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　　５　月　２６　日現在

機関番号：　１７４０１
研究種目：　基盤研究(C)
研究期間：　2011～2014
課題番号：　２３５４０１４８

研究課題名（和文）代数的符号理論を軸とした組合せ論・量子情報理論への多面的展開

研究課題名（英文）Some problems in combinatorial theory and quantum information theory based on algebraic coding theory

研究代表者

城本　啓介（Shiromoto, Keisuke）

熊本大学・自然科学研究科・教授

研究者番号：００３４３６６６

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）：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・組合せデザイン理論・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、整数環上の符号による量子信号系の通信路行列の解析解の導出や有限環上の符号によるマトロイドの構成法の提案などを行うことができた。

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, combinatorial design theory, and quantum information theory in this research period. One of the main results is to give a construction of matroids from codes over finite rings.

研究分野：　代数的符号理論およびマトロイド理論

キーワード：　符号　マトロイド　組合せデザイン　量子符号　組合せ論

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，どのように構成するかといった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．有限体上の符号とは，有限体上のベクトル空間の部分空間のことである．

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符号の存在性の検討・構成法の提案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について，母関数を用いた非同型な符号の数え上げ，重み多項式を用いた符号の解析，一般化重みの理論的決定などがある．

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．主な構成法としては，グラフの木構造や代数的閉体を用いた手法，有限体上の行列から構成する手法などが知られている．特に，与えられたマトロイドがどのような有限体上の行列から得られるか，与えられたサイズの有限体上の行列を用いて何個の非同型なマトロイドが構成できるか，といったマトロイドの表現問題や数え上げ問題が古典的問題として考えられている．

組合せデザインとは，有限集合と一様性・均整性をもつその部分集合族の組からなる組合せ構造であり，近年では暗号理論や情報通信分野との関連研究が盛んに行われている．与えられたパラメータをもつデザインの存在問題や一様な全部分集合族の共通なブロックをもたない排反なデザインへの分割可能性に関する考察，符号や他の組合せ構造を用いたデザインの系統的な構成法の考案などが古典的問題である．また，応用研究としてデザインに類似した均整性をもつ組合せ構造から，量子ジャンプといわれる量子状態の推移による通信誤りを訂正するための量子符号が構成されることが知られている．

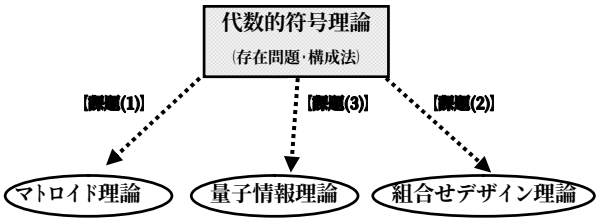
２．研究の目的

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)】：マトロイドの表現問題に対する符号理論的考察をおこなう．

【課題(2)】：排反な組合せデザインの構成および Large Set の存在問題の考察および量子符号の構成をおこなう．

【課題(3)】：整数剰余環上の（古典）符号を用いた量子符号の構成法を考案する．



各課題の相関図

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る．

(1)マトロイドの表現問題に対する符号理論的考察について

① 具体的に与えられたマトロイドに対して，そのマトロイド的重み多項式，表現可能な有限体上での表現行列を出力するプログラムを作成し，多数のデータを採取する．さらに，採取したデータを重み多項式のパターンによって分類し，対応するマトロイドの特徴を様々な方向から分析する．

② ①の段階で得られた分類を一般化し，マトロイド的重み多項式による各有限体上での表現可能性の条件付けをおこなう．

③ ②で得られた条件とマイナーによる条件付けとの統一化をおこなうことで，グラフと符号のマトロイドにおける統一的構造を見つける．

(2) 排反な組合せデザインの構成および Large Set の存在問題の考察について

① 既存の Large Set についての情報を収集し，もととなるデザインの自己同型群および同型なデザインを構成する置換の組に関して，計算機を用いたデータ採取をおこなう．

② ①で採取したデータを解析し，Large Set が存在するための自己同型群や置換の振る舞いに関する条件付けをおこなう．

③ ②で得られた存在条件を満たす Large Set を符号や他の組合せ構造を用いて理論的に構成し，Large Set の系統的な構成法を提案する．

④ ②で得られた条件を量子ジャンプ符号へ適用することで，次元に関する限界式を導く．さらに，等号を満たす最適符号をデザイン構造から構成する．

(3)量子符号の構成法の提案について
① 既存の素数次元の量子符号の情報を収集し,対応する素体上のベクトルから生成される符号の重み多項式や自己同型群について計算データの採取をおこなう.
② ①の計算結果をもとにしたアルゴリズムを考案し,より高次元の量子符号についても,プログラム計算による探索をおこなう.
③ ①で得られた素数次元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.
④ 整数剰余環上の符号を用いて,①, ②と同様な計算及びその解析をおこなうことで,環上の符号を用いた量子符号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) 整数環上の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（SRM）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,整数環上の符号が群共変的であることを確認し,SRM を用いた整数環上の符号に対する量子信号系の通信路行列の解析解を示した.さらにその有用性を確認するため,整数環上と拡大体上の符号による量子信号系の相互情報量及び平均誤り率の比較を行った.

(2)整数環上の符号によるマトロイドの構成法を提案した．ベクトル空間の概念を有限集合へ拡張した構造を持つマトロイドが,有限体上の符号から構成されることはよく知られている.そこで,本研究においては,マトロイドをさらに一般化した離散構造が有限環上の符号から構成されることを示し,その構成法に付随した結果として,すでにWoodによる代数的考察によって得られている有限フロベニウス環上の線形符号に対するマックウィリアムズ恒等式に対して,組合せ論的な別証明を与えた.

(3)群共変的量子信号系の通信路行列の解析解の導出を行った．本研究では,従来の狭義の群共変的信号の定義を拡張した信号を新たに定義し,その必要十分条件および具体例を示した.さらに,その信号に対するグラム行列の固有値と固有ベクトルの解析解を示し,この信号に対する通信路行列公式を与えた.

(3)マトロイドの臨界問題の符号理論的考察を行った．ベクトル空間の概念を有限集合へ拡張した構造を持つマトロイドと有限体上の符号の関係は古くから研究が行われている．そこで,本研究ではマトロイドにおける臨界問題と符号の次元に関する問題との対応付けを考察し,当該問題に対して,符号理論の手法を用いた新たな計算機を用いたアプローチを行った.

(4)拡張群共変的量子信号系の通信路行列の解析解の導出を行った．本研究では，従来の狭義の群共変的信号の定義を対応する群の指標に基づいて拡張した信号を新たに定義し，その解空間に関する必要十分条件を示した．さらに，その信号に対するグラム行列の固有値と固有ベクトルの解析解を示し，この拡張群共変的量子信号に対する通信路行列公式を与えた.

(5)ブロックマトロイドの構成法の提案を行った．ブロックマトロイドとは有限体上の表現マトロイドの１つのクラスである．本研究では，有限体上の符号と同一体上の行列に対応したブロックマトロイドとの関係性について符号理論の立場から考察を行った．特に,符号の生成行列から特徴的なベクトルを抽出して,直接的にブロックマトロイドを構成する手法を提案した.

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　７件）

① Thomas Britz, Keisuke Shiromoto, Thomas Westerbäck, Demi-matroids from codes over finite Frobenius rings, Designs, Codes, and Cryptography（印刷中）, DOI 10.1007/s10623-013-9895-3, 査読有
② Keisuke Shiromoto, The critical problem in coding theory, 第30回代数的組合せ論シンポジウム報告集, 2013, 80–85, 査読無
③ Yoshihiro Ishikawa, Keisuke Shiromoto, Takeshi S. Usuda, Formula for the channel matrix of a certain class of (G, χ)-covariant signals, 13th Asian Quantum Information Science Conference (AQIS2013), Chennai, India, Extended Abstracts of AQIS2013, pp.209-210, (2013), 査読有
④ Thomas Britz, Trygve Johnsen, Dillon Mayhew, Keisuke Shiromoto, Wei-type duality theorems for matroids, designs, Codes and Cryptography, 62 (2012), pp.331-341, DOI 10.1007/s10623-011-9524-y, 査読有
⑤ 太田征輝, 城本啓介, 臼田毅, 整数環上の任意の線形符号による量子信号系の通信路行列の解析解, 電子情報通信学会論文誌, J95-B, No.2 (2012), pp.110-118, 査読有
⑥ Masayuki Angata, Keisuke Shiromoto, Mutually disjoint 5-designs from Pless symmetry codes, Journal of Statistical Theory and Practice, 62 (2012), pp.78-87, DOI

10.1080/15598608.2012.647525, 査読有
⑦ 神保雅一, 城本啓介, Mutually orthogonal partial t-designs over C related to quantum jump codes, 第28回代数的組合せ論シンポジウム報告集(2011), pp.76-81, 査読無

〔学会発表〕(計　１０件)
① Keisuke Shiromoto, From codes to matroid and back, The 3rd Taiwan-Japan Conference on Combinatorics and its Applications (3TJCCA), 2014年3月21日, National Chiayi University (Chiayi City, Taiwan)
② Keisuke Shiromoto, On critical exponents of matroids and linear codes, The 37th Australasian Conference on Combinatorial Mathematics and Combinatorial Computing (37ACCMCC), 2013年12月11日, The University of Western Australia (Perth, Australia)
③ Keisuke Shiromoto, On critical exponents of matroids and linear codes, Designs, Codes, Graphs and Related Areas, 2013年7月1日, 京都大学数理解析研究所（京都）
④ 城本啓介, The critical problem in coding theory, 第30回代数的組合せ論シンポジウム, 2013年6月25日, 静岡大学（静岡）
⑤ 穴井佑弥, 岡美里, 城本啓介, 4元自己双対符号を用いた互いに排反な組合せデザインの構成について, 第35回情報理論とその応用シンポジウム, 2012年12月13日, 別府湾ロイヤルホテル（大分）
⑥ 石川喜啓, 城本啓介, 臼田毅, 古典-量子通信における通信路行列公式の一般化に向けて, 第35回情報理論とその応用シンポジウム, 2012年12月12日, 別府湾ロイヤルホテル（大分）
⑦ Keisuke Shiromoto, Codes over rings and matroids, The 36th Australasian Conference on Combinatorial Mathematics and Combinatorial Computing, 2012年12月10日, University of New South Wales (Sydney, Australia)
⑧ Keisuke Shiromoto, The critical problem for graphs, matroids, and codes, The 2nd Japan-Taiwan Conference on Combinatorics and its Applications, 2012年11月11日, 名古屋大学（愛知）
⑨ 城本啓介, Dualities in codes over rings and matroids, 応用数学合同研究集会, 2011年12月15日, 龍谷大学（滋賀）
⑩ 城本啓介, Codes over rings and matroids, 研究集会「離散数理構造とその応用」, 2011年11月19日, 名古屋大学（愛知）

〔図書〕(計　０件)

〔産業財産権〕
○出願状況（計　０件）

○取得状況（計　０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・大学院自然科学研究科・教授
研究者番号：００３４３６６６

(2)研究分担者
なし

(3)連携研究者
神保　雅一（JIMBO, Masakazu）
名古屋大学・大学院情報科学研究科・教授
研究者番号：５０１０３０４９

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

千吉良　直紀（CHIGIRA, Naoki）
熊本大学・大学院自然科学研究科・准教授
研究者番号：４０２９２０７３