様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

# 科学研究費助成事業　　研究成果報告書

令和　３ 年　 ６ 月　 ３ 日現在

機関番号：１３３０１
研究種目：基盤研究(C)（一般）
研究期間：2018～2020
課題番号：１８Ｋ１１４６５

研究課題名（和文）超離散カオス力学系に基づく最適相関最大周期列の効率的生成と多元接続通信への応用

研究課題名（英文）Efficient generation of full-length sequences with optimal correlation based on discretized chaotic transformations and its applications to multiple access communication systems

研究代表者

藤崎　礼志（Fujisaki, Hiroshi）

金沢大学・電子情報通信学系・准教授

研究者番号：８０３０４７５７

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：超離散カオス力学系に基づく最大周期列の効率的生成とその多元接続通信への応用に関して次の結果を得た．(i)Sawadaらのアルゴリズムで生成されるde Bruijn 系列の自己相関特性を明らかにし，良好な自己相関特性を有するde Bruijn 系列のファミリーを構成した．(ii)Sawadaらのアルゴリズムを拡張し，離散化黄金平均変換に基づく最大周期列を1ビット当たりならし計算量O(1)で生成し，その自己相関特性を明らかにした．(iii)ストリーム型データ圧縮アルゴリズム非対称2進数系(asymmetric binary systems (ABS))が正しく動作するための必要十分条件を与えた．

研究成果の学術的意義や社会的意義
de Bruijn 系列は暗号解読，衛星通信，ゲノム解析に応用されているが，位数nのde Bruijn 系列の自己相関関数は，時刻t=0に値1を取り，0<t<|n|において値0を取るという零相関帯を有すること，それ以外については上下界しか知られていない．相関特性は学術のみならず応用上も重要な統計量であるので，研究成果(i),(ii)は擬似乱数，系列の専門分野に留まらず，de Bruijn 系列を応用する分野にも貢献した．ストリーム型ABSは，アップル社オープンソースデータ圧縮アルゴリズムに採用される程，実用上優れた性能を有する．研究成果(iii)はそれをデータ圧縮として利用する人々に貢献した．

研究成果の概要（英文）：We have previously defined the discretized Markov transformations and the full-length sequences based on such transformations. De Bruijn sequences can be regarded as the full-length sequences based on the discretized Markov beta-transformation with beta=2. Recently, Sawada et al. proposed an efficient construction of de Bruijn sequence. We modify their construction and apply it to construct a full-length sequence based on the discretized Markov beta-transformation, where beta is the golden mean. We also give correlational properties of not only de Bruijn sequences constructed by Sawada et al. but the full-length sequences constructed in this research, which are based on the discretized golden mean transformation.
The stream version of asymmetric binary systems (ABS) is irreducible if it admits an irreducible finite-state Markov chain. For a probability p (0<p<1), where p is irrational, we give a necessary and sufficient condition for the stream version of ABS to be irreducible.

研究分野：情報工学

キーワード：超離散力学系　マルコフ連鎖　最大周期列　記号力学系　非対称2進数系(ABS)

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属します。

様　式　C－１９、F－１９－１、Z－１９ (共通)

1. 研究開始当初の背景

擬似乱数は，秘匿通信，フィンテックやランダム制御において必要不可欠であり，情報化社会を支える基盤の一つである．

Ulam と von Neumann が，カオス区間力学系の実数値解軌道から得られる数列を，擬似乱数として用いることを提案して以来，[1] の様々な分野への応用が試みられている．しかしながら，[1] の解軌道計算は実数演算を前提としているため，計算機に実装する際，次の問題が生ずる: 丸め誤差があるため，得られた数列が周期列に陥る (周期性の問題); 丸め誤差の，機種およびプログラミング言語依存性のため，同じアルゴリズムを用いたとしても同じ数列が得られるとは限らない (再現性の問題).

エルゴード理論に基づく [1] の発想から得られる確率過程 (無限列) を最大周期列 (ブロック) として実現するためには，ある種の離散化が必要である．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．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．本研究代表者は，先に，記号力学系とグラフ理論の手法を用いて，周期性と再現性の問題を有しない，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一般的に定義した [IEICE Trans. Fundamentals, 2005]．さらに，本研究代表者は，2 値の場合に，最適拡散符号と同一の自己相関関数と均等分布を有する，離散化マルコフ $\beta$ 変換に基づく最長周期列の実現に成功し，ビット誤り生起確率 (BER) に関する最適性を数値実験により確認した [NOLTA 2016].

2. 研究の目的

本研究の大きな目的は，所望の自己相関特性と均等分布を有する擬似乱数を，超離散カオス力学系に基づき効率的かつ大量に実現し，BER に関して最適なスペクトル拡散符号として，多元接続通信に応用することである．この目的を達成するために必要な要素研究とその目的を以下述べる．

(1) 超離散力学系に基づく最大周期列は，総数が系列長 $L$ に関して指数関数的に増大するという優れた特性を有する．これを性質 E と呼ぶ．しかしながら，性質 E ゆえに，$L$ が大きくなると，最大周期列を全て生成するのは計算困難問題となる．この問題を回避するため，本研究では，所望の相関特性を有する系列だけを選別し，効率的に生成する新たな手法を探求するのを目的 (研究目的 (1)) とする．

最近，Sawada らは，任意の自然数 $n$ に対して，$O(n)$ のメモリを用いて，1 ビット当たりならし計算量 $O(1)$ で，長さ $k^n$ の, 単一の $k(\geq 2)$ 進 de Bruijn 系列を生成するという驚く程高効率なアルゴリズムを発見した [2]．本研究課題の超離散力学系という立場では，$k$ 進 de Bruijn 系列は区間力学系 $k$ 進変換の超離散化である．

de Bruijn 系列の規格化自己相関関数は時刻 $t = 0$ に値 1 を取り，$0 < t < |n|$ において値 0 を取るという零相関帯 (zero correlation zone (ZCZ)) を有することが知られている．しかしながら，それ以外については上下界しか知られていない．本研究では，研究目的 (1) を達成するために，次の具体的な目標を設定する．

(1-1) Sawada らのアルゴリズムで生成される de Bruijn 系列の自己相関特性を明らかにする．その結果に基づき，良好な自己相関特性を有する de Bruijn 系列のファミリーを構成する．

(1-2) Sawada らのアルゴリズムを拡張し，離散化マルコフ $\beta$ 変換に基づく最長周期列を 1 ビット当たりならし計算量 $O(1)$ で生成すると共に，その自己相関特性を明らかにする．

(2) 本研究で提案する擬似乱数を多元接続通信に応用するためには，データ圧縮が必要不可欠である．

Duda は，ストリーム型データ圧縮アルゴリズム非対称 2 値数系 (asymmetric binary systems (ABS)) を提案した [5]．ストリーム型 ABS の状態集合は，状態パラメータと呼ばれる自然数 $l$ により定まる自然数の有限集合である．Duda は，[5] において，アルゴリズムの入力である確率 $p\,(0 < p < 1)$ と $l$ の与え方を原理的に指定しておらず，アルゴリズムが正しく動作しないような $p$ と $l$ が存在すること，特に $p = 1/2$ の近傍では，ストリーム型 ABS 符号化が妥当とならないことが，横尾により指摘された [6]．同時に,「アルゴリズムが正しく動作する $p$ と $l$ の条件を求めよ」という公開問題が提起された．本研究では，この問題を解決するのを目的 (研究目的 (2)) とする．

3. 研究の方法

研究目的 (1) に対する研究方法

任意の位数 $n$ に対して，単一の de Bruijn 系列を効率的に生成するアルゴリズムとして,「1 優先アルゴリズム」が古くから知られている [3]．最近，似て非なる新しいアルゴリズム「反転優先アルゴリズム」が発見され，de Bruijn 系列を辞書式にランレングス符号化するとき，1 優先アルゴリズムは最大の符号語長を与え，一方，反転優先アルゴリズムは最小の符号語長を与えることが示された [4]．これら二つのアルゴリズムと Sawada らのアルゴリズムから生成される三つの系列の特性を利用して，良好な自己相関特性を有す

る de Bruijn 系列のファミリーを構成する．

Sawada らのアルゴリズムは巡回シフトとネックレスに基づいている．シフトは記号力学系を定義するため，記号力学系的解析が可能である．記号力学系と $\beta$ 進展開の手法を用いて，長さ $n$ の両端固定 $k$ 進ネックレスの総数の公式を求め，Sawada らのアルゴリズムで生成された $k$ 進 de Bruijn 系列の時刻 $t = |n|$ のときの規格化自己相関関数の公式を得る．

研究目的 (2) に対する研究方法

ストリーム型 ABS アルゴリズムが，無理数回転 (ワイル変換) と呼ばれる力学系と同型な二つの区間力学系の超離散化を構成し，情報源によるランダムな入力を利用して，ランダム力学系を構成していることを明らかにし，アルゴリズムが既約なマルコフ連鎖を構成するための条件を得る．

Duda の ABS の状態は非負整数である．Duda の ABS を整数に基づく擬似乱数の生成と見ることによって，ABS の符号化関数がサブスティテューションと呼ばれる力学系から生ずるサブシフトのファクターを決定することを明らかにすれば，記号力学系，エルゴード理論からの接近法が可能となる．

4. 研究の成果

研究目的 (1) に対する研究成果

$k = 2$ のとき，Sawada らのアルゴリズムから生成される de Bruijn 系列が，自己相関特性に関して優れた特性を有することを実験的に示した．1 優先アルゴリズムおよび反転優先アルゴリズムから生成される de Bruijn 系列の自己相関特性について調べたところ，位数 $n = 6$ まで，両者は Sawada らのアルゴリズムから生成される系列よりも良好な特性を有することを発見した．この結果は，ランレングス符号化による符号化語長と自己相関特性には関係が無いことを示唆している．

これら二つのアルゴリズムと Sawada らのアルゴリズムから生成される三つの系列の特性を利用して，良好な自己相関特性を有する de Bruijn 系列のファミリーを構成することに成功した．位数 $n = 6$ のとき，de Bruijn 系列の総数 $67,108,864$ 個に対し，構成されたファミリーの符号語数は 692 個，すなわち総数の約 $1/10^5$ である．

さらに，Sawada らのアルゴリズムを，$\beta$ が黄金平均のとき，超離散化マルコフ $\beta$ 変換に基づく最大周期列の効率的生成への拡張に成功し，任意の $n$ に対して，$O(n)$ のメモリを用いて，1 ビット当たりならし計算量 $O(1)$ で，離散化黄金平均変換に基づく最大周期列を生成するアルゴリズムを提案した．$t = |n|$ のとき，Sawada らのアルゴリズムをで生成される 2 進 de Bruijn 系列と黄金平均変換に基づく最大周期列の規格化自己相関関数の公式を導出した [SITA2019]．Sawada らのアルゴリズムで生成された $k$ 進 de Bruijn 系列に対して，$k = 2$ の場合の結果を $k \geq 3$ の場合に拡張し，時刻 $t = |n|$ のときの規格化自己相関関数の公式を得た．$k \geq 3$ の場合の結果を IEEE ITW2021 に投稿した (2021 年 5 月 15 日)．

研究目的 (2) に対する研究成果

ストリーム型 ABS のアルゴリズムが正常に機能するための, $p$ と $l$ に関する必要十分条件を与え，横尾の公開問題を解決した [IEICE Trans. Fundamentals, 2021]．この条件に基づき，アルゴリズムが正常に機能する改良ストリーム型 ABS データ圧縮装置を開発した [特願 2019-189427]．

ABS の符号化関数がサブスティテューションと呼ばれる力学系から生ずるサブシフトのファクターを決定することを明らかにすると共に，サブシフト上の一意のエルゴード的不変測度を導出することによって，確率 $p$ の逆数が黄金平均の場合，ABS の状態の確率分布の陽な表式を得た [ISITA2018]．

5G 移動体通信に用いられる，Arikan が提案した分極 (Polar) 符号の発展として，一般化消失通信路に対する多段分極に基づく多元分極符号の構成法，符号化法，復号法の提案とその性能評価を行った．本研究代表者は，多段分極に基づく多元分極符号を，環上の加群への作用とみなし，確率解析の手法を用いて，多元分極符号の極限分布を与えるのに貢献した [IEEE Trans. IT, 2020]．

＜引用文献＞


[1] S.M. Ulam and J. von Neumann, “On combination of stochastic and deterministic processes,” *Bull. Amer. Math. Soc.*, vol. 53, p.1120, 1947.

[2] J. Sawada, A. Williams, and D. Wong “A simple shift rule for $k$-ary de Bruijn sequences,” *Discrete Math.*, vol. 340, pp. 524–531, 2017.

[3] M. H. Martin, “A problem in arrangements,” *Bull. Amer. Math. Soc.*, vol. 40 , pp. 859–864, 1934.

[4] A. Alhakim and M. Akinwande, “A recursive construction of nonbinary de Bruijn sequences,” *Designs, Codes and Cryptography*, vol. 60, pp. 155—169, 2011.

[5] J. Duda, “Asymmetric numeral systems,” `arXiv:0902.0271v5 [cs.IT]`, 2009.

[6] H. Yokoo, “On the stationary distribution of asymmetric binary systems,” *2016 IEEE Int. Symp. on Information Theory (ISIT 2016)*, pp. 11–15, 2016.

５．主な発表論文等

〔雑誌論文〕　計8件（うち査読付論文　5件／うち国際共著　0件／うちオープンアクセス　0件）

| | |
|---|---|
| １．著者名<br>Yuta Sakai, Ken-ichi Iwata, and Hiroshi Fujisaki | ４．巻<br>66 |
| ２．論文標題<br>Modular Arithmetic Erasure Channels and Their Multilevel Channel Polarization | ５．発行年<br>2020年 |
| ３．雑誌名<br>IEEE Transactions on Information Theory | ６．最初と最後の頁<br>3976-4006 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/TIT.2020.2996977 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>Hiroshi Fujisaki | ４．巻<br>E103.A |
| ２．論文標題<br>On Irreducibility of the Stream Version of Asymmetric Binary Systems | ５．発行年<br>2020年 |
| ３．雑誌名<br>IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences | ６．最初と最後の頁<br>757-768 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1587/transfun.2019EAP1140 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>Yuta Sakai, Ken-ichi Iwata, and Hiroshi Fujisaki | ４．巻<br>なし |
| ２．論文標題<br>Countably Infinite Multilevel Source Polarization for Non-Stationary Erasure Distributions | ５．発行年<br>2019年 |
| ３．雑誌名<br>Proc. of 2019 IEEE International Symposium on Information Theory (ISIT 2019) | ６．最初と最後の頁<br>2109-2113 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/ISIT.2019.8849487 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>Hiroshi Fujisaki | ４．巻<br>なし |
| ２．論文標題<br>A Simple Construction of the Full-Length Binary Sequences Based on the Discretized Markov β-Transformations and Their Correlational Properties | ５．発行年<br>2019年 |
| ３．雑誌名<br>Proc. of the 42th Symposium on Information Theory and its Applications (SITA2019) | ６．最初と最後の頁<br>388-392 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>なし | 査読の有無<br>無 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Hiroshi Fujisaki | 4．巻<br>1 |
| 2．論文標題<br>Invariant Measures for the Subshifts Associated with the Asymmetric Binary Systems | 5．発行年<br>2018年 |
| 3．雑誌名<br>Proc. of 2018 Int. Symp. on Information Theory and its Applications (ISITA 2018) | 6．最初と最後の頁<br>675-679 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.23919/ISITA.2018.8664268 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Yuta Sakai, Ken-ichi Iwata, Hiroshi Fujisaki | 4．巻<br>1 |
| 2．論文標題<br>Asymptotic Distribution of Multilevel Channel Polarization for a Certain Class of Erasure Channels | 5．発行年<br>2018年 |
| 3．雑誌名<br>Proc. of 2018 IEEE International Symposium on Information Theory (ISIT 2018) | 6．最初と最後の頁<br>856-860 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/ISIT.2018.8437921 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Hiroshi Fujisaki | 4．巻<br>1 |
| 2．論文標題<br>On Irreducibility of the Stream Version of the Asymmetric Binary Systems | 5．発行年<br>2018年 |
| 3．雑誌名<br>Proc. of the 41th Symposium on Information Theory and its Applications (SITA2018) | 6．最初と最後の頁<br>218-222 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>なし | 査読の有無<br>無 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Yuta Sakai, Ken-ichi Iwata, Hiroshi Fujisaki | 4．巻<br>1 |
| 2．論文標題<br>Concrete Examples of Countably Infinite Multilevel Source Polarization with a Certain Infinite Group | 5．発行年<br>2018年 |
| 3．雑誌名<br>Proc. of the 41th Symposium on Information Theory and its Applications (SITA2018) | 6．最初と最後の頁<br>206-211 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>なし | 査読の有無<br>無 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

〔学会発表〕　計4件（うち招待講演　0件／うち国際学会　0件）

1．発表者名
坂谷 航平，岩田 賢一，藤崎 礼志

2．発表標題
Minimum-Entropy Couplings問題に対するCicalese-Gargano-Vaccaroアルゴリズムの改善

3．学会等名
電子情報通信学会情報理論研究会

4．発表年
2021年

1．発表者名
藤崎 礼志

2．発表標題
ストリーム型非対称データ圧縮装置の高安定化技術

3．学会等名
科学技術振興機構 新技術説明会

4．発表年
2020年

1．発表者名
Hiroshi Fujisaki

2．発表標題
A simple construction of the full-length binary sequences based on the discretized Markov β-transformations and their correlational properties

3．学会等名
Workshop「数論とエルゴード理論」

4．発表年
2020年

1．発表者名
Hiroshi Fujisaki

2．発表標題
On Irreducibility of the Stream Version of the Asymmetric Binary Systems

3．学会等名
Workshop 「数論とエルゴード理論」

4．発表年
2019年

〔図書〕　計0件

〔出願〕　計1件

| 産業財産権の名称 | 発明者 | 権利者 |
|---|---|---|
| 改良型非対称2進数系データ圧縮装置の開発 | 藤崎礼志 | 金沢大学 |
| 産業財産権の種類、番号 | 出願年 | 国内・外国の別 |
| 特許、特願2019-189427 | 2019年 | 国内 |

〔取得〕　計0件

〔その他〕

金沢大学　研究者情報
https://ridb.kanazawa-u.ac.jp/public/detail.php?id=3123
金沢大学 教員情報データベース
https://ridb.kanazawa-u.ac.jp/public/detail.php?id=3123

6．研究組織

| | 氏名<br>（ローマ字氏名）<br>（研究者番号） | 所属研究機関・部局・職<br>（機関番号） | 備考 |
|---|---|---|---|

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

8．本研究に関連して実施した国際共同研究の実施状況

| 共同研究相手国 | 相手方研究機関 |
|---|---|