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　　4 月　　4 日現在

機関番号：17401
研究種目：研究活動スタート支援
研究期間：　2011～2012
課題番号：23840032
研究課題名（和文）　差集合族とその拡張概念に基づくアダマール行列の新しい構成法の提案
研究課題名（英文）New constructions of Hadamard matrices based on difference families and their generalizations
研究代表者
籾原　幸二　（MOMIHARA　KOJI）
熊本大学・教育学部・講師
研究者番号：70613305

研究成果の概要（和文）：
本研究の目標は，情報通信や統計の分野に応用を持つ組合せ構造である「アダマール行列」の新たな構成法を提案することであった．先行研究において，差集合族と呼ばれる組合せ構造を用いたアダマール行列の構成法が提案されたが，その多くは有限体上のある差集合に起因するものであった．その構成法が他の環上に拡張できることに注目し，アダマール行列と差集合族に関する既存の理論を拡張・進展させることをテーマとして研究した．特に差集合族の概念の一般化を考えることで，ガロア環上での新たな差集合族の構成法を発見し，そこから新たなアダマール行列の構成法を得ることに成功した．また，強正則グラフやアダマール型差集合といった他の組合せ構造との関係性についても明らかにした．

研究成果の概要（英文）：
The objective of this research project is to propose new constructions of Hadamard matrices. Hadamard matrices have several applications in the research areas of Communications, Statistics, etc. In the past researches, several constructions of Hadamard matrices have been presented based on difference families, which were obtained from difference sets in finite fields. In our research, by generalizing the known constructions of difference families using difference sets in finite fields to those in commutative rings, we extended both of the theories of Hadamard matrices and difference families. In particular, by introducing a new concept generalizing ordinary difference families, we found a new infinite series of difference families in Galois rings and a new construction of Hadamard matrices using the new ones. Furthermore, we investigated the linkage between Hadamard matrices, Hadamard difference sets, and strongly regular graphs.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2011 年度	1,200,000	360,000	1,560,000
2012 年度	1,000,000	300,000	1,300,000
年度			
年度			
年度			
総　計	2,200,000	660,000	2,860,000

研究分野：数物系科学
科研費の分科・細目：数学一般(含確率論・統計数学)
キーワード：組合せ論・応用数学・組合せデザイン・アダマール行列・差集合族・差集合・強

正則グラフ・アダマール型差集合

１．研究開始当初の背景

研究代表者は，組合せデザイン論などの離散数学やその情報通信への応用について興味を持って研究を行ってきた．本研究対象であるアダマール行列は，情報通信や統計の分野など多方面に応用を持つ組合せ構造である．アダマール行列の存在性については，現在も尚，組合せ論において大きな未解決な問題の一つであるが，その問題を解決する上で，新たな構成法を提示することは重要な解決方法の一つである．一方，先行研究において，「差集合族」と呼ばれる組合せ構造を利用したアダマール行列の構成法が多数提案され，実際に多くの位数でアダマール行列を生成する手法・理論として発展している．ここで，差集合族については，有限群論や有限幾何学の応用的位置付けとして，存在・非存在や構成法に関する研究がなされてきた．また，BIB design といった組合せデザインや情報通信に利用される様々な系列を構成する手法として発展してきた．

これらアダマール行列と差集合族の二つの概念は，全く別の組合せ構造であるが，上述のように，密接な関係があることが知られている．特に Sekeres が 1969 年に与えた特殊な差集合族の構成法とその差集合を利用したアダマール行列の構成法に着目し，そこで用いた手法が一般化可能であるということを予想し，より多くの差集合族およびアダマール行列が得られることを目標とし研究に着手した．また，その他の組合せ構造との関係性，特にアダマール型の差集合や強正則グラフといった構造との関係性についても明らかにすることも重要なテーマとして研究を開始した．

２．研究の目的

Szekeres が得た差集合族からは新しいアダマール行列は得られず，実はそれらは平方剰余型差集合と呼ばれる組合せ構造から得られるアダマール行列のクラスと一致することが知られている．よって，Szekeres の差集合族と平方剰余型差集合の間に何らかの関係があると予想し，既に私が得た結果として，Szekeres の差集合族が，平方剰余型差集合からある変形(Szekeres の変形法と呼ぶ)によって得られることを示した．また，一般に，有限可換環の単数部分群が差集合をなすとき，Szekeres の変形法の一般化を適用することで，ある条件下で差集合族が得られるという新たな構成法を得ることに成功した．この結果を契機に，下記で与える問題が自然と浮かび，この研究課題の着想に至った．

研究当初に挙げた明らかにしたい事項・目的について述べる．

(1) アダマール行列を生成する差集合は平方剰余型差集合以外にも数多く知られている．私が得た Szekeres の変形法の一般化を利用した差集合族の構成法をそれらの差集合へ適用した場合，どのような差集合族が得られるのか? また，差集合族が得られない場合，どのような組合せ構造が得られ，どのように差集合族の概念を拡張すればよいか?

(2) アダマール行列を生成する差集合から得られた差集合族を用いてアダマール行列を構成する場合は，その逆の順序を辿れば十分である．しかし，Szekeres は，彼自身が例として与えた Szekeres の差集合族を大きく含んだ差集合族のクラスからアダマール行列が構成できることを示した．この類似として，(1)の差集合族を含む差集合族のクラスから，アダマール行列が得られるか? (つまり，真に新しいアダマール行列の構成法が得られるか?)

(3) Whiteman (1971)は Szekeres の差集合族には含まれない差集合族の構成法を与えることで，平方剰余型差集合からは得られない新しい位数のアダマール行列の無限系列を与えた．よって，(2)のアダマール行列の構成法のパラメータや条件を満たし，かつ，(1)の差集合族には含まれない差集合族が得られるか?

(4) 差集合族とアダマール行列に関する理論を，他の組合せ構造(例えば，あだーる型差集合や強正則グラフ，アソシエーションスキームなど)との関係性も含めて拡張し，関係性をより明らかにできるか？.

これらの４つの問を解決することを研究目的とした．

３．研究の方法

研究は，以下の順序で実施した．

(1) 私が既に得た Szekeres の変形法の一般化を適用させる対象の差集合を，特に Yamamoto-Yamada (1988)が得たガロア環上の差集合に制限し，研究を行った．Yamamoto-Yamada が得た差集合は，標数 4 のガロア環の加法群上で，指数 2 の単数部分群からなり，有限体上の平方剰余型差集合の類似と言えるため，この差集合に我々の Szekeres の変形法の一般化を適用するのは，自然であると思われた．まずは，計算機を援用し，小さな位数でどのような差集合族が得られているかを確認し，その構造を明らかにしていくという研究方法を取った．

(2) (1)の研究に基づき，新たな差集合族の概念を定義し，その存在性を証明するという流れで研究を行った．

(3) (2)の新たな差集合族の概念を利用したアダマール行列の構成法を，(1)の逆を辿り，さらにそれを一般化し，新たな構成法を与えるという流れで研究を行った．

(4) 上記の(1),(2),(3)の研究方法をより標数の高いガロア環から得られる差集合に適用し，手法・結果の拡張を試みた．特に，証明に利用する手法は，標数 4 の場合の証明とは全く異なる手法を導入しなければならないと予想される．特に，研究協力者である山田美枝子教授(金沢大学)と研究打ち合わせを数回行い，ガロア環上のガウス和やヤコビ和といった指標和の計算が必要であるということが明らかとなり，ガロア環上の指標の計算についての研究を行った．

(5) 強正則グラフ・アダマール型差集合・アソシエーションスキームといった他の組合せ構造の新たな構成問題に取り組んだ．また，アダマール行列も含んだ，これらの組合せ構造間の関係性について研究を行った．特に，計算機を用いてどのような強正則グラフからアダマール型差集合やアダマール行列が得られるかについて調べ，研究を行った．

４．研究成果

平成 23 年度から平成 24 年度の 2 年間に以下のような研究成果を得た．

(1) 研究当初に既に得られていたSzekeresの差集合族の構成法の一般化を，Yamamoto-Yamadaの標数4のガロア環上の差集合に適用した場合，どのような組合せ構造(差集合族)が得られるかを計算機を援用しながら調べ，予想していた通り差集合族の概念を一般化させた構造であるグループ分割型差集合を成すことを証明することに成功した．この結果は，新たなパラメータを持つグループ分割型差集合族の無限系列が得られるという点で重要である．

(2) Yamamoto-Yamadaの差集合はアダマール型と呼ばれ，直ちにアダマール行列が構成できることが知られている．このことに注意し，我々の得たグループ分割型差集合族の構成法の逆をたどることで，差集合族の存在性を仮定したアダマール行列の構成法が得られた．ただし，パラメータを一般化することができ，これによって，「新しいアダマール行列の構成法を提示する」という研究目標を達成できた．この研究に関する結果について，現在金沢大学の山田美枝子教授と共同で論文を執筆し国際学術誌へ投降した．

(3) Zhejian大学(中華人民共和国)のFeng准教授，Delaware大学(アメリカ合衆国)のXiang教授との共同研究で，アダマール行列を生成するアダマール型差集合と呼ばれる差集合の構成法の提案を行った．特に，skewと呼ばれる特別な構造を持つものについて研究を行った．skewアダマール型差集合は，つい最近まで，数十年の間平方剰余型差集合という特別なものしか知られていなかったが，今回の我々の研究で，その平方剰余型差集合とは非同型のskewアダマール型差集合を発見し，新たなアダマール行列の構成法を得た．この結果は，計算機の援用と有限体上のガウス和と呼ばれる指標和の計算に基づいており，代数的整数論の視点からも興味深い結果であると言える.この結果についても，Feng氏とXiang氏との共同で論文を執筆し，国際学術誌へ投降した．

(4) アダマール行列の構成問題と密接な関係を持つ強正則グラフと呼ばれる組合せ構造について研究を行った．特に有限体の相対ガウス和と呼ばれる指標和の計算を行い，有限体上の強正則グラフの新たな構成法を与えることに成功した．特に，条件を満たす良い強正則グラフが一つあればそこから無限系列が得られるという再帰的構成法を与えた．また，強正則グラフとskewア

ダマール型差集合との関係についても計算機を用いて調べた．特に，特別なパラメータで強正則グラフとskewアダマール型差集合の存在性が一致していることを示した．この結果は，単著で論文を作成し既にEuropean Journal of Combinatoricsという国際学術誌に掲載された．

本研究における研究成果は概ね当初の予定通りの成果を得られたと考えている．
特に標数４のガロア環から差集合族の概念の一般化であるグループ分割型差集合族が得られ，またそこから新たなアダマール行列の構成法が得られたことは，研究当初予想していた通りの結果が得られたという点で，この研究目的は十分達せられたと考えられる．また，関連する研究として，アダマール型差集合や強正則グラフの新たな構成法を提示し，また，それらの間の相互関係やアダマール行列との関係を部分的ではあるが明らかにできたことは，予想以上の成果であったと言えるだろう．

今後の研究課題:
より高い標数のガロア環からどのような差集合族が得られ，また，アダマール行列がどのように構成できるかについては，いくつか興味深い例が計算機によって発見されたものの一般的な証明はできなかった．この問題は今後の重要な研究課題である．また，アダマール型差集合や強正則グラフの新たな構成法を提案することに成功したが，それらの相互関係は計算機を用いて部分的に明らかにしたのみであったので，理論的な裏付けを得ることも今後の研究課題である．

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　４件）
① Koji Momihara、Strongly regular Cayley graphs, skew Hadamard difference sets, and rationality of relative Gauss sums、European Journal of Combinatorics、査読有、34巻、2013、18頁
②Tao Feng、Koji Momihara、Three-class association schemes from cyclotomy、Journal of Combinatorial Theory, Series A、査読有、120巻、2013、14頁
③Koji Momihara、Miwako Mishima、Masakazu Jimbo、A decomposition of the 2-design formed by the planes in AG(2n,3)、Finite Fields and Their Applications、査読有、18巻、2012、956－970
④　籾原幸二、Tao Feng、Qing Xiang、Amorphous association scheme に関するIvanov予想の反例の一般化、応用数学合同研究集会報告集、査読無、2011、66－67

〔学会発表〕（計　８件）
① 籾原幸二、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)
② Koji Momihara、Strongly regular Cayley graphs and rationality of relative Gauss sums、Combinatorics 2012、2012年9月14日、Hotel Gio(イタリア・ペルージャ)
③籾原幸二、強正則グラフCay(F_q,D)と相対ガウス和の有理性について、RIMS 研究集会「デザイン、符号、グラフおよびその周辺」、2012年7月19日、京都大学(京都)
④籾原幸二、Recent progress on cyclotomic strongly regular graphs and skew Hadamard difference sets、研究集会「有限体とそれに関連する代数的組合せ論」、2012年3月3日、神戸学院大学(兵庫)
⑤ 籾原幸二、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」、2012年1月8日、京都大学(京都)
⑥ 籾原幸二、Lifting constructions of strongly regular Cayley graphs、研究集会「代数的グラフ理論、スペクトラルグラフ理論および周辺領域」、2012年1月6日、名古屋大学(愛知)
⑦　籾原幸二、Tao Feng、Qing Xiang、2011年度応用数学合同研究集会、2011年12月16日、龍谷大学(滋賀)
⑧　籾原幸二、Supplementary divisible difference sets over Galois rings of characteristic 4 from generalized Szekeres’s construction、日本数学会秋季総合分科会応用数学分科会、2011年9月29日、信州大学(長野)

〔その他〕
ホームページ等
http://combin-math-kumamoto.jp/
http://www.educ.kumamoto-u.ac.jp/~momihara/

６．研究組織

(1)研究代表者

籾原　幸二（MOMIHARA KOJI）
熊本大学・教育学部・講師
研究者番号：70613305

(2)研究協力者

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