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　２ 年　 ６ 月　 ５ 日現在

機関番号：１１１０１
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ０５１５３

研究課題名（和文）極大立方重偶符号の系列と、関連する数理構造の研究

研究課題名（英文）Research on families of maximal triply even codes and related mathematical structures

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）　　3,400,000円

研究成果の概要（和文）：本研究課題において得られた成果は次の通りである。
(1) いくつかの強正則グラフから自然に立方重偶符号を構成し、極大性、重み分布、自己同型群などの符号に付随する構造を得た。(2) ある種の有限幾何構造から構成される立方重偶符号の系列について、極大性を示すために必要と考えられるいくつかの補題の証明に成功した。(3) これまで得られた立方重偶符号を応用して、暗号理論における線形秘密分散体系を構成する方法を考案した。(4) 立方重偶符号との関連の中で、四元体上の符号から得られる二次体上の格子に意味づけを与えた。(5) Leech格子とその自己同型群であるConway0群に関する計算を行った。

研究成果の学術的意義や社会的意義
　これまでの研究を通して、立方重偶符号が共形場理論、有限群論、保型形式論、情報理論などの様々な数理構造と関連することが明らかとなっている。
　立方重偶符号の研究を通して、頂点作用素代数の性質が明らかになることや、散在型単純群やLie型の有限単純群の系列に関する新たな視点が得られることは意義深い。

研究成果の概要（英文）：We obtained the following results.
(1) From some strongly regular graphs, we constructed triply even codes. We showed the maximality, the weight distribution, the automorphism groups and showed some other equipped structures. (2) On a series of triply even codes constructed from finite geometries, we showed some lemmas. (3) From triply even codes, we constructed some secret sharing schemes. (4) We made some sense of a lattice over a quadratic field constructed from a quaternary code in relations to triply even codes. (5) We calculated some subgroups of the Conway0 group which is the automorphism group of the Leech lattice.

研究分野：代数学

キーワード：代数的組合せ論　符号理論　離散幾何　組合せデザイン　散在型有限単純群　グラフ理論　極大立方重偶符号　自己双対符号

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

(1) 頂点作用素代数と立方重偶符号

1996 年に線形二元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，線形二元符号を通した頂点作用素代数の研究が始められた。そこで見い出された方法によって、中心電荷 24 の枠付き頂点作用素代数と呼ばれるクラスのひとつとして，ムーンシャイン頂点作用素代数が線形二元符号の一種である立方重偶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。

(2) 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 2 次元共形場理論のひとつの公理化として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。

この群が重要視されているのは、単に位数が大きいというだけでなく、散在型単純群を解明するための鍵となる群であると見なされていることにある。同時に、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ることも大きい。

(3) 長さ 48 までの立方重偶符号

2012 年に研究代表者らの先行研究によって、長さ 48 までの極大な立方重偶符号の分類が得られている。

長さ 32 までは、素朴な総当たりアルゴリズムによって、長さ 48 については、群を用いた効率のよいアルゴリズムを考案することによって、極大な立方重偶符号の分類が得た。長さが 16 の倍数でない場合は長さが 16 の倍数の立方重偶符号の長さを小さくする操作ですべてが得られる。

その結果、長さ 48 の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。

長さ 48 の立方重偶符号の分類結果は、立方重偶符号の性質がよく調べられている重偶符号と比較して、著しく複雑な状況になっていることを示唆していた。特に極大性の判定は困難な問題であった。

(4) 立方重偶符号の性質

その後の研究代表者らの研究によって、立方重偶符号の一般的性質の解明が進められた。

特に、ある立方重偶符号が極大かどうかを判定する場合、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。

そこで、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、いくつかの特殊な場合に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となった。

(5) 立方重偶符号の存在性

同時に、いくつかの組合せ構造を基に具体的な立方重偶符号の存在が示され、知見が蓄積されている。

① Witt 3-$(22, 6, 1)$ デザイン (Steiner システム $S(3, 6, 22)$) との関連

Witt 3-$(22, 6, 1)$ デザインは別名 Sieiner システム $S(3, 6, 22)$ とも呼ばれている組み合わせ結合構造のひとつである。散在型有限単純群のひとつである Matheu 群 M_{22} はこの結合構造の自己同型群として実現することができる。同時に、この結合構造が Matheu 群 M_{22} の性質を規定しているものであると位置付けられている。この Witt 3-$(22, 6, 1)$ デザインの結合行列の偶数行の和全体が生成する符号が

[77, 10, 32] 極大立方重偶符号となる。

② Higman 2-(176, 50, 14) 対称デザインとの関連

Higman 2-(176, 50, 14) 対称デザインは先の例と同様に組み合わせ結合構造のひとつである。散在型有限単純群のひとつである Higman-Sims 群 HS はこの結合構造の自己同型群として実現することができる。同時に，この結合構造が Higman-Sims 群 HS の性質を規定しているものであると位置付けられている。この Higman 2-(176, 50, 14) 対称デザインの結合行列の偶数行の和全体が生成する符号が [176, 21, 56] 極大立方重偶符号となる。加えて、千吉良-原田-北詰符号と呼ばれる二元符号との関連が見出されている。

２．研究の目的

前節で述べたような立方重偶符号に持つ興味深い性質が見出される一方、以下に挙げる点について十分な知見が得られていない。

(1) 極大立方重偶符号に関する次元の規則性
(2) 極大立方重偶符号が散在型単純群や Lie 型の単純群の系列と関連もつ背景とメカニズム
(3) 極大性を確認する一般的な方法

そこで、これらの未解決の問題の解決につながるような知見を獲得することと同時に、これらを解明する過程で頂点作用素代数に関する新たな知見や、未知の組合せ構造に関する知見を獲得すること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進め、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、立方重偶符号に関する一般論の確立を進めていく。

(2) 計算機を用いることで、様々な条件を満たす組合せ構造や群構造に内在する、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やグラフ、組合せデザイン、格子などの構造の探索を進める。同時にそれらの自己同型群の構造を調べる。

４．研究成果

(1) これまで得られた無限系列について分析を進め、それらが強正則グラフと呼ばれるクラスのグラフと強い関連があることを確めた。具体的には、よく知られたいくつかの強正則グラフから自然に立方重偶符号が構成され、基になる強正則グラフの性質を用いることで立方重偶符号の極大性、重み分布、自己同型群などの符号に付随する構造を得た。

(2) ある種の有限幾何構造から構成される立方重偶符号の系列について、極大性を示すために必要と考えられるいくつかの補題の証明に成功した。

(3) これまで得られた立方重偶符号を応用して、暗号理論における線形秘密分散体系を構成する方法を考案し、実際に有用と思われる体系が得られることを示した。

(4) 立方重偶符号との関連の中で、四元体上の符号から得られる二次体上の格子に新たな意味づけを与えることができた。

(5) 立方重偶符号に関連する組合せ構造として、Leech 格子と呼ばれる数理構造に焦点を当て、その自己同型群である Conway0 群に関する計算を行った。具体的には、各元が固定する Leech 格子の部分構造などを決定し、それらがある種の数理構造とのつながりを持っていることを明らかにした。

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　0件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 別宮耕一	４．巻 30
２．論文標題 拡張ハミング符号と正六百胞体との対応について	５．発行年 2019年
３．雑誌名 第30回有限群論草津セミナー報告集	６．最初と最後の頁 37-42
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 別宮耕一	４．巻 -
２．論文標題 Triply even code の極大性判定	５．発行年 2018年
３．雑誌名 第29回有限群論草津セミナー報告集	６．最初と最後の頁 14-17
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計7件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 別宮耕一
２．発表標題 拡張ハミング符号と正六百胞体との対応について
３．学会等名 第30回有限群論草津セミナー
４．発表年 2018年

１．発表者名 別宮耕一
２．発表標題 正六百胞体格子と E_8 格子の対応について
３．学会等名 福井表現論小研究集会
４．発表年 2018年

１．発表者名
別宮耕一

２．発表標題
On triply even codes

３．学会等名
組合せ論的符号理論

４．発表年
2019年

１．発表者名
別宮耕一

２．発表標題
二次体の整数環上の格子について

３．学会等名
千葉大 群論特別セミナー

４．発表年
2019年

１．発表者名
Koichi BETSUMIYA

２．発表標題
A Distribution of known maximal triply even codes

３．学会等名
Workshop on Finite Groups, vertex algebras and algebraic combinatorics

４．発表年
2019年

１．発表者名
別宮耕一

２．発表標題
Triply even code の極大性判定

３．学会等名
第29回有限群論草津セミナー

４．発表年
2017年

１．発表者名
Koichi Betsumiya

２．発表標題
On some series of maximal triply even codes

３．学会等名
Hadamard Matrices and Their Applications（国際学会）

４．発表年
2018年

〔図書〕　計0件

〔産業財産権〕

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

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考