様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２５年　５月　２１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

研究成果の概要（和文）：標数が 2^t (t:偶数)である任意の拡大のガロア環上に標数 2^t のガロア環上の差集合が標数 2^{t+2} のガロア環の差集合のイデアル部分に埋め込まれているような差集合の系列を構成した．ガロア環に新しい演算を導入し、この演算に関する指標に付随するガウス和が証明に重要な役割を果たしている．さらに同じガロア環上に埋め込み構造を持つ Reed-Muller code が存在することを示し、その性質を明らかにした．

研究成果の概要（英文）：We constructed infinite families of difference sets over Galois rings of characteristic an even power of 2. The difference set over a Galois ring of characteristic 2^n is embedded in the ideal part of the difference set over a Galois ring of characteristic 2^{n+2}. We introduced a new operation in a Galois ring and the Gauss sums associated with the character under this new operation play an important role of the proof. Furthermore, we proved there exist Reed-Muller codes with embedding system and showed several properties of them.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,200,000	360,000	1,560,000
2009 年度	700,000	210,000	910,000
2010 年度	700,000	210,000	910,000
2011 年度	600,000	180,000	780,000
年度			
総　計	3,200,000	960,000	4,160,000

研究分野：数物系科学
科研費の分科・細目：数学・代数学
キーワード：ガロア環、差集合、符号理論、ガウス和、designs, Hadamard 行列

１．研究開始当初の背景

$\mathbb{Z}$ を有理整数環、p を素数、t≧2, r を正整数とするとき、$\mathbb{Z}/p^t\mathbb{Z}$ の r 次拡大環をガロア環と呼び、$GR(p^t, r)$と書く．
1994 年に Sloane 他は良く知られた非線形バイナリ符号が標数 2^2 のガロア環 $GR(2^2, r)$の線形符号の Gray map 像であることなどを示し、これを契機として新しい符号の発見を目指し、ガロア環上の符号の研究が盛んになった．彼らの研究はガロア環に有限体上のバイナリ符号を位置づけたもので、バイナリ符号の研究に新しいアプローチを与えた意味で画期的である．符号理論だけでなく、標数 4 のガロア環上の差集合、association scheme、design などの研究も盛んになった．
しかし、標数が８以上、あるいは奇素数ベキのガロア環上の組合せ巣学の研究はあまり進んでいない．標数が８以上のガロア環の構

造は複雑で標数４のガロア環での手法が応用できないところに難しさがある．符号に関して言えば、標数が 8 以上のガロア環に Gray map にあたる写像はまだみつかっていないことが理由の一つとして挙げられる．
最近になって、一般の素数ベキの標数のガロア環やガロア環の直積へと基礎環を拡張し、そこでの差集合、符号、design,graph などの研究も始まってきた．

(1) 差集合
パラメータが $v = 2^{2n}$, $k = 2^{n-1}(2^n - 1)$, $\lambda = 2^{n-1}(2^{n-1} - 1)$である(v, k, λ)差集合は Menon 差集合と呼ばれ Ma, Davis, Dillon によって様々な例が示されてきた．ガロア環上の差集合について、Dillon は $GR(2^t, 2)$上の差集合の存在を示し、山本-山田は $GR(2^2, r)$上に差集合が存在することを示した．
Menon 差集合が存在する必要十分条件は何か長い間問題になっていたが、Kraemer, Davis によって解決された．しかし、具体的な構成問題は依然として残っている．
本研究では Menon 差集合を有限体から始まるガロア環の列の上の差集合と捉え、帰納的、統一的に構成しようとする．言い換えると、標数と拡大次数を動かして、ガロア環上に埋め込み構造を持つ差集合の列を構成するものである．山本―山田の結果は、標数 2^2 を固定し拡大次数 r を動かして、Menon 差集合の系列を構成しているもので、研究の動機となった．次は、標数と拡大次数をともに動かして埋め込み構造をもつ Menon 差集合が構成できるかが問題になる．
2002 年に、代表者はすべての正整数 t について、$GR(2^t, 2)$に差集合が存在し、ある種（mod p ではない、この研究独自）の射影を用いて $GR(2^{t+2}, 2)$上の差集合にこの差集合が埋め込まれることを示した．これにより拡大次数 2 を固定した標数が 2 べきであるガロア環に Menon 差集合の列が構成できた．
2006 年に、$GR(2^t, r)$に新しい演算を導入した．この演算がこれまで捉えることのできなかったガロア環の指標を決定しガウス和が計算できる基になった．

(2) 符号
有限環に成分をもつ符号の研究は 1970 年代から始まった．Blake は $\mathbb{Z}/m\mathbb{Z}(m = \Pi p_i$、$p_i$ は素数）上の巡回符号を構成し、その後 Spiegel によって一般の自然数 m へ拡張された．Shankar による BCH 符号の研究などもある．1994 年の Sloane 他の研究は、標数 4 のガロア環に有限体上のバイナリ符号を位置づけたもので、バイナリ符号の研究に新しいアプローチを与えた．
その後、標数 4 のガロア環上の Goethals-Seidel 符号や BCH 符号などの研究が進んだが、標数が 8 以上のガロア環の符号の研究は現在においても進んでいるとは言えない．

２．研究の目的
本研究は基礎の代数構造を有限体からガロア環 $GR(p^t, r)$へ拡張し、そこでの組合せ数学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、一挙に 2 進体での理論構築に向かうのでなく、途中にあるガロア環上での差集合、符号の構造や「射影」を確定しながら、ガロア環の射影極限である 2 進拡大体へ進む．
具体的には、標数 2^t と拡大次数 r を動かして、$GR(2^t, r)$上に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．言い換えると、有限体から始まるガロア環の列の上の差集合、符号を帰納的、統一的に構成する新しい構成原理を確立する．
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、符号のどのような性質が 2 進拡大体の一般論から帰着し、あるいは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ないかが明らかになると予想する．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 予想のなどの解決への新しい手法の開発が期待できる．

３．研究の方法
ガロア環での組合せ数学、特に差集合、符号の新しい構成原理の理論構築のために、できるだけ多くの実例を得ることが必須である．また、理論の正しさを立証する計算機実験も不可欠である．
ガロア環の標数 2^t と拡大次数 r を固定して差集合、符号の検索を行う．計算量は t と r に比例して爆発的に増加するので、プログラムを工夫する必要がある．計算量に比例して計算時間も長くなる．そこで専用の計算機を購入し、多くの実例を得た．これらの実例は理論構築に大いに役にたった．

ガロア環に導入した新しい演算に関して指標を定義し、この指標に付随するガウス和の値を決定するために、標数、拡大次数、部分群を具体的に与えて計算を行った．
この具体的な計算結果から、ガロア環上のガウス和は、多くの場合において有限体のガウス和の性質と同様な性質を持つことが分かった．また、標数を一般の素数べきに拡張しても同様になりたつ性質があることも確認できた．今後、一般素数べきの標数のガロア環での組合せ数学の理論構築に役立てたい．

得られた結果は、申請時の方針通り、逐次国

内外の研究集会で発表した．特に、組合せ数学の研究者が多く参加する国際会議（学会発表(5),(7),(8),(10)）に標準をあわせて成果発表した．成果発表とは別に、国内外の研究集会に出席し、数論、組合せ数学の研究者との最新研究の進展の情報交換やトピックスに関する議論は、新しい視点を持って問題解決を考えることができ研究遂行に大変有用であった．

組合せ数学の研究者数人が、自然発生的に毎年2月に金沢大に集まり小研究会を開催するようになった．この小研究会での議論から新たな研究が始まっている．

４．研究成果

標数 2^t (t:偶数)である、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が標数 2^{t+2} のガロア環の差集合のイデアル部分に埋め込まれていることを証明した（雑誌論文(2)）．この証明には、ガウス和が重要な役割を果たしている．2006年に導入した新しい演算は、これまで捉えることのできなかったガロア環の乗法的指標を決定させ、この指標に付随するガウス和が計算できるようになった．これにより、上記の系列の存在が証明できた．
2011年にバンフ（カナダ）で開催された国際会議（学会発表(7)）およびシンガポール国立大学で開催された国際会議(学会発表(5))に招待され、この結果について発表した．
この研究結果を基に符号理論と関連するdifference familyおよびHadamard行列の構成について新たな結果を得た（雑誌論文(1)）．

一方、符号理論については、標数が2べきであるガロア環上に有限体と同様にReed-Muller codeを定義し、符号語がtraceを用いて表すことができること、符号語のLee weightを与える式を三角関数と1のべき根を用いて表せることなどを示した． さらに、イデアル部分に標数が小さいガロア環上の Reed-Muller code が埋め込まれていることを証明した．また符号語の長さの条件のもとで双対符号もまた Reed-Muller code であることを示した．
Sloane 他の論文にならい order 1 の Reed-Muller code を Kerdock code と呼ぶことにする．指標和の上限に関する Kummar 他の定理を用いて Kerdock code の minimum Lee-weight を決定した．標数が2べキであるガロア環上の shortened Kerdock code のイデアルを法とする coset の集合に、shift 写像が巡回的に作用することを示した．これにより、イデアルを除く coset の Lee-weight distribution は等しいことが導かれた（雑誌論文(3)）．

この他に、標数が2べきであるガロア環上の拡張BCH符号を定義し部分符号の性質の考察を行った．また、標数が奇素数べきであるガロア環上に Preparata code を定義し、標数が4のガロア環の Preparata code の復号アルゴリズムと同様に、有限体上の多項式に帰着される復号アルゴリズムが構築できることを示した．
これらの結果は応用数学合同研究集会で発表した（学会発表(1)，(2)，(4)，(6)）．
以上の結果は一般の標数のガロア環上の符号理論の研究の起点となると考えている．

本研究は、平成 24 年度科学研究費基盤研究(C)「ガロア環の組合せ数学の研究」（課題番号 2450013）に引き継がれ、統計学、工学への応用の視点を持った研究へと深化させる．
2012年3月に開催された国際会議で、これまでの成果をまとめて発表する予定であったが、代表者の個人的都合でかなわなかった．引き継がれる上記の研究成果とともに成果発表したいと考えている．

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) Koji Momihara and Mieko Yamada, Divisible difference family from Galois rings GR(4,n) and Hadamard matrices, Designs, Codes and Cryptography, 査読有, 掲載決定, (2013).
URL:http://link.springer.com/journal/10623
(2) Mieko Yamada, Difference sets over Galois rings with odd extension degree and characteristic an even power of 2, Designs, Codes and Cryptography, 査読有, 67(2013), 37-57
DOI: 10.1007/s10623-011-9584-z
(3) Soryo Kawasaki and Mieko Yamada, Reed-Muller codes over Galois rings of characteristic 2^n, Science Reports of Kanazawa University, 査読有,56(2012), 1-13.
URL:http://dspace.lib.kanazawa-u.ac.jp/dspace/bulletin/sci_rep
(4) R.Fuji-Hara, K.Momihara, Mieko Yamada, Perfect difference systems of set and Jacobi sums, Discrete Mathematics, 査読有, 309(2009), 3954-3961
DOI:10.1016/j.disc.2008.11.009
(5) Mieko Yamada, Self-dual Z_4-codes of Type IV generated by

skew-Hadamard matrices and conference matrices, Australasian Journal of Combinatorics, 査読有, 42(2008), 177-188.
URL:http://ajc.maths.u9.edu.au

〔学会発表〕(計10件)
(1) 河﨑宗亮、山田美枝子、標数４のガロア環上の Kerdock code から得られる association scheme, 2012 年応用数学合同研究集会、2012 年 12 月 21 日、龍谷大学 (滋賀).
(2) 皆川泰蔵、山田美枝子、Z_{p2} 上の Preparata code の復号アルゴリズム、2012 年応用数学合同研究集会、2012 年 12 月 20 日、龍谷大学 (滋賀).
(3) Pritta Etriana Putri, Mieko Yamada, The constructions of unreal Butson-type Hadamard matrices BH(n,6)’s, 2011 年応用数学合同研究集会、2011 年 12 月 16 日、龍谷大学(滋賀).
(4) 大江純矢、山田美枝子、標数 2^n のガロア環の拡張 BCH 符号の部分符号について、2011 年応用数学合同研究集会、2011 年 12 月 15 日、龍谷大学 (滋賀).
(5) Mieko Yamada, Difference sets, divisible families and codes over Galois rings of characteristic 2^n, Workshop on Combinatorial Designs, 2011 年 6 月 2 日、National University of Singapore(シンガポール).
(6) Muhammad Ilyas, Mieko Yamada, Generalized extended Hamming codes over Galois rings of characteristic 2^n, International Symposium on Computational Science 2011, 2011年2月16日, 金沢大学(石川)
(7) Mieko Yamada, 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(カナダ).
(8) Mieko Yamada, 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)
(9) Mieko Yamada, 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 (茨城)
(10) Mieko Yamada, Difference sets over Galois rings GR(2^n, s) for even n and even s, 2008年6月24日、Combinatorics 2008, Costermano(イタリア)

〔図書〕(計１件)
(1) Muhammad Ilyas and Mieko Yamada, Generalized extended Hamming codes over Galois rings of characteristic 2^n, Gakuto Mathematical Science and Applications 34, International Symposium on Computational Science 2011(eds. Seiro Omata and Karel Svadlenka), gakkotosho, 査読有, 139-150.

〔その他〕
ホームページ等

６．研究組織
(1)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

(2)研究分担者　なし

(3)連携研究者　なし