指定された相関特性と分布を有する大量な擬似乱数の実現とそのスペクトル拡散通信システムへの応用

藤 崎 礼 志　　金沢大学理工研究域准教授

概要

超離散力学系に基づく最大周期列は，系列長の増大と共に，その総数が指数関数的に増大するという，優れた特性を有する．多様な相関特性を有する系列ファミリーとして，離散化 β-変換に基づく最大周期列がある．この離散化 β-変換に基づく最大周期列ファミリーから，任意に指定された相関特性を有する最大周期列を実現する方法を与える．さらに，得られた最大周期列の分布を均等分布に変換 (符号化) する方法も与える．応用例として，スペクトル拡散多元接続 (SSMA) 通信システムを考え，本研究で得られた方法論により，ビット誤り生起確率に関して最適な二値マルコフ連鎖拡散符号を実現する．このとき，超離散化による誤差項を含む，自己相関特性の評価式も提案する．生成された最適二値マルコフ連鎖拡散符号を用いた SSMA 通信の数値伝送実験によって，通信の誤り生起確率を調査し，数値実験結果と確率論が与える理論値とが一致することを確認する．同時に，任意の長さの擬似乱数生成法も提案する．

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．学術分野のみならず，高機能携帯 (スマホ) 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．

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．本研究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．暗号や計算機科学では時間 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，情報通信や数理ファイナンスでは，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研究の目的である．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開発する．

最適スペクトル拡散符号の開発に関しては，確率解析の立場から，ビット誤り生起確率に関して最適な拡散符号の設計に既に成功した [1]．非線形力学系・確率解析に基づくこの結果は連続的なものであり，モンテカルロシミュレーションでその存在は保証されているものの，最適符号を実現するためにはある種の離散化が必要となる．エルゴード理論が保証する無限列の統計的性質は，コンピュータで実現不可能な実数論に基づいており，具体的な最大周期列 (有限列，ブロック) を構成しているわけではない．一般に，対応の定義域だけでなく値域も離散化することを超離散という．最適符号の実現において，離散力学系から如何にして超離散力学系を定義するかが問題となった．[2] において，エルゴード理論とグラフ理論の手法を融合することにより，de Bruijn 系列を含む非線形フィードバックシフトレジスタ (NLFSR) 最大周期列を与える超離散力学系を定義した．[3] では，最適拡散符号を生成する区分的線形マルコフ変換を含む，区分的単調増加 (PMI) マルコフ変換を考え，それらが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．

PMI マルコフ変換は，多様な相関特性を有する，β-変換族を含む．まず初めに，エルゴード理論の手法を用いて，β-変換族から，任意に指定された相関特性を有する確率変数列を生成する方法を与える．

超離散力学系に基づく最大周期列の典型例として，de Bruijn 系列が挙げられる．de Bruijn 系列の自己相関関数は，系列長 2^n に対して時間 $t = 0$ の前後それぞれ長さ $n - 1$ の間，値が零となる零相関範囲 (ZCZ) を有することが知られている．本研究では，離散化 β 変換に基づく最大周期列の時間 $t = 0$ の前後の自己相関特性を陽に

求め，確率論に基づく連続的な特性と比較し，超離散化による誤差を評価する．その結果を用いて，離散化 β-変換に基づく最適二値マルコフ連鎖拡散符号の，自己相関特性を陽に求める．

超離散化される前の元の変換を基本変換という．基本変換として二進展開写像を有する de Bruijn 系列は均等分布であるが，一般に PMI マルコフ変換を基本変換とする超離散力学系に基づく最大周期列は均等分布でない．得られた最大周期列を均等分布に変換 (符号化) することが重要な課題であるが，元の記号列の相関特性が不変となければならないという制約条件が符号化の開発を困難にしている．実際，うまく符号化しないと，基本変換の実数値解軌道の相関特性が現れてしまい，せっかく実現させた所望の最大周期列の相関特性が失われてしまう．この問題を解決するために，実数値解軌道を解析するエルゴード理論と記号列 (ブロック) を解析する記号力学系の両方を用いて，符号化開発を行い，均等分布を有する最適二値拡散符号 (最大周期列) を実現する．

生成された最適二値マルコフ連鎖拡散符号を用いた SSMA 通信の数値模擬実験を行い，通信の誤り生起確率を調査する．得られた数値実験結果と，確率論が与える理論値との比較を行い，本研究で提案する「指定された相関特性と分布を有する大量な擬似乱数」が，実際の SSMA 通信システムにおいて，最適拡散符号として応用できることを確認する．

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

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

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．

シフト変換 $\sigma : \Sigma^{\mathbb{Z}} \to \Sigma^{\mathbb{Z}}$ は

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

で定義される．全 $\Sigma^{\mathbb{Z}}$ 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 σ_X で表す．これは，Σ 上の σ の，X への制限である．簡単のため，σ_X よりむしろ $\sigma : X \to X$ と書くことにする．

元 $u = u_1u_2\cdots u_n \in \Sigma^n$ 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，X に属する点 (両側無限列) に現れる n ブロック全体の集合を $\mathcal{L}_n(X)$ で表す．このとき，X の言語は集合 $\mathcal{L}(X) = \bigcup_{n=0}^{\infty} \mathcal{L}_n(X)$ である．ここで，$\mathcal{L}_0(X) = \{\epsilon\}$.

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

定義 1 $G = (\mathcal{V}, \mathcal{A})$ はグラフであるとする．頂点 $u, v \in \mathcal{V}$ 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 $A = (a_{u,v})_{u,v\in\mathcal{V}}$ 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 $B = (b_{i,j})_{i,j=0}^{k-1}$ は，頂点集合 $\{0, 1, \cdots, k-1\}$ 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．

与えられた非負整数行列 A に対して，$G_A = (\mathcal{V}, \mathcal{A})$ と置く．

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

とする．このとき，$\sigma : X_A \to X_A$ 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 $\mathcal{F}$ に対して，SFT を表すのに $X_{\mathcal{F}}$ を用いる．

2 超離散力学系に基づく最大周期列

まず，離散化マルコフ変換の定義を述べる [2]．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．

定義 2 $T:[0,1)\to[0,1)$ とする．$\mathcal{P}$ は点 $0=a_0<a_1<\cdots<a_{|\mathcal{P}|}=1$ で与えられる区間 $[0,1)$ の分割であるとする．$i=1,\cdots,|\mathcal{P}|$ 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，$\mathcal{P}$ 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 $\mathcal{P}=\{I_i\}_{i=1}^{|\mathcal{P}|}$ は T に関するマルコフ分割と呼ばれる．

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 $\mathcal{P}$ が定まる．このとき，各部分区間 $I\in\mathcal{P}$ を一つの辺 $e(I)$ に対応させると，辺集合 $\mathcal{A}$ を得る．$\mathcal{A}$ に同伴して，頂点集合 $\mathcal{V}$ が

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

で与えられる．$\mathcal{P}$ 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 $J\subset T|_I(I)$ のときである．斯くして，マルコフ変換を表現するグラフ $G=(\mathcal{V},\mathcal{A})$ 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．

$H=(\mathcal{V},\mathcal{B})$ 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 $\mathcal{V}$ は G から H への変形に対して不変である．上で述べた，$\mathcal{P}$ と $\mathcal{A}$ の間の一対一対応の下で，$\mathcal{B}$ に対応する部分分割 $\mathcal{Q}$ を得る．このとき，離散化マルコフ変換 $\widehat{T}$ は，全ての $I\in\mathcal{Q}$ に対して，$\widehat{T}(I)\subset T|_I(I)$ を満たす置換 $\widehat{T}:\mathcal{Q}\to\mathcal{Q}$ によって定義される．

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 $|\mathcal{B}|$ で与えられる．T に関するマルコフ分割 $\mathcal{P}$ が与えられるとき，$|\mathcal{Q}|!$ 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 $\widehat{T}:\mathcal{Q}\to\mathcal{Q}$ が基本変換 $T:[0,1)\to[0,1)$ 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 $\widehat{T}$ 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 $w^\infty=\cdots www\cdots$ を考えれば，巡回置換 $\widehat{T}$ は $\mathcal{B}^{\mathbb{Z}}$ 上のシフトと見做すことができる．

離散化マルコフ変換に基づく最大周期列は $\mathcal{L}_{|\mathcal{B}|}(X_{A_H})$ 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 $\widehat{T}:\mathcal{Q}\to\mathcal{Q}$ が単に基本変換 $T:[0,1)\to[0,1)$ 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 [4].

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 $\mathcal{L}_{n-1}(X_{A_G})$ 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 $\mathbf{t}(e_1)=\mathbf{i}(f_1)$ 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．

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 $(G^{[n]})_{n=1}^{\infty}$ を得る．各 $n\geq 1$ に対して，$H_n=(\mathcal{L}_{n-1}(X_{A_G}),\mathcal{B}_n)$ 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 $\widehat{T}_n$ 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．

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 $0=x_0<x_1<\cdots<x_k=1$ が存在して，各整数 $i=1,\cdots,k$ 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．

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，本研究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 [5]，および [6] で定義された $k(\geq 2)$-方有尾シフト (k-way tailed shift) 変換を含む．

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 [3].

3 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 [7]．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 $M=2$ の場合を考える．

$M=2$ のとき，最適二値マルコフ連鎖拡散符号系列は

$$\mathbb{E}[Z_n]=0 \quad \text{and} \quad \mathbb{E}[Z_0Z_\ell]=\left(-2+\sqrt{3}\right)^\ell, \quad \ell\geq 0.$$

を有する $\{1,-1\}$ に値を取る定常マルコフ連鎖系列 $(Z_n)_{n=0}^{\infty}$ として特徴付けられる．ここで，確率変数 Z に対して，$\mathbb{E}[Z]$ は Z の期待値を表す.

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 $\boldsymbol{X}=(X_i)_{i=0}^{N-1}$ と $\boldsymbol{Y}=(Y_i)_{i=0}^{N-1}$ に対する，遅れ時間 ℓ の正規化相互相関関数は

$$r_N(\ell;\boldsymbol{X},\boldsymbol{Y})=\frac{1}{N}\sum_{i=0}^{N-1}X_iY_{i+\ell\,(\bmod N)}$$

で定義される．ここで，$\ell=0,1,\cdots,N-1$ である．整数 a と $b(\geq 1)$ に対して，$a\,(\bmod\ b)$ は法 b に関する a の最小剰余を表す．$\boldsymbol{X}=\boldsymbol{Y}$ のとき $r_N(\ell;\boldsymbol{X},\boldsymbol{X})$ を正規化自己相関関数と呼び，単に $r_N(\ell;\boldsymbol{X})$ で表す.

所望の $r_N(\ell;\boldsymbol{X})=\left(-2+\sqrt{3}\right)^\ell$ を有する系列 $\boldsymbol{X}$ を構成するために [8] で定義された Perron 数を導入する.

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，$\lambda>|\mu|$ が成り立つ．*Perron* 数全体の集合を $\mathbb{P}$ で表す.

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.

定理 1 (Lind [8]) $\lambda\in\mathbb{P}$ 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 $-2+\sqrt{3}$) しか持たないので，次数 2 を有する $\lambda\in\mathbb{P}$ 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，$\mathbb{Q}$ 上最小多項式は

$$f(t)=t^2-c_1t-c_2$$

で定義される．ここで，$c_1,c_2\in\mathbb{Z}$．多項式 $f(t)$ のコンパニオン行列は

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

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．マルコフ β 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 β 変換の $(c_1+1)\times(c_1+1)$ 隣接行列 A は

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

で与えられる.

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

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

で定義する．$n = 1, 2, \cdots$ に対して，変換 T の n 回反復 $T^n(x)$ は，$T^0(x) = x$ および $T^n(x) = T^{n-1}(T(x))$ により帰納的に定義される．このとき，$Z_n = \Psi(T^n(x))$ 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 $(Z_n)_{n=0}^{\infty}$ が生成される．斯くして，

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

を得る．ここで，$\overline{\lambda}$ は λ の代数的共役である．

条件 $0 < c_2 \leq c_1$ の下，方程式

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

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．

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

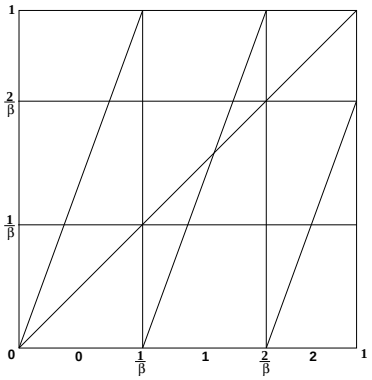

図 1: 傾き $\beta = 1 + \sqrt{3}$ を有するマルコフ β 変換.

このとき，相関特性は

$$\mathbb{E}[Z_0 Z_\ell] = \frac{1}{3} + \frac{2}{3}\left(-2 + \sqrt{3}\right)^\ell \ (\ell \geq 0)$$

となる．斯くして，相関特性 $\mathbb{E}[Z_0 Z_\ell]$ が定数と指数関数 $\left(-2 + \sqrt{3}\right)^\ell$ の線形和として表されるような，$\{1, -1\}$ に値を取るマルコフ連鎖系列 $(Z_n)_{n=0}^{\infty}$ をうまく得た．しかしながら，連鎖の定常分布は

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

で与えられ，一様分布でないため，

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

となり，所望の零でない.

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の指数関数部 $\left(-2 + \sqrt{3}\right)^\ell$ 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.

4 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 $\beta = 1 + \sqrt{3}$ を用いるとき，区間 $[0, 1)$ に属する実数 x の β 進展開は SFT $X_{\mathcal{F}} \subset \Sigma^{\mathbb{Z}}$ の右側無限列として与えられる．ここで $\Sigma = \{0, 1, 2\}$ および $\mathcal{F} = \{22\}$ である．実数 $x \in [0, 1)$ 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 $X_{\mathcal{F}}$ のグラフ表現 G は図 2 で与えられる．同時に，G は T の表現でもある．

初期グラフを $G = G^{[2]}$ として，G の高次辺グラフの列 $(G^{[n]})_{n=2}^{\infty}$ 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

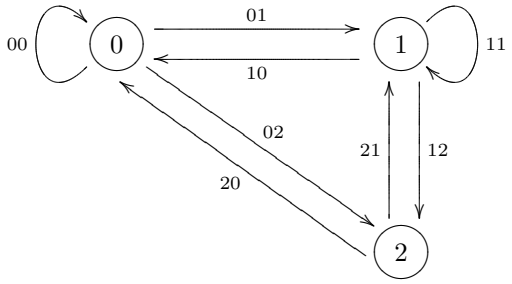

図 2: $X_{\{22\}}$ のグラフ表現 G.

$\beta = 1+\sqrt{3}$ 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，$n\ (\geq 3)$ 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．これを $H_3 \subsetneqq G^{[3]}$ で表す．任意の $n\ (\geq 3)$ に対して，$H_n \subsetneqq G^{[n]}$ となるのが確認される．

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 $|\mathcal{B}_n|$ は $|\mathcal{B}_n| = \beta^n + \overline{\beta}^n\ (n \geq 2)$ で与えられる [9]．ここで，$\overline{\beta} = 1-\sqrt{3}$ は β の代数的共役である．

以下，傾き $\beta = 1+\sqrt{3}$ 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 $\mathcal{L}(X_{\mathcal{F}}) \setminus \{\epsilon\}$ 上の全順序関係 $\leq$ を次で定義する：$\mathcal{L}(X_{\mathcal{F}})$ に属する任意の $u = u_1 \cdots u_m\ (m \geq 1)$ と $v = v_1 \cdots v_n\ (n \geq 1)$ に対して，$u \leq v$ は

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

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 $|\mathcal{B}_n|$ を表すのに L を用いる．L ブロック $v = v_1 v_2 \cdots v_L \in \{0,1,2\}^L$ に対して，ブロック符号 $\Phi : \{0,1,2\}^L \to \{1,-1\}$ を

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

で定義する．

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．即ち，$v = v_1 v_2 \cdots v_L \in \{0,1,2\}^L$ に対して，

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

斯くして，周期 L の周期列に対して，

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

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，$u^\infty = \cdots uuu \cdots$ である．

系列 $\boldsymbol{X}$ は，$\beta = 1+\sqrt{3}$ を有する離散化マルコフ β 変換に基づく，長さ $L = |\mathcal{B}_n|$ の，$\Sigma = \{0,1,2\}$ 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 $\boldsymbol{Y}$ が

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

により実現される．

長さ $|\mathcal{B}_n|$ 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，

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

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．

[10] 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 $0 \le \ell \le n-1$ 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 $r_{|\mathcal{B}_n|}(\ell;\boldsymbol{Y}) = \mathbb{E}[Z_0 Z_\ell] + O\left(\left(\frac{\overline{\beta}}{\beta}\right)^{n}\right)$ を示唆する．ここで，O はランダウの記号である．

5 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，および実現された最適二値マルコフ連鎖拡散符号の総数 $\widetilde{\nu_n}$ 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

$n=4$ 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 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 $|\mathcal{B}_n| = 56$ 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．この様にして，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．各々の図において，曲線は [11] で与えられた中心極限定理 (CLT) に基づく理論評価式を，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．同様にして，任意の長さの擬似乱数を得ることができる．

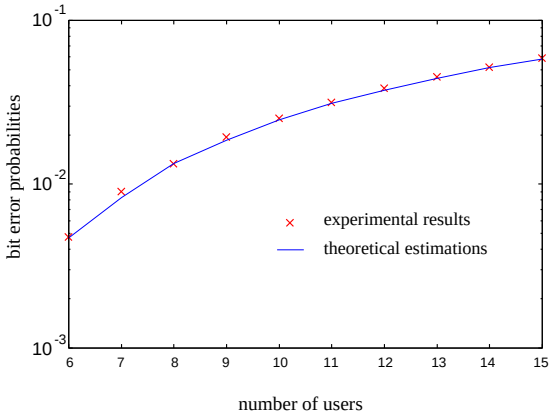

図 3: 系列長 56 のとき，ビット誤り生起確率のユーザ数依存性.

6 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，

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

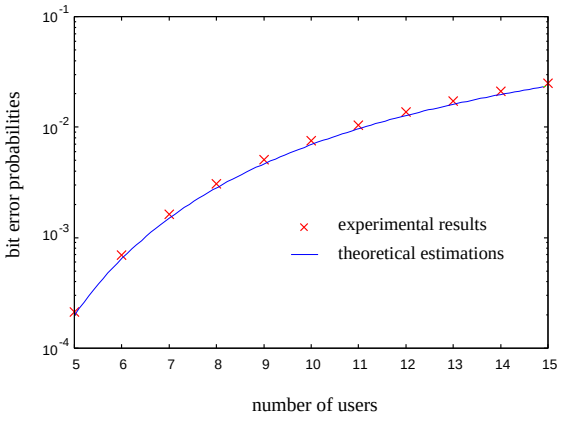

図 4: 系列長 32 のとき，ビット誤り生起確率のユーザ数依存性.

において，$\rho = -2 + \sqrt{3}$ の場合を考えた．ρ が一般の場合には (1) と同様に，

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

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．

簡単のため $c_1 + 1 = k$ とおく．離散化 β 変換により，$\{0, 1, \cdots, k-1\}$ 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．

貪欲算法による実数 $x \in [0, 1]$ の β 進展開を $\mathsf{d}_\beta(x)$ で表す．$|\mathcal{B}_n| = L$ とおく．L ブロック $v = v_1 v_2 \cdots v_L \in \{0, 1, \cdots, k-1\}^L$ 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．

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

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

7 結言

離散化 β-変換に基づく最大周期列ファミリーから，任意に指定された相関特性を有する最大周期列を実現する方法を与えた．さらに，得られた最大周期列の分布を均等分布に変換 (符号化) する方法も与えた．応用例として，スペクトル拡散多元接続 (SSMA) 通信システムを考え，本研究で得られた方法論により，ビット誤り生起確率に関して最適な二値マルコフ連鎖拡散符号を実現した．このとき，所望の最適符号は，離散化 β-変換に基づく最大周期列を用いて生成される．得られた最大周期列が均等分布を有することは容易に確認された．指定された相関特性と，生成された最大周期列が有する相関特性との誤差評価は重要な課題である．そのために，離散化 β-変換に基づく最適二値マルコフ連鎖拡散符号の，時間 $t = 0$ 前後の自己相関特性を陽に求めた．得られた理論結果を用いて，最大周期列の相関特性と，確率論に基づく連続的な特性とを比較し，超離散化による誤差を評価した．誤差は実用上無視できることを確認した．生成された最適二値マルコフ連鎖拡散符号を用いた SSMA 通信の

数値模擬実験を行い，通信の誤り生起確率を調査した．得られた数値実験結果と，確率論が与える理論値との比較を行い，両者が良く一致することを確認した．数値実験において，任意の長さの擬似乱数生成法も提案した．

参考文献

[1] H. Fujisaki, "Design of Optimum M-Phase Spreading Sequences of Markov Chains," *IEICE Trans. on Fundamentals*, vol. E90-A, pp. 2055–2065, 2007.

[2] H. Fujisaki, "Discretized Markov Transformations – An Example of Ultradiscrete Dynamical Systems –," *IEICE Trans. Fundamentals*, vol. E88-A, pp.2684–2691, 2005.

[3] 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.

[4] D. Lind and B. Marcus, *Symbolic Dynamics and Coding*, Cambridge Univ. Press, 1995.

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

[6] 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.

[7] 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.

[8] 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.

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

[10] 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.

[11] 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.

＜発　表　資　料＞

題　　名	掲載誌・学会名等	発表年月
Correlational Properties of the Full-Length Sequences Based on the Discretized Markov Transformations	Proc. of the the 2016 Int. Symp. on Information Theory and its Applications (ISITA2016), pp. 637-641	2016.11
A Realization of Optimum Binary Spreading Sequences of Markov Chains Based on Discretized β-transformations	Proc. of the 2016 Int. Symp. on Nonlinear Theory and its Applications (NOLTA2016), pp. 253-256	2016.11
A Realization of Optimum Binary Spreading Sequences of Markov Chains Based on Discretized β-transformations	Proc. of the 39th Symposium on Information Theory and its Applications (SITA2016), pp. 130-135	2016.12
On the topological entropy of the discretized Markov β-transformations	IEICE Trans. on Fundamentals, E99-A, no.12, pp. 2238-2247	2016.12
Correlational Properties of the Full-Length Sequences Based on the Discretized Markov β-transformations	NOLTA, IEICE, vol. 8, no.1, pp. 67-78	2017.1