

機関番号：17401

研究種目：若手研究 (B)

研究期間：2008～2011

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. 研究計画の概要

符号理論・マトロイド理論・組合せデザイン理論の各分野において、与えられたパラメータや諸性質を満たす組合せ構造が存在するか否かを考察する存在問題や、存在した場合の相当する構造の構成問題については、今日まで個別に、あるいは相互間においてのみ研究が行われてきた。

本研究においては、自身の代数的符号理論におけるこれまでの研究を軸として、上記の3分野を包括的に研究し、統一的構造の理解を進めることを広義の目標とする。本研究期間内においては、各分野の組合せ構造及び代数構造に着目し、互いの分野の特性を活かしながらそれぞれの分野での存在問題や構成問題等を中心に工学的応用をも視野に入れつつ新たなアプローチを行う。

2. 研究の進捗状況

(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、グレイ符号や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-matroid 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-matroid 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。

3. 現在までの達成度

②おおむね順調に進展している。

(理由)

当初の研究計画通り、研究が進んでいるとともに、得られた手法を拡張することで新たな研究内容へ発展する可能性が少しずつあるが見えてきたため

4. 今後の研究の推進方策

(1) Large Set の構成法の提案

互いに排反な組合せデザインの和集合が部分集合全体になるとき、それらから構成される離散構造を Large Set という。これまでの研究期間において、研究代表者らは組合せデザインを構成する符号に対して、置換を施すことで排反なデザインを構成する手法を提案した。本年度においては、この手法をより洗練かつ一般化することで、新たな Large Set のパラメータの発見および構成法の提案につなげる。

(2) マトロイドの表現問題

位数 2, 3, 4 の有限体上のマトロイドの表現問題に対する符号理論的考察 (マトロイド的加重多項式の特徴付け・限界式の導出等) を進めることで、従来のグラフ理論的条件付けとの統一的理解を得る。

5. 代表的な研究成果

(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 6 件)

- ① M. Angata and K. Shiromoto, Mutually disjoint 5-designs from Pless symmetry codes, Journal of Statistical Theory and Practice, 印刷中, 2011, 査読有
- ② M. Jimbo and K. Shiromoto, A construction of mutually disjoint Steiner systems from isomorphic Golay codes, Journal of Combinatorial Theory, Series A, 116, 1245-1251, 2009, 査読有
- ③ T. Britz, G. Royle and K. Shiromoto, Designs from matroids, SIAM Journal on Discrete Mathematics, 23, 1082-1099, 2009, 査読有
- ④ T. Britz and K. Shiromoto, A MacWilliams type identity for matroids, Discrete Mathematics, 308, 4551-4559, 2008, 査読有

[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
- ③ 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

- ④ 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
- ⑤ 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 神保 雅一 (編集)、オーム社、暗号とセキュリティ、2010、8-30
- ② D. Crnkovic (編集)、Ios Press, Information Security, Coding Theory and Related Combinatorics, 2011, 285-311