研　究　報　告　書

「代数的符号理論による組合せ構造の解析と量子符号への応用」

研究期間:　平成 20 年 10 月～平成 24 年 3 月
研 究 者:　原田　昌晃

1，研究のねらい

情報化社会においては数理科学が色々な形で役に立っているが、その1つが符号理論である。誤りの発生する可能性のあるデジタル通信路における情報伝達において必要な理論の1つであり、ある程度の誤りの発生であれば自動的に訂正をすることが出来ることを保証するのが（誤り訂正）符号理論である。その起源は情報科学であるが、その後、豊富な数学的な理論を有することが分かり、次第に数理科学の研究者の間で興味を持たれるに値する対象となっていった。本さきがけ研究では、特に、代数的な研究が古くから行われている自己双対符号の研究を行い、符号理論における基礎研究の発展を目指す。また、近年、量子コンピュータの開発のために多方面からの研究が情報科学や物理学の研究者を中心に行なわれている。通常の誤りに（古典的な）符号理論が必要であったように、量子通信に必要なものの1つに量子符号理論の構築があげられ、最近、様々なタイプの量子誤りに対応出来る量子符号についての研究が行なわれている。本さきがけ研究では、現在、進展が期待されている量子符号への応用も目指す。

本さきがけ研究では、主に、符号理論に関する次の3つのテーマについて、それぞれ関連させながら研究を行なうことをねらいとする:

- 長さ72の極値的な重偶自己双対2元符号の存在性を決定する未解決問題への挑戦、
- 計算機の支援による自己双対符号の分類問題への新たな方法での取り組み、
- 量子符号への応用を目指した組合せ構造の研究。

2，研究成果

まずは、上に挙げた3つのテーマに関する研究成果を述べる。

- 長さ72の極値的な重偶自己双対2元符号の存在性を決定する未解決問題への挑戦:

  双対符号に一致する符号を自己双対符号とよび、代数的な性質を多く含むことから活発に研究が行なわれている符号のクラスである。自己双対2元符号の各符号語の重みは偶数になるが、さらに全ての符号語の重みが4の倍数になる場合を重偶とよぶ。重偶自己双対2元符号の重み多項式はある有限群の不変式環に属することなどから、その長さ n は8の倍数であり、その最小重みは $4[n/24]+4$ 以下であることが知られている（Mallows-Sloane (1973)）。最小重みが $4[n/24]+4$ に一致する場合を極値的とよぶ。長さ64以下（8の倍数）と長さ80においては、1970年代前半にはすでに極値的な自己双対2元符号が少なくとも1つは存在することが分かっていたが、長さ72では、構成への様々試みは上手くいかなかった。このような背景のもとで、1973年に、この分野の第一人者の一人である Sloane が *IEEE Trans. Information Theory* に発表した論文の中で、長さ72の極値的な重偶自己双対2元符号の存在性を決定せよ、という問題提起を行なった。このこともあり、今日では、代数的符号理論において非常に有名な問題として認識されている。

  1990年代になって符号のアルファベットを有限体ではなく有限環、特に整数の剰余環にし

た研究も活発に行なわれるようになって来た。一つの結果として、重偶自己双対2元符号の自然な拡張として、位数 $2k$ の整数の剰余環$\mathbb{Z}_{2k}$ 上にも重偶自己双対符号が定義されていることが挙げられる（k =1 の場合がちょうど重偶自己双対2元符号に対応）。重偶自己双対2元符号との類似性も非常に多くみられ、例えば、長さ72に関しては極値的な符号が2元符号のときと同様に定義されている。

本さきがけ研究では、長さ72の$\mathbb{Z}_{2k}$ 上の極値的な重偶自己双対符号の構成に取り組んだ。2以上の全ての整数kに対して、長さ24の$\mathbb{Z}_{2k}$ 上の極値的な重偶自己双対符号が存在すること（Chapman (2000)、Gulliver-Harada (2001)）と72次元の極値的な偶ユニモジュラー格子の構成（Nebe（印刷中））を用いて、4以上の全ての偶数kに対して、長さ72の$\mathbb{Z}_{2k}$ 上の極値的な重偶自己双対符号が存在すること示すことが出来た（論文は投稿準備中）。あらゆるkに対しても長さ72の$\mathbb{Z}_{2k}$ 上の極値的な重偶自己双対符号の存在が分かったのは今回が初めてである。

このテーマに関するその他の研究成果としては、論文発表の [2], [3], [9] があり、特に [2] では長さ56と64において$\mathbb{Z}_4$ 上の極値的な重偶自己双対符号に成功した（長さ72については上で述べた通り未解決である）。

◆ 計算機の支援による自己双対符号の分類問題への新たな方法での取り組み：

組合せ構造における基本的な研究として構成と分類への取り組みが挙げられる。符号を組合せ構造の1つだと考えて、本さきがけ研究では、上のテーマでも扱った自己双対符号に対して、計算機の支援によりその分類問題に取り組んだ。その中で最も重要だと思われる結果は、長さ40の重偶自己双対2元符号の分類を完成させることが出来たことである（Betsumiya-Munemasa との共同研究、論文は投稿中）。上でも述べた通り、重偶自己双対2元符号は長さが8の倍数のときのみ存在することが分かっている。重偶自己双対2元符号の分類は1972年に Pless によって始められ、そこでは長さ8と16のときの分類が完成した。その後、1975年に Pless-Sloane によって長さ24のときの分類が完成し、1992年に Conway-Pless-Sloane によって長さ32のときの分類が完成している。長さ32までの分類において採用された方法では長さ40の分類は難しいと思われ、本さきがけ研究において、新たな方法を開発することで長さ40の分類を完成させることが出来た。非同値な重偶自己双対2元符号の個数を次の表にまとめる：

長さ	8	16	24	32	40
個数	1	2	9	85	94343

このテーマに関するその他の研究成果として、論文発表の [1] ではユニモジュラー格子のフレームとよばれる特別な部分集合の分類に帰着させることで$\mathbb{Z}_k$ 上の自己双対符号（k =4, 6, 8 ,9, 10）の分類を進めることが出来、例えばk=4 では長さ19まで分類を拡張させた。また、3元体、4元体上の自己双対符号とそれに関連したアダマール行列などの組合せ構造の分類についても取り組んだ（論文発表 [6], [7], [8], [10]）。

◆ 量子符号への応用を目指した組合せ構造の研究：

様々なタイプの量子符号に関する研究が行なわれているが、本さきがけ研究で主に考えた

量子符号は次の論文の中で考えられている加法的な [[n, k, d]] 量子符号とよばれるものである:

Calderbank-Rains-Shor-Sloane, Quantum error correction via codes over GF(4), *IEEE Trans. Information Theory* **44** (1998), 1369-1387。

特に、この論文では、4元体 GF(4) 上の(線形とは限らない)加法的な自己直交符号が加法的な量子符号に対応していることが示されている。ここで、与えられた符号が双対符号に含まれるときに自己直交符号とよばれる。(古典的な符号理論と同じように)n, k を固定した際に加法的な [[n, k, d]] 量子符号が存在する最大の d を決定することが基本的な問題として考えられる。なお、次のデータベースで最新の結果がまとめられている:

Grassl, Code Tables, http://www.codetables.de。

さきがけ研究の以前に行なって来た(線形である)自己双対符号の研究を広げることでGF(4) 上の加法的な自己直交符号の研究に取り組んだ。ここでは、全ての GF(4) 上の加法的な自己双対符号(k=0 となる自己直交符号)はあるグラフから構成されるという結果(Danielsen-Parker (2006)) に着目した。つまり、組合せ構造の1つであるグラフから自己双対量子符号が得られる訳である。正則(各頂点の次数が等しい)グラフの中から対称性の高いものを選び、構成される自己双対量子符号についての解析を行ない、特に、次の長さ n において上記のデータベースにおける今までの記録を更新する大きな d を持つ自己双対量子符号の構成に成功した:

n	56	57	63	70
d	15	15	16	16

このテーマに関するその他の研究成果として、論文発表の [4] と [5] では、ジャンプ量子符号とよばれる量子符号を与えることが出来る組合せ構造を構成するために互いに素な組合せデザインの構成に関する研究を行なった。

3つのテーマへの取り組み以外の研究活動の報告としては、まずはさきがけ研究の以前には参加していなかった工学的な立場での符号理論の研究集会やセミナーなどに参加した。また、2010年8月に開催されたRIMS合宿型セミナー「組み合わせ構造の解析と情報理論への応用」に参加し、工学的な立場での符号理論の研究者(企業に所属する研究者を含む)との交流を図った。数理科学的な立場と工学的な立場での符号理論における最新の動向を理解するために、2010年12月に上智大学理工学部で行なわれた「数学系と情報系の符号理論研究者の交流会」の世話人をした(共同)。さらに、何名かの工学的な立場での符号理論の研究者を山形大学理学部に直接招聘することで交流を行なった。また、この領域の一般に対する働きかけの活動の一環として、2011年2月に山形大学理学部で行なわれた第1回のJST数学キャラバン「拡がりゆく数学 in 山形」の世話人を行ない、2011年8月に金沢市で行なわれた第3回JST数学キャラバン「共生する数学」では符号理論の研究について一般向けに講演を行なった。

3, 今後の展開

有限環 $\mathbf{Z}_{2k}$ 上の長さ72の極値的な重偶自己双対符号の存在については、本さきがけ研究

で部分的な解決を行なうことが出来たことから、当初の目標であった長さ72の極値的な重偶自己双対2元符号の存在性を決定する未解決問題の解決の糸口を見付けることが出来るのではないかと期待している。次に、自己双対符号の分類問題については、本さきがけ研究で完成することが出来た分類の結果を他の組合せ構造などの問題に帰着させることを考えている。また、工学的な立場での興味の対象である符号の幾つかのクラスについて分類問題を考えることも意味があるのではないかと考えており、本さきがけ研究で得られたことを発展させることによって、今後はこのような符号の分類問題にも取り組みたい。量子符号への応用を目指した組合せ構造の研究については、今後はグラフ理論だけでなく幅広く量子符号に関係する組合せ構造の研究が行なえると考えている。また、量子符号の構成に用いたGF(4) 上の加法的な自己直交符号は、量子符号化における離散的な数理モデルとみなすことも出来る。本さきがけ研究では、3つのテーマの対象である符号を中心に研究をして来たが、今後は、離散的な現象や構造の数理モデルとみなせる符号以外の組合せ構造の研究も幅広く行ないたい。

4，自己評価

1つ目のテーマである「長さ72の極値的な重偶自己双対2元符号の存在性を決定する未解決問題への挑戦」については、k が4以上の偶数のときに位数 $2k$ の有限環 $\mathbf{Z}_{2k}$ 上の長さ72の極値的な重偶自己双対符号の存在性を決定することが出来たが、申請時の目標であった長さ72の極値的な重偶自己双対2元符号（上の符号のk=1 の場合にあたる）の存在性を決定させることは残念ながら本さきがけ研究期間内には達成出来なかった。原因としては上記の結果さえ得るのに非常に時間が掛かり、2元符号の場合への取り組みが十分出来なかったことが挙げられる。$\mathbf{Z}_{2k}$ 上の長さ72の極値的な重偶自己双対符号で存在が未解決な場合も含めて、今後も解決に向けての取り組みを続けていきたい。2つ目のテーマである「計算機の支援による自己双対符号の分類問題への新たな方法での取り組み」については、幾つかの自己双対符号の分類を行なう方法を開発し、特に、最大課題であった長さ40の重偶自己双対2元符号の分類を完成させることが出来たので、このテーマに関しては十分な結果が得られたと考えている。最後のテーマである「量子符号への応用を目指した組合せ構造の研究」については、今までの記録を更新する大きな最小重みを持つ加法的な自己双対量子符号の構成を組合せ構造であるグラフを考えることで行なった。このことは、古典的な符号理論における枠組みと比較すれば、量子符号の枠組みにおける代数的符号理論の立場での研究と見なすことが出来るはずで、この側面からの研究を行なうことはメリットがあると思われる。

また、3つのテーマへの取り組みの他に、さきがけ研究以前では参加していなかった工学的な立場での符号理論の研究集会やセミナーなどに参加し、工学的な立場での符号理論の研究者と交流を図る機会を作った。その交流から幾つかの研究の芽となるアイデアを得ることが出来たので、今後もこの活動を続けて、今までになかったような符号理論の展開に少しでも寄与したいと考えている。

5，研究総括の見解

符号理論の数学的整備はデジタル通信の発展に不可欠のものである。とりわけ誤り訂正符号理論は重要である。原田氏は代数的見地から自己双対符号の研究を行い、4以上の全ての偶数を位数とする整数の剰余環上の長さ72の極値的な重偶自己双対符号の存在証明を初めて

行うなどこの方面での顕著な成果を残したことは高く評価できる。

同時に計算機支援による自己双対符号の分類、とりわけ困難と思われた長さ40の分類を新たな方法の開発と共に成し遂げたことは、より一般的な状況への可能性を示唆するものである。さらに量子符号への応用を目指した組み合わせ構造からのアプローチは今後の発展が大いに期待される。

一方、企業での研究者を含む情報理論、符号理論の研究者との横断的交流会の組織やアウトリーチ活動も積極的に行い、本領域の認知度も高めることにも貢献したことも評価したい。

6, 主な研究成果リスト

(1)論文(原著論文)発表

1. M. Harada and A. Munemasa, On the Classification of Self-Dual $\mathbb{Z}_k$-Codes, *Lecture Notes in Comput. Sci.* **5921**, 78-90 (2009)
2. M. Harada, Extremal Type II $\mathbb{Z}_4$-Codes of Lengths 56 and 64, *Journal of Combinatorial Theory, Series A* **117**, 1285-1288 (2010)
3. M. Harada and T. Miezaki, An Upper Bound on the Minimum Weight of Type II $\mathbb{Z}_{2k}$-Codes, *Journal of Combinatorial Theory, Series A* **118**, 190-196 (2010)
4. M. Araya and M. Harada, Mutually Disjoint Steiner Systems $S(5,8,24)$ and 5-(24,12,48) Designs, *Electronic Journal of Combinatorics* **17**, #N1 (2010)
5. M. Araya, M. Harada, V.D. Tonchev and A. Wassermann, Mutually Disjoint Designs and New 5-Designs Derived from Groups and Codes, *Journal of Combinatorial Designs* **18**, 305-317 (2010)
6. K. Betsumiya, M. Harada and H. Kimura, Hadamard Matrices of Order 32 and Extremal Ternary Self-Dual Codes, *Designs, Codes and Cryptography* **58**, 203-214 (2011)
7. M. Harada, C. Lam, A. Munemasa and V.D. Tonchev, Classification of Generalized Hadamard Matrices H(6,3) and Quaternary Hermitian Self-Dual Codes of Length 18, *Electronic Journal of Combinatorics* **17**, #R171 (2010)
8. M. Harada and A. Munemasa, Classification of Quaternary Hermitian Self-Dual Codes of Length 20, *IEEE Trans. Information Theory* **57**, 3758-3762 (2011)
9. M. Harada and T. Miezaki, An Optimal Odd Unimodular Lattice in Dimension 72, *Archiv der Mathematik* **97**, 529-533 (2011)
10. M. Harada and A. Munemasa, On the Classification of Weighing Matrices and Self-Orthogonal Codes, *Journal of Combinatorial Designs* **20**, 40-57 (2012)

(2)特許出願

なし

(3)その他の成果(主要な学会発表、受賞、著作物等)

1. 招待講演:M. Harada、On the Classification of Extremal Type II $\mathbb{Z}_4$-Codes of Length 24、Korea-Japan Workshop on Algebra and Combinatorics、2009 年 2 月 9 日

2. 招待講演：M. Harada、Mutually disjoint 5-designs and new 5-designs、One Day Workshop on Algebraic Combinatorics、2009 年 10 月 14 日
3. 招待講演：原田昌晃、自己双対符号とその周辺、第 55 回代数学シンポジウム、2010 年 8 月 12 日
4. 招待講演：原田昌晃、Self-dual codes –an introduction–、第 9 回代数学と計算、2011 年 11 月 8 日
5. 解説記事： 原田昌晃・木田雅成、「Magma」、数学セミナー、2010 年 9 月号、44-47 日本評論社.
6. 解説記事： 原田昌晃、「72次元の極値偶ユニモジュラー格子の存在について」、数学セミナー、2012 年 1 月号、13-17 日本評論社.