

博士論文概要

論文題目

A Study on Burst Erasure Correction Methods
Using Low-Density Parity-Check Codes

低密度パリティ検査符号を用いたバースト
消失訂正法に関する研究

申請者

細谷	剛
Gou	Hosoya

経営システム工学専攻・情報数理応用研究

2008 年 9 月

情報通信を利用する機会が増大している現代社会では、信頼性の高い情報通信システムを実現することが益々重要になっている。近年のハードウェアの進歩、インターネットや携帯電話などの急速な普及に伴い、情報通信システムの用途は多様化・複雑化する傾向にある。情報システムにおいて、通信媒体や記録媒体などの情報が伝送・記憶される経路は通信路と呼ばれ、この通信路を介して伝送・記憶される情報は、電波障害や記録媒体の傷などの確率的に発生する雑音の影響を受ける。通信路によって加わる雑音は一般に誤り、もしくは消失となる。誤り、消失が発生する通信路はそれぞれ誤り通信路、消失通信路と呼ばれ、両者ともに重要である。雑音を取り除くために用いられる技術は一般に誤り訂正符号と呼ばれ、情報技術における重要な基盤技術の一つとなっている。

誤り訂正符号を用いた情報通信システムでは、情報系列に対し冗長性を付加する符号化の操作を行って符号語へ写像し、通信路を介して受信者へ送信する。通信路において確率的に雑音が発生し、受信側では雑音の影響を受けた受信系列を受け取る。受信側では受信系列に対して復号化の操作を行うことにより送信された符号語を推定し、推定された符号語を情報の受信者へ出力する。誤り訂正符号に対しては誤りの訂正・検出が可能な符号の構成法と、その復号法の二者に関する議論が中心であり、この両者を扱う符号理論が重要な役割を演じる。

誤り訂正符号の中で近年最も注目されている符号構成・復号法として、R.G.Gallager によって提案された低密度パリティ検査 (LDPC) 符号と確率伝播型 (BP) 復号法の組み合わせが挙げられる。この組み合わせは、C.E.Shannon によって示された誤り訂正符号の理論的な性能限界である Shannon 限界に近い性能をもつことが知られている。しかし当時の計算機の性能では、LDPC 符号の性能を発揮する長い符号に対する評価が難しかったことや、それ以外の多くの誤り訂正符号が同じ時期に開発されていたことなどから LDPC 符号は長らく忘れ去られていた。1996年に D. J. C. MacKay によってその優れた性能が再評価され、再び注目されるようになった。BP 復号法はグラフ上における確率伝播型の復号法であり、本構造でループがないグラフの場合正しい事後確率を計算する。しかし、一般の LDPC 符号は多くのループを含み、BP 復号法を実行したときの理論的な性能解析は非常に難しく、主として計算機による実験で評価されてきた。

BP 復号法の理論的な性能解析に関する最初の大きな成果は M. Luby らによって提案された 2 元消失通信路 (BEC) 上において効率的な計算量をもつ疎なパリティ検査行列をもつ符号である。インターネットで一般的なパケット通信では、パケットロスと呼ばれるデータのブロック単位ごとに消失した受信系列を訂正するために誤り訂正符号が用いられる。これは LT (Luby Transform) 符号と呼ばれ、LDPC 符号と非常に似た構造をもち、性能は LDPC 符号より劣るものの他の多くの符号に比べ優れた性能をもつ。同時に Luby は、復号を行ったときの振る舞いをグラフ上における離散確率過程で表現し、解析する方法を提案した。さ

らに，解析するにあたりランダムに構成された個々の符号ではなく，符号の集合として符号アンサンブルを導入し，アンサンブル平均としての性能を評価した．すなわち，ループが存在しない符号長が大となる符号の場合，個々の符号の性能は集合平均に収束することを示した．また，行列の各行，各列の1の要素の数が非一様な非正則 LDPC 符号を提案し，符号の性能限界である通信路容量に迫る次数分布を発見した．T. J. Richardson らは，Luby らの成果をより一般的な2入力の無記憶な通信路へ拡張し，密度発展法と呼ばれる手法を提案した．密度発展法は，LDPC 符号に対し BP 復号法を実行したときの性能を評価でき，同時に優れた性能をもつ非正則 LDPC 符号の次数分布を求める際にも利用できる．密度発展法は様々な通信路，符号，復号法に対し解析を行うことができ，現在でも幅広く利用されている解析方法である．しかし，Luby らの解析方法と同様に密度発展法ではタナグラフ上のループがない符号を仮定しているため，短いループが多数存在する有限の符号長の場合，解析した結果がそのまま当てはまるとは限らない．そのため，有限長の符号に対する解析方法が必要とされていた．

C. Di らは有限長の LDPC 符号を解析するために，まず BEC を仮定し，BP 復号法が失敗する消失ビット位置集合を **Stopping Set** として明確な定義を与え，解析法を提案した．**Stopping Set** のシンボル位置のみで構成される部分グラフは複数のループが組み合わさった構造になっており，従来不可能であったループを考慮した解析を可能にしている．その結果，符号理論で符号の性能を評価するために従来用いられた重み分布と同様の議論が可能になり，多くの研究成果に発展した．

このように BEC を仮定した Luby らの成果は，その後密度発展法などの優れた研究成果を生み出した．現在，BEC より一般的な通信路に対する有限長の LDPC 符号の解析方法が望まれているが，**Stopping Set** に対応する訂正のできないビットパターンである **Trapping Set** は，実験的にその傾向を示している段階であり，**Stopping Set** のような研究成果には未だ結びついていない．一方，LDPC 符号の研究成果の多くは，雑音の発生が誤り・消失に拘らず，送信する符号語の各ビットに対しランダムに雑音が生起することを仮定している．そのため，理論的に性能を保証する際には有用であるが，実用性を考慮するとバースト雑音のような連続した雑音が発生するモデルも考慮する必要がある．特にパケット通信では，パケット内の情報が一度に消失するため，バースト消失通信路を考慮することは有益であると考えられる．

本研究では，LDPC 符号を用いてバースト消失を効果的に訂正する方法を開発することを目的とする．バースト消失を訂正するために用いられる一般的な符号構成は，検査行列に対する列置換によって符号を構成することである．ただし，効果的に列置換を行う指標は知られておらず，従来の研究でも，受信系列の中に1本のバースト消失が発生する様々なパターンに対し復号を行い，訂正できるか

確認しつつ効果的な列置換パターンを探索している．しかし 2 本以上のバースト消失を考慮すると，探索するパターンがバーストの本数にしたがって指数関数的に増大するため，現実的な方法ではない．また 1 本のバースト消失の場合でも列置換を行う際の明確な指標を用いておらず，バースト消失のパターンに対し復号を行って探索し符号を構成している．

以上の点から次に挙げる 2 つの手法を提案する．

(1) 複数本のバースト消失が発生する通信路を対象とし，LDPC 符号の検査行列内の要素 1 の間隔を指標とし列置換によって符号を構成する手法．

(2) 検査行列を組み合わせることによって，1 本のバースト消失が発生する通信路に適した LDPC 符号の構成法とその理論的な性能解析法．

(1)と(2)では対象としているバースト消失の本数が異なり，アプローチとなる方法も元の符号を列置換によって構成する方法と符号を組み合わせで構成する方法と異なる．

本論文は 5 章から成る．

第 2 章において情報・通信システムのモデルや通信路符号化・復号化の原理，本研究において対象としている LDPC 符号と BP 復号法などについて述べる．また以下の各章で共通となる定義について記す．

第 3 章では 複数本のバースト消失が発生する通信路での消失訂正に適した LDPC 符号の構成法について述べる．Stopping set の定義より LDPC 符号の検査行列の各行における隣り合う要素 1 同士はできる限り離して構成した方がバースト消失訂正には良いことを述べる．次に DBE を全体的に大きくできる検査行列の構造を示し，そのような構造をもつ検査行列を得る列置換アルゴリズムを提案する．計算機によるシミュレーション結果により，提案した方法によって得られた LDPC 符号は，列置換を行う前の元の符号と比べ，特に複数本のバースト消失に対し大幅に復号性能が向上することを示す．また，ランダムに雑音が発生する通信路においては復号性能が何ら劣化しないことを示す．

第 4 章では第 3 章とは異なり，1 本のバースト消失が発生する通信路での消失訂正に適した LDPC 符号の構成法について述べる．提案する符号を LR-LDPC 符号と呼び，これは検査行列を組み合わせることによって得られる．また，その構造は第 3 章で示した DBE を全体的に大きくできる検査行列の構造と類似している．LR-LDPC 符号のアンサンブルがもつ訂正不可能な消失バースト長の最小値を理論的に導出し，数値計算を行った結果より，多くの符号パラメータにおいて従来の LDPC 符号がもつ値より向上することを示す．さらにランダム消失通信路における性能の劣化がないことも示す．また，乱数を用いて生成した符号同士を比較することで，両者に有意な差が存在することを確認する．

最後に，第 5 章において以上の結果をまとめ，結論を述べる．また，今後の課題と展望について記述する．

早稲田大学 博士（工学） 学位申請 研究業績書

氏名 細谷 剛 印

(2008年 7月 現在)

種 類 別	題名、 発表・発行掲載誌名、 発表・発行年月、 連名者（申請者含む）
論文	<p>(論文)</p> <p>[1] G. Hosoya, T. Matsushima, and S. Hirasawa, "A combined matrix ensemble of low-density parity-check codes for correcting a solid burst erasure," to appear in IEICE Trans. Fundamentals, 2008.</p> <p>[2] T. Sato, G. Hosoya, H. Yagi, and S. Hirasawa, "A method of grouping symbol nodes for shuffled BP decoding algorithm," to appear in IEICE Trans. Fundamentals, 2008.</p> <p>[3] G. Hosoya, H. Yagi, T. Matsushima, and S. Hirasaw, "A modification method for constructing low-density parity-check codes for burst erasures," IEICE Trans. Fundamentals, vol.E89-A, no.10, pp.2501-2509, Oct. 2006.</p> <p>(国際会議)</p> <p>[4] G. Hosoya, H. Yagi, T. Matsushima, and S. Hirasawa, "Performance of low-density parity-check codes for burst erasures," Proc. 2006 International Symposium on Information Theory and its Applications (ISITA2006), pp.491-496, Seoul, Korea Oct. 2006.</p> <p>[5] G. Hosoya, H. Yagi, T. Matsushima, and S. Hirasawa, "Modification method of construction and performance analysis of low-density parity-check codes over the Markov-modulated channel," Proc. 2004 International Symposium on Information Theory and its Applications (ISITA2004), pp.206-211, Parma, Italy, Oct. 2004.</p>
講演	<p>(講演)</p> <p>[6] G. Hosoya, T. Matsushima, and S. Hirasawa, "A combined matrix ensemble of low-density parity-check codes for a solid burst erasure," Proc. 30th Symposium on Information Theory and its Applications (SITA2007), pp.330-335, Kashiko-jima, Mie, Japan, Nov. 2007.</p> <p>[7] G. Hosoya, H. Yagi, T. Matsushima, and S. Hirasawa, "An adaptive decoding algorithm of LDPC codes over the binary erasure channel," Proc. 2007 Hawaii and SITA Joint Conference on Information Theory, pp.154-159, Hawaii, U.S.A, May 2007.</p> <p>[8] G. Hosoya, H. Yagi, T. Matsushima, and S. Hirasawa, "On correctable burst-erasure lengths for LDPC codes with column permuted parity-check matrices," Proc. 29th Symposium on Information Theory and its Applications (SITA2006), pp.645-648, Hakodate, Hokkaido, Japan, Nov. 2006.</p> <p>[9] G. Hosoya, H. Yagi, T. Matsushima, and S. Hirasawa, "A modification method for constructing low-density parity-check codes for burst erasures," IEICE Technical Report, vol.105, no.662, IT2005-121, pp.153-158, March 2006.</p> <p>[10] G. Hosoya, T. Matsushima, and S. Hirasawa, "A decoding algorithm of low-density parity-check codes using decisions of erasure correcting," Proc. 26th Symposium on Information Theory and its Applications (SITA2005), pp. 5-8, Onna, Okinawa, Japan, Nov. 2005.</p>

早稲田大学 博士（工学） 学位申請 研究業績書

種 類 別	題名、 発表・発行掲載誌名、 発表・発行年月、 連名者（申請者含む）
その他	<p>[11] 細谷 剛, 松嶋 敏泰, 平澤 茂一, "LDPC 符号の消失訂正と誤り訂正の関係," 電子情報通信学会技術研究報告, vol.105, no.311, IT2005-53, pp.13-17, 2005 年 9 月.</p> <p>[12] G. Hosoya, T. Matsushima, and S. Hirasawa, "A decoding method of low-density parity-check codes over the binary erasure channel," Proc. 27th Symposium on Information Theory and its Applications (SITA2004), pp. 263-266, Gero, Gifu, Dec. 2004.</p> <p>[13] 細谷 剛, 八木 秀樹, , 平澤 茂一, "記憶のある通信路に対する低密度パリティ検査符号の復号性能の解析" 第 26 回情報理論とその応用シンポジウム予稿集, 淡路島, 兵庫, pp.269-272, 2003 年 12 月.</p> <p>[14] 細谷 剛, 八木 秀樹, 小林 学, 平澤 茂一, "バースト誤り通信路に適した低密度パリティ検査符号の構成法," 電子情報通信学会技術研究報告, vol.103, no.214, IT2003-20, pp.61-66, 2003 年 7 月.</p> <p>[15] 細谷 剛, 八木 秀樹, 小林 学, 平澤 茂一, "隠れマルコフ型雑音通信路に対する低密度パリティ検査符号の復号に関する一考察," 電子情報通信学会技術研究報告, IT2002-23, vol.102, no.198, pp.19-24, 2002 年 7 月.</p> <p>(講演)</p> <p>[16] 佐野 利行, 細谷 剛, 八木 秀樹, 平澤 茂一, "元画像との差分ベクトルを特徴量とした学習による改変画像検出," 電子情報通信学会技術研究報告, vol. 107, no. 487, ITS2007-62, pp. 1-6, 2008 年 2 月.</p> <p>[17] 野口 達也, 細谷 剛, 八木 秀樹, 平澤 茂一, "JPEG2000 のビットプレーンを用いたテクスチャ画像の検索," 電子情報通信学会技術研究報告, vol. 107, no. 380, IE2007-119, pp. 39-43, 2007 年 12 月.</p> <p>[18] 佐藤 芳行, 細谷 剛, 八木 秀樹, 平澤 茂一, "Shuffled BP 復号法に対する探索的なシンボルノードのグループ分割法," 第 30 回情報理論とその応用シンポジウム予稿集, pp.18-23, 賢島, 三重, 2007 年 11 月.</p> <p>[19] 佐藤 芳行, 細谷 剛, 八木 秀樹, 平澤 茂一, "Group Shuffled BP 復号法における効果的な分割法," 電子情報通信学会技術研究報告, vol.107, no.42, IT2007-3, pp.13-18, 2007 年 5 月.</p> <p>[20] 長谷川 裕, 細谷 剛, 八木 秀樹, 平澤 茂一, "信頼度更新を用いた LDPC 符号の Bit-Flipping 復号法の改良," 第 29 回情報理論とその応用シンポジウム予稿集, pp.649-652, 函館, 北海道, 2006 年 11 月.</p> <p>[21] 小俣 順, 細谷 剛, 平澤 茂一, "静止画像圧縮における適応型予測木の改良," 第 29 回情報理論とその応用シンポジウム予稿集, pp.537-540, 函館, 北海道, 2006 年 11 月.</p> <p>[22] 作田 豊, 細谷 剛, 平澤 茂一, "SPITH アルゴリズムにおけるデータ埋め込み法," 第 29 回情報理論とその応用シンポジウム予稿集, pp.529-532, 函館, 北海道, 2006 年 11 月.</p> <p>[23] 金田 海渡, 細谷 剛, 平澤 茂一, "カラー成分間の相関を利用した SPIHT アルゴリズムによる静止画像圧縮," 第 29 回情報理論とその応用シンポジウム予稿集, pp.533-536, 函館, 北海道, 2006 年 11 月.</p> <p>[24] 佐藤 匡, 細谷 剛, 八木 秀樹, 平澤 茂一, "信頼度更新を用いた LDPC 符号の Weighted Bit-Flipping 復号法," 第 28 回情報理論とその応用シンポジウム予稿集, pp.9-12, 恩納, 沖縄, 2005 年 11 月.</p>

早稲田大学 博士（工学） 学位申請 研究業績書

種 類 別	題名、 発表・発行掲載誌名、 発表・発行年月、 連名者（申請者含む）
	<p>[25] 松下 大輔, 細谷 剛, 平澤 茂一, "適合文書から抽出した重要語に基づく文書検索," 第 28 回情報理論とその応用シンポジウム予稿集, pp.713-716, 恩納, 沖縄, 2005 年 11 月.</p> <p>[26] 山岸 英貴, 細谷 剛, 平澤 茂一, "単語の潜在的意味空間に基づく文書分類," 第 28 回情報理論とその応用シンポジウム予稿集, pp.717-720, 恩納, 沖縄, 2005 年 11 月.</p> <p>[27] 長谷川 裕, 細谷 剛, 八木 秀樹, 平澤 茂一, "トレリスの枝削除による q 元ターボ復号の計算量低減," 電子情報通信学会技術研究報告, vol.105, no.190, IT2005-37, pp.9-14, 2005 年 7 月.</p> <p>[28] 渡辺 祐介, 細谷 剛, 平澤 茂一, "ドキュメントの特徴を考慮した非階層的クラスタリング," 第 27 回情報理論とその応用シンポジウム予稿集, pp.61-64, 下呂, 岐阜, 2004 年 12 月.</p> <p>[29] 贅田 里詩, 細谷 剛, 八木 秀樹, 平澤 茂一, "ソート・マッチング法に基づく軟判定復号アルゴリズムの修正," 第 27 回情報理論とその応用シンポジウム予稿集, pp.567-570, 下呂, 岐阜, 2004 年 12 月.</p> <p>[30] 贅田 里詩, 細谷 剛, 八木 秀樹, 平澤 茂一, "確率伝播型復号法に適した低密度パリティ検査符号巡回型 LDPC 符号の短縮化法," 電子情報通信学会技術研究報告, vol.103, no.215, IT2003-32, pp.51-56, 2003 年 7 月.</p>