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　８日現在

機関番号：８２６２６
研究種目：若手研究（Ｂ）
研究期間：2010～2011
課題番号：２２７６０２８６

研究課題名（和文）　個々のＬＤＰＣ符号が持つ正確な誤り訂正性能評価法の研究

研究課題名（英文）　On Evaluation Methods of Accurate Error Rate for an LDPC Code

研究代表者
萩原　学　（HAGIHARA MANABU）
独立行政法人産業技術総合研究所・情報セキュリティ研究センター・研究員
研究者番号：８０４１５７２８

研究成果の概要（和文）：
本研究成果は大きく分けて２つある．一つは，いくつかのＬＤＰＣ符号の復号誤り率を正確に求める理論を構築し，さらに，具体例（SFA(3,11)-ＬＤＰＣ符号）を以って理論の正しさを検証したことである．この成果を得る過程で，ＬＤＰＣ符号を定義するタナーグラフと呼ばれる対象の二部グラフとしての対称性の重要性を認識した．そこで，もう一つの成果として，SFA(2,P)- SFA(3,P)-ＬＤＰＣ符号の対称性を調査した．特に，それらの重要なパラメータである重み分布の特徴付けを与えた．

研究成果の概要（英文）：
Our results invented a method that gives the accurate word error rate of LDPCcodes over a binary symmetric channel. We applied our results to some examples, known as SFA LDPC codes and verified the validity of our method. We also investigated the structure of FA(2,P)- and (3,P) LDPC codes. Our result characterizes the weight distribution of these LDPC codes.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２０１０年度	1,600,000	480,000	2,080,000
２０１１年度	1,500,000	450,000	1,950,000
年度			
年度			
年度			
総　計	3,100,000	930,000	4,030,000

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：ＬＤＰＣ符号，Ｓｕｍ－Ｐｒｏｄｕｃｔ復号，確率伝搬，ワード誤り率，検出不可能誤り，重み分布

１．研究開始当初の背景

誤り訂正符号研究の大きな動機づけとして，シャノンによる通信路符号化定理が知られている．この定理により得られる通信路容量と呼ばれる指標を達成する符号を「実用的に動作する意味で構成する」ことは，誤り訂正符号を研究する者にとって最大の目標である．

ＬＤＰＣ符号の符号空間は，要素の多数が０であるパリティ検査行列に対応する線形符号として定義され，復号方法としてＳｕｍ－Ｐｒｏｄｕｃｔアルゴリズムを誤り訂正に適用させたＳＰ復号が用いられる．この符号空間の定義は自由度が高いため，任意のＬ

ＤＰＣ符号に対して性能を評価する統一的手法は，計算機上の通信シミュレーション以外に知られていない．つまり，パリティ検査行列を１つ固定した後，符号語をランダムに定め，通信路から決まる確率分布に従い符号語に雑音を加え，復号アルゴリズムに入力し，出力した推定語が符号語と一致するか否かデータをとる．これを繰り返し，送信語と推定語のサンプルを集め，それらの一致率を統計的な意味で集計する．

この手法の正確さを上げる為には，シミュレーションを繰り返し，大数の法則が働くようサンプルを多く集める必要がある．しかし，ＬＤＰＣ符号の性能の高さゆえ，送信語と推定語が異なる確率は非常に低く，サンプルを集めるためのシミュレーションコストが膨大になる．その為，高い一致率が要求される実用的アプリケーションへ搭載するには，シミュレーションによる性能評価が難しくなっている．また，多少の誤差は避けられない．もし，短い時間で正確な性能評価方が発見されれば，学術的にも産業的にも大きな価値のある成果である．

ＬＤＰＣ符号の性能を理論的に解析する手法が検討・提案はこれまでにも色々となされてきた．それらの例をあげつつ，同時にそれらの問題点を指摘する．

密度発展法と呼ばれる手法は，複数のＬＤＰＣ符号の平均的な振る舞いを解析する手法である．この手法は平均的な意味で高い性能を持つＬＤＰＣ符号が何か特定できるために，符号構成の指針として利用されることが多い．複数の符号の平均的な振る舞いがわかる一方，本研究が目指す，固定された１つのＬＤＰＣ符号のみの解析には利用できない．

ストッピングセット・トラッピングセット・最小距離と呼ばれる視点からのパリティ検査行列の解析手法も注目されている．ＬＤＰＣ符号を与えるのはパリティ検査行列であるから，符号空間の特性を理解するには有用な手法である．特にストッピングセット・トラッピングセットは復号処理における問題点を表現しており，ＬＤＰＣ符号の一致率の上界を求める手法として活躍する．一方で，通信路のパラメータが反映されない手法である．例えば，二元消失通信路では一定の確率で送信シンボルが消失する．この一定の確率を定める数値を反映した解析ではない．そのため，本研究で目指すＬＤＰＣ符号の正確な一致率解析に用いることができない．

これまでにない，通信路パラメータを意識した解析方法を発明する価値は独創的で新規性の高い成果になると期待できる．

２．研究の目的

ＬＤＰＣ符号は，Ｇａｌｌａｇｅｒにより提案されＭａｃＫａｙにより再発見された符号として知られており，その最たる特徴として二元消失通信路などのいくつかの通信路においては通信路容量に接近する性能を持つ符号であることが挙げられる．つまり，ＬＤＰＣ符号は誤り訂正符号研究者の目標を実現した学術的意義の大きな符号である．この符号を深く掘り下げ研究・理解することで，二元消失通信路に限らず様々な通信路で通信路容量を達成する符号の実現へ近付くと期待でき，世界中でいまもなお，符号理論研究者が研究を進めている．

本研究では，低密度パリティ検査符号（以下，ＬＤＰＣ符号）を用いた通信における送信語と受信語の一致率（同値な評価として，誤り率）の正確な値を導く手法の創出を目指す．研究対象であるＬＤＰＣ符号はシャノンの通信路限界に接近する符号として学術的価値が高いのみならず，通信機器の国際的な標準仕様に選出された符号であり実用的意義が大きいことでも知られている．一方，誤り率の導出法は計算機シミュレーションによる実験・統計的に頼っており，正確な評価ができない．また，シミュレーションに多大な時間が必要なことも問題である．本研究により，ＬＤＰＣ符号の正確で時間が短くて済む新たな解析法を創出し，学術面・実用面の両面に良い影響を与えたい．さらに，より良い符号構成法や復号法の改良へのマイルストーンとしたい．

３．研究の方法

研究の方法は理論面と計算機面の二通りに分かれる．

理論面としては，アルゴリズムの数学的解析が主になる．また，アルゴリズムの解析結果を活用する符号の要件の導出も，理論的側面である．

理論面を進めるには，幅広い数学文献の調査や情報収集が有用である．なかでも代数学や組合せ論は，本研究を進める有効手段である．そして，得られた知識や経験を，数学者や工学者といった，共通の問題意識を持つ研究者と議論することで理解を深めることが有用である．その為には，学会に参加したり，研究者の研究室に訪問したりすることが，効率のよい方法である．

あとは，自分自身でじっくり計算できる環境をつくることで，理論展開が可能になる．

計算機的手法としては，理論を実現するためのデータを集めるソフトウェア，および，それらを随時実行し続けられるサーバを構築する．そして，定期的に計算環境をチューニングすることで，効率を良くする．これにより，手計算では得られない，大規模なデータを得ることが可能となる．

４．研究成果

(1) ＬＤＰＣ符号とＳｕｍ－Ｐｒｏｄｕｃｔ復号の訂正可能誤りとある特定のシンドロームとの間の一対一対応を理論的に解明した．そのシンドロームを，訂正可能シンドロームと名付け，計算機を用いてそのデータを集めた．計算機によるデータをもとに，本研究成果の有用性を実証した．

この成果は，符号の誤り率の解析において，次の意味を持つ．まず，ワード誤り率を求めるナイーブな方法は，全ての誤りパターンを，復号器に代入し，正しく訂正できたか否かを調べることで得られることを注意する．この方法では，符号長が８０を超える符号の解析は計算量的に，現実時間では不可能である．そこで本成果の訂正可能シンドロームが役に立つ．シンドローム長は符号長よりも真に小さいという特性をもつことから，訂正可能シンドロームを全てもとめることが計算量的に易しいことがある．実際，本研究ではＳＦＡ（３，１１）－ＬＤＰＣ符号を例として，本成果の有用性を確かめた．この符号は，符号長が１２１であり，シンドローム長が３３である．前者の総当たりは計算量的に不可能である．一方，後者は可能である．この性質を利用して，具田的にワード誤り率を導出したことは，既存研究と一線を画す成果である．

(2) 萌芽的な理論解析結果として，誤り訂正シンドロームを求める計算効率を向上した点も成果と言える．そのアイデアはＢｕｒｎｓｉｄｅの補題と呼ばれる群論の定理の応用である．この補題は，訂正可能シンドロームに対するグラフの同型群の作用による軌道の総数を数える手法である．このアイデアを用いることで，符号長１２１のＳＦＡ（３，１１）－ＬＤＰＣ符号の訂正可能誤りを求める時間を，元来の計算量である「2 の 121 乗」から「2 の 24 乗」まで，原理的に減らせることを示した．

(3) 符号の性能を左右する，重み分布の解析を行った．中でも，ＳＦＡ（３，１１）－ＬＤＰＣ符号よりも一般的な構造を持つＳＦＡ（３，Ｐ）－ＬＤＰＣ符号に着目し，検出不可能誤りの生成率を求める研究を進めた．ＳＦＡ　ＬＤＰＣ符号は正則ＬＤＰＣ符号のクラスの一つであり，準巡回ＬＤＰＣ符号でもある．特に，梶，杉山らにより最小距離の導出，最小距離をもつ符号語の個数などが研究されてきた経緯をもつ．本研究では，梶，杉山の考察したＳＦＡ　ＬＤＰＣ符号を一般化した構造を定義した．これまでＳＦＡ（Ｊ，Ｐ）－ＬＤＰＣは１つの線形符号を指す用語であったが，本定義では Ｐ choose Ｊ だけ自由度を持つ．特に，一見すると同値で無い符号をふくむクラスとなっている．（同値であるか否かの問題は，後述する）その上で，列重み 2 もしくは 3 のＳＦＡ　ＬＤＰＣ符号の検出不可能誤り率が，同一の列重みであれば，Ｐ のみに依存することを証明した．つまり Ｐ choose Ｊ ある符号がどれも，同じ誤り率を有することがわかった．

この成果は，国際シンポジウム ISITA2012 に投稿中である．

本研究結果から，今後の興味として次の２点が面白いと考えられる．

①ＳＦＡ（３，Ｐ）－ＬＤＰＣ符号の検出誤り率は Ｐのみに依存して，すべて同じ値であることを得た．では，実際には幾らであるか，正確な表示を求めよ．

②ＳＦＡ（３，Ｐ）－ＬＤＰＣ符号のパリティ検査行列は，どれも同値であるか調べよ．つまり，列置換と行置換だけで，それらのパリティ検査行列を移りあえるか調べよ．

本研究でも２．の解決を試みたが，完全な解は得られていない．計算機でも確認のできない，興味深い話題をみつけたと言える

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２件）

① M.Hagiwara, M.P.C.Fossorier, H.Imai, Fixed Initialization Decoding of LDPC Codes over Binary Symmetric Channel, IEEE Trans. On IT, vol.58 (4), pp.2321-2329, 2012.
DOI: 10.1109/TIT.2011.2177440

〔学会発表〕（計２件）

① 萩原学，空間結合構造を持つ量子ＬＤＰＣ符号，空間結合符号とその周辺ワークショップ，東京工業大学，2011/02/19

② M.Hagiwara, M.P.C.Fossorier, H.Imai, LDPC Codes with Fixed Initialization Decoding over Binary Symmetric Channel, IEEE International Symposium on Information Theory, Austin, USA, 15/06/2010.

〔図書〕（計１件）

萩原学，符号理論　～デジタルコミュニケーションの為の数学～，日本評論社，２０１２年８月発刊予定，３００ページ．

〔その他〕

ホームページ等

http://staff.aist.go.jp/hagiwara.hagiwara/

６．研究組織

(1)研究代表者

萩原　学（HAGIWARA MANABU）

独立行政法人産業技術総合研究所・情報セキュリティ研究センター・研究員

研究者番号：80415728