様式 C-7-2

# 自己評価報告書

平成２３年　４月２０日現在

機関番号：１３３０１
研究種目：基盤研究（Ｃ）
研究期間：2008～2012
課題番号：20540014
研究課題名（和文）　ガロア環上の組合せ数学の研究

研究課題名（英文）　Research on combinatorics over Galois rings

研究代表者
山田　美枝子（YAMADA MIEKO）
金沢大学・数物科学系・教授
研究者番号：70130226

研究分野：代数的組合せ数学
科研費の分科・細目：数学・代数学
キーワード：差集合、符号理論、ガロア環、ガウス和

## １．研究計画の概要

本研究は基礎の代数構造を有限体からガロア環へ拡張し、そこでの組合せ数学、特に差集合、符号の新しい構成原理を得ることを目的とする．最終目的は２進拡大体での組合せ数学の理論構築であるが、途中にあるガロア環上での差集合、符号の構造、projectionを確定しながら、ガロア環のprojective limitである２進拡大体へ進む．
具体的には、標数と拡大次数を動かしてガロア環上に、その性質を保持し相互に構造上関連性のある差集合、符号の系列を構成する．この理論が構築できれば有限で離散的な構造における差集合、符号等のどのような性質が、２進拡大体の一般論から帰着し、また帰着しないかが分かり、従って有限離散構造特有の性質であるかが明らかになると予想している．そして、組合せ数学の 新しい知見を得て未解決問題、例えばHadamard予想などの解決への新しい手法の開発が期待できる．
申請時に、次の2項目を22年度までに達成する具体的計画としてあげた．
（１）標数$2^t$(t:偶数)の任意の拡大次数をもつガロア環上に差集合の系列を構成する
（２）差集合、符号に関係するガウス和を決定する．

## ２．研究の進捗状況

19 年度から 21 年度にかけて、標数 $2^t$(t:偶数)、偶数拡大についてガロア環上の差集合が存在し、標数 $2^t$のガロア環上の差集合は、標数 $2^{t+2}$で同拡大次数のガロア環の差集合に埋め込まれていることを示した．22 年度にこの結果を奇数次拡大の場合に拡張することができた（論文投稿中）．
これを証明するために、ガロア環に新しい演算を導入した．標数 $2^{t-1}$のガロア環に定義した新しい演算の下でのある部分群が、標数 $2^t$のガロア環の乗法的指標を定める．この指標に付随するガウス和が、差集合の存在の証明に重要な役割を果たしている．この証明にあたって導入した新しい演算は、形式群と関係しているように思われる．差集合と似た性質を持ち符号理論を始めとする組合せ数学と関連する difference family の構成の研究に着手し本研究の手法を応用することで、いくつか結果を得た．
一方、22 年度に標数 $2^t$のガロア環上に基本原始多項式の根を用いて生成行列を定義し Reed-Muller codeの系列を構成した．そして標数$2^{t-1}$のガロア環上のReed-Muller code は標数$2^t$のガロア環のReed-Muller codeのイデアル部分に隙間なく埋め込まれることが分かった．これより、任意の標数$2^t$、任意のorderに対してReed-Muller codeの最小Hamming距離は有限体の同じorderのReed-Muller codeのそれと一致することが得られた．また、orderが1のReed-Muller codeの最小Lee距離は、標数が$2^3$の場合を除いて常に符号の長さに等しいこと証明することができた(論文投稿中)．この証明にはある種の指標和の評価が必要である．
Reed-Muller code の特別の場合である generalized extended Hamming codeの研究に着手し、標数8の場合について最小Lee距離を決定することができた（論文準備中）．

３．現在までの達成度

②おおむね順調に進展している．
（理由）
申請時に立てた、22 年度までに標数 $2^t$(t:偶数)、すべての拡大についてガロア環上の差集合が存在し、標数 $2^t$のガロア環上の差集合を構成し、その相互の関連性を解析するという計画は順調に予定通り達成され、ガウス和との関連も明らかになった．この研究結果を基に当初計画していなかった符号理論と関連する difference family の構成の研究に着手しいくつか結果を得ることができ、研究の幅が広がった．
一方、符号理論については、ガロア環上の Reed-Muller code の系列が構成でき性質も少しずつ明らかになってきている．この符号は巡回符号を内包していて、符号語の成分がトレースで与えられることが分かり、今後は当初の計画通り、重さとガウス和との関係を明らかにしたい．
当初には関連性がわからなかったが、標数4のガロア環上の1st order Reed-Muller codeのLee weightを用いてrelationを定義するとassociation schemeが得られる計算機実験結果を得て、研究はassociation schemeやグラフ理論へベクトルを広げて発展している．
以上の成果を2本の論文と3本の投稿論文、1本のプレプリント、9回の研究集会（4回の国際会議を含む）で発表している．以上より研究はおおむね順調に進展しているといえる．

４．今後の研究の推進方策

22 年度までに得られた差集合、符号の結果や用いた新しい演算、手法を difference family、
association scheme に応用することができ研究の幅が広がっている．これ以外の組合せ数学の様々な分野への応用も考えられ、今後は申請時の計画で中心テーマであった差集合、符号から組合せ数学の他の分野へ研究を広げて、帰納的、統一的構成原理の構築を目指したい．
有限体から始まるガロア環の列の上で、組合せ数学の研究対象のそれぞれ相互の関連性、離散的構造が明らかになれば、ｐ進体、特に 2 進体での組合せ数学の理論構築に重要な情報を得ることになる．従って、研究対象の広がりと構造、性質の情報が多くなればなるほど、次の段階の研究、p 進体の組合せ理論の構築、への大きな手がかりを得ることになる．
本研究の成果の発表と同時に、数論、組合せ数学の研究者との情報交換が不可欠であるので引き続き関連する研究集会に出席する．

５． 代表的な研究成果
（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）
①R.Fuji-Hara, K.Momihara, Mieko Yamada,(論文名) Perfect difference systems of set and Jacobi sums, Discrete Mathematics,309(2009),3954-3961,査読有
②Mieko Yamada(論文名)Self-dual $Z_4$-codes of Type IV generated by skew-Hadamard matrices and conference matrices, Australasian Journal of Combinatorics,42(2008),177-188,査読有

〔学会発表〕（計９件）
①Muhammad Ilyas, Mieko Yamada(発表標題) Generalized extended Hamming codes over Galois rings of characteristic $2^n$, International Symposium on Computational Science 2011, 2011年2月16日, 金沢大(石川県)
②Mieko Yamada(発表標題)Difference sets and Reed-Muller codes over Galois rings of characteristic $2^n$, Linear Algebraic Techniques in Combinatorics/Graph Theory, 2011年2月1日, Banff International Research Station(Canada)
③Mieko Yamada (発表標題) Difference sets over Galois rings GR($2^n$,s) of odd extensions, British Combinatorial Conference 2009, 2009年7月9日, University of St. Andrews (英国)
④Mieko Yamada (発表標題) 種々の差集合の構成とガウス和、ヤコビ和, 離散数学とその応用研究集会２００８, 2008年8月21日, 茨城大学 (水戸市)
⑤Mieko Yamada(発表標題) Difference sets over Galois rings GR($2^t$, s) for even n and even s, Combinatorics 2008, Costermano(Italy)