超離散力学系に基づく最大周期列の相関特性解析とそのスペクトル拡散通信への応用

藤 崎 礼 志　　金沢大学理工研究域准教授

概要

de Bruijn 系列は超離散力学系に基づく最大周期列の典型例である．de Bruijn 系列のペアに対する相互相関関数の最悪の場合は，最悪のペアに対する自己相関値で特徴付けられるので，まず初めに，長さ 2^n $(n \geq 4)$ の de Bruijn 系列の相異なる自己相関関数の個数の数え上げを試みる．さらに，最悪のペア以外の場合，de Bruijn 系列のペアに対する相互相関特性の上 · 下界を導出する．与えた上 · 下界は等号が成立する場合があるという意味において最良である．スペクトル拡散通信へ応用するために，理論および数値解析結果から，自己および相互相関特性に優れた特性を有する de Bruijn 系列のファミリーの効率的な構成方法も提案する．

1 緒言

本研究の大きな目的は，ビット誤り生起確率に関して最適な非線型力学系に基づくスペクトル拡散符号の実現，相関特性に関して最適な符号ファミリーの構成とその応用である．

スペクトル拡散通信システムの性能評価に関しては，確率解析の立場から，精確かつ簡明なビット誤り生起確率理論評価式を既に導出した [1]．この評価式に基づき，ビット誤り生起確率に関して最適な拡散符号の設計に成功した [2]．これらは，確率論に基づく理論，および，モンテカルロシミュレーションによる実験結果である．しかしながら，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．

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 [3]–[4]．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 $2^n/n$ より小さいが，後者の典型例である 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．

ビット誤り生起確率に関して最適な拡散符号を実現するために，[5] 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 [6] 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．

[7] では，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．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 系列の生成に応用した．

自己相関関数は通信の同期を確立する重要な統計量であるが，非線形フィードバックシフトレジスタ (NLFSR) 最大周期列の自己相関特性については，最も簡単な NLFSR 系列である de Bruijn 系列の場合でさえ，上界だけしか知られていなかった [8]．[9] において，de Bruijn 系列の自己相関値の下界を理論的に導出することに成功した．与えた下界は等号が成立する場合があるという意味において最良である．

一方，相互相関関数は通信の多元接続干渉を知るのに重要な統計量である．de Bruijn 系列のペアに対する相互相関関数の最悪の場合は，最悪のペアに対する自己相関値の上 · 下界で与えられる．本研究では，最適な符号ファミリーを構成するために，最悪のペア以外に対する特性に興味があるので，長さ 2^n $(n \geq 4)$ の de Bruijn 系列の相異なる自己相関関数の個数の数え上げを試みた．さらに，最悪のペア以外の場合の相互相関特性の上 · 下界を導出した．与えた上 · 下界は等号が成立する場合があるという意味において最良である．得られた相互相関特性の上 · 下界の理論値と先の自己相関特性の上 · 下界の理論値に基づき，両方の相関特性に優れた特性を有する

de Bruijn 系列のファミリーを構成した．得られたファミリーは同期捕捉だけでなく，多元接続干渉に関しても優れた特性を有する．理論および数値解析結果から，自己および相互相関特性に優れた特性を有する de Bruijn 系列のファミリーの効率的な構成方法も提案した．

2 準備

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 1 $\{-1,1\}$ 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 の相互相関関数は

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

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，$a\,(\mathrm{mod}\ b)$ は法 b に関する a の最小剰余を表す．系列 $\boldsymbol{X}$ と $\boldsymbol{Y}$ 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．
$\boldsymbol{X}=\boldsymbol{Y}$ のとき $R_N(\ell;\boldsymbol{X},\boldsymbol{X})$ および $r_N(\ell;\boldsymbol{X},\boldsymbol{X})$ をそれぞれ自己相関関数および正規化自己相関関数と呼び，単に $R_N(\ell;\boldsymbol{X})$ および $r_N(\ell;\boldsymbol{X})$ で表す．

本調査研究においては，緒言で述べた様に，超離散力学系に基づく最大周期列の典型例である，de Bruijn 系列の相関特性に注目する．後で見るように，de Bruijn 系列は通常 $\{0,1\}$ 上の系列として定義される．一方，相関関数は $\{-1,1\}$ 上の系列に対して定義された．そのため，本報告に渡って，de Bruijn 系列 $\boldsymbol{X}$ と $\boldsymbol{Y}$ に対する正規化相互相関関数値 $r_N(\ell;\boldsymbol{X},\boldsymbol{Y})$ を計算するとき，de Bruijn 系列における 0 を -1 とみなす．言い換えると，0 と -1 の間の一対一対応により，$\{0,1\}$ 上の長さ N の de Bruijn 系列 $\boldsymbol{X}$ と $\boldsymbol{Y}$ を $\{-1,1\}$ 上の長さ N の系列に変換して相関関数値を計算する．
系列の時間反転を扱うために，次を導入する．

定義 2 $\{-1,1\}$ 上の系列 $\boldsymbol{X}=(X_i)_{i=0}^{N-1}$ に対して，$\boldsymbol{X}$ の反転 ${}^r\boldsymbol{X}$ は ${}^r\boldsymbol{X}=(X_i)_{i=N-1}^{0}$ で定義される．

$R_N(0;\boldsymbol{X},\boldsymbol{Y})$ はベクトル空間 $\mathcal{V}=\mathbb{R}^N$ に属する $\boldsymbol{X}$ と $\boldsymbol{Y}$ の内積に他ならないので，$R_N(0;\boldsymbol{X},\boldsymbol{Y})$ を単に $(\boldsymbol{X},\boldsymbol{Y})$ で表して，内積空間 $(\mathcal{V},(\ ,\ ))$ を考える．$\mathcal{V}$ の上の変換 $S:\mathcal{V}\to\mathcal{V}$ がシフト変換であると呼ばれるのは $(\boldsymbol{X},S(\boldsymbol{Y}))=R_N(1;\boldsymbol{X},\boldsymbol{Y})$ のときである．$S^0(\boldsymbol{Y})=\boldsymbol{Y}$ および $\ell=1,\cdots,N-1$ に対して $S^\ell(\boldsymbol{Y})=S(S^{\ell-1}(\boldsymbol{Y}))$ と定義して，$\ell=1,\cdots,N-1$ に対して $(\boldsymbol{X},S^\ell(\boldsymbol{Y}))=R_N(\ell;\boldsymbol{X},\boldsymbol{Y})$ を得る．この一般的な設定において，次が成り立つ．

補題 1 任意の $\boldsymbol{X}\in\mathcal{V}$ に対して $(P(\boldsymbol{X}),S(P(\boldsymbol{X})))=(\boldsymbol{X},S(\boldsymbol{X}))$ となるのは，k $(0\leq k\leq N-1)$ が存在して，$P=S^k$ または $P=S^k\circ P_r=P_r\circ S^k$ のときまたそのときに限る．ここで P_r は $\boldsymbol{X}$ を反転 ${}^r\boldsymbol{X}$ に変換する置換変換である．すなわち $P_r(\boldsymbol{X})={}^r\boldsymbol{X}$．

補題 1 の次の直接の帰結を用いることになる．

系 1 $\mathbb{R}$ 上の任意の $\boldsymbol{X}=(X_i)_{i=0}^{N-1}$ に対して，正規化自己相関関数 $r_N(\ell;\boldsymbol{X})$ は

$$r_N(\ell;\boldsymbol{X})=r_N(\ell;{}^r\boldsymbol{X}),\quad 0\leq\ell\leq N-1$$

を満たす．

また，上に述べた数え上げ問題を解決するために，$\boldsymbol{X}\in\mathcal{V}$ のスカラー $c\in\mathbb{R}$ との積を考える必要がある．直ちに次を得る．

観察 1 $\boldsymbol{X}\in\mathcal{V}$ と $c\in\mathbb{R}$ に対して，$(c\boldsymbol{X},S(c\boldsymbol{X}))=(\boldsymbol{X},S(\boldsymbol{X}))$ は $c=\pm1$ のときまたそのときに限る．

超離散力学系の観点から，de Bruijn 系列を離散化マルコフ変換に関して定義することができる [5]. しかしながら，ここでは，次の様に，離散化マルコフ変換に無関係に定義する.

二進語は有限二値系列である．長さ k の語は k-語と呼ばれる.

長さ k の二進サイクルは，循環順序に関する，二進 k-語の列 $a_1a_2\cdots a_k$ の列である．サイクル $a_1a_2\cdots a_k$ においては，a_1 が a_k に続く．$a_2\cdots a_ka_1, \cdots, a_ka_1\cdots a_{k-1}$ は全て $a_1a_2\cdots a_k$ と同じサイクルである．二つの列 $\boldsymbol{X} = (X_i)_{i=0}^{N-1}$ と $\boldsymbol{Y} = (Y_i)_{i=0}^{N-1}$ が同値であると言われるのは，$\boldsymbol{X}$ と $\boldsymbol{Y}$ が同じサイクルであるときであり，これを記号 $\boldsymbol{X} \simeq \boldsymbol{Y}$ で表す.

長さ 2^n の二進完全サイクルは二進 2^n-語のサイクルであって，二進 n-語の， 2^n 個の可能な順序列が全て異なるものである．任意の二進 n-語は，完全サイクルに丁度一回現れる.

例 **1** 長さ 2^n の完全サイクルの例を与える*:*

$$\begin{aligned} &n = 1, \quad 01, \\ &n = 2, \quad 0011, \\ &n = 3, \quad 00010111, \quad 00011101. \end{aligned}$$

次の定理のために，完全サイクルは de Bruijn 系列と呼ばれる.

定理 1 (de Bruijn [12], Flye Sainte-Marie [13]) 各正の整数 n に対して，長さ 2^n の完全サイクルは，丁度 $2^{2^{n-1}-n}$ 個存在する.

3 既知の結果

$N = 2^n\,(n \geq 1)$ と置く. $a \in \{0,1\}$ に対して，$\overline{a}$ を用いて，a の補数を表す，即ち，$\overline{0} = 1$ および $\overline{1} = 0$.

$\boldsymbol{X} = (X_i)_{i=0}^{N-1}$ は長さ $N = 2^n$ の de Bruijn 系列であるとする．本研究に密接に関係する既知の結果を以下に纏める.

観察 2 (Fredricksen [10]) $\boldsymbol{X}$ は完全サイクルであるので，$\overline{\boldsymbol{X}} = (\overline{X_i})_{i=0}^{N-1}$ もまた完全サイクル，すなわち，*de Bruijn* 系列である．同様に， ${}^r\boldsymbol{X}$ もまた *de Bruijn* 系列である.

補題 2 (Chan, Games, and Key [14]) $n \geq 3$ に対して，$\boldsymbol{X} \not\simeq \overline{\boldsymbol{X}}$.

補題 3 (Etzion and Lempel [11]) $n \geq 3$ に対して，$\boldsymbol{X} \not\simeq {}^r\boldsymbol{X}$.

定義により，${}^r({}^r\boldsymbol{X}) = \boldsymbol{X}$，$\overline{(\overline{\boldsymbol{X}})} = \boldsymbol{X}$，および ${}^r\overline{\boldsymbol{X}} = \overline{{}^r\boldsymbol{X}}$．$\boldsymbol{X} \simeq {}^r\boldsymbol{X}$ ならば，または同等であるが，$\overline{\boldsymbol{X}} \simeq {}^r\boldsymbol{X}$ ならば，$\boldsymbol{X}$ は *CR (complement reverse)* 系列と呼ばれる．定義により， $\boldsymbol{X}$ が CR 系列であれば、$\overline{\boldsymbol{X}}$ と ${}^r\boldsymbol{X}$ もそうである.

補題 4 (Fredricksen [10]) 偶数 $n \geq 4$ に対して，$\boldsymbol{X} \not\simeq {}^r\overline{\boldsymbol{X}}$.

一方， [10] において， $n = 5$ に対して，$\boldsymbol{X} \simeq {}^r\overline{\boldsymbol{X}}$ が起こると指摘された．実際， $n = 5$ に対して，32 対の CR 系列が存在する．その様な CR 系列の一例が与えられた:

例 2 (Fredricksen [10]) $\boldsymbol{X} = 11111001000101011101100000110100$ は $\overline{\boldsymbol{X}} \simeq {}^r\boldsymbol{X}$ を満たす.

自然に， [10] において，次の問題が Fredricksen により与えられた: $n\,(\geq 3)$ が奇数であるとき常に CR 系列が存在することを示せ．この問題はしばしば議論された．特に， [11] において， CR 系列の特徴付けが与えられた.

補題 5 (Etzion and Lempel [11]) $\boldsymbol{Y} = (Y_i)_{i=0}^{N-1}$ は，必ずしも *de Bruijn* 系列でない， $\{0,1\}$ 上の系列であるとする．系列 $\boldsymbol{Y}$ が *CR* 系列であるのは， N が偶数，かつ，ある $N/2$-語 w に対して $\boldsymbol{Y} \simeq {}^r\overline{w}w$ のとき，またそのときに限る.

語 u と v に対して，uv は u と v の連接を表す．

しかしながら，残念であるが，筆者の知る限り，上記 Fredricksen の問題は未だ未解決である．本研究では，この問題を部分的に解決する．

4 de Bruijn 系列の自己相関関数の数え上げについて

この章では，上で得られた結果および既知の結果に基づき，長さ $N = 2^n\,(n \geq 4)$ の de Bruijn 系列全体の集合に対して，相異なる自己相関関数の総数を数え上げについて考察する．

$\{0,1\}$ 上の $\boldsymbol{X}$ の補数表現 $\overline{\boldsymbol{X}}$ は，$\{-1,1\}$ 上の $\boldsymbol{Y}$ のスカラー倍 $-\boldsymbol{Y}$ に対応することに注意して，観察 1 から直ちに次を得る．

注 1 $\boldsymbol{X}$ は長さ 2^n の *de Bruijn* 系列であるとする．このとき，

$$r_N(\ell;\boldsymbol{X}) = r_N(\ell;\overline{\boldsymbol{X}}), \quad 0 \leq \ell \leq N-1.$$

系 1 における $r_N(\ell;\boldsymbol{X})$ に対する一般式と共に，サイクルに関する同値関係を考慮して，長さ 2^n の de Bruijn 系列 $\boldsymbol{X}$ に対して，

$$r_N(\ell;\boldsymbol{X}) = r_N(\ell;{}^r\boldsymbol{X}) = r_N(\ell;\overline{\boldsymbol{X}}) = r_N(\ell;{}^r\overline{\boldsymbol{X}}), \quad 0 \leq \ell \leq N-1 \tag{1}$$

を得る．

章 2 において，de Bruijn 系列の集合に同値関係 $\simeq$ を既に導入した．$\mathcal{T}_n$ は，長さ $2^n\,(n \geq 4)$ の de Bruijn 系列全体の集合の，$\simeq$ による商集合であるとする．$\mathcal{T}_n$ に別の同値関係 $\sim$ を次の様に導入する．各 $n\,(\geq 4)$ に対して，$\mathcal{T}_n$ に属する $\boldsymbol{X}$ と $\boldsymbol{Y}$ が自己相関関数に関して同値であるのは，全ての $\ell\,(0 \leq \ell \leq 2^n-1)$ に対して，$r_{2^n}(\ell;\boldsymbol{X}) = r_{2^n}(\ell;\boldsymbol{Y})$ のときであると定義し，これを記号 $\boldsymbol{X} \sim \boldsymbol{Y}$ で表す．$\mathcal{T}_n$ の $\sim$ による商集合を表すのに $\mathcal{T}_n/\sim$ を用いる．$\mathcal{T}_n/\sim$ の濃度は，長さ 2^n の de Bruijn 系列に対する，相異なる自己相関関数の総数を与える．ν_n を用いて，$\mathcal{T}_n/\sim$ の濃度を表す．

補題 2，3, および 4 から，偶数 $n \geq 4$ に対して，$\boldsymbol{X}$, ${}^r\boldsymbol{X}$, $\overline{\boldsymbol{X}}$，および ${}^r\overline{\boldsymbol{X}}$ は全て相異なる．一方，[17] において，長さ $2^{2p+1}\,(p \geq 1)$ の de Bruijn 系列に含まれる CR 系列の存在に関して，CR グラフを定義し，Fredricksen によって提起された基本的な問題を部分的に解決した:

定理 2 p が素数であるとき常に，長さ 2^{2p+1} の *de Bruijn* 系列に $4\sum_{i=0}^{2^{p-1}-1}\Delta^{(v^{(i)})}$ 個の *CR* 系列が存在する．ここで $v^{(i)} \in \mathcal{V}_{2p+1}^{CR}$.

ここで，$\mathcal{V}_{2p+1}^{CR}$ は CR 頂点の集合，$\Delta^{(v^{(i)})}$ は CR 頂点 $v^{(i)}$ に同伴する CR グラフのアドミタンス行列の $(1,1)$ 成分の余因子を表す．

結局，定理 1 と定理 2 により，次を得る．

系 2 各正の偶数 $n \geq 4$ に対して，

$$\nu_n \leq 2^{2^{n-1}-n-2}. \tag{2}$$

奇数 $n = 2p+1$ に対して，ここで p は任意の素数である，

$$\nu_n \leq 2^{2^{n-1}-n-2} + \sum_{i=0}^{2^{p-1}-1}\Delta^{(v^{(i)})}. \tag{3}$$

ここで $v^{(i)} \in \mathcal{V}_{2p+1}^{CR}$.

[9] の実験結果は次を示唆する．

注 2 $n = 4$ のとき，*(2)* において等号が成立する．この意味において，ν_n の上界 *(2)* は最良である．

次に，$n \geq 5$ に対して，$\mathcal{T}_n$ に距離関数 d を，$d(\boldsymbol{X},\boldsymbol{Y}) = \min\limits_{0\leq\ell\leq 2^n-1} d_H(\boldsymbol{X},S^\ell(\boldsymbol{Y}))$ により導入する．ここで $d_H(\boldsymbol{X},\boldsymbol{Y})$ は，$\boldsymbol{X},\boldsymbol{Y} \in \{0,1\}^{2^n}$ に対する，$\boldsymbol{X}$ と $\boldsymbol{Y}$ の Hamming 距離，すなわち，$\boldsymbol{X}$ と $\boldsymbol{Y}$ において異なる要素数である．章 2 で定義された様に，$\{0,1\}^{2^n}$ 上のシフト変換を表すのに S を再び用いた．$\mathcal{T}_n$ に属する $\boldsymbol{X}$ と $\boldsymbol{Y}$ は完全サイクルであるので，$d(\boldsymbol{X},\boldsymbol{Y})$ は非負偶整数を取るのが容易にわかる．この設定において，次が成り立つ．

補題 **6** $\boldsymbol{X}=(X_i)_{i=0}^{2^n-1}$ と $\boldsymbol{Y}=(Y_i)_{i=0}^{2^n-1}$ は $\mathcal{T}_n\,(n\geq 5)$ に属するとする．このとき，$d(\boldsymbol{X},\boldsymbol{Y})=2$ かつ $\boldsymbol{X}\sim\boldsymbol{Y}$ であるのは，$i\,(0\leq i\leq 2^n-1)$ と $\ell\,(0\leq \ell\leq 2^n-1)$ が存在して，$X_i\neq Y_{i+\ell\,(\bmod 2^n)}$，$X_{i+2^{n-1}\,(\bmod 2^n)}\neq Y_{i+\ell+2^{n-1},(\bmod 2^n)}$，および $0\leq j\leq 2^n-1\,(j\neq i,\,j\neq i+2^{n-1}\,(\bmod 2^n))$ に対して，$X_j=Y_{j+\ell\,(\bmod 2^n)}$ を満たすとき，並びに，$1\leq k\leq 2^{n-1}-1$ に対して，

$$X_{i-k+2^n\,(\bmod 2^n)}+X_{i+k\,(\bmod 2^n)}=X_{i-k+2^{n-1}\,(\bmod 2^n)}+X_{i+k+2^{n-1}\,(\bmod 2^n)}$$

を満たすときまたそのときに限る．

この必要十分条件は，$d(\boldsymbol{X},\boldsymbol{Y})=2$ かつ $\boldsymbol{X}\sim\boldsymbol{Y}$ を満たすような，$\mathcal{T}_n\,(n\geq 5)$ に属する $\boldsymbol{X}$ と $\boldsymbol{Y}$ を特徴付ける．しかしながら，その様な対の存在を保証するわけではない．その様な対全体の集合は空集合であり得る．そのため，上記条件を満たすような，$\mathcal{T}_n$ に属する $\boldsymbol{X}$ と $\boldsymbol{Y}$ が存在するかどうかを未だ検証しなければならない．実験的に次を得る．

例 **3** $n=5$ のとき，$\boldsymbol{X}=00000100101100110101000111110111$ と $\boldsymbol{Y}=00000100101101110101000111110011$ は $d(\boldsymbol{X},\boldsymbol{Y})=2$ かつ $\boldsymbol{X}\sim\boldsymbol{Y}$ を満たす．

この例は，$p=2$ のとき，(3) に等号が成立しないことを意味する．さらに，$n\geq 5$ のとき，上記条件を満たすような，$\mathcal{T}_n$ に属する $\boldsymbol{X}$ と $\boldsymbol{Y}$ が常に存在するかどうかを示すのは興味深い問題であることも示唆する．

5 de Bruijn 系列の相互相関関数の上 · 下界

本章では，de Bruijn 系列の相互相関関数を考える．定理 1 により，$n\geq 3$ に対して，長さ 2^n の de Bruijn 系列の相互相関関数を定義することができる．既に述べた様に，de Bruijn 系列に対して，自己相関関数の上 · 下界は [9] で既に明らかになった．de Bruijn 系列の相互相関関数の次の上 · 下界は [8] で得られた．この結果から出発する．

定理 **3 (Zhang and Chen [8])** $\boldsymbol{X}$ と $\boldsymbol{Y}$ が長さ 2^n の相異なる *de Bruijn* 系列であるならば，

$$-1\leq r_N(\ell;\boldsymbol{X},\boldsymbol{Y})\leq 1-\frac{4}{2^n},\quad 0\leq\ell\leq N-1.$$

左辺の等号が成立するのは $\boldsymbol{Y}=\overline{\boldsymbol{X}}$ かつ $\ell=0$ のときまたそのときに限る．

定理 3 における下界に対して等号が成立する条件は，相互相関関数に関する de Bruijn 系列の最悪のペアおよびそのペアに対する相互相関関数の最悪の場合を特徴付ける．この条件に基づき，de Bruijn 系列のペア $(\boldsymbol{X},\overline{\boldsymbol{X}})$ を最悪ペアと呼ぶ．

定理 3 により，$\boldsymbol{Y}\neq\overline{\boldsymbol{X}}$ または $\ell\neq 0$ の場合を考察する必要があるだけである．

$\ell\neq 0$ の場合を考える．(1) から一般に次を得る．

補題 **7** $\boldsymbol{X}$ は長さ $2^n\,(n\geq 3)$ の *de Bruijn* 系列であるとする．このとき，

$$\begin{aligned}r_N(\ell;\boldsymbol{X},\overline{\boldsymbol{X}})&=r_N(\ell;\overline{\boldsymbol{X}},\boldsymbol{X})=r_N(\ell;{}^r\boldsymbol{X},{}^r\overline{\boldsymbol{X}})=r_N(\ell;{}^r\overline{\boldsymbol{X}},{}^r\boldsymbol{X})\\&=-r_N(\ell;\boldsymbol{X})=-r_N(\ell;{}^r\boldsymbol{X})=-r_N(\ell;\overline{\boldsymbol{X}})=-r_N(\ell;{}^r\overline{\boldsymbol{X}}),\quad 0\leq\ell\leq N-1.\end{aligned}$$

したがって，$\ell\neq 0$ かつ $\boldsymbol{Y}=\overline{\boldsymbol{X}}$ の場合に対して，[8] で得られた $r_N(\ell;\boldsymbol{X})$ に対する上界と [9] で得られた $r_N(\ell;\boldsymbol{X})$ に対する下界から，この補題により次が導かれる．

系 **3** $\boldsymbol{X}$ が長さ $2^n\,(n\geq 3)$ の *de Bruijn* 系列であるならば，

$$-1+\frac{4}{2^n}\cdot\left[\frac{2^n}{2n}\right]\leq r_N(\ell;\boldsymbol{X},\overline{\boldsymbol{X}})\leq 1-\frac{4}{2^n},\quad 1\leq\ell\leq N-1.\tag{4}$$

残るは $\boldsymbol{Y}\neq\overline{\boldsymbol{X}}$ の場合である．定理 1 により，$n\geq 4$ に対して $2^{2^{n-1}-n}\geq 4$ が満たされる．その様な n に対して，次を得る．

定理 4 $\boldsymbol{X}$ と $\boldsymbol{Y}$ が長さ 2^n $(n \geq 4)$ の相異なる *de Bruijn* 系列であり，かつ $\boldsymbol{Y} \neq \overline{\boldsymbol{X}}$ ならば，

$$-1 + \frac{4}{2^n} \leq r_N(\ell; \boldsymbol{X}, \boldsymbol{Y}) \leq 1 - \frac{4}{2^n}, \quad 0 \leq \ell \leq N-1. \tag{5}$$

6 実験結果

$n = 4$ に対して，16 個の長さ 2^4 の相異なる de Bruijn 系列を得る．これにより，$\binom{16}{2} = 120$ 個の相互相関関数を得る．

ケース i) $\boldsymbol{Y} = \overline{\boldsymbol{X}}$
この場合，最悪ペアを得る．その様な最悪ペアを選ぶとき，長さ 2^4 の相異なる de Bruijn 系列が 16 個存在するという事実から，8 個の正規化相互相関関数を得る．

さらに，系 2 により，$n = 4$ のとき，全部で 16 個の de Bruijn 系列に対する正規化自己相関関数は 4 つのパターンに分類される．全てのパターンを図 1 (a) から (d) に示す．これらにより，次のことがわかる．

注 3 $n = 4$ かつ $\ell \neq 0$ のとき，*(4)* における $r_N(\ell; \boldsymbol{X}, \overline{\boldsymbol{X}})$ の上 · 下界に対して，等号が成立する．

この意味において，(4) で与えられる $r_N(\ell; \boldsymbol{X}, \overline{\boldsymbol{X}})$ の上 · 下界の評価は最良である．

ケース ii) $\boldsymbol{Y} \neq \overline{\boldsymbol{X}}$
残りの正規化相互相関関数は 112 個である．記法を簡明にするために，

$$\max_{0 \leq \ell \leq N-1} |r_N(\ell; \boldsymbol{X}, \boldsymbol{Y})| = |r|_{\max}$$

と書く．これを用いて，表 1 に 112 個の正規化相互相関関数の最悪絶対値を示す．

表 1: 正規化相互相関関数の最悪絶対値

$\lvert r\rvert_{\max}$	系列数
0.75	32
0.5	80

$|r|_{\max} = 0.75$ を満たす 32 個のペアの中で，$\max_{0 \leq \ell \leq N-1} r_N(\ell; \boldsymbol{X}, \boldsymbol{Y}) = 0.75$ および $\min_{0 \leq \ell \leq N-1} r_N(\ell; \boldsymbol{X}, \boldsymbol{Y}) = -0.75$ を満たすペアの数は同じ 16 である．この事実により次を得る．

注 4 $n = 4$ のとき，*(5)* における $r_N(\ell; \boldsymbol{X}, \overline{\boldsymbol{X}})$ の上 · 下界に対して，等号が成立する．

この意味において，(5) で与えられる $r_N(\ell; \boldsymbol{X}, \overline{\boldsymbol{X}})$ の上 · 下界の評価は最良である．

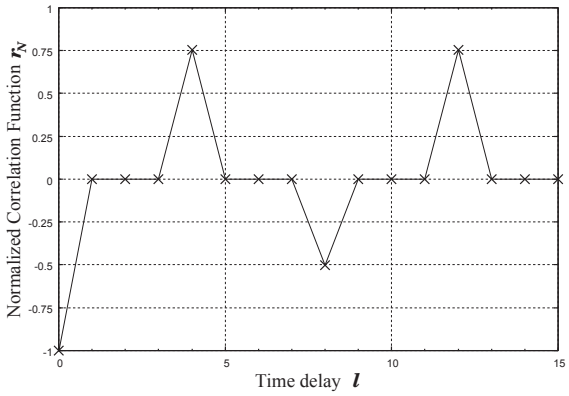
表 1 は正規化相互相関関数に関して最悪な系列の族を提供する．最悪な系列の族を取り除くことにより，その様な相関関数に関して良い性質を有する de Bruijn 系列の族を構成することができる．

補題 7 から，図 1 (b) と (c) は正規化自己相関関数関して良い性質を有する de Bruijn 系列を特徴付ける．この観察に基づき，(b) と (c) から任意のペア $(\boldsymbol{X}, \boldsymbol{Y})$ が $\boldsymbol{Y} \neq \overline{\boldsymbol{X}}$ を満たすような極大族を構成することができる．実験結果により (b) と (c) から得られる 6 ペアは全て $|r|_{\max} = 0.5$ を満たすことが確認された．

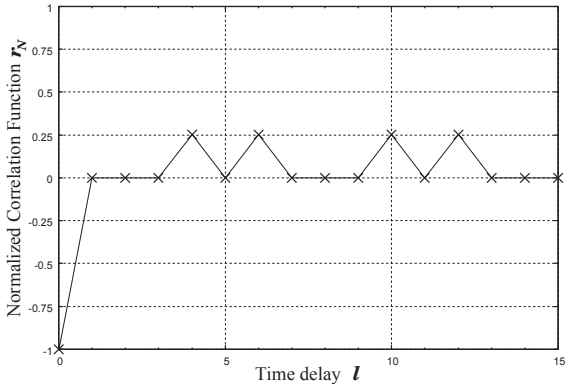
この事実は，正規化自己だけでなく相互相関関数に関しても良い性質を有する de Bruijn 系列の族を構成する効果的な方法を示唆する．すなわち，まず初めに，自己相関関数関して良い性質を有する族を構成する．次に，この族から得られる任意のペア $(\boldsymbol{X}, \boldsymbol{Y})$ が $\boldsymbol{Y} \neq \overline{\boldsymbol{X}}$ を満たすような極大族を構成する．最後に，相互相関関数に関して最悪な系列を取り除けばよい．

7 結言

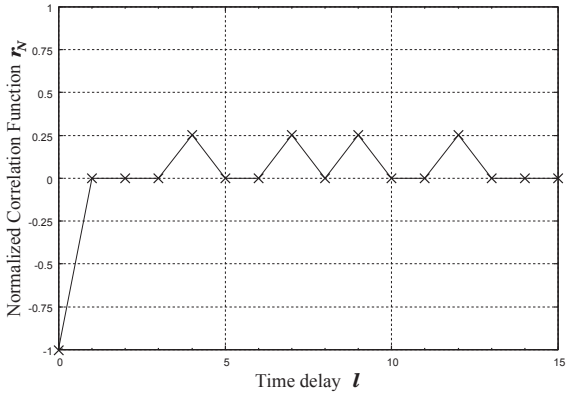
de Bruijn 系列のペアに対する相互相関関数の最悪の場合は，最悪のペアに対する自己相関値で特徴付けられるので，長さ 2^n $(n \geq 4)$ の de Bruijn 系列の相異なる自己相関関数の個数の数え上げを試みた．そのために，CR 系列に関する Fredricksen の問題を部分的に解決した．すなわち，p が素数の場合，長さ 2^{2p+1} の CR 系列を構成的に求め，実現した．さらに，最悪のペア以外の場合の相互相関特性の上 · 下界を導出した．与えた上 · 下界



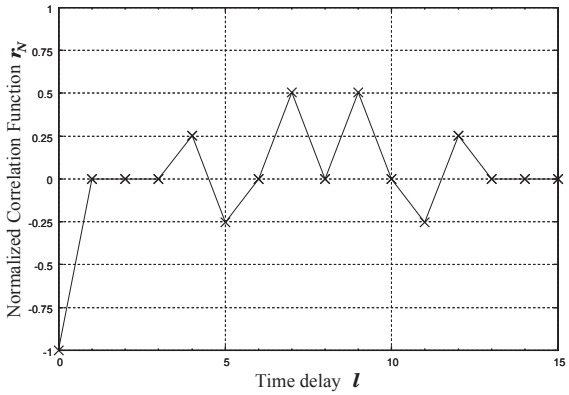
(a) 自己相関関数関して最悪の系列を特徴付ける正規化相互相関関数



(b) 自己相関関数関して最良の系列の一つを特徴付ける正規化相互相関関数



(c) 自己相関関数関して最良の系列の一つを特徴付ける正規化相互相関関数



(d) 自己相関関数関して二番目に悪い系列を特徴付ける正規化相互相関関数

図 1: 長さ 2^4 の de Bruijn 系列の最悪ペアに対する正規化相互相関関数

は，$n = 4$ のとき，等号が成立する場合があるという意味において最良である．得られた相互相関特性の上・下界の理論値と先の自己相関特性の上・下界の理論値に基づき，両方の相関特性に優れた特性を有する de Bruijn 系列のファミリーを構成した．得られたファミリーは同期捕捉だけでなく，多元接続干渉に関しても優れた特性を有する．理論および数値解析結果から，自己および相互相関特性に優れた特性を有する de Bruijn 系列のファミリーの効率的な構成方法も提案した．

参考文献

[1] H. Fujisaki, "Performance Analysis of SSMA Communication Systems with Spreading Sequences of Markov Chains: Large Deviations Principle versus the Central Limit Theorem," *IEEE Trans. on Information Theory*, vol. 57, pp. 1959–1967, 2011.

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

[3] 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).

[4] 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.

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

[6] R. Hirota and D. Takahashi, *Discrete and Ultradiscrete Systems*, Kyoritsu Shuppan, 2003 (in Japanese).

[7] 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.

[8] Z. Zhang and W. Chen, "Correlation properties of de Bruijn sequences," *Systems Science and Mathematical Sciences*, vol. 2, pp. 170–183, 1989.

[9] H. Fujisaki and Y. Nabeshima, "On Auto-Correlation Values of de Bruijn Sequences," *NOLTA, IEICE*, vol. 3, pp. 400–408, 2011.

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

[11] T. Etzion and A. Lempel, "On the distribution of de Bruijn sequences of given complexity," *IEEE Trans. on Information Theory*, vol. 30, pp. 611–614, 1984.

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

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

[14] A. H. Chan, R. A. Games, and E. L. Key, "On the Complexities of de Bruijn Sequences," *J. Comb. Theory, Ser. A*, vol. 33, pp. 233–246, 1982.

[15] W. T. Tutte, "The dissection of equilateral triangles into equilateral triangles," *Proc. Cambridge Phil. Soc.*, vol. 44, pp. 463–482, 1948.

[16] T. van Aardenne-Ehrenfest and N. G. de Bruijn, "Circuits and trees in oriented linear graphs," *Simon Stevin*, vol. 28, pp. 203–217, 1951.

[17] H. Fujisaki "A construction of all CR sequences in the de Bruijn sequences of length 2^{2p+1} where p is a prime number," submitted to *NOLTA, IEICE*, 2013.

＜発　表　資　料＞

題　　名	掲載誌・学会名等	発表年月
On embedding conditions of shifts of finite type into the Fibonacci-Dyck shift	Proc. of the IEEE Int. Symp. on Information Theory (ISIT2012), pp. 279-283	2012.7
On Cross-Correlation Values of de Bruijn Sequences	Proc. of the 2012 Int. Symp. on Nonlinear Theory and its Applications (NOLTA2012), pp. 883-886	2012.10
Number Theoretic Analysis of the Induced Transformations Associated with the Interval Algorithm	Proc. of the 35th Symposium on Information Theory and its Applications (SITA2012), pp. 437-442	2012.12