

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6788167号
(P6788167)

(45) 発行日 令和2年11月25日(2020.11.25)

(24) 登録日 令和2年11月4日(2020.11.4)

(51) Int. Cl.		F I			
G06F	7/58	(2006.01)	G06F	7/58	620
H04J	13/16	(2011.01)	H04J	13/16	

請求項の数 13 (全 30 頁)

(21) 出願番号	特願2016-207576 (P2016-207576)	(73) 特許権者	504160781
(22) 出願日	平成28年10月24日(2016.10.24)		国立大学法人金沢大学
(65) 公開番号	特開2018-72867 (P2018-72867A)		石川県金沢市角間町ヌ7番地
(43) 公開日	平成30年5月10日(2018.5.10)	(74) 代理人	100141519
審査請求日	令和1年9月24日(2019.9.24)		弁理士 梶田 邦之
		(74) 代理人	100172199
			弁理士 松山 浩也
		(74) 代理人	100201374
			弁理士 福澤 昌俊
		(72) 発明者	藤崎 礼志
			石川県金沢市角間町ヌ7番地 国立大学法人金沢大学内
		審査官	征矢 崇

最終頁に続く

(54) 【発明の名称】 系列生成装置、符号化処理装置、送信装置

(57) 【特許請求の範囲】

【請求項1】

自己相関特性に基づいて設定された区分単調増加マルコフ変換の傾きに応じて、第1系列を生成する生成部と、

均等分布と前記区分単調増加マルコフ変換の傾きとに基づいて設定された変換条件に基づいて、前記第1系列を第2系列に変換する変換部と、
を備える系列生成装置。

【請求項2】

前記自己相関特性は、下記式の である、請求項1記載の系列生成装置。

【数1】

$$\mathbb{E}[Z_0 Z_\ell] = \rho^\ell, \quad \ell \geq 0$$

ここで、Zは、前記第1系列の確率変数である。

【請求項3】

前記変換部は、下記式により、前記第1系列を前記第2系列に変換する、請求項1又は2記載の系列生成装置。

【数 2】

$$Y = \Phi(X) \Phi(SX) \Phi(S^2 X) \cdots \Phi(S^{L-1} X)$$

ここで、 X は前記第 1 系列であり、 Φ は前記変換条件を表すブロック符号であり、 Y は前記第 2 系列であり、 S は、 L ブロック全体の集合 $\{0, 1, 2\}^L$ 上のシフト変換であって、 $v = v_1 v_2 \cdots v_L \in \{0, 1, 2\}^L$ に対して下記式で表される。

【数 3】

$$S(v_1, v_2, \cdots, v_{L-1}, v_L) = (v_2, v_3, \cdots, v_L, v_1) \quad 10$$

【請求項 4】

前記変換条件を表すブロック符号は、下記式で定義される、請求項 3 記載の系列生成装置。

【数 4】

i) $\frac{1}{2} + \frac{\bar{\beta}}{\beta - \bar{\beta}} \leq \frac{c_2}{\beta - \bar{\beta}} \left(\frac{1}{\beta} + \frac{1}{\beta^2} \right)$ のとき

$$\Phi(v) = \begin{cases} 1, & v \leq d_\beta(\xi) \text{ のとき,} \\ -1, & d_\beta(\xi) < v \leq c_1 \text{ のとき,} \\ 1, & c_1 < v \text{ のとき.} \end{cases} \quad 20$$

ここで $\xi = \frac{\beta - \bar{\beta}}{2 \left(\frac{1}{\beta} + \frac{1}{\beta^2} \right)}$.

【数 5】

ii) $\frac{1}{2} + \frac{\bar{\beta}}{\beta - \bar{\beta}} > \frac{c_2}{\beta - \bar{\beta}} \left(\frac{1}{\beta} + \frac{1}{\beta^2} \right)$ のとき

$$\Phi(v) = \begin{cases} 1, & v \leq c_2 + d_\beta(\eta) \text{ のとき,} \\ -1, & c_2 + d_\beta(\eta) < v \leq c_1 \text{ のとき,} \\ 1, & c_1 < v \text{ のとき.} \end{cases} \quad 30$$

ここで $\eta = \frac{1}{2} + \bar{\beta} - c_2 \left(\frac{1}{\beta} + \frac{1}{\beta^2} \right)$.

【請求項 5】

前記変換条件を表すブロック符号は、下記式で定義される、請求項 3 又は 4 記載の系列生成装置。

【数 6】

$$\Phi(v) = \begin{cases} 1, & v \leq 02 \text{ のとき,} \\ -1, & 02 < v \leq 2 \text{ のとき,} \\ 1, & 2 < v \text{ のとき} \end{cases}$$

【請求項 6】

前記第 2 系列は、拡散符号である、請求項 1 乃至 5 のうちいずれか 1 項記載の系列生成

40

50

装置。

【請求項 7】

前記第 2 系列は、暗号化又は復号のための系列である、請求項 1 乃至 5 のうちいずれか 1 項記載の系列生成装置。

【請求項 8】

第 1 系列から変換された第 2 系列を、記憶する記憶部と、
前記第 2 系列に基づいて、信号列の符号化を行う符号化部と、
を備え、

前記第 1 系列は、自己相関特性に基づいて設定された区分単調増加マルコフ変換の傾きに応じて生成された系列であり、

前記第 2 系列は、前記第 1 系列を、均等分布と前記区分単調増加マルコフ変換の傾きとに基づき変換条件に基づいて変換した系列である、
符号化処理装置。

10

【請求項 9】

前記第 2 系列は、前記第 1 系列から変換された拡散符号であり、
前記符号化は、前記信号列の拡散である、
請求項 8 記載の符号化処理装置。

【請求項 10】

前記符号化は、前記信号列の暗号化である、請求項 8 記載の符号化処理装置。

【請求項 11】

第 1 系列から変換された第 2 系列に基づいて、信号列の符号化を行う符号化部と、
前記符号化後の前記信号列を、他の装置に送信する送信部と、
を備え、

前記第 1 系列は、自己相関特性に基づいて設定された区分単調増加マルコフ変換の傾きに応じて生成された系列であり、

前記第 2 系列は、前記第 1 系列を、均等分布と前記区分単調増加マルコフ変換の傾きとに基づき変換条件に基づいて変換した系列である、
送信装置。

20

【請求項 12】

前記第 2 系列は、前記第 1 系列から変換された拡散符号であり、
前記符号化は、前記信号列の拡散である、
請求項 11 記載の送信装置。

30

【請求項 13】

前記符号化は、前記信号列の暗号化である、請求項 11 記載の送信装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、系列生成装置、符号化処理装置、送信装置に関する。

【背景技術】

40

【0002】

擬似乱数が使用される分野は、情報通信系、暗号系、計算機科学、経済学(数理ファイナンス)、地球科学(地球シミュレーション)、気象学、ゲノム・サイエンスと枚挙に暇がない。また、学術分野のみならず、高機能携帯端末(スマートフォン)、通信、金融と情報技術(IT)を融合させたフィンテック(電子決済、クラウド会計)、多元センサーのランダム制御(自動給水装置及び自動給水システム)を証左として、「擬似乱数は我々の社会生活に必要な不可欠なインフラ技術の一つである」と言っても過言ではない。

【0003】

例えば、特許文献 1 には、区分単調増加マルコフ変換を用いて最大周期列を生成するアルゴリズムが開示されている。

50

【先行技術文献】

【特許文献】

【0004】

【特許文献1】特開2011-227632号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

上述した特許文献1に開示されたアルゴリズムを用いることで、効率的に系列を生成することができるが、様々な分野において、相関特性および均等分布性を有する系列を生成することが望まれる。

10

【0006】

例えば、暗号、計算機科学などの分野では、時間 t に関して $t=0$ で1、それ以外で0を取るようなデルタ関数的な規格化自己相関関数が要求される。また、情報通信、数理ファイナンスなどの分野では、短期に指数関数的に減少する自己相関特性、及び長周期に振動する自己相関特性を有する系列が必要とされる。すなわち、自己相関特性と均等分布を有し、しかも互いに無相関な系列（擬似乱数）が大量に必要なことになる。

【0007】

そこで、本発明の目的は、任意に指定された自己相関特性と均等分布を有する互いに無相関な系列を大量生成可能な系列生成装置、当該系列を用いる符号化処理装置、送信装置を提供することにある。

20

【課題を解決するための手段】

【0008】

本発明のある態様は、系列生成装置に関する。この系列生成装置は、所定の相関特性に基づいて設定された区分単調増加マルコフ変換の傾きに応じて、第1系列を生成する生成部と、所定の分布と区分単調増加マルコフ変換の傾きとに基づいて設定された変換条件に基づいて、第1系列を第2系列に変換する変換部と、を備える。

【0009】

このような態様によると、所定の相関特性に基づいて設定された区分単調増加マルコフ変換の傾きに応じて生成された第1系列を、所定の分布と区分単調増加マルコフ変換の傾きとに基づいて設定された変換条件に基づいて変換することにより、任意に指定された自己相関特性と均等分布を有する互いに無相関な系列を大量に生成することができる。

30

【0010】

本発明の別の態様は、符号化処理装置である。この符号化処理装置は、第1系列から変換された第2系列を、記憶する記憶部と、第2系列に基づいて、信号列を符号化する符号化部と、を備え、第1系列は、所定の相関特性に基づいて設定された区分単調増加マルコフ変換の傾きに応じて生成されたものであり、第2系列は、第1系列を、所定の分布と区分単調増加マルコフ変換の傾きとに基づく変換条件に基づいて変換したものである。

【0011】

本発明の別の態様は、送信装置である。この送信装置は、第1系列から変換された第2系列を、記憶する記憶部と、第2系列に基づいて、信号列を符号化する符号化部と、符号化された信号列を、他の装置に送信する送信部と、を備え、第1系列は、所定の相関特性に基づいて設定された区分単調増加マルコフ変換の傾きに応じて生成されたものであり、第2系列は、第1系列を、所定の分布と区分単調増加マルコフ変換の傾きとに基づく変換条件に基づいて変換したものである。

40

【0012】

なお、以上の構成要素の任意の組み合わせ、本発明の表現を方法、装置、システム、コンピュータプログラムなどの間で変換したのもまた、本発明の態様として捉えることができる。

【発明の効果】

【0013】

50

本発明によれば、任意に指定された自己相関特性と均等分布を有する互いに無相関な系列を大量に生成することが可能である。

【図面の簡単な説明】

【0014】

【図1】図1は、傾き $= 1 + 3$ を有するマルコフ変換Tのグラフを示す図である。

【図2】図2は、 $X\{22\}$ のグラフ表現Gを示す図である。

【図3】図3は、系列長56のときの、ビット誤り生起確率のユーザ数依存性を示す図である。

【図4】図4は、系列長32のときの、ビット誤り生起確率のユーザ数依存性を示す図である。

【図5】図5は、実施例1にかかる系列生成装置100を示す図である。

【図6】図6は、実施例2にかかる符号化装置200を示す図である。

【図7】図7は、実施例3にかかる送信装置300を示す図である。

【図8】図8は、実施例4にかかる受信装置400を示す図である。

【発明を実施するための形態】

【0015】

以下においては、まず本発明が適用される理論を説明した上で、実施例を用いて説明していくものとする。つまり説明は、以下の順序で行われる。

1. 理論

1.1. 緒言

1.2. 有限タイプのシフト

1.3. 超離散力学系に基づく最大周期列

1.4. 変換に基づく指定された相関特性を有するマルコフ連鎖の実現

1.5. 離散化変換に基づく所望の相関特性と均等分布を有するマルコフ連鎖の実現

1.6. 実験結果

1.7. 一般の場合について

2. 実施例

2.1. 実施例1

2.2. 実施例2

2.3. 実施例3

2.4. 実施例4

3. その他

【0016】

< 1. 理論 >

< 1.1. 緒言 >

擬似乱数が使用される分野は、情報通信系、暗号系、計算機科学、経済学(数理ファイナンス)、地球科学(地球シミュレーション)、気象学、ゲノム・サイエンスと枚挙に暇がない。また、学術分野のみならず、高機能携帯端末(スマートフォン)、通信、金融と情報技術(IT)を融合させたフィンテック(電子決済、クラウド会計)、多元センサーのランダム制御(自動給水装置及び自動給水システム)を証左として、「擬似乱数は我々の社会生活に必要不可欠なインフラ技術の一つである」と言っても過言ではない。

【0017】

要求される性能は、次ビット予測可能性、高次均等分布性、相関特性と、使用する目的に応じて種々挙げられる。本理論では、広い分野に要求される相関特性および均等分布性に注目する。暗号、計算機科学などでは時間tに関してt=0で1、それ以外で0を取るようなデルタ関数的な規格化自己相関関数が要求される。一方、情報通信、数理ファイナンスなどでは、短期に指数関数的に減少する自己相関特性や長周期に振動する自己相関特性が必要とされる。さらに、暗号だけでなく通信システムにおいても均等分布を有するビット列が用いられる。その様な自己相関特性と均等分布を有し、しかも互いに無相関な擬

10

20

30

40

50

似乱数が大量に必要である。斯様な要求に答えること、すなわち、任意に指定された自己相関特性と均等分布を有する互いに無相関な擬似乱数を大量に実現することが本理論の目的である。実用の一例として、スペクトル拡散多元接続 (SSMA) 通信システムを考え、実際の携帯通信システムに使用可能な最適スペクトル拡散符号を取り上げる。

【0018】

< 1.2. 有限タイプのシフト >

集合 Σ は有限アルファベットであるとする。全シフトは、

【数1】

$$\Sigma^{\mathbb{Z}} = \{x = (x_i)_{i \in \mathbb{Z}} : \forall i \in \mathbb{Z}, x_i \in \Sigma\} \quad 10$$

で表される。これには、 Σ 上の離散位相から生ずる直積位相が付与される。

【0019】

シフト変換 σ :

【数2】

$$\Sigma^{\mathbb{Z}} \rightarrow \Sigma^{\mathbb{Z}}$$

20

は、

【数3】

$$\sigma((x_i)_{i \in \mathbb{Z}}) = (x_{i+1})_{i \in \mathbb{Z}}$$

で定義される。全

【数4】

$$\Sigma^{\mathbb{Z}}$$

30

シフトの閉シフト不変部分集合はサブシフトと呼ばれる。サブシフト X に対して、 X 上のシフト変換を σ_X で表す。これは、 $\Sigma^{\mathbb{Z}}$ 上の σ の、 X への制限である。簡単のため、 σ_X よりむしろ $\sigma : X \rightarrow X$ と書くことにする。

【0020】

元 $u = u_1 u_2 \dots u_n \in \Sigma^n$ を長さ n ($n \geq 1$) の Σ 上のブロックと呼ぶ、これを単に n ブロックとも言う。空ブロックを表すのに ϵ を用いる。サブシフト X に対して、 $\mathcal{L}_n(X)$ ($n \geq 0$) は X に属する点に現れる n ブロック全体の集合を表す。このとき、 X の言語は集合

40

【数5】

$$\mathcal{L}(X) = \bigcup_{n=0}^{\infty} \mathcal{L}_n(X)$$

である。

ここで、 $\mathcal{L}_0(X) = \{\epsilon\}$ である。

【0021】

50

(有向) グラフ $G = (V, A)$ は頂点の有限集合 V と辺の有限集合 A から成る。各辺 $e \in A$ は、初期状態と呼ばれ、 $i(e) \in V$ で表される頂点を出発し、終状態と呼ばれ、 $t(e) \in V$ で表される頂点に到達する。

【0022】

(定義1)

$G = (V, A)$ はグラフであるとする。頂点 $u, v \in V$ に対して、 $a_{u,v}$ は、初期状態 u と終状態 v を有する G の辺の数を表すとする。このとき、 G の隣接行列は $A = (a_{u,v})_{u,v \in V}$ で定義される。隣接行列 A が G から構成されるのを $A = A(G)$ または $A = A_G$ で表す。逆に、 $k \times k$ 非負整数行列

【数6】

10

$$B = (b_{i,j})_{i,j=0}^{k-1}$$

は、頂点集合 $\{0, 1, \dots, k-1\}$ と、初期状態 i から終状態 j への $b_{i,j}$ 個の相異なる辺を有するグラフ H を決定する。グラフ H が B から構成されるのを $H = G(B)$ または $H = G_B$ で表す。 $A = A(G_A)$ となること、および G と $H = G(A_G)$ がグラフ同型であることは注目に値する。

20

【0023】

与えられた非負整数行列 A に対して、 $G_A = (V, A)$ と置く。

【数7】

$$X_A = \{(x_n)_{-\infty}^{\infty} \in \mathcal{A}^{\mathbb{Z}} : \mathbf{t}(x_n) = \mathbf{i}(x_{n+1}) \text{ for all } n \in \mathbb{Z}\}$$

とする。このとき、 X_A は、行列 A によって決定される両側位相的マルコフ連鎖と呼ばれる。位相的マルコフ連鎖はまた有限タイプのシフト (SFT) とも呼ばれる。SFT とは禁止語の有限集合によって表現することができるようなサブシフトである。与えられた禁止語の有限集合 F に対して、SFT を表すのに X_F を用いる。

【0024】

30

< 1.3. 超離散力学系に基づく最大周期列 >

集合 E の濃度 (有限の場合には要素数) を表すのに $|E|$ を用いる。

【0025】

(定義2)

$T : [0, 1) \rightarrow [0, 1)$ とする。 P は点 $0 = a_0 < a_1 < \dots < a_{|P|} = 1$ で与えられる区間 $[0, 1)$ の分割であるとする。 $i = 1, \dots, |P|$ に対して、 $I_i = (a_{i-1}, a_i)$ とし、 T の I_i への制限を $T|_{I_i}$ で表す。 $T|_{I_i}$ が、 I_i から、 P の区間の閉包のある連結和集合の内部の上への同相写像であるとき、 T はマルコフであると言われる。このとき、分割

【数8】

40

$$\mathcal{P} = \{I_i\}_{i=1}^{|\mathcal{P}|}$$

は、 T に関するマルコフ分割と呼ばれる。

【0026】

既約かつ非周期的マルコフ変換 T に対して、 T に関するマルコフ分割 P が定まる。このとき、各部分区間 $I \in P$ を一つの辺 $e(I)$ に対応させると、辺集合 A を得る。 A に同伴して、頂点集合 V が

50

【数 9】

$$\mathcal{V} = \{ \mathbf{i}(e), \mathbf{t}(e) : e \in \mathcal{A} \}$$

で与えられる。P の元の各順序対 (I , J) に対して、 $\mathbf{t}(e(I)) = \mathbf{i}(e(J))$ が成り立つのは、丁度 $J = T|_I(I)$ のときである。斯くして、マルコフ変換を表現するグラフ $G = (V, A)$ を得る。一般に、得られたグラフはオイラーグラフではない。

【0027】

10

$H = (V, B)$ は、最大辺数を有する G の全域オイラー部分グラフであるとする。既約かつ非周期的マルコフ変換を考えているので、頂点集合 V は G から H への変形に対して不変である。上で述べた、P と A の間の一対一対応の下で、B に対応する部分分割 Q を得る。このとき、離散化マルコフ変換

【数 10】

$$\hat{T}$$

は、全ての $I \in Q$ に対して、

20

【数 11】

$$\hat{T}(I) \subset T|_I(I)$$

を満たす置換

【数 12】

$$\hat{T} : Q \rightarrow Q$$

30

によって定義される。

【0028】

離散化マルコフ変換に基づく最大周期列は、丁度 H 上のオイラー回路であり、その長さは $|B|$ で与えられる。T に関するマルコフ分割 P が与えられるとき、 $|Q|!$ 個の離散化マルコフ変換を得る。任意の置換は互いに素な巡回置換の積で (順序を除いて) 一意に表されることは良く知られている。この事実に鑑み、離散化マルコフ変換

【数 13】

40

$$\hat{T} : Q \rightarrow Q$$

が基本変換 $T : [0, 1) \rightarrow [0, 1)$ を近似すると見做されるのは、丁度一つの巡回置換として表現されるときに限る。

この場合、離散化マルコフ変換

【数 1 4】

$$\hat{T}$$

それ自身は最大周期列 w として見る事ができる。さらに、最大周期列 w に対して、両側無限列 $w = \dots w w w \dots$ を考えれば、巡回置換

【数 1 5】

$$\hat{T}$$

10

は

【数 1 6】

$$B^{\mathbb{Z}}$$

上のシフトと見做すことができる。

【0 0 29】

20

離散化マルコフ変換に基づく最大周期列は

【数 1 7】

$$\mathcal{L}_{|\mathcal{B}|}(X_{A_H})$$

に属するブロックに他ならないことが観察される。これは離散化マルコフ変換

【数 1 8】

30

$$\hat{T} : \mathcal{Q} \rightarrow \mathcal{Q}$$

が単に基本変換 $T : [0, 1) \rightarrow [0, 1)$ の近似の一段階に過ぎないことを示唆する。より精密な近似を定義するために、記号力学系から高次辺グラフという概念を導入する [参考文献 1]。

【0 0 30】

(定義 3)

G はグラフであるとする。 $n \geq 2$ に対して、 G の n 次高次辺グラフ $G^{[n]}$ は頂点集合

40

【数 1 9】

$$\mathcal{L}_{n-1}(X_{A_G})$$

を持ち、また、 $e_2 e_3 \dots e_{n-1} = f_1 f_2 \dots f_{n-2}$ のとき (但し $n = 2$ の場合は $t(e_1) = i(f_1)$ のとき) には常に $e_1 e_2 \dots e_{n-1}$ から $f_1 f_2 \dots f_{n-1}$ へ丁度一つの辺を含むが、それ以外の際には何も無いような、辺集合を持つと定義される。辺は $e_1 e_2 e_3 \dots e_{n-1} f_{n-1} = e_1 f_1 f_2 \dots f_{n-1}$ と名付けられる。 $n = 1$

50

に対して、 $G^{[1]} = G$ と置く。

【0031】

グラフ G はマルコフ変換を表すとする。このとき、 G の高次辺グラフの列

【数20】

$$\left(G^{[n]} \right)_{n=1}^{\infty}$$

を得る。各 $n \geq 1$ に対して、

【数21】

$$H_n = \left(\mathcal{L}_{n-1} \left(X_{A_G} \right), \mathcal{B}_n \right)$$

は最大辺数を有する $G^{[n]}$ の全域オイラー部分グラフを表すとする。各々は、離散化マルコフ変換

【数22】

$$\hat{T}_n$$

を導く。最大周期列の長さは $| \mathcal{B}_n |$ で与えられることに注意しておく。

【0032】

ここまで、離散化される変換として、一般の既約かつ非周期的マルコフ変換 T を考えてきた。以下、離散化される変換 T に対して、次の単調性を要求する。 $[0, 1]$ のある分割 $0 = x_0 < x_1 < \dots < x_k = 1$ が存在して、各整数 $i = 1, \dots, k$ に対して、 T の区間 $[x_{i-1}, x_i)$ への制限は単調増加関数である。

【0033】

既約かつ非周期的マルコフ変換 T がこの条件を満たすとき、 T を区分的単調増加(PMI)マルコフ変換と呼ぶ。以下、離散化される変換は、その様な単調性を有するとしよう。ここで、区分的単調増加マルコフ変換は実用的に十分広いクラスのマルコフ変換を含むことを強調しておく。実際、PMIマルコフ変換は、本理論で考える黄金平均変換や変換だけでなく、Bernoulli変換、Kalmanのマルコフ変換[参考文献2]、および[参考文献3]で定義された $k(\geq 2)$ 方有尾シフト変換を含む。

【0034】

PMIマルコフ変換に対しては、離散化された変換に基づく最大周期列を全て生成するような、有界単調真理値表アルゴリズムを与えた[参考文献4]。

【0035】

< 1.4. 変換に基づく指定された相関特性を有するマルコフ連鎖の実現 >

非同期スペクトル拡散多元接続(SSMA)通信システムにおけるビット誤り生起確率に関して、最適 $M(\geq 2)$ 相マルコフ連鎖拡散符号が設計された[参考文献5]。最適拡散符号を生成するマルコフ連鎖は、その確率行列の第二固有値が $-2 + \sqrt{3}$ を有することで M に無関係に特徴付けられる。簡単のため、以下 $M = 2$ の場合に制限するが、[参考文献5]の結果を用いることにより、 $M \geq 3$ の場合も同様に得られる。

【0036】

$M = 2$ の場合、最適二値マルコフ連鎖拡散符号系列は

10

20

30

40

【数 2 3】

$$\mathbb{E}[Z_n] = 0 \quad \text{and} \quad \mathbb{E}[Z_0 Z_\ell] = \left(-2 + \sqrt{3}\right)^\ell, \quad \ell \geq 0$$

を有する $\{1, -1\}$ に値を取る定常マルコフ連鎖系列

【数 2 4】

$$\left(Z_n\right)_{n=0}^{\infty}$$

10

として特徴付けられる。ここで、確率変数 Z に対して、

【数 2 5】

$$\mathbb{E}[Z]$$

は Z の期待値を表す。

【0 0 3 7】

系列に対する相関関数は、二つの系列の間の類似性または関係性の測度であり、数学的に次の様に定義される。

20

(定義 4)

$\{-1, 1\}$ 上の系列

【数 2 6】

$$\mathbf{X} = \left(X_i\right)_{i=0}^{N-1}$$

30

と

【数 2 7】

$$\mathbf{Y} = \left(Y_i\right)_{i=0}^{N-1}$$

に対する、遅れ時間

【数 2 8】

ℓ

40

の正規化相互相関関数は

【数 2 9】

$$r_N(\ell; \mathbf{X}, \mathbf{Y}) = \frac{1}{N} \sum_{i=0}^{N-1} X_i Y_{i+\ell} \pmod{N}$$

で定義される。ここで、

【数 3 0】

10

$$\ell = 0, 1, \dots, N - 1$$

である。整数 a と b ($b > 0$) に対して、 $a \pmod{b}$ は法 b に関する a の最小剰余を表す。 $X = Y$ のとき

【数 3 1】

$$r_N(\ell; \mathbf{X}, \mathbf{X})$$

20

を正規化自己相関関数と呼び、単に

【数 3 2】

$$r_N(\ell; \mathbf{X})$$

30

で表す。

所望の

【数 3 3】

$$r_N(\ell; \mathbf{X}) = (-2 + \sqrt{3})^\ell$$

を有する系列 X を構成するために [参考文献 6] で定義された Perron 数を導入する。

【0 0 3 8】

40

(定義 5)

数 μ が Perron 数であるのは、次を満たすときである。 $i)$ μ は正の代数的整数である。および $ii)$ μ 以外の全ての代数的共役 μ' に対して、 $|\mu| > |\mu'|$ が成り立つ。Perron 数全体の集合を

【数 3 4】

$$\mathbb{P}$$

で表す。

【0 0 3 9】

50

行列 A は非負整数行列であるとする。ある整数 n に対して、 $A^n > 0$ ならば、 A は原始的であると言われる。ここで、行列 B に対して、 $B > 0$ は B が正行列であることを表す。 A が原始的であるのは、 A が既約かつ非周期的であることと同等である。原始的行列 A に対して、 A の Perron - Frobenius 固有値を λ_A で表す。斯くして、Perron 数は次の定理により特徴付けられる。

【0040】

定理 1 (Lind [参考文献 6])

【数 35】

$$\lambda \in \mathbb{P}$$

10

はある原始的 A に対して $\lambda = \lambda_A$ のときまたそのときに限る。

所望の相関関数はパラメータを一個 (すなわち $-2 + 3$) しか持たないので、次数 2 を有する

【数 36】

$$\lambda \in \mathbb{P}$$

20

を考えれば十分である。一般に、パラメータ数 m に対して、次数 $m + 1$ を考えればよい。次数 2 を有する Q の、 Q 上最小多項式は

【数 37】

$$f(t) = t^2 - c_1 t - c_2$$

で定義される。ここで、

【数 38】

30

$$c_1, c_2 \in \mathbb{Z}$$

である。多項式 $f(t)$ のコンパニオン行列は、

【数 39】

$$B = \begin{pmatrix} 0 & c_2 \\ 1 & c_1 \end{pmatrix}$$

40

で与えられる。コンパニオン行列 B の特性多項式と最小多項式は $f(t)$ に等しいことに注意する。

50

【0041】

変換は、次のように定義される。すなわち、 $\beta > 1$ に対して、変換 $T : [0, 1] \rightarrow [0, 1]$ は $T(x) = \frac{x}{\beta} \pmod{1}$, $x \in [0, 1]$ で定義される。ここで $x = y \pmod{1}$ は 1 を法とする実数上の合同、すなわち、 $x - y$ が整数であることを表す。さらに、変換が (定義 2) を満たすとき、マルコフ変換と呼ばれる。

【0042】

マルコフ変換に行列 B を同伴するために、 $0 < c_2 \leq c_1$ とする。このとき、コンパニオン行列 B に同伴するマルコフ変換の $(c_1 + 1) \times (c_1 + 1)$ 隣接行列 A は

【数40】

$$A = \left(\begin{array}{ccc|ccc} & \overbrace{\hspace{10em}}^{c_1+1} & & & & \\ \hline 1 & \cdots & 1 & 1 & \cdots & 1 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 1 & \cdots & 1 & 1 & \cdots & 1 \\ \hline 1 & \cdots & 1 & 0 & \cdots & 0 \\ \underbrace{\hspace{10em}}_{c_2} & & & & & \end{array} \right) \Bigg\} c_1$$

10

20

で与えられる。

【0043】

実数値を二値に符号化する写像 $\Psi : [0, 1) \rightarrow \{1, -1\}$ を

【数41】

$$\Psi(x) = \begin{cases} 1 & x < \frac{c_1}{\beta} \text{ のとき,} \\ -1 & \text{それ以外,} \end{cases}$$

30

で定義する。 $n = 0, 1, 2, \dots$ に対して、変換 T の n 回反復 $T^n(x)$ は、 $T^0(x) = x$ 及び $T^n(x) = T^{n-1}(T(x))$ により帰納的に定義される。このとき、 $Z_n = (T^n(x))$ と置くことにより、区間 $[0, 1)$ に属するほとんど全ての x に対して、 $\{1, -1\}$ に値を取るマルコフ連鎖系列

【数42】

$$(Z_n)_{n=0}^{\infty}$$

40

が生成される。斯くして、

【数 4 3】

$$\mathbb{E}[Z_0 Z_\ell] = \left(\frac{\lambda + \bar{\lambda}}{\lambda - \bar{\lambda}} \right)^2 - \frac{4\lambda\bar{\lambda}}{(\lambda - \bar{\lambda})^2} \left(\frac{\bar{\lambda}}{\lambda} \right)^\ell, \quad \ell \geq 0$$

を得る。ここで、

【数 4 4】

$$\bar{\lambda}$$

10

は の代数的共役である。

【0 0 4 4】

条件 $0 < c_2 < c_1$ の下、方程式

【数 4 5】

$$-2 + \sqrt{3} = \frac{\lambda}{\bar{\lambda}} = \frac{c_1 - \sqrt{c_1^2 + 4c_2}}{c_1 + \sqrt{c_1^2 + 4c_2}} \tag{1}$$

20

の整数解 (c_1, c_2) は $c_1 = c_2 = 2$ として一意に与えられる。

【0 0 4 5】

結局、傾き $= 1 + \sqrt{3}$ を有するマルコフ変換 T を得る。 $x = 1 + \sqrt{3} = t^2 - 2t - 2 = 0$ の正の解である。図 1 に T のグラフを示す。

【0 0 4 6】

相関特性

【数 4 6】

$$\mathbb{E}[Z_0 Z_\ell] = \left(-2 + \sqrt{3} \right)^\ell \quad (\ell \geq 0)$$

30

を有するような、 $\{1, -1\}$ に値を取るマルコフ連鎖系列

【数 4 7】

$$\left(Z_n \right)_{n=0}^\infty$$

40

をうまく得た。しかしながら、連鎖の定常分布は

【数 4 8】

$$(p_1, p_2) = \frac{1}{(\lambda - \bar{\lambda})} (-\bar{\lambda}, \lambda) = \frac{1}{2\sqrt{3}} (-1 + \sqrt{3}, 1 + \sqrt{3})$$

で与えられ、一様分布でないため、

【数49】

$$\mathbb{E}[Z_n] = \frac{\lambda + \bar{\lambda}}{\lambda - \bar{\lambda}} = \frac{1}{\sqrt{3}} \neq 0$$

となり、所望の零でない。

【0047】

10

次に、得られた最適二値マルコフ連鎖拡散符号の相関特性を変更すること無く、スライディング・ブロック符号を用いて、系列の分布 (p_1, p_2) を一様分布に変換する。

【0048】

< 1.5. 離散化 変換に基づく所望の相関特性と均等分布を有するマルコフ連鎖の実現 >

基数 $= 1 + \sqrt{3}$ を用いるとき、区間 $[0, 1)$ に属する実数 x の 進展開は SFT

【数50】

$$X_{\mathcal{F}} \subset \Sigma^{\mathbb{Z}}$$

20

の右側無限列として与えられる。ここで $\Sigma = \{0, 1, 2\}$ 及び $\mathcal{F} = \{2, 2\}$ である。実数 $x \in [0, 1)$ の 進展開から得られる右側無限列は、図1に示した 変換 T の、初期値を x とする。実数値解軌道の記号力学的表現である。SFT $X_{\mathcal{F}}$ のグラフ表現 G は、図2に示すように与えられる。同時に、 G は T の表現でもある。

【0049】

初期グラフを $G = G^{[2]}$ として、 G の高次辺グラフの列

【数51】

$$(G^{[n]})_{n=2}^{\infty}$$

30

を得る。各 $n \geq 2$ に対して、 H_n は最大辺数を有する $G^{[n]}$ の全域オイラー部分グラフを表すとする。各オイラー部分グラフ H_n のオイラー回路が、傾き $= 1 + \sqrt{3}$ を有する 変換 T の超離散化に基づく最大周期列である。図2において、 G はオイラーグラフであることがわかる。この場合、 $G = G^{[2]} = H_2$ を得る。しかしながら、 $n \geq 3$ に対して、 $G^{[n]}$ はオイラーグラフであるとは限らない。実際、 H_3 は $G^{[3]}$ の真部分グラフである。

40

これを

【数52】

$$H_3 \subsetneq G^{[3]}$$

で表す。任意の $n \geq 3$ に対して、

【数 5 3】

$$H_n \subsetneq G^{[n]}$$

となるのが確認される。

【0 0 5 0】

図 2 のオイラー部分グラフ H_2 において、例えば、最大周期列 0 0 1 0 2 1 1 2 0 を得る。 10

最大周期列の長さ $|B_n|$ は

【数 5 4】

$$|B_n| = \beta^n + \overline{\beta}^n \quad (n \geq 2)$$

で与えられる [参考文献 7]。ここで、

【数 5 5】

20

$$\overline{\beta} = 1 - \sqrt{3}$$

は の代数的共役である。

【0 0 5 1】

以下、傾き $= 1 + \sqrt{3}$ を有する 変換の超離散化に基づき、最適二値マルコフ連鎖拡散符号を構成する。集合 $L(X_F) \setminus \{ \}$ 上の全順序関係 を次で定義する。すなわち、 $L(X_F)$ に属する任意の $u = u_1 \dots u_m$ ($m \geq 1$) と $v = v_1 \dots v_n$ ($n \geq 1$) に対して、 $u \leq v$ は 30

【数 5 6】

$$\frac{u_1}{\beta} + \frac{u_2}{\beta^2} + \dots + \frac{u_m}{\beta^m} \leq \frac{v_1}{\beta} + \frac{v_2}{\beta^2} + \dots + \frac{v_n}{\beta^n}$$

のときまたそのときに限る。

簡単のため、最大周期列の長さ $|B_n|$ を表すのに L を用いる。 L ブロック $v = v_1 v_2 \dots v_L \in \{0, 1, 2\}^L$ に対して、ブロック符号 $\Phi(v) = \{0, 1, 2\}^L \setminus \{1, -1\}$ を 40

【数 5 7】

$$\Phi(v) = \begin{cases} 1, & v \leq 02 \text{ のとき,} \\ -1, & 02 < v \leq 2 \text{ のとき,} \\ 1, & 2 < v \text{ のとき} \end{cases}$$

で定義する。

50

【 0 0 5 2 】

L ブロック全体の集合 $\{0, 1, 2\}^L$ 上のシフト変換を S で表す。すなわち、 $v = v_1 v_2 \dots v_L \in \{0, 1, 2\}^L$ に対して、

【数 5 8】

$$S(v_1, v_2, \dots, v_{L-1}, v_L) = (v_2, v_3, \dots, v_L, v_1)$$

と表す。斯くして、周期 L の周期列に対して、

【数 5 9】

$$\phi(v^\infty) = (\Phi(v) \Phi(Sv) \Phi(S^2v) \dots \Phi(S^{L-1}v))^\infty$$

10

で定義されるスライディング・ブロック符号 ϕ を得る。ここで、ブロック u に対して、 $u = \dots u u u \dots$ である。

【 0 0 5 3 】

系列 X は、 $\beta = 1 + \sqrt{3}$ を有する離散化マルコフ変換に基づく、長さ $L = |B_n|$ の、 $\beta = \{0, 1, 2\}$ 上の最大周期列であるとする。スライディング・ブロック符号 ϕ を用いて、最適二値マルコフ連鎖拡散符号系列 Y が

【数 6 0】

$$Y = \Phi(X) \Phi(SX) \Phi(S^2X) \dots \Phi(S^{L-1}X)$$

20

により実現される。

【 0 0 5 4 】

長さ $|B_n|$ の最適二値マルコフ連鎖拡散符号の例を示す。

(例 1) $n = 3$ のとき、 $L = 20$ であり、

【数 6 1】

$$00010020110121021112 \xrightarrow{\phi|_{\Sigma^L}} 11101011001010010001$$

30

を得る。ここで、表記を簡単にするため、右辺の 0 は - 1 を表す。

【 0 0 5 5 】

[参考文献 8] の結果を最適二値マルコフ連鎖拡散符号に適用して、次の評価を得る。

(定理 2)

【数 6 2】

$0 \leq \ell \leq n-1$ に対して、

$$r_{|B_n|}(\ell; Y) = (-2 + \sqrt{3})^\ell + \left\{ \left(\frac{\beta}{\bar{\beta}} \right)^\ell - \left(\frac{\bar{\beta}}{\beta} \right)^\ell \right\} \cdot \frac{\left(\frac{\bar{\beta}}{\beta} \right)^n}{1 + \left(\frac{\bar{\beta}}{\beta} \right)^n}$$

40

を得る。

これは

【数 6 3】

$$r_{|\mathcal{B}_n|}(\ell; \mathbf{Y}) = \mathbb{E}[Z_0 Z_\ell] + O\left(\left(\frac{\bar{\beta}}{\beta}\right)^n\right)$$

を示唆する。ここで、

【数 6 4】

O

10

はランダウの記号である。

【0056】

< 1.6. 実験結果 >

最大周期列の長さ $|\mathcal{B}_n|$ 、 H_n における $\{0, 1, 2\}$ 上の最大周期列の総数 ν_n 、及び実現された最適二値マルコフ連鎖拡散符号の総数

【数 6 5】

$\widetilde{\nu}_n$

20

をそれぞれ表 1 に示す。

【表 1】

系列長 $|\mathcal{B}_n|$ ，最大周期列数 ν_n ，および最適拡散符号数 $\widetilde{\nu}_n$

n	系列長	最大周期列数	最適拡散符号数
2	8	12	6
3	20	1728	945

30

【0057】

$n = 4$ のとき、最大周期列の長さは $|\mathcal{B}_n| = 56$ となる。この場合に、離散化変換に基づいて実現された最適二値マルコフ連鎖拡散符号を用いた非同期 SSMA 通信システムにおけるビット誤り生起確率の、ユーザ数依存性を図 3 に示す。現在、実用化されている Gold 符号の系列長は 32 である。 $n = 4$ のとき、長さ $|\mathcal{B}_n| = 56$ の最適二値マルコフ連鎖拡散符号に対して、開始点をランダムに選び、そこから長さ 32 で系列を打ち切ることにより、長さ 32 の系列が得られる。このようにして、長さ 56 の最適二値マルコフ連鎖拡散符号から長さ 32 の系列を抽出した場合の結果を図 4 に示す。

40

【0058】

図 3 及び図 4 の各々において、曲線は [参考文献 9] で与えられる中心極限定理 (CLT) に基づく理論評価式を表し、点 \times は数値実験結果を表す。いずれにおいても両者は良く一致していることが確認される。同様に、任意の長さの疑似乱数を得ることができる。

【0059】

< 1.7. 一般の場合について >

これまで、最適二値マルコフ連鎖拡散符号を実現するため、

【数 6 6】

$$\mathbb{E}[Z_n] = 0 \quad \text{and} \quad \mathbb{E}[Z_0 Z_\ell] = \rho^\ell, \quad \ell \geq 0$$

において、 $\rho = -2 + 3$ の場合を考えた。 ρ が一般の場合には上記 (1) 式と同様に、

$$\rho = \frac{\lambda}{\bar{\lambda}} = \frac{c_1 - \sqrt{c_1^2 + 4c_2}}{c_1 + \sqrt{c_1^2 + 4c_2}} \quad 10$$

の整数解 (c_1, c_2) を求めることにより、傾き ρ が得られる。

【0060】

簡単のため $c_1 + 1 = k$ とおく。離散化変換により、 $\{0, 1, \dots, k-1\}$ 上の最大周期列を得る。残るはブロック符号 σ の定義だけである。

【0061】

貪欲算法による実数 $x \in [0, 1]$ の β 進展開を $d_\beta(x)$ で表す。 $|B_n| = L$ とおく。 L ブロック $v = v_1 v_2 \dots v_L \in \{0, 1, 2\}^L$ に対して、ブロック符号 $\sigma : \{0, 1, \dots, k-1\}^L \rightarrow \{1, -1\}$ を次のように定義すればよい。

【数 6 8】

i) $\frac{1}{2} + \frac{\bar{\beta}}{\beta - \bar{\beta}} \leq \frac{c_2}{\beta - \bar{\beta}} \left(\frac{1}{\beta} + \frac{1}{\beta^2} \right)$ のとき

$$\Phi(v) = \begin{cases} 1, & v \leq d_\beta(\xi) \text{ のとき,} \\ -1, & d_\beta(\xi) < v \leq c_1 \text{ のとき,} \\ 1, & c_1 < v \text{ のとき.} \end{cases} \quad 30$$

ここで $\xi = \frac{\beta - \bar{\beta}}{2 \left(\frac{1}{\beta} + \frac{1}{\beta^2} \right)}$.

【数 6 9】

ii) $\frac{1}{2} + \frac{\bar{\beta}}{\beta - \bar{\beta}} > \frac{c_2}{\beta - \bar{\beta}} \left(\frac{1}{\beta} + \frac{1}{\beta^2} \right)$ のとき

$$\Phi(v) = \begin{cases} 1, & v \leq c_2 + d_\beta(\eta) \text{ のとき,} \\ -1, & c_2 + d_\beta(\eta) < v \leq c_1 \text{ のとき,} \\ 1, & c_1 < v \text{ のとき.} \end{cases} \quad 40$$

ここで $\eta = \frac{1}{2} + \bar{\beta} - c_2 \left(\frac{1}{\beta} + \frac{1}{\beta^2} \right)$.

【0062】

以下に、参考文献を列挙する。

[参考文献 1] D. Lind and B. Marcus, Symbolic Dynamics and Coding, Cambridge Univ. Press, 1995.

[参考文献 2] R. E. Kalman, "Nonlinear aspects of sampled-data control systems", Proc. Symp. Nonlinear Circuit Analysis VI, pp. 273-313, 1956.

[参考文献 3] G. Mazzini, G. Setti, and R. Rovatti, "Chaotic Complex Spreading Sequences for Asynchronous DS-CDMA Part I: System Modeling and Results" IEEE Trans. Circuit Syst.-I vol. CAS-44, no.10, pp.937-947, 1997.

[参考文献 4] H. Fujisaki, "An Algorithm For Generating All Full-Length Sequences Which Are Based On Discretized Markov Transformations," NOLTA, IEICE, vol. 1, pp. 166-175, 2010.

[参考文献 5] H. Fujisaki and H. Sugimori, "Phase-Shift-Free M-Phase Spreading Sequences of Markov Chains," IEEE Trans. on Circuit and Systems Part I, vol.CAS-55, pp. 876-882, 2008.

[参考文献 6] D. A. Lind, "The entropies of topological Markov shifts and a related class of algebraic integers," Ergodic Theory and Dynamical Systems, vol. 4, pp. 283 - 300, 1984. 10

[参考文献 7] H. Fujisaki, "On the topological entropy of the discretized Markov -transformations," to appear in IEICE Trans. Fundamentals, vol. E99-A, total 10 pages, 2016.

[参考文献 8] H. Fujisaki, "Correlational Properties of the Full-Length Sequences Based on the Discretized Markov -transformations," to appear in NOLTA, IEICE, vol. 7, total 11 pages, 2017.

[参考文献 9] H. Fujisaki and G. Keller, "The central limit theorem for the normalized sums of the MAI for SSMA communication systems using spreading sequences of Markov chains," IEICE Trans. Fundamentals, vol. E89-A, no.9, pp. 2307-2314, 2006. 20

【 0 0 6 3 】

< 2 . 実施例 >

< 2 . 1 . 実施例 1 >

次に、実施例 1 を用いて、本発明の実施の形態について説明する。図 5 は、実施例 1 にかかる系列生成装置 1 0 0 を示す図である。系列生成装置 1 0 0 は、記憶部 1 1 0、生成部 1 3 0、及び変換部 1 5 0 を含む。系列生成装置 1 0 0 は、所定の自己相関特性と均等分布を有する互いに無相関な系列を生成する。

【 0 0 6 4 】

(記憶部 1 1 0)

記憶部 1 1 0 は、生成部 1 3 0 と変換部 1 5 0 とそれぞれ接続され、生成部 1 3 0 により生成された系列 (第 1 の系列) を記憶し、記憶している情報を変換部 1 5 0 に出力する。

【 0 0 6 5 】

(生成部 1 3 0)

生成部 1 3 0 は、上述した < 理論 > に従い、所定の相関特性に基づいて設定された区分単調増加マルコフ変換の傾きに応じて、第 1 系列を生成する。まず、所定の相関特性は、下記式の により与えられる。

【 数 7 0 】

$$\mathbb{E}[Z_0 Z_\ell] = \rho^\ell, \quad \ell \geq 0$$

ここで、Z は第 1 系列の確率変数である。具体的な の値は、ユーザが例えば記憶部 1 1 0 に予め記憶しておき、記憶した情報 (の値) を生成部 1 3 0 に出力することができる。

【 0 0 6 6 】

このようにして が与えられることで、生成部 1 3 0 は、下記式において整数解 (c , 50

, c_2) を求めることにより、区分単調増加マルコフ変換の傾き を得ることができる。

【数 7 1】

$$\rho = \frac{\lambda}{\bar{\lambda}} = \frac{c_1 - \sqrt{c_1^2 + 4c_2}}{c_1 + \sqrt{c_1^2 + 4c_2}}$$

具体例として、 $\lambda = -2 + \sqrt{3}$ の場合には、区分単調増加マルコフ変換の傾き は、 $1 + \sqrt{3}$ となる。

【0067】

生成部 130 は、 $Z_n = (T^n(x))$ の T を、区分単調増加マルコフ変換の傾き とすることで、下記式により表される第 1 系列を生成する。生成した第 1 系列は、記憶部 110 に記憶される。

【数 7 2】

$$(Z_n)_{n=0}^{\infty}$$

20

【0068】

具体例で挙げたように T を傾き $1 + \sqrt{3}$ の 変換とした場合、区間 $[0, 1)$ に属するほとんど全ての x に対して、所定 $\lambda = -2 + \sqrt{3}$ の相関特性を有し、 $\{1, -1\}$ に値を取る第 1 系列を生成することができる。

【0069】

(変換部 150)

変換部 150 は、上述した <理論> に従い、所定の分布と区分単調増加マルコフ変換の傾きとに基づいて設定された変換条件に基づいて、第 1 系列を第 2 系列に変換する。

【0070】

所定の分布は、均等分布、言い換えれば一様分布である。一様分布を満たす限り、

【数 7 3】

$$\mathbb{E}[Z_n] = 0$$

となる。

【0071】

一様分布と、区分単調増加マルコフ変換の傾きとに基づいて得られる変換条件は、下記式のブロック符号 により表される。

30

40

【数 7 4】

i) $\frac{1}{2} + \frac{\bar{\beta}}{\beta - \bar{\beta}} \leq \frac{c_2}{\beta - \bar{\beta}} \left(\frac{1}{\beta} + \frac{1}{\beta^2} \right)$ のとき

$$\Phi(v) = \begin{cases} 1, & v \leq d_\beta(\xi) \text{ のとき,} \\ -1, & d_\beta(\xi) < v \leq c_1 \text{ のとき,} \\ 1, & c_1 < v \text{ のとき.} \end{cases}$$

$$\text{ここで } \xi = \frac{\beta - \bar{\beta}}{2 \left(\frac{1}{\beta} + \frac{1}{\beta^2} \right)}.$$

10

【数 7 5】

ii) $\frac{1}{2} + \frac{\bar{\beta}}{\beta - \bar{\beta}} > \frac{c_2}{\beta - \bar{\beta}} \left(\frac{1}{\beta} + \frac{1}{\beta^2} \right)$ のとき

$$\Phi(v) = \begin{cases} 1, & v \leq c_2 + d_\beta(\eta) \text{ のとき,} \\ -1, & c_2 + d_\beta(\eta) < v \leq c_1 \text{ のとき,} \\ 1, & c_1 < v \text{ のとき.} \end{cases}$$

$$\text{ここで } \eta = \frac{1}{2} + \bar{\beta} - c_2 \left(\frac{1}{\beta} + \frac{1}{\beta^2} \right).$$

20

【0072】

具体例として、区分単調増加マルコフ変換の傾き が 1 + 3 の場合には、ブロック符号 は下記式により表される。

【数 7 6】

$$\Phi(v) = \begin{cases} 1, & v \leq 02 \text{ のとき,} \\ -1, & 02 < v \leq 2 \text{ のとき,} \\ 1, & 2 < v \text{ のとき} \end{cases}$$

30

【0073】

変換部 150 は、変換条件を表すブロック符号 に基づいて、下記式により第 1 系列 X を第 2 系列 Y に変換する。

【数 7 7】

$$\mathbf{Y} = \Phi(\mathbf{X}) \Phi(S\mathbf{X}) \Phi(S^2\mathbf{X}) \cdots \Phi(S^{L-1}\mathbf{X})$$

40

【0074】

ここで、S は、L ブロック全体の集合 $\{0, 1, 2\}^L$ 上のシフト変換であって、 $v = v_1 v_2 \cdots v_L \in \{0, 1, 2\}^L$ に対して下記式で表される。

【数 7 8】

$$S(v_1, v_2, \cdots, v_{L-1}, v_L) = (v_2, v_3, \cdots, v_L, v_1)$$

【0075】

以上のような構成からなる系列生成部 100 は、所定の相関特性に基づいて設定された

50

区分単調増加マルコフ変換の傾きに応じて生成された第1系列を、所定の分布と区分単調増加マルコフ変換の傾きとに基づいて設定された変換条件に基づいて変換することにより、任意に指定された自己相関特性と均等分布を有する互いに無相関な第2系列を大量に生成することができる。

【0076】

第2系列は、拡散符号として用いることができる。つまり、CDMA方式などの無線通信の拡散符号として用いることができる。また、第2系列は、暗号化又は復号(decryption)のための系列として用いることができる。

【0077】

< 2.2. 実施例2 >

次に、実施例2を用いて、本発明の実施の形態について説明する。図6は、実施例2にかかる符号化処理装置200を示す図である。符号化処理装置200は、記憶部210、及び符号化部230を含む。符号化処理装置200は、上述した系列生成部100により生成された系列、すなわち、任意に指定された自己相関特性と均等分布を有する第2系列を利用して、任意の信号列の符号化を行う。

【0078】

(記憶部210)

記憶部210は、上述した系列生成装置100により第1系列から変換された第2系列を記憶し、記憶している情報を符号化部230に出力する。ここで、上述したように、第1系列は、所定の相関特性に基づいて設定された区分単調増加マルコフ変換の傾きに応じて生成されたものである。また、第2系列は、第1系列を、所定の分布(均等分布)と区分単調増加マルコフ変換の傾きとに基づく変換条件に基づいて変換したものである。

【0079】

(符号化部230)

符号化部230は、記憶部210から第2系列を読み出し、読み出した第2系列に基づいて信号列の符号化を行って出力する。

【0080】

具体的に、符号化処理装置200が、CDMA方式で通信を行う用途で用いられる場合には、第2の系列は、第1系列から変換された拡散符号であり、符号化部230は、信号列を拡散する。

【0081】

また、符号化処理装置200が、暗号化を行う用途で用いられる場合には、符号化部230は、信号列を暗号化する。

【0082】

以上のような構成からなる符号化処理装置200は、記憶部210が、自己相関特性と均等分布を有する互いに無相関な第2系列を大量に記憶することができる。このため、例えば、CDMA方式の無線通信において同一の周波数帯域内で2つ以上の複数の通信を行う際に、第2系列を用いた拡散を行った信号列を用いて通信することで、ビット誤りを少なくして信頼性を高めることができる。また、符号化処理装置200は、第2系列を用いて信号列を暗号化することで、暗号の信頼性を高めることができる。

【0083】

< 2.3. 実施例3 >

次に、実施例3を用いて、本発明の実施の形態について説明する。図7は、実施例3にかかる送信装置300を示す図である。

【0084】

送信装置300は、記憶部310、符号化部330、及び送信部350を含む。送信装置300は、上述した系列生成部100により生成された系列、すなわち、任意に指定された自己相関特性と均等分布を有する第2系列を利用して、任意の信号列を符号化して、他の装置へ送信する。

【0085】

10

20

30

40

50

(記憶部 3 1 0)

記憶部 3 1 0 は、上述した系列生成装置 1 0 0 により第 1 系列から変換された第 2 系列を記憶し、記憶している情報を符号化部 3 3 0 に出力する。ここで、上述したように、第 1 系列は、所定の相関特性に基づいて設定された区分単調増加マルコフ変換の傾きに応じて生成されたものである。また、第 2 系列は、第 1 系列を、所定の分布（均等分布）と区分単調増加マルコフ変換の傾きとに基づく変換条件に基づいて変換したものである。

【 0 0 8 6 】

(符号化部 3 3 0)

符号化部 3 3 0 は、記憶部 3 1 0 から第 2 系列を読み出し、読み出した第 2 系列に基づいて信号列の符号化を行って送信部 3 5 0 に出力する。具体的に、第 2 の系列は第 1 系列から変換された拡散符号であり、符号化部 3 3 0 は、第 2 系列を用いて信号列の拡散を行う。なお、拡散に代えて暗号化を行ってもよい。すなわち、符号化部 3 3 0 は、第 2 系列を用いて信号列の暗号化を行ってもよい。

【 0 0 8 7 】

(送信部 3 5 0)

送信部 3 5 0 は、符号化部 3 3 0 により符号化（拡散）された信号列を無線信号に変換して、他の装置に送信する。

【 0 0 8 8 】

以上のような構成からなる送信装置 3 0 0 は、記憶部 3 1 0 が、自己相関特性と均等分布を有する互いに無相関な第 2 系列を大量に記憶することができ、このような第 2 系列を用いて信号列を拡散して他の装置に送信することができる。

【 0 0 8 9 】

例えば CDMA 方式の無線通信では、同一の周波数帯域内で 2 つ以上の複数の通信を行う際にビット誤りを軽減する観点から、長周期の系列を大量に用いることが必要となる。このため、送信装置 3 0 0 では、上述したように、第 2 系列を用いて信号列を拡散して他の装置に送信することで、同一の周波数帯域内で 2 つ以上の複数の通信を行う際に、ビット誤りを少なくして信頼性を高めることができる。

【 0 0 9 0 】

< 2 . 4 . 実施例 4 >

次に、実施例 4 を用いて、本発明の実施の形態について説明する。図 8 は、実施例 4 にかかる受信装置 4 0 0 を示す図である。

【 0 0 9 1 】

受信装置 4 0 0 は、記憶部 4 1 0、受信部 4 3 0、及び復号部 4 5 0 を含む。受信装置 4 0 0 は、上述した系列生成部 1 0 0 により生成された系列、すなわち、任意に指定された自己相関特性と均等分布を有する第 2 系列を利用して、符号化された信号列を復号する。

【 0 0 9 2 】

(記憶部 4 1 0)

記憶部 4 1 0 は、上述した系列生成装置 1 0 0 により第 1 系列から変換された第 2 系列を記憶し、記憶している情報を復号部 4 5 0 に出力する。ここで、上述したように、第 1 系列は、所定の相関特性に基づいて設定された区分単調増加マルコフ変換の傾きに応じて生成されたものである。また、第 2 系列は、第 1 系列を、所定の分布（均等分布）と区分単調増加マルコフ変換の傾きとに基づく変換条件に基づいて変換したものである。

【 0 0 9 3 】

(受信部 4 3 0)

受信部 4 3 0 は、他の装置から、第 2 系列に基づいて符号化された信号列の無線信号を受信して復号部 4 5 0 に出力する。

【 0 0 9 4 】

(復号部 4 5 0)

復号部 4 5 0 は、記憶部 3 1 0 から第 2 系列を読み出し、読み出した第 2 系列に基づい

10

20

30

40

50

て、受信部 430 が受信した信号列を復号 (decoding) する。具体的に、第 2 の系列は第 1 系列から変換された拡散符号であり、復号部 450 は、第 2 系列を用いて信号列の逆拡散を行う。なお、逆拡散に限らず、信号列が暗号化されている場合には、復号部 450 は、第 2 系列を用いて信号列の復号 (decryption) を行ってもよい。

【0095】

以上のような構成からなる受信装置 400 は、記憶部 410 が、自己相関特性と均等分布を有する互いに無相関な第 2 系列を大量に記憶することができ、このような第 2 系列を利用して信号列を逆拡散することができる。

【0096】

例えば CDMA 方式の無線通信では、同一の周波数帯域内で 2 つ以上の複数の通信を行う際にビット誤りを軽減する観点から、長周期の系列を大量に用いることが必要となる。このため、受信装置 400 では、上述したように、第 2 系列を用いて信号列を逆拡散することで、同一の周波数帯域内で 2 つ以上の複数の通信を行う際に、ビット誤りを少なくして信頼性を高めることができる。

【0097】

< 3 . その他 >

以上、本発明を実施の形態をもとに説明した。本発明は上述した実施例並びに各実施例の内容に限定されるものではなく、本発明の要旨の範囲内において種々に変形して実施することが可能である。上記実施の形態は例示であり、それらの各構成要素や各処理プロセスの組み合わせにいろいろな変形例が可能で、またそうした変形例も本発明の範囲

【0098】

例えば、以下の発明も、本発明の態様として捉えることができる。

【0099】

(発明 1)

第 1 系列から変換された第 2 系列に基づいて符号化が行われた信号列を、他の装置から受信する受信部と、

前記第 2 系列に基づいて、前記受信した信号列の復号を行う復号部と、
を備え、

前記第 1 系列は、所定の相関特性に基づいて設定された区分単調増加マルコフ変換の傾きに応じて生成された系列であり、

前記第 2 系列は、前記第 1 系列を、所定の分布と前記区分単調増加マルコフ変換の傾きとに基づき変換条件に基づいて変換した系列である、
受信装置。

(発明 2)

前記第 2 系列は、前記第 1 系列から変換された拡散符号であり、

前記符号化は、拡散であり、

前記復号は、前記受信した信号列の逆拡散である、

(発明 1) の受信装置。

(発明 3)

前記符号化は、暗号化であり、

前記復号 (decoding) は、前記信号列の復号 (decryption) である、(発明 1) 記載の受信装置。

(発明 4)

所定の相関特性に基づいて設定された区分単調増加マルコフ変換の傾きに応じて、第 1 系列を生成することと、

所定の分布と前記区分単調増加マルコフ変換の傾きとに基づいて設定された変換条件に基づいて、前記第 1 系列を第 2 系列に変換することと、
を含む系列生成方法。

(発明 5)

10

20

30

40

50

第 1 系列から変換された第 2 系列を取得することと、
前記第 2 系列に基づいて、信号列の符号化を行うことと、
を含み、

前記第 1 系列は、所定の相関特性に基づいて設定された区分単調増加マルコフ変換の傾きに応じて生成された系列であり、

前記第 2 系列は、前記第 1 系列を、所定の分布と前記区分単調増加マルコフ変換の傾きとに基づく変換条件に基づいて変換した系列である、
符号化処理方法。

(発明 6)

第 1 系列から変換された第 2 系列に基づいて、信号列の符号化を行うことと、
前記符号化後の前記信号列を、他の装置に送信することと、
を含み、

10

前記第 1 系列は、所定の相関特性に基づいて設定された区分単調増加マルコフ変換の傾きに応じて生成された系列であり、

前記第 2 系列は、前記第 1 系列を、所定の分布と前記区分単調増加マルコフ変換の傾きとに基づく変換条件に基づいて変換した系列である、
送信方法。

(発明 7)

第 1 系列から変換された第 2 系列に基づいて符号化が行われた信号列を、他の装置から受信することと、

20

前記第 2 系列に基づいて、前記受信した信号列の復号を行うことと、
を含み、

前記第 1 系列は、所定の相関特性に基づいて設定された区分単調増加マルコフ変換の傾きに応じて生成された系列であり、

前記第 2 系列は、前記第 1 系列を、所定の分布と前記区分単調増加マルコフ変換の傾きとに基づく変換条件に基づいて変換した系列である、
受信方法。

【産業上の利用可能性】

【 0 1 0 0 】

任意に指定された自己相関特性と均等分布を有する互いに無相関な系列を大量に生成することが可能である。

30

【符号の説明】

【 0 1 0 1 】

1 0 0 系列生成装置

1 1 0、2 1 0、3 1 0、4 1 0 記憶部

1 3 0 生成部

1 5 0 変換部

2 0 0 符号化装置

2 3 0、3 3 0 符号化部

3 5 0 送信部

4 3 0 受信部

4 5 0 復号部

40

【図1】

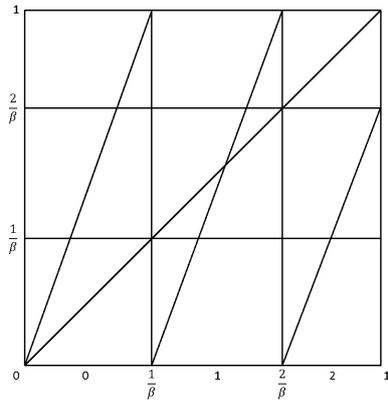


Figure 1

【図2】

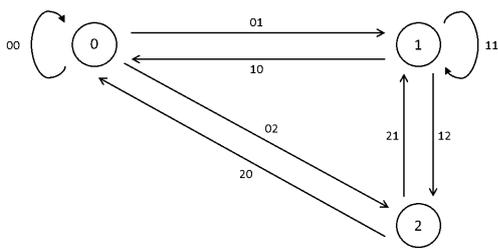


Figure 2

【図3】

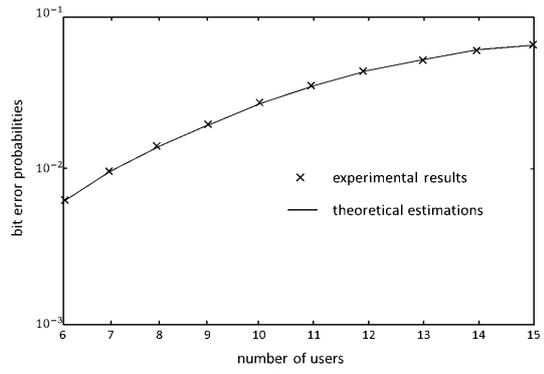


Figure 3

【図4】

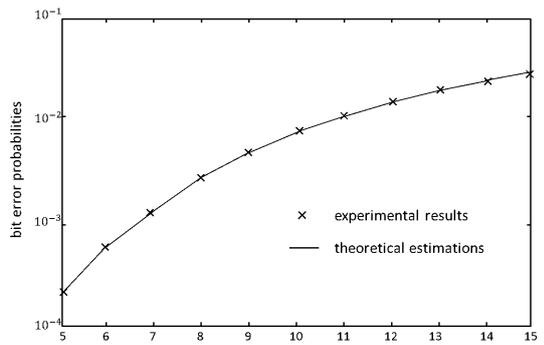


Figure 4

【図5】

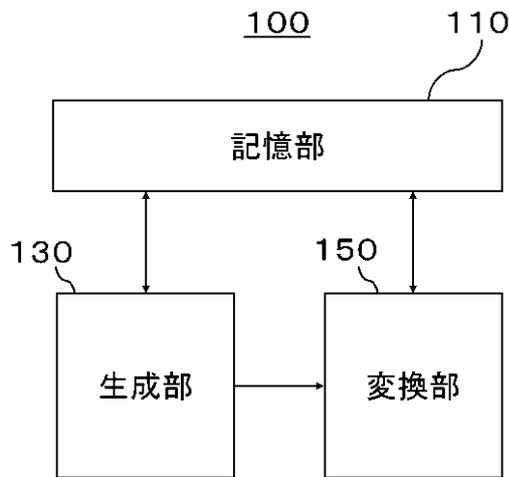


Figure 5

【図6】

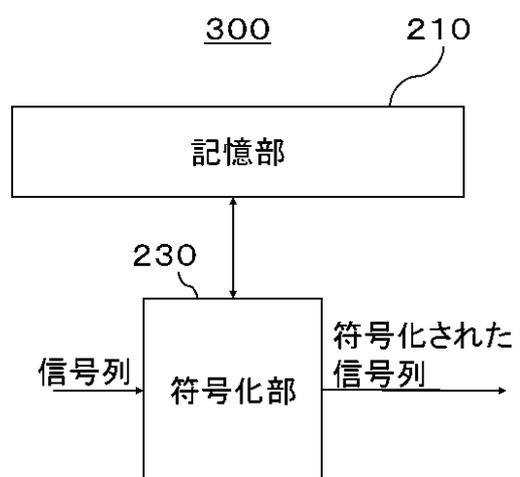


Figure 6

【図7】

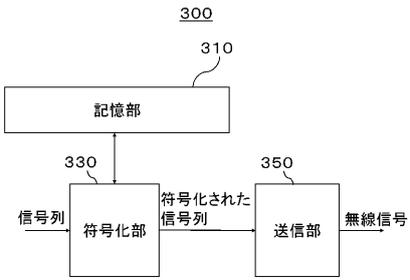


Figure 7

【図8】

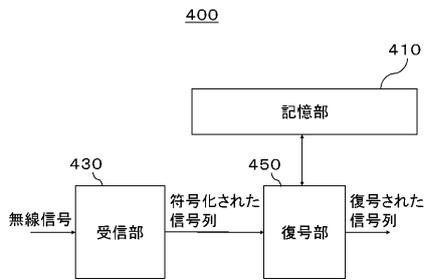


Figure 8

フロントページの続き

(56)参考文献 特開2011-227632(JP,A)
特開平10-240500(JP,A)
特開平05-216630(JP,A)
米国特許出願公開第2013/0103731(US,A1)

(58)調査した分野(Int.Cl., DB名)
G06F7/58
H04J13/00-13/22