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 １８ 日現在

機関番号：１１３０１
研究種目：基盤研究(B)
研究期間：2011～2014
課題番号：２３３４００２１

研究課題名（和文）代数的符号理論の新展開を目指して

研究課題名（英文）A New Development 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）　　12,600,000円

研究成果の概要（和文）：代数的符号理論、その中でも特に代数的な研究が古くから多く行なわれている self-dual code の研究を行った。特に、長さ 36 の self-dual codeの分類および長さ40 doubly even self-dual code の分類を完成させることが出来た。また、extremal self-dual Z2k-code の構成にも取り組んだ。

研究成果の概要（英文）：In this research project, I studied algebraic coding theory, especially, self-dual codes. As results, classifications of self-dual codes of length 36 and doubly even self-dual codes of length 40 are completed. Also, I considered the construction of extremal self-dual Z2k-codes.

研究分野：代数的符号理論

キーワード：組合せ論　代数的符号理論　自己双対符号　格子

１．研究開始当初の背景

符号理論は 1948 年の Shannon の論文に端を発し、誤りが発生する可能性のあるデジタル通信路においてある程度の誤りであれば訂正することが出来ることを保証するための理論である。起源は情報科学であるが、その後、豊富な数学的な理論を有することが分かった。

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、代数的な立場(手法) で研究を行な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 (自己双対符号) があり、代数的および組合せ論的な研究が活発に行なわれていたので、本研究課題でも self-dual code の研究の発展を目指す。

２．研究の目的

代数的符号理論、その中でも特に代数的な研究が古くから多く行なわれており、研究代表者が今までに中心的に研究を行なって来た、self-dual code の研究を、整数論との関係も深い対象の unimodular lattice の研究と関連付けて行なうことを本研究の中心的な柱とする。

また、従来の代数的符号理論とは全く異なる手法での研究が行なわれている quantum code (量子符号) などの新しい研究対象への応用(関連) を確立することで代数的符号理論における新たなる発展を目指す。

３．研究の方法

(1) Self-dual code の構成と分類、self-dual code による unimodular lattice の研究：

self-dual code の構成と分類は、基本的なテーマではあるが code 自身が非常に簡単な構造をしていることから離散数学を始めとして多くの他の分野との結びつきがあり、符号理論だけに留まらず他の分野との関連性で非常に威力を発揮する重要なテーマである。

まず、他の分野との関連を意識し self-dual code の分類に、分類方法の精密化、計算の高速化を図りながら取り組む。その際に、self-dual code の分類のように、符号理論や組合せ論の研究では、代数的な理論整備の後、研究対象を計算機上で実現して結果を得ることも多く、計算機による計算を実行することは本研究の特徴的な方法の一つである。構成については、code のパラメータとして最も重要である minimum weight が最大となる extremal self-dual code が対象となる。長さ 72 の binary extremal doubly even code の存在性は決定されておらず、代数的符号理論の有名な未解決問題の一つになっている。unimodular lattice の frame とよばれる内積に関するある種の性質をもつ部分集合に着目して、Z_{2k} 上の extremal self-dual code の構成を試みる。

(2) Quantum code などの代数的符号理論的な研究：

通常の誤りに(古典的な) 符号理論が必要であったように、例えば、量子通信を行なう際に量子誤りを訂正するためには quantum code (量子符号) の研究が必要となる。1990 年代から量子力学的な手法による quantum code の研究が行なわれている。従来の代数的符号理論とは全く異なる手法での研究が中心的に行なわれており、本研究では、代数的符号理論の立場で行なうことで、代数的符号理論の新展開を目指す。

４．研究成果

(1) Self-dual code の構成と分類、self-dual code による unimodular lattice の研究：

他の分野との関連を意識した self-dual code の分類結果について述べる。まず binary self-dual code には doubly even self-dual code（Type II code ともよばれる）という特別なクラスがあり、長さが 8 の倍数のときのみに存在し、代数的にも組合せ論的にも良い性質をもつ。doubly even self-dual code の分類は長さ 32 まで、self-dual code 全体の分類は長さ 34 まで完成していた。本研究課題では、分類方法の精密化や計算の高速化を図ることで、まず、長さ 36 の self-dual code の分類を完成させることが出来た。さらに別の分類方法を構築することで長さ 40 の doubly even self-dual code の分類を完成させることが出来た。長さの 32 の分類は 1993 年に Conway 達によって完成されたが、彼らの分類から 20 年近く経って長さ 40 の分類を進展させることが出来たことは特筆すべき結果である。その後、この分類から得られる他の組合せ構造の考察を行なったが、特に、長さ 40 の extremal singly even self-dual code の分類問題をこの分類結果に帰着させることが出来、その分類を完成させることが出来た。別の視点からの分類結果としては、２重可移群を自己同型群にもつ extremal doubly even self-dual code の分類も得た。

符号理論において optimal である code の存在、分類は基本的な問題である。上記に述べた self-dual code とは異なる題材ではあるが、幅広く研究を進めるために、今回、この問題にも取り組み、具体的な成果としては 5 元体での存在の分かっていなかった optimal 符号の中で最少の長さである [21,5,14] code が存在しないことを確かめた。

本研究で取り組む主な課題の一つとして extremal self-dual $\mathbf{Z}_{2k}$-code の構成が挙げられるが、これは unimodular lattice のフ

レームとよばれるある種の部分集合を構成する方法を確立することで進展が得られた。具体的には 8 の倍数である長さ 64 以下において、全ての k に対して extremal Type II $\mathbb{Z}_{2k}$-code が存在することを示すことが出来た。extremal Type II $\mathbb{Z}_{2k}$-code は binary doubly even self-dual code を含む一般的な self-dual code のクラスである。また、ここで得られた手法をさらに発展させることで、長さ 48 以下の Type II ではない extremal self-dual $\mathbb{Z}_{2k}$-code の存在に関しての新たな結果を得た。ここでも unimodular lattice のフレームの構成が重要な役割を演じており、self-dual code の研究に unimodular lattice が非常に役立った一例となっている。また、逆な視点として、ある種の長さ 36 の binary code と self-dual Z_4-code の構成に帰着させることで、36 次元の extremal unimodular lattice の構成を行った。

(2) Quantum code などの代数的符号理論的な研究：
quantum（stabilizer）code の構成には、(linear とは限らない)位数 4 の有限体上の additive self-orthogonal code を考えれば良いことが 1998 年の Calderbank などの結果によって分かっている。本研究においては、研究代表者が今までに行って来た代数的符号理論の研究で培った self-dual code の構成方法を位数 4 の有限体上の additive self-dual code に適用させることで（構成した時点で）知られていた誤り訂正能力を更新するパラメータをもつ quantum [[56,0,15]] code と quantum [[57,0,15]] code を含む quantum code の構成を行うことが出来た。これらの２つの quantum code は、現在でも知られている[[56,0]] code と [[57,0]] code において最大の誤り訂正能力をもつ code であり、データベース「Code Tables（http://www.codetables.de/）」にてその結果が記載されている。

(3) その他：
本研究において計算機を用いた研究は主に代数計算ソフト Magma を用いて行ったが、Magma を用いた代数系の研究発展のために、研究集会「Magma で開く数学の世界」を２０１２年７月に高知大学にて主催し、講演者の旅費などの援助を行うことで開催を支援した。また研究期間を通じて、毎年度、本研究と密接な関係のある「代数的組合せ論シンポジウム」（毎年６月開催）および「応用数学合同研究集会」（毎年１２月開催）において連携研究者を始めとして講演者の旅費などの援助などで両イベントの開催支援を行うことで代数的符号理論の発展に貢献した。

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１０件）

① M. Harada, On a 5-design related to a putative extremal doubly even self-dual code of length a multiple of 24, *Designs, Codes and Cryptogr.*, 査読有, (2015) 印刷中
DOI 10.1007/s10623-014-9963-3

② M. Harada, Extremal Type I $\mathbb{Z}_k$-codes and k-frames of odd unimodular lattices, *IEEE Trans. Inform. Theory*, 査読有, **61** (2015) 72-81
DOI 10.1007/s10623-014-9963-3

③ M. Harada, Extremal unimodular lattices in dimension 36, *Inter. J. Combinatorics*, 査読有, **2014** (2014) 1-7
DOI 10.1155/2014/792471

④ M. Harada, C.H. Lam, A. Munemasa, Residue codes of extremal Type II $\mathbb{Z}_4$-codes and the moonshine vertex operator algebra, *Math. Zeitschrift*, 査読有, **274** (2013) 685-700
DOI 10.1007/s00209-012-1091-z

⑤ M. Araya, M. Harada, There is no [21, 5, 14] code over $\mathbb{F}_5$, *Discrete Math.*, 査読有, **313** (2013) 2872-2874
DOI 10.1016/j.disc.2013.08.027

⑥ N. Chigira, M. Harada, M. Kitazume, On the classification of extremal doubly even self-dual codes with 2-transitive automorphism groups, *Designs, Codes and Cryptogr.*, 査読有, **73** (2014) 33-35
DOI 10.1007/s10623-013-9807-6

⑦ M. Harada, T. Miezaki, On the existence of extremal Type II $\mathbb{Z}_{2k}$-codes, *Math. Computation*, 査読有, **73** (2014) 33-35
DOI 10.1090/S0025-5718-2013-02750-0

⑧ S. Bouyuklieva, I. Bouyukliev, M. Harada, Some extremal self-dual codes and unimodular lattices in dimension 40, *Finite Fields Their Appl.*, 査読有, **21** (2013) 67-83
DOI 10.1016/j.ffa.2013.01.009

⑨ K. Betsumiya, M. Harada, A. Munemasa, A complete classification of doubly even self-dual codes of length 40, *Electronic J. Combin.*, 査読有, **19** (2012) #P18
http://www.combinatorics.org/ojs/ind

ex.php/eljc/article/view/v19i3p18/pdf

⑩ M. Harada, A. Munemasa, Classification of self-dual codes of length 36, *Advances Math. Com.*, 査読有, **6** (2012) 229-235
DOI 10.3934/amc.2012.6.229

〔学会発表〕（計４件）

① 原田昌晃、Self-dual code とその周辺、日本数学会 2013 年度秋季総合分科会、２０１３年9月２４日、愛媛大学（愛媛県）

② 原田昌晃、Magma へ貢献できること、Magma で開く数学の世界、２０１２年7月２２日、高知大学（高知県）

③ 原田昌晃、Unimodular lattices with long shadows、離散数理構造とその応用、２０１１年１１月１８日、名古屋大学（愛知県）

④ 宗政昭弘、Frames of the Leech lattice、Workshop on Algebraic Combinatorics、２０１１年9月１５日、上海交通大学（中国）

６．研究組織

(1)研究代表者
原田　昌晃（HARADA, MASAAKI）
東北大学・大学院情報科学研究科・教授
研究者番号：90292408

(2)研究分担者
宗政　昭弘（MUNEMASA, AKIHIRO）
東北大学・大学院情報科学研究科・教授
研究者番号： 50219862

(3)連携研究者
北詰　正顕（KITAZUME, MASAAKI）
千葉大学・大学院理学研究科・教授
研究者番号：60204898

和田山　正（WADAYAMA, TADASHI）
名古屋工業大学・大学院工学研究科・教授
研究者番号：20275374

新谷　誠（ARAYA, MAKOTO）
静岡大学・情報学部・准教授
研究者番号：70303526

萩原　学（HAGIWARA, MANABU）
千葉大学・大学院理学研究科・准教授
研究者番号：80415728