超離散力学系に基づく位相シフトフリー M-相スペクトル拡散符号の実現とその応用

藤 崎 礼 志　　金沢大学理工研究域講師

概要

位相シフトフリー M-相スペクトル拡散符号を実現する区分的線形マルコフ変換を含む，区分的単調増加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る．現在，最大周期列の総数を計算する既知のアルゴリズムの計算量は指数関数的オーダである．最大周期列の総数を計算することなく，全ての最大周期列を生成するという意味において，提案するアルゴリズムは効率的である．典型例として，アルゴリズムを全ての de Bruijn 系列の生成に応用する．

1 緒言

電子計算機をインフラ基盤とする，現代社会において，最大周期列の応用範囲は広大であり，暗号系，通信系，計算機科学系，経済 (ファイナンス) 系と多岐にわたる．最大周期列を生成するために， LFSR (線形フィードバックシフトレジスタ (linear feedback shift register)) が通常用いられている．一方，一次元エルゴード的変換のカオス力学系におけるランダム性の観点から，離散化された Bernoulli 変換に基づく系列が提案された [1]–[2]. 後者はファミリーサイズ (系列の総数) という点で非常に優れている．例えば，長さ 2^n の二値系列に対して，前者の総数は $2^n/n$ よりずっと小さいが，有名な de Bruijn 系列の総数は $2^{2^{n-1}-n}$ であることが知られている．

先の研究 [3] において，離散化されたマルコフ変換を一般的に定義し，離散化されたマルコフ変換に基づく最大周期列の総数を与えるアルゴリズムを提案した．離散化されたマルコフ変換とは，変換から決定されるマルコフ分割に属する部分区間の置換であり，超離散系 [4] の例とみなすことができる．この観点から， de Bruijn 系列は単に離散化マルコフ変換から得られる最大周期列の特別な例である．実際，それらは，離散化二進変換の部分族に基づく最大周期列である．

マルコフ変換が与えられると， [3] で定義されたように，可算個の離散化マルコフ変換を得る．離散化マルコフ変換を固定すれば， [3] で得られたアルゴリズムにより，離散化変換に基づく最大周期列の総数を計算することができる．

最大周期列の総数がわかれば，それらを全て生成するような，アルゴリズムを与えるという問題を考察するのは自然であろう．この問題は単に数学的問題として興味深いだけでなく，実用的にも重要である．というのは，先に述べたように，最大周期列の応用は広範囲にわたるからである．しかしながら，この問題は難問である．実際， de Bruijn 系列の場合，単一の系列もしくはいくつかの系列を生成するアルゴリズムは数多く提案されているものの，系列を全て生成するアルゴリズムは数えられる位しか存在しない [5]–[6].

最近，いくつかの最大周期列が既に与えられたという仮定の下，系列を決定する置換の互換によって， $r = 2$ の場合に de Bruijn 系列を含む，離散化された $r(\geq 2)$-進変換に基づき，相対的に多くの系列を生成するアルゴリズムが提案された [7]. これは，全てではないものの，比較的多くの系列を効率的に生成する，興味深いアルゴリズムである．

本研究では，最大周期列を全て生成するようなアルゴリズムを与えるという問題に取り組む．そのために，区分的単調増加マルコフ変換を定義し，離散化された区分的単調増加マルコフ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る．

区分的単調増加マルコフ変換は，既約かつ非周期的マルコフ変換の集合の部分集合である．しかしながら，それは， [8] において本研究者が先に提案した位相シフトフリー M-相スペクトル拡散符号を実現する区分的線形マルコフ変換を含む．さらに， Bernoulli 変換だけでなく，黄金平均変換， Kalman のマルコフ変換 [9]，および [10] において定義された $r(\geq 2)$-方有尾シフト変換 ($r(\geq 2)$-way tailed shift transformations) を含むので，実用的に十分広いクラスである．

現在，最大周期列の総数を計算する既知のアルゴリズムの計算量は指数関数的オーダである．したがって，最大周期列の総数を計算することなく，全ての最大周期列を生成するという意味において，本研究で提案するアル

ゴリズムは効率的である．

さらに， de Bruijn 系列は離散化された区分的単調増加マルコフ変換から得られる最大周期列に含まれるので，本研究で提案する有界単調真理値表アルゴリズムを全ての de Bruijn 系列の生成に応用する．

2 de Bruijn 系列の生成に関する従来の結果

[3] において，離散化されたマルコフ変換を定義し，離散化されたマルコフ変換に基づく最大周期列の総数を与えるアルゴリズムを発見した．まず初めに，その概略を述べる．

重複を避けるために，本報告では， [3] で定義した技術的用語を自由に用いる．

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 $\mathcal{P}$ が与えられる．このとき，各部分区間 $I \in \mathcal{P}$ に一つの辺 $a(I)$ が対応し，辺 $a(I)$ の集合 $\mathcal{A}$ を得る． $\mathcal{P}$ の要素の各順序対 (I, J) に対して， $a(I)$ から $a(J)$ へ隣接する一つの頂点 $v(I, J)$ が許されるのは丁度 $J \subset T|_I(I)$ のときである．これより，マルコフ連鎖を表現する有向グラフ $G = (\mathcal{V}, \mathcal{A})$ 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．

上に述べた， $\mathcal{P}$ と $\mathcal{A}$ の間の一対一対応の下で， $\mathcal{B}$ に対応する分割 $\mathcal{Q}$ を得る．このとき，離散化されたマルコフ変換 $\widehat{T}$ 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 $\widehat{T} : \mathcal{Q} \to \mathcal{Q}$ として定義される．結局，離散化されたマルコフ変換から生成される最大周期列の総数は， H のアドミタンス行列 C の余因子 C_{11} により与えられる．

この定義により， de Bruijn 系列は，離散化されたマルコフ変換から得られる最大周期列の特別な例となる．

次に，離散化された黄金平均変換の例を手短に述べる．図 1 に黄金平均変換に関するマルコフ分割 $\mathcal{P}$ の例を示す．各分割は長さ 5 のブロックにより表現される： $\mathcal{P} = \{00000, 00001, 00010, 00100, 00101, 01000, 01001, 01010, 10000, 10001, 10010, 10100, 10101\}$． 0 と 1 をそれぞれ区間 $[0, 1/\beta)$ と $[1/\beta, 1]$ に同一視することにより，各二値ブロック $a_1a_2 \cdots a_5$ は筒集合 $\{x \in [0,1] : T^{i-1}(x) \in a_i, 1 \le i \le 5\}$ に対応することに注意する．ここで， β は黄金平均数 $(1 + \sqrt{5})/2$ であり， T は黄金平均変換である．マルコフ分割 $\mathcal{P}$ が与えられると，黄金平均変換のグラフ表現 G が，図 2 の様に，直ちに得られる． $\mathcal{P}$ に属する各分割は G に属する辺に対応する．図 2 の G はオイラーグラフでないことに注意されたい．辺 10001 と 10101 を消去することにより，図 3 に描かれた様に，最大辺数を有する G の全域オイラー部分グラフ H を得る． H の辺集合は分割 $\mathcal{Q} = \{00000, 00001, 00010, 00100, 00101, 01000, 01001, 01010, 10000, 10010, 10100\}$ を定める．辺の隣接に随伴する， $\mathcal{Q}$ の置換により，離散化された黄金平均変換が定義される．ここで，一般に， $\mathcal{Q}$ の置換全体の集合に比べると，少ない量だけしか離散化されたマルコフ変換を与えることができないに注意されたい[1]． H の 11×11 アドミタンス行列 C の余因子 C_{11} を計算することにより，離散化された黄金平均変換から得られる最大周期列は二であることがわかる．ここで行列の大きさ 11 は $\mathcal{Q}$ の濃度に由来する．離散化された黄金平均変換の例を図 4 に示す．図 4 において陰をつけた四角形が $\mathcal{Q}$ の置換の一対一対応を定める．この場合，最大周期列 00000100101 を生成する．

次に，全ての de Bruijn 系列を生成する，これまでに知られているアルゴリズムを検討する．

各正の整数 n に対して，長さ 2^n の de Bruijn 系列が丁度 $2^{2^{n-1}-n}$ 個存在する [11]-[12]． de Bruijn による，この事実の証明の最も重要な部分は，グラフ G_n と G_{n+1} の間の次の関係に気付いたことにある：

$$G_{n+1} = G_n^*. \tag{1}$$

ここで， $G_n = (\mathcal{V}_n, \mathcal{A}_n)$ $(n > 1)$ は $\mathcal{V}_n = \{0,1\}^{n-1}$ と $\mathcal{A}_n = \{0,1\}^n$ を有する de Bruijn グラフである．辺 $a_1a_2 \cdots a_n \in \mathcal{A}$ は $a_1a_2 \cdots a_{n-1}$ から $a_2a_3 \cdots a_n$ へ隣接する． G_n^* は G_n の辺有向グラフである．

関係 (1) を用いた，全ての de Bruijn 系列を生成するアルゴリズムが [6] に述べられている．しかしながら，このアルゴリズムは，長さ 2^n の全ての de Bruijn 系列を生成するために， $2^{2^{n-2}}$ ビットの初期記憶を常に必要とする．これは，要求される記憶量の観点から非常に高価である．

また，残念ながら， (1) の様な関係は，一般に成立しないので，このアルゴリズムを一般の離散化されたマルコフ変換から得られる最大周期列の生成に応用することはできない．実際， [3] において，離散化された黄金平均変換に対して， (1) が成り立たないことを示した．

[1] 実際，全ての de Bruijn 系列は 2^{2^n-n} 個であるのに対して，それらの辺の全ての置換は $2^n!$ 個である．

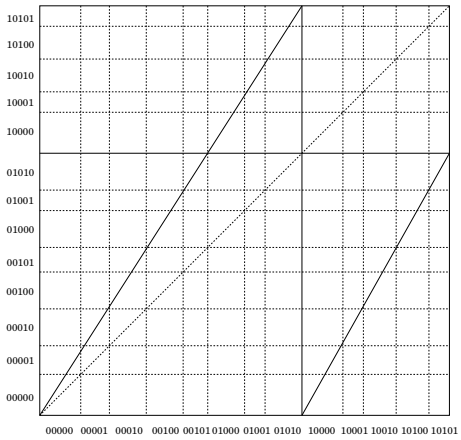

図 1: An example of Markov partition $\mathcal{P}$ with respect to the golden mean transformation.

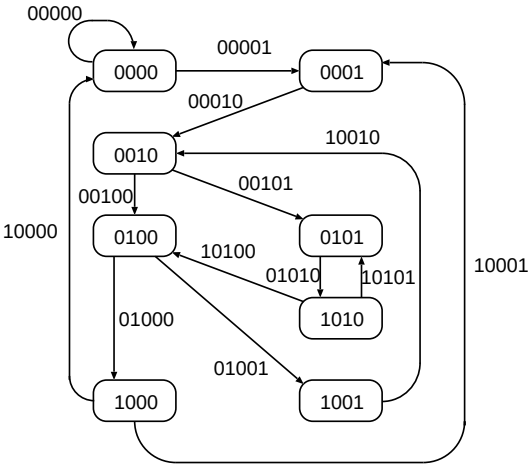

図 2: A graph representation G of the golden mean transformation.

全ての de Bruijn 系列を生成するが，(1) を使用しない既知のアルゴリズムを述べるために，[5] に従い，次を導入する：

定義 1 *優先関数 p は $n-1$ $(n \geq 2)$ 変数 $k(\geq 2)$-次ベクトル値関数であって，k-アルファベット $\{0,1,\cdots,k-1\}$ からの各選択 $a_1, a_2, \cdots, a_{n-1}$ に対して，$(p_1(a_1,\cdots,a_{n-1}),\cdots,p_k(a_1,\cdots,a_{n-1}))$ は $0,\cdots,k-1$ の再配列である.*

特に，二値アルファベットに対して，$p_1(a_1,\cdots,a_{n-1}) \equiv 1$ ならば，p は 1 優先関数と呼ばれる [6]．引き返し法 (backtracking) と共に 1 優先関数を用いて，全ての de Bruijn 系列を生成するアルゴリズムが [6] に紹介されている．結果的に，長さ 2^n の単一の de Bruijn 系列を生成するためには，$n2^n$-ビットの線形のオーダの記憶を常に必要とし，少なくともオーダ $O(2^n)$ の演算が要求される．ここで，O は Landau の記号である．したがって，全ての de Bruijn 系列を生成するためには，オーダ $O(2^{2^{n-1}})$ の演算が全体として必要である．実際，1 優先関数を用いるアルゴリズムは，要求される記憶量の観点から非常に高価であることが [6] で指摘されている．

優先関数は常にうまく定義されるとは限らないので，再びこのアルゴリズムを一般の離散化されたマルコフ変換から得られる最大周期列の生成に応用することはできない．実際，離散化された黄金平均変換に対して，常に $(p_1(a_1,\cdots,a_{n-2},1), p_2(a_1,\cdots,a_{n-2},1)) = (0,0)$ を得るが，これは $0,1$ の再配置ではない.

これまでのところ，筆者が知り得る限り，全ての de Bruijn 系列を生成するアルゴリズムはそれ程知られていない．また，それらは de Bruijn 系列の性質に強く依存する．したがって，一般の離散化されたマルコフ変換か

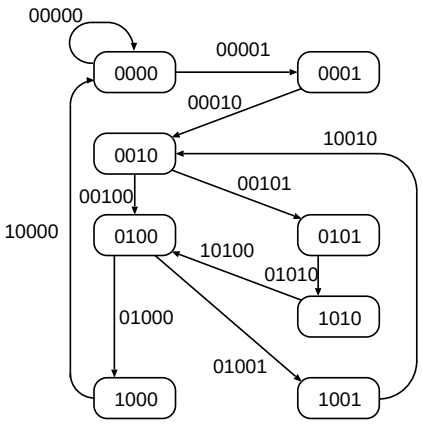

図 3: The Eulerian subgraph H spanning G with maximal number of arcs.

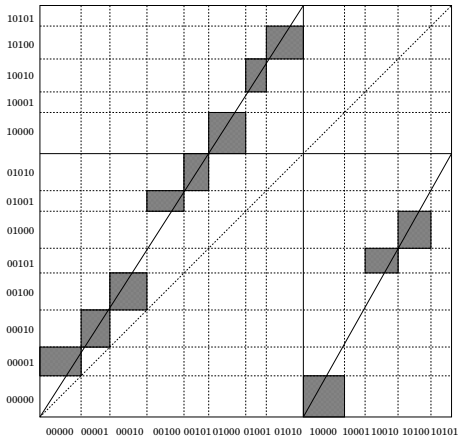

図 4: An example of the discretized golden mean transformation.

ら得られる最大周期列の生成に直接適用することはできない．ゆえに，本研究で提案するアルゴリズムは新規であると同時に自明でない．

3 離散化されたマルコフ変換の集合における距離関数

議論を簡単にするため，$k(\geq 2)$-アルファベットを二値アルファベット $\{0,1\}$ に制限する．この簡単化は，$k>2$ の場合に対して，$k!$ 個の場合を数え上げることを除いて，数学的処理を本質的に変えない．

与えられた離散化マルコフ変換に基づき，全ての最大周期列を生成するためには，章 2 の冒頭で手短に概説した [3] の結果により，最大辺数を有する G の全域オイラー部分グラフ $H=(\mathcal{V},\mathcal{B})$ から始めることができる．

H はオイラーグラフであるので，連結であり，すべての頂点は偶数次数を持つ．これより，二値アルファベットの場合，各頂点の次数は 2 または 4 である．$\mathcal{V}=\mathcal{U}\cup\mathcal{W}$ は直和であるとする．ここで，$\mathcal{U}$ は次数 2 の頂点の集合であり，$\mathcal{W}$ は次数 2 の頂点の集合である．

$\mathcal{U}=\{u_1,u_2,\cdots,u_{\sharp\mathcal{U}}\}$ および $\mathcal{W}=\{w_1,w_2,\cdots,w_{\sharp\mathcal{W}}\}$ とする．ここで，集合 A に対して，$\sharp A$ は A の濃度を表す．$\sharp\mathcal{V}=\sharp\mathcal{U}+\sharp\mathcal{W}$ に注意する．

表現を簡明にするために，各頂点は，二値ブロックにより，$u_j=a_1^{(j)}a_2^{(j)}\cdots a_{|u_j|}^{(j)}\in\{0,1\}^{|u_j|}$, $1\leq j\leq\sharp\mathcal{U}$ および $w_i=b_1^{(i)}b_2^{(i)}\cdots b_{|w_i|}^{(i)}\in\{0,1\}^{|w_i|}$, $1\leq i\leq\sharp\mathcal{W}$ と表現されるとしよう．ブロック w に対して，$|w|$ は w の長さを表す．0 および 1 をそれぞれ区間 $[0,x_1)$ および $[x_1,1]$ と同一して，各二値ブロック u_j または w_i はそれぞれ筒集合 $\{x\in[0,1]\colon T^{i-1}(x)\in a_m^{(j)},1\leq m\leq|u_j|\}$ または $\{x\in[0,1]\colon T^{i-1}(x)\in b_m^{(i)},1\leq m\leq|w_i|\}$ に対

応する．ここで，$\{[0,x_1),[x_1,1]\}$ は，次の節で定義される，離散化される変換 T の分割である．ただし，この仮定が常に成立するわけではないことが知られている．実際，[3] で示された図 3 において考察された離散化二進変換の全ての部分区間は，有限の二値ブロックで表現することはできない．しかしながら，その場合は表記が煩雑になるだけであり，任意の既約かつ非周期的マルコフ変換に対して，下記のオイラーグラフの真理値表を定義することができる．

各頂点 u_j は次数 2 を持つので，u_j は $\mathcal{B}$ に属する二つの辺 $a^{(j)}u_j$ と $u_jb^{(j)}$ を一意に決定する．ここで，$a^{(j)},b^{(j)}\in\{0,1\}$.

今，H において，二つの辺 $0w_i$ と $1w_i$ は w_i で終端となる．一方，w_i0 と w_i1 は w_i で開始する．経路が $0w_i0$ を許すとき，これはその経路が $1w_i1$ を許す (すなわち，その経路が $0w_i0\cdots1w_i1$ を許す) かまたは他の経路が $1w_i1$ を許す (すなわち，その経路が $1w_i1$ を許さない) ときであり，$t_i=0$ と置く．一方，経路が $0w_i1$ を許すとき，これはその経路が $1w_i0$ を許す (すなわち，その経路が $0w_i1\cdots1w_i0$ を許す) かまたは他の経路が $1w_i0$ を許す (すなわち，その経路が $1w_i0$ を許さない) ときであり，$t_i=1$ と置く．これより，$\sharp\mathcal{W}$-次ベクトル $t=(t_1,t_2,\cdots,t_{\sharp\mathcal{W}})\in\{0,1\}^{\sharp\mathcal{W}}$ を得る．これを H の真理値表 (truth table) と呼ぶ．

例 1 *de Bruijn グラフ $G_n=(\{0,1\}^{n-1},\{0,1\}^n)$ $(n>1)$ の真理値表は $(t_1,t_2,\cdots,t_{n-1})\in\{0,1\}^{n-1}$ で与えられる．*

例 2 *離散化された黄金平均変換に随伴する図 3 のグラフ H の真理値表は $(t_1,t_2,t_3)\in\{0,1\}^3$ で与えられる．*

H の真理値表 t により，置換 $\sigma_t\colon\mathcal{B}\to\mathcal{B}$ が

$$\sigma_t=\begin{pmatrix} a^{(1)}u_1 & \cdots & a^{(\sharp\mathcal{U})}u_{\sharp\mathcal{U}} & 0w_1 & \cdots & 0w_{\sharp\mathcal{W}} & 1w_1 & \cdots & 1w_{\sharp\mathcal{W}} \\ u_1b^{(1)} & \cdots & u_{\sharp\mathcal{U}}b^{(\sharp\mathcal{U})} & w_it_1 & \cdots & w_it_{\sharp\mathcal{W}} & w_i\overline{t_1} & \cdots & w_i\overline{t_{\sharp\mathcal{W}}} \end{pmatrix}$$

で定義される．これは，離散化マルコフ変換を表現する．$a\in\{0,1\}$ に対して，$\overline{a}$ は a の二値補数を表す．すなわち，$\overline{0}=1$ および $\overline{1}=0$.

次に，離散化マルコフ変換の集合における距離関数 d を，$t,t'\in\{0,1\}^{\sharp\mathcal{W}}$ に対して，$d(\sigma_t,\sigma_{t'})=d_H(t,t')$ で定義する．ここで，d_H は t と t の Hamming 距離，すなわち，t と t の異なる要素数である．

次の補題により，提案するアルゴリズムにおける次のステップが定まる：

補題 1 *σ_t は，最大周期列を生成する離散化マルコフ変換である，すなわち，σ_t それ自身が全巡回置換 (full cycle) であるとする．このとき，$d(\sigma_t,\sigma_{t'})=1$ を満たす任意の離散化マルコフ変換 $\sigma_{t'}$ は全巡回置換になり得ない．*

この補題は，提案するアルゴリズムの Step 3) において，線形オーダの効率的な計算を実行する指針を与える．

4 有界単調真理値表アルゴリズム

本報告に渡って，w_i を非負整数に対する底 2 を用いた位取り表記と見做し，$w_1<w_2<\cdots<w_{\sharp\mathcal{W}}$ を仮定する．

これまで，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．この節においては，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 を区分的単調増加マルコフ変換 (piecewise-monotone-increasing Markov transformation) 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．緒言で述べたように，それは，Bernoulli 変換だけでなく，黄金平均変換，Kalman のマルコフ変換 [9]，および [10] で定義された $k(\geq 2)$-方有尾シフト変換を含む．議論を簡単にするために，分割の数 k はアルファベットの大きさ k に対応すると仮定する．先の節の様に，簡単のため，$k=2$ の場合を考える．

主要ステップに進む前に，もう一つの準備が必要である：

Step 0) $i=1,2,\cdots,\sharp\mathcal{W}$ に対して，辺 $0w_i$ が $0w_i=w_i0$ を満たすならば，$t_i=1$ と置く．また，辺 $1w_i$ が $1w_i=w_i1$ を満たすならば，$t_i=0$ と置く．これにより，単一の辺の巡回置換が予め避けられる．離散化され

る変換は既約かつ非周期的であるので，いずれかが少なくとも一度起こるが，両方は高々一度しか起こらない．以下，その様な t_i を固定する． t からその様な固定された t_i を全て除去し， t_i の残りの成分の座標の番号を付け直した後， $\sharp\mathcal{W}-1$- または $\sharp\mathcal{W}-2$-次ベクトルを得る．それを $\tilde{t}=(\tilde{t}_1,\cdots,\tilde{t}_W)$ で表す． $\tilde{t}$ を縮約真理値表 (contracted truth table) と呼ぶ．定義により，一対一対応 $\gamma\colon t\mapsto\tilde{t}$ および $\gamma^{-1}\colon\tilde{t}\mapsto t$ を得る．

例 3 *de Bruijn グラフ* $G_n=(\{0,1\}^{n-1},\{0,1\}^n)$ $(n>1)$ *の縮約真理値表は，* $(\tilde{t}_1,\tilde{t}_2,\cdots,\tilde{t}_{n-3})(\in\{0,1\}^{n-3})$ *で与えられる．これは，真理値表* $(1,\tilde{t}_1,\tilde{t}_2,\cdots,\tilde{t}_{n-3},0)$ *に対応する．*

例 4 *離散化された黄金平均変換に随伴する図 3 のグラフ* H *の縮約真理値表は，* $(\tilde{t}_1,\tilde{t}_2)(\in\{0,1\}^2)$ *で与えられる．これは，真理値表* $(1,\tilde{t}_1,\tilde{t}_2)$ *に対応する．*

次のサブルーチンは，提案するアルゴリズムにおいて，重要な役割を果たす．

Step B1) m $(1<m\le\sharp\mathcal{U}+2\sharp\mathcal{W}=\sharp\mathcal{B})$ は

$$\sigma_t^m(0w_1)=0w_1$$

を満たす最小の周期であるとする．各 i $(1\le i\le\sharp\mathcal{W})$ に対して， n $(1\le n\le m\le\sharp\mathcal{B})$ が存在して， $\sigma_t^n(0w_1)=0w_i$, を満たすならば， $r_i=1$ と置く．そうでないならば， $r_i=0$ と置く．これより， $r=(r_1,\cdots,r_{\sharp\mathcal{W}})$ を得る．全ての i $(1\le i\le\sharp\mathcal{W})$ に対して $r_i=1$ ならば，全巡回置換 σ_t を得，元に戻る．そうでないならば， B2) へ進む．

Step B2) $\tilde{r}=\gamma(r)$ および $\tilde{r}=(\tilde{r}_1,\cdots,\tilde{r}_W)$ と置く． $R_0=\max\{i\colon\tilde{r}_i=0,\ 1\le i\le W\}$ および $R_1=\max\{i\colon\tilde{r}_i=1,\ 1\le i\le W\}$ とする． n $(1\le n\le m\le\sharp\mathcal{B})$ が存在して， $\sigma_t^n(0w_1)=1w_{\sharp\mathcal{W}}$ を満たすならば， $t=\gamma^{-1}(\tilde{t}_1,\cdots,\tilde{t}_{R_0-1},\overline{\tilde{t}_{R_0}},\tilde{t}_{R_0+1},\cdots,\tilde{t}_W)$ と置き， B1) へ進む．そうでないならば， $t=\gamma^{-1}(\tilde{t}_1,\cdots,\tilde{t}_{R_1-1},\overline{\tilde{t}_{R_1}},\tilde{t}_{R_1+1},\cdots,\tilde{t}_W)$ と置き， B1) へ進む．

以下， $\tilde{t}$ を非負整数に対する底 2 を用いた位取り表記と見做す．次の補題は提案するアルゴリズムの本質的な構成要素である：

補題 2 $\widetilde{\mathcal{T}}=\{\tilde{t}\in\{0,1\}^W\colon\sigma_t=\sigma_{\gamma^{-1}(\tilde{t})}$ *は全巡回置換である* $\}$ *とする．* $\tilde{t}=(\underbrace{0,\cdots,0}_{W})$ *として， t を B1) に入力するならば，その縮約真理値表* $\tilde{t}$ *が* $\widetilde{\mathcal{T}}$ *の下界であるような，全巡回置換* σ_t *を得る．一方，* $\tilde{t}=(\underbrace{1,\cdots,1}_{W})$ *として， t を B1) に入力するならば，その縮約真理値表* $\tilde{t}$ *が* $\widetilde{\mathcal{T}}$ *の上界であるような，全巡回置換* σ_t *を得る．*

節 2 で述べた様に，各正の整数 n に対して， $2^{2^{n-1}-n}$ 個の長さ 2^n の de Bruijn 系列が存在する．これより，全ての de Bruijn 系列を生成する際，生成された相異なる系列の個数を確認することによって，いつアルゴリズムが停止するかを判定する条件を直ちに得る．一方，離散化されたマルコフ変換から最大周期列を生成する際，それ程単純ではない．同様に，最大周期列の総数を知りたい場合， H のアドミタンス行列 C の余因子 C_{11} を計算する必要がある．

$N\times N$ 行列に対して，余因子を計算するのは，漸近的に $O((N-1)^{2.376})$ の複雑度であることが知られている [13]．離散化マルコフ変換に対して， $N=\sharp\mathcal{B}$ は底 2 の指数関数オーダであることに注意する．

補題 2 は，最大周期列の総数を計算することなく，提案するアルゴリズムが停止することを保証するので，非常に有用である．

今，主要ステップに進む準備が整った．主要ステップを以下に示す．

Step 1)(上界の計算) t を $\tilde{t}=(\underbrace{1,\cdots,1}_{W})$ として B1) に進む． B1) から戻って来た後， σ_t を出力し， $v=(v_1,\cdots,v_W)=\tilde{t}$ と置く． 2) に進む．

Step 2) t を $\tilde{t}=(\underbrace{0,\cdots,0}_{W})$ として B1) に進む． B1) から戻って来た後， σ_t を出力し， $\tilde{t}^{(1)}=(\tilde{t}_1^{(1)},\cdots,\tilde{t}_W^{(1)})=\tilde{t}$ と置く． $i=1$ と置いて 3) に進む．

Step 3) $\tilde{t}_W^{(i)}=0$ ならば， $\tilde{t}=\tilde{t}^{(i)}+11$ と置く． $\tilde{t}_W^{(i)}=1$ ならば， $\tilde{t}=\tilde{t}^{(i)}+1$ と置く．ここで，加法は， $\tilde{t}$ と $\tilde{t}^{(i)}$ を非負整数に対する底 2 を用いた位取り表記と見做した，二進数系における演算である． B1) に進む． B1) から戻って来た後， 4) に進む．

Step 4) $\tilde{t} < \upsilon$ ならば，σ_t を出力する．$\tilde{t}^{(i+1)} = (\tilde{t}_1^{(i+1)}, \cdots, \tilde{t}_W^{(i+1)}) = \tilde{t}$ と置く．$i = i+1$ と置いて 3) に進む．$\tilde{t} = \upsilon$ ならば，停止する．

次の注意のために，提案するアルゴリズムを有界単調真理値表 (bounded monotone truth-table) アルゴリズムと呼ぶ．

注 1 *結果として得られる縮約真理値表の列は有界単調増加である：*

$$\tilde{t}^{(1)} < \tilde{t}^{(2)} < \cdots \leq \upsilon.$$

5 全ての De Bruijn 系列生成への応用

提案したアルゴリズムが正しく動作することを実証するために，この章では，アルゴリズムを，長さ 2^n の de Bruijn 系列を全て，$2^{2^{n-1}-n}$ 個生成するのに応用する．その前に，離散化マルコフ変換に基づく全ての最大周期列を生成する簡単な例を手短かに述べる．

5.1 離散化黄金平均変換に基づく全最大周期列の生成

例 4 で見たように，離散化された黄金平均変換に随伴する図 3 のグラフ H の縮約真理値表は，$(\tilde{t}_1, \tilde{t}_2)(\in \{0,1\}^2)$ で与えられる．これは，真理値表 $(1, \tilde{t}_1, \tilde{t}_2)$ に対応する．以下，二値ブロック $\tilde{t}_1\tilde{t}_2$ を二値ベクトル $(\tilde{t}_1, \tilde{t}_2)$ と見做す．

サブルーチン B1)–B2) を用いて，ベクトル 11 により，上界 $\upsilon = 10$ を得る．同様に，初期ベクトル 00 により，下界 $\tilde{t}^{(1)} = 01$ を得る．このとき，提案したアルゴリズムは，次の様に，縮約真理値表の有界単調増加列を生成する：

$$\tilde{t}^{(1)} = 01 < 10 = \upsilon,$$

これは，節 2 で考察した離散化黄金平均変換に基づく，相異なる二つの最大周期列 00000100101 および 00000101001 を与える．

5.2 全 De Bruijn 系列の生成

今，全 de Bruijn 系列の生成を考える．

$n = 4$ の場合，長さ 2^4 の de Bruijn 系列は全部で 16 個存在する．単一の辺の巡回置換を予め避けるてめ，例 3 の様に，その真理値表を $(1, t_2, t_3, \cdots, t_7, 0) \in \{0,1\}^8$ で定義する．これより，縮約真理値表 $\tilde{t} = (\tilde{t}_1, \cdots, \tilde{t}_6)$ を得る．以下，二値ブロック $\tilde{t}_1 \cdots \tilde{t}_6$ を二値ベクトル $(\tilde{t}_1, \cdots, \tilde{t}_6)$ と見做す．

サブルーチン B1)–B2) を用いて，ベクトル $\underbrace{1\cdots1}_{6}$ により，上界 $\upsilon = 111110$ を得る．同様に，初期ベクトル $\underbrace{0\cdots0}_{6}$ により，下界 $\tilde{t}^{(1)} = 000111$ を得る．このとき，提案したアルゴリズムは，次の様に，縮約真理値表の有界単調増加列を生成する：

$$\begin{aligned}\tilde{t}^{(1)} = 000111 &< 001110 < 010011 < 010110 < 010101 < 011010 < 011100 < 011111 \\ &< 100011 < 101010 < 110001 < 110010 < 110111 < 111000 < 111011 < 111110 = \upsilon,\end{aligned}$$

これは，相異なる 16 個の de Bruijn 系列を与える．

6 結言

位相シフトフリー M-相スペクトル拡散符号を実現する区分的線形マルコフ変換を含む，区分的単調増加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．提案したアルゴリズムは，最大周期列の総数を計算することなく，全ての最大周期列を生成するという意味において，効率的である．また，1 優先関数を使用しないので，計算時間と記憶量の観点から，1 優先関数を使用するアルゴリズムに比べて経済的である．提案したアルゴリズムを全ての de Bruijn 系列の生成に応用した．

参考文献

[1] N. Masuda and K. Aihara, "Chaotic cipher by finite-state baker's map," *Trans. of IEICE*, vol. 82-A, pp.1038–1046, 1999 (in Japanese).

[2] A. Tsuneda, Y. Kuga, and T. Inoue, "New Maximal-Period Sequences Using Extended Nonlinear Feedback Shift Registers Based on Chaotic Maps," *IEICE Trans. on Fundamentals*, vol. E85-A, pp.1327–1332, 2002.

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

[4] R. Hirota and D. Takahashi, *Discrete and Ultradiscrete Systems*, Kyoritsu Shuppan, 2003.

[5] S. W. Golomb, *Shift Register Sequences*, Revised Edition, Aegean Park Press, 1982.

[6] H. Fredricksen, "A Survey of Full Length Nonlinear Shift Register Cycle Algorithm," *SIAM Review*, vol.24, pp. 195–221, 1982.

[7] D. Yoshioka and A. Tsuneda, "On generation of pseudochaotic sequences obtained by discretized chaos maps," *Proc. of NOLTA 2007*, pp. 136–139, 2007.

[8] H. Fujisaki and H. Sugimori, "Phase-Shift-Free M-Phase Spreading Sequences of Markov Chains," IEEE Trans. on Circuit and Systems Part I, Vol. 55, Issue: 3 pp. 876-882, 2008.

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

[10] 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.

[11] N. G. de Bruijn, "A Combinatorial Problem," *Nederl. Akad. Wetensch. Proc.*, vol. 49, pp.758–764, 1946.

[12] C. Flye Sainte-Marie, "Solution to problem number 58," *L'Intermediare des Mathematiciens,*, vol. 1, pp. 107–110, 1894.

[13] J. R. Bunch and J. Hopcroft, "Triangular factorization and inversion by fast matrix multiplication," *Mathematics of Computation*, vol. 28, pp. 231–236, 1974.

＜発　表　資　料＞

題　　名	掲載誌・学会名等	発表年月
An Algorithm For Generating All Full-Length Sequences Which Are Based On Discretized Markov Transformations	Proc. of the 2009 Int. Symp. on Nonlinear Theory and its Applications, pp. 191-194	2009.10
Entropy of the Induced Transformations Associated with the Interval Algorithm	Proc. of the IEEE Int. Symp. on Information Theory, pp. 2056-2060	2009.6
On Auto-Correlation Values of de Bruijn Sequences	Proc. of the 2009 Int. Symp. on Nonlinear Theory and its Applications, to appear	2010.9
On Embedding of Shifts of Finite Type into the Golden-Mean-Dyck Shift	Proc. of the 2010 Int. Symp. on Information Theory and its Applications and the 2020 Int. Symp. on Spread Spectrum Techniques and Applications, to appear	2010.10