1版

様　式　C－１９、F－１９、Z－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ５ 月 １８ 日現在

機関番号：１１３０１
研究種目：若手研究(A)
研究期間：2012～2015
課題番号：２４６８４００７
研究課題名（和文）力学系・グレブナー基底・層コホモロジーを用いた超高性能符号開発

研究課題名（英文）Development of high performance error-correcting codes by using dynamical systems, Groebner basis, and sheaf cohomology

研究代表者
平岡　裕章（Hiraoka, Yasuaki）

東北大学・原子分子材料科学高等研究機構・准教授

研究者番号：１０４３２７０９

交付決定額（研究期間全体）：（直接経費）　　11,000,000円

研究成果の概要（和文）：有理写像の上で成立していた符号-復号双対定理を，多項式写像として一般化双対定理の形で定式化した．ここで重要になる発見は，一般化MacWilliams恒等式をもちいて最尤推定復号を表示できることを示したことである．具体的な数値実験も試み，次数を5次程度まであげておけば従来法に比べて格段にパフォーマンスが良くなることが確認できた．ネットワーク符号と層コホモロジーに関する課題では，クイーバーの表現としての定式化を考察し，幾つかの具体的なクイーバーに対してその表現圏の構造を調べた．

研究成果の概要（英文）：We generalized the encode-decode duality theorem into polynomial maps. The key idea is to represent maximum likelihood decoding as generalized MacWilliams identity. We also studied numerical experiments and found that the performance of the proposed method is quite better than conventional methods. For the subject on network coding and sheaf cohomology, we studied a formulation using quiver representations. We derived an algorithm for indecomposable decompositions on several explicit examples, and studied the structure on representation category.

研究分野：応用トポロジー

キーワード：近似最尤推定復号　位相的データ解析　パーシステントホモロジー

１．研究開始当初の背景

本研究では情報通信分野の重要課題，

課題 A:シャノン限界を実現する実用的誤り訂正符号の開発
課題 B:マルチソース型ネットワーク符号の最大送信容量の決定と符号開発

に対して，新たな数学手法を開発し解決することを目指す．ここで用いる手法は力学系理論，グレブナー基底，層コホモロジーであり，いずれの課題も理論的研究のみならず具体的な符号構成アルゴリズムの提案まで行う．

課題 A では，送信者から雑音が発生する通信路を介してつながっている受信者へ如何に高信頼・高効率な情報伝送を行うか，という問題を扱う．ここで誤り訂正符号とは符号化と復号化の対のことであり，シャノン限界とは伝送誤り確率を 0 にすることが可能な効率の限界値のことである．課題 A ではこのシャノン限界を実現する誤り訂正符号を具体的に開発することを目指す．

一方課題 B では，複数の送信・受信・中継点およびそれらの間の雑音なし通信路がグラフで表されるより大域的な問題を考える．ここでデータは有限体係数線形空間のベクトルで表され，各辺の容量（線形空間の次元）は有限値が設定されている．課題 B の目標は，複数の送信点が存在する場合の最大送信データ容量を決定し更にその符号の開発を行うことである．

申請者はこれらの重要課題 A，B に対して力学系理論および層コホモロジーを用いた独自の解析手法をこれまでに確立し，新たな理論構造を見いだすことに成功した．

まず課題 A では，受信語から復号メッセージを決める復号化を有理写像で表現しその写像が定める離散力学系のダイナミクスを解析することで，現在実用化されている誤り訂正符号の性能を上回る高精度復号法を開発した．この成果の理論的基盤は，申請者によって明らかにされた符号化と復号化の間に成り立つ双対定理である．この双対定理は符号化で用いられる生成行列の列ベクトルの 1 次関係式と，最尤推定復号と呼ばれる普遍的な復号法の有理写像表現に現れる非線形性を関係づける．またこの双対定理は高精度復号法の開発のみならず，代数幾何符号に代表される代数的符号理論と確率論的符号理論の両者を結ぶものとしても非常に高い評価を得ている．

一方課題 B に対して申請者は，グラフトポロジーと各頂点の演算ルールから有限体係数の層（以後 ネットワーク符号層とよぶ）を構成し，その層コホモロジーが送信データを表すことを解明した．さらにホモロジー代数に現れる完全系列を工学上の問題（マイヤー-ヴィートリス系列とデータ融合，切除定理とネットワークロバスト性等）へ応用しその有用性を示した．また最近では層の導来圏上でポアンカレ-ヴェルディエ双対性を応用することで最大送信容量の評価について予備的な結果を得ている．

２．研究の目的

これまでの研究成果を更に発展させ，それぞれの課題 A,B ごとに以下のサブテーマに取りかかる．

課題 A：
A1 グレブナー基底を用いた高精度復号法の構成：開発した復号法は有理写像の多項式近似写像により構成され，近似の精度が復号特性に直接影響を及ぼす．一方双対定理により符号化の対称性は有理写像を経由して多項式近似写像の対称性として現れるため，多項式近似写像は不変式環の生成元から構成されることになる．そこでグレブナー基底を用いて不変式環の高次生成元を計算し，多項式近似写像を高次項まで求めることで更なる高精度復号法を提案する．

A2 シャノン限界を実現する誤り訂正符号の提案：符号化は高い対称性を持つ巡回符号と代数幾何符号を適用し，それらに対する復号法を A1 の手法により構成することで高性能な誤り訂正符号を開発する．次にそれぞれの誤り訂正符号ごとに具体的に求まる多項式近似写像の各項の情報から伝送誤り確率の評価を行い，シャノン限界を実現する符号を提案する．

課題 B：
B1 導来圏上でのネットワーク符号理論の構成：ポアンカレ-ヴェルディエ双対性と最大送信容量に関する予備結果をふまえて，これまでの理論体系を導来圏上で構成する．これをもとに導来圏の解析で強力な道具である双対層，テンソル層，偏屈層等のネットワーク符号での役割を考察する．

B2 最大送信容量を実現するネットワーク符号を構成：B1 で行う導来圏での理論整備をもとに，ネットワーク符号を与える層の複体上の写像で層コホモロジーの次元が増加するものを構成する．このような写像の不動点は層コホモロジーの次元が最大のものであり，最大送信容量を実現するネットワーク符号を定める．次にレフシェッツ不動点定理をもちいて写像の不動点の存在を調べ最大送信容量の決定と符号の開発を行う．

３．研究の方法

課題 A：
(1)グレブナー基底を用いた高精度復号法の構成：グレブナー基底を用いて不変式環の高次生成元を特定し，多項式近似写像の高次項を具体的に求めることで高精度復号法を開

発する．ここでは対称群の部分群からなる対称性と代数曲線から誘導される対称性について研究を進める．前者は巡回符号を含むクラスであり後者は代数幾何符号として構成され，有理写像の特徴からこの 2 種類の不変式環構造を調べれば多項式近似写像に現れる全ての対称性を考察することができる．

(2)有理写像力学系の不変集合の解析：有理写像力学系に現れる不動点の安定／不安定／中心多様体上の軌道を多項式近似写像の軌道として近似し，多項式の近似次数ごとに真軌道との誤差を評価する．また有理写像の不確定点近傍の軌道については，特異点解消法を用いて近似軌道との誤差を評価する．

(3)伝送誤り確率の評価とシャノン限界を実現する誤り訂正符号の提案：まず指定された対称性を持つ符号化の集まりを考え，その中から一様分布で符号化を選んだ際の伝送誤り確率の期待値を評価する．次にこの期待値と各符号化の伝送誤り確率との差を評価する．この評価は多項式近似写像の次数構造からドゥーブ分解を構成しそのマルチンゲール過程を調べることで得られるが，ここに(2)で調べる力学系の詳細な情報が必要となる．これらの評価をもとに，最終的に伝送誤り確率が 0 に漸近する符号化の存在を示し，シャノン限界を実現する誤り訂正符号を提案する．ここでの評価の際に有理写像の不確定点から不動点へのヘテロクリニック軌道の情報が必要になる可能性もある．その場合にはメルにコフの方法を用いることで対応する予定である．

課題 B：
(1)導来圏上でのネットワーク符号理論の構成：ネットワーク符号層の単射分解の構成と各次数に現れる単射層のネットワーク符号としての意味を考察する．これをもとにネットワーク符号を与える導来圏の部分圏を明らかにする．一方予備研究により幾つかのグラフの例では与えられたネットワーク符号層に対して，その双対層とのテンソル層をとることで最大容量を実現するネットワーク符号層が構成できる．ここでの考察を一般化する為に，ネットワーク符号部分圏の双対層，テンソル層，偏屈層についての理論整備を行う．

(2)不動点定理を用いた最大送信容量決定と符号構成：ネットワーク符号に対応する層の複体から別の層の複体への写像であって層コホモロジーの次元が増加するものを構成する．このような写像の不動点は層コホモロジーの次元が最大になる層の複体であり，最大送信を実現するネットワーク符号に対応する．具体的な写像は,これまで考察してきた例を任意のグラフへ一般化することにより構成する．その後レフシェッツ不動点定理を用いて最大送信ネットワーク符号を構成し，その次元から最大送信容量を決定する．なお適切な写像を構成することが困難な場合は，既に最大容量の特徴付けが知られているシングルソース型問題や本課題の原型であるグラフ理論の最大フロー・最小カット問題にここでの論法を適用して修正・改良を試みる．

(3)課題 A との融合とその他の実問題への応用：課題 A と融合させた各辺で雑音が発生する状況での誤り訂正ネットワーク符号についても研究を進める．まずエルディッシュ-レンイ(1959)のランダムグラフの連結成分の個数に関する結果が 0 次コホモロジーの次元として解釈できる点に着目し，層コホモロジーの確率的漸近挙動を特徴づける問題として一般化することで，雑音状況下での最大送信容量の決定を行う．またこれをもとに予備研究で行っているホモロジー代数とネットワークの部分的欠損問題の関係を課題 A とあわせて考え，より現実的な問題への応用を行う．

４．研究成果
　有理写像の上で成立していた符号-復号双対定理を，多項式写像として新たに理解し，その上で一般化双対定理の形で定式化しなおした．まず，一般の有限体において，最尤推定復号を多項式写像として再現することができた．ここで重要になる発見は，一般化 MacWilliams 恒等式をもちいて最尤推定復号を表示できることを示したことである．これにより，これまで行ってきた有理写像型近似化方法を，一般の有限体上の誤り訂正符号に対して適用できるようになった．さらに，有理写像ではなく多項式写像で扱えることになる，という単純化も実現される．また,MacWilliams 恒等式をもちいて, 近似の一般項の形を具体的に書き下すこともできる．これにより，近似最尤推定復号の高次数化について，重みが低い双対符号語からリストアップすることで，原理的には希望の次数まであげることができることを明らかにした．
　また具体的な数値実験も試みた．ここでの実験は BCH 符号化と Gallager の方法をベースにしたランダム行列を用いる方法を試した. まず BCH についてであるが, 符号長が 512 ビットまで実験を行い, Berlekamp-Massey 復号法との比較をおこなった．全体としての傾向は，次数をあげることで復号パフォーマンスの改善が確認できた．一方で，単に次数をあげるだけでは不十分であるいくつかの事例も構成できた．例えば，それぞれの次数は双対符号語の重みに対応するが，双対符号語のある重みの符号語を部分的に近似最尤推定復号に入れるより，その重みのすべての双対符号語を入れた方が,パフォーマンスが向上する傾向があるようである．ただ，次数を 5 次程度まであげておけば Berlkamp-Massey

復号に比べて格段にパフォーマンスが良くなることが確認できることから，本提案手法の有効性は十分示されたと思われる．ここで得られた一連の一般化 MacWilliams 恒等式に関する結果は現在論文を執筆中である．

また，研究期間の後半は復号化に使われる有理写像や多項式写像の力学系的性質を，計算機をもちいて調べる，一般的な手法の開発にも取り組んだ．力学系の性質は不変集合およびそれらをつなぐコネクティング軌道によって大きく分類されるため，まずは不変集合の効率的な構成法を開発することが重要になってくる．そこで，相空間から有限個の点列を選びそれらをポイントクラウドデータとしてパーシステントホモロジーを適用することで，近似的に不変集合を構成する手法を提案した．ここでパーシステントホモロジーはアルファ複体からなるフィルトレーションから構成し，これにより空間的にロバストな特徴づけが可能となる．一方で，時間発展の情報を取り込むために，An クイーバとしてパーシステントホモロジーを扱うのみならず，2 つの An クイーバからなるテンソル積に対して表現を考えるアイディアを提案した．しかしながら，一般に An クイーバのテンソル積上の表現に対して，直既約分解をしらべることは数学的に非常に難しい問題となるため，最初のステップとして A2 と An クイーバのテンソル積に問題を制限した commutative ladder 型の表現について研究を実施した．長さ n に応じた表現型の分類，および有限型の場合の直既約表現のリストアップとその具体的構成法について結果が得られた．

さらに符号理論全般の問題としては，有限体上の線形問題として復号を扱うことが可能であるが，その際に圧縮センシングの手法が使えるかどうか検討をおこなった．そこで得られた副産物としては，二元体上のホモロジー群の最小代表元をもとめる問題を離散最適化問題とみなすことで，圧縮センシングの手法を用いたアルゴリズムを提案することに成功した．

ネットワーク符号と層コホモロジーに関する課題では，当初導来圏としての定式化を試みる予定であったが，いくつかの問題点が明らかになった．まず，層としてネットワーク符号を設計することは可能であるが，そこから送信容量を決定するには，独立な情報流を決定する必要がある．これはクイーバの表現としては直既約分解を調べる事に対応する．そこで層としての定式化から表現として情報流を表し，その直既約成分を調べる形で問題を定式化し直した．そこで課題 A とも連携させる意味で，commutative ladder 型のクイーバについて，その表現圏の構造を精密に調べ上げた．さらに，近年 Justin Curry 氏によって開発された層コホモロジーを用いたパーシステントホモロジーの拡張についても調査を行い，ネットワーク符号への適用可能性を検討した．また，グラフ上の符号理論でも使われる最小全域木とランダムグラフの関係を，ランダム単体複体へ一般化することにも成功した．この成果は将来的には，グラフではなく単体複体からなる組み合わせ構造上で符号を構成する際に重要になることが期待される．

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　4　件）

① E. Escolar and Y. Hiraoka, Persistence Modules on Commutative Ladders of Finite Type, Discrete and Comput. Geom, 査読有, Vol.55, 2015, pp.100-157, DOI:10.1007/s00454-015-9746-2

② E. G. Escolar and Y. Hiraoka, Optimal Cycles for Persistent Homology via Linear Programming, Optimization in the Real World -Towards Solving Real-World Optimization Problems-, Mathematics for Industry, Springer, 査読有, Vol.13, 2015, pp.79-96, DOI:10.1007/978-4-431-55420-2-5

③ E. Escolar and Y. Hiraoka, Computing Optimal Cycles of Homology Groups, A Mathematical Approach to Research Problems of Science and Technology - Theoretical Basis and Developments in Mathematical Modeling, Springer, 査読有, Vol. 5, 2014, pp.101-118, DOI:10.1007/978-4-431-55060-0-8

④ E. Escolar and Y. Hiraoka, Computing Persistence Modules on Commutative Ladders of Finite Type, Lecture Notes in Computer Science, 査読有, Vol.8592, 2014, pp.144-151, DOI:10.1007/978-3-662-44199-2-25

〔学会発表〕（計　4　件）

① 平岡裕章, The lifetime sum and the Tutte polynomial in Linial-Meshulam random complexes, Workshop on Random and Statistical Topology, 平成 28 年 2 月 17 日-19 日，「東北大学原子分子材料科学高等研究機構（宮城県仙台市）」

② 平岡裕章, Topological data analysis on materials science: statistics and continuation、Workshops at Oberwolfach in 2015 (Computational Geometric and Algebraic Topology), 平成 27 年 10 月 11 日-10 月 17 日，「Oberwolfach(ドイツ)」

③ 平岡裕章, Topological Data Analysis: Network, Sensor, and Material、22 世紀創造のための数学, 平成 27 年 9 月 28 日-29 日, 「富士ソフトアキバプラザ／アキバホール(東京都千代田区)」

④ 平岡裕章, Random topology, minimum spanning acycle, and persistent Homology, DYNAMICS, TOPOLOGY AND COMPUTATIONS, 平成 27 年 6 月 15 日-6 月 20 日,「Będlew(ポーランド)」

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計 0 件）

名称：
発明者：
権利者：

種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等
http://www.wpi-aimr.tohoku.ac.jp/hiraoka_labo/index.html

６．研究組織
(1)研究代表者
平岡 裕章 （HIRAOKA, Yasuaki）
東北大学・原子分子材料科学高等研究構・准教授
研究者番号：10432709