様式Ｆ－１９

科学研究費助成事業（学術研究助成基金助成金）研究成果報告書

平成２５年４月８日現在

機関番号：１１５０１
研究種目：挑戦的萌芽研究
研究期間：2011～2012
課題番号：２３６５４０２９
研究課題名（和文）　長さ７２の極値的重偶自己双対符号の構成への試み

研究課題名（英文）　Challenging to construction of an extremal doubly even self-dual code of length 72

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、代数的符号理論のおける有名な未解決問題の一つである長さ７２の極値的重偶自己双対符号の構成への試みを行った。その試みの過程で、今までに存在の分かっていなかった７２次元の最適な奇ユニモジュラー格子の構成が出来た。また、長さ７２の極値的タイプＩＩの Z_{2k} 上の符号の存在を k が 4 以上の偶数の場合に示すことが出来た。

研究成果の概要（英文）：In this research project, I tried to construction of an extremal doubly even self-dual code of length 72.　The existence of such a code is a famous problem in algebraic coding theory.　In this process, a 72-dimensional optimal odd unimodular lattice was constructed for the first time.　Also, it was shown that there is an extremal Type II Z_{2k}-code of length 72 for an integer k satisfying that k is even and k is greater than or equal to 4.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
交付決定額	2,500,000	750,000	3,250,000

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：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

代数的符号理論の重要な対象として doubly even self-dual code （重偶自己双対符号）があり、符号理論において代数的な立場からの研究が歴史的に幅広く行なわれて来た。

まず doubly even self-dual code の重み多項式に関する代数的な考察より、この多項式の属する環構造が決定されている（Gleason の定理として知られている）。この有名な結果により 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ることが直ちに分かる。さらに、Gleason の定理より、各長さ n において、最も重要なパラメータの一つある minimum weight d（最小重さ）に関する上限

$$d \leqq 4[n/24] + 4$$

を１９７３年に Mallows-Sloane が導いた。この上限に一致する場合、extremal（極値的）とよばれる。

この上限は、代数的な背景より得られたものであり、それを満たす extremal doubly even self-dual code が各長さで存在するかどうかは、その背景からも

基本的ではあるが重要な問題であると考えられている。さらに長さ８、１６、２４、３２、４０、４８、５６、６４においては１９７０年代に既に一つ以上のextremal doubly even self-dual codeが存在することが分かっていた。当初、次の長さの７２においても構成への試みが行われたと思われるが、誰も成功しなかった。このような背景の中で、１９７３年に、符号理論における第一人者の一人と言えるN.J.A. Sloane が、このcode の存在について注目を与えるためにIEEE Trans. Information Theory に論文を出版した。そのこともあり、代数的符号理論における有名な未解決問題の一つとして広く知れ渡ることになった。

Assmus-Mattson の定理として、与えられた code の各 weight の codeword 全体が t-design になるかどうかの判定条件が知られている。この結果を用いることで、この存在が分かっていない、長さ７２の extremal doubly even self-dual code がもし存在すれば、その minimum weight である weight 16 の codeword 全体はブロックの交わりが偶数となる 5-(72,16,78) design となることが Assmus-Mattson の定理より分かる。２００４年に北詰正顕氏、宗政昭弘氏との共同研究により、もし、ブロックの交わりが偶数となる 5-(72,16,78) design が存在すれば、この design が長さ７２の extremal doubly even self-dual code を生成することを示した。また、長さ７０の self-dual code で最大の minimum weight をもつ code の存在もこの code の存在は同値であることが分かっている。このように、今までに、幾つかの存在性に関する同値条件が見つけられている。

２．研究の目的

上に述べた通り、doubly even self-dual code は代数的符号理論の重要な対象であり、符号理論において代数的な立場からの研究が歴史的に幅広く行なわれて来た。

この doubly even self-dual code の重み多項式の代数的な特性から得られた minimum weight d に関する上限

$$d \leqq 4[n/24] +4$$

において等号が成立する extremal doubly even self-dual code が各長さ n （$\equiv 0 \pmod 8$）で存在するかどうかは基本的ではあるが重要な問題である。上でも述べた通り、長さ n が８、１６、２４、３２、４０、４８、５６、６４においては１９７０年代に既に一つ以上のextremal doubly even self-dual codeが存在することが分かっていた。

本研究での主目的は、代数的符号理論での有名な未解決問題の一つとして広く知られている、存在の分かっていない最小の長さである長さ７２の extremal doubly even self-dual code の構成にチャレンジすることである。

３．研究の方法

長さ７２の extremal doubly even self-dual code の構成に取り組むために、今までに知られている構成方法の確認を行う。特に、長さが７２以上においては extremal doubly even self-dual code の存在が分かっている長さは８０、８８、１０４と１３６だけであったが、２００８年に、研究代表者は、長さ１１２において初めて extremal doubly even self-dual code の構成を行うことが出来た。新たな長さで存在が分かったのは約３０年ぶりであった。したがって、その構成で扱った方法の一般化を試みることを行う。

また「研究開始当初の背景」の項目で述べたように、ブロックの交わりが偶数となる5-(72,16,78) design の存在と長さ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た。このように長さ７２の extremal doubly even self-dual code に深く関係する組合せ構造や離散構造の構成や特徴付けなどの研究も行う。さらに研究を進めていく上で、このことは最も必要とされる新たな手法や道具の開発に繋がる。

例えば unimodular lattice や（ある種の）頂点作用素代数においては self-dual code とパラレルとなる結果が比較的多く成立することが知られている。したがって、連携研究者の専門知識の助けを得ながら、どのようなことが成り立っているかを確認することで、研究を遂行する。特に、本研究のターゲットである code と同じようにごく最近まで存在の分かっていなかった７２次元の extremal even unimodular lattice の構成が Nebe によって行なわれた（２０１２年に論文として出版された）。存在性については直接の関係はなさそうに思われるが、それぞれの背景の類似により、これらの code と

lattice の存在がどちらも分かっていなかったことは不思議ではないと思われていた。したがって、片方の lattice の存在が肯定的に解決されたことは大きな影響を与えることになり Nebe による７２次元の extremal even unimodular lattice の構成方法について考察を行なうことも、研究を進めていく上で重要な方法の一つである。

４．研究成果

（１）
本研究の主なターゲットは長さ７２の extremal doubly even self-dual code であり、その存在を決めることに挑戦することが目的ではあるが、上で述べた通り、この code の存在とその背景が非常に良く似ていると思われる Nebe によって構成された７２次元の extremal even unimodular lattice の構成の考察を行った。

その結果、今までに存在の分かっていなかった７２次元の optimal odd unimodular lattice の構成が出来たことが、本研究で得られた主な結果として挙げられる。今回構成されたこの lattice は $\mathbf{Z}_8$ 上の self-dual code として構成することが出来たことは、self-dual code との関連も幅広く考えられるので、特筆できる点である。この結果は発表論文［1］として公表している。

（２）
次に行った取り組みは、長さ７２の extremal doubly even self-dual code の構成に挑戦するために、これを含む一般的なクラスとして extremal Type II $\mathbf{Z}_{2k}$-code という対象を考えたことである。

さらに詳しく述べると、Type II $\mathbf{Z}_{2k}$-code は１９９９年に研究代表者らが doubly even self-dual code の一般化として定義したものであり k=1 の場合が通常の doubly even self-dual code となっている。７２（以下）の長さ n において、その (Euclidean) minimum weight d について

$$d \leqq 4k[n/24] + 4k$$

が成り立ち、通常の場合と同様に等号が成り立つときを exremal とよぶ。extremal doubly even self-dual code をより一般的な枠組みで考えることで、その存在についての考察を行った（k=1 の場合が、本研究での主題となるターゲットとなる）。

この取り組みにおいて得られた主な結果は、長さ７２の extremal Type II $\mathbf{Z}_{2k}$-code の存在を k が 4 以上の偶数の場合に示すことが出来たことである。k=1 の場合が、本研究での主題となるターゲットではあるが、これまでに長さ７２での extremal Type II $\mathbf{Z}_{2k}$-code に関してその存在性は全く分かっていなかったので、今後の進展が期待される。k = 4 の場合、k が奇数の場合など、今後も継続して研究を行っていきたい。なお、この結果は発表論文［2］として公表している。

（３）
ブロックの交わりが偶数となる 5-(72,16,78) design の存在と長さ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た。上は minimum weight の codeword に関連する 5-design であるが Assmus-Mattson の定理はその他の weight の codeword にも適用されるので、その他の codeword がなす 5-design と同じパラメータの一般の 5-design が生成する code に関しての考察を進め、存在の同値性についての観察を行った。さらに、長さが２４の倍数である extremal doubly even self-dual code の各 weight の codeword についても同様に 5-design になることが分かるが、これらの 5-design と同じパラメータの一般の 5-design が生成する code に関しての研究を進めた。このアプローチに関しては、今後も継続して行っていく課題である。

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２件）

[1]
M. Harada, T. Miezaki, An optimal odd unimodular lattice in dimension 72, Archiv der Mathematik, 査読有, 97, 2011, 529-533
DOI: 10.1007/s00013-011-0333-3

[2]
M. Harada, T. Miezaki, On the existence of extremal Type II $\mathbf{Z}_{2k}$-codes, Mathematics of Computation, 査読有, (掲載決定)

〔学会発表〕（計１件）

原田昌晃、On the existence of extremal Type II $\mathbf{Z}_{2k}$-codes、離散数学とその応用研究集会２０１２、２０１２年８月９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

なし

(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

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