数理解析研究所講究録
第1873巻 2014年 52-58

Generalizations of cyclic codes over finite fields

大阪樟蔭女子大学・児童学部　松岡　学
Manabu Matsuoka
Faculty of Child Science,
Osaka Shoin Women's University

1　はじめに

有限体 $\mathbf{F}$ 上のベクトル空間 $\mathbf{F}^n = \{(a_0, \cdots, a_{n-1}) \mid a_i \in \mathbf{F}\}$ の部分空間 C のことを長さ n の線形符号という。線形符号 $C \subseteq \mathbf{F}^n$ が条件

$$(a_0, a_1, \cdots, a_{n-1}) \in C \text{ ならば } (a_{n-1}, a_0, a_1, \cdots, a_{n-2}) \in C$$

を満たすとき、巡回符号であるという。巡回符号の概念には様々な拡張の方法がある。C を有限体 $\mathbf{F}$ 上の長さが n の線形符号とし, $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathbf{F}^n$ を固定する。このとき, 任意の $(a_0, a_1, \cdots, a_{n-1}) \in C$ に対して、

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

が成り立つとき, C を c に誘導される逐次符号と呼ぶ。

S. R. López-Permouth と B. R. Parra-Avila, S. Szabo は多巡回符号と逐次符号の関係を [5] において調べた。彼らの結果を踏まえて、ここでは逐次符号を多項式環の剰余環のイデアルとして具体的に実現する方法を考える。また、巡回符号の有限環上への拡張方法についても考察する。

以後特に断らない限り、$\mathbf{F}$ は $1 \neq 0$ である有限体、n は2以上の自然数、(g) は $g \in \mathbf{F}[X]$ によって生成される両側イデアルを表すものとする。

2　多重巡回符号

$\mathbf{F}$ を有限体とする。 $\mathbf{F}^n$ における k 次元部分空間 C のことを線形 $[n, k]$ 符号という。

定義 1. C を有限体 $\mathbf{F}$ 上の長さが n の線形符号とし, $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathbf{F}^n$ を固定する。このとき、 任意の $(a_0, a_1, \cdots, a_{n-1}) \in C$ に対して

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

が成り立つとき, C を c によって誘導される多重巡回符号と呼ぶ。

巡回符号と同じように多重巡回符号も多項式環の剰余環のイデアルとして表現される。$c = (c_0, c_1, \cdots, c_{n-1}) \in \mathbf{F}^n$ 固定し $f(X) = X^n - c(X)$ とおく、ここで $c(X) = c_{n-1}X^{n-1} + \cdots + c_1X + c_0$ である。このとき、$\mathbf{F}$-線形同形写像 $\rho : \mathbf{F}^n \to \mathbf{F}[X]/(f(X))$ を $a = (a_0, a_1, \cdots, a_{n-1})$ に対し $a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ を対応させる写像として定める。このとき、この写像 ρ によって c に誘導される多重巡回符号と剰余環 $\mathbf{F}[X]/(f(X))$ のイデアルを同一視することができる。すなわち、C を $\mathbf{F}[X]/(f(X))$ における多巡回符号とすると、モニックな多項式 g と h が存在して $C = (g)/(f)$ と表せる。ただし、$f = hg$ である。

命題 2. 線形符号 $C \subseteq \mathbf{F}^n$ が c に誘導される多重巡回符号であるための必要十分条件は C が次のような形の $k \times n$ 生成行列をもつことである

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix}$$

であり $g_{n-k} \neq 0$。このとき、

$$\rho(C) = \left(\overline{g_{n-k}X^{n-k} + \cdots + g_1X + g_0}\right)$$

は $\mathbf{F}[X]/(f(X))$ のイデアルとなる。

$c = (c_0, c_1, \cdots, c_{n-1}) \in \mathbf{F}^n$ に対して、D_c を次の形の正方行列とする。

$$D_c = \begin{pmatrix} 0 & 1 & & 0 \\ & & \ddots & \\ 0 & & & 1 \\ c_0 & c_1 & \cdots & c_{n-1} \end{pmatrix}.$$

線形符号 $C \subseteq \mathbf{F}^n$ が $c \in \mathbf{F}^n$ に誘導される多重巡回符号であるための必要十分条件は D_c の右からの乗法で C が閉じていることである。

3 逐次符号

定義 3. C を R 上長さ n の線形符号とし、$c=(c_0,c_1,\cdots,c_{n-1})\in \mathbf{F}^n$ を固定する。このとき、任意の $(a_0,a_1,\cdots,a_{n-1})\in C$ に対して

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

が成り立つとき C を c によって誘導される逐次符号と呼ぶ。

線形符号 $C\subseteq \mathbf{F}^n$ が $c=(c_0,c_1,\cdots,c_{n-1})$ に誘導される逐次符号であるための必要十分条件は 次の行列の右からの乗法で C が閉じていることである。

$$ {}^tD_c=\begin{pmatrix} 0 & & 0 & c_0 \\ 1 & & & c_1 \\ & \ddots & & \vdots \\ 0 & & 1 & c_{n-1} \end{pmatrix}$$

$\mathbf{F}^n$ 上に次のような標準的な内積を定義する。
$x=(x_0,x_1,\cdots,x_{n-1})$, $y=(y_0,y_1,\cdots,y_{n-1})\in \mathbf{F}^n$ に対して

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

線形符号 C の双対符号 $C^{\perp}$ を次のように定義する。

$$C^{\perp}=\{a\in \mathbf{F}^n|\ \text{任意の } c\in C \text{ に対して } <c,a>=0\}.$$

明らかに $C^{\perp}$ は $\mathbf{F}$ 上の線形符号になる。関係式 $\dim C^{\perp}=n-\dim C$ はよく知られている。

定理 4. $C\subseteq \mathbf{F}^n$ を線形符号とする。このとき、C が多重巡回符号（逐次符号）であるための必要十分条件は $C^{\perp}$ が逐次符号（多重巡回符号）であることである。

4 逐次符号の多項式表現

$\mathbf{F}$-線形同型写像 $\tau:\mathbf{F}^n\to \mathbf{F}[X]/(X^n-c_{n-1}X^{n-1}-\cdots-c_0)$ を

$$\tau(a_0,a_1,\cdots,a_{n-1})=\overline{b_{n-1}X^{n-1}+\cdots+b_1X+b_0}$$

ただし、

$$b_i=a_{n-i-1}-a_{n-i-2}c_{n-1}-a_{n-i-3}c_{n-2}-\cdots-a_0c_{i+1},\ (i=0,1,\cdots,n-2),\ b_{n-1}=a_0$$

と定める。

定理 5. C が c により誘導された逐次符号のとき、
$\tau(C)$ は $\mathbf{F}[X]/(X^n-c_{n-1}X^{n-1}-\cdots-c_0)$ のイデアルである。

定理 5 より、次の系が成り立つ。

系 6. 任意の逐次符号 $C \subseteq \mathbf{F}^n$ に対して、$\tau(C) = (g)/(f)$ かつ $f = hg.$ を満たす適当なモニックな多項式 $g, h \in \mathbf{F}[X]$ が存在する。

例 7. $n = 5$ の場合、$f(X) = X^5 - c_4X^4 - c_3X^3 - c_2X^2 - c_1X - c_0$ とすると、
$\tau : \mathbf{F}^5 \to \mathbf{F}[X]/(f(X))$ は $(a_0, a_1, a_2, a_3, a_4)$ を $b_4X^4 + b_3X^3 + b_2X^2 + b_1X + b_0$ に移す。
ここで、
$b_4 = a_0,$
$b_3 = a_1 - a_0c_4,$
$b_2 = a_2 - a_1c_4 - a_0c_3,$
$b_1 = a_3 - a_2c_4 - a_1c_3 - a_0c_2,$
$b_0 = a_4 - a_3c_4 - a_2c_3 - a_1c_2 - a_0c_1,$
である。逐次符号 $C \subseteq \mathbf{F}^5$ に対して、$\tau(C)$ は $\mathbf{F}[X]/(f(X))$ のイデアルとなる。

5 有限可換 QF 環上の符号

R を（必ずしも可換とは限らない）環とする。左 R-加群 P は、任意の全射 R-準同型写像 $g : M \to N$ と任意の R-準同型写像 $f : P \to N$ に対して、$f = g \circ h$ を満たすような適当な R-準同型写像 $h : P \to M$ が存在するとき、射影加群と呼ばれる。

左 R-加群 Q は任意の単射 R-準同型写像 $g : N \to M$ と任意の R-準同型写像 $f : N \to Q$ に対して、$f = h \circ g$ を満たすような適当な R-準同型写像 $h : M \to Q$ が存在するとき、入射加群と呼ばれる。

環 R は左（右） R-加群として入射加群であるとき、左（右）自己入射と呼ばれる。R が左かつ右自己入射であるとき、単に自己入射と呼ばれる。

左 R-加群 M は部分加群に関する降鎖条件を満たすとき、アルティン加群と呼ばれる。環 R は左（右） R-加群としてアルティン加群のとき、左（右）アルティン環という。環 R が左かつ右アルティン環のとき、単にアルティン環と呼ばれる。

明らかに有限環はアルティン環である。

定義 8. R を（必ずしも可換とは限らない）環とする。R が左アルティンかつ左自己入射であるとき、R は QF (quasi-Frobenius) 環と呼ばれる。

QF 環になるための条件は左-右対象であることがよく知られている。

任意の R-部分加群 $C \subseteq R^n$ に対して、C° は次のように定義される。

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

定理 9. R を（必ずしも可換とは限らない）環とする。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。

QF 環は射影加群や入射加群を用いて、次のように特徴づけることもできる。

定理 10. R を（必ずしも可換とは限らない）環とする。次の条件は同値である。
(1) R は QF 環である。
(2) 左加群が射影加群であること入射加群であることは同値である。

次に可換有限環上の符号について考える。可換有限環 R 上の加群 R^n の部分加群 C を環 R 上の長さ n の線形符号という。C が階数 r の自由加群のとき、C を階数 r の自由符号と呼び $\mathrm{rank}C = r$ と表す。

以後特に断らない限り、R は可換有限環を表すものとする。

有限体の場合と同様に、可換有限環においても巡回符号、多重巡回符号、逐次符号、双対符号などが定義される。多重巡回符号と逐次符号の関係について、次が成り立つ。

定理 11. 線形符号 $C \subseteq R^n$ 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。

R-加群準同型写像 $\delta_x : R^n \to R$ を任意の $x \in R^n$ に対して $\delta_x(y) =< y, x >$ であるように定義する。

命題 12. x を δ_x へ対応させるような準同型写像 $\delta : C^{\perp} \to C^{\circ}$ は R-加群の間の準同型写像である。

可換有限 QF 環上の多重巡回符号や逐次符号の代数的な性質を調べたい。

定理 13. R を可換有限 QF 環とする。任意の部分加群 $C \subseteq R^n$ に対して、$(C^{\perp})^{\perp} = C$ が成り立つ。

定理 11 と 定理 13 から、次の系が成り立つ。

系 14. R を可換有限 QF 環とする。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。

定理 15. R を可換有限 QF 環とする。$C \subseteq R^n$ が有限階数の自由 R-加群であるとき、$C^{\perp}$ も有限階数の自由 R-加群であり、$\mathrm{rank}C^{\perp} = n - \mathrm{rank}C$ が成り立つ。

有限体上の多項式環は単項イデアル整域であったが、一般に可換有限環においてはそうではない。ここでは、1 つの多項式から生成される線形符号について考える。

定義 16. R を可換有限環とし、C を $R[X]/(f(X))$ における 多重巡回符号とする。モニックな多項式 g, h が存在して $\rho(C) = (g)/(f)$ かつ $f = hg$ を満たすとき、C を単項多重巡回符号と呼ぶ。さらに、g の定数項が可逆のとき、C を可逆な定数項をもつ単項多重巡回符号という。

C を $R[X]/(f(X))$ における多重巡回符号とする。$f = X^n - \alpha \in R[X]$ の形のとき、C を定数的巡回符号と呼ぶ。

可換有限 QF 環上の定数的巡回符号のパリティ検査行列を決定する。

命題 17. R を可換有限 QF 環とし、$f = X^n - \alpha \in R[X]$ とする。$f = hg \in R[X]$ であり、g と h はそれぞれ次数が $n-k$ と k の多項式であるとする。C を $R[X]/(X^n - \alpha)$ において g により生成されるイデアルに対応する線形 $[n,k]$-符号とし、$h(X) = h_k X^k + h_{k-1}X^{k-1} + \cdots + h_1 X + h_0$ とする。このとき、C は次のような $(n-k) \times n$ パリティ検査行列 H をもつ

$$H = \begin{pmatrix} h_k & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ 0 & h_k & \cdots & h_1 & h_0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \cdots & 0 & h_k & \cdots & h_1 & h_0 \end{pmatrix}.$$

定義 18. R を可換有限 QF 環とし、$C \subseteq R^n$ を逐次符号とする。C は、$C^\perp$ が単項多重巡回符号であるとき、単項逐次符号と呼ばれる。さらに、$C^\perp$ が可逆な定数項をもつ単項多重巡回符号であるとき、C を可逆な定数項をもつ単項逐次符号という。

最終的に、次の定理が成り立つ。

定理 19. R を可換有限 QF 環とし、C を R^n における自由符号とする。このとき、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符号であり、可逆な定数項をもつ単項逐次符号である。

(4) $C^\perp$ は可逆な定数項をもつ単項多重巡回符号であり、可逆な定数項をもつ単項逐次符号である。

(5) $C = (g)/(X^n - \alpha)$ は可逆な α をもつ定数的巡回符号である。

(6) $C^\perp = (q)/(X^n - \beta)$ は可逆な β をもつ定数的巡回符号である。

これまで可換有限 QF 環上の多重巡回符号や逐次符号の代数的な性質を調べてきたが、有限体の場合と同様に、逐次符号と多項式環の剰余環との関係を可換有限 QF 環上で構築することが今後の課題である。

参考文献

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

[2] Y. Hirano, *On admissible rings*, Indag. Math. **8** (1997), 55–59.

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

[4] T. Y. Lam, *Lectures on Modules and Rings, Graduate Texts in Mathematics*, Vol. 189, Springer-Verlag, New York, 1999.

[5] S. R. López-Permouth, B. R. Parra-Avila and S. Szabo, *Dual generalizations of the concept of cyclicity of codes*, Advances in Mathematics of Communications, Volume **3**, No. **3** (2009), 227–234.

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

[7] M. Matsuoka, *Polynomial realization of sequential codes over finite fields*, SUT Journal of Mathematics, Vol. **48** (2012), No. **1**, 47–53.

[8] B. R. McDonald, *Finite Rings With Identity, Pure and Applied Mathematics*, Vol. 28, Marcel Dekker, Inc., New York, 1974.

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