様式 C-19

科学研究費補助金研究成果報告書

平成２３年４月１５日現在

機関番号：１１５０１
研究種目：基盤研究（C）
研究期間：２００８～２０１０
課題番号：２０５４０１０３
研究課題名（和文）　代数的符号理論と組合せデザイン

研究課題名（英文）　Algebraic coding theory and combinatorial designs

研究代表者
原田　昌晃（HARADA MASAAKI）
山形大学・理学部・准教授
研究者番号：90292408

研究成果の概要（和文）：本研究では、代数的符号理論、特に代数的な研究が古くから行なわれている self-dual code についての研究を行なって来た。特に、基本的な問題である self-dual code の分類についての研究を色々なアプローチによって行なった。また、self-dual code の中でも最小重さがその長さで最大となる extremal self-dual code の構成も行なった。組合せ論の一つの分野である design についての研究についても self-dual code と関連付けることで行なってきた。
研究成果の概要（英文）：The main aim of this research is to study self-dual codes, which are of interest from an algebraic point of view. In self-dual codes, it is a fundamental problem to classify these codes. We completed classifications of several types of self-dual codes using some different approaches. We constructed extremal self-dual codes which have the largest minimum weights among all self-dual codes of that length. Using self-dual codes, we also studied combinatorial designs.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008年度	1,300,000	390,000	1,690,000
2009年度	1,000,000	300,000	1,300,000
2010年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,300,000	990,000	4,290,000

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：組合せ論、自己双対符号、組合せデザイン、格子

１．研究開始当初の背景

代数的符号理論は、代数的組合せ論の一つの分野であり、情報科学とも深い関わりをもった応用代数学の一分野でもある。近年、離散数学を始めとする他の諸分野との関連が注目されている。
本研究では self-dual code や組合せ論の一つの分野である design についての研究を self-dual code と関連付けて行なうことを目的としているが、研究開始当初の背景について、次の３つのテーマに分けて、説明をする。
（１）「extremal self-dual code の構成および分類」
まず doubly even self-dual code の weight enumerator はある有限群の不変式環に属することなどから、長さが 8 の倍数において doubly even self-dual code が存在することが分かり、code の最も重要なパラメータである最小重さについての上限が得られる。こ

の上限に一致する場合を extremal と呼ぶ。長さ 64 以下においては extremal doubly even self-dual code が少なくとも一つは存在することが分かっているが、長さ 72 においては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。

（２）「code を利用した self-orthogonal design などの t-design の研究」
design の研究においては、その結合行列を通して code を利用するということは古くから行なわれていた。Tonchev は 1980 年代に Witt design に関係した design の特徴付けを行なうことに、Golay [24,12,8] code とそれに関係した code に帰着させることで成功した。その当時に比べて分類などの self-dual code の研究は確実に進歩しているので、組合せ論全般に渡って非常に特徴的である 24 次元に限らず他の場合においても同様な研究が行なわれている。

（３）「有限単純群を自己同型群としてもつ self-dual code の研究」
有限単純群の分類は 1980 年代後半に完成された。3 つの無限系列とそれらに含まれない 27 個の散在型の単純群があり、現在も主に散在型の単純群の研究が行なわれている。散在型単純群の一つである 24 次のマシュー群 M_{24} は Golay [24,12,8] code の自己同型群に一致することが古くから知られており、Golay code の性質が M_{24} の構造を調べるのに役立った。なお、この Golay code は self-dual code になることを注意しておく。

２．研究の目的
本研究では、代数的符号理論、特に代数的な研究が古くから行なわれている self-dual code についての研究と、組合せ論の一つの分野である design についての研究を self-dual code と関連付けて行なうことを目的とする。「研究開始当初の背景」の欄で述べた３つのテーマにそって説明をする。

（１）「extremal self-dual code の構成および分類」
長さ 72 の extremal doubly even self-dual code の存在性は決定されておらず、有名な未解決問題となっているが、この code の存在と self-orthogonal 5-(72, 16, 78) design の存在が同値であることが分かっている。30 年以上も未解決であるこの問題が簡単に解決されるとは思ってはいないが、この存在についての同値性を利用し、長さ 72 の extremal doubly even self-dual code の存在に関するある種の特徴付けを行なう。
また self-dual code の分類を行なうことは、基本的な問題であり幾つかのアルファベットに対して、それぞれ self-dual code の分類を進めていく。特に、GF(3) 上の長さ 28 の extremal self-dual code は 28 次元の optimal unimodular lattice の 3-frame と呼ばれるある部分集合に対応していることが分かっている。これらの lattice の分類を利用して長さ 28 の extremal self-dual code の分類を完成させる。

（２）「code を利用した self-orthogonal design などの t-design の研究」
design において古くから研究されている quasi-symmetric などの self-orthogonal design の構成や分類を self-dual code の構成や分類に帰着させながら行なう。特に、存在の分かっていない quasi-symmetric 2-design の構成などを目的とする。

（３）「有限単純群を自己同型群としてもつ self-dual code の研究」
最近、幾つかの散在型単純群を自己同型群（またはその部分群）としてもつ self-dual code を構成した。自己同型群として得られる単純群の構造を理解するために、構成された self-dual code の性質を調べる。

３．研究の方法
「研究開始当初の背景」の欄で述べた３つのテーマにそって研究の方法の説明をする。

（１）「extremal self-dual code の構成および分類」
長さ 72 の extremal doubly even self-dual code の存在と self-orthogonal 5-(72, 16, 78) design の存在が同値であることが分かっている訳であるが、この design に着目をして code の存在性について調べていく。このアプローチは本研究における２つ目のテーマである design に関する研究とも関連するものである。今までに存在の分かっていない長さ 128 の extremal doubly even self-dual code の構成にも取り組む。
また、self-dual code の分類については、まずは GF(3) 上の長さ 28 の extremal self-dual code は 28 次元の optimal unimodular lattice の 3-frame を分類することでその分類を完成させる。この方法をさらに一般化させることで、その他のアルファベットでの self-dual code の分類を行なう。また、すでに知られている分類方法を精査することにより、新たな、効率良い分類方法の確立を目指し、分類を進めていく。

（２）「code を利用した self-orthogonal design などの t-design の研究」
quasi-symmetric などの self-orthogonal

design の構成や分類を self-dual code の構成や分類に帰着させながら行なう。また、通常の t-design だけに限らず、アダマール行列などのその他のタイプの design についても同様な研究を行なう。その際には、最近行なった位数 62 と 74 の circulant D-optimal design の分類で得られたことを役立たせる。

（３）「有限単純群を自己同型群としてもつ self-dual code の研究」
24 次のマシュー群 M_{24} を自己同型群としてもつ Golay code に対して行なわれている考察と同様なことを行なう。特に、最近構成した幾つかの散在型単純群を自己同型群としてもつ self-dual code に対して、各重さのベクトルの集合の組合せ構造に関する考察を行なう。

４．研究成果
本研究では、代数的符号理論、特に代数的な研究が古くから行なわれている self-dual code についての研究を行なった。主に次の４つの研究成果を得られたので、その報告をする。

（１）基本的な問題である self-dual code の分類について、一定の成果を得ることが出来た。まず、unimodular lattice の分類問題に帰着させることで、self-dual code の分類を行なった。具体的には unimodular lattice の frame と呼ばれるある種の部分集合を分類することが素数位数の有限体と整数の剰余環 Z_k 上の self-dual code の分類を導くことを利用して、実際にまだ分類が完成していない場合において分類を本研究経費で購入した高速な計算機を用いて行なった。さらに、self-dual code の分類問題については、上記とは異なる方法で長さ 36 の self-dual code と GF(4) 上の長さ 18 と 20 の self-dual code の分類を完成させることが出来た。

（２）24 次元の unimodular lattice に関係して次の２つの結果を得た。まず GF(5)上の self-dual [24,12,10] code の非存在の証明を unimodular lattice の 5-frame の考察によって行った。また、同型を除いて 24 個あることが知られている even lattice である Niemeier lattice の有限体上の self-dual code による構成を行なった。

（３）同じブロックを持たない design は互いに素であるとよばれる。互いに素な S(5,8,24) などの 5-design の構成を本研究経費で購入した高速な計算機を用いて行なった。構成された互いに素なデザインから今までに存在の知られていなかったパラメータを持つ 5-design の構成も行なった。
また、self-dual code に関係した組合せデザインの分類や特徴付けも行なった。特に、位数 32 のアダマール行列について GF(3) 上の extremal self-dual code の立場からの特徴付けを行なうことが出来た。（１）で行なった GF(4) 上の長さ 18 の self-dual code の分類を用いて一般化アダマール行列 H(6, 3) の分類も行なった。

（４）長さ 72 の extremal doubly even self-dual code の存在性については未だに決定されておらず、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。Z_{2k} 上の長さ 72 の extremal Type II code を定義することが出来るが、特に k=1 の場合が上で挙げた存在の決定されていない extremal doubly even self-dual code となる。k=1 を含めて一般の k に対してその存在性を調べた。72 次元の extremal even unimodular lattice の存在に関連づけることで、k が 4 以上の偶数の場合に長さ 72 の extremal Type II code の存在性を示すことが出来た。

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] A. Munemasa and V.D. Tonchev, The twisted Grassmann graph is the block graph of a design, Innov. Incidence Geom. [掲載決定]（査読有）

[2] M. Harada and A. Munemasa, Classification of quaternary Hermitian self-dual codes of length 20, IEEE Trans. Inform. Theory [掲載決定]（査読有）

[3] M. Harada, Extremal Type II Z_4-codes of lengths 56 and 64, J. Combin. Theory Ser. A 117 (2010), 1285-1288 （査読有）

[4] M. Harada and T. Miezaki, An upper bound on the minimum weight of Type II Z_{2k}-codes, J. Combin. Theory Ser. A 118 (2010), 190-196 （査読有）

[5] M. Harada, C. Lam, A. Munemasa and V.D. Tonchev, Classification of generalized Hadamard matrices H(6, 3) and quaternary Hermitian self-dual codes of length 18, Electronic J. Combin. 17 (2010), #R171 (14

pp.）（査読有）

[6] M. Harada and A. Munemasa, On the classification of self-dual Z_k-codes, Lecture Notes Comput. Sci. 5921 (2009), 78-90.

[7] M. Harada, A. Munemasa and B. Venkov, Classification of ternary extremal self-dual codes of length 28, Mathematics of Comput. 78 (2009), 1787-1796 （査読有）

[8] M. Harada and A. Munemasa, A complete classification of ternary self-dual codes of length 24, J. Combin. Theory Ser. A 116 (2009), 1063-1072 （査読有）

[9] M. Harada, On the existence of frames of the Niemeier lattices and self-dual codes over Fp, J. Algebra 321 (2009), 2345-2352 （査読有）

[10] M. Harada and A. Munemasa, There exists no self-dual [24, 12, 10] code over F_5, Designs, Codes and Cryptogr. 52 (2009), 125-127 （査読有）

〔学会発表〕（計５件）

[1] 原田昌晃,自己双対符号とその周辺，第５５回代数学シンポジウム ２０１０年８月１２日 北海道大学

[2] 原田昌晃, Extremal Type II Z_{2k}-codes, 代数学と計算 ２００９年１２月２日 首都大学東京

[3] 宗政昭弘, Twisted Grassmann graph is the block graph of a design, Summer School on Designs and Codes ２００９年６月２１日 ヒルズサンピア山形

[4] M. Harada, On the classification of extremal Type II Z_4-codes of length 24, Korea-Japan Workshop on Algebra and Combinatorics ２００９年２月９日 Pusan National University、韓国

[5] 原田昌晃, Self-dual code の分類について，離散数学とその応用研究集会，２００８年８月２１日 茨城大学

６．研究組織

(1)研究代表者

原田　昌晃（HARADA MASAAKI）

山形大学・理学部・准教授

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

新谷　誠　（ARAYA MAKOTO）

静岡大学・情報学部・准教授

研究者番号：７０３０３５２６