様式 C-19

科学研究費補助金研究成果報告書

平成２３年　５月３０日現在

機関番号：１１１０１
研究種目：基盤研究(C)
研究期間：2007～2010
課題番号：１９５４００４８
研究課題名（和文）　代数的符号理論の研究とその頂点作用素代数への応用

研究課題名（英文）　Research on algebraic coding theory and its applications for vertex operator algebras

研究代表者
別宮　耕一（BETSUMIYA KOICHI）
弘前大学・大学院理工学研究科・准教授
研究者番号：６０３６４６８４

研究成果の概要（和文）：
立方重偶符号の構造を調べ上げることを通して、新たな符号の検索アルゴリズムを考案し、計算機に実行させることで長さ 48 以下の極大な立方重偶符号の分類を完成させた。その結果、三角グラフと呼ばれるものに由来する構造を備える、それまでの規則性に反する新たな極大立方重偶符号の存在を確認するに至った。
さらに、得られた分類リストの符号から、これまで知られていなかった多くの枠付き頂点作用素代数を構成することにつながった。

研究成果の概要（英文）：
We have presented an efficient algorithm for finding triply even codes by investigating the structure of triply even codes. This algorithm has produced a classification of maximal triply even codes of length up to 48. As a result, we have found a new maximal triply even code which is contrary to the expected behavior constructed by a triangular graph.
Moreover, new framed vertex operator algebras have been constructed from the list of codes.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	700,000	210,000	910,000
２００８年度	900,000	270,000	1,170,000
２００９年度	900,000	270,000	1,170,000
２０１０年度	700,000	210,000	910,000
年度			
総　計	3,200,000	960,000	4,160,000

研究分野：代数的組合せ論
科研費の分科・細目：数学・代数学
キーワード：群論、符号理論

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。この一連の理論は宮本理論と呼ばれる。

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．研究の目的

(1)立方重偶符号の分類

長さ 48 までの極大な立方重偶符号の分類を完成させる。

(2)符号理論の頂点作用素代数への応用

立方重偶符号の分類結果を応用して、枠付き頂点作用素代数におけるムーンシャイン頂点作用素代数の位置付けを明らかにする。同時に未知の頂点作用素代数を構成することで全体像の解明を進める。

(3)その他の対象との関連

共形場理論、有限群論、保型形式論、情報理論などが係わり合う中で突発的に捉えられる構造間の関連を見出す。具体的には以下に関する知見を得る。

①符号理論を経由した新たな理論の存在
②そこから生まれる双方に与える刺激
③立方重偶符号から得られる重偶自己双対符号の情報

３．研究の方法

(1) 立方重偶符号の分類

長さ32までの分類は総当りアルゴリズムによる直接的な方法で可能であることが予想された。しかし、その方法では計算量が長さに対して指数関数的に増大するため、長さ48以上の場合は明らかに不可能である。そこで、高速な計算機サーバーによる数値実験や、組合せ論的な手法によって構造を解析するなど、立方重偶符号の構造を調べ上げることを通して、効率の良い分類アルゴリズムを構築し、それを用いて長さ48の分類を完成させることを目指した。

(2)頂点作用素代数への応用

新たに構成された符号から宮本理論の手法を通して頂点作用素代数を構成する。その際、次の２点について調べることが重要であると考えている。

①どのような符号からムーンシャイン頂点作用素代数が構成されるか。
②これまで知られていない新しい頂点作用素代数は構成されるか。

前者からは、ムーンシャイン頂点作用素代数の位置付けが得られることが期待でき、後者に関しては、多くの研究者が異なる方法で同じ問題に取り組んでおり、これまで確認されているものについては完全なリストが与えられている。また、知られていないものについても、存在が期待される頂点作用素代数の型のリストがすでに得られており、それらとの対照を通して研究を進める。

(3) その他の対象との関連

新たに得られた符号に内在する構造については、常に文献調査、もしくは研究者間の情報交換を通して、既存の構造との対応付けを行う。

４．研究成果

(1)長さ32までの分類

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可能であった。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。

(2)立方重偶符号の分類アルゴリズム

線形符号 $C \subset F_2^n$ について、C のすべての符号語の Hamming 荷重が 8 の倍数となるものを**立方重偶符号**という。また、C を真に含む立方重偶符号が存在しないとき、C を**極大**な立方重偶符号という。

先に述べたように、長さ 32 までの極大な立方重偶符号を分類するためには、総当りによる方法で十分であるが、長さ 48 の場合は機能しない。そのため、次のような三次形式の全体がなす群を用いた分類アルゴリズムを研究成果のひとつとして与えることができた。

三次形式の定義は次の通りである。V を二元体 F_2 上のベクトル空間とする。写像 $Q : V \to F_2$ が**三次形式**であるとは、次の式

$$Q(x+y) = Q(x) + Q(y) + B(x, y)$$

$$B(x+y, z) = B(x, z) + B(y, z) + T(x, y, z)$$

で定義される写像

$$T : V \times V \times V \to F_2$$

が三重線形写像となることとする。今、V を F_2 上の重偶符号とし、Q を次のように定義する。

$$Q(x) = \mathrm{wt}(x)/4 \pmod 2$$

そのとき、

$$B:\ V\times V\to F_2$$
$$T:\ V\times V\times V\to F_2$$
は次のようになる。
$$B(x,\ y)\ =\ \mathrm{wt}(x*y)/2\ \ (\mathrm{mod}\ 2)$$
$$T(x,\ y,\ z)\ =\ \mathrm{wt}(x*y*z)\ \ (\mathrm{mod}\ 2)$$
ただし、* は成分ごとの積を表すものとする。このとき、定義より Qは三次形式となる。

また、符号 $C\subset F_2^n$, $S\subset\{1,\ldots,n\}$, $S'=\{1,\ldots,n\}\setminus S$について、
$$\{(c_j|\ j\in S')\in F^{\#S'}\ \ |(c_j|\ j\in S)=0,\ \ c\in C\}$$
を Sに関する Cの短縮符号と呼び、
$$\{(c_j|\ j\in S')\in F^{\#S'}\ \ |\ \ c\in C\}$$
を Sに関する Cのパンクチャ符号と呼ぶ。今、$C\in F_2^{48}$を極大な立方重偶符号とし、$(1^{24}|0^{24})$, $(0^{24}|1^{24})\ \in C$と仮定する。このとき、$\{25,26,\ldots,48\}$に関する Cの短縮符号を R_1 とし、パンクチャ符号を C_1とする。同様に、$\{1,2,\ldots,24\}$に関する Cの短縮符号を R_2とし、パンクチャ符号を C_2とすると、Cの元としての自然な対応が、非退化部分 C_1/R_1、C_2/R_2の間に三次形式 Qに関する全単射な等長写像を与える。

逆に考えれば、荷重 24 の符号語を含んでいる長さ 48 の極大な立方重偶符号は、次のアルゴリズムで分類できることが判る。

① 長さ 24 の重偶符号の分類を与える。

② 非退化部分が同型となる重偶符号の組に対して、すべての等長写像それぞれについて、非退化部分の対応関係で生成される符号を列挙する。

③ 得られた符号について、同値類にまとめる。

研究成果のひとつとして、符号の存在性をグラフの連結性の議論に帰着させることで、すべての長さ 48 の極大な立方重偶符号は、長さ 24 の符号語を含んでいることを証明することができた。つまり、ここで与えられたアルゴリズムで長さ 48 のすべての極大な立方重偶符号を分類することができることが示された。

(3)群論を用いた計算量の軽減

研究成果のひとつとして、長さ 48 の極大な立方重偶符号を分類する際、群論を用いて計算量を大幅に軽減させる方法を与えることができた。

まず、$f:\ C_1/R_1\to C_2/R_2$を等長写像のひとつとし、$\mathrm{Aut}(C_1/R_1)$を C_1/R_1からそれ自身への等長写像全体すると、C_1/R_1から C_2/R_2への等長写像全体は
$$\{f\circ g\ |\ g\in\mathrm{Aut}(C_1/R_1)\}$$
となることが判る。

また、符号 C_iに対して、C_iを不変とする座標の置換全体を $\mathrm{Aut}(C_i)$と記述すると、$\mathrm{Aut}(C_i)$の元は座標の置換によって、C_1/R_1 に等長写像として働く。

これは、次のような自然な準同型が存在することを意味する。
$$\pi_i:\mathrm{Aut}(C_i)\to\mathrm{Aut}(C_i/R_i)$$
立方重偶符号の分類に必要なのは同値類の代表系のみであるため、すべての等長写像について検証する必要はない。つまり、両側剰余類
$$D=(f^{-1}\circ\mathrm{Im}(\pi_2)\circ f)\setminus(\mathrm{Aut}(C_1/R_1)/\mathrm{Im}(\pi_1)$$
の代表元について、等長写像の集合
$$\{f\circ g\ |\ g\in D\}$$
のみを検証すれば、立方重偶符号の分類には十分である。

この方法の有効性は次の例に顕著に現れている。まず $C_1=C_2=d_{24}^+$とすると、
$$R_i=\langle 1\rangle,\ \ C_i/R_i=\ d_{24}^+/\langle 1\rangle$$
となる。前述の議論にある群は次のようになる。
$$|\mathrm{Aut}(C_i/R_i)|=51231497335603200$$
$$|\mathrm{Aut}(C_i)|=980995276800$$
$$|\mathrm{Ker}(\pi_i)|=2$$
$$|\mathrm{Aut}(C_i/R_i)/\pi_i(\mathrm{Aut}(C_i))|=104448$$
ここで, $f:C_1\to C_2$ を恒等写像に定めると、両側剰余類の大きさは 6 となる。このことは, C_1/R_1 から C_2/R_2 への等長写像は全部で 51231497335603200 個存在し、それぞれに立方重偶符号が対応するが、両側剰余類の 6 個の代表元に対応する立方重偶符号のいずれかと同値となることとが判る。実際、6 個の両側剰余類の代表元それぞれに非同値な 6 個の立方重偶符号が対応する。

(4)長さ 48 の分類結果

ここまでで述べたアルゴリズムを用いることによって、少ない計算量で長さ 48 の極大な立方重偶符号の分類が得られる。具体的には、汎用のノート PC 上 10 分程度で分類を完了させることができる。

まず、$C=C_1=C_2$とし、fを恒等写像として得られる立方重偶符号を $D(C)$とする。長さ 24 の重偶な自己双対符号は分類がなされており、次のような 9 個であることが知られている。
$$\Delta\ =\ \{g_{24},\ \ d_{24}^+,\ \ {d_{12}}^{2+},\ \ (d_{10}{e_7}^2)^+,$$
$${d_8}^{3+},\ \ {d_6}^{4+},\ \ {d_4}^{6+},\ \ {d_{16}}^+\oplus e_8,\ \ {e_8}^{\oplus 3}\}$$
前述の分類アルゴリズムを用いて、長さ 48 の極大な立方重偶符号は次のように分類が与えられる。

長さ 48 の極大な立方重偶符号は次の 10 個のいずれかと同値である。

・$D(C)$ $\ (C\in\Delta)$

・三角グラフから定義される 9 次元の符号 T_{10}

(5)三角グラフから定義される符号の性質

長さ 32 までの極大な立方重偶符号は長さが半分の重偶自己双対符号と一対一の対応をなしており、それぞれの立方重偶符号の次元は、対応する重偶自己双対符号の次元と直和因子の個数を加えたものと一致していた。

当初、長さ 48 の場合についても同様の対応が存在するとの期待の下に研究を進めていた。実際分類結果を見て判る通り、10 種類ある長さ 48 の極大な立方重偶符号のうち、9 種類は同様の性質を満している。つまり、対応する重偶自己双対符号が存在し、その次元と直和因子の和が立方重偶符号の次元と一致している。

しかしながら、残りの 1 種類 T_{10} については、対応する重偶自己双対符号は存在せず、その次元も極端に小さいことが判明した。

研究を進めた結果、ここで得られた極大な立方重偶符号 T_{10} は三角グラフと呼ばれるものに由来する構造を備えていることが判明した。

(6)頂点作用素代数への応用

まず、研究協力者の C.H.Lam によって、ここで得られた例外的な符号 T_{10} から、また、研究協力者の C.H. Lam と島倉裕樹によって $D(d_{16}^{+}\oplus e_8)$、$D(e_8^{\oplus 3})$から、それぞれ新たな頂点作用素代数の構成にすることに成功した。

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１９件）

①別宮耕一・原田昌晃・木村浩、Hadamard matrices of order 32 and extremal ternary self-dual codes 、 Designs, Codes and Cryptography、査読有、58、2011、203-214
② Lam, Ching Hung・山内博、The FLM conjecture and framed VOA、Vertex operator algebras and related areas、Contemporary Mathematics、 査読有、497、2009、125-138
③別宮耕一・Rowana Alma L. Betty・宗政昭弘、Mass formula for even codes over Z_8、Cryptography and Coding, Springer LNCS、査読有、5921、2009、65-77
④別宮耕一、Minimum Lee weights of Type II code over F_{2^r}、Discrete Mathematics、査読有、308、2008、3018-3022
⑤C.H. Lam・山内博、On the structure of framed vertex operator algebras and their pointwise frame stabilizers 、Communications in Mathematical Physics、査読有、277、2008、237-285

〔学会発表〕（計８件）

①山内博、散在型有限単純群と頂点作用素代数、日本数学会 2010 年度年会、3 月 27 日、慶應義塾大学
②別宮耕一、Mass formula for even codes over Z_8、The 8th Korea-Japan Workshop on Algebra and Combinatorics、2010 年 2 月 6 日、浦項工科大学校（大韓民国）
③別宮耕一、Mass formula for even codes over Z_8 、 Twelfth IMA International Conference on Cryptography and Coding、2009 年 12 月 15 日、王立農業大学（英国）
④宗政昭弘、リーチ格子のフレームとその応用、第 54 回代数学シンポジウム、2009 年 8 月 6 日、明治大学
⑤別宮耕一、Codes over integer residue rings constructed by bases of Galois rings、The 6th Korea-Japan Workshop on Algebra and Combinatorics、2008 年 2 月 9 日、国立釜山大学校（大韓民国）

〔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
http://www.st.hirosaki-u.ac.jp/~betsumi/
http://www.math.is.tohoku.ac.jp/~munemasa/

６．研究組織
(1)研究代表者
別宮　耕一　（BETSUMIYA　KOICHI）
弘前大学・大学院理工学研究科・准教授
研究者番号：６０３６４６８４
(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
（H20→H22：連携研究者）
原田　昌晃　（HARADA　MASAAKI）
山形大学・理学部・准教授
研究者番号：９０２９２４０８
（H20→H22：連携研究者）
山内　博　（YAMAUCHI　HIROSHI）
東京女子大学・講師
研究者番号：４０４５２２１３
（H20→H22：連携研究者）
(3)連携研究者

(4)研究協力者
島倉　裕樹　（SHIMAKURA　HIROKI）
愛知教育大学・教育学部・講師
研究者番号：９０３９９７９１
Lam, Ching Hung
台湾中央研究所・教授