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　元 年　 ５ 月 ２７ 日現在

機関番号：１１３０１
研究種目：基盤研究(B)（一般）
研究期間：2015～2018
課題番号：１５Ｈ０３６３３

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）Comprehensive research on 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）　　11,500,000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 singly even self-dual code の存在および非存在問題に関する成果が得られた。
当初、研究の対象としていなかった、近年、暗号理論などへの応用により注目を浴びつつある linear complementary dual code についての研究成果も得ることが出来た。

研究成果の学術的意義や社会的意義
代数的符号理論は、誤りの発生する可能性のある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である符号を代数的な立場で研究を行った。組合せ構造の研究において、基本的な課題である良い符号の構成と分類についての成果を得ることが出来たことが本研究における学術的な意義である。また、暗号理論との関連のある符号についての研究成果も得ることが出来た。

研究成果の概要（英文）：In this research project, I studied algebraic coding theory, especially, self-dual codes. I obtained results about the existence and the nonexistence of singly even self-dual codes.
Moreover, I obtained results about linear complementary dual codes. These codes are a class of linear codes which are related to cryptography.

研究分野：離散数学、組合せ論、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　組合せデザイン

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

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。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。その中でも self-dual code は代数的な研究が古くから多く行われており、また研究代表者が今までに中心的に研究を行って来た研究対象である。また self-dual code は、design などの様々な組合せ構造、有限群論、整数論の対象でもある unimodular lattice との関連を重視して研究が行われてきた。

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。本研究では、研究代表者が今までに精力的に研究を行って来た self-dual code を中心とした研究を、特に整数論との関係も深い unimodular lattice や design などの組合せ構造との関連を重視して行う。さらに、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ことで新たなる発展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目的とする。self-dual code との関連の有効性は十分に分かっている unimodular lattice や design などの対象に限らず新たな研究対象に対して、研究代表者が今までに行って来た self-dual code を中心とした代数的符号理論の研究を応用させるだけでなくそれらの研究対象の研究過程から新たな代数的符号理論の研究テーマの開発を行うことで、それぞれの分野を互いに発展させることの出来るような双方向の貢献が行えるように取り組むことを目標とし、またこれが本研究の特色である。

３．研究の方法

本研究では、self-dual code の分類や構成および optimal unimodular lattice の構成に取り組み、また、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、代数的符号理論の総合的な研究を行った。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

組合せ構造の研究において、対象とする組合せ構造の分類問題は、基本的でありかつ今後の研究の発展へのステップとなる重要な課題であると言える。研究代表者がこれまでに行って来た self-dual code の分類・構成手法の精密化、一般化を図り、有限体上だけに限らず様々なタイプの self-dual code の分類および構成に取り組んだ。まず、長さ９０から９６の extremal double circulant self-dual code の分類を完成させることが出来た。また、Z4-code の分類について取り組み、長さ７までの分類を完成させることが出来た。

本研究課題の主な対象である extremal doubly even self-dual code については、被覆半径という概念について調べることで s-extremal singly even self-dual code との関係を確立させることに成功した。また、minimal shadow をもつ binary singly even self-dual code の構成および非存在に関する結果を得た。さらに design との関係を考察するためにある種の design から得られる長さ１２８の self-dual code についてその重さ分布を代数的な手法を用いて決定することが出来た。

研究代表者の研究成果である長さ４０の doubly even self-dual code の分類を用いて、quasi-symmetric 2-(37,9,8) design の非存在を証明することが出来た。新たな code と design の関連を構築出来た。

今までに扱っていなかった符号のクラスである量子符号への応用を動機として、新たな位数４の有限体上の additive self-dual code で今までに達成していなかった最小重さを持つものの構成に成功した。

これまで研究の対象としていなかった、近年、暗号理論などへの応用により注目を浴びつつある linear complementary dual code についての研究に本研究で初めて取り掛かり、幾つかの成果を得ることも出来たので、今後の研究につなげたい。

５．主な発表論文等

〔雑誌論文〕（計　２２件）

(1) Masaaki Harada, New doubly even self-dual codes having minimum weight 20, Advances Math. Communications,（印刷中）[査読有]
(2) T. Aaron Gulliver and Masaaki Harada, On extremal double circulant self-dual codes of lengths 90-96, Applicable Algebra in Eng. Communi. Comput.,（印刷中）[査読有]
(3) Masaaki Harada and Ken Saito, Binary linear complementary dual codes, Cryptography and Communications,（印刷中）[査読有]
(4) Masaaki Harada, Singly even self-dual codes of length 24k+10 and minimum weight 4k+2,

Cryptography and Communications, (印刷中) [査読有]
(5) Makoto Araya and Masaaki Harada, On the classification of linear complementary dual codes, Discrete Math. 342 (2019), 270-278, 10.1016/j.disc.2018.09.034 [査読有]
(6) Damyan Anev, Masaaki Harada and Nikolay Yankov, New extremal singly even self-dual codes of lengths 64 and 66, J. Algebra Comb. Discrete Struct. Appl. 5 (2018), 143-151, 10.13069/jacodesmath.458601 [査読有]
(7) Masaaki Harada and Akihiro Munemasa, Some restrictions on weight enumerators of singly even self-dual codes II, Interdiscip. Inform. Sci. 24 (2018) 77-85, 10.4036/iis.2017.R.03 [査読有]
(8) Masaaki Harada, New quantum codes constructed from some self-dual additive F4-codes, Information Processing Letters 138 (2018) 35-38, 10.1016/j.ipl.2018.05.008 [査読有]
(9) Masaaki Harada, Binary extremal self-dual codes of length 60 and related codes, Designs, Codes and Cryptogr. 86 (2018) 1085-1094, 10.1007/s10623-017-0380-2 [査読有]
(10) Stefka Bouyuklieva, Masaaki Harada and Akihiro Munemasa, Nonexistence of certain singly even self-dual codes with minimal shadow, Electronic J. Combin. 25 (2018), #P1.13, https://www.combinatorics.org/ojs/index.php/eljc/article/view/v25i1p13 [査読有]
(11) Makoto Araya, Masaaki Harada and Yuichi Suzuki, Ternary maximal self-orthogonal codes of lengths 21, 22 and 23, J. Algebra Comb. Discrete Struct. Appl. 5 (2018), 1-4, 10.13069/jacodesmath.327391 [査読有]
(12) Masaaki Harada and Ken Saito, Singly even self-dual codes constructed from Hadamard matrices of order 28, Australasian J. Combin. 70 (2018), 288-296, https://ajc.maths.uq.edu.au/pdf/70/ajc_v70_p288.pdf [査読有]
(13) Makoto Araya, Masaaki Harada, Hiroki Ito and Ken Saito, On the classification of Z4-codes, Advances Math. Communications 11 (2017), 747-756, 10.3934/amc.2017054 [査読有]
(14) T. Aaron Gulliver and Masaaki Harada, On the performance of optimal double circulant even codes, Advances Math. Communications 11 (2017), 767-775, 10.3934/amc.2017056 [査読有]
(15) T. Aaron Gulliver and Masaaki Harada, Performance of ternary double circulant, double twistulant, and self-dual codes, Applicable Algebra in Eng. Communi. Comput. 28 (2017), 409-424, 10.1007/s00200-017-0312-4 [査読有]
(16) Masaaki Harada and Akihiro Munemasa, On s-extremal singly even self-dual [24k+8,12k+4,4k+2] codes, Finite Fields and Their Applications 48 (2017), 306-317, 10.1016/j.ffa.2017.08.008 [査読有]
(17) Masaaki Harada, Akihiro Munemasa and Vladimir D. Tonchev, Self-dual codes and the non-existence of a quasi-symmetric 2-(37,9,8) design with intersection numbers 1 and 3, J. Combin. Designs 25 (2017), 469-476, 10.1002/jcd.21556 [査読有]
(18) Masaaki Harada, Extremal Type II Z4-codes constructed from binary doubly even self-dual codes of length 40, Discrete Math. 340 (2017), 2466-2468, 10.1016/j.disc.2017.06.009 [査読有]
(19) Makoto Araya, Masaaki Harada and Sho Suda, Supplementary difference sets related to a certain class of complex spherical 2-codes, Australasian J. Combin. 65 (2016), 71-83, https://ajc.maths.uq.edu.au/pdf/65/ajc_v65_p071.pdf [査読有]
(20) Masaaki Harada, Ethan Novak and Vladimir D. Tonchev, The weight distribution of the self-dual [128,64] polarity design code, Advances Math. Communications 10 (2016), 643-648, 10.3934/amc.2016032 [査読有]
(21) Markus Grassl and Masaaki Harada, New self-dual additive F4-codes constructed from circulant graphs, Discrete Math. 340 (2017), 399-403, 10.1016/j.disc.2016.08.023 [査読有]
(22) Masaaki Harada and Akihiro Munemasa, On the classification of self-dual Zk-codes II, Interdiscip. Inform. Sci. 22 (2016), 81-85, 10.4036/iis.2015.R.01 [査読有]

〔学会発表〕(計　2件)
(1) 原田昌晃、On linear complementary dual codes、組合せ論的符号理論（東北大学・情報科学研究科)、２０１９年
(2) 原田昌晃、On the nonexistence of certain extremal doubly even self-dual codes、離散数学とその応用研究集会２０１６（宮城県・高城コミュニティセンター)、２０１６年

〔図書〕(計　0件)

〔産業財産権〕
○出願状況（計　0件）

名称：
発明者：
権利者：
種類：
番号：
出願年：
国内外の別：

○取得状況（計　0件）

名称：
発明者：
権利者：
種類：
番号：
取得年：
国内外の別：

〔その他〕
ホームページ等

６．研究組織

(1)研究分担者
研究分担者氏名：宗政　昭弘
ローマ字氏名：(MUNEMASA, akihiro)
所属研究機関名：東北大学
部局名：大学院情報科学研究科
職名：教授
研究者番号（8桁）：50219862

(2)研究協力者
研究協力者氏名：宮本　雅彦
ローマ字氏名：(MIYAMOTO, masahiko)

研究協力者氏名：北詰　正顕
ローマ字氏名：(KITAZUME, masaaki)

研究協力者氏名：和田山　正
ローマ字氏名：(WADAYAMA, tadashi)

研究協力者氏名：新谷　誠
ローマ字氏名：(ARAYA, makoto)

研究協力者氏名：別宮　耕一
ローマ字氏名：(BETSUMIYA, koichi)

研究協力者氏名：大浦　学
ローマ字氏名：(OURA, manabu)

研究協力者氏名：島倉　裕樹
ローマ字氏名：(SHIMAKURA, hiroki)

研究協力者氏名： 田中　太初
ローマ字氏名：（TANAKA, hajime）

研究協力者氏名：須田　庄
ローマ字氏名：（SUDA, sho）