様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ６ 月　 ９ 日現在

機関番号：１３３０１
研究種目：基盤研究(C)
研究期間：2012～2014
課題番号：２４５６０４４５

研究課題名（和文）非線型力学系に基づく最適拡散符号の実現，最適ファミリーの構成と応用

研究課題名（英文）A realization of optimum spreading sequences based on nonlinear dynamical systems, a construction of their optimum family, and their applications

研究代表者
藤崎　礼志（FUJISAKI, HIROSHI）

金沢大学・電子情報学系・准教授

研究者番号：８０３０４７５７

交付決定額（研究期間全体）：（直接経費）　　4,100,000円

研究成果の概要（和文）：BER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を実現し，相関特性に関して最適な符号ファミリーを構成するために，最も基本的なNLFR最大周期列であるde Bruijn系列に注目し，以下の結果を得た．i)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構成方法を提案した．ii)de Bruijn系列に属するCR系列の存在に関するFredricksen の公開問題を解決し，de Bruijn系列の相異なる自己相関関数の個数の上界を導出した．iii)区間アルゴリズムの性能評価に関して，成分が有理数である一般の分布の場合に，既知の上界よりも良い評価式を与えた．

研究成果の概要（英文）：In this research, we studied a realization of optimum spreading sequences based on nonlinear dynamical systems and a construction of their optimum family. For their applications, we considered asynchronous spread spectrum multiple access communication systems. The main results in the three-year study are summarized as follows. i) Based on the theoretical bounds of the normalized auto- and cross-correlation functions for de Bruijn sequences, we experimentally characterized a good family of de Bruijn sequences in terms of the both normalized auto- and cross-correlation functions. ii) We settled the fundamental problem posed by Fredricksen on existence of the CR sequences in the de Bruijn sequences of length 2 to the n for any odd n. We obtained upper bounds of the total number of distinct auto-correlation functions for the de Bruijn sequences. iii) Using the induced transformations, we obtained sharp upper and lower bounds on the mean value of the stopping time of the interval algorithm.

研究分野：情報工学

キーワード：de Bruijn 系列　スペクトル拡散符号　最大周期列　CR系列　記号力学系　超離散力学系

1. 研究開始当初の背景

第 4 の IT 革命を迎えた携帯通信網は，使用量の爆発的増大と使用方法の質的激変を伴う大転換点にある．斯様な情報無線通信分野の発展を支える通信方式が CDMA(符号分割多元接続) である．3G(第三世代) 携帯電話通信や近距離無線通信では，CDMA 通信方式が製品化され，現行の 3.9G 通信 LTE(ロング・ターム・エボリューション) では， OFDMA(直交周波数分割多元接続) と相補的な役割を果たしている．この CDMA を実現するのがスペクトル拡散多元接続 (SSMA) 通信システムである．

現在，実用化された携帯電話のスペクトル拡散符号として，最大周期系列 (M 系列) に代表される代数的符号が使用されている．一方，独立同分布 (i.i.d.) 系列やマルコフ連鎖系列などの確率過程を実現する，非線型力学系 (カオス) に基づくランダム符号を拡散符号として用いることが提案されている．前者は代数系符号，後者は解析系符号とも言えるであろう．システム全体の性能評価を考えたとき，代数的な結果は相性が悪く，解析的な結果がビット誤り率 (BER) という重要な指標を与える．ここに力学系に基づくランダムな符号を用いる最大の利点があり，符号だけでなく，その符号が使用されるシステムまでも考えるという視点は，力学系から生成される符号を考えることによって初めて得られる．

本研究代表者は，線型フィードバックシフトレジスタ (LFSR) 最大周期列拡散符号設計の基礎となる代数学・線型数学とは全く異なる立場から，非線型力学系・確率解析の手法に基づいて，BER を精確に評価した [**IT11**]．この結果ゆえに種類数の大きい BER に関して最適な位相シフトフリー符号の設計に成功した [**IEICE07**], [**CAS08**]．しかし，非線型力学系・確率解析に基づくこれらの結果は連続的なものであり，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．

2. 研究の目的

本研究の目的は，BER 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．

上で述べた，非線型力学系・確率解析に基づく連続的な結果を離散化し，実際の二値有限系列 (ブロック) として具体的に与えるために，非線型フィードバックシフトレジスタ (NLFSR) 最大周期列を離散力学系の離散化 (超離散化) と考える [**IEICE05**]．本研究では，最も簡単かつ基本的な NLFSR 系列である de Bruijn 系列に注目する．

研究目的 I: 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，NLFSR 最大周期列の自己相関特性については，最も簡単な 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 [**Zhang**]．先に，本研究代表者は，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 [**NOLTA11**]．

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．最悪のペア以外の場合の相互相関特性の上界は [**Zhang**] で既に導出されている．

本研究では，最悪のペア以外の場合の相互相関特性の下界を考察する．さらに，これらの結果を統合することにより，自己および相互相関特性に優れた特性を有する de Bruijn 系列のファミリーを構成する．

研究目的 II: 上・下界は最悪値についての情報しか与えない．最適な符号ファミリーを構成するためには，どれだけ最悪値を与えるペアが存在するか，どのようなペアが最悪値を与えるかを知ることが必要である．そもそも相異なる自己相関関数の個数でさえ知られていない．

本研究では，長さ 2^n の de Bruijn 系列の相異なる自己相関関数の個数を数え上げを試みる．

陽に数え上げるためには，Fredricksen の問題を解決しなければならないことが明らかになる．ここで，Fredricksen は，長さ 2^n の de Bruijn 系列に対する相補反転 (complement reverse (CR)) 系列を定義し，n が偶数のときにはそれが存在しないことを指摘した．さらに，$n = 3, 5$ の場合にその存在例を示し，n が一般の奇数の場合に CR 系列が存在するか否かを問うた [**Fredricksen**]．これを Fredricksen の問題という．

研究目的 III: 擬似乱数の性能評価は，擬似乱数応用の可否の客観的判断基準を与える基本的かつ重要な課題である．

de Bruijn 系列は，最も簡単な Bernoulli 変換である二進展開写像における実数値解軌道の，有限列 (ブロック) による記号力学系的実現と見ることができる．一方，情報理論的乱数生成アルゴリズムである区間アルゴリズム [**Han & Hoshi**] の背後に，二進展開写像を含む Bernoulli 変換を見ることができる．

本研究では，離散力学系的立場から，区間アルゴリズムの性能を解析し，新たな知見を与える．

3. 研究の方法

研究目的 I に対する研究方法: [**Zhang**] の結果を考察し，[**NOLTA11**] の結果と統合することによって，de Bruijn 系列の最悪ペアとそれ以外のペアのそれぞれについて，相互および相互相関特性の上・下界の理論値を得ることができる．

本研究代表者が [**NOLTA10**] で与えた有界単調真理値表アルゴリズムにより，所望の長さの de Bruijn 系列を全て生成することができる．

計算機を用いて数値的に生成した各系列の自己および相互相関特性を解析し，相関値，その最大および最小値のデータベースを構築する．理論結果と数値実験より得たデータベースを利用して，自己および相互相関特性に優れた特性を有する de Bruijn 系列のファミリーを構成する．

研究目的 II に対する研究方法: グラフ理論ならびに系列全体の空間を考える記号力学系の手法を用いる．

まず，記号力学系的観点から CR 系列を特徴づける．得られた CR 系列の性質を考慮しながら，de Bruijn グラフを変形することによって，CR 系列を構成的に求め，de Bruijn 系列に属する CR 系列を全て生成するアルゴリズムを開発する．

開発したアルゴリズムを実装し，計算機を用いて，de Bruijn 系列に属する CR 系列を全て生成する．

研究目的 III に対する研究方法: 記号力学系的観点から，区間アルゴリズムを記号空間上の符号化と捉えることができることに注意する．エルゴード理論の手法を用いて，区間アルゴリズムを誘導変換として表現する．

次に，得られた変換を記号力学系的立場から解析し，区間アルゴリズムに付随する M-進展開写像の代数的構造を明らかにする．

以上の結果に基づき，区間アルゴリズムの基本的性能である停止時間の期待値を評価する．

4. 研究成果

研究目的 I に対する研究成果: 自己および相互相関特性の上・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構成方法も提案した [8].

研究目的 II に対する研究成果: 記号力学系的観点から CR 系列を特徴づける補題を導出した．補題を用いて，de Bruijn グラフを変形し，p が素数の場合に，長さ 2^{2p+1} の CR 系列を構成的に求めた．その結果を用いて，長さ 2^n の de Bruijn 系列の相異なる自己相関関数の個数の上界を導出した [4].

さらに、任意の奇数 $2m+1$ $(m \geq 1)$ に対して，長さ 2^{2m+1} の de Bruijn 系列に属する CR 系列を全て生成するアルゴリズムを開発し，Fredricksen の公開問題を完全に解決した [2].

計算機を用いて，$n = 5, 7$ の場合に長さ 2^n の全ての CR 系列を生成した．

研究目的 III に対する研究成果: 区間アルゴリズムを誘導変換で表現し，区間アルゴリズムはスライディング・ブロック符号でないことを明らかにした．

区間アルゴリズムの停止時間の期待値に対する新たな下界を与えた．均等分布の場合だけでなく，確率ベクトルの成分が有理数である一般の分布の場合に，停止時間の期待値に対して，[**Han & Hoshi**] の上界よりも良い評価式を陽に与えた [3].

＜引用文献＞

[**IT11**] 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, **57** (2011), pp. 1959–1967.

[**IEICE07**] H. Fujisaki, "Design of Optimum M-Phase Spreading Sequences of Markov Chains," IEICE Trans. on Fundamentals, **E90-A** (2007), pp. 2055–2065.

[**CAS08**] H. Fujisaki and H. Sugimori, "Phase-Shift-Free M-Phase Spreading Sequences of Markov Chains," IEEE Trans. on Circuit and Systems Part I, **55** (2008), pp. 876–882.

[**IEICE05**] H. Fujisaki, "Discretized Markov Transformations – An Example of Ultradiscrete Dynamical Systems –," IEICE Trans. Fundamentals, **E88-A** (2008), pp.2684–2691.

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

[**NOLTA11**] H. Fujisaki and Y. Nabeshima, "On Auto-Correlation Values of de Bruijn Sequences," NOLTA, IEICE, **3** (2011), pp. 400–408.

[**NOLTA10**] H. Fujisaki, "An Algorithm For Generating All Full-Length Sequences Which Are Based On Discretized Markov Transformations," NOLTA, IEICE, **1** (2010), pp. 166–175.

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

[**Han & Hoshi**] T. S. Han and M. Hoshi, "Interval algorithm for random number generation," IEEE Trans. Inform. Theory, **43** (1997), pp. 599–611.

5. 主な発表論文等

【雑誌論文】(計 9 件)

[1] Hiroshi Fujisaki, "An algorithm for generating all CR sequences in the de Bruijn sequences of length 2^n where n is any odd number," Proc. of the 37th Symposium on Information Theory and its Applications (2014), pp. 439–444.

[2] Hiroshi Fujisaki, “An algorithm for generating all CR sequences in the de Bruijn sequences of length 2^n where n is any odd number,” Proc. of the 2014 International Symposium on Nonlinear Theory and its Applications (2014), pp. 680–683, 査読有

[3] Hiroshi Fujisaki, “Entropy of the induced transformations associated with the interval algorithm,” NOLTA, IEICE, **5** (2014), pp.127–139, 査読有
DOI:http://doi.org/10.1587/nolta.5.127

[4] Hiroshi Fujisaki, “A construction of all CR sequences in the de Bruijn sequences of length 2^{2p+1} where p is a prime number,” NOLTA, IEICE, **5** (2014), pp.235–249, 査読有
DOI:http://doi.org/10.1587/nolta.5.235

[5] Hiroshi Fujisaki, “On Invariant Measures for the Markov-Dyck Shift,” Proc. of the 36th Symposium on Information Theory and its Applications (2013), pp. 411–416.

[6] 藤崎礼志, “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,” 電気通信普及財団 研究調査報告書, **28** (2013), pp. 355–363, 審査有

[7] Hiroshi Fujisaki, “Number Theoretic Analysis of the Induced Transformations Associated with the Interval Algorithm,” Proc. of the 35th Symposium on Information Theory and its Applications (2012), pp. 437–442.

[8] Hiroshi Fujisaki and Daisuke Yoshikawa, “On Cross-Correlation Values of de Bruijn Sequences,” Proc. of the 2012 International Symposium on Nonlinear Theory and its Applications (2012), pp. 883–886, 査読有

[9] Hiroshi Fujisaki, “On embedding conditions of shifts of finite type into the Fibonacci-Dyck shift,” Proc. of the IEEE Int. Symp. on Information Theory (2012), pp. 279–283, 査読有
DOI:10.1109/ISIT.2012.6284023

【学会発表】(計 4 件)
① Hiroshi Fujisaki, “A realization of optimum binary spreading sequences of Markov chains based on discretized β-transformations,” Workshop「数論とエルゴード理論」, 2015.2.8, 金沢大学サテライトプラザ (石川県)

② Hiroshi Fujisaki, “A construction of all CR sequences in the de Bruijn sequences of length 2^n where n is any odd number,” Workshop「数論とエルゴード理論」, 2014.2.8, 金沢大学サテライトプラザ (石川県)

③ Hiroshi Fujisaki, “A construction of all CR sequences in the de Bruijn sequences of length 2^{2p+1} where p is a prime number,” Sino-Japanese Workshop on Fractals and Dynamic Systems, 2013.12.27, Morningside Center of Mathematics & Tsinghua University Beijing, China

④ Hiroshi Fujisaki, “On Invariant Measures for the Markov-Dyck Shift,” Workshop「数論とエルゴード理論」, 2013.2.9, 金沢大学サテライトプラザ (石川県)

【図書】 (計 0 件)

【産業財産権】
○ 出願状況 (計 1 件)

名称：符号生成装置，符号生成方法，通信装置，解析装置
発明者：藤崎 礼志
出願人：金沢大学
種類：特許願
番号：特願 2013-166128
出願年月日：2013.8.1
国内外の別：国内

【その他】ホームページ等
http://ridb.kanazawa-u.ac.jp/public/detail.php?id=3123

6. 研究組織

(1) 研究代表者
藤崎　礼志 (FUJISAKI　HIROSHI)
金沢大学・電子情報学系・准教授
研究者番号：80304757

(2) 研究分担者
なし

(3) 連携研究者
なし