

## 科学研究費助成事業 研究成果報告書

平成 28 年 5 月 24 日現在

機関番号：24403

研究種目：基盤研究(C) (一般)

研究期間：2012～2015

課題番号：24540138

研究課題名(和文) 線形符号の誤り訂正限界に関する幾何学的研究

研究課題名(英文) A Geometric Study on the Bound for Error-Correcting Linear Codes

研究代表者

丸田 辰哉 (MARUTA, Tatsuya)

大阪府立大学・理学(系)研究科(研究院)・教授

研究者番号：80239152

交付決定額(研究期間全体)：(直接経費) 3,900,000円

研究成果の概要(和文)：長さ  $n$ 、次元  $k$ 、最小距離  $d$  の  $q$  元体上の線形符号を  $[n, k, d]_q$  符号と呼ぶ。 $[n, k, d]_q$  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、 $[n, k, d]_q$  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る。本研究では、射影空間を通じた幾何学的手法を用いて、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 with length  $n$ , dimension  $k$  and minimum distance  $d$  is called an  $[n, k, d]_q$  code. A fundamental research problem in coding theory is to find  $d_q(n, k)$ , the maximum value of  $d$  for which an  $[n, k, d]_q$  code exists (this problem is equivalent to find  $n_q(k, d)$ , the minimum value of  $n$  for which an  $[n, k, d]_q$  code exists). In this work, 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 using the geometric methods through projective geometry over finite fields.

研究分野：代数的符号理論

キーワード：線形符号 最適符号 符号の拡張 Griesmer 限界 有限幾何 射影幾何

### 1. 研究開始当初の背景

(1)  $q$  元体上の長さ  $n$ , 次元  $k$ , 最小距離  $d$  の線形符号 ( $[n,k,d]_q$  符号) が存在する限界を決定する (具体的には、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  $d_q(n,k)$  や、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) 問題は、代数的符号理論において最も基本的かつ古典的な研究課題の一つである。

(2)  $n_q(k,d)$  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、 $q=4$  のときは 4 次元まで、 $q=5,7,8,9$  のときは 3 次元までしか完全には解決していない。11 以上の  $q$  に対しては、 $n_q(3,d)$  の値すら決定できていない  $d$  の値が存在する。

(3) 新しい符号の構成と符号の非存在証明の両方に応用可能な研究として注目されている線形符号の拡張可能性については、 $q=3$  の場合はほぼ調べ尽くされているが、 $q$  が 4 以上の場合に定理として知られている結果は極めて限定的である。

### 2. 研究の目的

(1) 研究全体の目的は、「研究開始当初の背景」(1) で述べた線形符号の存在限界に関する未解決問題を解決すること、即ち、全ての  $q, k, d$  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  $n_q(k,d)$  を求めることである。 $q$  と  $k$  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が、 $(q, k) = (3,6), (4,5), (5,4)$  などの場合で長年未解決である難問が存在する。

(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いないため、 $q=4$  の場合の拡張可能性のメカニズムの解明やその一般化が本研究の当初の目的となる。

### 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手法の開発、(2) 4 元線形符号の拡張可能性の解明とその一般化、(3) (1), (2) に基づいた線形符号の存在限界に関する研究、特に、新しい符号の幾何学的手法の開発や Griesmer 符号の非存在証明の研究を行う。

(1) 比較的調べ易い奇素数 (特に  $q=3,5$ ) の場合の最適な符号の構成方法をコンピュータを用いて調べ、生成行列から得られる射影空間の多重集合の幾何学的手法を解明す

る。 $q$  が素数でない場合は、3 次元の最適な符号に対応する射影平面上の arc や blocking set を調べる。

(2) 4 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のは 3 次元の場合のみで、最小距離が奇数の場合に限られていた。そこで、4 元線形符号の拡張可能性に関連して現れる有限射影空間の奇集合 (任意の line と奇数個の点で交わる集合) の幾何学的手法を決定し、更に一般化を図る。

(3) 小さな体上の線形符号について得られた知見を分析し、 $q$  元体上のより広範囲の  $d$  に対する最適な線形符号の構成方法や Griesmer 符号の非存在証明へ発展させる。

### 4. 研究成果

(1) 最適な符号、またはそれに近い線形符号の生成行列から得られる射影空間の多重集合から、幾何学的手法を削除することによって最適な符号を構成する Geometric Puncturing に関する新たな知見を得た。特に、長さが比較的小さい divisible な (符号語の重みが全てある正整数 ( $>1$ ) で割り切れる) 線形符号を用いて、長さが比較的大きな値の新しい符号を構成する際に有効であると考えられる。

(2) まず  $q=4, k=5$  の場合に取り組み、 $d \equiv 2 \pmod{4}$  の 4 元線形符号に関連して現れる射影空間  $PG(r,4)$  の奇集合について調べ、 $r=4$  のときの分類を得た。更に、その分類を応用して、4 元線形符号に対する新しい拡張定理を証明した。また、 $PG(r,4)$  の奇集合の分類を応用して、 $d \equiv 2 \pmod{4}$  のときの 4 元線形符号の 2 重拡張可能性や  $d \equiv 1 \pmod{4}$  のときの 4 元線形符号の 3 重拡張可能性などに関する新たな拡張定理を得た。これらの成果は、今後、4 元線形符号の存在限界を求める研究において活用されることが期待される。一方、一般の  $q$  元線形符号の拡張可能性についても、Hill-Lizak (1995) や Simonis (2000) らの拡張定理の新たな一般化が得られた。その成果の一つは、符号語の重みが  $q$  を法として 4 種類しかない 4-weight ( $\pmod{q}$ ) 符号に対する初めての拡張定理を与えている点で、注目に値する。

(3) 具体的な問題として、まず  $n_5(5,d)$  の決定問題に取り組み、Projective Dual や Geometric Puncturing といった幾何学的手法を駆使して、新しい線形符号を構成することができた。Projective Dual を適用する上で必要な 5-divisible な線形符号は、主に QC(quasi-cyclic) 符号やその拡張符号として、コンピュータを用いて構成した。更に、幾何学的手法を使って、存在性が不明であった Griesmer 符号の非存在証明も行った。これらの成果は、ブルガリア科学アカデミーの Iliya Bouyukliev 教授および大学院生との共同研究として、国際学術雑誌 Discrete Mathematics に掲載された。次に、この研究

の中で発見された 5-divisible である線形符号を詳細に分析した結果、それらの 1 つを  $q$  元体上の  $q$ -divisible な線形符号の構成に一般化することに成功し、 $q$  元体上の新しい最適な線形符号の構成が得られた。特に、 $q$  元体上の Griesmer 符号を構成した結果は、著名な国際学術雑誌 Designs, Codes and Cryptography に掲載された。また、新たな試みとして、 $q$  が比較的大きな値のときの 4 次元線形符号の存在限界についても、大学院生達と共に考察を行い、巡回符号の一般化である QC 符号や QT 符号を更に代数的に一般化した符号として最適な線形符号を構成する手法や、Griesmer 符号の非存在に関する新たな知見が得られた。4 次元の Griesmer 符号の非存在結果の一部は、minihyper の分類に関する最新結果を利用することにより、 $k$  次元 ( $k > 4$ ) の非存在定理に一般化することができた。一方、上記以外の海外の研究者との共同研究としては、8 元体上の射影平面の arc の分類を一般化して、射影平面の新たな多重 blocking set の構成を行った。その成果は、国際学術雑誌 Designs, Codes and Cryptography に掲載された。

#### 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 18 件)

K. Kumegawa, T. Maruta, Nonexistence of some Griesmer codes over  $F_q$ , Discrete Mathematics 339, 査読有, 2016, 515-521

DOI:10.1016/j.disc.2015.09.030

H. Kanda, T. Tanaka, T. Maruta, On the 1-extendability of quaternary linear codes, Finite Fields and their Applications 35, 査読有, 2015, 159-171

DOI:10.1016/j.ffa.2015.04.004

I. Bouyukliev, Y. Kageyama, T. Maruta, On the minimum length of linear codes over  $F_5$ , Discrete Mathematics 338, 査読有, 2015, 938-953

DOI:10.1016/j.disc.2015.01.010

Y. Kageyama, T. Maruta, On the construction of Griesmer codes of dimension 5, Designs, Codes and Cryptography 75, 査読有, 2015, 277-280

DOI:10.1007/s10623-013-9914-4

T. Maruta, T. Tanaka, H. Kanda, Some generalizations of extension theorems for linear codes over finite fields, Australasian J. Combinatorics 60, 査読有, 2014, 150-157

[http://ajc.maths.uq.edu.au/?page=get\\_volumes&volume=60](http://ajc.maths.uq.edu.au/?page=get_volumes&volume=60)

T. Tanaka, T. Maruta, A character-

ization of some odd sets in projective spaces of order 4 and the extendability of quaternary linear codes, Journal of Geometry 105, 査読有, 2014, 79-86

DOI:10.1007/s00022-013-0195-x

T. Tanaka, T. Maruta, Classification of the odd sets in  $PG(4,4)$  and its application to coding theory, Applicable Algebra in Engineering, Communication and Computing 24, 査読有, 2013, 179-196

DOI:10.1007/s00200-013-0201-4.

T. Maruta, Construction of optimal linear codes by geometric puncturing, Serdica Journal of Computing 7, 査読有, 2013, 73-80

<http://serdica-comp.math.bas.bg/index.php/serdicajcomputing/issue/view/39>

T. Maruta, Y. Oya, On the minimum length of ternary linear codes, Designs, Codes and Cryptography 68, 査読有, 2013, 407-425

DOI:10.1007/s10623-011-9593-y

A. Betten, E.J. Cheon, S.J. Kim, T. Maruta, Three families of multiple blocking sets in Desarguesian projective planes of even order, Designs, Codes and Cryptography 68, 査読有, 2013, 49-59

DOI:10.1007/s10623-012-9634-1

N. Hamada, T. Maruta, Y. Oya, A necessary and sufficient condition for the existence of an  $(n,r)$ -arc in  $PG(2,q)$  and its applications, Serdica Journal of Computing 6, 査読有, 2012, 253-266

<http://serdica-comp.math.bas.bg/index.php/serdicajcomputing/issue/view/37>

[学会発表](計 29 件)

T. Maruta, On the construction of triple blocking sets in  $PG(2, q)$ , 第 4 回 日台組合せ論コンファレンス(4th JTCCA), 2016 年 3 月 5 日, 北九州国際会議場(福岡県)

T. Maruta, On the constructions of optimal linear codes, Combinatorics and Computer Algebra 2015(CoCoA15), 2015 年 7 月 22 日, コロラド州立大学, Fort Collins(アメリカ)

T. Maruta, On the geometric construction of optimal linear codes, ALCOMA 15, 2015 年 3 月 17 日, Kloster Banz(ドイツ)

Y. Kageyama, T. Maruta, On the construction of optimal codes over  $F_q$ , 14th International Workshop on Algebraic and Combinatorial Coding

Theory, 2014年9月10日, Svetlogorsk (ロシア)

陰山佑樹, 丸田辰哉, On the minimum length of linear codes over  $F_5$ , 2013年度応用数学合同研究集会, 2013年12月21日, 龍谷大学(滋賀県)

T. Maruta, Extension problem for linear codes, 37ACCMCC, 2013年12月9日, Crawley (オーストラリア)

T. Maruta, T. Tanaka, H. Kanda, New extension theorems for codes over  $F_q$ , 7th International Workshop on Optimal Codes and Related Topics, 2013年9月7日, Albena (ブルガリア)

T. Maruta, Geometric puncturing for linear codes over finite fields, 36ACCMCC, 2012年12月11日, Kensington (オーストラリア)

T. Maruta, Optimal 4-dimensional linear codes over finite fields, KIAS International Conference on Coding Theory and Applications, 2012年11月15日, Seoul (韓国)

丸田辰哉, Constructing new linear codes by projective puncturing, 離散数学とその応用研究集会 2012, 2012年8月10日, 茨城大学(茨城県)

T. Maruta, Optimal 4-dimensional linear codes over  $F_8$ , 13th International Workshop on Algebraic and Combinatorial Coding Theory, 2012年6月16日, Pomorie (ブルガリア)

〔図書〕(計0件)

〔産業財産権〕

出願状況(計0件)

名称：  
発明者：  
権利者：  
種類：  
番号：  
出願年月日：  
国内外の別：

取得状況(計0件)

名称：  
発明者：  
権利者：  
種類：  
番号：  
取得年月日：  
国内外の別：

〔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・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：