科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　　６　日現在

機関番号：　１１１０１
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５４０００２

研究課題名（和文）立方重偶符号についての研究

研究課題名（英文）Research on triply even codes

研究代表者
別宮　耕一（BETSUMIYA, Koichi）

弘前大学・理工学研究科・准教授

研究者番号：６０３６４６８４

交付決定額（研究期間全体）：（直接経費）　　3,900,000円、（間接経費）　　1,170,000円

研究成果の概要（和文）：1．重偶符号の既約因子の個数は符号のスター積の双対符号の次元等しいことを示した。2．立方重偶符号が極大であるための必要十分条件が符号自身とその根基が一致することであることを示した。また、立方重偶符号に関するこれらの直接的な成果に加えて、3．長さ40の重偶な自己双対符号の分類を与えた。さらに、4.長さ64の極限的な３元体上の符号を構成する32次のHadamard行列Paley型に限ることを示した。

研究成果の概要（英文）：1. We have shown that the number of irreducible factors is equal to the dimension of dual code of the star product. 2. We have shown that a triply even code is maximum if and only if the code is equal to the radical. 3. We have given a classification of doubly even self-dual codes of length 40. 4. We have shown that the Paley-Hadamard matrix is the only Hadamard matrix of order 32 which gives an extremal self-dual code of length 64.

研究分野：　数物系科学

科研費の分科・細目：　数学・代数学

キーワード：　群論　代数的符号理論　頂点作用素代数

１．研究開始当初の背景

(1) 頂点作用素代数の重要性

頂点作用素代数は数理物理学における共形場理論から生まれた概念である。そして散在型有限単純群のひとつであるモンスター単純群が、その頂点作用素代数のひとつであるムーンシャイン頂点作用素代数の自己同型写像全体のなす巨大な群として構成されたことで、頂点作用素代数は有限群論における重要な研究課題として注目されるようになった。

また、モンスター単純群は保型形式論や共形場理論などの一見何の関連を持つように思われない分野との密接な関係を示唆する興味深い現象が観測されていた。

(2) 頂点作用素代数と符号理論

1996 年に符号から頂点作用素代数を構成する方法が開発されたことで、符号を通した頂点作用素代数の研究が始められた。その中で、ムーンシャイン頂点作用素代数が中心電荷 24 の枠付き頂点作用素代数のひとつとして、符号から構成された。

その後、理論の精密化が進む中で、中心電荷 24 の枠付き頂点作用素代数は、長さ 48 の立方重偶符号とある種の対応関係にあることが明らかとなった。こうして、長さ 48 の立方重偶符号の分類を通して、ムーンシャイン頂点作用素代数の位置付けの解明が期待されるようになった。

(3)長さ 32 までの立方重偶符号

研究代表者らの先行研究によって、長さ 32 までは、素朴な総当たりアルゴリズムによってコンピュータによる立方重偶符号の分類は得られた。その結果、立方重偶符号はすべて長さが半分の重偶自己双対符号を並べて構成される符号のみであり、次元についても単純な規則性に従っていることが明らかとなった。

(4)長さ 48 の立方重偶符号

研究代表者らの先行研究によって、群を用いた効率のよいアルゴリズムが考案された。これによって、長さ 48 の極大な立方重偶符号の分類が得られた。その結果、極大な立方重偶符号は全部で 9 個存在し、そのうち 8 個については、長さが半分の重偶自己双対符号を並べて構成されるものであり、残りの１個は三角グラフとよばれるものの隣接行列によって生成される符号であることが明らかとなった。こうして、立方重偶符号に関する知見が深まることで一般的な理論の構築が期待されることとなった。

２．研究の目的

前節で述べたように、長さ 48 以下については、極大な立方重偶符号の分類が得られていたが、以下に点について十分な知見が得られていなかった。

1. 極大立方重偶符号に関する次元の規則性
2.重偶な自己双対符号の貼り合せ、もしくは、三角グラフに由来しない極大立方重偶符号の存在非存在。 3.三次形式と立方重偶符号との関係性。

そこで、これらの未解決な問題の解決につながるような知見の獲得を本研究課題の目的とした。

３．研究の方法

(1) まず、長さ 48 の立方重偶符号の分類の際に得られた長さ 48 の極大な立方重偶符号の性質について考察をすすめ、一般の長さに関する極大な立方重偶符号が持つ性質、構造について考察を行う。同時に立方重偶符号を構成する際に用いた重偶な自己双対符号や三角グラフについての考察を行うことを通して、立方重偶符号の一般論の確立を進めていく。
(2) 計算機を用いることで、まだ存在が知られていない立方重偶符号を探索する。
(3) 立方重偶符号の構造に密接に関連する重偶符号などの構造の探索を進める。

４．研究成果

(1)立方重偶符号が備える基本的な性質の解明

立方重偶符号に関して次の性質を明らかにした。

① 重偶符号の既約因子の個数の判定

２つの符号語に対して成分ごとの積によって得られる新たな符号語をスター積とよぶこととし、スター積全体によって生成される部分空間を２つの符号のスター積と呼ぶこととする。このとき、重偶符号の既約因子の個数がその符号とそれ自身とのスター積の双対の次元で与えられることを明らかにした。特に、スター積によって得られる符号の双対が１次元であるとき、符号は既約となる。

本来、規約性の判定を行うためには、符号の座標順序をうまく設定する必要があり、それ程容易ではなかった。しかし、今回得られた定理を適用するために必要なスター積の計算は容易であり、その双対の計算も容易であるので、既約因子の個数が容易に求めることができるようになった。

② 立方重偶符号について、極大性の判定

ある立方重偶符号が極大かどうかの判定する場合、長さがある程度小さければ計算機を用いて直接的な方法を用いることで判定することができる。しかし、長さが大きくなれば急速に計算量が増大し、判定が現実的ではなくなってしまう。

今回、重偶符号に対して代数的な概念である根基と呼ばれる概念を定義した。この概念を用いることで、ある立方重偶符号が極大であるための必要十分条件は、立方重偶符号とその根基が一致すること

となることを示した。根基の計算は比較的容易であるので、これによって、極大性の判定は容易となった。加えて、重偶符号の極大性は自己双対性と同値であるが、それと類似の意味づけを立方重偶符号にも与えることができたと考えている。これらの成果に加え、立方重偶符号に関する理解を進めることができた。また、それらの結果を用いることで、長さ 48 の立方重偶符号の分類結果をより簡潔に記述することができた。これらの成果と分類結果をまとめたものを〔雑誌論文〕③として出版した。

(2) 長さ 40 の重偶な自己双対符号の分類

重偶な自己双対符号は多くの組み合わせ構造と密接な関係を有しており、それ自身も代数的符号理論において重要な構造と見なされ研究が進められている。さらに、(1)で述べた通り、立方重偶符号を解明するうえで重要な概念のひとつである。

重偶な自己双対符号は長さが 8 の倍数の場合のみ存在することが知られており、長さが 32 以下符号については、完全な分類が与えられていた。しかし、J. H. Conway, V. Pless, N. J. S. Sloane らによって長さ 32 の分類が 1992 年に完成したのを最後に進展はなかった。今回の分類は 20 年ぶりの成果である。

長さ 40 の重偶な自己双対符号の最小重みは Mallows-Sloane の限界式より限界が与えられているため、4 または 8 であることが知られていた。そこで、まず、立方重偶符号の分類の際用いた、長さ 16 の符号と長さ 24 の符号を自己同型で張り合わせることによって、長さ 40、最小重み 8 の符号を全て構成した。この方法を用いることで、固定した符号の組の張り合わせによって全ての符号を構成するために必要な計算量が、自己同型群の両側剰余類の大きさで抑えられるため、分類の成功につながったと考えている。

その結果、最小重みが 8、長さが 40 の重偶な自己双対符号の個数は同値なものを除いて全部で 16470 個あることが求められた。

次にすでに知られている長さ 36 の自己装置符号の分類結果をもちいて、それを拡張することで、長さ 40、最小重み 4 の重偶な自己双対符号がえられるが、この構成法を用いることで、長さ 40、最小重み 4 の重偶な自己双対符号の分類が得られた。

その結果、最小重みが 4、長さが 40 の重偶な自己双対符号の個数は同値なものを除いて全部で 77873 個であることが求められた。

両者を合わせて長さ 40 の重偶な自己双対符号の個数は同値なものを除いて、全部で 94343 個であることが求められた。この結果については〔雑誌論文〕②として出版した。

(3) 極限的な符号に関わる 32 次の Hadamard 行列の分類

極限的な自己双対符号は立方重偶符号に密接な関連をもつ組合せ構造である。また長さ $2n$ の３元体上の自己双対符号が n 次の Hadamard 行列から構成できることはよく知られている。この事実をもとに、計算機を用いて、長さ 64 の極限的な３元体上の符号を構成する 32 次の Hadamard 行列の分類を与えることができた。

結果として、そのような 32 次の Hadamard 行列は Paley 型のものに限るということが判明した。この結果については〔雑誌論文〕④として出版した。

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７件）

① Koichi Betsumiya, Mitsugu Hirasaka, Takao Komatsu, Akihiro Munemasa, “Upper bounds on cyclotomic numbers”, Linear Algebra and its Applications, 査読有, 438, 2013, 111 - 120 DOI:10.1016/j.laa.2012.06.045

② Koichi Betsumiya, Masaaki Harada, Akihiro Munemasa, “A complete classification of doubly even self-dual codes of length 40”, The Electronic Journal of Combinatorics, 査読有, 19, 2012, Paper #18

③ Koichi Betsumiya, Akihiro Munemasa, “On triply even binary codes”, Journal of the London Mathematical Society, 査読有, 86, 2012, 1-16 DOI:10.1112/jlms/jdr054

④ Koichi Betsumiya, Masaaki Harada, Hiroshi Kimura, “Hadamard matrices of order 32 and extremal ternary self-dual codes”, Designs, Codes and Cryptography, 査読有, 58, 2011, 203-214

⑤ Koichi Betsumiya, YoungJu Choie, “Invariant ring of Clifford-Weil group, and Jacobi forms over totally real field”, Séminaires et Congrès, 査読有, 21, 2011, 1-16

⑥ 別宮耕一, “Classification of doubly even self-dual codes of length 40”, 第29回代数的組合せ論シンポジウム報告集, 査読無, 2013, 10-16

⑦ 別宮耕一, “Triply even codes について”, 数理解析研究所講究録, 査読無, 1844, 2013, 139-145

〔学会発表〕（計５件）

① 別宮耕一、Hamming codes の code words と E_8 simple roots の対応について、第25回有限群論草津セミナー、2013 年 8 月 2 日～8 月 5 日、国立大学共同利用草津セミナーハウス

② 別宮耕一、Classification of doubly even self-dual codes of length 40、第29回代数的組み合せ論シンポジウム、2012 年 6 月 18 日、弘前大学

③ 別宮耕一、Triply even code について、

RIMS 共同研究：デザイン、符号グラフおよびその周辺、2012 年7月19日、京都大学数理解析研究所

④ 別宮耕一、群を用いた二元体上の[48, 24, 12]自己双対符号の一意性証明、第 23 回有限群論草津セミナー、2011年7月31日、国立大学共同利用草津セミナーハウス

⑤ 別宮耕一、Even self-dual code over GF(4)、Workshop on Algebraic Combinatorics、2011 年 9 月 16 日、上海交通大学

〔図書〕（計0件）

〔産業財産権〕
○出願状況（計0件）

○取得状況（計0件）

〔その他〕
ホームページ等
DATABASE: Triply Even Codes of Length 48
http://www.st.hirosaki-u.ac.jp/~betsumi/triply-even/

6．研究組織
(1)研究代表者
別宮　耕一（BETSUMIYA, Koichi）
研究者番号：60364684