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 ３０ 日現在

機関番号：３３９２４
研究種目：研究活動スタート支援
研究期間：2014～2015
課題番号：２６８８７０４３

研究課題名（和文）表現論やグレブナー基底の理論からのアプローチによる代数的符号理論の問題の研究

研究課題名（英文）Study of algebraic coding theory via representation theory and via the theory of Groebner bases

研究代表者
中島　規博（NAKASHIMA, Norihiro）

豊田工業大学・工学部・研究員

研究者番号：９０７３２１１５

交付決定額（研究期間全体）：（直接経費）　　1,800,000円

研究成果の概要（和文）：本研究の目的は、表現論やグレブナー基底の理論を代数的符号の研究に応用することであった。アフィン多様体符号には、誤り位置の決定にグレブナー基底の理論を使い、誤り値の決定に離散フーリエ変換を使う誤り訂正アルゴリズムが提案されている。研究期間内の研究では、アフィン多様体符号の誤り訂正アルゴリズムを応用し、射影Reed-Muller符号に適用可能な誤り訂正アルゴリズムを構成した。さらに訂正数、計算量、復号誤り率の評価も行った。
また、GarciaとStichtenothにより定義された符号系列に対して、離散フーリエ変換を改良し、既存アルゴリズムの計算量を削減した。

研究成果の概要（英文）：The aim of this research is to apply representation theory and the theory of Groebner bases to algebraic coding theory. There is an error correcting algorithm for affine variety codes such that the theory of Groebner bases is used to determine error positions and that the discrete Fourier transform is used to determine error values. I constructed an error correcting algorithm for the projective Reed-Muller codes via the algorithm for affine variety codes. Moreover, I evaluated the number of correctable errors, the computational complexity and codeword error rates.
I also modified the discrete Fourier transform for towers of codes defined by Garcia and Stichtenoth. The computational complexity of the error correcting algorithm for codes by Garcia and Stichtenoth is reduced.

研究分野：代数的符号理論

キーワード：代数的符号理論　グレブナー基底　表現論　超平面配置

１．研究開始当初の背景

代表者は本研究の開始以前に、表現論、グレブナー基底の理論、超平面配置の理論といった代数学の分野で研究し、それぞれの分野で成果を残してきた。これら数学分野は誤り訂正符号理論との強い関わりが知られている（誤り訂正符号理論とは、ディジタル通信の際に冗長データを付け加え、一定個数以下の誤り訂正を可能にする理論である）。具体例として、グレブナー基底の理論と離散フーリエ変換(DFT)を用いたアフィン代数多様体符号の復号法や有限鏡映群の不変式論を用いた self-dual 符号の重み多項式の計算法などが挙げられる。研究開始当初の目的は、

(1)アフィン代数多様体符号の復号法の類似を射影代数多様体符号に構成する研究

(2)一般化準巡回符号の符号探索に重み多項式の明示式や古典群の表現論を導入する研究

を表現論やグレブナー基底の理論を用いて進めることであった。

２．研究の目的

上述した(1)、(2)について、研究開始当初の目的の詳細を以下に示す。

(1) 本研究では、射影代数多様体符号に対して誤り訂正能力と計算量の面で性能の高い復号法を構成することを当初の目的とした。Reed-Muller(RM)符号の射影化である射影 RM 符号には error-locating pairs を用いた計算量が符号長の 3 乗のオーダーである復号法が適用できる。これに対して代表者はアフィン代数多様体符号の理論を応用して低次元の射影 RM 符号に復号法を構成した。この復号法の計算量は符号長の 3 乗より少ない。しかし一方で、誤り位置に偏りがある場合には、最少距離から導かれる訂正限界まで誤り訂正ができないという課題もある。本研究では、現在の射影 RM 符号の復号法を高次元化し、一般的な射影代数多様体から定義される符号の復号法を構成することを目的とした。さらにグレブナー基底にかかわる Berlekamp-Massey-Sakata(BMS) アルゴリズムあるいは DFT を改良し、誤り訂正能力面でよりよい射影代数多様体符号の復号法の構成を試みる。

上述のアフィン代数多様体符号の復号法において、シンドロームを使って誤り位置の集合を零点に持つ多項式からなるイデアルのグレブナー基底を計算する方法が、BMS アルゴリズムである。グレブナー基底は多変数多項式環での割り算を可能にし、上述のアフィン代数多様体符号の復号法では離散フーリエ変換につなげる拡張写像の定義に不可欠である。シンドロームの違いに注意しながら射影代数多様体符号にも BMS アルゴリズムの類似を作り、誤り訂正数に関係のある最小距離や Feng-Rao 設計距離を計算することも目的とした。Feng-Rao 設計距離はアフィン多様体符号の誤り訂正能力を計る値である。

(2) 一般化準巡回符号の探索から、Sloane の未解決問題と低密度パリティ検査(LDPC)符号の探索を目指した。1972 年に Sloane により符号長 72 の extremely doubly even self-dual 符号が存在するか否かの問題が提起され、現在も未解決のままである。また一般化準巡回符号は、多くの場合、データ転送速度に関する限界である Shannon 限界に 0.0045dB まで迫る復号法を持つ LDPC 符号である。これら二つの問題意識の下に、所属研究室で研究が進められ、生成行列がみたすべき条件がいくつか予想されていた。本研究では、探索途中で得られる部分符号の重み多項式を探索に導入するとともに予想された条件を証明し、探索範囲を狭めることで探索効率を上げることを試みた。

３．研究の方法

(1)研究室のメンバーとセミナーを行い、先行研究の論文から射影 RM 符号の性質を学んだ。また、Hermitian 符号などの具体例を計算した際に、復号計算量が削減できることに気付き、Garcia-Stichtenoth による符号の復号算量削減に発展した。計算面では数式計算ソフト MATLAB を使い、復号法の具体例計算や Feng-Rao 設計距離を計算した。MATLAB には有限体上の計算プログラムを組むのが手軽であるというメリットがある。

(2) 所属研究室のメンバーと協力して計算順序の改良と計算途中で重みをチェックする計算アルゴリズム作成を試みた。計算順序の面では、符号の生成行列を構成する際に決定する成分の順番と、符号が self-dual であるための４つの条件（１つでもみたされれば self-dual になる条件）を使う順番を試行錯誤した。また、生成行列の各行が最小重みを超えたら求める符号でないことを利用するチェック機能の導入も試みた。

４．研究成果

(1) 代数的符号の１クラスであるアフィン多様体符号には、BMS アルゴリズムと DFT を応用した符号化・復号化アルゴリズムが提案されている。本研究では、一般的な射影代数多様体から定義される符号の符号化・復号化に関する成果は得られなかったが、大きく分けて「射影 RM 符号」と「Garcia-Stichtenoth により定義された２種類の曲線上のアフィン多様体符号」の二つに関する成果が得られた。

射影 RM 符号の研究では、既存の手法（符号長の 3 乗のオーダーの計算量）と比べて計算量の少ない復号法を構成し、誤り訂正数の

決定と計算量の議論、誤り制御性能の比較を行った。本復号法は、内定日以前に計算した低次元の具体例を内定日以降に一般の次元に拡張したものであり、復号法の性能評価も内定日以降に行った。また、本復号法の鍵は、射影空間をアフィン空間の和集合とみなして、各アフィン空間に対応する（アフィン多様体符号である）RM 符号のシンドロームを得ることである。各アフィン空間に対応する RM 符号の復号には、BMS アルゴリズムと DFT による既存復号法を適用した。

Garcia-Stichtenoth により定義された２種類の曲線上のアフィン多様体符号の研究では、定義域のインデックスを曲線上に制限した DFT を提案し、DFT の計算にかかる有限体演算回数を削減した。また、提案 DFT を使ってもアフィン多様体符号のアルゴリズムが機能することを示し、符号化・復号化アルゴリズムの計算量も削減した。さらに、本研究では Garcia-Stichtenoth により定義された符号系列が Miura の提案した代数曲線符号のクラスに属しているかどうかも検証している。代数曲線符号の復号には変数の極位数を計算しなくてはならないが、Miura の符号として表すことができれば、複雑な極位数の計算をすることなくアフィン多様体符号として復号アルゴリズムを適用できる。本研究期間内に、２種類のうち１種類は Miura の符号として表すことができた。現在は、残りの１種類についても Miura の符号として表す研究を進めている。

(2)研究開始以前に探索が終わっていた符号長 40、次元 20、最小重み 10 までの符号で探索時間の削減ができたが、符号長を伸ばす意味でのめざましい発展は得られなかった。最小重みによるチェック機能の働きを上げるために、今後は、各行だけでなく行の線形和の重みもチェックする機能の導入を試みる。

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　１　件）
① Norihiro Nakashima, Hajime Matsui, Decoding of Projective Reed-Muller Codes by Dividing a Projective Space into Affine Space, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Volume E99-A, No. 3, pp. 733-741, 2016, 査読あり
DOI: 10.1587/transfun.E99.A.733

〔学会発表〕（計　１４　件）
①Norihiro Nakashima, Discrete Fourier transforms on some asymptotically good towers of curves, Workshop on Hyperplane Arrangements and Singularity Theory （招待講演）（国際学会）, Hokkaido University, Sapporo, Hokkaido, Mar. 22, 2016

②中島規博、アフィン多様体符号の誤り訂正における離散フーリエ変換、九州産業大学数学教室セミナー（招待講演）、九州産業大学（福岡県福岡市）、2015 年 12 月 9 日

③中島規博、松井一、Modified DFTs for Affine Variety Codes、第 38 回情報理論とその応用シンポジウム (SITA2015)、岡山県倉敷市下電ホテル、2015 年 11 月 25 日

④中島規博、松井一、グレブナー基底と DFT を用いたエルミート曲線符号の符号化・復号化、平成 27 年度電気・電子・情報関係学会東海支部連合大会, 名古屋工業大学（愛知県名古屋市）、2015 年 9 月 28 日

⑤中島規博、松井一、有限体の部分半群における DFT のアフィン多様体符号への応用, 2015 年電子情報通信学会ソサイエティ大会, 東北大学川内北キャンパス（宮城県仙台市）, 2015 年 9 月 11 日

⑥ 中島規博、符号の Locality と Availability について、第４回誤り訂正符号のワークショップ、石川県加賀市白山菖蒲亭、2015 年 9 月 3 日

⑦ Norihiro Nakashima, Hajime Matsui, A semigroup DFT over finite fields applied to affine variety codes, The IEEE International Symposium on Information Theory 2015, Recent Results Poster Session, Hong Kong Convention and Exhibition Centre, Hong Kong, China, June 17, 2015

⑧中島規博、代数的な誤り訂正符号の符号化と復号化について、大阪組合せ論セミナー（招待講演）、大阪市立大学梅田サテライト（大阪府大阪市）、2015 年 4 月 18 日

⑨中島規博、松井一、離散フーリエ変換と BMS アルゴリズムを用いた射影 Reed-Muller 符号の復号法, 2015 日本数学会年会, 明治大学駿河台キャンパス（東京都千代田区）, 2015 年 3 月 22 日

⑩中島規博、射影空間の分解を用いた射影 Reed-Muller 符号の復号法とその性能評価, 第 11 回数学総合若手研究集会、北海道大学理学部５号館（北海道札幌市）、2015 年 3 月 7 日

⑪中島規博、代数的誤り訂正符号の復号法について、信州代数セミナー、信州大学松本キャンパス（長野県松本市）、2015 年 2 月 2 日

⑫中島規博、松井一、 Correction of Errors for Projective RM Codes by Decomposing Projective Space into Affine Spaces、第３７回情報理論とその応用シンポジウム（SITA2014)、富山県黒部市宇奈月温泉宇奈月ニューオータニホテル、2014 年 12 月 10 日

⑬中島規博、射影空間の分解を用いた射影 Reed-Muller 符号の復号法、2014 年度第２回九州大学組合せ数学セミナー、九州工業大学サテライト福岡天神（福岡県福岡市)、2014 年 10 月 18 日

⑭中島規博、松井一、射影 Reed-Muller 符号の誤り値決定と計算量、2014 年電子情報通信学会ソサイエティ大会、徳島大学常三島キャンパス（徳島県徳島市)、2014 年 9 月 25 日

〔図書〕（計　０　件）

〔産業財産権〕
○出願状況（計　０　件）

○取得状況（計　０　件）

〔その他〕
ホームページ等
NAKASHIMA Norihiro’s page
http://www.math.sci.hokudai.ac.jp/~naka_n/index.html
（個人ウェブページ）

６．研究組織
(1)研究代表者
中島　規博　（NAKASHIMA, Norihiro）
豊田工業大学・工学部・研究員
研究者番号：９０７３２１１５