(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2018-72867
(P2018-72867A)
(43)公開日　平成30年5月10日(2018.5.10)

(51)Int.Cl.			F I			テーマコード（参考）
G06F	7/58	(2006.01)	G06F	7/58	620	
H04J	13/16	(2011.01)	H04J	13/16		

審査請求 未請求　請求項の数 14　ＯＬ　（全 30 頁）

(21)出願番号　特願2016-207576 (P2016-207576)
(22)出願日　平成28年10月24日 (2016.10.24)

(71)出願人　504160781
国立大学法人金沢大学
石川県金沢市角間町ヌ７番地
(74)代理人　100141519
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

(54)【発明の名称】系列生成装置、符号化処理装置、送信装置

(57)【要約】
【課題】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可能な系列生成装置、当該系列を利用する符号化装置、送信装置、及び受信装置を提供する。
【解決手段】系列生成装置１００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１３０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１５０と、を備える。
【選択図】図５

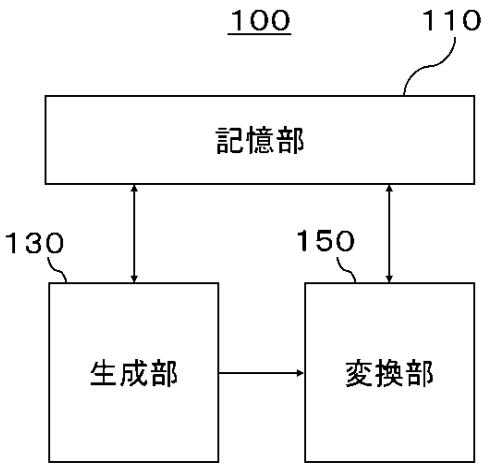

Figure 5

【特許請求の範囲】
【請求項１】
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】
前記所定の分布は、均等分布である、請求項１記載の系列生成装置。
【請求項３】
前記所定の相関特性は、下記式のρである、請求項１又は２記載の系列生成装置。
【数１】

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

ここで、Ｚは、前記第１系列の確率変数である。
【請求項４】
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乃至３のうちいずれか１項記載の系列生成装置。
【数２】

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

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】

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

【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４記載の系列生成装置。
【数４】

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

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

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

【数５】

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

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

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

【請求項６】

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４又は５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７】

前記第２系列は、拡散符号である、請求項１乃至６のうちいずれか１項記載の系列生成装置。

【請求項８】

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６のうちいずれか１項記載の系列生成装置。

【請求項９】

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、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、

符号化処理装置。

【請求項１０】

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９記載の符号化処理装置。

【請求項１１】

前記符号化は、前記信号列の暗号化である、請求項９記載の符号化処理装置。

【請求項１２】

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、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、
送信装置。
【請求項１３】
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１２記載の送信装置。
【請求項１４】
前記符号化は、前記信号列の暗号化である、請求項１２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】
【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。
【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。
【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。
【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。

【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。

【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ものもまた、本発明の態様として捉えることができる。

【発明の効果】

【００１３】

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β＝１＋√３を有するマルコフβ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．β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β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

【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Σシフトは、

【数１】

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

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】

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

は、

【数３】

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

で定義される。全

【数４】

$$\sum^{\mathbb{Z}}$$

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σＸで表す。これは、Σ上のσの、Ｘへの制限である。簡単のため、σＸよりむしろσ：Ｘ→Ｘと書くことにする。

【００２０】

元ｕ＝ｕ$_1$ｕ$_2$…ｕ$_n$∈Σ^{n}を長さｎ（ｎ≧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、Ｌ$_n$（Ｘ）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

【数５】

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

である。

ここで、Ｌ$_0$（Ｘ）＝｛ε｝である。

【００２１】

（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∈Ａは、初期状態と呼ばれ、ｉ（ｅ）∈Ｖで表される頂点を出発し、終状態と呼ばれ、ｔ（ｅ）∈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∈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×ｋ非負整数行列

【数６】

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

は，頂点集合｛０，１，…，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。

【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、σ：Ｘ$_{A}$→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】

＜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）→［０，１）とする。Ｐは点０＝ａ$_{0}$＜ａ$_{1}$＜…＜ａ$_{|P|}$＝１で与えられる区間［０，１）の分割であるとする。ｉ＝１，…，｜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】

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

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∈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

【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、ｔ（ｅ（Ｉ））＝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】

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】

$$\widehat{T}$$

は、全てのＩ∈Ｑに対して、

【数１１】

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

を満たす置換

【数１２】

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

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】

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

が基本変換Ｔ：［０，１）→［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１４】

$$\hat{T}$$

それ自身は最大周期列ｗとして見ることができる。さらに、最大周期列ｗに対して、両側無限列w^{∞}＝…ｗｗｗ…を考えれば、巡回置換

【数１５】

$$\hat{T}$$

は

【数１６】

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

上のシフトと見做すことができる。

【００２９】

離散化マルコフ変換に基づく最大周期列は

【数１７】

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

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１８】

$$\widehat{T}:\mathcal{Q}\to\mathcal{Q}$$

が単に基本変換Ｔ：［０，１）→［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］。

【００３０】

（定義３）

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

【数１９】

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

を持ち、また、$e_2e_3\cdots e_{n-1}=f_1f_2\cdots f_{n-2}$のとき(但しｎ＝２の場合はｔ（$e_1$）＝ｉ（$f_1$）のとき)には常に$e_1e_2\cdots e_{n-1}$から$f_1f_2\cdots f_{n-1}$へ丁度一つの辺を含むが、それ以外のときには何も無いような、辺集合を持つと定義される。辺は$e_1e_2e_3\cdots e_{n-1}f_{n-1}=e_1f_1f_2\cdots f_{n-1}$と名付けられる。ｎ＝１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】

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

を得る。各ｎ≧１に対して、

【数２１】

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

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。各々は、離散化マルコフ変換

【数２２】

$$\widehat{T}_n$$

を導く。最大周期列の長さは｜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$_1$＜…＜ｘ$_k$＝１が存在して、各整数ｉ＝１，…，ｋに対して、Ｔの区間［ｘ$_{i-1}$，ｘｉ）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β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（≧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．β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）通信システムのおけるビット誤り生起確率に関して、最適Ｍ（≧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＋√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≧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

【数２３】

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

を有する｛１，－１｝に値を取る定常マルコフ連鎖系列

【数２４】

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

として特徴付けられる。ここで、確率変数Ｚに対して、

【数２５】

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

はＺの期待値を表す。

【００３７】

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。

（定義４）

｛－１，１｝上の系列

【数２６】

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

と

【数２７】

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

に対する、遅れ時間

【数２８】

$$\ell$$

の正規化相互相関関数は

【数２９】

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

で定義される。ここで、

【数３０】

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

である。整数ａとｂ（≧１）に対して、ａ（ｍｏｄ　ｂ）は法ｂに関するａの最小剰余を表す。Ｘ＝Ｙのとき

【数３１】

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

を正規化自己相関関数と呼び、単に

【数３２】

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

で表す。

所望の

【数３３】

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

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。

【００３８】

（定義５）

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

【数３４】

$$\mathbb{P}$$

で表す。

【００３９】

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】

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

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】

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

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λ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】

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

である。多項式ｆ（ｔ）のコンパニオン行列は、

【数３９】

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

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。

【００４１】

β変換は、次のように定義される。すなわち、β＞１に対して、β変換Ｔ：［０，１］→［０，１］はＴ（ｘ）＝βｘ（ｍｏｄ　１），ｘ∈［０，１］で定義される。ここでｘ＝ｙ（ｍｏｄ　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、β変換が（定義２）を満たすとき、マルコフβ変換と呼ばれる。

【００４２】

マルコフβ変換に行列Ｂを同伴するために、０＜ｃ$_2$≦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β変換の（ｃ$_1$＋１）×（ｃ$_1$＋１）隣接行列Ａは

【数４０】

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

で与えられる。

【００４３】

実数値を二値に符号化する写像Ψ：［０，１）→｛１，－１｝を

【数４１】

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

で定義する。ｎ＝０，１，２，…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$_{n}$＝Ψ（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】

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

が生成される。斯くして、

【数４３】

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

を得る。ここで、

【数４４】

$$\overline{\lambda}$$

はλの代数的共役である。

【００４４】

条件０＜ｃ$_2$≦ｃ$_1$の下、方程式

【数４５】

$$-2+\sqrt{3}=\frac{\lambda}{\overline{\lambda}}=\frac{c_1-\sqrt{c_1^2+4c_2}}{c_1+\sqrt{c_1^2+4c_2}} \qquad (1)$$

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。

【００４５】

結局、傾きβ＝１＋√３を有するマルコフβ変換Ｔを得る。β＝１＋√３＝λはｔ^2－２ｔ－２＝０の正の解である。図１にＴのグラフを示す。

【００４６】

相関特性

【数４６】

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

を有するような、｛１，－１｝に値を取るマルコフ連鎖系列

【数４７】

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

をうまく得た。しかしながら、連鎖の定常分布は

【数４８】

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

で与えられ、一様分布でないため、

【数４９】

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

となり、所望の零でない。

【００４７】

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β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β＝１＋√３を用いるとき、区間［０，１）に属する実数ｘのβ進展開はＳＦＴ

【数５０】

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

の右側無限列として与えられる。ここでΣ＝｛０，１，２｝及びＦ＝｛２２｝である。実数ｘ∈［０，１）のβ進展開から得られる右側無限列は、図１に示したβ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_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】

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

を得る。各ｎ≧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β＝１＋√３を有するβ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（≧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。

これを

【数５２】

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

で表す。任意のｎ（≧３）に対して、

【数５３】

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

となるのが確認される。

【００５０】

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００１０２１１２０を得

る。
最大周期列の長さ｜Ｂ$_{n}$｜は
【数５４】

$$\left|\mathcal{B}_n\right| = \beta^n + \overline{\beta}^n \ (n \geq 2)$$

で与えられる［参考文献７］。ここで、
【数５５】

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

はβの代数的共役である。
【００５１】
以下、傾きβ＝１＋√３を有するβ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$_{F}$）＼｛ε｝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$_{1}$…ｕ$_{m}$（ｍ≧１）とｖ＝ｖ$_{1}$…ｖ$_{n}$（ｎ≧１）に対して、ｕ≦ｖは
【数５６】

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

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$_{2}$…ｖ$_{L}$∈｛０，１，２｝^{L}に対して、ブロック符号Φ：｛０，１，２｝^{L}→｛１，－１｝を
【数５７】

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

で定義する。
【００５２】
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$_{2}$…ｖ$_{L}$∈｛０，１，２｝^{L}に対して、
【数５８】

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

と表す。斯くして、周期Ｌの周期列に対して、

【数５９】

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

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$^{\infty}$＝…ｕｕｕ…である。

【００５３】

系列Ｘは、β＝１＋√３を有する離散化マルコフβ変換に基づく、長さＬ＝｜Ｂ$_{n}$｜の、Σ＝｛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６０】

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

により実現される。

【００５４】

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６１】

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

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。

【００５５】

［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６２】

$0 \le \ell \le n-1$に対して,

$$r_{|\mathcal{B}_n|}(\ell;\boldsymbol{Y}) = (-2+\sqrt{3})^{\ell} + \left\{\left(\frac{\overline{\beta}}{\beta}\right)^{-\ell}\left(\frac{\beta}{\overline{\beta}}\right)^{\ell} - \left(\frac{\overline{\beta}}{\beta}\right)^{\ell}\right\}\cdot\frac{\left(\frac{\overline{\beta}}{\beta}\right)^{n}}{1+\left(\frac{\overline{\beta}}{\beta}\right)^{n}}$$

を得る。

これは

【数６３】

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

を示唆する。ここで、

【数６４】

$$O$$

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｜Ｂｎ｜、Ｈｎにおける｛０，１，２｝上の最大周期列の総数νｎ、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６５】

$$\widetilde{\nu_n}$$

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

【００５７】

ｎ＝４のとき、最大周期列の長さは｜Ｂｎ｜＝５６となる。この場合に、離散化β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通信システムの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｜Ｂｎ｜＝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。

【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×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。同様にして、任意の長さの擬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６６】

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

において、ρ＝－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、

【数６７】

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

の整数解（c_1，c_2）を求めることにより、傾きβが得られる。

【００６０】

簡単のため$c_1+1=k$とおく。離散化β変換により、｛０，１，…，ｋ－１｝上の最大周期列を得る。残るはブロック符号Φ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$v=v_1v_2\cdots v_L\in\{0,1,2\}^L$に対して、ブロック符号$\Phi:\{0,1,\cdots,k-1\}^L\to\{1,-1\}$を次のように定義すればよい。

【数６８】

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

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

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

【数６９】

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

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

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

【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.

［参考文献７］ H. Fujisaki, “On the topological entropy of the discretized Markov β-transformations,” to appear in IEICE Trans. Fundamentals, vol. E99-A, tot

al 10 pages, 2016.
［参考文献８］ H. Fujisaki, “Correlational Properties of the Full-Length Sequences Based on the Discretized Markov β-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.

【００６３】

＜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１００を示す図である。系列生成装置１００は、記憶部１１０、生成部１３０、及び変換部１５０を含む。系列生成装置１００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。

【００６４】

（記憶部１１０）

記憶部１１０は、生成部１３０と変換部１５０とそれぞれ接続され、生成部１３０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１５０に出力する。

【００６５】

（生成部１３０）

生成部１３０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ρにより与えられる。

【数７０】

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

ここで、Ｚは第１系列の確率変数である。具体的なρの値は、ユーザが例えば記憶部１１０に予め記憶しておき、記憶した情報（ρの値）を生成部１３０に出力することができる。

【００６６】

このようにしてρが与えられることで、生成部１３０は、下記式において整数解（c_1, 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βを得ことができる。

【数７１】

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

具体例として、ρ＝－２＋√３の場合には、区分単調増加マルコフ変換の傾きβは、１＋√３となる。

【００６７】

生成部１３０は、$Z_n = \Psi(T^n(x))$のＴを、区分単調増加マルコフ変換の傾きβ

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７２】

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

【００６８】

具体例で挙げたようにＴを傾き１＋√３のβ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ρ＝－２＋√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７３】

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

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Φにより表される。

【数７４】

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

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

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

【数７５】

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

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

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

【００７２】
具体例として、区分単調増加マルコフ変換の傾きβが１＋√３の場合には、ブロック符号Φは下記式により表される。
【数７６】

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

【００７３】
変換部１５０は、変換条件を表すブロック符号Φ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７７】

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

【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＝$v_1v_2\cdots v_L\in\{0,1,2\}^L$に対して下記式で表される。
【数７８】

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

【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】
（記憶部３１０）
記憶部３１０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３３０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。
【００８６】
（符号化部３３０）
符号化部３３０は、記憶部３１０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３５０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３３０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３３０は、第２系列を用いて信号列の暗号化を行ってもよい。
【００８７】
（送信部３５０）
送信部３５０は、符号化部３３０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。
【００８８】
以上のような構成からなる送信装置３００は、記憶部３１０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。
【００８９】

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３００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。

【００９０】

＜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４００を示す図である。

【００９１】

受信装置４００は、記憶部４１０、受信部４３０、及び復号部４５０を含む。受信装置４００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、符号化された信号列を復号する。

【００９２】

（記憶部４１０）

記憶部４１０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復号部４５０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。

【００９３】

（受信部４３０）

受信部４３０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４５０に出力する。

【００９４】

（復号部４５０）

復号部４５０は、記憶部３１０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、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を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なこと、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。

【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く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）

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、

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、

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】

【０１００】

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。

【符号の説明】

【０１０１】

１００　系列生成装置

１１０、２１０、３１０、４１０　記憶部

１３０　生成部

１５０　変換部

２００　符号化装置

２３０、３３０　符号化部

３５０　送信部

４３０　受信部

４５０　復号部

【図１】

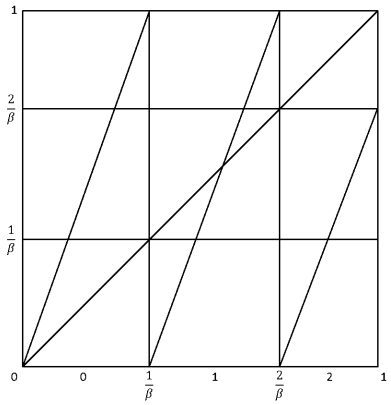

Figure 1

【図２】

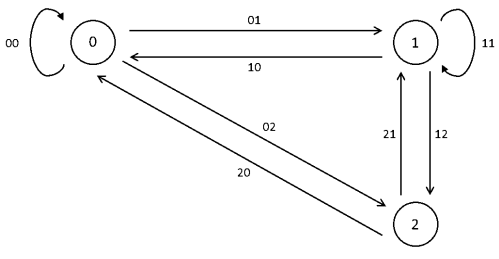

Figure 2

【図３】

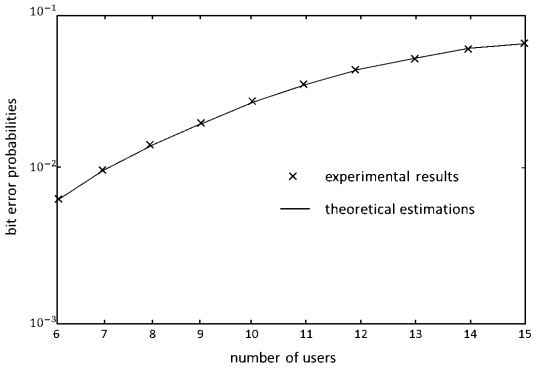

Figure 3

【図４】

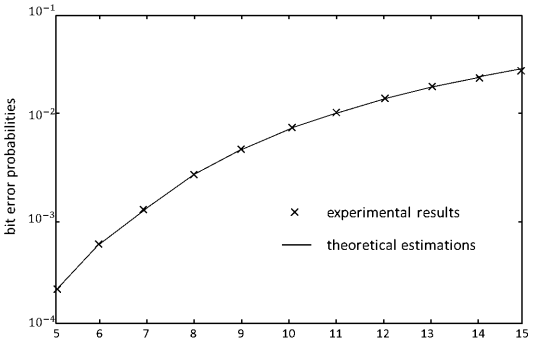

Figure 4

【図５】

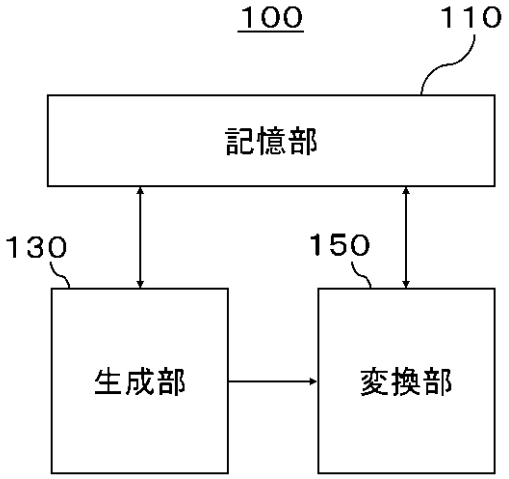

Figure 5

【図６】

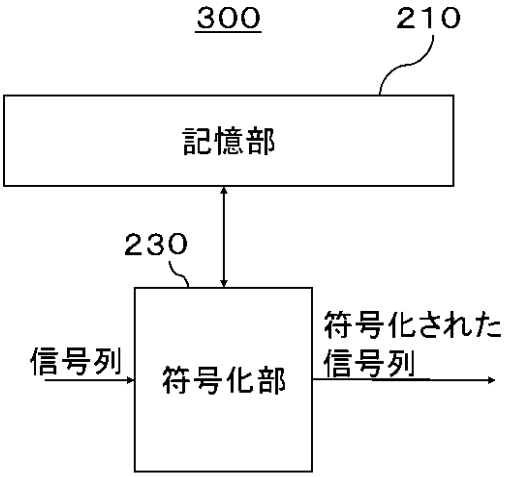

Figure 6

【図７】

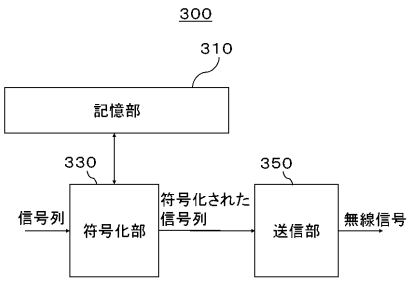

Figure 7

【図８】

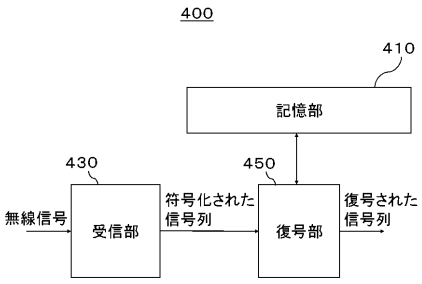

Figure 8

【手続補正書】
【提出日】平成28年11月17日(2016.11.17)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００５５
【補正方法】変更
【補正の内容】
【００５５】
［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６２】

$0 \leq \ell \leq n-1$に対して,

$$r_{|\mathcal{B}_n|}(\ell;\boldsymbol{Y}) = (-2+\sqrt{3})^{\ell} + \left\{ \left(\frac{\beta}{\overline{\beta}}\right)^{\ell} - \left(\frac{\overline{\beta}}{\beta}\right)^{\ell} \right\} \cdot \frac{\left(\frac{\overline{\beta}}{\beta}\right)^{n}}{1+\left(\frac{\overline{\beta}}{\beta}\right)^{n}}$$

を得る。
これは
【数６３】

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

を示唆する。ここで、
【数６４】

$$O$$

はランダウの記号である。