

令和 3 年 5 月 20 日現在

機関番号：24403

研究種目：基盤研究(C) (一般)

研究期間：2016～2020

課題番号：16K05256

研究課題名(和文)最適線形符号問題に関する幾何学的研究

研究課題名(英文)A Geometric Study on Optimal Linear Codes Problem

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) 3,500,000円

研究成果の概要(和文)： $q$ 元体上の長さ  $n$ 、次元  $k$ 、最小重み  $d$  の線形符号を  $[n,k,d]_q$  符号と呼ぶ。線形符号の存在限界を決定する問題(特に、 $[n,k,d]_q$  符号が存在するような長さ  $n$  の最小値  $n_q(k,d)$  を求める問題)は、符号理論において重要な研究課題の一つであり、最適線形符号問題と呼ばれる。本研究では、線形符号の生成行列から構成される射影空間の多重集合を幾何学的に分析する手法を用いて、Griesmer 符号等の非存在証明による  $n_q(k,d)$  の確定、最適な線形符号のコンピュータによる探索と構造解析、有限射影空間における集合の特殊な構造を用いた符号の構成等について成果を得た。

研究成果の学術的意義や社会的意義

情報の電子化が進み、情報ネットワークが社会の基盤として不可欠となった現在、情報の伝送や記録の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。現在、実用化されている誤り訂正符号の多くは、Reed-Solomon 符号を代表とする有限体上の線形符号であるが、情報の伝達速度を左右する符号長や伝達できる情報量を示す次元を固定しても、誤り訂正能力の限界が確定できていない場合が多い。本研究は、線形符号を生成するために必要な射影空間上の集合を数学的に解析することにより、符号の誤り訂正能力の限界を解明しようとするものである。

研究成果の概要(英文)：A linear code with length  $n$ , dimension  $k$  and minimum weight  $d$  over the field of  $q$  elements is called an  $[n,k,d]_q$  code. A classical and fundamental research problem in coding theory is to find  $n_q(k,d)$ , the minimum length  $n$  for which an  $[n,k,d]_q$  code exists, which is called "Optimal Linear Codes Problem".

In this work, considering the multiset consisting the columns of a generator matrix of a given code as a multiset in the projective space, we have obtained several new results on the problem by showing the nonexistence of some linear codes attaining the known bound using the geometric methods, constructing new codes and corresponding arcs and blocking sets in the projective spaces by the heuristic search with the aid of computers.

研究分野：代数的符号理論

キーワード：線形符号 最適線形符号 符号の拡張可能性 有限射影幾何 Griesmer 限界

## 1. 研究開始当初の背景

(1)  $q$  元体上の線形符号 ( $q$  元線形符号) には、情報の伝達速度を左右する符号長  $n$ 、伝達できる情報量を示す次元  $k$ 、及び、誤り訂正能力を表す符号の最小距離  $d$  という3つの重要なパラメータがある (このような線形符号を  $[n, k, d]_q$  符号と呼ぶ)。  $n, k, q$  の値が与えられたとき、  $[n, k, d]_q$  符号が存在するような  $d$  の最大値  $d_q(n, k)$  を求めれば、誤り訂正能力が最も高い符号 (最適な線形符号) が得られる。全ての  $n, k, q$  に対して  $d_q(n, k)$  を決定する問題は、全ての  $d, k, q$  に対して、  $[n, k, d]_q$  符号が存在するような  $n$  の最小値  $n_q(k, d)$  を決定する問題と等価であり、最適線形符号問題 (Optimal Linear Codes Problem) と呼ばれている。

(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。

(3) 新しい符号の構成と符号の非存在証明の両面で活用される情報として重要な線形符号の拡張可能性については、  $q = 3$  の場合は詳細が明らかになっているのに対して、  $q$  が4以上の場合に知られている結果は極めて限定的であり、更なる研究が期待されている。

## 2. 研究の目的

(1) 本研究の主な目的は、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。符号の長さ  $n$  については Griesmer 限界と呼ばれる下限が知られており、与えられた  $q$  と  $k$  に対して  $d$  が十分大きければ Griesmer 符号 ( $n$  が Griesmer 限界の値と一致する符号) 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。具体的には、Griesmer 符号の非存在証明や Griesmer 限界に近い長さの新しい符号の構成が必要になる。

(2) 線形符号の拡張可能性については、  $q = 4$  の場合の拡張可能性の幾何学的なメカニズムの解明とその最適線形符号問題への応用が本研究の目的である。

## 3. 研究の方法

本研究を遂行するために、(1) 最適な線形符号を構成する幾何学的な手法の開発、(2) 4元線形符号の多重拡張可能性の解明、(3) Griesmer 符号の非存在証明に役立つ新しい証明技法の開発と主に4次元線形符号の存在限界に関する研究を行う。

(1)  $q = 5$  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、その幾何学的な解析結果から、一般の  $q$  元体上の最適な線形符号の生成行列の構成方法を導く。  $q$  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3次元の場合を手がかりとして、4次元以上での特に3重拡張可能となる条件について、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) の幾何学的な構造を用いて明らかにする。また、5次元4元線形符号で未解決な最適線形符号問題にも取り組む。

(3)  $q = 5, 8, 9$  といった具体的な体上の線形符号についても最適線形符号問題にも取り組むと共に、得られた知見を分析し、  $q$  元体上の広範囲の  $d$  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) 与えられた  $q$  と  $k$  に対して、  $d$  が十分大きい値のときに Belov 型 Griesmer 符号の構成方法が知られている。この方法を一般化して、Belov 型 Griesmer 符号が構成できない場合の  $d$  の値に対しても Griesmer 限界に近い長さの最適な線形符号が構成できるための条件と、そのような符号の生成行列の幾何学的な構成方法を見出すことが出来た。その成果は、国際学術雑誌 Designs, Codes and Cryptography に掲載された。

(2) まず  $q = 8, 9, k = 4$  の場合の最適線形符号問題に大学院生と共に取り組み、コンピュータを用いた  $q$ -divisible 符号の探索と拡張定理を用いた非存在証明により、一定の成果を得た。  $q = 9$  の場合の成果は国際学術雑誌 Electronic J. Combinatorics に掲載され、  $q = 8$  の場合の成果は国際会議 OC 2017 にて発表を行った。また、  $q = 9$  の場合の非存在結果の一部は4次元  $q$  元線形符号の場合に一般化することができた。その成果は、国際学術雑誌 Journal of Algebra Combinatorics Discrete Structures and Applications に掲載された。

(3)  $q = 5, k = 5$  の場合にコンピュータを用いた射影変換の軌道の組合せ探索によって得られ

た新しい 5-divisible 符号 (符号語の重みが全て 5 の倍数であるような 5 元線形符号) の生成行列を分析し、 $q$  元体上の 4 次元射影空間  $PG(4, q)$  の normal rational curve を用いた構成の形に一般化し、この符号の projective dual として最適な  $q$  元 5 次元線形符号が得られることを示した。この成果は、国際学術雑誌 Finite Fields and their Applications に掲載された。

(4)  $PG(r, 4)$  の奇集合の分類を応用して、 $d \equiv 1 \pmod{4}$  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。更に、 $q = 4$ ,  $k = 5$  の場合の最適線形符号問題に取り組み、 $d = 31, 47, 48, 59, 60, 61, 62, 138$  に対する  $n_4(5, d)$  の値を決定することが出来た。これらの成果は、それぞれ国際学術雑誌 Finite Fields and their Applications および Discrete Mathematics に掲載された。

(5) ブルガリア科学アカデミーの Iliya Bouyukliev 教授らとの共同研究として、 $PG(2, 7)$  の  $(29, 5)$ -arc を分類し、その構成方法を明らかにすると共に、その一部を  $PG(2, q)$  の 3 重 blocking set の構成の形に一般化することができた。これらの成果は、国際会議 ACCT2016 にて発表を行うと共に、国際学術雑誌にも掲載された。

## 5. 主な発表論文等

〔雑誌論文〕 計14件（うち査読付論文 12件 / うち国際共著 3件 / うちオープンアクセス 9件）

1. 著者名 Iliya Bouyukliev, Eun Ju Cheon, Tatsuya Maruta, Tsukasa Okazaki	4. 巻 8
2. 論文標題 On the $(29,5)$ -Arcs in $PG(2,7)$ and Some Generalized Arcs in $PG(2,q)$	5. 発行年 2020年
3. 雑誌名 Mathematics	6. 最初と最後の頁 320-320
掲載論文のDOI (デジタルオブジェクト識別子) 10.3390/math8030320	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 該当する
1. 著者名 K. Kumegawa, T. Maruta	4. 巻 5
2. 論文標題 Non-existence of some 4-dimensional Griesmer codes over finite fields	5. 発行年 2018年
3. 雑誌名 Journal of Algebra Combinatorics Discrete Structures and Applications	6. 最初と最後の頁 101-116
掲載論文のDOI (デジタルオブジェクト識別子) 10.13069/jacodesmath.427968	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -
1. 著者名 H. Kanda, T. Maruta	4. 巻 52
2. 論文標題 On the 3-extendability of quaternary linear codes	5. 発行年 2018年
3. 雑誌名 Finite Fields and their Applications	6. 最初と最後の頁 126-136
掲載論文のDOI (デジタルオブジェクト識別子) 10.1016/j.ffa.2018.04.002	査読の有無 有
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 Y. Koga, T. Maruta, K. Shiromoto	4. 巻 86
2. 論文標題 On Critical Exponents of Dowling Matroids	5. 発行年 2018年
3. 雑誌名 Designs, Codes and Cryptography	6. 最初と最後の頁 1947-1962
掲載論文のDOI (デジタルオブジェクト識別子) 10.1007/s10623-017-0431-8	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -

1. 著者名 H. Kanda, T. Maruta	4. 巻 341
2. 論文標題 Nonexistence of some linear codes over the field of order four	5. 発行年 2018年
3. 雑誌名 Discrete Mathematics	6. 最初と最後の頁 2676-2685
掲載論文のDOI (デジタルオブジェクト識別子) 10.1016/j.disc.2018.06.024	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -

1. 著者名 Y. Inoue, T. Maruta	4. 巻 55
2. 論文標題 Construction of new Griesmer codes of dimension 5	5. 発行年 2019年
3. 雑誌名 Finite Fields and their Applications	6. 最初と最後の頁 231-237
掲載論文のDOI (デジタルオブジェクト識別子) 10.1016/j.ffa.2018.10.007	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -

1. 著者名 E.J. Cheon, Y. Kageyama, S.J. Kim, N. Lee, T. Maruta	4. 巻 54
2. 論文標題 Construction of two-weight codes over finite fields and its applications	5. 発行年 2017年
3. 雑誌名 Bulletin of the Korean Mathematical Society	6. 最初と最後の頁 731-736
掲載論文のDOI (デジタルオブジェクト識別子) 10.4134/BKMS.b151011	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 該当する

1. 著者名 N. Bono, T. Maruta	4. 巻 8
2. 論文標題 Some new 4-dimensional linear codes	5. 発行年 2017年
3. 雑誌名 Proceedings of 8th International Workshop on Optimal Codes and Related Topics (OC 2017)	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 有
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 M. Fujii, T. Maruta	4. 巻 8
2. 論文標題 Nonexistence of some Griesmer codes of dimension 4 over $F_8$	5. 発行年 2017年
3. 雑誌名 Proceedings of 8th International Workshop on Optimal Codes and Related Topics (OC 2017)	6. 最初と最後の頁 87--92
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 有
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 E.J. Cheon, T. Maruta, T. Okazaki	4. 巻 15
2. 論文標題 Construction of some triple blocking sets in $PG(2,q)$	5. 発行年 2016年
3. 雑誌名 Proceedings of 15th International Workshop on Algebraic and Combinatorial Coding Theory	6. 最初と最後の頁 96-101
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 有
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 該当する

1. 著者名 Y. Kageyama, T. Maruta	4. 巻 81
2. 論文標題 On the geometric constructions of optimal linear codes	5. 発行年 2016年
3. 雑誌名 Designs, Codes and Cryptography	6. 最初と最後の頁 469-480
掲載論文のDOI (デジタルオブジェクト識別子) 10.1007/s10623-015-0167-2	査読の有無 有
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 K. Kumegawa, T. Okazaki, T. Maruta	4. 巻 24
2. 論文標題 On the minimum length of linear codes over the field of 9 elements	5. 発行年 2017年
3. 雑誌名 Electronic J. Combinatorics	6. 最初と最後の頁 #P1.50
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 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -

[学会発表] 計23件(うち招待講演 0件/うち国際学会 13件)

1. 発表者名 T. Maruta, H. Kanda, M. Shirouzu
2. 発表標題 On the extendability of linear codes over the field of order four
3. 学会等名 The 42nd Australasian Conference on Combinatorial Mathematics and Combinatorial Computing (42ACCMCC) (国際学会)
4. 発表年 2019年

1. 発表者名 Y. Inoue, T. Maruta
2. 発表標題 Constructing new linear codes over the field of order five
3. 学会等名 Japanese Conference on Combinatorics and its Applications (JCCA 2018) (国際学会)
4. 発表年 2018年

1. 発表者名 W. Kuranaka, T. Maruta
2. 発表標題 Nonexistence of some Griesmer codes over the field of order five
3. 学会等名 Japanese Conference on Combinatorics and its Applications (JCCA 2018) (国際学会)
4. 発表年 2018年

1. 発表者名 Y. Inoue, T. Maruta
2. 発表標題 Construction of new Griesmer codes of dimension 5
3. 学会等名 The 41st Australasian Conference on Combinatorial Mathematics and Combinatorial Computing (41ACCMCC) (国際学会)
4. 発表年 2018年

1. 発表者名 N. Bono, T. Maruta, K. Shiromoto, K. Yamada
2. 発表標題 On the non-trivial blocking sets in binary projective spaces
3. 学会等名 The 41st Australasian Conference on Combinatorial Mathematics and Combinatorial Computing (41ACCMCC) (国際学会)
4. 発表年 2018年

1. 発表者名 丸田辰哉
2. 発表標題 On the construction of optimal linear 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 Y. Inoue, T. Maruta
2. 発表標題 Construction of new Griesmer codes of dimension 5
3. 学会等名 代数系、論理、言語と計算機科学の周辺
4. 発表年 2019年

1. 発表者名 W. Kuranaka, T. Maruta
2. 発表標題 Nonexistence of some Griesmer codes of dimension 5
3. 学会等名 代数系、論理、言語と計算機科学の周辺
4. 発表年 2019年

1. 発表者名 T. Maruta
2. 発表標題 Nonexistence of some linear codes over the field of order four
3. 学会等名 The 5th International Combinatorics Conference (5ICC) (国際学会)
4. 発表年 2017年

1. 発表者名 苅田仁, 丸田辰哉
2. 発表標題 Nonexistence of some linear codes over $F_4$
3. 学会等名 2017年度応用数学合同研究集会
4. 発表年 2017年

1. 発表者名 Eun Ju Cheon, Tatsuya Maruta, Tsukasa Okazaki
2. 発表標題 Construction of some triple blocking sets in $PG(2,q)$
3. 学会等名 Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT 2016) (国際学会)
4. 発表年 2016年

1. 発表者名 丸田辰哉, 苅田仁
2. 発表標題 On the extendability of quaternary linear codes
3. 学会等名 2016年度応用数学合同研究集会
4. 発表年 2016年

〔図書〕 計0件

〔産業財産権〕

〔その他〕

Griesmer Bound for Linear Codes over Finite Fields  
<http://www.mi.s.osakafu-u.ac.jp/~maruta/>

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
--	---------------------------	-----------------------	----

7. 科研費を使用して開催した国際研究集会

〔国際研究集会〕 計0件

8. 本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関			
ブルガリア	Bulgarian Academy of Sciences			
韓国	Gyeongsang National University			