称号及び氏名　　博士(理学)　苅田 仁

学位授与の日付　2021 年 3 月 31 日

論　文　名　　Geometric approach to the extendability of linear codes over finite fields
（有限体上の線形符号の拡張可能性に関する幾何学的研究）

論文審査委員　　主査　丸田 辰哉
副査　山口　睦
副査　壁谷 喜継
副査　松永 秀章

2020 年度 博士論文要旨

Geometric approach to the extendability of linear codes over finite fields

（有限体上の線形符号の拡張可能性に関する幾何学的研究）

大阪府立大学大学院理学系研究科　数理科学専攻　　苅田 仁

現在、デジタル通信において、より信頼性が高くより高速な通信が望まれている。そのためには、情報を通信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高い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符号の多くは有限体（位数 q の有限体を q 元体と呼び、$GF(q)$ と表す）上の線形符号であり、線形符号の 3 つのパラメータ、長さ n、次元 k、最小距離 d はそれぞれ、通信の速さ、メッセージの多様性、訂正能力の高さを表している。これらのパラメータを持つ線形符号を $[n,k,d]_q$ 符号と呼ぶ。この 3 つのパラメータのうち 2 つを与えて残りの 1 つを最適化する問題、最適線形符号問題（英名：Optimal Linear Codes Problem）は、符号理論において古くから取り組まれている研究で、現在も未解決問題が多数残っている。その一つが与えられた正整数 q,k,d に対して $[n,k,d]_q$ 符号が存在するような n の最小値 $n_q(k,d)$ （存在限界）を求める問題である。

$[n,k,d]_q$ 符号 $\mathcal{C}$ の基底を成す行ベクトルを並べてできる $k\times n$ 行列を生成行列と呼ぶ。符号に属する符号語は係数ベクトルと生成行列の積で算出できる。$[n,k,d]q$ 符号 $\mathcal{C}$ の生成行列に 1 列追加して、$[n+1,k,d+1]_q$符号 $\mathcal{C}'$ が構成できるとき、$\mathcal{C}$ は拡張可能という。符号の構成や上記の問題を解くために、符号の拡張可能性は極めて重要な役割を持つ。古くから符号の性質を調べるために、各符号語と零ベクトルとの距離である重みの分布が調べられてきた。2 元体 $GF(2)$ 上の奇数の最小重み（線形性より最小距離と等しい）を持つ符号が拡張可能であることはよく知られており、パリティチェックとして実用化もされている。先行研究では、重み分布によって符号の性質が分類されることにより、$q\geq 3$ に対する $GF(q)$ 上の線形符号の拡張可能性が解明されてきた。例えば、2 元体上の線形符号に対する拡張定理は、R.Hill 教授の論文 “An extension theorem for linear codes, Des. Codes Cryptogr. 17 (1999) 151-157” にて、 $q\geq 3$ である q 元線形符号の拡張定理に一般化された。その結果は最適線形符号の存在限界の決定にも頻繁に使われている。本論文を構成する各章の概要は、以下の通りである。

第１章では、本論文の序論として、背景と目的を説明している。

第２章では、初めに有限体上の線形符号の基本的な概念やよく知られている定理を紹介する。続いて、本研究の主テーマである線形符号の拡張可能性について知られている結果を紹介する。ここで紹介する拡張可能性は q-WS（符号の重み分布から計算される q 個の整数の組）をもとに判別する。最後に、q 元体上の射影幾何の概念と q-WS や生成行列を関連付ける方法を説明する。

第３章では、重みが 9 を法として 0, -1, -2 のいずれかと合同で、最小距離 d が -2 か -1 と合同である 3 元線形符号が拡張可能であること証明する。この定理は 3-WS を特定しない重みが 3 種類の定理としては初である。また、その定理を応用して $[512,6,340]_3$ 符号が存在しないことも示す。

第４章と第５章では、4 元線形符号に関する研究結果を述べる。まず第 4 章では、4 元線形符号の拡張可能性に関する新しい定理をいくつか紹介する。3 次元線形符号の 4-WS や 4 元体の射影空間上の odd set に関する先行研究を参照し、いくつかの 4-WS の値について、k 次元符号 $\mathcal{C}$ に対応する射影空間 $\mathrm{PG}(k-1,4)$ 上の集合の構造を明らかにし、$\mathcal{C}$ が拡張可能であるための十分条件を与える。更に、その定理を適用した例を挙げる。第 5 章では、4 元 5 次元線形符号の最適線形符号問題について取り組んだ成果を述べる。ここでも、4 元線形符号の拡張定理が重要な役割を果たす。

第６章では、q 元体上の線形符号に適用できるように一般化された拡張可能性に関する新しい定理を紹介する。特に特徴的な結果として、定理 6.1 は、符号語の重みが q を法として 4 種類の q 元体上の線形符号に対する初めての拡張定理である。

最後の第７章では、第３章と第４章で更新した $n_3(6,d)$ および $n_4(5,d)$ の表を掲載する。

研究論文（査読付き）

[1] T. Maruta, T. Tanaka, H. Kanda, New extension theorems for codes over F_q, Proceedings of the 7th International Workshop on Optimal Codes and Related Topics (OC 2013), Albena, Bulgaria, 2013, pp. 152-157.

[2] T. Maruta, T. Tanaka, H. Kanda, Some generalizations of extension theorems for linear codes over finite fields, Australasian J. Combinatorics 60 (2014), pp. 150-157.

[3] H. Kanda, T. Tanaka, T. Maruta, On the l-extendability of quaternary linear codes, Finite Fields and their Applications 35 (2015), pp. 159-171.

[4] H. Kanda, T. Maruta, On the 3-extendability of quaternary linear codes, Finite Fields and their Applications 52 (2018), pp. 126-136.

[5] H. Kanda, T. Maruta, Nonexistence of some linear codes over the field of order four, Discrete Mathematics 341 (2018), pp. 2676-2685.

[6] H. Kanda, A new extension theorem for ternary linear codes and its application, Finite Fields and their Applications 67 (2020), Article 101711, pp. 1-9.

[7] H. Kanda, The non-existence of [383,5,286] and [447,5,334] quaternary linear codes, Serdica Math. J., to appear.

学位論文審査結果の要旨

学位論文提出者氏名：　苅田　仁

学位論文題目：Geometric approach to the extendability of linear codes over finite fields
（有限体上の線形符号の拡張可能性に関する幾何学的研究）

q 元体（位数 q の有限体）上の線形符号（q 元線形符号）には、３つの重要なパラメータ、すなわち、符号の伝送速度に影響する長さ n、符号語の個数を決定する次元 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 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、符号理論において最も基礎的な研究課題の一つで、最適線形符号問題と呼ばれている。例えば、(q,k)=(3,6),(4,5) の場合でも多くの d の値について $n_q(k,d)$ が未決定である。これを決定するには、既知の符号より最小距離が大きい（誤り訂正能力が高い）新しい符号の構成や、存在するか否か不明な線形符号の非存在証明が必要になる。最適線形符号問題を考える上で強力な手掛かりになるのが、本研究で扱っている線形符号の拡張可能性である。実際、最適な符号が拡張可能な場合は拡張された符号も最適であり、d が q の倍数でないときの符号の非存在証明にも拡張定理が利用される場合が多い。本論文では、線形符号の生成行列から定義される射影空間の分割集合の幾何学的な構造を調べることによって線形符号の拡張可能性を考察すると共に、新たに得られた拡張定理の最適線形符号問題への適用例も示している。本論文の主な内容は、以下の通りである。

1. q 元体上の(k-1)次元射影空間 Σ の各点 P に対して、$[n,k,d]_q$ 符号の生成行列から P の重みが定義される。そこから自然に定義される Σ の line の重みが q の倍数になることは知られていたが、Σ の一般の s 次元射影部分空間の重みについて成り立つ重要な等式を発見し、簡明な証明を与えた(Lemma 3.2)。これを用いて、３元及び４元線形符号に対する新しいタイプの拡張定理を証明し、それらを適用して最適線形符号問題で未解決であったいくつかの問題を解決した。
2. q 元線形符号の生成行列から定義される射影空間の分割集合が含む点の個数の組は、符号の重み分布から算出される整数の組で、q-WS（weight spectrum modulo q）と呼ばれる。４元線形符号から得られる射影空間の分割集合の幾何学的な構造の多くが 4-WS によって特徴付けられることを示し、４元線形符号が複数回拡張可能となるための幾何学的な条件を求めることにより、４元線形符号が複数回拡張可能であるための新たな十分条件を示した。
3. 先行研究による拡張可能性の考察から得られたいくつかの十分条件を一般の q 元線形符号に対して成り立つ拡張定理の形に一般化することに成功した。これらの定理の一部は、既に最適線形符号問題の研究において応用されている。

上記の研究成果は、有限体上の線形符号の基礎研究に大きく貢献するものであり、今後、最適線形符号問題に関する研究において活用されることが期待される。以上により、本委員会は当該論文が学位論文として十分な内容を有しているものと判断した。

学位論文審査委員会

主査　丸田　辰哉
山口　睦
壁谷　喜継
松永　秀章