Study of Coding Theory over Finite Frobenius Rings

有限フロベニウス環上の符号理論の研究

児童学部　児童学科　松岡　　学

要旨：この論文では、有限体上の符号理論を環上の符号理論へ拡張する方法を考察する。最初に、有限体の拡張として有限可換 QF 環を考え、線形符号の巡回性を調べる。巡回符号の自然な拡張として、多重巡回符号と逐次符号を定義し、有限可換 QF 環上の双対性を調べる。また、有限可換 QF 環上の自由符号において、可逆な定数項をもつ単項多重巡回符号の特徴づけを行う。最後に、有限可換 QF 環上の線形符号を有限非可換環上へ拡張することを考え、今後の研究の方向性をまとめる。

キーワード：フロベニウス環、非可換環、双対符号、多重巡回符号、逐次符号

1　はじめに

近年、有限体上の符号理論を環上の符号理論へ拡張する試みがなされている。最初の段階として、Z/(4) などのガロア環への拡張が考えられる。

一般的に、体の代数的な拡張としては、斜体への拡張と可換環への拡張が考えられるが有限体においては、有限斜体は可換体であるという Wedderburn の定理があるため、有限可換環への拡張が自然である。よって、有限体上の符号理論の拡張としては、最初の段階として有限可換環への拡張を考え、次の段階として有限非可換環への拡張を考えることとなる。

環論のアプローチとして、T. Sumiyama (1979) は、有限局所環の極大ガロア部分環を考察した。ガロア環の拡張として、フロベニウス環や QF 環を考えることができる。Y. Hirano (1997) は環論的に有限フロベニウス環を特徴づけた。

一方、有限フロベニウス環上の符号理論の研究も進んでいる。A. A. Andrade and Palazzo Jr. (2005) は、有限環上の線形符号を調べた。 有限フロベニウス環上の符号理論における拡張定理は、J. A. Wood (1999) により確立された。 K. Shiromoto and L. Storme (2003) は、有限 QF 環上の符号理論におけるある種の上限を与えた。

本論文においては、有限体上の巡回符号は多項式環の剰余環のイデアルとして表現されるという事実を出発点として、符号理論の代数的な理論体系の構築を試みる。最初に、有限可換環上において巡回符号の一般化である多重巡回符号と逐次符号を定義し、その双対符号を調べる。これらのことは、S. R. Lopez−Permouth 達（2009）の研究の流れを受け継いでいる。

次に、これらの概念を有限可換 QF 環上の線形符号に拡張し、その階数や双対符号を調べる。そして、多重巡回符号と逐次符号がある種の双対性をもつことを考察し、自由符号が可逆な定数項をもつ単項多重巡回逐次符号であるための条件を決定する。さらに、有限可換 QF 環上の線形符号を非可換環へ拡張することを考え、理論体系を定式化する。最後に、非可換 QF 環を拡張する方向性について述べ、今後の可能性を考える。

この論文を通して特に断らない限り、環 R は 0 と異なる単位元をもつ環とし、n は 2 以上の自然数とする。

また、符号理論における基本的な用語は、「表 1」の通りとする。

表 1　用語の説明

有限可換環 R と 2 以上の自然数 n に対して、R 加群 R^n を、

$$R^n = \{(a_0, a_1, \ldots\ldots, a_{n-1}) \mid a_i \in R\}$$

と定める。

R 上の長さ n の線形符号 C とは、R 加群 R^n の空でない部分加群として定める。

線形符号 $C \subseteq R^n$ が自由 R 部分加群のとき、自由符号という。特に、C の階数が k のとき、$[n, k]$ 線形自由符号、または単に $[n, k]$ 符号という。

線形符号 $C \subseteq R^n$ が条件

$(a_0, a_1, \ldots\ldots, a_{n-1}) \in C$ ならば、

$$(a_{n-1}, a_0, a_1, \ldots\ldots, a_{n-2}) \in C$$

を満たすとき、巡回符号という。

予備知識として、環論の基本的な結果は、T. Y. Lam (1999) や B. R. McDonald (1974) を、ホモロジー代数は、H. Cartan, S. Eilenberg (1956) や J. J. Rotman (2008) を、符号理論は、J. H. van Lint (1992) を参照されたい。

2　有限可換環上の多重巡回符号と逐次符号

有限体上の符号理論の拡張を考える際、有限斜体は可換体であるという Wedderburn の定理があるため、有限可換環上の符号理論へと拡張することが自然である。

最初に、有限可換環 R 上の長さ n の線形符号 C に対して、多重巡回符号や逐次符号を定義し、その性質を考察する。この節では、以下 R を有限可換環とする。

定義 2.1.

$c=(c_0, c_1, \ldots\ldots, c_{n-1}) \in R^n$ とする。線形符号 $C \subseteq R^n$ が条件

$(a_0, a_1, \ldots\ldots, a_{n-1}) \in C$ ならば、

$(0, a_0, a_1, \ldots\ldots, a_{n-2})+a_{n-1}(c_0, c_1, \ldots\ldots, c_{n-1}) \in C$

を満たすとき、C を c に誘導された多重巡回符号という。

有限体上の巡回符号のときと同様に、多重巡回符号は多項式環の剰余環のイデアルとみなすことができる。

$c=(c_0, c_1, \ldots\ldots, c_{n-1}) \in R^n$ に対して、

$$f(x)=x^n-c_{n-1}x^{n-1}-\cdots-c_1x-c_0$$

と定め、自然な写像

$$\rho : R^n \to R[x]/(f(x))$$

を $a=(a_0, a_1, \ldots\ldots, a_{n-1})$ に対して、

$$\overline{a_{n-1}x^{n-1}+\cdots+a_1x+a_0}$$

を対応させることで定める。

この写像により、多重巡回符号 C を、剰余環 $R[x]/(f(x))$ のイデアルと同一視することができる。

定義 2.2.

多重巡回符号 $C \subseteq R[x]/(f(x))$ に対して、$R[x]$ におけるモニックな多項式 g, h が存在して、

$$C=(g)/(f) \quad \text{かつ} \quad f=hg$$

と表されるとき、C を単項多重巡回符号という。特に、g の定数項が可逆なとき、可逆な定数項をもつ単項多重巡回符号という。

定義 2.3.

$c=(c_0, c_1, \ldots\ldots, c_{n-1}) \in R^n$ とする。線形符号 $C \subseteq R^n$ が条件

$(a_0, a_1, \ldots\ldots, a_{n-1}) \in C$ ならば、

$(a_1, a_2, \ldots, a_{n-1}, a_0c_0+a_1c_1+\cdots+a_{n-1}c_{n-1}) \in C$

を満たすとき、C を c に誘導された逐次符号という。

R^n 上に標準的な内積を

$$< x, y >= \sum_{i=0}^{n-1} x_i y_i$$

と定める。ここで、

$$x=(x_0, x_1, \ldots, x_{n-1}),\ \ y=(y_0, y_1, \ldots\ldots, y_{n-1})$$

とする。

また、線形符号 $C \subseteq R^n$ に対して、

$C^{\perp}=\{a \in R^n \mid$ 任意の $c \in C$ に対して $< c, a >=0\}$

と定めると、$C^{\perp}$ は明らかに線形符号となる。$C^{\perp}$ を C の双対符号という。

定理 2.4

長さ n の線形符号 C に対して、次が成り立つ。

(1) C が多重巡回符号ならば、$C^{\perp}$ は逐次符号である。

(2) C が逐次符号ならば、$C^{\perp}$ は多重巡回符号である。

証明

[M. Matsuoka (2011) 定理 1] を参照されたい。□

3　フロベニウス環と QF 環

前節では、有限可換環上の多重巡回符号や逐次符号を定義した。フロベニウス環や QF 環の符号理論を考える前に、フロベニウス環や QF 環の定義をまとめておく。

M を環 R の左加群とし、X をその部分集合とする。X の零化イデアルを

$ann_l(X)=\{r \in R \mid$ 任意の $x \in X$ に対して $rx=0\}$

と定めると、これは左イデアルとなる。右加群の部分集合 X に対して、$ann_r(X)$ が同様に定義される。

このとき、次の定理が成り立つ。

定理 3.1.

環 R に対して、次の条件は同値である。

(1) R は右アルチン環かつ右自己入射的環である。

(2) R は左アルチン環かつ左自己入射的環である。

(3) R は右ネーター環かつ次の条件を満たす。

(3a) R の任意の右イデアル A に対して、

$ann_r(ann_lA)=A$

(3b) R の任意の左イデアル I に対して、

$$ann_l(ann_r I) = I$$

証明

[T. Y. Lam (1999) 定理 15.1] を参照されたい。□

定義 3.2.

環 R が定理 3.1. の条件を満たす時、準フロベニウス環（以下、QF 環）という。

定理 3.3.

環 R に対して、次の条件は同値である。

(1) R は QF 環である。

(2) 任意の左 R 加群に対して、射影的であることと入射的であることは同値である。

証明

[T. Y. Lam (1999) 定理 15.9] を参照されたい。□

単純右 R 加群は、R/M の形をしている。ここで、M は環 R の極大右イデアルである。

このとき、次の命題を証明することができる。

命題 3.4.

R を QF 環とする。このとき、すべての単純右 R 加群環は R に埋め込まれる。

すべての単純右 R 加群環が R に埋め込まれるとき、環 R を右カッシュ環という。よって、QF 環は右カッシュ環となる。

定理 3.4.

R をアルチン環とする。J を R のジャコブソン根基とし、$\overline{R} = R/J$ とおくとき、次の条件は同値である。

(1) R は QF 環であり、$soc(R_R) \cong \overline{R}_R$

(2) R は QF 環であり、$soc({}_R R) \cong {}_R\overline{R}$

(3) $soc(R_R) \cong \overline{R}_R$ かつ $soc({}_R R) \cong {}_R\overline{R}$ が成り立つ。

証明

[T. Y. Lam (1999) 定理 16.14] を参照されたい。□

定義 3.5.

R 環が定理 3.4.の条件を満たす時、フロベニウス環という。

定義から明らかに、フロベニウス環は QF 環である。

4 準フロベニウス環上の線形符号

この節では、有限可換 QF 環上の自由符号を考察する。

線形符号 $C \subseteq R^n$ に対して、C° を

$$C^\circ = \{\lambda \in Hom_R(R^n, R) \mid \lambda(C) = 0\}$$

と定める。

このとき、次の命題から C° は R 加群として、$C^\perp$ と同じ構造をもつことが分かる。

命題 4.1.

R を有限可換環とする。部分加群 $C \subseteq R^n$ に対して、C° と $C^\perp$ は R 加群として同型である。

証明

[M. Matsuoka (2011) 命題 2] を参照されたい。□

一方、有限可換 QF 環の特徴づけとして、次が知られている。

定理 4.2.

有限可換環 R に対して、次の条件は同値である。

(1) R は QF 環である。

(2) 任意の部分加群 $M \subseteq R^n$ に対して、$M^{\circ\circ} = M$ が成り立つ。

証明

[J. A. Wood (1999) 定理 7.2] を参照されたい。□

定理 4.2. から次が分かる。

定理 4.3.

R を有限可換 QF 環、$C \subseteq R^n$ を自由符号とするとき、

$$(C^\perp)^\perp = C$$

が成り立つ。

定理 4.4.

有限可換 QF 環 R に対して、$C \subseteq R^n$ が自由符号ならば $C^\perp$ も自由符号であり、階数は

$$rankC^\perp = n - rankC$$

が成り立つ。

証明

$k = rankC$ とする。C は自由符号なので、射影加群である。よって、入射加群になるので、C は R^n の直和因子となる。R^n の適当な部分加群 K が存在し、

$$R^n = C \oplus K$$

となる。このとき、K は階数が $n-k$ の自由加群となり、

$$C^{\perp} \cong C^{\circ} \cong Hom(K, R) \cong Hom(R^{n-k}, R) \cong R^{n-k}$$

が成り立つ。

よって、$C^{\perp}$ は階数が $n-k$ の自由加群である。 □

定理 4.4. から次の系が分かる。

系 4.5.

R を有限可換 QF 環、$C \subseteq R^n$ を自由符号とする。このとき、C が多重巡回符号であるための必要十分条件は、$C^{\perp}$ が逐次符号であることである。

次の定理により、有限可換 QF 環 R 上の長さ n の自由符号 C が、可逆な定数項をもつ単項多重巡回逐次符号であるための条件を特徴づけることができる。

定理 4.6.

有限可換 QF 環 R と、長さ n の自由符号 C に対して、次の条件は同値である。

(1) C と $C^{\perp}$ は共に、可逆な定数項をもつ単項多重巡回符号である。
(2) C と $C^{\perp}$ は共に、可逆な定数項をもつ単項逐次符号である。
(3) C は、可逆な定数項をもつ単項多重巡回逐次符号である。
(4) $C^{\perp}$ は、可逆な定数項をもつ単項多重巡回逐次符号である。
(5) $C = (g)/(x^n-\alpha)$ は、可逆な α をもつ定数巡回的符号である。
(6) $C^{\perp} = (q)/(x^n-\beta)$ は、可逆な β をもつ定数巡回的符号である。

証明

［M. Matsuoka (2011) 定理 5］を参照されたい。 □

今後は、可逆な定数項をもつ単項多重巡回逐次符号を拡張することが自然に考えられるが、単項でない場合は困難が伴い拡張は現在の所なされていない。

5 非可換環上の符号理論

可換環上の符号理論を非可換環上へ拡張することを考える。

左 R 加群 M に対して、$M^* = Hom_R(M, R)$ は、右 R 加群となる。環 R の右からの作用は、

$$(f \cdot r)(m) = f(m) \cdot r$$

と定まる。ここで、$r \in R, m \in M, f \in M^*$ である。

また、自然な準同型写像 $\zeta : M \to M^{**}$ が

$$\zeta(m)(f) = f(m)$$

として定まる。ここで、$m \in M, f \in M^*$ である。

M は $\zeta : M \to M^{**}$ が単射のとき捩れがないといい、全単射のとき反射的であるという。

命題 5.1.

R を QF 環とする。このとき、双対関手 $Hom_R(-, R)$ は、完全関手である。すなわち、左 R 加群の任意の短完全系列

$$0 \to K \xrightarrow{\varphi} M \xrightarrow{\phi} N \to 0$$

に対して、

$$0 \to N^* \xrightarrow{\phi^*} M^* \xrightarrow{\varphi^*} K^* \to 0$$

も短完全系列となる。

証明

環 R は入射的であり、$\varphi : K \to M$ は単射なので、任意の $g \in K^*$ に対して、$h \circ \varphi = g$ を満たすような適当な $h : M \to R$ が存在する。従って、φ^* は全射である。

一方、双対関手 $Hom_R(-, R)$ は左完全なので、

$$0 \to N^* \xrightarrow{\phi^*} M^* \xrightarrow{\varphi^*} K^* \to 0$$

は短完全系列となる。 □

次の命題は、直接証明することができる。

命題 5.2.

環 R に対して、左 R 加群 R^n は反射的である。

命題 5.2. より、次の定理を証明することができる。

定理 5.3.

R を QF 環とする。このとき、任意の有限生成左 R 加群 M は反射的である。

任意の部分加群 $A \subseteq M$ に対して、M^* の部分加群 A° を

$$A^{\circ} = \{f \in M^* \mid f(A) = 0\}$$

と定める。

また、任意の部分加群 $I \subseteq M^*$ に対して、M の部

分加群 I° を

$$I^{\circ} = \cap \ker_{f \in I}(f)$$

と定める。

このとき、次の 2 つの補題を直接証明することができる。

補題 5.4.

R を環とし、M を反射的左 R 加群、I を M^* の部分加群とする。このとき、左 R 加群としての同型

$$I^{\circ} \cong I^{\circ}$$

が成り立つ。

補題 5.5.

R を QF 環とし、M を左 R 加群、A を M の部分加群とする。このとき、

$$A^{\circ\circ} = A$$

が成り立つ。

補題 5.4. と補題 5.5. から次の定理が分かる。

定理 5.6.

R を QF 環とし、M を有限生成左 R 加群、A を M の部分加群とする。このとき、R 加群としての同型

$$A^{\circ\circ} \cong A$$

が成り立つ。

系 5.7.

R を QF 環とし、C を左 R 加群 R^n の部分加群とする。このとき、R 加群としての同型

$$C^{\circ\circ} \cong C$$

が成り立つ。

系 5.8.

自然数 n と環 R に対して、次の条件は同値である。

(1) R は QF 環である。

(2) R は次の条件を満たす。

(2a) 任意の左 R 加群 $M \subseteq R^n$ に対して、
$M^{\circ\circ} = M$ が成り立つ。

(2b) 任意の右 R 加群 $N \subseteq R^n$ に対して、
$N^{\circ\circ} = N$ が成り立つ。

非可換環上においては、線形符号を左加群と右加群で区別する必要がある。よって、必ずしも可換とは限らない環に対しては、次のように定める。

環 R 上の長さ n の線形左符号 C とは、R 加群 R^n の空でない部分左加群として定義する。線形右符号についても、部分右加群として同様に定める。

線形左符号 $C \subseteq R^n$ に対して、$C^{\perp}$ が

$$C^{\perp} = \{a \in R^n \mid \text{任意の } c \in C \text{ に対して } < c, a > = 0\}$$

として定義される。$C^{\perp}$ は線形右符号となることが分かる。$C^{\perp}$ を C の双対符号という。

次の補題を直接証明することができる。

補題 5.9.

R を環とし、C を左 R 加群 R^n の部分加群とする。このとき、

$$C^{\circ\circ} = (C^{\perp})^{\perp}$$

が成り立つ。

系 5.8. と補題 5.9. から次の定理が導かれる。

定理 5.10.

自然数 n と環 R に対して、次の条件は同値である。

(1) R は QF 環である。

(2) R は次の条件を満たす。

(2a) 任意の左 R 加群 $C \subseteq R^n$ に対して、
$(C^{\perp})^{\perp} = C$ が成り立つ。

(2b) 任意の R 加群 $D \subseteq R^n$ 対して、
$(D^{\perp})^{\perp} = D$ が成り立つ。

定理 5.10. から、非可換環上の符号理論の定理として、次のことが分かる。

定理 5.11.

R を有限 QF 環、$C \subseteq R^n$ を左線形符号とするとき、

$$(C^{\perp})^{\perp} = C$$

が成り立つ。

定理 5.12.

有限 QF 環 R に対して、$C \subseteq R^n$ が自由左符号ならば $C^{\perp}$ は自由右符号であり、階数は

$$rank C^{\perp} = n - rank C$$

が成り立つ。

6 今後の展開

本研究を踏まえて今後の方向性を記述する。

(1) 有限フロベニウス環上の符号理論

M. Matsuoka (2012) において、有限体上の多重巡回符号と逐次符号の関係を調べ、逐次符号の多項式表現を構成した。有限体を拡張し、有限フロベニウス環や有限 QF 環上においても逐次符号の多項式表現等を考察することが考えられる。

(2) 非可換 QF 環を拡張した符号理論

本研究において最も広いクラスの環は、非可換 QF 環である。今後、非可換 QF 環をさらに拡張した環上における符号理論を展開することが考えられる。

(3) 圏論的手法による考察

本研究においては、環論やホモロジー代数を用いて符号理論の展開を考えた。今後はさらに抽象化し、圏論的手法を用いて考察することも考えられる。

参考文献

A. A. Andrade and Palazzo Jr. (2005) "Linear Codes over Finite Rings", TEMA Tend. Mat. Apl. Comput. 6, No. 2, 207–217.

D. Boucher and P. Sole (2008) "Skew constacyclic codes over Galois rings", Advances in Mathematics of Communications, Volume 2, No. 3, 273–292.

H. Cartan and S. Eilenberg (1956) "Homological Algebra", Princeton Univ. Press.

M. Greferath, M. E. O'Sullivan (2004) "On bounds for codes over Frobenius rings under homogeneous weights", Discrete Math, 289, 11–24.

Y. Hirano (1997) "On admissible rings", Indag. Math. 8, 55–59.

S. Ikehata (1980) "On separable polynomials and Frobenius polynomials in skew polynomial rings", Math. J. Okayama. Univ. 22, 115–129.

T. Y. Lam (1999) "Lectures on Modules and Rings, Graduate Texts in Mathematics", Vol. 189, Springer–Verlag, New York.

S. R. Lopez–Permouth, B. R. Parra–Avila and S. Szabo (2009) "Dual generalizations of the concept of cyclicity of codes", Advances in Mathematics of Communications, Volume 3, No. 3, 227–234.

M. Matsuoka (2011) "Polycyclic codes and sequential codes over finite commutative QF rings", JP Journal of Algebra, Number Theory and Applications, Vol. 23, No. 1, 77–85.

M. Matsuoka (2012) "Polynomial realization of sequential codes over finite fields", SUT Journal of Math., Vol. 48, No. 1, 47–53.

B. R. McDonald (1974) "Finite Rings With Identity", Pure and Applied Mathematics, Vol. 28, Marcel Dekker, Inc., New York.

J. J. Rotman (2008) "An Introduction to Homological Algebra", second edition, Springer.

K. Shiromoto and L. Storme (2003) "A Griesner bound for linear codes over finite quasi–Frobenius rings", Discrete Applied Mathematics 128, 263–274.

T. Sumiyama (1979) "Note on maximal Galois subrings of finite local rings", Math. J. Okayama. Univ. 21, No. 1, 31–32.

J. H. van Lint (1992) "Introduction to Coding Theory", second edition, New York, Springer.

J. A. Wood (1999) "Duality for modules over finite rings and applications to coding theory", Amer. J. Math, 121, 555–575.

＊本研究は 2014 年度大阪樟蔭女子大学特別研究助成費の助成を受けて行われたものである。

Study of Coding Theory over Finite Frobenius Rings

Faculty of Child Sciences, Department of Child Sciences
Manabu MATSUOKA

Abstract

In this paper we generalize coding theory over finite fields to finite rings. First, we consider finite commutative QF rings instead of finite fields, and we study cyclicity of linear codes. We define polycyclic codes and sequential codes, natural generalization of cyclic codes, and study duality of these codes over finite commutative QF rings. Next, we characterized the family of principal polycyclic codes with invertible constant terms over finite commutative QF rings. Finally, we generalize coding theory over finite commutative QF rings to finite noncommutative rings, and we show results and problems of the neighbourhood last.

Keywords: Frobenius Rings, Noncommutative Rings, Dual Codes, Polycyclic Codes, Sequential Codes.