様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　１２　日現在

機関番号：　１７４０１
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2017
課題番号：　２６４００１８７

研究課題名（和文）代数的符号理論に基づくマトロイド理論の新展開と量子情報理論への応用

研究課題名（英文）Matroids, Quantum Information Theory, and Codes

研究代表者
城本　啓介（Keisuke, Shiromoto）

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）　　3,700,000円

研究成果の概要（和文）：　研究代表者の代数的符号理論におけるこれまでの主な研究内容である符号の存在問題および構成問題を軸として、マトロイド理論・および量子情報理論のそれぞれの分野における同種の問題を統一的に考察した。主な結果としては、有限体上の表現マトロイドの臨界指数に関する分類定理および限界式を導出したことやDowling matroidの臨界指数に関する分類定理を証明したことが挙げられる。

研究成果の概要（英文）：In algebraic coding theory, I have studied mainly the existence problem and the construction problem of codes. Based on these problems, I tried to consider a kind of the similar problems in matroid theory and quantum information theory in this research period. The main results contain a classification theorem and an upper bound on critical exponents of any representative matroids over finite fields and a classification result on the critical exponent of a Dowling matroid over a finite field.

研究分野：　代数的符号理論

キーワード：　マトロイド　量子情報　線形符号

１．研究開始当初の背景

様々な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おいては，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おこなわれている．

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, … ,’05) 等），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の考察（例：Shiromoto (’96, ’99) 等）や符号族内での非同型なものの分類（例：Sloane, et al. (’72) 等），最適な符号族に関する高次重み多項式の理論的決定（例：Shiromoto (’06), Britz-Shiromoto, et al. (’07) 等），符号を用いた組合せデザインの構成法の提案（例：Assmus-Mattson (’69), Britz-Shiromoto (’07) 等）などがある．

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．主な種類としては，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．古典的問題としては，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），与えられた表現マトロイドの族に関して特性多項式と表現体の位数から得られる値である臨界指数（グラフの頂点彩色数の概念に対応）は決定可能か（極値問題），あるいは与えられたパラメータ（列数，階数，臨界指数等）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．主な結果として知られているのは，位数 2, 3, 4 の体ごとの各表現問題に関して，グラフでの削除・縮約によるグラフマイナーに対応したマトロイドマイナーを用いた禁止マイナーによる条件付け（例：Whittle (’05) 等），臨界指数に関しては極小マイナー族を用いた複雑な形での限界式（Oxley (’83)）や禁止マイナーによって類別された族に応じた限界式（Kung (’86) 他）や限界値の予想（Walton-Welsh (’80)）などである．

量子情報理論における SIC（Symmetric Informationally Complete) set とは，d 次元ヒルベルト空間内の 個の擬直交性・正規性をもつベクトルの集合のことである．特に，与えられた次元に対して，この集合を見つける（構成する）ことや非同値な集合の数え上げは，量子鍵配布プロトコルや量子トモグラフィへの応用として近年研究されているが，純粋物理学としても意義がある．構成法に関する研究としては，67 次元までは計算機を用いた探索によって発見されている（Grassel, et al. ('09) 他）が，理論的な構成法は明らかにされていない．

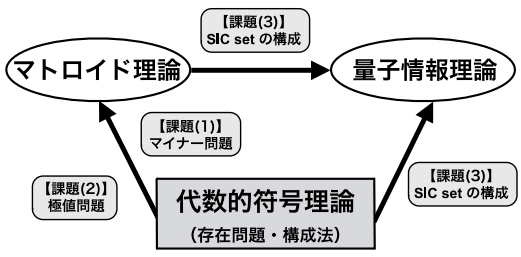
２．研究の目的

研究代表者の代数的符号理論におけるこれまでの主な研究として，与えられたパラメータや性質をもつ符号の存在問題の考察および構成法の提案がある．本研究においては，これらの研究を軸として，工学的応用も視野に入れた組合せ論および量子情報理論における同種の問題を新たな視点から研究し，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する．特に，研究期間内においては以下を具体的な研究の目的とした．

【課題(1)】：マトロイドとそのマイナーの関係を符号理論的に把握するために，それらの自己同型群の関係，マトロイド的重み多項式の因子関係，フラットの階層構造の関係を明確にして，マトロイドが与えられたマイナーをもつための必要条件または必要十分条件をこれらの関係を用いて考察する．

【課題(2)】：極値問題へ符号理論的にアプローチするために，任意の表現マトロイドに対して，符号の次元や最小重みなどに対応したパラメータを用いた臨界指数の限界式の導出およびその等号をみたすマトロイド族の構成，様々な禁止マイナーにより類別された表現マトロイド族に応じた臨界指数の限界式（あるいは限界値）の導出，をおこなう．

【課題(3)】：高次元 SIC set を系統的に構成することを目指して，有限環上の符号，双対性を保持した準マトロイドを用いた構成法を考案する．



本研究における各研究課題の構造

３．研究の方法

課題ごとの具体的な研究計画・方法は以下の通りであった．

(1) マトロイドとそのマイナーの関係を符号理論的に把握するために，下記の計画・手法を用いることとした．

① 代表的なマトロイドマイナーに対応する完全グラフ・完全 2 部グラフやファノ平面･アフィン平面の接続行列から生成される符号やその双対符号をマイナーとする体上の符号を構成し,符号とそのマイナーについて, 自己同型群の構造比較, 重み多項式系の係数や因子比較,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する. さらに, 得られた計算結果を代数的および符号理論的に考察し, 各対象のパターンにより分類することで,対応する符号族の特徴を様々な方向から分析する.
② これらの特徴を一般化することで,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考察する.

(2) 任意の表現マトロイドに対する臨界指数の限界式の導出のために, 下記の計画・手法を用いることとした.
① 体上の表現マトロイドに関して,その特性多項式および臨界指数を出力する計算プログラムを作成し, 対応する符号の次元・重み分布･一般化重み等のパラメータと共に計算データを採取する.
② 採取した臨界指数等に関する計算データの解析をもとに,次元や最小重み等の符号のパラメータを用いて目標としていた簡素な限界式を導出し,その等号をみたす符号を構成する. さらに, 禁止マイナーによる表現マトロイドおよび符号の類別をおこない,それぞれの族における臨界指数の計算データをもとに限界式または限界値を証明する.

(3) 古典符号を用いた SIC set の系統的な構成法を考案するために, 下記の計画・手法を用いることとした.
① 既存の SIC set についての情報を収集・整理し, 特に素数次元に限定して, それを含有するシンプレクティック量子符号の探索プログラムを作成し,対応する素体上の符号の生成行列や自己同型群等の数理構造についての計算データを採取する.
② 得られた素数次元 SIC set の計算結果の分析を一般化することで,素体上の符号を用いた構成法を提案する. さらに, 構成法を整数剰余環上の符号へと拡張することで, 符号を用いた一般次元 SIC Set の理論的構成法を提案する.

４．研究成果

本研究期間における具体的に研究成果は以下の通りである.

(1) マトロイドのそのマイナーの関係を符号理論的に把握することを目的として, 様々な計算データによるマイナーの考察をおこなった. その結果, 2 元符号については, 射影幾何上での包含関係における部分構造に着目することで関係性を視覚化できることが分かった. このことから, 特に完全グラフをマイナーとする符号の幾何学的特徴付けをおこなうことができた.

(2) 様々な臨界指数をもつ有限体上の表現マトロイドの特徴付けおよび分類を目的として, Dowling matroid の臨界指数に関する必要十分条件について研究をおこなった. 特に, Griesmer 限界式や現時点での最適符号の存在状況等の符号理論的構造を利用することで, 大きな臨界指数をもつ Dowling matroid については, 目標としていた必要十分条件を導くことができた. また, 具体的な表現体や臨界指数に応じた必要十分条件も導出することができた.

(3) 任意の表現マトロイドに対する臨界指数の限界式の導出を目的として, 表現マトロイドの基集合の各部分集合に対して一般化臨界指数を新たに定義し, 符号の一般化ハミング重みの研究で用いた研究手法を用いて, 様々な限界式の導出, 双対ハミング符号の一般化臨界指数の決定をおこなった.

(4) 整数剰余環上の線形符号のリー重み多項式およびユークリッド重み多項式に関する MacWilliams 型恒等式を代数的アプローチにより証明した.

(5) 整数剰余環上の線形符号による量子信号系の通信路行列の解析解の導出を行った. 量子情報理論において,測定過程として Square-root measurement を用いることにより様々な成果が示されている.本研究では, 整数剰余環上の線形符号が群共変的である事実を用いて量子信号系の通信路行列の解析解の存在について考察をおこなった.

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 13 件）

① Shuya Chiba, Tomoki Yamashita, Degree sum conditions for vertex-disjoint cycles passing through specified vertices, Discrete Mathematics 340 (2017), 678 ～ 690, DOI: 10.1016/j.disc.2016.12.010, 査読有.
② Roman Cada, Shuya Chiba, Kenta Ozeki, Kiyoshi Yoshimoto, On dominating even subgraphs in cubic graphs, SIAM Journal on Discrete Mathematics 31 (2017), 890 ～907, DOI: 10.1137/16M1066622, 査読有.
③ Thomas Britz, Keisuke Shiromoto, On the covering dimension of a linear code, IEEE Transaction on Information Theory 62 (2016), 2694 ～ 2701, DOI: 10.1109/TIT.2016.2538768, 査読有.
④ Trygve Johnsen, Keisuke Shiromoto, Hugues Verdure, A generalization of Kung's theorem, Designs, Codes and

Cryptography 81 (2016), 169～178, DOI: 10.1007/s10623-015-0139-6, 査読有.

⑤ Shuya Chiba, Yuji Nakano, Remarks on upper and lower bounds for matching sequencibility of graphs, FILOMAT 30 (2016), 2091 ～ 2099, DOI: 10.2298/FIL1608091C, 査読有.

⑥ 千葉 周也, 山下 登茂紀, 二部グラフ上の完全マッチングを含む 2-因子と有向グラフ上の有向 2-因子, 2016 年度応用数学合同研究集会報告集, 2016, 122～129, 査読無.

⑦ Trygve Johnsen, Keisuke Shiromoto, Hugues Verdure, A generalization of Kung ' s theorem, Designs, Codes and Cryptography 81 (2016), 169～178, DOI: 10.1007/s10623-015-0139-6, 査読有.

⑧ Shuya Chiba, Nicolas Lichiardopol, Vertex-disjoint subgraphs with high degree sums, Electronic Notes in Discrete Mathematics 49 (2015), 359～366, DOI: 10.1016/j.endm.2015.06.050, 査読有.

⑨ Shuya Chiba, On lower bounds for matching sequencibility of general graphs, Proceedings of The 2015 Engineering Workshop among Ajou University, Shandong University and Kumamoto University, 2015, p. 52, 査読有.

⑩ Minjia Shi, Keisuke Shiromoto, Patrick Sole, A note on a basic exact sequence for the Lee and Euclidean weights of linear codes over Z_l, Linear Algebra and its Applications 475 (2015), 213～215, DOI: 10.1016/j.laa.2015.01.033, 査読有.

⑪ Keisuke Shiromoto, On critical exponents of matroids and linear codes, 数理解析研究所講究録 1889 (2014), 7～12, 査読無.

⑫ M. Tanaka, T. Sogabe, K. Shiromoto, and T. S. Usuda, Group covariance and formula of channel matrix of coded 4PSK signals by linear codes over F_4, 2014 International Symposium on Information Theory and Its Applications (ISITA2014), 2014, p. 348, 査読有.

⑬ T. S. Usuda, T. Sogabe, and K. Shiromoto, Formula of channel matrix for covariant signal set with respect to a direct product of groups, 12th International Conference on Quantum Communication, Measurement and Computing (QCMC2014), 2014, p. 45, 査読有.

〔学会発表〕(計 20 件)

① Keisuke Shiromoto, Critical problem for matroids and codes, Discrete Mathematics Research Group meeting, 2017 年 03 月 08 日, Monash University (Melbourne, Australia)

② 城本 啓介, 符号理論的マトロイド理論について, 近畿大学数学教室講演会,2017年02月21日, 近畿大学(大阪府東大阪市)

③ 城本 啓介, 符号理論的マトロイド理論へのいざない, 筑波大学組合せ論・情報理論セミナー, 2017 年 02 月 08 日, 筑波大学（茨城県つくば市）

④ 千葉 周也, 山下 登茂紀, 二部グラフ上の完全マッチングを含む 2-因子と有向グラフ上の有向 2-因子, 2016 年度応用数学合同研究集会, 2016 年 12 月 16 日, 龍谷大学（滋賀県大津市）

⑤ Keisuke Shiromoto, On the covering number of matroids, The 40th Australasian Conference on Combinatorial Mathematics and Combinatorial Computing (40ACCMCC), 2016 年 12 月 14 日, University of Newcastle (Newcastle, Australia)

⑥ Shuya Chiba, On 2-factors through specified perfect matchings in bipartite graphs, The Japanese Conference on Combinatorics and its Applications (JCCA 2016), 2016 年 05 月 22 日, Kyoto University, Clock Tower Centennial Hall (Kyoto, Japan)

⑦ Keisuke Shiromoto, On the covering number of matroids, The Japanese Conference on Combinatorics and its Applications (JCCA 2016), 2016 年 05 月 22 日, Kyoto University, Clock Tower Centennial Hall (Kyoto, Japan)

⑧ 千葉周也, 次数条件と 2-因子について, RIMS 共同研究「閉曲面上のグラフの彩色問題への因子・閉路を利用してのアプローチ」, 2016 年 03 月 07 日, 京都大学数理解析研究所（京都府京都市）

⑨ Keisuke Shiromoto, Critical problem in coding theory, The 4th Japan-Taiwan Conference on Combinatorics and its Applications, 2016 年 03 月 07 日, 北九州国際会議場（福岡県北九州市）

⑩ Shuya Chiba, Degree conditions for 2-factors with k cycles in bipartite graphs, The 4th Japan-Taiwan Conference on Combinatorics and its Applications, 2016 年 03 月 05 日, 北九州国際会議場(福岡県北九州市)

⑪ 千葉周也, On 2-factors with k cycles in graphs, Hakata Workshop 2016 - Discrete Mathematics and its Applications, 2016 年 02 月 23 日, 九州大学（福岡県福岡市）

⑫ 古賀義孝, 城本啓介, Critical exponents of Dowling matroids, 2015 年度応用数学合同研究集会, 2015 年 12 月 18 日, 龍谷大学（滋賀県大津市）

⑬ Yoshitaka Koga, Keisuke Shiromoto, Critical exponents of Dowling matroids,

39th Australasian Conference on Combinatorial Mathematics and Combinatorial Computing, 2015 年 12 月 07 日, University of Queensland (Brisbane, Australia)

⑭ Keisuke Shiromoto, Shunpei Yamaguchi, Codes from complete bipartite graphs and 3-regular graphs, 39th Australasian Conference on Combinatorial Mathematics and Combinatorial Computing, 2015 年 12 月 07 日, University of Queensland (Brisbane, Australia)

⑮ Shuya Chiba, On lower bounds for matching sequencibility of general graphs, The 2015 Engineering Workshop among Ajou University, Shandong University and Kumamoto University, 2015 年 11 月 12 日, Kumamoto University (Kumamoto, Japan)

⑯ Keisuke Shiromoto, On covering dimension of linear codes and matroids, 25th British Combinatorial Conference, 2015 年 07 月 09 日, University of Warwick (Coventry, UK)

⑰ 城本 啓介, On the covering dimension of a linear code, 研究集会「有限幾何と組合せデザイン」, 2015 年 03 月 06 日, 東京理科大学（東京都）

⑱ 千葉 周也, グラフにおける次数条件と点素な閉路, 第 11 回組合せ論若手研究集会, 2015 年 03 月 06 日, 慶應義塾大学（東京都）

⑲ Keisuke Shiromoto, On the critical exponent of a linear code and a matroid, The 13th Japan-Korea Workshop on Algebra and Combinatorics, 2015 年 01 月 29 日, 九州工業大学(福岡県北九州市)

⑳ Keisuke Shiromoto, On the covering dimensions of a linear code and its relation to matroids, 38th Australasian Conference on Combinatorial Mathematics and Combinatorial Computing (38ACCMCC), 2014 年 12 月 04 日, Victoria University of Wellington (Wellington, New Zealand)

〔図書〕（計　0件）

〔産業財産権〕

○出願状況（計　0件）

○取得状況（計　　件）

〔その他〕
ホームページ等
http://www.srik.kumamoto-u.ac.jp

６．研究組織
(1)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・教授
研究者番号：00343666

(2)研究分担者
千葉　周也（CHIBA, Syuya）
熊本大学・大学院先端科学研究部・講師
研究者番号：80579764

(3)連携研究者
臼田　毅（USUDA, Takeshi）
愛知県立大学・情報科学部・教授
研究者番号：80273308

千吉良　直紀（CHIGIRA, Naoki）
熊本大学・大学院先端科学研究部・准教授
研究者番号：40292073

(4)研究協力者
Thomas Britz
University of New South Wales・School of Mathematics・Senior Lecturer