様　式　Ｆ－１９－２

科学研究費助成事業　　研究成果報告書

令和　　３ 年　　６ 月　　４ 日現在

機関番号：１７４０１
研究種目：国際共同研究加速基金（国際共同研究強化）
研究期間：2017～2020
課題番号：１６ＫＫ０１０３

研究課題名（和文）マトロイドの表現・被覆問題への符号理論的アプローチ（国際共同研究強化）

研究課題名（英文）Coding Theoretical Approach to the Representation and Covering Problems for Matroids(Fostering Joint International Research)

研究代表者
城本　啓介（Shiromoto, Keisuke）

熊本大学・大学院先端科学研究部（工）・教授

研究者番号：００３４３６６６

交付決定額（研究期間全体）：（直接経費）　　8,600,000円
渡航期間：　　８ヶ月

研究成果の概要（和文）：　本国際共同研究においては，基課題となる代数的符号理論の研究課題のうち，マトロイドと関連した研究に焦点を絞り，それぞれを発展課題へと進展させることで，主に以下の成果を得ることができた．(1) 弱アフィン符号の関連符号であるパワフル集合について，公理化や双対パワフル集合の導入および拡張構成をもとにして，非線形符号の構成をおこなった．(2) マトロイドの最小被覆数の上限界式およびその等号が成立するマトロイドの構成をおこなった．

研究成果の学術的意義や社会的意義
　符号理論とは，デジタル情報を伝送または記録する際に生じる誤りを理論的に訂正するための誤り訂正符号の理論であり，その代数構造に着目して数理的研究をおこなうことが代数的符号理論である．本国際共同研究において得られた研究成果については，主に誤り訂正能力の高い非線形符号の構成法や秘密分散共有法や暗号理論等の情報セキュリティ分野において情報の秘匿化に有用なマトロイドの構成法を提案することで，今後の高度情報化社会におけるIoTやデータサイエンス分野への貢献が期待される．

研究成果の概要（英文）：In this fostering joint international research project, we focused on some matroid problems in our based research project on algebraic coding theory and then we mainly had the following results: (1) We gave some constructions of non-linear codes from powerful sets. (2) We derived an upper bound on covering numbers of matroids and we gave some constructions of matroids which attain the bound.

研究分野：代数的符号理論

キーワード：符号理論　マトロイド　組合せ論　非線形符号　最小被覆数

１．研究開始当初の背景

数学の諸分野において，ある数学的特性をもつ構造が存在するか否かを考察する存在問題，また存在する場合には，どのようにしてその対象を構成するかという構成法についての研究がある．符号理論・マトロイド理論においても同様で，主に以下のような研究がある．

(1) 符号理論における存在問題・構成法

符号理論とは，デジタル情報を伝送または記録する際に生じる誤りを理論的に訂正するための誤り訂正符号の理論であり，その代数構造に着目して数理的研究をおこなうことが代数的符号理論である．有限体（有限環）上の（線形）符号とは，有限体上のベクトル空間の部分空間（有限環上の自由加群の部分加群）のことである．

代表的な存在問題・構成法の研究としては，与えられたパラメータ（符号長，次元，最小重み，重み分布，一般化重み等）をもつ符号の存在・非存在を考察するために，各パラメータに関する限界式の導出およびその等号を満たす最適な符号の存在性の検討・構成法の提案(例:Shiromoto, et al. (’99, … ,’09) 等）や自己双対性や巡回性のような特殊な数理構造をもつ符号族について，自己同型群や重み多項式などを用いた存在条件・分類問題の考察（例：Shiromoto (’96, ’99) 等）あるいは最適な符号族に関する多項式的特徴付け（例：Shiromoto (’06), Britz-Shiromoto, et al. (’07) 等）などがある．

(2) マトロイド理論における存在問題・構成法

マトロイドとは，ベクトルの１次独立・従属の概念を公理化し，有限集合上に拡張した組合せ構造である．純粋な構造研究のみならず，組合せ最適化問題やその他の工学分野等への応用研究が積極的に展開されている．主な種類として，グラフの木構造から得られるグラフ的マトロイドや代数的閉体から得られる代数的マトロイド，有限体上の行列から得られる表現マトロイドなどがある．特にグラフ理論との関係は深く，マトロイド理論の創成に貢献した W. T. Tutte は次のように記している．

『*It has been said that to get a theorem on matroids we should take a known one on graphs, rewrite it and its proof so as to make no mention of vertices, and then replace the word “graph” by “matroid”.*』

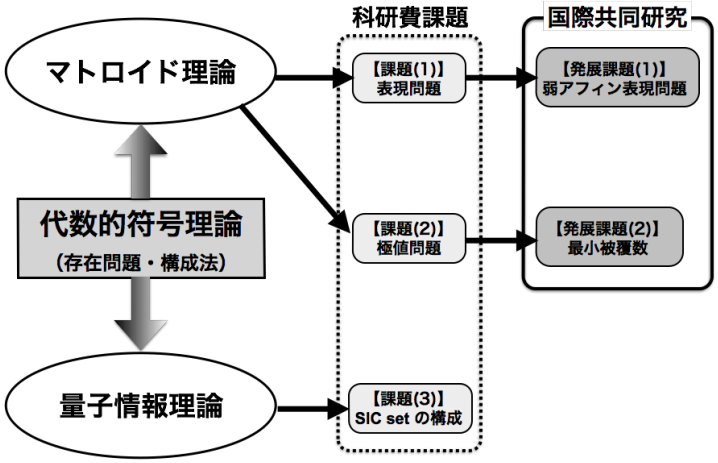
主な古典的問題として，与えられたマトロイドがどの体上の表現マトロイドか（表現問題），与えられたパラメータや数理構造をもつマトロイドの存在・分類問題などが考えられている．

２．研究の目的

研究開始当時採択されていた科研費では，自身の代数的符号理論におけるこれまでの研究（与えられたパラメータや数理構造をもつ符号の存在問題および構成法の研究）を土台にして，マトロイド理論と量子情報理論の２分野における同種の問題を新たに符号理論的な視点から研究し，異なる分野間における統一的構造の理解をより深めることを目的としていた．具体的な研究課題は，**【課題(1)】マトロイドマイナーの符号理論的考察**，**【課題(2)】マトロイドの臨界指数（critical exponent）に関する極値問題**，**【課題(3)】量子情報理論における SIC set の理論的（系統的）構成法の提案**，の３つであった．そこで，本研究では，これらの研究課題のうち，それまでの進捗状況と研究内容を踏まえて，マトロイドと関連した研究に焦点を絞り（【課題(1)】と【課題(2)】），それぞれを発展課題へと進展させることで国際共同研究を実施することとした．具体的な研究目的は以下の通りであった．

【発展課題(1)】マトロイドの弱アフィン表現問題の考察

弱アフィン符号とは有限集合上で定義された均一座標性のみをもつ非線形符号であり，有限体上の線形符号の一般化と見なすことができる．この符号は Ashikhimin, et al. (’03) によって導入され，符号自体の構造解析以外にもマトロイドや秘密分散システムの構成への応用に関する結果が知られている．本課題においては，【課題(1)】において考察しているマトロイドの表現問題を，与えられたマトロイドが弱アフィン符号から構成可能かどうかの構成判定問題へと進展させ，



これまで用いた符号理論における手法を一般のマトロイドへ拡張すること（マトロイド的符号理論の構築）で，(1)マトロイド的重み多項式の因子関係及び(2)フラットの階層構造の関係を明確した上で禁止マイナーを用いた判定条件を導く．

【発展課題(2)】マトロイドの最小被覆数に関する符号理論的考察

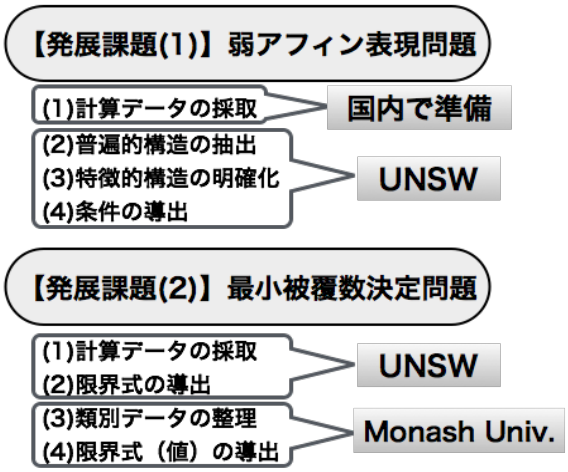
マトロイドの最小被覆数とは，基集合を被覆可能なコサーキットの最小個数のことであり，【課題(2)】において考察している表現マトロイドの臨界指数の概念のある種の拡張と考えることが

できる．従って，その決定問題は前述の古典的問題である極値問題の一般化と考えることができる．それにも関わらず，このパラメータに関する研究結果はそれほど多くなく，いくつかの単純な限界式が知られているのみである（Oxley(’78)等）．本課題においては，その決定問題へ符号理論的に新たにアプローチするために，(1)任意のマトロイドに対して，階数や内周などの符号パラメータに対応するものを用いた最小被覆数の限界式の導出とその等号をみたすマトロイド族の構成・分類及び(2)様々な禁止マイナーにより類別されたマトロイド族に応じた最小被覆数の限界式（あるいは限界値）の導出を目的とした．

上記の研究の主な波及効果としては，弱アフィン符号の組合せ構造を明確にすることで，対応する秘密分散システムの新たな数理構造も把握できると予想している．また，最小被覆数に関して様々な限界式（値）を導出することで，マトロイドの極値問題以外にも関係が深いグラフの頂点彩色問題である 4 色定理や符号の古典的最適化問題に関する新たなアプローチになり得ると考えている．

３．研究の方法

上記の各発展課題に関して，以下のような研究方法により研究を実施した．



【発展課題(1)】(1)計算限界を考慮し，位数 5 以下の集合上の符号長 40 以下の弱アフィン符号を Python プログラムで数多く構成し，得られた符号とそのマイナーに対して，MAGMA プログラムを用いて重み多項式系の係数や因子比較及び次元による部分符号の分布比較についての計算データを採取，(2)得られた計算結果を考察し，各マイナーのパターンにより分類，(3)対応する弱アフィン符号族の特徴を様々な方向から検討，(4)これらの特徴を普遍化することで，弱アフィン符号が与えられたマイナーをもつための必要条件あるいは必要十分条件を導く．

【発展課題(2)】(1)【発展課題(1)】で得た弱アフィン符号から得られるマトロイド及び他の非表現マトロイドに関して，その特性多項式・Tutte 多項式および最小被覆数を出力する MAGMA プログラムを作成し，計算データを採取，(2)それらをもとにして，階数や内周等のパラメータを用いて限界式を導出し，その等号を満たすマトロイドを構成・分類，(3)(1)の最小被覆数の計算データを禁止マイナーによる類別によって再度整理・検討，(4)これらをもとに限界式または限界値を【課題(1)】および【発展課題(1)】で考察した符号特性を利用して証明する．

４．研究成果

前述の研究方法に従い研究を実施し，以下の通り各課題において研究成果が得られた．

【発展課題(1)】マトロイドの弱アフィン表現問題の考察

弱アフィン符号のマトロイド的離散構造の１つであるパワフル集合について，マトロイドにおける公理の拡張を行い，公理化の導入をおこなった．また，マトロイドの双対性を一般化することで双対パワフル集合を新たに定義し，拡張構成とその双対に関する関係を明確化した．さらに，パワフル集合を表現する弱アフィン符号について，それまでに実施した公理化や双対パワフル集合の導入および拡張構成をもとにして，符号としての復号アルゴリズムについて考察をおこなった．加えて，パワフル集合を表現するための弱アフィン符号のマイナー構造について，数種類の分類を実施した．

【発展課題(2)】マトロイドの最小被覆数に関する符号理論的考察

計算機による探索により，マトロイドのいくつかのクラスの最小被覆数については，一意的に決定できるものが複数個存在することを把握することができた．また，一般のマトロイドの最小被覆数に関する上限界式を導出して，等号が成立する最適なマトロイドの分類を目指して，様々な条件の下で考察をおこない，その結果，最小コサーキット位数がある程度小さいものに関しては分類することができた．

また，マトロイドの最小被覆数の上限界式を得ることを目的として，最小被覆数と双対の関係にある最大充填数について考察をおこなった．特に，表現マトロイドの最大充填数に関しては，符号理論的考察により，新たな２つの下限界式を証明することができ，等号の成立状況についてもある程度の状況は把握することができた．さらに，一般のマトロイドに関しても，１つの下限界式の成立を予想することができた．

さらに，これまでに証明したマトロイドの最小被覆数の上限界式をポリマトロイドに一般化し，Kung 型の限界式を得ることができた．ただし，現段階においては等号の成立状況については，ごく僅かの例しか得ることが出来ていない．同様に，これまでに証明したマトロイドの最小被覆数の上限界式を空間マトロイドに一般化し，Kung 型の限界式を得ることができた．ただし，現段階においては等号の成立状況については，完全には把握できていない．

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　4件／うち国際共著　1件／うちオープンアクセス　0件）

１．著者名 Britz Thomas、Mammoliti Adam、Shiromoto Keisuke	４．巻 88
２．論文標題 Wei-type duality theorems for rank metric codes	５．発行年 2020年
３．雑誌名 Designs, Codes and Cryptography	６．最初と最後の頁 1503～1519
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10623-019-00688-9	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 Keisuke Shiromoto	４．巻 87
２．論文標題 Codes with the rank metric and matroids	５．発行年 2019年
３．雑誌名 Designs, Codes and Cryptography	６．最初と最後の頁 1765-1776
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10623-018-0576-0	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 －

１．著者名 Koga Yoshitaka、Maruta Tatsuya、Shiromoto Keisuke	４．巻 86
２．論文標題 On critical exponents of Dowling matroids	５．発行年 2018年
３．雑誌名 Designs, Codes and Cryptography	６．最初と最後の頁 1947～1962
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10623-017-0431-8	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 －

〔学会発表〕　計18件（うち招待講演　4件／うち国際学会　9件）

１．発表者名 今村浩二，城本啓介
２．発表標題 An upper bound on critical exponents of Z_{p^m}-codes
３．学会等名 JCCA2020-DMIA2020-SGT9
４．発表年 2020年

１．発表者名
近藤集史，城本啓介

２．発表標題
Classification on Generalized Weight Enumerators of Rank-Metric Codes

３．学会等名
JCCA2020-DMIA2020-SGT9

４．発表年
2020年

１．発表者名
今村浩二，城本啓介

２．発表標題
有限環上の符号を用いたマトロイドの構成について

３．学会等名
2020年度応用数学合同研究集会

４．発表年
2020年

１．発表者名
今村浩二，城本啓介

２．発表標題
有限環上のマトロイドの表現問題について

３．学会等名
2021年日本数学会年会

４．発表年
2021年

１．発表者名
Shuji Kondo, Keisuke Shiromoto

２．発表標題
Generalized Weight Enumerators of Rank-Metric Codes and Matroids

３．学会等名
42nd Australasian Conference on Combinatorial Mathematics and Combinatorial Computing（国際学会）

４．発表年
2019年

１．発表者名
Koji Imamura, Keisuke Shiromoto

２．発表標題
Critical problem forces over Z_{p^e}

３．学会等名
42nd Australasian Conference on Combinatorial Mathematics and Combinatorial Computing（国際学会）

４．発表年
2019年

１．発表者名
近藤 隼史, 城本啓介

２．発表標題
Generalized Weights of Rank-Metric Codes and Matroids

３．学会等名
Japanese Conference on Combinatorics and its Applications (JCCA-2019)

４．発表年
2019年

１．発表者名
今村 浩二, 城本啓介

２．発表標題
Critical Problem for Codes over Finite Rings

３．学会等名
Japanese Conference on Combinatorics and its Applications (JCCA-2019)

４．発表年
2019年

１．発表者名
Keisuke Shiromoto

２．発表標題
The Critical Problem for Binary Matroids

３．学会等名
27th British Combinatorial Conference（国際学会）

４．発表年
2019年

１．発表者名
Keisuke Shiromoto

２．発表標題
Critical Problem for Binary Matroids

３．学会等名
Monash Univ. Discrete Maths Research Group Meeting（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
Keisuke Shiromoto

２．発表標題
Critical Problem for Binary Matroids

３．学会等名
The 17th Japan-Korea Workshop on Algebra and Combinatorics（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Keisuke Shiromoto

２．発表標題
Codes with Rank Metric and Matroids

３．学会等名
The Japanese Conference on Combinatorics and its Applications (JCCA 2018)（国際学会）

４．発表年
2018年

１．発表者名
Keisuke Shiromoto

２．発表標題
Critical Problem for Binary Matroids

３．学会等名
41st Australasian Conference on Combinatorial Mathematics and Combinatorial Computing (41ACCMCC)（国際学会）

４．発表年
2018年

１．発表者名
城本　啓介

２．発表標題
Critical Problem for Binary Matroids

３．学会等名
研究集会「組合せ論的符号理論」

４．発表年
2019年

１．発表者名
Keisuke Shiromoto

２．発表標題
Critical Problem for matroids and Codes

３．学会等名
Discrete Structures and Algorithms Seminar in University of Melbourne（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
Keisuke Shiromoto

２．発表標題
Matroids and Codes with Rank Metric

３．学会等名
5th International Combinatorics Conference (5ICC)（国際学会）

４．発表年
2017年

１．発表者名
城本 啓介

２．発表標題
Codes with Rank-Metric and Matroids

３．学会等名
Japanese Conference on Combinatorics and its Applications (JCCA2017)・離散数学とその応用研究集会2017

４．発表年
2017年

１．発表者名
城本 啓介

２．発表標題
On the Critical Problem for Matroids and Codes

３．学会等名
愛媛大学数学科談話会/第45回代数セミナー（招待講演）

４．発表年
2017年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
所属学科のホームページの研究紹介
https://www.fast.kumamoto-u.ac.jp/wp/wp-content/uploads/2018/04/keisuke_shiromoto.pdf

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
主たる渡航先の主たる海外共同研究者	トーマス　ブリッツ (Thomas Britz)	ニューサウスウェールズ大学・School of Mathematics and Statistics・Senior Lecture	

６．研究組織（つづき）

	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
主たる渡航先の主たる海外共同研究者	グラハム　ファー (Graham Farr)	モナシュ大学・Faculty of Information Technology・Professor	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関			
オーストラリア	Monash University			
オーストラリア	University of New South Wales			