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 6 月 6 日現在

機関番号：82636
研究種目：基盤研究（C）
研究期間：2009 ～ 2011
課題番号：21560388
研究課題名（和文）　情報理論における基本的未解決問題の探求

研究課題名（英文）　Studies on Fundamental Problems in Information Theory

研究代表者
小林　欣吾（Kobayashi Kingo）
独立行政法人情報通信研究機構ネットワークセキュリティ研究所 R&D アドバイザー
研究者番号：20029515

研究成果の概要（和文）：
現代の情報ネットワークシステムの理論的基礎理論において未だ解決されていない基本的問題のうちから干渉通信路や有限状態通信路などに焦点をあて、問題の解明に向けた理論的検討を行い、さらに、マルチユーザ通信への適用が期待されている低密度の格子に基づくLDPC符号についての理論的解析、近似的ガウス分布を用いた計算量を大幅に削減する復号方法の提案等を行い、実用性を高める研究も行った。

研究成果の概要（英文）：
We proceeded the theoretical studies on several open topics of modern information network systems, especially focused on problems of the interference channel and finite state channels such as the trapdoor channels. We gave transparent aspects on the difficulties contained in the problems. Moreover, we also concentrated the topics on LDPC codes based on the lattice, and proposed decoding algorithms using approximated Gaussian distributions for real-world applications.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,500,000	450,000	1,950,000
2010 年度	1,000,000	300,000	1,300,000
2011 年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,500,000	1,050,000	4,550,000

研究分野：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：情報理論，符号化，ネットワーク・LAN，有限状態通信路，隠れマルコフ情報源，離散情報システム

１．研究開始当初の背景

多元情報理論，多端子情報理論とも呼ばれる，現代の情報ネットワークシステムの理論的基礎を研究するマルチユーザ情報理論で

は大きな成果とともに，未だ解決されていない基本的問題が山積している。放送通信路，中継通信路，干渉通信路，双方向通信路などの通信路容量域決定問題は特殊な条件の下で以外は未解決であった。ことに、本来的にマルチユーザ環境である通信ネットワーク，ワイヤレス情報通信においてみられる多利用者が発する信号，データの互いの干渉をいかに克服するべきかという問題の本質を捉えている干渉通信路の問題が欧米の通信理論の研究者の注目を集めており，その通信路容量決定問題は最近の国際的な情報通信のワークショップでは重要なテーマとして位置づけられていた。これらのマルチユーザ情報理論研究の状況を認識した上で，古典的な情報理論に目を向けてみると，そこにも基本的な未解決問題が数多く横たわっていることがわかる。通信路が記憶をもつ場合については，特殊な例を除いて通信路容量を解析的あるいは数値的に求めることができていない。このことは，記憶ある通信路を通して効率的に情報を伝達するには入力する符号系列を如何に構成すべきかの指針さえ与えられていないことを意味していた。

２．研究の目的

見かけは単純なことでも未だに解決困難な問題が数多く残されている。その中で，有限状態通信路の通信路容量決定問題を取り上げ，解決に向けての道筋をつけることを一つの目標とした。関連して，隠れマルコフ情報源のエントロピーの計算法の高速化アルゴリズム，および，そのデータ系列の圧縮アルゴリズムの提案に向けて研究を進めた。次に，マルチユーザ情報理論の大きな課題である干渉通信路の容量問題に取り組んだ。それとともに，干渉通信路における符号の構成，復号アルゴリズムの提案することを目的とした。

３．研究の方法

情報理論における諸問題を理論的解析,符号化方式・アルゴリズムの提案・実装,および関連分野への展開,の３つに分類し,体系的に取り組んだ。平成 21 年度では，有限状態通信路の通信路容量解析,ならびに隠れマルコフ情報源からのデータの情報圧縮技術の確立をめざし，平成 22 年度以降は，干渉通信路の理論的検討と，実用に向けての符号設計ならびに復号アルゴリズムの提案と実装を計画した。また，単純な機械による系列の秩序生成問題に理論的検討にあたった。

４．研究成果

21年度（初年度）は、有限状態通信路の通信路容量問題に関して，入力系列を隠れマルコフ情報源で近似することによる効果について研究を行い，ドイツで開催されたDagstuhl Seminarで発表した。さらに，マルチユーザー情報理論の基本問題である干渉通信路容量問題についての最近の展開を情報とダイナミクスIII研究集会（九州大学）における招待講演で展開し，また残された問題に対する展望を電子情報通信学会IT研究会の特別講演として与えた。さらに，電子透かしと誤り訂正符号化に関する問題に関して、QIM（Quantization Index Modulation）方式、dither modulationなどの埋め込み手法を用いた音楽電子透かしに対するMP3圧縮符号化攻撃の特性を探求した。音楽電子透かしとしてLDPC符号を用いた実用的な方式の提案を行うとともに、情報理論的な通信路解析、LDPC符号の復号法についての提案を行っている。また，新しい誤り訂正符号の研究として今後の発展が期待される格子符号をとりあげ、低密度の格子に基づくLDPC符号についてNoise Thresholdsを用いた理論的解析、近似的なガウス分布を用いる復号方法の提案等を行い、実用性を高める研究を行った。

22年度（次年度）は、有限状態通信路の通信路容量問題に関連してハノイの塔の問題にみられる再帰構造の特徴について，Bielefeld（ドイツ）で開催されたZIF Workshop Search Methodologiesで発表した。さらに，マルチユーザ情報理論の基本問題である干渉通信路容量問題についての最近の展開を台中（台湾）で開かれた 2010 International Symposium on Information Theory and its Applications (ISITA)において特別講演として与えた。また，干渉のある通信路の問題として、すぐれた性能をもつ符号化と復号のアルゴリズムの検討を行った。多様なマルチユーザ通信へ適用可能なものとして格子符号(lattice)は通信路容量の限界に達する符号化として知られているが、実用面では復号の複雑さに問題がある。本研究ではlatticeの復号の計算量を大幅に削減する新しいアルゴリズムを提案した。このアルゴリズムは低密度lattice符号(LDLC)に対して、belief-propagation復号においてメッセージの単一ガウス近似を用いることにより、性能の劣化なしで計算の大幅な削減を実現している。干渉通信路符号化の例として、(1)フラッシュメモリの符号化、(2)音楽、動画の電子透かし方式を取りあげた。(1)においては、干渉通信路に対するdirty-paper codingとして解釈できることを示し、latticeを利用した符号化法を与えた。(2)では、埋め込みデータ量は大きいが、攻撃耐性が比較的弱いQIM方式とLDPC符号を組み合わせた方式が優れることを確認し、それに基づく電子透かし方式を実現した。音楽用の電子透かしとしてデータ埋め込み量がこれまで世界で提案された方式の中で最大で、攻撃耐性の面でも64kBPSのMP3圧縮にも耐えうる最良の性能を有している。

23 年度（最終年度）は、有限状態通信路の問

題について探求を深め、Boppard(ドイツ)で開催された 7-th Asia-Europe workshop on Information Theoryにおける招待講演として、落し戸通信路の通信路容量の値をこれまでより精密に求めた結果を含めて発表した。さらに、San Diego(USA)にて開催された ITA 2012 において、2 進系列の部分列の構造を詳細に調査した結果を発表した。これは新しいデータ圧縮の方式や情報セキュリティへの応用が期待される内容を含んでいる。また、一般的な離散無記憶通信路における量子化問題の具体例として、２元入力通信路に対して有効な量子化器を求める多項式時間アルゴリズムを提案した。この量子化アルゴリズムは通信路の入力と量子化器の出力の間の相互情報量を最大化することを証明し、量子化通信路の容量の新しい計算方法を提案した．さらに，1）データのクリッピングにより生じる同期誤りに対してより優れた誤り制御方式を提案し，また，画像電子透かしなどの２次元データへの適切な符号語配置を提案した。2）振幅攻撃に弱点を持つ LDPC 符号を用いた前年提案した音楽電子透かし方式に対し、音の位相情報にデータを埋め込む方式を導入し改善を行った。3)E8 lattice 符号、Low Density Lattice 符号などの記憶素子に対する符号化の新しい構成、および、理論的な解析を行った。

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 6 件）

1. B. Kurkoski and J. Dauwels, Reduced-memory decoding of low-density lattice codes, IEEE Communications Letters, Vol. 14 No.7, pp.659-661, 2010, 査読有..
2. J. A. Mendoza-Noriega, B. M. Kurkoski, M. Nakano-Miytake, and H. Perez-Meana, Image authentication and recovery using BCH error-correcting codes, International Journal of Computers, Vol. 5 No.11, pp.26-33, 2010, 査読有.
3. Raul MartinezZ-Noriega, Isao Abe, Kazuhiko Yamaguchi, Self-synchronizable decoding algorithms for transmission with redundant information at decoder, IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E93-A No.11, pp.1958-1965, 2010, 査読有.
4. Brian Kurkoski and Hideki Yagi, Concatenation of a Discrete Memoryless Channel and a Quantizer, in Proceeding of IEEE Information Theory Workshop, pp. 160-164, 2010, 査読有.
5. Brian Kurkoski, Kazuhiko Yamaguchi and Kingo Kobayashi, Single Gaussian Messages and Noise Thresholds for Decoding Low-Density Lattice Codes, in Proceeding of IEEE Intl. Symposium on Information Theory, pp. 734-738, 2009, 査読有.
6. Brian Kurkoski, Justin Dauwels and Hans-Andrea Loeliger, Power-Constrained Communications Using LDLC Lattices, in Proceeding of IEEE Intl. Symposium on Information Theory, pp. 739-743, 2009, 査読有.

〔学会発表〕（計 27 件）

1. B. M. Kurkoski, Write Amplification and WOM codes in SSDs, フラッシュメモリ符号化に関するワークショップ, 電気通信大学、東京都, 2012年3月15日.
2. B. M. Kurkoski, Towards computation of the capacity of quantized discrete memoryless channels, 2012 Information Theory and Applications Workshop, Catamaran Hotel and Resort, San Diego, CA, USA, Feb. 7, 2012.
3. K. Kobayashi, A Structure in Compositions of Subsequences of Binary Sequence, 2012 Information Theory and Applications Workshop, Catamaran Hotel and Resort, San Diego, CA, USA, Feb. 6, 2012.
4. B. M. Kurkoski, Improved analytic expression for write amplification in NAND flash, International Conference on Computing, Networking and Communications 2012, Hyatt Regency Maui Lahaina, Hawaii, USA, Feb. 1, 2012.
5. B. .M Kurkoski, Notes on a lattice-based WOM construction that guarantees two writes, 第３４回情報理論とその応用シンポジウム，ホテル森の風鶯宿，岩手県，2011年12月1日.
6. B. M. Kurkoski, One-bit LDPC message passing decoding algorithm based on maximization of mutual information, LDPC符号ワークショップ, 東京工業大学, 東京都, 2011年9月30日.
7. B. M. Kurkoski, Robust image hashing using image normalization and SVD

decomposition, 54rd IEEE International Midwest Symposium on Circuits and Systems, Yonsei University, Seoul, Korea, Aug. 9, 2011.

8. K.Kobayashi, Some Aspects on Finite State Channels (invited talk), 7-th Asia-Europe Workshop on Concepts in Information Theory, Bellevue Rheinhotel, Boppard, Germany, July 28, 2011.
9. B. M. Kurkoski, The E8 lattice and error correction in multi-level flash memory, IEEE International Conference on Communications, 国際京都国際会館、京都府, June 6, 2011.
10. B. M. Kurkoski, Lattices for error correction and rewriting in flash memories, Non-Volatile Memories Workshop, UCSD, San Diego, USA, March 7, 2011.
11. B.M.Kurkoski, Rewriting flash memories and dirty paper coding, Information Theory and Applications Workshop, UCSD, San Diego, USA, Feb. 7, 2011.
12. 齋藤真吾・栗原正純・山口和彦, 信頼度情報と消失訂正を用いた動画像向け電子透かし, 電子情報通信学会情報セキュリティ研究会, 機械振興会館, 東京都, 2010年12月15日.
13. B. M. Kurkoski, Rewriting codes for flash memories based upon lattices, and an example using the E8 lattice, IEEE Global Telecommunications Conference, Hyatt Regency Miami, Miami, USA, Dec. 6, 2010.
14. K. Kobayashi, An overview of multi-user information theory(Plenary Lecture), Int. Symposium on Information Theory and its Applications (ISITA), IEICE, Evergreen Laurel Hotel,Taitun, Taiwan, Oct.20, 2010.
15. R. Martinez-Noriega, B. Kurkoski, K. Yamaguchi and K. Kobayashi, Recovering synchronization with iterative decoders: LDPC codes, Int. Symposium on Information Theory and its Applications (ISITA), IEICE, Evergreen Laurel Hotel, Taitun, Taiwan, Oct.19, 2010.
16. R. Martinez-Noriega, M. Nakano, and K.Yamaguchi, Self-Synchronous Time-Domain Audio Watermarking Based on Coded-Watermarks, Int. Symposiumon Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Darmstadtium, Darmstadt, Germany, Oct.15, 2010.
17. J. A. Mendoza-Noriega, B. M. Kurkoski, M. Nakano-Miyatake, and H. Perez-Meana, Image authentication based on DCT with recovery capability, 10th WSEAS International Conference on Applied Computer Science, Iwate Prefectural Univ., 岩手県, Oct. 6, 2010.
18. J. A. Mendoza-Noriega, B. M. Kurkoski, M. Nakano-Miyatake, and H. Perez-Meana, Halftoning-based self-embedding watermarking for image authentication and recovery, 53rd IEEE International Midwest Symposium on Circuits and Systems, Westin Hotel, Seattle, USA, Aug. 3, 2010.
19. Kingo Kobayashi, Recursive structure of Hanoi tower with more than three poles, Information Theory and Applications Workshop, UCSD, San Diego, USA, Feb. 5, 2010.
20. Brian Kurkoski and Hideki Yagi, Optimal non-uniform quantization of LDPC decoders, Information Theory and Applications Workshop, UCSD, San Diego, USA, Feb. 2, 2010.
21. Brian Kurkoski and Hideki Yagi, Concave Programming Approaches for Mutual Information Minimization, 第３２回情報理論とその応用シンポジウム, SITA2009, pp. 527-531, 湯田温泉かめ福, 山口県, 2009年12月3日.
22. 小林欣吾, 干渉通信路に対する符号化問題の歴史と展望(特別講演), 電子情報通信学会, 情報理論研究会, 信学技報, 湯田温泉かめ福, 山口県, 2009年12月1日.
23. 小林欣吾, 干渉通信路符号化問題の最近の展開(招待講演), 第１部, 第２部, 情報とダイナミクスIII研究集会, 九州大学, 福岡県, 2009年10月9日.
24. Brian Kurkoski and Hideki Yagi, Locally Optimal Message Quantization for Binary LDPC Decoding, 電子情報通信学会 LDPC符号ワークショップ, IT2009-43, vol. 109, no. 212, pp. 61-66, 上智大学, 東京都, 2009年9月30日.
25. R. Martinez-Noriega, M. Nakano and K. Yamaguchi, “On the channel characteristic of dither modulation data hiding for MP3 compression,”IEEE Int. conf. on Intelligent Information Hiding and Multimedia Signal Processing, Ritsumeikan Univ., Kyoto Japan, Sep. 14, 2009.
26. R. Martinez-Noriega, M. Nakano, B. Kurkoski, K. Yamaguchi and K. Kobayashi, “Analysis of QIM-based audio watermarking using LDPC codes,”

IEEE Midwest Symposium on Circuits and Systems (MWSCAS), Fiesta Americana Condesa Cancun, Cancun Mexico, August 3, 2009.
27. Kingo Kobayashi, Some Aspects of Finite State Channel related to Hidden Markov Process, in Dagstuhl Seminar Proceedings on Search Problems, Schloss Dagstuhl, Dagstuhl, Germany, July 10, 2009. http://drops.dagstuhl.de/portals/index.php?semnr=09281

〔図書〕（計２件）

1. 小林　欣吾, 朝倉数学ハンドブック[応用編］ IX 情報の理論, 朝倉書店、pp. 573-605, 2011.
2. 小林 欣吾, 現代数理科学事典第２版　第VIII章 情報の理論, 丸善, pp. 823-971, 2009.

６．研究組織

(1)研究代表者

小林　欣吾(Kobayashi Kingo)
独立行政法人情報通信研究機構ネットワークセキュリティ研究所R&Dアドバイザー
研究者番号：20029515

(2)研究分担者

山口　和彦(Yamaguchi Kazuhiko)
電気通信大学大学院情報理工学研究科・准教授
研究者番号：60220258

ブライアン クルカスキー(Brian Kurukoski)
電気通信大学大学院情報理工学研究科・准教授
研究者番号：80444123

(3)連携研究者

（　　）

研究者番号：