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　２７　年　　６　月　１３　日現在

機関番号：　３２６５２
研究種目：　基盤研究(C)
研究期間：　2012～2014
課題番号：　２４５４００１３

研究課題名（和文）ガロア環の組合せ数学の研究

研究課題名（英文）A study of combinatorics over Galois rings

研究代表者
山田　美枝子（YAMADA, Mieko）

東京女子大学・現代教養学部・研究員

研究者番号：７０１３０２２６

交付決定額（研究期間全体）：（直接経費）　　3,900,000円

研究成果の概要（和文）：局所体の部分集合の射影像として組合せ構造を捉えるという新しい視点と研究方法を与えた．２進体の整数環のある部分集合をガロア環に射影すると、入れ子構造を持つ差集合の無限系列が得られることを示した．また、標数が4のガロア環にdifference family, Hadamard行列が構成できることを示した．標数が奇素数べきのガロア環については、BCH codeの2エラーまで復号できるアルゴリズムの構築、標数が一般の素数の２乗であるガロア環の差集合族の構成の結果がある．この他、有限体のCayley graphとそのlifting, skew Hadamard 行列の分類の新しい知見等の結果がある．

研究成果の概要（英文）：We gave a new approach and a new perspective on the study of combinatorics, that is,recognizing a combinatorial structure over finite fields and Galois rings as an image of a subset of a local field by natural projections. We obtained an infinite family of Menon-Hadamard difference sets over Galois rings of characteristic a power of 2 from a subset of 2-adic field by natural projections, which has a nested structure. Furthermore we showed that there exist difference families and Hadamard matrices over Galois rings of characteristic 4. For odd characteristics, we constructed a decoding algorithm of BCH codes with at most 2 errors. For a characteristic a square of a prime and an extension degree 2, we constructed difference families and Hadamard matrices.
In addition to the above results, we constructed Cayley graphs and their lifting and provided a new insight of the classification of skew Hadamard matrices over finite fields.

研究分野：　組合せ数学

キーワード：　ガロア環　差集合　ガウス和　Hadamard行列　difference family　符号

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．その後、標数2^2上の組合せ数学のさまざまな分野の研究へと発展していった．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り、標数が一般の場合のガロア環上の組合せ数学の研究はなかなか進まなかった．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などの研究成果が見られるようになった．

(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-Hadamard差集合と呼ばれMa, Davis, Dillon等によって様々な基礎の代数構造の上で多くの例が示されてきた．

Menon-Hadamard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．本研究ではMenon-Hadamard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、ガロア環上に入れ子構造を持つ差集合の列を構成するものである．

ガロア環の差集合については、Dillonの$GR(2^t, 2)$上の差集合や、山本-山田による$GR(2^2, r)$上の差集合の系列の研究結果がある．その後、山田により$GR(2^t, 2)$上に入れ子構造を持つ差集合の系列が構成された．

2007年に、$GR(2^t, r)$に新しい演算を導入した．この演算の導入が、これまで捉えることができなかったガロア環の指標を決定させ、この指標に関するガウスの和の値が計算できたことにより研究は大きく進展した．まず、標数2^t(t:偶数)、偶数拡大について，次に奇数次拡大の場合に拡張し$GR(2^t, r)$上に差集合の系列を構成した．この差集合の系列は入れ子構造を持つ．すなわち、$GR(2^t, r)$上の差集合は、$GR(2^{t+2}, r)$上の差集合のイデアル部分に埋め込まれていることが、大きな特徴である．

(2) 符号

有限環上の符号の研究は1970年代から始まった．Blake,Spiegel, Shankarによる巡回符号やBCH符号の研究がある．1994年のSloaneの研究は符号理論研究に新しいアプローチを与えた意味で画期的である．

2010年に標数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，すなわち入れ子構造を持つことが分かった．Lee重さは、1のべき根とcos関数によって表される．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を証明することができた．この証明にはある種の指標和の評価が必要である．この研究の手法は、ガロア環の他の符号に対しても応用できると思われ、Reed-Muller codeの特別の場合であるgeneralized extended Hamming code、BCH codeなどの研究に着手した．generalized extended Hamming codeやGoethals-Seidel codeの復号アルゴリズムは標数4のときのみ知られていたが、標数が2べきのガロア環の符号に拡張できる手ごたえを得ている．

(3) difference family他

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．この研究にも標数4のガロア環のガウス和が大きな役割を果たしている．

(4) 有限体上の組合せ数学

有限体を標数が最小である素数のガロア環として位置づける．この新しい視点を持って、有限体上の組合せ数学の研究を行うことや、これまでの研究を検証することは、本研究に大いに役立つ情報を与えると思われる．整数論、特にガウス和、ヤコビ和、相対ガウス和などの指標和を用いた研究は、本研究と最終目的であるp進体での組合せ数学の理論構築に重要である．

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．具体的には、標数と拡大次数を動かしてガロア環（あるいはガロア環の直積）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, difference family, Hadamard行列などの系列を構成する．最終目的はp進体での組合せ数学の理論構築で、理論が構築できれば新しい知見を得て有限離散構造特有の性質の解明や未解決問題，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．

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p^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し計算

時間が長くなるので、プログラムを工夫する必要がある．計算機実験により多くの実例を得ることができた．
本研究で得られた結果は、国内・国際会議で成果発表し、そこで数論、組合せ数学の研究者との最新研究の進展に関する情報交換やトピックスに関する議論を行った．特に、H.Kharaghani(Canada)，R.Craigen(Canada)，Q．Xiang(U.S.A.)，J．Seberry(Australia)との情報交換は、 新しい視点を持って問題解決を考えることができて、研究遂行に大変有用であった．

４．研究成果
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の新しい構成原理を得ることを目的とし、最終目的は p 進体での組合せ数学の理論構築である．
前研究において、標数が２べきで任意の拡大のガロア環 GR(2^t, r)に差集合の系列を構成した。この系列は入れ子構造を持つ．すなわち、GR(2^t, r) 上の差集合は、GR(2^{t+2}, r) 上の差集合のイデアル部分に埋め込まれている．
この差集合の射影極限は、ガロア環の射影極限である 2 進体の整数環の空でない部分集合である．逆に、２進体の整数環の部分集合で、ガロア環に射影するといつでも差集合を構成するものがあるかという疑問が自然に生じる．
ガロア環の差集合に関する先の結果を踏まえて、局所体である２進体の整数環のある部分集合をガロア環に射影すると、入れ子構造を持つ差集合の系列が得られることを示した。この研究では、p 進 log 関数や形式群が重要な役割を果たす。２進体の整数環のイデアルに形式群で演算を定義する。その自然な準同型写像でガロア環に演算が導入され、2007 年にガロア環に定義した演算に一致する．これよりガロア環の演算を形式群に拠って定義できることが分かり、ガロア環に新たな演算の導入が可能となった．整数環の部分集合は形式群の準同型である p 進 log 関数によって定義され、そのガロア環のイデアルへの自然な準同型によって定まる部分集合の和集合が差集合となる．構成から、入れ子構造を持つことは明らかである．
この研究結果を、第３１回代数的組合せ論シンポジウム（2014 年 6 月、東北大学）および Workshop on Algebraic Designs Theory and Hadamard Matrices 2014(Lethbridge 大学, Canada)で招待講演した．Workshop の報告集である Springer Proceedings in Mathematics and Statistics に掲載が決まった．
この結果は、ガロア環、有限体の組合せ構造を局所体の整数環の部分集合の射影像として捉えるという新しい視点と研究方法を与えた．また、最終目的である p 進体での組合せ数学の理論構築に大きな手がかりになると確信している．
標数が 2^2 であるガロア環上について、divisible difference family, symmetric Hadamard matrix が構成できることを示した．この結果は一般の標数へ拡張できる可能性がある．
標数が奇素数べきのガロア環については、BCH code の 2 エラーまで復号できるアルゴリズムの構築、Preparata code の復号アルゴリズムについて結果を得た．BCH code の復号アルゴリズムについて、The 3rd Taiwan-Japan Conference on Combinatorics and its Applications(2014 年 3 月, Chiayi 大学, Taiwan)で招待講演した．標数が p^2 のガロア環の差集合族を発見し、その構成法の一般化に取り組んでいる．
有限体の組合せ数学に関してもいくつか重要な結果，skew Hadamard 行列の非同値性に関する新しい知見、相対ガウス和を用いた Cayley graph，skew Hadamard 行列の構成、ガウス和を用いた 3class association scheme の構成、などを得た．

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　15 件）

(1) Mieko Yamada, Menon-Hadamard difference sets obtained from a local field by natural projections, Springer Proceedings in Mathematics and Statistics(Algebraic Design Theory and Hadamard Matrices)，査読有，(2015) 掲載決定．
URL:www.springer.com/series/10533
(2) T. Feng and Koji Momihara, Nonsymmetric primitive translation schemes of prime power order, Journal of Algebraic Combinatorics，査読有，41 (2015)，1-20，
DOI:1007/s10801-014-0523-8
(3)T. Feng, Koji Momihara, Q. Xiang, Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes，Combinatorica，査読有，(2015)，印刷中．
DOI:10.1007/s00493-014-2895-8
(4)T. Feng, Koji Momihara, Q. Xiang, Cameron-Liebler line classes with parameter x = q^2 − 1/2, Journal of Combinatorial Theory, Series A，査読有，133 (2015)，307-338．
DOI: 10.1016/j.jcta.2015.02.004
(5) Koji Momihara and Mieko Yamada, Divisible difference family from Galois rings GR(4, n) and Hadamard matrices, Designs, Codes and

Cryptography, 査読有, 73 (2014), 897-909
DOI:10.1007/s10623-013-9833-4

(6) Koji Momihara, Q. Xiang, Lifting constructions of strongly regular Cayley graphs, Finite Fields and their Applications, 査読有, 26 (2014), 86-99.
DOI:10.1016/j.ffa.2013.11.003

(7) 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

(8) Koji Momihara, Skew Hadamard difference sets from cyclotomic strongly regular graphs, SIAM Journal on Discrete Mathematics, 査読有, 27 (2013), 1112-1122.
DOI:10.1137/120888788

(9) T. Feng and Koji Momihara, Evaluation of the weight distribution of a class of cyclic codes based on index 2 Gauss sums, IEEE Transactions on Information Theory, 査読有, 59 (2013), 5980-5984
DOI: 10.1109/TIT.2013.2259538

(10) Koji Momihara, Inequivalence of skew Hadamard difference sets and triple intersection numbers modulo a prime, Electronic Journal of Combinatorics, 査読有, 20-P35 (2013), 1-19
URL: www.combinatorics.org

(11) Koji Momihara, Strongly regular Cayley graphs, skew Hadamard difference sets, and rationality of relative Gauss sums, European Journal of Combinatorics, 査読有, 34 (2013).
DOI:10.1016/j.ejc.2012.10.006

〔学会発表〕(計 21 件)

(1) 籾原幸二, 古典的な指標和とそれに関連する組合せ論, 第 11 回組合せ論若手研究集会, 2015 年 3 月 4-5 日, 慶應義塾大学（神奈川県・横浜市）

(2) 山田美枝子, 局所体の部分集合から得られるガロア環の差集合、第３１回代数的組合せ論シンポジウム、2014 年 6 月 19-20 日, 東北大学（宮城県・仙台市）

(3) Mieko Yamada, Menon-Hadamard difference sets obtained from a local field by natural projections, Workshop on Algebraic Design Theory and Hadamard Matrices 2014, 2014 年 7 月 8-11 日, Lethbridge(Canada)

(4) 山田美枝子, Menon-Hadamard difference sets obtained from a local field by natural projections, Workshop on Hadamard Matrices and Combinatorial Designs, 2014 年 10 月 31 日-11 月 1 日, 東北大学（宮城県・仙台市）

(5) 籾原幸二, Cyclotomic schemes and related problems, 代数的組合せ論「夏の学校 2014」, 2014 年 6 月 15-18 日, ホテルクレセント（宮城県・仙台市）

(6) 籾原幸二, Three-valued Gauss periods and related designs and association schemes, RIMS 研究集会「有限群とその表現、頂点作用素代数、代数的組合せ論の研究」, 2014 年 12 月 16-19 日、京都大学（京都府・京都市）

(7) Koji Momihara,Inequivalence of skew Hadamard difference sets, The 3rd Taiwan-Japan Conference on Combinatorics and its Applications, 2014 年 3 月 21 日, Chiayi(Taiwan)

(8) T. Minagawa and Mieko Yamada, A decoding algorithm of BCH codes over Galois rings, The 3rd Taiwan-Japan Conference on Combinatorics and its Applications, 2014 年 3 月 21 日, Chiayi(Taiwan)

(9) 籾原幸二, skew Hadamard difference set とその非同値性について, 離散数学とその応用研究集会, 2013 年 8 月 8 日, 山形保健センター（山形県・山形市）

(10) Koji Momihara, Lifting constructions of strongly regular graphs and association schemes in F_q, RIMS 研究集会「有限群とその表現、頂点作用素代数, 代数的組合せ論の研究」, 2013 年 1 月 8 日, 京都大学（京都府・京都市）

(11) Koji Momihara, Lifting construction of strongly regular Cayley graphs in F_q, The 2nd Japan-Taiwan Conference on Combinatorics and its Applications, 2012 年 11 月 12 日, 名古屋大学（愛知県・名古屋市）

(12) Koji Momihara, Strongly regular Cayley graphs and rationality of relative Gauss sums, Combinatirics 2012, 2012年9月14日、Perugia(Italy)

〔その他〕
ホームページ等
http://www.educ.kumamoto-u.ac.jp/~momihara (籾原幸二)

６．研究組織

(1)研究代表者
山田 美枝子 (YAMADA, Mieko)
東京女子大学・現代教養学部・研究員
研究者番号：70130226

(2)研究分担者
籾原 幸二 (MOMIHARA, Koji)
熊本大学・教育学部・講師
研究者番号： 70613305