様式 C-19

科学研究費補助金研究成果報告書

平成２３年　６月　７日現在

機関番号：３２６２１
研究種目：基盤研究（C）
研究期間：2008～2010
課題番号：２０５６０３８３
研究課題名（和文）線形符号の基本多面体の構造解明に関する研究

研究課題名（英文）Study on the structure of fundamental polytope of linear codes

研究代表者
澁谷　智治（SHIBUYA TOMOHARU）
上智大学・理工学部・准教授
研究者番号：２０２６２２８０

研究成果の概要（和文）：本研究の主要な成果は以下の３点である．(1) sum-product アルゴリズムが収束するための十分条件に基づく，sum-product 復号の収束条件と LDPC 符号の構造との関係解明，(2) 反復復号と同様のアルゴリズムによって符号化可能な線形符号の数学的枠組みの整備とその組織的構成法の提案，(3) LDPC 符号の線形オーダ符号化アルゴリズムの開発．

研究成果の概要（英文）：The contributions of this research are summarized in the following three issues: (1) Clarification of the relation between the condition on which the sum-product decoding converges and the structure of LDPC codes from the view point of the sufficient condition on which the sum-product algorithm converges, (2) Introduction of the mathematical framework for the reversible codes and their systematic construction, (3) Developing linear time encoding algorithm for LDPC codes.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００８年度	800,000	240,000	1,040,000
２００９年度	1,300,000	390,000	1,690,000
２０１０年度	900,000	270,000	1,170,000
総　計	3,000,000	900,000	3,900,000

研究分野：情報通信工学
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，線形計画法，LP 復号，基本多面体，反復復号，リバーシブル符号，線形符号の符号化

１．研究開始当初の背景

(1) LDPC 符号

LDPC (Low-Density Parity-Check) 符号とは，疎な検査行列で定義される線形符号の総称である．LDPC 符号と反復復号法とを組み合わせた LDPC 符号化システムは，BCH 符号や畳込み符号といった従来の誤り訂正符号化システムをはるかに凌ぐ性能を示す．このことから，LDPC 符号化システムは次世代誤り訂正符号化システムの中核をなすものと期待されている．

(2) 反復復号の性質

誤り訂正符号化システムの性能は，最小距離や重み分布といった符号自体の特徴と，復号法の誤り訂正能力とに依存する．LDPC 符号化システムでは，反復復号が失敗するケースとして以下の場合が考えられる．

1. 復号の反復が収束しない.
2. 復号の反復は収束するが,
   (a) 送信符号語以外の符号語が得られる.
   (b) 送信符号語でも他の符号語でもない語(**疑似符号語**)が得られる.

これまでの研究では，特に 2-(b)にあたる，符号語以外の語(疑似符号語)に収束する場合(図 1 参照)が性能劣化の主因となることが実験的に確かめられている．従って，符号語および疑似符号語からなる反復復号の収束点全体の構造を解明することは，高性能 LDPC 符号化システムの開発には必要不可欠であり，近年，この問題に関して世界的な注目が集まっている．

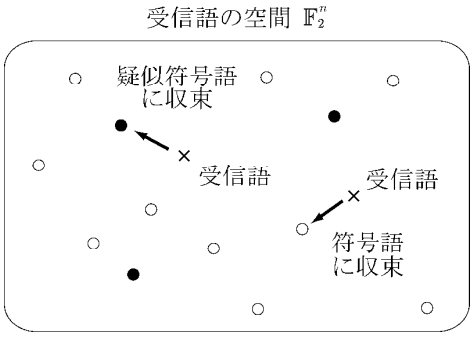

図 1　反復復号の収束の様子．反復復号の収束点は，符号語(○)と疑似符号語(●)とに分けられる．収束先は受信語に依存し，疑似符号語に収束した場合は復号失敗となる．

2．研究の目的

本研究では，線形符号の基本多面体の構造の探究を目的とする．これは，以下に説明するように，反復復号の収束点集合の構造を解明するための有力なアプローチと位置づけられる．

(1) 線形符号の基本多面体

Feldman らは, 線形符号の最尤復号を線形計画 (Linear Programming, LP) 問題として記述し直した．しかしながら，この LP 問題の制約集合の定義には指数オーダの線形不等式を要するため，Feldman らはさらに，この制約集合を含み記述の容易な制約集合(線形符号の基本多面体)を定義した(図 2 参照)．この基本多面体上での LP 問題を解くことにより，最尤復号の近似復号を効率よく実現できる(LP 復号).

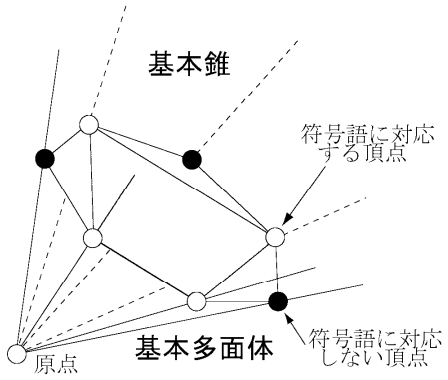

図 2　基本多面体と符号語との関係．○(符号語)を頂点とする凸多面体が，最尤復号の LP 表現の制約集合となる．また，制約条件の緩和により，○，●を頂点とする表現の容易な基本多面体が得られる．さらに，基本多面体を原点と反対方向に延長したのが基本錐となる．

(2) 反復復号の収束点集合と基本多面体

近年の研究から，基本多面体の頂点集合は，反復復号におけるほとんどの収束点を含むことが明らかになった．つまり，基本多面体の構造を明らかにすることは，反復復号の収束点集合の構造解明につながるものと期待される．そこで本研究では以下の課題について探究することとした．

課題 1 基本多面体の頂点の表現に関する研究

LP 問題の実行可能領域である基本多面体は線形不等式の共通部分として定義されるが，これは，以降の課題の探求に適しているとは言い難い．そこで，課題の探求に適した基本多面体およびその頂点の表現について研究する.

課題 2 基本多面体の頂点の重み分布に関する研究

二元対称通信路における最尤復号では，受信語にハミング距離の意味でもっとも近い符号語が送信符号語と推定される．このため，符号化システムの性能は符号の重み分布により評価される．一方，LP 復号では，ハミング距離とは別の距離尺度に基づいて復号領域が定められる．そこで，この距離尺度に関する頂点間の最小距離や距離の分布，それらに関する構造等を明らかにし，LP 復号の性能評価に役立てる.

課題 3 反復復号の収束点集合の構造解析と反復復号の性能評価への応用に関する研究

課題１，２において明らかになった基本多面体の構造を，反復復号の収束点集合の構造解析や反復復号の性能評価に応用する手法について研究する．

３．研究の方法

(1) 当初の予定

研究の当初は以下の手順に従って研究を進めるものとした．

① スケジュール

３年間の研究期間に，研究目的の項に記した３つの研究課題を記載順に遂行する．なお，平成２０年度に課題１，平成２１年度以降に課題２，３を遂行する．また，課題１は理論的な解析が研究の中心となる．一方，課題２，３は理論的な解析と計算機による例題構成や数値実験とを併用した研究となる．

基本多面体の性質を探求する上で，「基本多面体をどのように表現するか」という問題は極めて重要であり，また本研究課題を遂行する上で最も基本的である．そこで，研究の初年度においては，研究目的に記した３つの研究課題のうち，課題１：「基本多面体の頂点の表現に関する研究」について研究を進める．具体的な検討項目・手順は以下のとおりである．

② Koetter らの理論の拡張

基本多面体を原点と反対方向に延長して得られる凸錐(基本錘，図１参照)上の整数格子点の集合は，基本多面体の頂点に関して基本多面体と本質的に同等の情報を含むことが知られている．Koetter らは，基本錐上の整数格子点を全て列挙する母関数を，Tanner グラフから導かれるあるグラフ上で定義される枝ゼータ関数を用いて表現することに成功した．この母関数は，基本多面体の頂点に関する多くの情報を含んでいることから，重み分布の解析などに有用であると考えられている．しかしながら，Koetter らの手法が適用可能な線形符号は極めて限られているため，本研究では，より広範な線形符号へ Koetter らの手法を拡張する．

なお，この拡張においては，この分野における従来の研究ではほとんど用いられることのなかった，線形空間における独立性の概念を拡張したある概念の利用が極めて有効であると考えている．この概念に，グラフ理論やゼータ関数の理論を組み合わせることによって，本課題が達成できるものと予想している．

③ 基本錐上の母関数と基本多面体の頂点との関係について

基本多面体の頂点に関する様々な情報を上で得られた母関数から効率よく引き出すためには，基本錐上の整数格子点と基本多面体の頂点とを適切に結びつける必要がある．これは，課題２以降の研究課題を進める上で重要な問題である．そこで，これらについて検討を行う．

なお，この段階で研究の成果が十分に得られない場合，一般的な符号への拡張の前段階として，いくつかの線形符号に限定した拡張を検討する．これには，Smarandache らの手法についての検討などが考えられる．

(2) 研究の進展に伴う修正

研究の進展に伴い，研究の方法を以下のように修正した

① 反復復号の収束と符号の構造との関係について

研究の進展の中で，反復復号を実現するための基本的なアルゴリズムである sum-product アルゴリズムに関し，それが収束するためのより精密な十分条件が発見された．この条件を精査することによって当初の目的が達成される可能性があることから，研究の１年目では，反復符号の収束と符号の構造との関係についての検討を同時に行った．

② 線形符号の高速符号化について

研究年度の途中で，反復復号と同様のアルゴリズムより符号化可能な符号化クラス（リバーシブル符号）が発見された．符号化時の反復の収束条件が復号時の反復の収束条件と異なる特異なものであったことから，本研究の目的達成に有用であることが見込まれ，研究の２年目より線形符号の高速負後かに関する検討を合わせて行った．

４．研究成果

本研究の成果は以下の３点にまとめられる．

(1) Sum-Product 復号の収束条件と LDPC 符号の構造との関係解明

近年の研究から，基本多面体の頂点集合は，反復復号におけるほとんどの収束点を含む

ことが明らかになっている．また，反復復号を実現するための基本的なアルゴリズムである sum-product アルゴリズムに関し，それが収束するためのより精密な十分条件が近年発見されている．

本研究の初年度では，この十分条件を線形符号に適用した場合に，反復復号が収束するための十分条件がどのように記述されるかについて考察した．この結果，線形符号のタナーグラフの構造に関する強い制約を導くとともに，この制約が満たされる下では，基本多面体の頂点集合が符号語集合と完全に一致することを明らかにした．この成果は，電子情報通信学会情報理論研究会で報告されると共に，同学会英文論文誌に掲載された．

なお，基本多面体の構造解明という観点に立つと，上で述べた事実は必ずしも新たな知見ではない．従って，基本多面体の構造をより深く理解するためには，ここで得られた収束条件をさらに精密化する必要があるものと考えられ，現在，その方向での研究を進めている．

(2) リバーシブル符号の数学的枠組みの整備とその組織的構成について

研究の２年目では，LDPC 符号の反復復号法と同様のアルゴリズムによって符号化が可能な線形符号の数学的枠組みの整備とその組織的構成について検討した．線形符号の符号化は，与えられた情報ビットからパリティビットを計算することにより行われる．これは，係数行列の与えられた有限体上の線形連立方程式を解くことに等しく，一般に $O(n^2)$の計算量を必要とする(n は符号長を表す)．これに対し，Haley らは，線形連立方程式の反復解法である Jacobi 法を有限体上の場合に拡張し，その収束条件を明らかにするとともに，O(n)で実行可能な符号化アルゴリズムを開発した．さらに，このアルゴリズムが適用可能な符号の検査行列を，巡回行列に基づいて構成する手法を与えた．

本研究では，Haleyらのアルゴリズムが適用できる符号クラスを数学的に明確に特徴づけ，巡回行列に基づく検査行列に関する必要十分条件として明示することに成功した．これにより，符号化・復号化がともにO(n)の反復アルゴリズムで実行可能な符号クラスの一部が明確になり，またそのようなクラスの符号の組織的構成が可能となった．

なお，この成果は電子情報通信学会情報理論研究会にて報告され，同学会英文論文誌に投稿中である．

(3) LDPC 符号の高速符号化について

研究の最終年度では，２年目の研究に関連して，LDPC 符号の高速符号化を取り上げた．先に述べたように，LDPC 符号を含む線形符号の符号化は，与えられた情報ビットからパリティビットを計算することにより行われる，一般に $O(n^2)$の計算量を必要とする(n は符号長を表す)．従来の研究では，与えられた検査行列のパリティ部に対して行および列置換を施し，近似的な(上もしくは下)三角行列に変形したあとで後退代入を行うことによって，比較的少ない計算量で符号化を行う手法が提案されていていた．このとき，近似的な三角行列と真の三角行列との差異を表すパラメータ g の二乗に比例する計算量の符号化アルゴリズムが得られるが，g は一般にｎのオーダを有するため，依然として $O(n^2)$のアルゴリズムしか得られていなかった．

これに対し本研究では，検査行列のパリティ部にブロック三角化とよばれる変形を施した後で，主対角線上に現れる部分ブロック行列に対して近似的な三角行列への変形を施すと，O(n)の符号化アルゴリズムが得られることを明らかにした．さらに，任意の LDPC 符号の検査行列に対して，このような変形が常に可能であることを明らかにし，LDPC 符号の符号化の計算量の削減に関して大きな進展をもたらした．

なお，この成果は電子情報通信学会情報理論研究会で報告され，２０１１年７月に開催される国際会議にてさらなる精密化を行った成果が報告される予定である．

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 5 件）

① T. Shibuya, “Characterization of Factor Graph by Mooij's Sufficient Condition for Convergence of the Sum-Product Algorithm,” IEICE Transactions on Fundamentals, vol.E93-A, no.11, pp.2083-2088, 2010. (査読有)

② T. Shibuya, “Encoding of Linear Codes Based on the Rearrangement of

Block-Triangular Parity-Check Matrices," Technical Report of IEICE, IT2010-45, pp.69-74, 2010. (査読無)

③ T. Shibuya, "On the Size of Circulant Matrices for which Reversible Codes Exist," Technical Report of IEICE, IT-2009-94, pp.147-151, 2010. (査読無)

④ T. Shibuya, "Sufficient Conditions for Convergence of the Sum-Product Decoding," Technical Report of IEICE, IT2008-110, pp.441-446, 2009. (査読無)

⑤ T. Nozaki, K. Kasai, T. Shibuya, and K. Sakaniwa, "Detailed Evolution of Degree Distributions in Residual Graphs with Joint Degree Distribution," IEICE Transactions on Fundamentals, vol.E91-A, no.11, pp.2737-2744, 2008. (査読有)

〔学会発表〕(計 3 件)

① T. Shibuya, "Encoding of Linear Codes Based on the Rearrangement of Block-Triangular Parity-Check Matrices," 電子情報通信学会情報理論研究, 2010 年 9 月 22 日, 東北学院大学 (宮城県多賀城市).

② T. Shibuya, "On the Size of Circulant Matrices for which Reversible Codes Exist," 電子情報通信学会情報理論研究会, 2010 年 3 月 4 日, 信州大学 (長野県長野市).

③ T. Shibuya, "Sufficient Conditions for Convergence of the Sum-Product Decoding," 電子情報通信学会情報理論研究会, 2009 年 3 月 10 日, 公立はこだて未来大学 (北海道函館市).

６．研究組織

(1)研究代表者

澁谷　智治 (SHIBUYA TOMOHARU)
上智大学・理工学部・准教授
研究者番号：20262280