様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　２８　日現在

機関番号：　３３９２４
研究種目：　挑戦的萌芽研究
研究期間：　2015～2017
課題番号：　１５Ｋ１３９９４

研究課題名（和文）グレブナー基底を用いた高性能な誤り訂正符号の構成

研究課題名（英文）Construction of high-performance error-correcting codes using Grobner bases

研究代表者
松井　一（Matsui, Hajime）

豊田工業大学・工学（系）研究科（研究院）・准教授

研究者番号：８０３２９８５４

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：1. 射影Reed-Muller符号の高速復号法が得られた（中島規博氏との共同研究）．ガウス消去法を用いた復号化と比較して計算量のオーダーを下げることができた．
2. ユークリッド整域における剰余環上の誤り訂正符号について調べた．これは特別な場合として準巡回符号や整数符号を含む．それぞれの符号に対し被約生成行列を一意に定めることができることを示した．これは符号の構成や探索にとって有用である．
３．あるクラスの多値論理多項式に対する畳み込み定理を導出し，それらの間の積に対する高速計算法を確立した．その際用いられる離散フーリエ変換が，アフィン多様体符号の復号化で用いるものの転置になっていることを示した．

研究成果の概要（英文）：1. A fast decoding method of projective Reed-Muller codes has been established (collaboration with Dr. Norihiro Nakashima). Compared to decoding using the Gaussian elimination method, the order of its computational complexity could be reduced.
2. The error-correcting codes over the residue rings of the Euclidean domains have been investigated. They include quasi-cyclic codes and integer codes as special cases. We showed that we can uniquely determine the generator matrix for each code. This fact is useful for code construction and search.
3. The convolution theorem for a class of multiple-valued logic polynomials has been established and a fast calculation method for the multiplication of them has been derived. We showed that the discrete Fourier transform used in the convolution theorem has a transposition relation to that used for decoding affine variaty codes.

研究分野：　情報理論

キーワード：　離散フーリエ変換　多値論理関数　準巡回符号　離散Fourier変換　ユークリッド整域　畳み込み定理　整数符号　代数的符号

１．研究開始当初の背景
(1) 符号理論における根本的な問題として，誤り訂正能力が高い符号を見つけるという問題がある．研究代表者によるグレブナー基底を応用した「基本等式」を用いる手法（後述）は，この問題に有効である．この手法の実用的な応用としては，LDPC 符号の探索と構成が挙げられる．LDPC 符号（低密度パリティ検査符号，LDPC＝Low Density Parity Check）とは，現在最も高性能であると言われる誤り訂正符号である．しかし，状況に応じた最適な LDPC 符号を見つけることは，現在のところまだ難しい問題である．また，多元 LDPC 符号についても構成手法を確立し，産業界との共同研究につなげる．

(2) 研究代表者はこの符号の構成問題において，最近，基本的で重要なアイディアを得た．それは研究代表者が基本等式と呼んでいるものである．符号の構成を，基本等式を解くことに帰着でき，これにより従来技術と比べて全探索の計算量を削減できる．さらに研究代表者はこの符号の構成問題において，独自のアルゴリズムを 2 つ考案した．当研究室では，一つは「全探索法」，もう一方は「素因子分解法」と呼んでいる．これらの結果については，論文誌に最近受理され，またウェブ上で既に公開している．従来の符号探索法は，ベクトル空間とガウス消去法を基礎としていたが，我々の手法は，多項式環上の加群とグレブナー基底を基礎としており，理論的に優位性が示される．しかも実際に計算機で高速性が実証されている．また自己直交性や自己双対性の検証についても効率の良い方法を考案し，国内研究集会で発表済である．

(3) 研究代表者は新たなアルゴリズムを開発しつつあるため，早急に符号探索を開始する必要がある．このような状況の中で，研究代表者の符号探索手法はブレーク・スルーとなりうる．また LDPC 符号については，現在広く用いられているリード・ソロモン符号から，次世代の LDPC 符号に，まさに今，置き換わりつつある状況である．効率的な探索手法が確立すれば，LDPC 符号や多元 LDPC 符号の高性能化の鍵となるという意味で，重要性が高い．

２．研究の目的
第一に，研究代表者による独自のアルゴリズムを用いて，高い訂正能力を持つ一般化準巡回符号や一般化整数符号，p 進数体上の誤り訂正符号の構成を行う．
第二に，研究で培った符号の探索手法を応用して，実用的な各種の誤り訂正符号，例えば LDPC 符号や多元 LDPC 符号等を構成し，通信路モデルに適用する．

３．研究の方法
(1) 一般化準巡回符号の構成
基本等式による一般化準巡回符号の構成において，探索順序はかなり自由度があることがわかった．現在はまだ forward（辞書式）および backward（逆辞書式）の探索順序しか検討していないため，さらに次数付き辞書式順序などの探索順序も検討し，効率化を行う．このように探索順序にもグレブナー基底の考え方を応用し高速化する．また，数式処理ソフトウェアとして，現在は主に MATLAB と MAGMA を用いている．MATLAB においては，一部は並列計算を導入している（parfor の使用）．MATLAB の distributed computing server や，C 言語の CUDA を導入し，より強力な並列計算を行い，高性能符号を探索する．

(2) ガウス整数環上の一般化整数符号
一般化整数符号の探索手法は，ユークリッド整域と呼ばれる代数構造に適用できる．代表的なユークリッド整域としては，有限体上の１変数多項式環，整数の他に，ガウス整数環がある．このガウス整数環上の一般化整数符号の探索手法を確立する．

(3) ガウス整数やアイゼンシュタイン整数の素元に対する掘割問題への応用
一般化整数符号についてはある種の素因子分解が有効に働くことが示されており，ガウス整数環上の一般化整数符号についても同様に素元分解が有効に働く．ガウス整数の素元に対しては掘割問題と呼ばれる未解決問題があり関係が深い．また掘割問題はアイゼンシュタイン整数や他の虚二次数体の素元に対しても定式化されるため，これらの一般化された掘割問題についても考察する．

(4) Lee 距離による探索
これまでの整数符号に対しては，Lee 距離による復号法が有効であった．一般化整数符号に対しても Lee 距離が定義されるので，最小 Hamming 距離ではなく最小 Lee 距離による探索を行う．最小 Lee 距離の大きな一般化整数符号を見つけ，通信路モデルへ応用する．

(5) p 進数体上の誤り訂正符号
p 進整数環はユークリッド整域の例であり，上記の一般化整数符号の探索手法が適用できる．よって，探索を行い，高性能な符号を構成する．また，p 進整数環には p 進距離と呼ばれる自然な距離が備わっているので，最小 p 進距離が最大の符号を探索する．

４．研究成果
(1) 射影 Reed-Muller 符号の高速復号法が得られた（中島規博氏との共同研究）．射影空間を複数のアフィン空間に分解した後，Berlekamp-Massey-Sakata アルゴリズムおよび研究代表者によるグレブナー基底と離散フーリエ変換を用いたアフィン多様体符号の復号化を応用する手法である．ガウス消去法を用いた復号化と比較して計算量のオー

ダーを下げることができた．この結果は査読付き論文誌に掲載された．

(2) ユークリッド整域における剰余環上の誤り訂正符号について調べた．これは特別な場合として準巡回符号や整数符号を含み，かなり一般的な枠組みである．本研究の前半では，modulo a および modulo b の符号の生成行列の積により，modulo ab の全ての符号の生成行列が作られることを示した．また， a と b が互いに素の時，この対応は１対１であることも示した．中国剰余定理により，これら 2 つの符号が存在することは分かるが，我々の結果によりそのような符号を明示的に与えることができる．本研究の後半では，有理整数環、1 変数多項式環、Gauss および Eisenstein 整数環、p 進整数環，1 変数形式的巾級数環のような典型的なユークリッド整域についてより詳細に調べた．このとき，それぞれの符号に対し被約生成行列を一意に定めることができることを示した．これは符号の構成や探索にとって有用である．最後に，これらのユークリッド整域上の行列の Hecke 環に，被約生成行列の理論を応用して，ある種の数え上げ公式を得た．以上の結果は査読付き論文誌に受理された．

(3) あるクラスの多値論理多項式に対する畳み込み定理を導出し，それらの間の積に対する高速計算法を確立した．このクラスの多値論理多項式は，有限体の直積から有限体への関数（多値論理関数）のうち，特に有限体に含まれる半群の直積を定義域とする関数と１対１に対応している．この１対１対応は，離散フーリエ変換の類似によって与えられ，またこの離散フーリエ変換の類似はアフィン多様体符号の復号化で用いるものとは転置の関係になっている．この結果は査読付き論文誌に受理された．また，更に大きなクラスの多値論理多項式に対する畳み込み定理と，それらの間の積に対する高速計算法を考案中であり，結果の一部について学会発表を行った．

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３件）

1. H. Matsui, “Multiplicative structure and Hecke rings of generator matrices for codes over quotient rings of Euclidean domains,” MDPI Mathematics, vol.5, no.4, 82, Dec. 2017. 査読有. Doi:10.3390/math5040082
2. H. Matsui, “A convolution theorem for multiple-valued logic polynomials of a semigroup type and their fast multiplication,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E99-A, no.6, pp.1025-1033, Jun. 2016. 査読有. DOI:10.1587/transfun.E99.A.1025
3. N. Nakashima, H. Matsui, “Decoding of projective Reed-Muller codes by dividing a projective space into affine spaces,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E99-A, no.3, pp.733-741, Mar. 2016. 査読有. DOI:10.1587/transfun.E99.A.733

〔学会発表〕（計１３件）

1. 松井一, “多値論理多項式に対する離散フーリエ変換の応用と積の高速化,” 電子情報通信学会 情報理論研究会, 3 月 8-9 日, 信学技報, vol.117, no.487, IT2017-116, p.71, 2018 年 3 月.
2. 市川翔太, 井上直樹, 椋野純一, 松井一, “論理多項式を用いたベイズ学習における漸近評価の分類”（ポスター発表） 第 40 回情報理論とその応用シンポジウム, 11 月 28 日－12 月 1 日, 2017.
3. H. Matsui, “On multiple-valued logic polynomials of a subset type”, Recent Results Posters at The International Symposium on Information Theory and Its Applications (ISITA2016), p.547, Monterey, California, October 30-November 2, 2016.
4. 中島規博, 松井一, “Garcia-Stichtenoth による代数曲線符号の誤り訂正計算量の削減,” 日本数学会秋季総合分科会 応用数学分科会講演アブストラクト, pp.51-54, 9 月 15 日－18 日, 2016.
5. H. Matsui, “On Multiple-Valued Logic Polynomials of a Product Type”, 第 38 回情報理論とその応用シンポジウム予稿集, pp.748-751, 11 月 24 日－27 日, 2015.
6. N. Nakashima, H. Matsui, “Modified DFTs for Affine Variety Codes”, 第 38 回情報理論とその応用シンポジウム予稿集, pp.177-182, 11 月 24 日－27 日, 2015.
7. 木下真志, 松井一, “ガウス素数の掘割問題についての虚二次数体への一般化と右手法,” 電気・電子・情報関係学会東海支部連合大会, A5-1, 9 月 28-29 日, 2015.
8. 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,” 電気・電子・情報関係学会東海支部連合大会, K1-2, 9 月 28-29 日, 2015.
9. 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,” 電子情報通信学会ソサイエティ

大会基礎・境界講演論文集 A-6-3, p.97, 9 月 8-11 日, 2015.
10. 木下真志, 松井一, “右手法を用いた虚二次数体の素元における掘割探索法の並列化, ”電子情報通信学会ソサイエティ大会 基礎・境界講演論文集 A-12-2, p.123, 9 月 8-11 日, 2015.
11. 松井一, “符号理論と離散フーリエ変換, ”第 4 回誤り訂正符号のワークショップ, 石川県白山菖蒲亭, 9 月 2-4 日, 2015.
12. N. Nakashima, H. Matsui, “A semigroup DFT over finite fields applied to affine variety codes”, Recent Results Session at the 2015 IEEE International Symposium on Information Theory (ISIT 2015), Hong Kong, June 14-19, 2015.
13. 木下真志, 松井一, “虚二次数体の素元に対する掘割問題についての高速探索法, ”電子情報通信学会 技術研究報告（コンピュテーション研究会）, COMP2015-10 (2015-06), pp.67-74, 6 月 12-13 日, 2015.

〔その他〕
豊田工業大学情報通信研究室
http://www.toyota-ti.ac.jp/Lab/Denshi/InfoComm/index_ja.html
豊田工業大学研究者情報システム
http://ttiweb.toyota-ti.ac.jp/1432/pub_teacher_show.php?t=154

６．研究組織
(1)研究代表者
松井　一（Hajime MATSUI）
豊田工業大学・大学院工学研究科・准教授
研究者番号：80329854