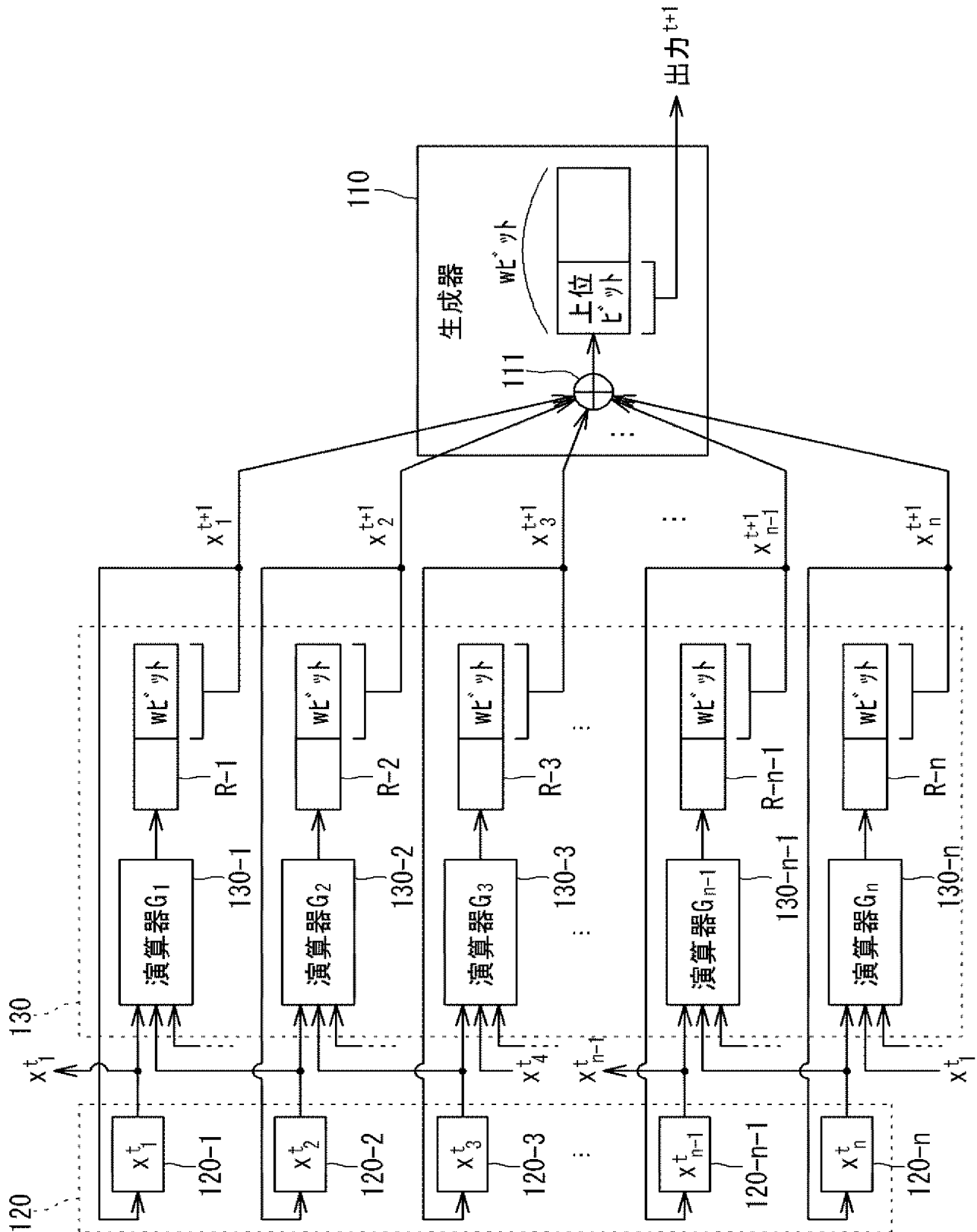


[図2]

$F_2(X) = 4X^2 + X + 1$  による  $\mathbb{Z}/2^3\mathbb{Z}$  上の軌道  $\Rightarrow$  一筆書き



[図3]



**INTERNATIONAL SEARCH REPORT**

International application No.  
PCT/JP2017/008294

A. CLASSIFICATION OF SUBJECT MATTER  
G06F7/58(2006.01)i, G09C1/00(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
G06F7/58, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2017  
Kokai Jitsuyo Shinan Koho 1971-2017 Toroku Jitsuyo Shinan Koho 1994-2017

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2005/073842 A1 (Victor Company of Japan, Ltd.), 11 August 2005 (11.08.2005), paragraphs [0014] to [0036] & US 2007/0174374 A1 paragraphs [0022] to [0043] & CN 1914590 A	1-6
A	JP 2002-99408 A (Hitachi Kokusai Electric Inc.), 05 April 2002 (05.04.2002), paragraphs [0018] to [0048] (Family: none)	1-6

Further documents are listed in the continuation of Box C.  See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search  
05 April 2017 (05.04.17)

Date of mailing of the international search report  
18 April 2017 (18.04.17)

Name and mailing address of the ISA/  
Japan Patent Office  
3-4-3, Kasumigaseki, Chiyoda-ku,  
Tokyo 100-8915, Japan

Authorized officer  
  
Telephone No.



**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP2017/008294

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2005-107910 A (National Institute of Information and Communications Technology), 21 April 2005 (21.04.2005), paragraphs [0004] to [0015] (Family: none)	1-6

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl. G06F7/58(2006.01)i, G09C1/00(2006.01)i

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl. G06F7/58, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2017年
日本国実用新案登録公報	1996-2017年
日本国登録実用新案公報	1994-2017年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	WO 2005/073842 A1 (日本ビクター株式会社) 2005.08.11, 段落 [0014]-[0036] & US 2007/0174374 A1, 段落[0022]-[0043] & CN 1914590 A	1-6
A	JP 2002-99408 A (株式会社日立国際電気) 2002.04.05, 段落 [0018]-[0048] (ファミリーなし)	1-6
A	JP 2005-107910 A (独立行政法人情報通信研究機構) 2005.04.21, 段 落[0004]-[0015] (ファミリーなし)	1-6

☞ C欄の続きにも文献が列挙されている。

☞ パテントファミリーに関する別紙を参照。

\* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
 「O」 口頭による開示、使用、展示等に言及する文献  
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献  
 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
 「&」 同一パテントファミリー文献

国際調査を完了した日

05.04.2017

国際調査報告の発送日

18.04.2017

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)  
 郵便番号100-8915  
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

田川 泰宏

電話番号 03-3581-1101 内線 3565

5U

4236