様式 C-19

科学研究費補助金研究成果報告書

平成２１年　３月３１日現在

研究種目：基盤研究（Ｃ）
研究期間：２００７～２００８
課題番号：１９５６０３７１
研究課題名（和文）情報理論的手法用いた非二元ＬＤＰＣ符号とその復号法設計
研究課題名（英文）Information-Theoretic Methods for Non-binary LDPC and Their Decoders
研究代表者
Brian Kurkoski（クルカスキー　ブライアン）
電気通信大学・電気通信学部・准教授
研究者番号：80444123

研究成果の概要：
非二元 LDPC 符号に対する新しい復号アルゴリズムを開発した。領域計算量（メモリ量）が大幅に軽減されている。密度発展法に基づいた性能解析を行い、noise threshold を求めた。非二元では計算量が大きい belief propagation 復号に近い性能（訂正能力）を実現している。また非二元 LDPC 符号タイプに対して、復号アルゴリズムの計算量が低減する情報理論的な方法の開発、不均一保護能力に基づく解析、記憶のある通信路に対する復号、電子透かしへの応用などを行っている。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	1,500,000	450,000	1,950,000
２００８年度	900,000	270,000	1,170,000
総　計	2,400,000	720,000	3,120,000

研究分野：工学
科研費の分科・細目：電気電子工学・ネットワーク工学
キーワード：情報基礎、情報通信工学、Lattice codes、Non-binary LDPC Codes、誤り訂正符号、復号アルゴリズム、密度発展法、Kullback-Leibler ダイバージェンス

１．研究開始当初の背景

我々は確率伝播(belief propagation)を用いた誤り訂正符号の復号アルゴリズムを低密度パリティ検査符号(LDPC codes, low density parity check codes)、ターボ符号などの符号だけでなく、磁気記録通信路やバースト誤り通信路への適用やターボ等価、復調の量子化問題など、様々な分野への適用を検討してきた。
そうした中で、二元 LDPC 符号は、誤りの無い符号化通信を実現可能な限界、シャノン限界(Shannon limit)に迫る性能を実現する実用的誤り訂正符号として、次世代の無線通信(WiMAX IEEE 802.16)やデジタルビデオ放送(digital video broadcasting; DVB)等への誤り訂正符号として標準化案が提案されている。
一方リード・ソロモン符号等の非二元符号はデジタルビデオ/オーディオや、ハードディスクなどの磁気記録システムで広く使われている。さらに通信は、我々一般社会の様々な分野に広がっている。大容量記録システムや光ファーバーによる高速大容量の応用はもちろんのこと、センサーネットワーク、ア

ドホックネットワーク、ソフトウエア無線といった新しい応用に対して、高信頼の通信(記録)を実現する努力が不可欠である。

近年非２元の LDPC 符号も研究が始められているが、有効な解析手法、設計方法が利用されておらず成果は限定的であった。

２．研究の目的

本研究では非2元誤り訂正符号を対象として、符号の解析と設計およびと非2元符号に適した復号アルゴリズムの開発と解析をあわせて行うことを目的とする。本研究ではこれまでの二元符号などへの成果をさらに発展させて新しい非二元の符号すなわち実用的なGF(q)上のLDPC符号の設計とそれに適する復号アルゴリズムの開発を目的とする。 これには、二元符号に対するベクトル量子化を復号アルゴリズムの状態尺度(state metrics)に利用したことや、効率的な復号アルゴリズムをさらに発展させた方式を実現し、そのための解析設計手法を構築する。

（１）研究目的の詳細(2詳細:なにをどこまで明らかにしようとするのか)

本研究では確率伝播を用いた復号をそのまま利用するのではなく、より一般化したmessage passing 復号法で置き換えた新しい復号法を新たに提案し、その上でより優れた方式の実現を図る。
この復号法では確率伝播(あるいはmessage-passing)させる値をベクトル量として捕らえることで解析を容易にし、さらに復号アルゴリズムの高速化や計算領域の削減による省力化等の最適化を実現できる。
これはベクトル量としてとらえることで情報理論のベクトル量子化の手法に基づく解析、効率化の手法が適用できることやこれまでのテーブルルックアップ復号アルゴリズムの設計手法が利用できる。
これにより局所的に最適(ローカルオプティマル)なだけの結果に陥ることを避けてグローバルオプティマルな出力結果を得られるように復号アルゴリズムの最適化も実現しうる。
そうした方式の実現のため以下の点①～③を明らかにする:

① 解析: 非二元のLDPC符号に対して、密度発展法や一般化EXITチャート法による解析手法を利用して収束性の解析を行う。この手法はLDPC符号やターボ符号の雑音に対する特性限界(以下、noise thresholds)を解析する手法としてよく用いられている。この解析手法により非正則非二元のLDPC符号が現在得られている最良の二元LDPC符号(こちらも当然非正則符号である)より優れた性能を有することがすでに示唆されている。この研究では以下②で具体的に設計した非二元のLDPC符号に対して解析を行う。また、③で検討する新しい復号アルゴリズムにも適する様に、解析アルゴリズムを拡張する。
注)ここに正則非正則とはLDPC符号の検査行列内の各行および各列の非零の要素の数が行、列それぞれに一定であるものを正則、そうでないものを非正則という。

② 符号設計： 正則、非正則両方の非二元のLDPC符号を設計する。 Noise thresholdsを改善するため符号設計と復号アルゴリズムの最適化を一体に行う必要がある。初めによいnoise thresholds特性を持つ符号を求める。その後、 progressive edge growth (PEG) の方式やarray符号化の方式などを利用して有限長の符号を設計する。最終的な性能評価のため、そうした符号に対して、最小距離、girthなどの量の解析や計算機シミュレーションによる実験評価を行う。

③ 実装: この研究の最終的な目標はよい非二元のLDPC符号とそれにてきした新しい準最適復号アルゴリズムを実現することである。これは現在実用化進められている二元LDPC符号と確率伝播復号の組み合わせより優れた性能を有することが期待される。この復号アルゴリズムでは量子化問題を含めて最適化した復号アルゴリズムが設計される。ルックアップテーブルを利用する高速な実装が可能な方法も検討される。性能はアルゴリズム適用によるビット誤り率とあわせてアルゴリズムの効率や複雑さを検証することで行われる。

（２）研究背景(研究の学術的背景:研究動向補足)
近年、非二元のLDPC符号の研究は増えており、実用に対する期待が高まってきている。すでに正則な符号においては非二元符号の優位性は明白になっている。特に実用的な観点においてDaveyらは、すでに1998年の時点において短い符号長の場合に非2元符号の方が優れた性能を示すことをsphere packing boundを用いて示している。2004年にDeclecqらは非2元符号の方が良いnoise thresholdsを持つことを示した。しかしながら、非二元という性質から、フーリエ変換を利用する、大きなメッセージベクトルを扱わねばならないなど、非二元のLDPC符号の確率伝播に基づく復号アルゴリズムやその解析は大変複雑である。解析においてはガウス近似法が利用できるが、厳密な解析には向かないしそもそも復号そのものには適用できない(Bennetan, et al., 2006)。 一方、この研究で検討する方法はそうした非二元の復号を量子化された受信情報

の精度を含めて厳密に解析できる。また検討する復号アルゴリズムは、LDPC符号の提案者Gallager提案するの復号法にも通じるものでり優れた方式の実現が期待される。Gallagerの復号法は良い復号特性と計算量が小さいことが確認されており(Richardson, et al 2001)、そうした性質を生かす方式が期待される。またこの研究に関連して有限長のLDPC符号とストカスティックな復号器の解析などのさらに進んだ問題への発展も可能と考えられる。

（3）おわりに(学術的な特色・独創的な点・予想される結果と意義)

非2元のLDPC符号は今後の情報通信システムにおいて重要な役割を持つことが期待される。そうした符号やそれに関する解析方法、復号法の設計がなされることは大きな意義
がある。また本研究では確率伝播に基づく復号とそのための符号に関して新しい解析方法を実現する。この解析方法は漸近的な手法ではなく、実用に即した符号化方法や復号方法の細かな部分を含めて解析できるので理論的、実用的両面から符号設計・復号アルゴリズムの設計の方法を与えることができる。また情報源符号化の手法を取り入れる解析は独創的かつ有効な手法と考える。なお、この研究課題に関係する内容の一部分は2006年情報理論とその応用シンポジウムにて発表予定である。

3．研究の方法

（1）平成 19 年度

既存の復号アルゴリズムとして Gallager らの BCJR アルゴリズム等を基にしてアドホックな message-passing 集合に関して量子化された復号アルゴリズムのデザインと解析を行った。この研究は続く平成 20 年度に計画する詳細な理論的な解析の下地となる。研究は以下のようなステップを掲げ進められた。

①第一段階:アドホックな message-passing 復号器の設計（平成 19 年度前半）

提案する解析方法、符号設計法、復号アルゴリズムに加えて、message-passing 情報の集合の表現法について基本的な検証を加えた。これにより必要かつ十分な評価対象を設定した。

・アドホックな message-passing 情報の集合と復号アルゴリズムの基本的則のデザイン。
・実用に近い形での評価の準備。

②第二段階: 高度な最適化手法の適用と検証(平成 19 年度後半より)

第一段階で設計したアドホックな message-passing 復号器に基づいて message-passing 手法の一般化させた新しい復号アルゴリズムを実装を図った。

・新しい復号アルゴリズムへの展開。
・新しい復号アルゴリズム検証と修正。
・非正則な非二元 LDPC 符号の設計
・量子化されたシステムと実用の見地からの基礎的な検討。

（2）平成 20 年度

第二段階の後期としてさらに詳細に進めた。19 年度後半では、第二段階の前期として、検証範囲を限定した guided search であったが、対象を拡大し、より一般的な成果を得ている。

③第三段階:実用化に向けた検討(平成 20 年度)

・精度を高めた復号アルゴリズムの最適化。
・正則および非正則な非 2 元 LDPC 符号の詳細な解析と設計。
・実用に即した性能評価。

という形で進めた。

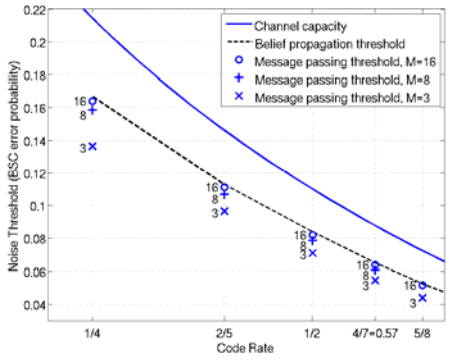

図 1. Noise thresholds for proposed LDPC decoding method.

4．研究成果

研究の第一段階として、我々は、非二元LDPC符号に対する新しい復号アルゴリズムを開発した。 その目標は、計算量の小さいアルゴリズムとくに、このアルゴリズムで負担の多い領域計算量（メモリ量）の軽減を達成した。このアルゴリズの解析・性能評価を密度発展法に基づき行い、noise thresholdを求めた。よく知られるが、非二元では計算量が大きいbelief propagation復号に近い性能を実現している。

研究の第二段階として、より高度な解析をすすめた。解析評価は、q 元消失通信路に対して行い、さらに実用的な視点からの評価として二元対称通信路に対して行っている。より基本的な二元元符号に対する評価と比較してアルゴリズムの最適化を進めた。

また、より実践的な非二元LDPC符号として実数体上の低密度のLattice符号を再定義として提案されたものを対象として実際上の性能評価を行った。10000の大きな格子ではメモリ量が、高々3.4%にまで削減でき、復号性能

の劣化はほとんど無かった。次元数が100程度の格子符号の場合でも0.2dB程度の劣化であることを確認している。

また非正則LDPC符号の設計のため不均一保護能力に基づく解析などの研究、記憶のある通信路に対する復号アルゴリズムの研究、様々な電子透かしへの応用とそのための高度な復号方法の検討を関連する問題として行った。

研究の最終段階として、以下の2つの非二元LDPC符号タイプに対して、復号アルゴリズムの計算量が低減する情報理論的な方法を開発した。この方法の1番目の応用として、有限体上(二元を含め)で定義された符号に対して、相互情報量を局所的に最大化する方法を提案した。VLSIなどでbelief propagation復号を実現する場合に対しては、メッセージを表現するビット数を少なくできることを発見した。例えば、図１のように、4ビットで表現する代わりに3ビット表現を用いても性能劣化が無いことが確認されている。

さらに、2番目の応用として、低密度行列で定義された格子符号に対して、Kullback-Leiblerダイバージェンスを局所的に最大化する復号アルゴリズムも提案した。図2に示すように３つのガウス分布の混合（波線）をmoment matchingで近似できる。

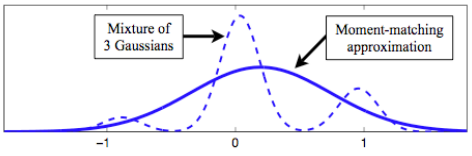

図 2. Moment-matching approximation minimizes Kullback-Leiber divergence

ここにおいて、メッセージを2つの数字だけで表現する我々のアルゴリズムの特長を反映した密度発展法を用いることにより効率的な性能解析を行い、格子符号の最適設計を与えた。最適なパラメータを適切に選べば、図３のように通信路容量から0.68 dB (full-complexityアルゴリズムからは0.08 dB)に迫る性能を保障できることを確認している。さらに、AWGN通信路に対して、新しい符号と復号アルゴリズムを設計した。この符号に関しては、sphere boundから3.6 dBのギャップが存在していることを確認している。 また、繰り返し送信されるようなLDPC符号への応用において、例えば、音楽の電子透かし符号化や繰り返し送出するデータ放送を想定し、フレーム同期無しに、同期を取りながら復号を行う手法について、復号性能の劣化が無く、計算量の増加を抑えた高速な復号法を提案した。

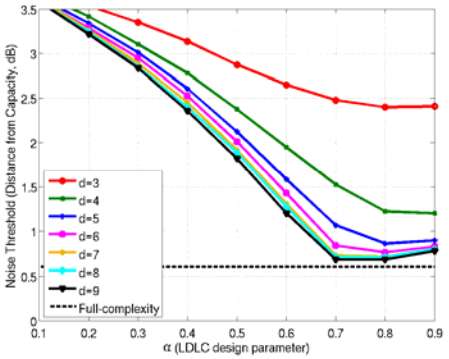

図 3. Noise thresholds for low-density lattice codes (LDLC) using single-Gaussian approximation.

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１８件）

① Brian Kurkoski, Justin Dauwels and Hans-Andrea Loeliger, "Power-Constrained Communications Using LDLC Lattices," in Proc. of the Intl. Symposium on Information Theory, 5 pages, June 2009. (査読有)

②Hyunho Kang, Koutarou Yamaguchi, Brian Kurkoski, Kazuhiko Yamaguchi, and Kingo Kobayashi, "Full-Index-Embedding Patchwork Algorithm for Audio Watermarking", IEICE Trans. Inf. & Syst., Volume and Number: Vol. E91-D, No.11, pp. 2731-2734, Nov. 2008. (査読有)

③Brian M. Kurkoski, Kazuhiko Yamaguchi, Kingo Kobayashi, "Noise Thresholds for Discrete LDPC Decoding Mappings," in Proc. of IEEE Global Communications Conf. (GLOBECOM 2008), pp. 1-5, December 2008. (査読有)

④Brian M. Kurkoski, "Towards Efficient Detection of Two-Dimensional Intersymbol Interference Channels," IEICE Transactions, Vol. E91-A, No.10, pp. 2696-2703, Oct. 2008. (査読有)

⑤Hyunho Kang, Brian Kurkoski, Kazuhiko Yamaguchi and Kingo Kobayashi, "Tracing illegal users of video: reconsideration of tree-specific and endbuyer-specific methods", Lecture Notes in Computer Science, Springer-Verlag, Vol. 4707, Part III, pp. 1046-1055, 2007. (査読有)

〔学会発表〕(計２７件)

①Brian Kurkoski, ″Digital Watermarking Techniques and Some Recent Results,″ (招待講演), Texas A&M University, College Station, Texas, USA, 2008年7月15日.
(査読無)

②Brian M. Kurkoski, ″When Variables Are Real, Beliefs Are Functions: Belief-Propagation Decoding of Lattices,″ (招待講演), 情報統計力学の深化と展開(DEX-SMI)「情報通信にみる″沢山あること″の数理」ワークショップ, pp.13-24, 京都府メルパク京都, 2007年12月17日.
(査読無)

６．研究組織
(1)研究代表者
Brian Kurkoski
電気通信大学・電気通信学部・准教授
研究者番号：８０４４４１２３

(2)研究分担者
小林 欣吾 (Kobayashi Kingo)
電気通信大学・電気通信学部・教授
研究者番号：２００２９５１５

山口 和彦 (Yamaguchi Kazuhiko)
電気通信大学・電気通信学部・准教授
研究者番号：６０２２０２５８

(3)連携研究者　なし