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 ２８ 年　 ５ 月 １９ 日現在

機関番号：１１３０１
研究種目：挑戦的萌芽研究
研究期間：2014～2015
課題番号：２６６１００３２

研究課題名（和文）組合せデザインと格子によるある自己双対符号の存在問題の解決への試み

研究課題名（英文）Challenging of the existence problem of a certain self-dual code through combinatorial designs and lattices

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）　　2,700,000円

研究成果の概要（和文）：長さ７２の extremal doubly even self-dual code と存在が同値である self-orthogonal 5-(72,16,78) design を含む self-orthogonal design について、統一的な研究を連携研究者の宗政昭弘氏と進めた（現在、論文作成中）。
unimodular lattice の分類を用いて、self-dual Zk-codeの分類を進めた（出版準備中）。さらに complex spherical 2-code に関連した supplementary difference set についての研究も行った（出版済み）。

研究成果の概要（英文）：In this project, I studied self-orthogonal designs including a self-orthogonal 5-(72,16,78) design, where the existences of such a design and an extremal doubly even self-dual code of length 72 are equivalent, with Akihiro Munemasa.
Using the classification of unimodular lattices, I gave some classification of self-dual Zk-codes. In addition, I studied supplementary difference sets related to complex spherical 2-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　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 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。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。

代数的符号理論において重要な対象として doubly even self-dual code（重偶自己双対符号）がある。まず doubly even self-dual code が存在するためには長さは８の倍数であることが必要であり、各長さにおいて minimum weight（最小重さ）が Mallows－Sloane による上限に一致する場合、extremal（極値的）とよばれる。その存在は、代数的な動機だけに限らず様々な理由で関心が持たれており、長さ７２の未満の全ての８の倍数の長さで extremal doubly even self-dual code の存在は分かっているが、長さ７２については存在が分かっていない。1973 年にすでにこの分野の第一人者の一人である N.J.A. Sloane は解決すべき問題として挙げており、代数的符号理論における有名な未解決問題の１つとなっている。

２．研究の目的

研究代表者は、連携研究者である宗政昭弘氏らとの共同研究において長さ７２の extremal doubly even self-dual code の存在と self-orthogonal 5-(72,16,78) design（自己直交組合せデザイン）の存在が同値であることを示していた（M. Harada, M. Kitazume and A. Munemasa, On a 5-design related to an extremal doubly even self-dual code of length 72, Journal of Combinatorial Theory Ser. A 107 (2004), 143-146）。

さらに、この結果の拡張として、研究代表者は、長さ７２、９６、１２０、１４４の extremal doubly even self-dual code の各 weight の codeword がなす 5-design と同じパラメータの self-orthogonal 5-design の結合行列が生成する binary doubly even code が self-dual になるかどうか、extremal になるかどうかの考察を与えた（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. 76 (2015), 373-384）。

研究代表者らは unimodular lattice（格子）との関連に着目して k = 1 の場合が extremal doubly even self-dual code となる新たなクラスとして導入された extremal Type II $\mathbb{Z}_{2k}$-code に対して、特に、長さ７２において、k が偶数で４以上の場合にその存在を示すことが出来た（M. Harada and T. Miezaki, On the existence of extremal Type II $\mathbb{Z}_{2k}$-codes, Mathematics of Computation 83 (2014), 1427-1446）。

N.J.A. Sloane の問題提起から 40 年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、本研究課題では、上記のこれまでの研究成果を背景として、長さ 72 の extremal doubly even self-dual code の存在性の決定へ、組合せ構造である design と整数論の対象でもある unimodular lattice という両軸からアプローチを行うことを主目的とする。また、関連する design や unimodular lattice に関連した self-dual code の研究を行う。

３．研究の方法

上で述べたように、self-orthogonal 5-(72,16,78) design の存在は、長さ７２の extremal doubly even self-dual code の存在が同値であることが分かっている。この特定のパラメータについての考察を進めるのではなく、このパラメータを含むような self-orthogonal design のクラスを導入して、統一的な考察を行うことを本研究課題における方法とする。具体的には、長さ７２に限らずに extremal doubly even self-dual code の各 weight の codeword のなす self-orthogonal t-design と同じパラメータをもつ self-orthogonal t-design の結合行列がどのような code を構成するかを決定する。この過程で得られたことから self-orthogonal 5-(72,16,78) design の存在についての何らかの考察を得ることを試みる。

研究代表者らが導入した extremal Type II $\mathbb{Z}_{2k}$-code についての研究を進めることで、長さ７２の extremal doubly even self-dual code の存在性についての何らかの考察を得ることを試みる。上での述べたように、長さ７２において、k が偶数で４以上の場合に extremal Type II $\mathbb{Z}_{2k}$-code の存在を示すことが出来た。その手法は、G. Nebe によって発見された７２次元の extremal Type II lattice における 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、その存在を示すことであった。本研究課題においては、Nebe による７２次元の extremal Type II lattice の構成方法を Type II $\mathbb{Z}_{2k}$-code に応用することで、extremal な code の構成に挑戦する。特に、k=4 の場合に精力的にその構成に挑戦することで、その存在を示すことに挑戦する。その結果、k=2 の場合、つまり、長さ７２の extremal doubly even self-dual code の存在性についての何らかの考察を得ることを試みる。その際に、self-dual code の構成

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課題の特徴的な方法の一つであり、占有出来る計算機を購入して、本研究課題を遂行する。

さらに self-dual $\mathbb{Z}_k$-code の存在や分類をする際には、関連する 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することを有効であると考えており、本研究課題においても、上記の問題設定に限らずに、幅広く研究を進める。

４．研究成果

上記に述べた通り、研究代表者は、連携研究者である宗政昭弘氏らとの共同研究において長さ７２の extremal doubly even self-dual code の存在と self-orthogonal 5-(72,16,78) design（自己直交組合せデザイン）の存在が同値であることを示している。この一般化として、本研究課題においては、このパラメータを含む self-orthogonal design について、統一的な研究を宗政昭弘氏との共同研究において進めた。具体的には、長さは７２に限らずに、また doubly even の仮定も外して extremal self-dual code の各 weight の codeword のなす self-orthogonal t-design と同じパラメータをもつ self-orthogonal t-design の結合行列がどのような code を構成するかを決定した。

残念ながら、未解決問題への解決となる self-orthogonal 5-(72,16,78) design の存在性を決定するには至らなかったが、その結果、多くの self-orthogonal design と self-dual code の関係についての解明することが出来たので、関連する分野における発展に寄与できたと思われ、この結果が本研究課題における最も重要な結果であると言える。この結果については、現在、論文作成中である。

上記に述べた通り、Nebe による７２次元の extremal Type II lattice の構成方法を Type II $\mathbb{Z}_{2k}$-code に応用した self-dual code の構成方法を具体的に計算代数ソフト Magma によるプログラムを書くことで、実際に、本研究課題において購入した計算機を用いて、長さ７２の extremal Type II $\mathbb{Z}_4$-code の構成に挑戦したが、研究期間中には構成に至らなかった。今後も計算機による探索を継続して構成に挑戦したいと考えている。

次に、self-dual $\mathbb{Z}_k$-code の存在や分類をする際には、関連する 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することを有効であると考えていることは既に述べた通りであるが、本研究期間に得られた結果について紹介する。まず、連携研究者である宗政昭弘氏と知られている unimodular lattice の分類を用いて長さ９以下の self-dual $\mathbb{Z}_k$-code（$k \leqq 24$）の分類を完成させることが出来た。この結果をまとめた論文は、現在、出版準備中である。さらに、ある２０次元の unimodular lattice D_{20}^+ に対して、Construction A でこの lattice を与える GF(7) 上の self-dual [20,10,9] code は一意的であることを示すことが出来た。その手法は、対象である self-dual [20,10,9] code が D_{20}^+ を構成するときに必ず skew-symmetric なアダマール行列から構成されることを示し、アダマール行列の分類結果に帰着させることであった。この研究成果を得るためにも計算機による計算が重要な役割を果たした。この結果は、現在、論文として投稿中である。

上の段落にも登場したアダマール行列であるが、組合せデザイン理論の一つの重要な研究対象であり、その起源は数学であるが、電子通信工学など幅広い応用先をもつ。self-orthogonal design にも関係の深い行列である。最近、活発に研究が行われている不偏性という概念があり、不偏なアダマール行列における基本的な問題は何個まで互いに不偏なアダマール行列が存在するかを決定することである。不偏なアダマール行列は古くから考えられている概念ではあるが、最近、その２種類の一般化として擬不偏と弱不偏とよばれる概念が H. Kharaghani 氏らによって導入されており、擬不偏および弱不偏なアダマール行列に関して符号理論からのアプローチを新谷誠氏と須田庄氏との共同研究で行った。この研究成果を得るためにも計算機による計算が重要な役割を果たした。この結果をまとめた論文は、現在、出版準備中である。

最後に、新谷誠氏と須田庄氏との共同研究である種の complex spherical 2-code に関連した supplementary difference set についての分類を行った。complex spherical 2-code の濃度に関して知られている上限より１つ小さい場合について、2-code を与える supplementary difference set の分類を位数５１以下について完成させた。この研究成果を得るためにも計算機による計算が重要な役割を果たした。この結果については、既に論文として出版されている。

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３件）

① Makoto Araya, Masaaki Harada and Sho

Suda, Quasi-unbiased Hadamard matrices and weakly unbiased Hadamard matrices: a coding-theoretic approach, *Mathematics of Computation*, 査読有, （印刷中）

② Masaaki Harada and Akihiro Munemasa, On the classification of self-dual $\mathbb{Z}_k$-codes II, *Interdiscip. Inform. Sci.* 査読有,（印刷中）

③ Makoto Araya, Masaaki Harada and Sho Suda, Supplementary difference sets related to a certain class of complex spherical 2-codes, *Australasian J. Combin.* 査読有, 65 (2016), 71-83 http://ajc.maths.uq.edu.au/pdf/65/ajc_v65_p071.pdf

〔学会発表〕（計１件）

① 原田昌晃, On a 5-design related to an extremal doubly even self-dual code of length 72, 「Workshop on Hadamard Matrices and Combinatorial Designs」 ２０１４年１０月３１日, 東北大学大学院情報科学研究科（宮城県仙台市）

〔図書〕（計０件）

〔その他〕
ホームページ等
http://www.math.is.tohoku.ac.jp/~mharada/

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

(3)連携研究者
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

島倉 裕樹　（SHIMAKURA, Hiroki）
東北大学・大学院情報科学研究科・准教授
研究者番号：90399791