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２４年　５月２１日現在

機関番号：１７４０１
研究種目：若手研究（B）
研究期間：2008～2010
課題番号：２０７４００６３
研究課題名（和文）　代数的符号理論の多角的研究～符号・マトロイド・デザインの三角形からみえるもの～
研究課題名（英文）　Manifold research on algebraic coding theory
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

研究成果の概要（和文）：本研究期間において、自身の代数的符号理論おけるこれまでの研究を軸として符号理論・マトロイド理論・組合せデザイン理論を包括的に研究した結果、(1) 互いに排反な組合せデザインの構成法の提案、(2) 符号の双対性を利用したマトロイドの双対理論の構築、(3) マトロイドにおける新たな Tutte 型多項式の導入の３つの成果を得た。

研究成果の概要（英文）：In this research term, I had tried to study coding theory, matroid theory, and combinatorial design theory from my past research in algebraic coding theory. Then I gave a construction of mutually disjoint designs from some codes, I found a duality theorem for matroids by using the duality in coding theory, and I introduced a new Tutte type polynomial for matroids.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００８年度	1,000,000	300,000	1,300,000
２００９年度	700,000	210,000	910,000
２０１０年度	700,000	210,000	910,000
年度			
総　計	2,400,000	720,000	3,120,000

研究分野：数物系科学
科研費の分科・細目：数学、数学一般（含確率論・統計数学）
キーワード：符号理論、組合せデザイン、マトロイド

１．研究開始当初の背景

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行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。符号の性能を表す主な指標として、復号誤り率等の復号特性の解析に有効である重み多項式、誤り訂正能力の限界や通信路における雑音の抑制などの検討に有効な最小重みや通信傍受周波数帯の研究と関連した一般化重み（ベクトルに対して定義されていた従来の最小重みを符号の部分空間へ拡張して定義、V. Wei が導入）などがある。主な研究としては、重み多項式を用いた符号の解析・特徴付け、最小重みに関する限界式の導出及びその等号を満たす符号の存在性の検討・構成法の提案や様々な符号に関する一般化重みの理論的決定などがある。特に、有限体上の自己双対符号の最小重みに

関しては、N. Sloane らによって様々な限界式が証明され、そのことで極値的（限界的）な自己双対符号に関する存在・非存在問題がクローズアップされた。

マトロイドとは、有限集合と行列の階数の概念を集合上へ一般的に拡張した写像の組からなる組合せ構造である。主なマトロイドの構成法としては、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、というマトロイドの表現問題が古典的問題として考えられている。しかし、これまではグラフ理論的条件付け（グラフマイナーの概念の拡張）が位数２，３，４の有限体毎に行われているだけである。符号との相互間研究としては、C. Greene や A. Barg らによるマトロイドの双対性を用いた符号の重み多項式に対するマックウィリアム恒等式の別証明やマトロイドを用いた符号の構成・解析等、符号をマトロイドの一種と捉えた研究（符号が持つマトロイド構造を利用した研究）が主に知られている。

組合せデザインとは、有限集合とある特徴をもった部分集合族の一部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。符号との相互間研究としては、デザイン構造を持つ符号の解析や符号から系統的にデザインを構成するための重み多項式による条件付けなどがある。また、マトロイドと組合せデザインの相互間研究としては、デザイン構造を持つ特殊なマトロイド(matroid designs)の解析及びその構成に関する研究などが知られている。さらに近年注目されているマトロイドの応用として、秘密保持を目的とした秘密分散共有法がある。これは秘密情報を分散符号化し、特徴的な分散情報を集めると秘密情報が復号可能であり、それ以外の分散情報では復号不可能であるような符号化システムである。このシステムに関しては、マトロイド構造との関連性が指摘されており、どのようなマトロイドがこのシステムの構成に有効か、という適合問題などが数理的研究として行われている。

２．研究の目的

本研究期間内における中核的な目的及び具体的な研究方針は、以下のとおりであった。

(1) 一般化重みの拡張

自己双対符号等のデザイン構造やマトロイド構造（特に、matroid design の構造）を持つ符号について、各構造の特性を活かした符号の一般化重みに関する限界式の導出及び極値的な自己双対符号に関する一般化重みの理論的決定を行う。

(2) マトロイドにおける新たな多項式の導入

マトロイドの表現問題を各有限体上の特徴的な符号の存在問題へと観点を変化させ、符号理論的アプローチ（マトロイド的重み多項式及び限界式の考察等）により、新たに表現に関する条件を導出する。さらに同様の視点で、秘密分散共有法へのマトロイドの適合問題を考察する。

(3) 符号を用いたデザインの構成

符号からデザインを構成するための Assmus-Mattson の定理や自己同型群による特徴付けをマトロイドへ拡張し、符号とマトロイドの両構造が持つ組合せデザインを構成するための共通構造を捉えることで、新たなパラメータを持つ組合せデザインを系統的に構成する。

３．研究の方法

本研究期間内に符号理論・マトロイド理論・組合せデザイン理論の包括的研究を行うために、中核的な目的 (1)、(2)、(3) に応じた研究を年度ごとにバランスを取りながら研究の進捗状況に合わせて、独立にあるいは並行に進めていった。主な方法としては、研究の基盤づくりのために計算機による支援の下で各組合せ構造の諸問題に対応した豊富な例を作り出すことで理論的展開を進めた一方で、構築した理論体系やその応用の妥当性を論じるために、計算機を用いたシミュレーションにも力を入れた。また、国内外の当該分野の研究者に協力を仰ぎながら研究を推進していった。

４．研究成果

(1) 互いに素な組合せデザインの構成法の考察

量子誤り訂正符号の構成を目標として、その１つの手法として各ブロック集合族間に共通なブロック集合が存在しないような組合せデザインの集合族の構成法について研究を行った。特に、ゴレイ符号や QR 符号等の組合せデザインを構成する自己双対符号の生成行列の構造に着目することで、置換写像を用いた新たな構成法を提案した。

さらにこの手法を Pless symmetry 符号に拡張することで、幅広い範囲で互いの排反な 5-デザインが構成できることを証明した。また、これらのデザインの和集合から新たなパラメータをもつ 5-デザインの存在およびその構成法を提案することができた。

(2) 符号の双対性のマトロイド的考察

符号の一般化ハミング重みに関する双対定理をマトロイドへ拡張することで、マトロイドとその双対マトロイド間の新たな関係

を導出することができた。これにより、グラフ等の他の組合せ構造に関する双対性へと応用することができた。また、逆にマトロイドの双対性を符号の概念へ引き戻すことで、有限環上の符号の一般化ハミング重みの双対性も同時に導くことができた。さらに、符号の一般化ハミング重みに関する双対定理を組合せ論的に考察することで、マトロイドをより一般化した離散構造（demi-matoroidという）における双対定理に拡張した。

このことで、順序集合をもとに構成されたposet code における一般化ハミング重みの双対定理を導くことができた。

(3) マトロイドの Tutte 多項式の符号多項式の関連性

マトロイドの Tutte 多項式やその一般化された多項式について、符号理論で用いられる多項式との関係を解明することで、様々なマトロイドの Tutte 多項式の形を決定することを目的として研究をおこなった。本研究では、まずマトロイドの概念を拡張して定義した demi-matoroid に対して Tutte 型多項式を導入し、demi-matroid の双対性を多項式を用いて表現した。

５．主な発表論文等

〔雑誌論文〕（計７件）

① 城本啓介、符号とマトロイドにおける双対性、査読無、2010 年度応用数学合同研究集会報告集、pp.35-36、2010

②M.Jimbo and K.Shiromoto, A construction of mutually disjoint Steiner systems from isomorphic Golay codes, Journal of Combinatorial Theory, Series A, 116, pp.1245-1251, 2009, 査読有

③ T.Britz, G.Royle and K.Shiromoto, Designs from matroids, SIAM Journal on Discrete Mathematics, 23, pp.1082-1099, 2009, 査読有

④T.Britz and K.Shiromoto, A MacWilliams type identity for matroids, Discrete Mathematics, 308, pp.4551-4559, 2008, 査読有

⑤ 城本啓介、量子ジャンプ符号の構成法について、査読無、京都大学数理解析研究所講究録、1593 巻 140-144、2008

⑥ 城本啓介、A Wei-type duality for matroids、査読無、第 25 回代数的組合せ論シンポジウム報告集、pp.128-132、2008

⑦ 安形昌幸、城本啓介、Pless symmetry code から構成される互いに排反な組合せデザインについて、査読無、2008 年度応用数学合同研究集会報告集、pp.51-54、2008

〔学会発表〕（計１０件）

① 城本啓介、量子情報理論と組合せデザイン、RIMS 共同研究「代数的符号理論、組合せデザインとその周辺」、2011 年 3 月 8 日、京都大学（京都）

② 城本啓介、符号とマトロイドにおける双対性、2010 年度応用数学合同研究集会、2010 年 12 月 16 日、龍谷大学（滋賀）

③M.Ota, Formula of channel matrix for coded quantum signals by classical linear codes over Zm, 2010 International Symposium on Information Theory and Its Applications, 2010 年 10 月 20 日, Taichung（Taiwan）

④ T.S.Usuda, Analytical expression of s-th power of Gram matrix for group covariant signals and its application, The Tenth International Conference on Quantum Communication, Measurement and Computation, 2010 年 7 月 22 日, University of Queensland（Australia）

⑤ K.Shiromoto, A construction of mutually disjoint 5-designs from self-dual codes, The 4th International Conference on Combinatorial Mathematics and Combinatorial Computing, 2008 年 12 月 16 日, University of Auckland (New Zealand)

⑥ 安形昌幸、Pless symmetry code から構成される互いに排反な組合せデザイン、2008 年度応用数学合同研究集会、2008 年 12 月 16 日、龍谷大学（滋賀）

⑦ 城本啓介、自己双対符号から構成される t-SEED について、RIMS 共同研究「代数的符号理論と組合せデザイン」、2008 年 10 月 14 日、京都大学数理解析研究所（京都）

⑧ 城本啓介、デザイン構造をもつマトロイド、研究集会「離散数学の統計科学および関連分野への応用」、2008 年 9 月 17 日、ホテルくさかべアルメリア（岐阜）

⑨ 安形昌幸、互いに素な組合せデザインについて、純粋数学及び応用数学としての組合せ論・離散数学そしてその周辺ワークショップ、2008 年 7 月 5 日、電気通信大学（東京）

⑩ 城本啓介、A Wei-type duality theorem for matroids、第 25 回代数的組合せ論シンポジウム、2008 年 6 月 24 日、北海道大学（北海道）

〔図書〕（計２件）

① D. Crnkovic （編集）,Ios Press, Information Security, Coding Theory and Related Combinatorics, 2011, pp.285-311

② 神保 雅一（編集）、オーム社、暗号とセキュリティ、2010、pp.8-30

〔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)研究協力者

Thomas　Britz
University of New South Wales・School of Mathematics and Statistics・Lecture
研究者番号：なし

安形　昌幸（ANGATA　MASAYUKI）
株式会社デンソー・知的財産部・社員
研究者番号：なし