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

令和　６ 年　 ６ 月　 ４ 日現在

機関番号：１１３０１
研究種目：基盤研究(B)（一般）
研究期間：2019～2023
課題番号：１９Ｈ０１８０２

研究課題名（和文）代数的符号理論の総合的研究

研究課題名（英文）A synthetic study of algebraic coding theory

研究代表者
原田　昌晃（Harada, Masaaki）

東北大学・情報科学研究科・教授

研究者番号：９０２９２４０８

交付決定額（研究期間全体）：（直接経費）　　8,500,000円

研究成果の概要（和文）：代数的符号理論の重要な対象としてself-dual code があり、代数的および組合せ論的な研究が活発に行われている。本研究課題では、self-dual code を研究対象の中心とし、最小重みの大きな self-dual code の構成を精力的に行うだけでなく、optimal unimodular lattice の構成を行った。Hadamard 行列の self-dual code を用いた特徴づけも行った。
近年、暗号理論などへの応用により注目を浴びつつある LCD code について、基本的ではあるが重要な分類と構成についての成果を得た。

研究成果の学術的意義や社会的意義
誤りが発生する通信路において信頼性が高い情報伝達を行うための理論が符号理論である。代数的符号理論は符号化の部分に現れる組合せ構造としての符号を代数的な立場で研究を行う。
self-dual code は代数的符号理論の重要な対象であり、本研究課題では、それ自身の研究だけでなく、他の分野への関連に着目して、精力的に取り組んだ。符号自身が取り扱いやすい構造をしているためにより難しい構造の研究に役立つ。
また、この先の実用化技術となりうる符号理論の研究が必要だと思っており、近年、暗号理論などへの応用により注目を浴びつつある LCD code についての研究を本格化させた。

研究成果の概要（英文）：Self-dual codes are an important class in algebraic code theory. Both algebraic and combinatorial studies have been done. In this research project, I focus on self-dual codes. I constructed good self-dual codes and optimal unimodular lattices. Some characterization of Hadamard matrices using self-dual codes was given. Recently, much work has been done concerning LCD codes for applications in cryptography and other fields. I made classification and construction of LCD codes, which is a basic but important subject.

研究分野：代数的符号理論

キーワード：自己双対符号　組合せデザイン

１．研究開始当初の背景

符号理論は 1948 年の C. Shannon の論文に端を発し、誤りが発生する可能性のある通信路において、いかに効率よくかつ信頼性が高い情報伝達を行うことを研究する分野であると言える。その中でも、代数的符号理論は、代数的組合せ論とも密接な関係があり、主に通信路の数理モデルにおける符号化の部分に現れる組合せ構造としての符号を代数的な立場（手法）で研究を行う符号理論のことである。

代数的符号理論の重要な対象として self-dual code があり、代数的および組合せ論的な研究が古くから活発に行われている対象である。本研究課題では、研究代表者がこれまでに精力的に研究を行って来た self-dual code を研究対象の中心とした。組合せ論の研究における基本的なテーマでもある存在性と分類問題について取り組むことが重要であると思われていた。

研究代表者の所属する東北大学大学院情報科学研究科では、情報科学を基礎とした学際研究が活発に行われており、次世代の情報化社会の基盤技術の開発も一つのテーマになっている。そのような環境にいることから、１０年先の実用化技術となりうる次世代の（量子）計算機や（耐量子計算機）暗号などの基礎理論としての符号理論の構築が必須であることを感じている。これまでの研究で扱っている対象に加え、Hadamard 行列などの組合せ構造や unimodular lattice などの代数構造との新たな関連を確立させる、未だ発展途上であり大きな可能性を秘めている他の分野との関連に着目した self-dual code を主とした研究により、さらに視野を拡げて代数的符号理論の総合的な発展を目指す、このようなことが重要であると思われていた。

２．研究の目的

代数的符号理論の重要な対象として self-dual code があり、代数的および組合せ論的な研究が活発に行われている。本研究課題では、研究代表者がこれまでに精力的に研究を行って来た self-dual code を研究対象の中心とし、組合せ論の研究における基本的なテーマである存在性と分類問題について、他分野との関連を視野に入れて、取り組むことを研究の目的とする。

特に、整数論との関係も深い unimodular lattice や、組合せデザイン、Hadamard 行列を中心とした組合せ構造との関連を重視するのはもちろんのこと、self-dual code の新たな研究対象への応用（関連）を確立することに取り組む。また、最近、暗号理論への応用が見つかった linear complementary dual (LCD) code や代数的符号理論の範疇に留まらずに新たな応用や実用化が期待される quantum code（量子符号）などの研究にも取り組み、新たなる展開を目指して代数的符号理論の総合的な研究を行うことを研究の目的とする。

３．研究の方法

本研究課題では、self-dual code の構成、optimal unimodular lattice の構成および LCD code の分類や特徴づけに取り組むことで代数的符号理論の総合的な研究を行った。

組合せデザインや Hadamard 行列などの組合せ構造の研究に code を用いることは古くから行われてきたが、新しい研究手法として ternary self-dual code を用いた Hadamard 行列の研究成果を得ることが出来た。

研究組織のメンバーとの継続的な連携を基盤に、代数的な理論整備の後に研究対象を計算機上で実現して結果を得る方法と、計算機による実験結果より代数的な理論構築を行う方法の両軸により、研究を遂行した。

４．研究成果

まず、本研究課題の主な対象である self-dual code について、これまでの研究代表者が行って来た研究の延長として、誤り訂正能力の高い最小重みの大きな self-dual code の構成を精力的に行って来た。これまでに知られていなかった最小重みが２０である doubly even self-dual code の構成をすることが出来た。s-extremal とよばれる singly even self-dual code の構成にも成功している。また、新たな extremal Type II Z_{2k}-code の構成を行った。それだけでなく最小重みの大きな self-dual code を構成することで optimal unimodular lattice の構成も行うことが出来た。構成だけでなく ternary self-dual code、quaternary Hermitian self-dual code の重み多項式に関して組合せ論的な考察を行うことで新たな制限を与えることが出来た。さらに、重み多項式のどの可能性について実際に self-dual code が存在するかの考察も行った。この研究では、組合せ論的なアプローチが非常に役立った。

組合せデザインや Hadamard 行列などの組合せ構造の研究を code に関連付けて行うことは E.F. Assmus Jr.などによって古くから活発に行われている組合せ構造の研究の手法の一つである。V.D.Tonchev (2022) による長さ３６の Pless symmetry code と Paley

Hadamard 行列の研究に刺激を受けて、Hadamard 行列の ternary self-dual code を用いた新たな特徴づけを行った。例えば Nebe-Villar (2013) で与えられた新たな ternary self-dual code の系列が Hadamard 行列を含むことを証明した。また、長さ３６の ternary self-dual code で Hadamard 行列を含むことが計算機を用いて確認された。

1992 年に J.L. Massey によって導入された linear complementary dual (LCD) code は当初はそれほど注目をされなかった code のクラスであったが Carlet-Guilley (2018) で暗号理論の応用が見つかり、それ以降、活発に研究が行われている。これまで研究代表者は研究の対象としていなかったが、本研究課題において、研究を本格化することが出来たのは評価したい。具体的には、binary LCD codes、ternary LCD code、quaternary Hermitian LCD code に着目して構成、分類、特徴づけを行うことが出来た。また、その応用として、新たな optimal entanglement-assisted quantum code（量子符号の一種）の構成を LCD code から行うことも出来た。LCD code は self-dual code と共に今後の研究の２本柱になると考えている。

５．主な発表論文等

〔雑誌論文〕　計17件（うち査読付論文　17件／うち国際共著　1件／うちオープンアクセス　1件）

１．著者名 Makoto Araya、Harada Masaaki、Vladimir Tonchev	４．巻 31
２．論文標題 Hadamard matrices of orders 60 and 64 with automorphisms of orders 29 and 31	５．発行年 2024年
３．雑誌名 The Electronic Journal of Combinatorics	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.37236/12249	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Harada Masaaki、Ishizuka Keita	４．巻 347
２．論文標題 Hadamard matrices of order 36 formed by codewords in some ternary self-dual codes	５．発行年 2024年
３．雑誌名 Discrete Mathematics	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.disc.2023.113661	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 Araya Makoto、Harada Masaaki	４．巻 91
２．論文標題 Some restrictions on the weight enumerators of near-extremal ternary self-dual codes and quaternary Hermitian self-dual codes	５．発行年 2023年
３．雑誌名 Designs, Codes and Cryptography	６．最初と最後の頁 1813～1843
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10623-022-01172-7	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 Araya Makoto、Harada Masaaki、Momihara Koji	４．巻 91
２．論文標題 Hadamard matrices related to a certain series of ternary self-dual codes	５．発行年 2022年
３．雑誌名 Designs, Codes and Cryptography	６．最初と最後の頁 795～805
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10623-022-01127-y	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 Harada Masaaki	4．巻 87
2．論文標題 Construction of extremal Type II Z2k-codes	5．発行年 2023年
3．雑誌名 Finite Fields and Their Applications	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.ffa.2022.102154	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 Harada Masaaki	4．巻 346
2．論文標題 Self-dual codes over F5 and s-extremal unimodular lattices	5．発行年 2023年
3．雑誌名 Discrete Mathematics	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.disc.2022.113126	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 Araya Makoto、Harada Masaaki	4．巻 14
2．論文標題 On the classification of quaternary optimal Hermitian LCD codes	5．発行年 2022年
3．雑誌名 Cryptography and Communications	6．最初と最後の頁 833～847
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s12095-021-00552-5	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 Araya Makoto、Harada Masaaki、Saito Ken	4．巻 76
2．論文標題 On the minimum weights of binary LCD codes and ternary LCD codes	5．発行年 2021年
3．雑誌名 Finite Fields and Their Applications	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.ffa.2021.101925	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 Harada Masaaki	4．巻 89
2．論文標題 Construction of binary LCD codes, ternary LCD codes and quaternary Hermitian LCD codes	5．発行年 2021年
3．雑誌名 Designs, Codes and Cryptography	6．最初と最後の頁 2295～2312
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10623-021-00916-1	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 Araya Makoto、Harada Masaaki、Saito Ken	4．巻 89
2．論文標題 Characterization and classification of optimal LCD codes	5．発行年 2021年
3．雑誌名 Designs, Codes and Cryptography	6．最初と最後の頁 617～640
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10623-020-00834-8	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 －

1．著者名 Harada Masaaki	4．巻 13
2．論文標題 On the existence of s-extremal singly even self-dual codes	5．発行年 2020年
3．雑誌名 Discrete Mathematics, Algorithms and Applications	6．最初と最後の頁 2150014～2150014
掲載論文のDOI（デジタルオブジェクト識別子） 10.1142/S1793830921500142	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 Harada Masaaki	4．巻 5
2．論文標題 Construction of s-extremal optimal unimodular lattices in dimension 52	5．発行年 2020年
3．雑誌名 International Journal of Computer Mathematics: Computer Systems Theory	6．最初と最後の頁 87～91
掲載論文のDOI（デジタルオブジェクト識別子） 10.1080/23799927.2020.1755367	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 Araya Makoto、Harada Masaaki、Saito Ken	4．巻 66
2．論文標題 Quaternary Hermitian Linear Complementary Dual Codes	5．発行年 2020年
3．雑誌名 IEEE Transactions on Information Theory	6．最初と最後の頁 2751～2759
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2019.2949040	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 Harada Masaaki、Saito Ken	4．巻 159-160
2．論文標題 Remark on subcodes of linear complementary dual codes	5．発行年 2020年
3．雑誌名 Information Processing Letters	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.ipl.2020.105963	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 Araya Makoto、Harada Masaaki	4．巻 12
2．論文標題 On the minimum weights of binary linear complementary dual codes	5．発行年 2019年
3．雑誌名 Cryptography and Communications	6．最初と最後の頁 285～300
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s12095-019-00402-5	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 Harada Masaaki	4．巻 14
2．論文標題 New doubly even self-dual codes having minimum weight 20	5．発行年 2020年
3．雑誌名 Advances in Mathematics of Communications	6．最初と最後の頁 89～96
掲載論文のDOI（デジタルオブジェクト識別子） 10.3934/amc.2020007	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 Harada Masaaki	4．巻 17
2．論文標題 Some optimal entanglement-assisted quantum codes constructed from quaternary Hermitian linear complementary dual codes	5．発行年 2019年
3．雑誌名 International Journal of Quantum Information	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1142/S0219749919500539	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0件

〔図書〕　計0件

〔産業財産権〕

〔その他〕

－

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
研究分担者	宗政　昭弘 (Munemasa Akihiro) (50219862)	東北大学・情報科学研究科・教授 (11301)	
研究分担者	大浦　学 (Oura Manabu) (50343380)	金沢大学・数物科学系・教授 (13301)	

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			
米国	Michigan Technological University			