様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成　24　年　5　月　11　日現在

機関番号：２４４０３
研究種目：基盤研究（C）
研究期間：2008 ～ 2011
課題番号：20540129
研究課題名（和文）　最適線形符号問題に関する研究

研究課題名（英文）　Optimal Linear Codes Problem

研究代表者
丸田　辰哉（MARUTA TATSUYA）
大阪府立大学・大学院理学系研究科・教授
研究者番号：80239152

研究成果の概要（和文）：
q 元体上の線形符号には、３つの重要なパラメータ：長さ n、次元 k、誤り訂正能力を表す最小距離 d がある。このような線形符号を $[n,k,d]_q$ 符号と呼ぶ。与えられた n, k, q の値に対して $[n,k,d]_q$ 符号が存在するような d の最大値 $d_q(n,k)$ を求める問題（これは、与えられた q, k, d の値に対して $[n,k,d]_q$ 符号が存在するような n の最小値 $n_q(k,d)$ を求める問題と等価）は代数的符号理論における基礎的な未解決問題の一つであり、最適線形符号問題と呼ばれている。具体的には、q=3,4,5,8 や一般の q に対して、最適線形符号問題に取り組み、（誤り訂正能力の高い）新しい線形符号の構成、及び、存在性が不明な線形符号（例えば、既知の限界式で等号をみたすような符号）の非存在の証明等の成果を得た。

研究成果の概要（英文）：
A linear code over the field of q elements has three important parameters: length n, dimension k and minimum distance d which indicates the ability for error correction. Such a code is called an $[n,k,d]_q$ code. A fundamental problem in coding theory is to optimize one of the parameters n,k,d for given the other two, which is called the Optimal Linear Codes Problem. We have mainly tackled the problem to find $n_q(k,d)$, the smallest possible length n for fixed dimension k and the minimum distance d over the field of q elements, especially for q=3,4,5,8. We have obtained several new results on the problem by constructing new codes and showing the nonexistence of some linear codes attaining the known bound.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,100,000	330,000	1,430,000
2009 年度	700,000	210,000	910,000
2010 年度	700,000	210,000	910,000
2011 年度	700,000	210,000	910,000
年度			
総　計	3,200,000	960,000	4,160,000

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：線形符号、誤り訂正、最適符号、符号の拡張、Griesmer 限界、射影幾何

１．研究開始当初の背景

(1) 情報ネットワーク化の進む現在、より高品質で高効率の情報の伝送・記録の手段及び方法が求められている。そのためには、情報を伝送または記録する際に生じる誤りを正しく訂正できる確率が大きな「誤り訂正符号」を構成する必要がある。

(2) q 元体上の線形符号には、３つの重要なパラメータ：長さ n、次元 k、誤り訂正能力を表す最小距離 d がある。このような線形符号を $[n,k,d]_q$ 符号と呼ぶ。与えられた n, k, q の値に対して $[n,k,d]_q$ 符号が存在するような d の最大値 $d_q(n,k)$ を求める問題は、与えられた q, k, d の値に対して $[n,k,d]_q$ 符号が存在するような n の最小値 $n_q(k,d)$ を求める問題と等価であり、これは「最適線形符号問題」と呼ばれる代数的符号理論における基礎的な未解決問題の一つである。

(3) (2) の $n_q(k,d)$ を決定する問題は、$q=2$ のときは８次元まで、$q=3$ のときは５次元までしか完全には解決していない。特に、$(q,k)=(3,6)$ の場合は、1993 年に先行研究が始まっているが、長年研究が停滞していた。

２．研究の目的

(1) 研究全体の目的は、「研究開始当初の背景」で述べた最適線形符号問題を解決することである。q, k を固定した場合、d が十分大きければ Griesmer 符号（n の下限を与える Griesmer 限界で等号をみたす符号）が存在することから、有限個の d の値について $n_q(k,d)$ を決定すればよいことになる。

(2) $n_q(k,d)$ を決定するためには、存在性が不明なパラメータを持つ新しい線形符号を構成して $n_q(k,d)$ の上限を改良するか、存在性が不明なパラメータを持つ線形符号の非存在を証明して $n_q(k,d)$ の下限を改良するか、或いは、これら両方を行う必要がある。

(3) 線形符号の非存在を証明するために有効な手段として、線形符号の拡張可能性を利用する方法がある。しかし、線形符号の拡張可能性に関する研究は、$q=2,3$ 以外は未だあまり進んでおらず、解明すべきことが数多く残されている。一方、拡張可能性が分かると、新しい符号から更に新しい符号の構成が可能になるメリットもあり、拡張可能性のメカニズムを解明することも最適線形符号問題を解く重要な鍵と言える。

３．研究の方法

本研究を遂行するために、(1) 新しい線形符号を構成する幾何学的な手法の開発、(2) 3 元線形符号の拡張可能性の解明とその一般化、(3) (1), (2)に基づいた 3 元線形符号の最適線形符号問題の研究、(4) 3 元以外の線形符号の拡張可能性の解明、(5) 3 元以外の最適線形符号問題の研究、を行う。

(1) 新しい符号を構成する従来の研究は、巡回符号を一般化した QC 符号や QT 符号として構成するか、自己同型群の要素を仮定してコンピュータを用いて探索する方法が主流であったが、最適な線形符号は幾何学的に意味のある構造を持つ場合が多く、その構造に着目してヒューリスティックに構成する方法を開発する。

(2) 3 元線形符号の拡張可能性については、先行研究において詳細に調べられているが、完全に解明されているとは言い難い。また、それらの一般化は部分的にしか知られていない。この研究においても、幾何学的な手法は非常に有効である。

(3) (1), (2) の結果を駆使して、$(q,k)=(3,6)$ の場合の最適線形符号問題に取り組む。

(4) 3 元線形符号の拡張可能性に関する結果は、gcd(d, q)=1 の場合の$[n,k,d]_q$ 符号の拡張可能性に一般化することができる場合がある。しかし、gcd(d, q)>1 の場合は別に検討する必要がある。

(5) (4) に関連して、(q, k)=(8, 4)の場合の最適線形符号問題に取り組む。このためには、射影平面 PG(2,8)の最適な(n,r)-arc の分類が必要となる。また、一般の q 元体での未解決な場合にも取り組む。

４．研究成果

「研究方法」の(1)～(5)のそれぞれについて、以下のような成果が得られた。

(1) d が十分大きい場合の Griesmer 符号の構成を一般化して、ある条件を満たす既存の最適な符号に対応する射影空間の多重集合から flat を取り除くことによって最適な符号を構成する方法を開発した。この方法と射影双対による構成方法を組み合わせることにより、$(q,k)=(3,6)$, $(8,4)$ の場合に多くの新しい線形符号を構成することができた。今後は、与えられた多重集合が必要な flat を含むか否かを判定する効率の良いアルゴリズムを開発したい。

(2) q 元線形符号の拡張定理として最も有名な Hill-Lizak の定理は、符号語の重みが q を法として２種類しかない非常に特別な場合であるが、我々は 3 元線形符号の拡張定理を符号語の重みが q を法として 3 種類しかない 3-weight (mod q) 符号の拡張定理に一般化することができた。また、3 元線形符号の拡張可能性が、quadric（2 次超曲面）と深い関わりがあることが分かった。このことから、拡張不可能な 3 元線形符号が満たすべき新たな条件が得られた。q>3 の場合も同様の結果が得られるか否かは、今後の課題である。

(3) (2) の条件を使って、今まで存在性が不明であったいくつかの 3 元線形符号の非存在

を幾何学的に証明することができた。結果として、未解決であった 23 個の d について、n3(6, d)の値を決定することができた。
(4) (q,k)=(8,4) の場合の最適線形符号問題に取り組むために、gcd(d, q)=2 の場合の q 元線形符号の拡張定理を証明した。これは、gcd(d, q)=1 でない場合の初めての拡張定理であり、特に最適線形符号問題の研究が盛んなヨーロッパの研究者に大きなインパクトを与え、イタリアで開かれた組合せ論に関する大きな国際会議 Combinatorics2010 にて招待講演を行うことになった。
(5) (q,k)=(8,4) の場合の最適線形符号問題に取り組み、多くの成果を上げた。この場合で全ての d について n8(4,d)の表を可能な限り作成したのは世界初の試みであり、著名な学術雑誌に掲載された。また、これに関連して、PG(2,8)の(42,6)-arc の分類が必要になり、コロラド州立大学の A. Betten 准教授らと共に理論とコンピュータを駆使して分類を行った。また、大阪女子大学名誉教授の濱田昇氏と共に、一般の q 元体上の Griesmer 限界の改良にも取り組み、成果を得た。

以上のように、(q,k)=(3,6), (8,4) 等の場合の最適線形符号問題において、多くの成果を上げることができたが、未解決のまま残っている場合も多数あり、完全解決までには更に新しいアイデアが必要であると考えられる。

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 15 件）

① T. Maruta, Y. Yoshida, A generalized extension theorem for linear codes, Designs, Codes and Cryptography 62, 査読有, 2012, 121-130
② A. Betten, E.J. Cheon, S.J. Kim, T. Maruta, The classification of $(42,6)_8$-arcs, Advances in Mathematics of Communications 5, 査読有, 2011, 209-223
③ T. Maruta, Y. Oya, On optimal ternary linear codes of dimension 6, Advances in Mathematics of Communications 5, 査読有, 2011, 505-520
④ N. Hamada, T. Maruta, Note on an improvement of the Griesmer bound for q-ary linear codes, Serdica Journal of Computing 5, 査読有, 2011, 199-206
⑤ T. Maruta, Extension theorems for linear codes over finite fields, Journal of Geometry 101, 査読有, 2011, 173-183
⑥ R. Kanazawa, T. Maruta, On optimal linear codes over F_8, Electronic J. Combinatorics 18, 査読有, 2011, #P34(27pp)
⑦ Y. Yoshida, T. Maruta, An extension theorem for [n,k,d]q codes with gcd(d,q) = 2, Australasian J. Combinatorics 48, 査読有, 2010, 117-131
⑧ N. Hamada, T. Maruta, An improvement to the achievement of the Griesmer bound, Serdica Journal of Computing 4, 査読有, 2010, 301-320
⑨ E.J. Cheon, T. Maruta, A new extension theorem for 3-weight modulo q linear codes over F_q, Designs, Codes and Cryptography 52, 査読有, 2009, 171-183
⑩ T. Maruta, A. Kikui, Y. Yoshida, On the uniqueness of (48,6)-arcs in PG(2,9), Advances in Mathematics of Communications 3, 査読有, 2009, 29-34
⑪ Y. Yoshida, T. Maruta, Ternary linear codes and quadrics, The Electronic Journal of Combinatorics 16, 査読有, 2009, #9(21pp)

〔学会発表〕（計 17 件）

① T. Maruta, On optimal ternary linear codes, The 35th Australasian Conference on Combinatorial Mathematics & Combinatorial Computing, 2011年 12月 5日, Monash大学, Melbourne(オーストラリア)
② T. Maruta, On the minimum length of ternary linear codes, Finite Geometries 2011 - Third Irsee Conference, 2011年 6月 24日, Irsee（ドイツ）
③ 丸田辰哉, On optimal ternary linear codes, 実験計画法およびその周辺領域における組合せ構造の解明とその応用, 2010年 11月 30日, 城崎（兵庫）
④ T. Maruta, New ternary linear codes of dimension 6, ACCT2010, 2010年 9月 6日, Novosibirsk（ロシア）
⑤ 丸田辰哉, A generalized extension theorem for linear codes, 離散数学とその応用研究集会 2010, 2010 年 7 月 31 日, 高知大学
⑥ T. Maruta, Extension theorems for linear codes over finite fields, Combinatorics 2010, 2010年 6月 29日, Verbania (イタリア)
⑦ T. Maruta, An improvement of Landjev-Rousseva's extension theorem for linear codes, 33rd Australasian Conference on Combinatorial Mathematics and Combinatorial Computing, 2009 年 12 月 8 日,

Newcastle (Australia)

⑧ T. Maruta, On the nonexistence of some q-ary linear codes meeting the Griesmer bound, 9th International Conference on Finite Fields and Applications (Fq9), 2009年 7月 13日, Dublin (Ireland)

⑨ T. Maruta, On the classification of (n,r)-arcs in PG(2,q), Fourth Int. Conference on Combinatorial Mathematics and Combinatorial Computing, 2008年 12月 18日, Auckland (ニュージーランド)

⑩ T. Maruta, Extendability of linear codes over F_q, Eleventh International Workshop on Algebraic and Combinatorial Coding Theory, 2008年 6月 18日, Pamporovo (ブルガリア)

〔図書〕(計0件)

〔その他〕
ホームページ等
http://www.mi.s.osakafu-u.ac.jp/~maruta/griesmer.htm

6．研究組織

(1)研究代表者
丸田　辰哉 (MARUTA TATSUYA)
大阪府立大学・大学院理学系研究科・教授
研究者番号：80239152

(2)研究分担者
(　　)

研究者番号：

(3)連携研究者
(　　)

研究者番号：