様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年 ４ 月 １ 日現在

機関番号：１３３０１
研究種目：基盤研究（Ｃ）
研究期間：2009～2011
課題番号：21560392
研究課題名（和文） 超離散力学系に基づく最適拡散符号の実現とその応用

研究課題名（英文） Construction of and applications for optimal spreading sequences based on ultra discrete dynamical systems

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

研究成果の概要（和文）：本研究では，超離散力学系に基づく最適拡散符号を実現し，SSMA 通信システムに応用するために，以下の結果を得た．i）SSMA 通信システムの性能評価に関する Yao の問題に対して，確率解析の立場から,完全な解答を与えた．ii）最適な位相シフトフリー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．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．iii）NLFSR 系列の内，de Bruijn 系列の自己相関特性の下界を理論的に導出することに成功した．

研究成果の概要（英文）：In this research we constructed optimal spreading sequences based on ultra discrete dynamical systems. For their applications, we considered asynchronous spread spectrum multiple access communication systems with spreading sequences of Markov chains. The main results in the three-year study are summarized as follows. i)By refinement of the large deviations analysis, we obtained exact asymptotic analyses of bit error probabilities in such systems. Comparing theoretical expressions of bit error probabilities with experimental results, we confirmed that for too small numbers of users compared to the lengths of spreading sequences,the central limit asymptotic analyses became invalid, but for large deviations asymptotic analyses turned out to be relevant. ii) We considered discretized piecewise-monotone-increasing Markov transformations and gave an algorithm, called the bounded monotone truth-table algorithm, for generating all full-length sequences which were based on the discretized transformations. The algorithm was applicable to generation of all de Bruijn sequences. iii) We gave a novel lower bound of the minimum values of the normalized auto-correlation functions for de Bruijn sequences.

交付決定額

（金額単位：円）

	直接経費	間接経費	合 計
2009 年度	1,400,000	420,000	1,820,000
2010 年度	1,200,000	360,000	1,560,000
2011 年度	1,000,000	300,000	1,300,000
年度			
年度			
総 計	3,600,000	1,080,000	4,680,000

研究分野：情報工学
科研費の分科・細目：電気電子工学・通信・ネットワーク工学
キーワード：超離散力学系，最大周期列，de Bruijn 系列，記号力学系，スペクトル拡散符号

１．研究開始当初の背景

今世紀に入ってから，情報無線通信分野の技術進歩に伴い，通信量は時間的にも空間的にも世界的に爆発した．斯様な情報無線通信分野の発展を支えている通信方式が 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た．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．

SSMA 通信システムにおいては，SS 変調の原理から，たとえ外部雑音のない理想的な通信路を用いたとしても，ビット誤りが起こり得る．この原因は，拡散符号の相互および自己相関であり，多元接続干渉(MAI)と呼ばれる．従って，拡散符号がシステムの性能を決定するといっても過言ではない．

現在，実用化された携帯電話の拡散符号として，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．

２．研究の目的

本研究の目的は，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とその応用である．そのためには，まず第一に，非同期 SSMA 通信システムのビット誤り生起確率の正確な理論評価式が必要である．

研究目的 I: Pursley が平均干渉パラメータ(AIP)を定義して以来,「ビット誤り生起確率は，AIP を分散とする標準正規分布（これを AIP を分散とする SGA と呼ぶ）で与えられる」という前提に基づき，非同期 SSMA 通信システムの性能評価が行われたきた．しかしながら,Yao は,i) ユーザ数が少ないとき,ii) 拡散符号の周期 N が短いとき，iii) 外部雑音が大きいときに，AIP を分散とする SGA は正確でないことを指摘した.このとき，次の問題が自然に生ずる：i) 何故，ユーザ数が少なく，周期 Nが短いとき，AIP を分散とする SGA は正確でないのか？ ii) ユーザ数が少なく，周期 Nが短い場合にも，より実験に近い簡明なビット誤り生起確率の理論評価式を導出せよ．この Yao の問題は，多くの通信工学者により考えられ，多種の評価式が提案されている．しかしながら，ある評価式は組合せ論を用いて厳密ではあるものの，式が複雑であり，計算量がユーザ数、拡散符号の周期 N に対して幾何級数的に爆発する，また，ある評価式は導出の物理的または理論的根拠が明確でない，などという問題があった．

以上の非同期 SSMA 通信システムの性能評価に関する Yao の問題に対して，確率解析の立場から，完全な解答を与えるのが本研究の目的の一つである．

研究目的 II: 非同期 SSMA 通信システムの性能評価に関する Yao の問題に対して，本研究代表者は，既に，独立同分布(i.i.d.)系列を特別な場合として含む，一般の区分線形(PL)マルコフ変換から生成される系列を考え，中心極限定理(CLT)に基づく独自の指標を提案した．これは，ユーザ数が少ない場合でさえ実験値をより良く説明する簡明な理論評価式である．さらに，AIP を分散とする SGA は CLT に基づく理論評価式の 0 次近似式であることを明らかにした．その結果に基づき，ビット誤り生起確率に関して最適な位相シフトフリーM(≧3)-相スペクトル拡散符号の設計に成功した．非線形力学系・確率解析に基づく以上の結果は連続的なものであり，最適な拡散符号を実現するためにはある種の離散化が必要となる．これに関して，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，その個数を与えるアルゴリズムを示した．しかしながら，その生成法は未解決の難問である．ここで，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．

非線形力学系・確率解析に基づいて得られた最適な位相シフトフリースペクトル拡散符号を実現するための一技術として，NLFSR 最大周期列を全て生成するアルゴリズムを与えるのが本研究の目的の一つである．

研究目的 III: 通信システムや暗号システムにおいて，基本的で重要な統計量として，相関特性が挙げられる．特に，自己相関関数は SSMA 通信の同期を確立する重要な統計量である．しかしながら，NLFSR 系列の相関特性については，最も簡単な de Bruijn 系列の場合でさえ，最大値の上界だけしか知られていない．LFSR 最大周期列の相関特性は，ガロア理論を用いて代数的に完全に解析できる．一方，NLFSR 最大周期列は，生来的に非線型性を有するため，その相関特性解析に代数的アプローチ・組み合わせ論的手法を用いても困難である．

相関関数に関して優れた性能を有する拡散符号ファミリーを構成するために，NLFSR

最大周期列の相関特性の理論的上下界を与えるのが本研究の目的の一つである．

３．研究の方法

研究目的 I に対する研究方法: 非同期 SSMA 通信システムのビット誤り生起確率の精確な理論評価式を導出し，上記 Yao の問題に対する完全な解答を与えるため，確率解析の手法を用いる．本研究では，特に，大偏差原理(LDP)を用いる．一方，マルコフ連鎖に基づく非同期 SSMA 通信によるデータ伝送数値実験を行い，通信の誤り生起確率を調べ，確率論が与える理論値との比較を行う．これらと既に得られている CLT の評価式を合わせることにより，非同期 SSMA 通信システムのビット誤り生起確率の漸近挙動を精確に考察することができる．

研究目的 II と III に対する研究方法: NLFSR 最大周期列を超離散力学系に基づく最大周期列と捉えることにより，NLFSR 最大周期列を全て生成するアルゴリズムを与え，NLFSR 最大周期列の相関特性の理論的解析を行う．そのために，系列全体の空間を考える記号力学系の手法を用いる．理論的証明には，力学系的な発想だけでなく，組合わせ論とグラフ理論が大きな役割を果たす．数値実験は NLFSR 最大周期列全ての場合を尽くし，実現される系列および相関値の最大・最小値のデータベースが作成される．これら理論および実験結果により，実現される全ての NLFSR 最大周期列から，相関値に関して最良な最大周期列のファミリーが構成される．

４．研究成果

研究目的Ｉに対する研究成果: マルコフ連鎖拡散符号を用いた非同期 SSMA 通信システムを考え，MAI の経験平均に LDP が成立する事を示した．得られた結果を精密化し，拡散符号の周期長 Nが短く，且つ，ユーザ数 Jが少ない場合のビット誤り確率の理論評価式を求めた．それと先の研究で既に求めた CLT に基づく理論評価式及び実験値との比較を行ない，$J/N<1/10$ になると，CLT に基づく評価式よりも LDP に基づく評価式の方がより実験に近くなることを確認した．これは，$J/N<1/10$ になると，LDP で説明される漸近挙動が支配的となることを意味する[IEEE Trans. IT, 57(2011)]．

研究目的 II に対する研究成果: NLFSR 最大周期列を全て生成法は未解決の難問であったが，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ことができるという意味において，提案したアルゴリズムは効率的である．また，これまでに提案されたアルゴリズムの様に，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，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．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[NOLTA, IEICE, 1(2010)]．

研究目的 III に対する研究成果: NLFSR 最大周期列の内，最も基本的な de Bruijn 系列の自己相関関数に注目し，その最小値の下界を理論的に与えた．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．同時に，実験的に，ワーストケースを与える最大周期列を調べ，自己相関関数を利用した系列の選別方法，良い自己相関数を有するファミリーの構成法を提案した[NOLTA, IEICE, 2(2011)]．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 8 件）

①Hiroshi Fujisaki and Yuhki Nabeshima, ″On Auto-Correlation Values of de Bruijn Sequences,″ Nonlinear Theory and Its Applications, IEICE, 2(2011), 400-408, 査読有

②Hiroshi 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), 1959-1967, 査読有

③藤崎 礼志, 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, 電気通信普及財団研究調査報告書, 25(2010), 274-282,審査有

④Hiroshi Fujisaki, ″ On embeddings of shifts of finite type into the golden-mean-Dyck shift,″ Proc. of the 2009 International Symposium on Information Theory and its Applications, (2010), 583-588, 査読有

⑤ Hiroshi Fujisaki, ″An Algorithm For Generating All Full-Length Sequences Which Are Based On Discretized Piecewise-Monotone-Increasing Markov Transformations,″ Nonlinear Theory and Its Applications, IEICE, 1(2010), 166-175, 査読有

⑥Hiroshi Fujisaki and Yuhki Nabeshima, ″On Auto-Correlation Values of de Bruijn Sequences,″ Proc. of the 2010 International Symposium on Nonlinear Theory and its Applications, (2010), 414-417, 査読有
⑦ Hiroshi Fujisaki, ″An Algorithm For Generating All Full-Length Sequences Which Are Based On Discretized Markov Transformations,″ Proc. of the 2009 International Symposium on Nonlinear Theory and its Applications, (2009), 191-194, 査読有
⑧ Hiroshi Fujisaki, ″Entropy of the Induced Transformations Associated with the Interval Algorithm,″ Proc. of the IEEE Int. Symp. on Information Theory, (2009), 2056-2060, 査読有
〔学会発表〕(計 4 件)
① Hiroshi Fujisaki, ″On Invariant Measures for the Fibonacci Dyck Shift,″ Workshop「数論とエルゴード理論」, 2012.2.18, 金沢大学サテライトプラザ(石川県)
② Hiroshi Fujisaki, ″On Embeddings of Shifts of Finite Type into the Golden-Mean-Dyck Shift,″ 研究集会「記号力学系とその応用」, 2011.3.30, 九州大学西新プラザ(福岡県)
③ Hiroshi Fujisaki, ″On Embeddings of Shifts of Finite Type into the Golden-Mean-Dyck Shift,″ Workshop「数論とエルゴード理論」, 2011.2.20, 金沢大学サテライトプラザ(石川県)
④ Hiroshi Fujisaki, ″On Invariant Measures for the Golden-Mean-Dyck Shift″ Workshop「数論とエルゴード理論」, 2010.3.7, 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, 通信装置, 符号生成方法, 及びプログラム
発明者：藤崎　礼志
権利者：藤崎　礼志
種類：特許願
番号：特願 2010-95566
出願年月日：2010.4.17
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