

令和 2 年 4 月 6 日現在

機関番号：17401

研究種目：若手研究(B)

研究期間：2017～2019

課題番号：17K14236

研究課題名(和文)有限幾何と代数的手法に基づく有限体上のデザイン・グラフ・符号の新たな構成法の提案

研究課題名(英文) New constructions of designs, graphs and codes over finite fields based on finite geometry and algebraic methods

研究代表者

梶原 幸二 (Momihara, Koji)

熊本大学・大学院先端科学研究部(理)・准教授

研究者番号：70613305

交付決定額(研究期間全体)：(直接経費) 2,100,000円

研究成果の概要(和文)：先行研究において、次元の小さな有限幾何構造や有限体上の指数の小さな乗法部分群の構造を利用した有限体上のデザイン・グラフ・符号構成法が提案されたが、超平面交差数やガウス和の計算困難性から得られる構造のクラスが制限されてきた。本研究では、有限群の作用と有限体の拡大の性質を利用した高次元有限幾何構造を扱う手法や高い指数の円分数を計算する手法を開発した。特に、既存の歪アダマール差集合とは非同型な差集合の構成、新たなパラメータでの歪アダマール差集合族の構成、新たな次数のアダマール行列の構成、3値のガウス周期に基づく強正則グラフの構成を行い、既存の構成理論を一般化することができた。

研究成果の学術的意義や社会的意義

デザイン・グラフ・符号はそれぞれ、統計学・ネットワーク・情報通信に応用され、我々の日常生活の背後にある重要な離散構造である。一方、その存在性に関しては、未解決な部分が多く組合せ論における重要な研究課題である。特に、本研究は、有限体上の差集合・強正則グラフ・Griesmer符号と呼ばれるデザイン・グラフ・符号について、有限幾何・整数論・群論的手法を組み合わせた新手法を考案し、多くのパラメータで存在性が未知であった上記組合せ構造の存在性の解明を行った。

研究成果の概要(英文)：In past researches, some constructions for combinatorial objects such as designs, graphs and codes have been presented based on finite geometry of small dimension and cyclotomy of small index over finite fields. However, because of the difficulty of computations of the size of hyperplane sections and Gauss sums, the classes of such objects found before has been limited. In this research, we found new approaches to treat geometric objects of large dimension and compute Gauss sums of large index using a combination of actions of finite groups and field extensions. In particular, we succeeded to give new families of skew Hadamard difference sets inequivalent to known ones, skew Hadamard difference families with new parameters, Hadamard matrices of new order, and new strongly regular graphs based on three-valued Gauss periods. Thus, we generalized known construction theories for designs, graphs and codes over finite fields.

研究分野：離散数学, 組合せ論

キーワード：差集合 強正則グラフ Griesmer符号 アダマール行列 アソシエーションスキーム 有限幾何 ガウス周期

科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属されます。

1. 研究開始当初の背景

差集合・強正則グラフ・Griesmer 符号の問題は、組合せ論、特にデザイン論・グラフ理論・符号理論における主要な研究テーマであるが、異分野であるため独立に研究がなされてきた。一方、有限体上で定義されるものに限れば、どれも『有限体から「良い」部分集合を選ぶ』問題に帰着される。また、実際にそれらの構造をなすかどうかは、その部分集合の群の指標値で判定でき、この計算が本質的である。これら有限体上の組合せ構造を、システマチックに扱う手法として、有限体の乗法部分群の剰余類(円分類と呼ぶ)を用いる手法が知られている。うまく部分群と剰余類を選ぶ必要があり、部分群の指数が小さい場合は総当たりでチェックできることから、計算機との相性が良く、例の構成によく用いられてきた。一方、理論的に指標値を計算する際、ガウス和と呼ばれる指標和の計算が必要となる。しかし、部分群の指数が大きくなると、ガウス和の明示的な計算は困難である。この整数論的な計算困難性から、得られる組合せ構造のクラスが制限されてきたという背景がある。

一方、有限体上の強正則グラフは、1980 年以降有限幾何の分野でも研究されてきた。特に、 m -ovoid と呼ばれる幾何構造が、ある条件下で強正則グラフを与えることが示された。これは有限射影空間の点集合であり、その基礎にある線形空間(有限体)の部分集合として、強正則ケーリーグラフが得られる。この構造に対する既存の構成法として、ある幾何構造に付随した大きな位数の群の、点上への作用による軌道を選ぶことで部分集合をつくるという、幾何構造と有限群を組み合わせたデザイン論で用いられてきた古典的手法がある。しかし、この手法は、作用する群の位数が相対的に大きい場合にのみ有用であり、位数が小さい場合には、軌道数が膨大になり一般化が困難であるという問題点がある。また、上記の指標和を用いる整数論を基礎にした研究とは独立に研究され、相互間研究も全くない状況であった。

一方、研究代表者は、J. Bamberg 氏、M. Lee 氏、Q. Xiang 氏と 5 次元射影空間における hemisystem と呼ばれる幾何構造の存在を調べていたが(論文)、その研究で幾何構造への有限群の作用と有限体の円分類を組み合わせる手法を導入し、部分的に成果を得ることができた。そのため、この研究手法を、差集合・強正則グラフ・Griesmer 符号にも応用できるはずであると考え、研究の着想に至った。

2. 研究の目的

研究背景で述べた、有限幾何における hemisystem の存在問題の研究で、部分的に成功した群の作用と有限体の円分類を組み合わせる手法を一般化することで、理論を整備し、既存の差集合・強正則グラフ・Griesmer 符号の新たな構成手法提案することを大きな目的とした。特に、以下の事項について明らかにすることを目標とした。

(1) 有限幾何と円分類を用いて解釈できる、有限体上の歪アダマール差集合・強正則グラフを、計算機を用いて数多く発見する。その際、集合のサイズの大きな例に対する群の作用と指標和の計算に基づく探索アルゴリズムと全自己同型群の理論的計算法について明らかにする。

(2) 先行研究と事前の計算機実験で発見されている m -ovoid および有限体上の強正則グラフの例に対し、背後にある幾何構造・アソシエーションスキーム・群の作用の仕方、さらに、指標値の計算手法・公式についてすべて明らかにする。特に、それらの無限系列への一般化を行い、存在性を明らかにする。

(3) 有限幾何と円分類を組み合わせる手法を有限体上の歪アダマール差集合族や対称アダマール差集合族に対し展開する。これらの差集合族は、歪アダマール行列や対称アダマール行列と呼ばれる、極めて条件の強いデザインのクラスに対応し、いまだ存在性が未解決である。これらの組合せデザインについても、(1)と(2)の同様の流れで研究を行い、新たな構成法の提案を試みる。

(4) 先行研究では、ある条件下で有限極空間上の m -ovoid が、対応する有限体上で強正則グラフを与えることが示された([Bamberg et al. 2007])。その条件を排除した際に、どのような場合にアソシエーションスキームが得られるかという自然な問が生じるが、その問題は未だ解明されていない。この問について明らかにし、また、(1),(2)と同様の流れで、アソシエーションスキームに対しても新たな構成法の提案を試みる。

(5) Griesmer 限界と呼ばれる符号長に関する下限界式の等号を満たす符号を, Griesmer 符号と呼ぶ. この符号は, その存在条件を有限幾何の言葉で記述でき, 符号理論と有限幾何の双方において盛んに研究されてきた. しかし, 小さな自己同型群をもつ符号(幾何構造)を理論的な枠組みで扱う手法がないため, 大部分が未解決のまま残されている. そこで, 有限幾何と円分群を用いる手法から新しい Griesmer 符号が得られるかという問が生じる. この問について明らかにし, 新たな構成法の提案を試みる.

3. 研究の方法

以下の項目について研究を実施した.

(1) 小さな位数の有限体上の比較的小さい巡回群を自己同型群にもつ, 強正則グラフと差集合の例を計算機を用いて発見する. 特に, 一般化を視野に入れ, グラフや差集合の位数の平方根と小さな巡回群の積程度の位数の自己同型群が作用する例を発見する. 方法としては, Tactical 分解と呼ばれる幾何構造の軌道分解の方法を利用した, 超平面交差数の計算アルゴリズムを応用し, プログラム開発を行った.

(2) (1)の研究で得られた強正則グラフと差集合の例について, パラメータに規則性のあるものに制限し, その理論的な指標値の計算を試みた. また, 指標値の計算を行う際に, その背後にある幾何構造およびアソシエーションスキームの構造の特定を行った. 最終的に, 既存の有限体上の強正則グラフや差集合の例の無限系列化を試みた.

(3) (1), (2)の研究の流れを, 歪アダマール差集合族および対称アダマール差集合へ応用し, 新たなパラメータの差集合族や既存のものと非同値な差集合族の構成を試みた. また, 得られた研究結果について, 群に関する構造を抜き, 代わりにアソシエーションスキームの構造を利用するという手法を考案して, 差集合や差集合族から得られるものだけでなく, 一般のアダマール行列への構成法の一般化を試みた.

(4) Schmidt-White (2003)によって, 2 値のガウス周期をとる指数の有限体の乗法部分群を用いた強正則グラフの研究がなされてきた. 一般に, 3 値のガウス周期をとる場合は, アソシエーションスキームに対応するが, 3 値のガウス周期の特別な場合に強正則グラフヘクラスが持ち上がることを例で見出した. この現象を一般化することで, 新たな強正則グラフおよびアソシエーションスキームの構成に取り組んだ.

(5) (1), (2)の研究の流れを有限体上の多重集合へ適用させ, 超平面交差数が計算可能かつ特定の限界式(Griesmer 限界)を満たすものの発見を試みた. これにより, 新たな Griesmer 符号の構成を試みた.

4. 研究成果

2017 年度から 2019 年度の 3 年間に以下の研究成果を得た.

(1) 5次元の有限射影空間において, 比較的小さな巡回群が作用するhemisystemと呼ばれる幾何構造を発見した. 特に, 有限群の作用と有限体の4乗剰余の性質を組み合わせることで, 既存のものとは非同型なものを無限個含む系列の存在性を証明した. この結果は, 20年以上有限幾何の分野で未解決問題とされてきたものであり, 本研究手法が真に新しく有用なものであることを意味する研究成果である. この結果は, Combinatoricaという国際学術誌へ共著(Bamberg氏, Lee氏, Xiang氏)で論文を投稿し採択された.

(2) 研究手法(1)における計算機を用いた手法を, Schmidt-White (2003)が発見した2値のガウス周期をとる11個の散在的な例が存在する場合に実装し, 既存の強正則グラフを分解することで, 新たなパラメータを持つ強正則グラフの例を発見することに成功した. 特に, 位数は2の100乗程度の強正則グラフを含むため, 計算機での単なる総当たりでは決して得られない研究成果である. この結果は, Finite Fields and Their Applicationsという国際学術誌へ共著(Xiang氏)で論文を投稿し採択された.

(3) 研究手法(4)から, 既存の2値のガウス周期を用いた強正則グラフの構成法を3値のガウス周期の特別な場合にも拡張できることを示した. これにより, 強正則グラフの非常に大きな無限系列を与えることに成功した. この結果は, (1)の研究成果を包含する結果であり, 本研究の

研究手法が強正則グラフの分野にも有用であることを確証する研究成果である。この結果は、European Journal of Combinatoricsという国際学術誌へ単著で論文を投稿し採択された。また、いつ3値のガウス周期を取りうるのか、また、強正則グラフをなす場合の位数の密度についての問題が残されたが、最近Xiang氏と共同で研究を進め、どの程度その構成法が適用できるかについて完全解決をすることができた。この結果については、現在Xiang氏とともに論文を執筆中である。

(4) 有限体の乗法部分群とその剰余類を用いて、歪アダマール差集合族を構成する手法が古くから知られている(Szekeres, 1969)。しかし、その証明には、ガウス和の計算が必要であるため、扱われた乗法部分群の指数は非常に小さなものであった。一方、代表者らは、有限体の拡大とそれに伴うガウス和の計算手法(Hasse-Davenportの定理等)を応用して、一般の2のべきを指数にもつガウス和の計算手法を考案し、Szekeres以降未解決であったある歪アダマール差集合族の存在性を証明することに成功した。これにより、新たな次数の歪対称アダマール行列の存在性を示した。この結果は、European Journal of Combinatoricsへ共著(Xiang氏)で論文を投稿し採択された。

(5) Xiang-Wilson (1997)は、対称アダマール行列を生成する対称アダマール差集合について小さな位数で計算機を用いて発見した。その後、Chen(1997)によって、対称アダマール差集合の存在性は解決したが、Xiang-Wilsonが発見したものは、非同値なものであった。一方、Xiang-Wilsonの例が無限系列に一般化できるかどうかは、未解決問題として残されていた。代表者らは、研究手法(2)を応用して、Xiang-Wilsonの散在的例を無限系列へ一般化することに成功した。この結果は、Finite Fields and Their Applicationsへ共著(Xiang氏)で論文を投稿し採択された。

(6) 良いグラフ分解であるアソシエーションスキームが、Chen(1997)の対称アダマール行列に付随することを発見した。特に、そのアソシエーションスキームの隣接行列を用いて、アダマール行列を分解し、Chenのアダマール行列を2倍、3倍に拡大することができることを示した。これにより、新たな次数のアダマール行列の大きな無限系列を構成した。この結果は、Journal of Combinatorial Theory, Series Aという国際学術誌へ共著(Leung氏)で論文を投稿し採択された。

(7) 強正則グラフに含まれるクリークやコクリークの大きさについて、有名なホフマン(またはデルサルテ)の限界式が知られている。一方、代表者らは、歪対称アダマール行列の特徴づけとして、歪対称アダマール行列から得られる2重正則トーナメントに含まれる推移的トーナメントの大きさについて、ホフマン限界の類似としての限界式を得ることができた。この結果は、Integersという国際学術誌へ共著(須田氏)で論文を投稿し採択された。

(8) 有限体の素数べき位数の巡回群への一般化であるガロア環上の差集合族について、既存有限体上の乗法部分群とその剰余類を用いた構成法を一般化する形で与え、差集合族の新たな無限系列を与えることに成功した。この結果は、Electronic Journal of Combinatoricsという国際学術誌へ単著で論文を投稿し採択された。

(9) Griesmer符号に関しては、tight setと呼ばれる幾何構造の分解から超平面交差数が計算可能な有限体の多重部分集合を構成することに成功し、新たな3または4種の重み分布を持つ符号を構成することができた。しかし、完全には、Griesmer限界式を満たすものは得られなかった。この研究成果については、tight setの論文として、現在Feng氏、Rodjers氏、Xiang氏、Zou氏とともに論文を執筆し、現在投稿中である。

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、有限群の作用と有限体の乗法部分群の剰余類らを併せて用いる手法を整備し、差集合や強正則グラフへ適用し、これまで知られていなかった無限系列を大量に発見できたことは、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、この研究目的は達せられたと考えられる。特に、新たな位数でアダマール行列の存在性を証明できたことは、近年アダマール行列の研究に停滞感がある状況であるように思われるので、他の研究者へのインパクトは大きいものと思われる。今後も研究の推進も期待されるところである。また、古くから未解決とされた組合せ論における未解決問題を数多く解くことができたという点は予想以上の成果であったと言えるだろう。一方、Griesmer符号の存在性については、今後も改良の余地が見込まれるので、継続して研究を行う予定である。

5. 主な発表論文等

〔雑誌論文〕 計8件（うち査読付論文 7件/うち国際共著 7件/うちオープンアクセス 0件）

1. 著者名 Koji Momihara, Qing Xiang	4. 巻 76
2. 論文標題 Constructions of skew Hadamard difference families	5. 発行年 2019年
3. 雑誌名 European Journal of Combinatorics	6. 最初と最後の頁 73--81
掲載論文のDOI (デジタルオブジェクト識別子) 10.1016/j.ejc.2018.09.007	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する
1. 著者名 Koji Momihara, Qi Wang, Qing Xiang	4. 巻 印刷中
2. 論文標題 Cyclotomy, difference sets, sequences with low correlation, strongly regular graphs, and related geometric substructures	5. 発行年 2019年
3. 雑誌名 Combinatorics and Finite Fields. Difference Sets, Polynomials, Pseudorandomness and Applications	6. 最初と最後の頁 印刷中
掲載論文のDOI (デジタルオブジェクト識別子) 10.1515/9783110642094-009	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する
1. 著者名 John Bamberg, Melissa Lee, Koji Momihara, Qing Xiang	4. 巻 38
2. 論文標題 A new infinite family of hemisystems of the Hermitian surfaces	5. 発行年 2018年
3. 雑誌名 Combinatorica	6. 最初と最後の頁 44-66
掲載論文のDOI (デジタルオブジェクト識別子) 10.1017/s00493-016-3525-4	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する
1. 著者名 Koji Momihara, Qing Xiang	4. 巻 50
2. 論文標題 Strongly regular Cayley graphs from partitions of subdifference sets of the Singer difference sets	5. 発行年 2018年
3. 雑誌名 Finite Fields and Their Applications	6. 最初と最後の頁 222-250
掲載論文のDOI (デジタルオブジェクト識別子) 10.1016/j.ffa.207.11.010	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1. 著者名 Koji Momihara	4. 巻 70
2. 論文標題 Construction of strongly regular Cayley graphs based on three-valued Gauss periods	5. 発行年 2018年
3. 雑誌名 European Journal of Combinatorics	6. 最初と最後の頁 232-250
掲載論文のDOI (デジタルオブジェクト識別子) 10.1006/j.ejc.2018.01.007	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1. 著者名 初原幸二	4. 巻 36
2. 論文標題 A large family of strongly regular Cayley graphs	5. 発行年 2020年
3. 雑誌名 第36回代数的組合せ論シンポジウム報告集	6. 最初と最後の頁 -
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 Koji Momihara, Qing Xiang	4. 巻 61
2. 論文標題 Generalized constructions of Menon-Hadamard difference sets	5. 発行年 2020年
3. 雑誌名 Finite Fields and Their Applications	6. 最初と最後の頁 -
掲載論文のDOI (デジタルオブジェクト識別子) 10.1016/j.ffa.2019.101601	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1. 著者名 Ka Hin Leung, Koji Momihara	4. 巻 171
2. 論文標題 New constructions of Hadamard matrices	5. 発行年 2020年
3. 雑誌名 Journal of Combinatorial Theory, Series A	6. 最初と最後の頁 -
掲載論文のDOI (デジタルオブジェクト識別子) 10.1016/j.jcta.2019.105160	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

〔学会発表〕 計12件（うち招待講演 2件 / うち国際学会 4件）

1. 発表者名 初原幸二
2. 発表標題 Skew Hadamard 行列の存在性に関するG. Szekeres の主張の修正について
3. 学会等名 研究集会「離散数学とその応用研究集会2018」
4. 発表年 2018年

1. 発表者名 初原幸二
2. 発表標題 Skew Hadamard 行列の存在性に関するG. Szekeres の主張の修正について
3. 学会等名 研究集会「実験計画法ならびに情報数理論と 関連する組合せ構造2018」
4. 発表年 2018年

1. 発表者名 Koji Momihara
2. 発表標題 Transformation of Hadamard matrices into regular or almost regular Hadamard matrices
3. 学会等名 Workshop on difference sets at Zhejiang University (国際学会)
4. 発表年 2018年

1. 発表者名 Koji Momihara
2. 発表標題 On Hadamard matrices with maximum excess
3. 学会等名 Hadamard Matrices and Their Applications (国際学会)
4. 発表年 2018年

1. 発表者名 Koji Momihara
2. 発表標題 Switching for Hadamard Matrices -A new approach to the excess problem-
3. 学会等名 The 5th Taiwan-Japan Conference on Combinatorics and its Applications (招待講演) (国際学会)
4. 発表年 2018年

1. 発表者名 Koji Momihara
2. 発表標題 Three-valued Gauss periods and related strongly regular Cayley graphs
3. 学会等名 Hakata Workshop; Summer Meeting 2017
4. 発表年 2017年

1. 発表者名 Koji Momihara
2. 発表標題 Strongly regular Cayley graphs from three-valued Gauss periods
3. 学会等名 Japanese Conference on Combinatorics and its Applications
4. 発表年 2017年

1. 発表者名 Koji Momihara
2. 発表標題 On regular or biregular Hadamard matrices
3. 学会等名 研究集会「実験計画法と符号および関連する組合せ構造」
4. 発表年 2017年

1. 発表者名 Koji Momihara
2. 発表標題 Construction of strongly regular Cayley graphs based on three-valued Gauss periods
3. 学会等名 RIMS研究集会「代数的組合せ論および有限群・頂点作用素代数とその表現の研究」
4. 発表年 2017年

1. 発表者名 初原幸二
2. 発表標題 A big family of strongly regular graphs from three-valued Gauss periods
3. 学会等名 第36回代数的組合せ論シンポジウム
4. 発表年 2019年

1. 発表者名 Koji Momihara
2. 発表標題 A large family of strongly regular Cayley graphs from three-valued Gauss periods
3. 学会等名 Finite Geometry and Extremal Combinatorics (招待講演) (国際学会)
4. 発表年 2019年

1. 発表者名 初原幸二
2. 発表標題 A recursion on skew Hadamard difference sets
3. 学会等名 研究集会「実験計画法と符号および関連する組合せ構造2019」
4. 発表年 2019年

〔図書〕 計0件

〔産業財産権〕

〔その他〕

Homepage of Koji Momihara
<https://www.educ.kumamoto-u.ac.jp/~momihara/researchmap>
<https://researchmap.jp/7000016996/>

6. 研究組織

	氏名 (ローマ字氏名) (研究者番号)	所属研究機関・部局・職 (機関番号)	備考
研究協力者	丸田 辰也 (Maruta Tatsuya)		
研究協力者	宮本 暢子 (Miyamoto Nobuko)		