Piret の巡回たたみ込み符号と接合積

武田二郎*, 西内　信**

(昭和53年 9月 4日受理)

Piret's Cyclic Convolutional Code and Crossed Product

ZIRŌ TAKEDA and MAKOTO NISHIUCHI

Abstract: — A cyclic block code is given as an ideal in the residual polynomial algebra modulo X^n-1. This fact became a clue to the intense research of the algebraic theory for block codes in the last two decades. On the contrary, such an algebraic construction of a convolutional code was not found until recently. G.D. Forney [1] filled up the vacancy and gave an algebraic description for a convolutional code using the delay operator D and P. Piret [2] introduced and discussed the concept of cyclic convolutional code basing on Forney's formulation.

In this paper we give a construction of a large linear algebra which contains the set of all code word sequences as a left ideal using the crossed product technique familiar in the ring theory. Thus we acquire an algebraic system for a cyclic convolutional code corresponding to the residual polynomial algebra for the case of cyclic block code.

1　序

情報源から発生する情報記号の列をk個ごとのブロックに区切り，符号器によってこれをn個の記号からなるコード単語に変える符号化のプロセスについて考察する。

$[i_{k-1}, i_{k-2}, \cdots, i_0]$ → **符号器** → $[v_{n-1}, v_{n-2}, \cdots, v_0]$
（情報記号）　　（コード単語）

この符号を（n，k）符号という。符号はブロック符号とたたみ込み符号の2種に大別される。

1ブロックの符号化が，それ以前に符号器に送り込まれた記号列に無関係に，ブロックごとに遂行されるのが**ブロック符号**であり，それ以前のいくつかのブロックにも関係して符号化が行われるのが**たたみ込み符号**である。ブロック符号の方は原理的に単純なので研究が進み，現在までの符号理論の文献の大部分はブロック符号に関するものである。しかし符号器の装置化の点では，ブロック符号では1ブロックの符号化が済むごとに符号器の内容をクリヤーする必要があるのに対し，たたみ込み符号では符号化を中断せず，連続的に実行できる利点をもっている。

ブロック符号では巡回符号が発見され，符号理論に代数学の知識が活用されるようになって，研究が飛躍的に進捗している。すなわち

$$[v_0, v_1, \cdots, v_{n-1}] \longrightarrow v(X) = v_0X^{n-1}+v_1X^{n-2}+\cdots+v_{n-1}$$

によって，コード単語にコード多項式を対応させると，巡回符号ではコード多項式の全体は，X^n-1を法とする有限体上の剰余多項式環のイデアルとなる。この事実がいわゆる代数的符号理論の出発点となる。最近までたたみ込み符号にはこれに対応するような理論が無く，研究の主題は，符号化のアルゴリズムが指定されている場合の効率的な復号法についての議論であった。しかしG.Forney [1] が遅延演算子Dを含む代数系を用いて，たたみ込み符号の符号化の過程をブロック符号のそれに

* 茨城大学工学部情報工学科（日立市中成沢町）
** 茨城大学大学院工学研究科情報工学専攻（日立市中成沢町）　現職日本ソフトウェア開発KK勤務

類似した形式に表現することに成功して以来，たたみ込み符号の代数理論の研究が盛んになっている。P.Piret〔2〕はこのブロック符号との類似性をたどって巡回たたみ込み符号の研究をおこなっている。この論文では環論における接合積の概念を用いて，Piretの巡回たたみ込み符号列をその左イデアルとして含むような，ブロック符号の場合のX^n-1を法とする剰余多項式環に相当する，線形環の構成法について述べる。Delsarte－Piret〔3〕の正規たたみ込み符号についても同じ方法で，その符号語列の集合を左イデアルとして含む拡大環が構成できる。

2　ブロック符号とたたみ込み符号

ブロック符号の代表例として，（7,4）Hamming符号の符号化回路について述べよう。

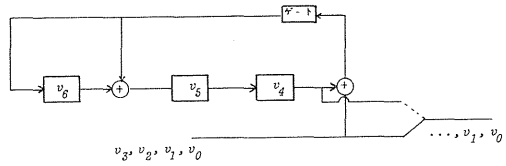

Fig. 1

〔v_0，v_1，v_2，v_3〕を符号化しようとする，4個の0，1の系列とする。ゲートを閉じてこの情報記号列を入力すると，そのまま出力されるとともに，3個のシフトレジスターにv_4，v_5，v_6がストアされる。つぎにゲートを開き，レジスターの内容を出力させると

入力 $[v_0, v_1, v_2, v_3] \longrightarrow$

出力 $[v_0, v_1, v_2, v_3, v_4, v_5, v_6]$

となる。この回路は$GF(2)$係数の入力多項式

$$i(X)=v_0X^6+v_1X^5+v_2X^4+v_3X^3$$

を　$g(X)=X^3+X+1$　で割ったときの剰余

$r(X)=v_4X^2+v_5X+v_6$を計算するもので，（7,4）Hamming符号は$\boldsymbol{i}=$〔v_0，v_1，v_2，v_3〕を$\boldsymbol{v}=$〔v_0，v_1，v_2，v_3，v_4，v_5，v_6〕にコード化する符号である。これは

$$\begin{aligned}1000 &\longrightarrow 1000101\\ 0100 &\longrightarrow 0100111\\ 0010 &\longrightarrow 0010110\\ 0001 &\longrightarrow 0001011\end{aligned}$$

となる線形符号だから，行列

$$G=\begin{bmatrix}1000101\\0100111\\0010110\\0001011\end{bmatrix}$$

を用いれば，符号化は$\boldsymbol{i}\ G=\boldsymbol{v}$ すなわち

$[v_0, v_1, v_2, v_3,]G=[v_0, v_1, v_2, v_3, v_4, v_5, v_6]$ (*)

で与えられる。

たたみ込み符号では普通符号器にk個の情報記号が並列で入力し，それに対応するコード単語も並列で出力するものとする。下図は並列に2個の記号が入力して，3個の記号が出力する（3,2）たたみ込み符号器の回路である。

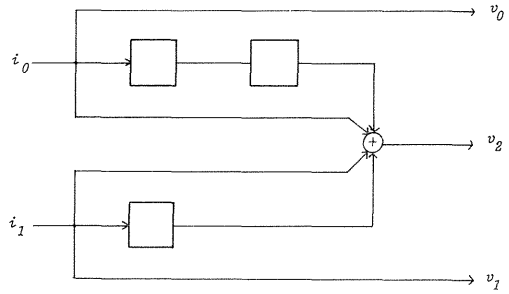

Fig. 2

入力はベクトル列

$$\boldsymbol{i}=(\cdots, \boldsymbol{i}_0, \boldsymbol{i}_1, \boldsymbol{i}_2, \cdots)\equiv$$

$$\left(\cdots, \begin{bmatrix}i_{00}\\i_{01}\end{bmatrix}, \begin{bmatrix}i_{10}\\i_{11}\end{bmatrix}, \begin{bmatrix}i_{20}\\i_{21}\end{bmatrix}, \cdots\right)$$

で，出力は

$$\mathsf{v}=(\cdots, \mathsf{v}_0, \mathsf{v}_1, \mathsf{v}_2, \cdots)\equiv$$

$$\left(\cdots, \begin{bmatrix}v_{00}\\v_{01}\\v_{02}\end{bmatrix}, \begin{bmatrix}v_{10}\\v_{11}\\v_{12}\end{bmatrix}, \begin{bmatrix}v_{20}\\v_{21}\\v_{22}\end{bmatrix}, \cdots\right)$$

である。この場合

$$\begin{aligned}i_0(D)&=\cdots+i_{00}D^0+i_{10}D^1+i_{20}D^2+\cdots\cdots\\ i_1(D)&=\cdots+i_{01}D^0+i_{11}D^1+i_{21}D^2+\cdots\cdots\\ v_0(D)&=\cdots+v_{00}D^0+v_{10}D^1+v_{20}D^2+\cdots\cdots\\ v_1(D)&=\cdots+v_{01}D^0+v_{11}D^1+v_{21}D^2+\cdots\cdots\\ v_2(D)&=\cdots+v_{02}D^0+v_{12}D^1+v_{22}D^2+\cdots\cdots\end{aligned}$$

と表わし

$$g_{00}(D)=1,\ g_{11}(D)=1,$$
$$g_{02}(D)=1+D^2,\ g_{12}(D)=1+D$$

と置くと，入力と出力の関係は

$$v_0(D)=i_0(D)$$
$$v_1(D)=i_1(D)$$
$$v_2(D)=i_0(D)g_{02}(D)+i_1(D)g_{12}(D)$$

となる。あるいは行列を用いて

$$[v_0(D),\ v_1(D),\ v_2(D)]=$$
$$[i_0(D),i_1(D)]\begin{bmatrix} g_{00}(D) & 0 & g_{02}(D) \\ 0 & g_{11}(D) & g_{12}(D)\end{bmatrix}$$

と表わされる。上式の右辺の生成行列は

$$G(D)=\begin{bmatrix}1&0&1+D^2\\0&1&1+D\end{bmatrix}$$
$$=\begin{bmatrix}101\\011\end{bmatrix}+\begin{bmatrix}000\\001\end{bmatrix}D+\begin{bmatrix}001\\000\end{bmatrix}D^2$$

と行列係数のDの多項式で表示することもできる。

一般に（n，k）たたみ込み符号ではその生成行列を

$$G(D)=\begin{bmatrix} g_{00}(D) & g_{01}(D) & \cdots g_{0,n-1}(D)\\ g_{10}(D) & g_{11}(D) & \cdots g_{1,n-1}(D)\\ \vdots & \vdots & \vdots \\ g_{k-1,0}(D) & g_{k-1,1}(D) & \cdots g_{k-1,n-1}(D)\end{bmatrix}$$

その入力記号列，出力記号列をそれぞれ

$$\boldsymbol{i}(D)=[i_0(D),\ i_1(D),\ \cdots,\ i_{k-1}(D)]$$
$$\mathrm{v}(D)=[v_0(D),\ v_1(D),\ \cdots,\ v_{n-1}(D)]$$

とすると，符号化の過程は

$$\mathrm{v}(D)=\boldsymbol{i}(D)G(D) \qquad (**)$$

で表わされる。ここで

$$m=\max_{i,\,j}[\deg g_{ij}(D)]$$

とすると

$$G(D)=G_0+G_1D+\cdots+G_mD^m$$

（G_i（$0\leqq i\leqq m$）はGF（q）の元の$k\times n$行列）と，行列係数のDの多項式に表示され，出力列は

$$v_j(D)=\cdots+v_{0j}D^0+v_{1j}D^1+v_{2j}D^2+\cdots$$
$$(v_{lj}\in \mathrm{GF}(q),\ 0\leqq j\leqq n-1,\ l=0,\pm1,\pm2,\cdots)$$

のとき

$$\boldsymbol{v}(D)=\begin{bmatrix}v_0(D)\\v_1(D)\\\vdots\\v_{n-1}(D)\end{bmatrix}$$

$$=\cdots+\begin{bmatrix}v_{00}\\v_{01}\\\vdots\\v_{0n-1}\end{bmatrix}D^0+\begin{bmatrix}v_{10}\\v_{11}\\\vdots\\v_{1n-1}\end{bmatrix}D^1+$$

$$\begin{bmatrix}v_{20}\\v_{21}\\\vdots\\v_{2n-1}\end{bmatrix}D^2+\cdots\equiv\sum_{j=-\infty}^{\infty}v_j(X)D^j$$

ただし

$$v_j(X)=v_{j0}X^{n-1}+v_{j1}X^{n-2}+\cdots+v_{jn-1},$$

（$v_j(X)$はX^n-1を法とするGF（q）上の多項式環の元）と書き表わされる。

たたみ込み符号の表示を用れば，ブロック符号は$m=0$すなわち生成多項式がDを含まない定多項式，$G(D)=G_0$の場合となる。前述の（7, 4）Hamming符号は，4個の情報記号が並列に符号器に入力されるものとすると，生成行列の形から，下のようなシフトレジスターを1つも含まない線形回路によって生成される符号である。

ブロック符号でも，たたみ込み符号でも，整理すればその符号化の過程は（＊）および（＊＊）と同一の形式に表わされるから，ブロック符号に導入された概念の中のいくつかをたたみ込み符号に拡張し，ブロック符号の理

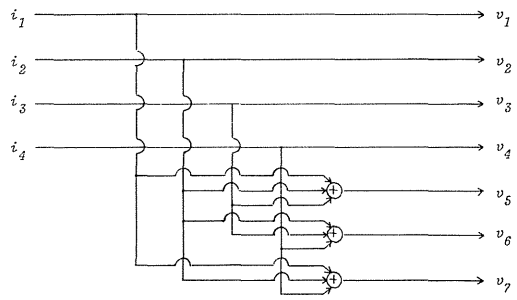

Fig. 3

論に並行してたたみ込み符号の性質を調べることが可能になる。

3　巡回符号

ブロック符号では，コード単語の全体を$\boldsymbol{C}$とするとき条件

$$[v_0, v_1, \cdots, v_{n-1}] \in \boldsymbol{C} \Rightarrow [v_1, v_2, \cdots, v_{n-1}, v_0] \in \boldsymbol{C}$$

を満たすとき，巡回符号と呼び，符号理論の中のもっとも重要な概念の1つになっている。たとえば前掲の（7, 4）Hamming符号はその1例である。なぜなら生成行列の第1行を巡回的にシフトすると

〔1000101〕（第1行）→〔0001011〕（第4行）
〔0001011〕（第4行）→〔0010110〕（第3行）
〔0010110〕（第3行）→〔0101100〕（第2行＋第4行）
〔0100111〕（第2行）→〔1001110〕（第1行＋第4行）

となるから，これらの行の1次結合で表わされる任意のコード単語について，その単語を巡回的にシフトしたものはまたこれらの行の1次結合となり，$\boldsymbol{C}$に属する。

たたみ込み符号の表示法を用い，符号器から生成されるコード単語列を$\boldsymbol{v}(D)$で表わせば，コード単語列について巡回性の条件は

$$\boldsymbol{v}(D) = \cdots + \begin{bmatrix} v_{00} \\ v_{01} \\ \vdots \\ v_{0n-1} \end{bmatrix} D^0 + \begin{bmatrix} v_{10} \\ v_{11} \\ \vdots \\ v_{1n-1} \end{bmatrix} D^1 + \begin{bmatrix} v_{20} \\ v_{21} \\ \vdots \\ v_{2n-1} \end{bmatrix} D^2 + \cdots \in \boldsymbol{C}(D)$$

ならば

$$\boldsymbol{v}^*(D) = \cdots + \begin{bmatrix} v_{01} \\ v_{02} \\ \vdots \\ v_{0n-1} \\ v_{00} \end{bmatrix} D^0 + \begin{bmatrix} v_{11} \\ v_{12} \\ \vdots \\ v_{1n-1} \\ v_{10} \end{bmatrix} D^1 + \begin{bmatrix} v_{21} \\ v_{22} \\ \vdots \\ v_{2n-1} \\ v_{20} \end{bmatrix} D^2 + \cdots \in \boldsymbol{C}(D)$$

となる。（ここで$\boldsymbol{C}(D)$は符号器から生成されるコード単語列全部の集合とする。）

$X^n - 1$を法とするGF(q)上の剰余多項式環の元を

$$v_j(X) = v_{j0}X^{n-1} + v_{j1}X^{n-2} + \cdots + v_{jn-1}$$

とすると

$$Xv_j(X) = v_{j1}X^{n-1} + v_{j2}X^{n-2} + \cdots + v_{jn-1}X + v_{j0}$$

であるから，巡回符号の性質は

$$V(D) = \sum_{j=-\infty}^{\infty} v_j(X)D^j \in \boldsymbol{C}(D) \Rightarrow V^*(D) = \sum_{j=-\infty}^{\infty} Xv_j(X)D^j \in \boldsymbol{C}(D)$$

と表わされる。

たたみ込み符号でもコード単語列$\boldsymbol{v}(D)$はブロック符号のときと同様に表わされるから，上と同じ条件で巡回たたみ込み符号を定義することが考えられる。しかし，P.Piretはこの条件を満たす巡回たたみ込み符号は生成行列にDを含まず，実質的にブロック符号に等しいことを証明している〔4〕。そしてπをnと素な正整数とするとき条件

$$\boldsymbol{v}(D) = \sum_{j=-\infty}^{\infty} v_j(X)D^j \in \boldsymbol{C}(D) \Rightarrow \boldsymbol{v}^{\pi}(D) = \sum_{j=-\infty}^{\infty} X^{\pi j}v_j(X)D^j \in \boldsymbol{C}(D)$$

によって巡回たたみ込み符号を定義することを提唱し，その性質を調査している〔2〕。たとえば$\pi = 2$，$n =$奇数のとき上述の$\boldsymbol{v}(D)$に対して

$$\boldsymbol{v}^{\pi}(D) = \cdots + \begin{bmatrix} v_{01} \\ v_{02} \\ \vdots \\ v_{0n-1} \\ v_{00} \end{bmatrix} D^0 + \begin{bmatrix} v_{12} \\ v_{13} \\ \vdots \\ v_{1n-1} \\ v_{10} \\ v_{11} \end{bmatrix} D^1 + \begin{bmatrix} v_{14} \\ v_{15} \\ \vdots \\ v_{1n-1} \\ v_{10} \\ v_{11} \\ v_{12} \\ v_{13} \end{bmatrix} D^2 + \cdots$$

となる。$\pi=1$の場合には前述のv^*(D)と一致する。

以下でPirctの巡回性の定義の意味づけを考察する。

4　線形環の接合積

$\mathfrak{o}$は体$\boldsymbol{F}$上の線形環とする。すなわち$x, y\in\mathfrak{o}$，$a, b\in\boldsymbol{F}$とするとx，yの和$x+y$，積xyとスカラー倍axが定義されてつぎが満たされるものとする：

（A0）　$x+y\in\mathfrak{o}$，$xy\in\mathfrak{o}$，$ax\in\mathfrak{o}$

（A1）　$(x+y)+z=x+(y+z)$

（A2）　$x+y=y+x$

（A3）　$\exists 0: x+0=x$

（A4）　$\forall x\exists -x: x+(-x)=0$

（A5）　$a(x+y)=ax+ay$

（A6）　$(a+b)x=ax+bx$

（A7）　$(ab)x=a(bx)$

（A8）　$1x=x$

（A9）　$(xy)z=x(yz)$

（A10）　$x(ay+bz)=a(xy)+b(xz)$

（A11）　$(ay+bz)x=a(yx)+b(zx)$

更に

（A12）　$xy=yz$

が成り立つとき$\mathfrak{o}$は可換という。

$\boldsymbol{F}$係数のXの多項式

$$P(X)=a_0X^n+a_1X^{n-1}+\cdots+a_n\quad(a_i\in\boldsymbol{F})$$

の全体$\boldsymbol{F}[X]$は通常の多項式の和，積，スカラー倍に関して体$\boldsymbol{F}$上の可換な線形環である。また$\boldsymbol{F}$係数の$n-1$次以下の多項式の全体を$\boldsymbol{F}_n[X]$，$g(X)$をn次の多項式として，通常の和，スカラー倍のほかに，積を

$$p(X)\cdot q(X)\mod g(X)$$

で定義すると$\boldsymbol{F}_n[X]$も体$\boldsymbol{F}$上の可換な線形環となる。これを$g(X)$を法とする体$\boldsymbol{F}$上の剰余多項式環という。

線形環$\mathfrak{o}$から$\mathfrak{o}$への1：1写像σ（$x\in\mathfrak{o}$の像をx^σで示す）がつぎの条件を満たすときに，σを$\mathfrak{o}$の自己同型写像という：$x, y\in\pi, a\in\boldsymbol{F}$に対して

$$(x+y)^\sigma=x^\sigma+y^\sigma,\ (ax)^\sigma=ax^\sigma,$$
$$(xy)^\sigma=x^\sigma y^\sigma$$

$\mathfrak{o}$の自己同型写像の全体をAut（$\mathfrak{o}$）で示す。$\sigma, \tau\in$Aut（$\mathfrak{o}$）のときその積を

$$\sigma\tau:\quad x\longrightarrow x^{\sigma\tau}=(x^\sigma)^\tau$$

で定義すれば$\sigma\tau$もまた$\mathfrak{o}$の自己同型写像である。そしてこの積に関してAut（$\mathfrak{o}$）は群となる。この場合Aut（$\mathfrak{o}$）の単位元は恒等写像ιであり，σの逆元は逆写像

$$\sigma^{-1}:\quad x^\sigma\longrightarrow x$$

である。Aut（$\mathfrak{o}$）を線形環$\mathfrak{o}$の自己同型群という。

以下Gを任意の有限群，eをその単位元とし，σを群GよりAut（$\mathfrak{o}$）への準同型写像とする。すなわち$\sigma(g)$はGの元gに対応する$\mathfrak{o}$の自己同型写像でつぎを満たすものとする：

$$\sigma(gh)=\sigma(g)\sigma(h),\ \sigma(e)=\iota,\ \sigma(g^{-1})=\sigma(g)^{-1}$$

σによるGの像$\sigma(G)\equiv\{\sigma(g)\mid g\in G\}$はAut（$\mathfrak{o}$）の部分群となる。

群Gより線形環$\mathfrak{o}$の自己同型群Aut（$\mathfrak{o}$）への準同型写像σが与えられると，つぎのようにしてσを用いて$\mathfrak{o}$の拡大環をつくることができる。

$\mathfrak{o}$の拡大環の構成

有限群G上で定義され，線形環$\mathfrak{o}$に値をとる関数で，Gの特定の元hで値x_hを，その他の元では0をとるものをu_hx_hと表わし，単項関数とよぶことにする。G上で

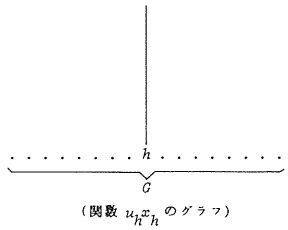

Fig. 4

定義され，点gで値x_gをとる一般の$\mathfrak{o}$値関数はこのような単項関数の和で表わされる：

$$u_ex_e+u_gx_g+u_hx_h+\cdots\cdots\equiv\Sigma_g u_gx_g$$

G上で定義された$\mathfrak{o}$値関数の全体を$\mathfrak{F}_{\mathfrak{o}}(G)$とし，その2つの関数の和とスカラー倍を

$$\Sigma_g u_gx_g+\Sigma_g u_gy_g=\Sigma_g u_g(x_g+y_g),$$
$$a\Sigma_g u_gx_g=\Sigma_g u_g(ax_g)\quad(a\in\boldsymbol{F})$$

と定めると，$\mathfrak{F}_{\mathfrak{o}}(G)$は（A0）～（A8）を満たし，体$\boldsymbol{F}$上の線形空間となることは明らかである。さらに群$G$から$\mathfrak{o}$の自己同型群Aut（$\mathfrak{o}$）への準同型写像$\sigma$が与

えられていると，積を定義して $\mathfrak{F}_{\sigma\mathfrak{l}}(G)$ を線形環とすることができる。そのためにまず単項関数に対しては

$$u_g x_g \cdot u_h y_h = u_{gh} x_g^{\sigma(h)} y_h$$

と定める。このとき結合律

$$u_g x_g (u_h y_h \cdot u_k z_k) = (u_g x_g \cdot u_h y_h) u_k z_k$$

が成り立つ，なぜなら

$$\begin{aligned}(u_g x_g \cdot u_h y_h) u_k z_k &= (u_{gh} x_g^{\sigma(h)} y_h) u_k z_k \\ &= u_{ghk} (x_g^{\sigma(h)} y_h)^{\sigma(k)} z_k \\ &= u_{ghk} (x_g^{\sigma(h)\sigma(k)} y_h^{\sigma(k)}) z_k \\ &= u_{ghk} x_g^{\sigma(hk)} y_g^{\sigma(k)} z_k\end{aligned}$$

一方

$$\begin{aligned}u_g x_g (u_h y_h \cdot u_k z_k) &= u_g x_g \cdot u_{hk} y_h^{\sigma(k)} z_k \\ &= u_{ghk} x_g^{\sigma(hk)} y_h^{\sigma(k)} z_k\end{aligned}$$

また

$$u_e 1 \cdot u_g x_g = u_g x_g = u_g x_g \cdot u_e 1$$

である。実際

$$u_e 1 \cdot u_g x_g = u_g 1^{\sigma(g)} x_g = u_g x_g$$

$$u_g x_g \cdot u_e 1 = u_g x_g 1 = u_g x_g$$

ただし

$$u_g x_g \cdot u_h y_h = u_{gh} x_g^{\sigma(h)} y_h,$$

$$u_h y_h \cdot u_g x_g = u_{hg} y_h^{\sigma(g)} x_g$$

となるから，群 G と環 $\sigma\mathfrak{l}$ が可換であっても，この積は一般には可換とならない。

$\mathfrak{F}_{\sigma\mathfrak{l}}(G)$ に属する一般の関数に対して積を

$$\begin{aligned}\sum_g u_g x_g \cdot \sum_g u_g y_g &= \sum_g u_g x_g \cdot \sum_h u_h y_h \\ &= \sum_g (\sum_h u_{gh} x_g^{\sigma(h)} y_h) = \sum_g (\sum_h u_g x_{gh^{-1}}^{\sigma(h)} y_h) \\ &= \sum_g u_g (\sum_h x_{gh^{-1}}^{\sigma(h)} y_h) \qquad (***)\end{aligned}$$

と定めると，積の結合律と分配率が成り立ち，$\mathfrak{F}_{\sigma\mathfrak{l}}(G)$ は $u_e 1$ を乗法の主単位元とする体 $\boldsymbol{F}$ 上の非可換な線形環となる。

結合率（A9）

$$(\sum_g u_g x_g \cdot \sum_g u_g y_g) \cdot \sum_g u_g z_g = \sum_g u_g x_g (\sum_g u_g y_g \cdot \sum_g u_g z_g)$$

証明

$$\begin{aligned}(\sum_g u_g x_g \cdot \sum_h u_h y_h) \cdot \sum_k u_k z_k &= \sum_g u_g (\sum_h x_{gh^{-1}}^{\sigma(h)} y_h) \cdot \sum_k u_k z_k \\ &= \sum_g u_g (\sum_k (\sum_h x_{gk^{-1}h^{-1}}^{\sigma(h)} y_h)^{\sigma(k)} z_k) \\ &= \sum_g u_g (\sum_k \sum_h x_{g(hk)^{-1}}^{\sigma(hk)} y_h^{\sigma(k)} z_k)\end{aligned}$$

一方

$$\sum_g u_g x_g \cdot (\sum_h u_h y_h \cdot \sum_k u_k z_k) = \sum_g u_g x_g \cdot \sum_h u_h (\sum_k y_{hk^{-1}}^{\sigma(k)} z_k)$$

$$= \sum_g u_g (\sum_h x_{gh^{-1}}^{\sigma(h)} (\sum_k y_{hk^{-1}}^{\sigma(k)} z_k)) = \sum_g u_g \sum_k (\sum_h x_{gh^{-1}}^{\sigma(h)} y_{hk^{-1}}^{\sigma(k)}) z_k$$

$$= \sum_g u_g \sum_k (\sum_h x_{g(hk)^{-1}}^{\sigma(hk)} y_h^{\sigma(k)}) z_k$$

分配律（A10）

$$\sum_g u_g x_g (a \sum_g u_g y_g + b \sum_g u_g z_g) =$$

$$a(\sum_g u_g x_g)(\sum_g u_g y_g) + b(\sum_g u_g x_g)(\sum_g u_g z_g)$$

証明

$$\sum_g u_g x_g (a \sum_g u_g y_g) = a(\sum_g u_g x_g)(\sum_g u_g y_g)$$

は明らかだから，$a = b = 1$ の場合を証明する。

$$\begin{aligned}\sum_g u_g x_g (\sum_h u_h y_h + \sum_h u_h z_h) &= \sum_g u_g x_g \cdot \sum_h u_h (y_h + z_h) \\ &= \sum_g u_g (\sum_h x_{gh^{-1}}^{\sigma(h)} y_h) + \sum_g u_g (\sum_h x_{gh^{-1}}^{\sigma(h)} z_h) \\ &= (\sum_g u_g x_g)(\sum_h u_h y_h) + (\sum_g u_g x_g)(\sum_h u_h z_h)\end{aligned}$$

同様にして分配率A（11）も証明される。

$\mathfrak{F}_{\sigma\mathfrak{l}}(G)$ の部分環 $\{ u_e a \mid a \in \sigma\mathfrak{l} \}$ は $\sigma\mathfrak{l}$ と同型だから，$\mathfrak{F}_{\sigma\mathfrak{l}}(G)$ は $\sigma\mathfrak{l}$ の拡大環である。この拡大環を $G \otimes_\sigma \sigma\mathfrak{l}$ で表わし，σ についての $\sigma\mathfrak{l}$ の G による接合積という。

注意　線形環 $\sigma\mathfrak{l}$ の元で $\sigma\mathfrak{l}$ の任意の元と可換なものの全体を $\sigma\mathfrak{l}$ の中心といい，Z で表わす。$\sigma\mathfrak{l}$ が可換なときには $\sigma\mathfrak{l} = Z$ である。群 G の元の任意の組（g，h）に対して定まる Z の元 $a_{g.h}$ が

$$a_{gh,k} a_{g,h}^{\sigma(k)} = a_{g,hk} a_{h,k}$$

を満たすとき，$\{ a_{g.h} \}$ を**因子団**という。因子団を用いれば上述の接合積の定義をもっと一般化することができる。単項関数の積を

$$u_g x_g \cdot u_h y_h = u_{gh} x_g^{\sigma(h)} y_h$$

の代りに

$$u_g x_g \cdot u_h y_h = u_{gh} a_{g,h} x_g^{\sigma(h)} y_h$$

と定めても，積の結合律が成り立つ。実際

$$(u_g x_g \cdot u_h y_h)\cdot u_k z_k = (u_{gh} a_{g,h} x_g^{\sigma(h)} y_h)\cdot u_k z_k$$

$$= u_{ghk} a_{gh,k} (a_{g,h} x_g^{\sigma(h)} y_h)^{\sigma(k)} z_k$$

$$= u_{ghk} a_{gh,k} a_{g,h}^{\sigma(k)} x_g^{\sigma(hk)} y_h^{\sigma(k)} z_k,$$

$$u_g x_g \cdot (u_h y_h \cdot u_k z_k) = u_g x_g \cdot u_{hk} a_{h,k} y_h^{\sigma(k)} z_k$$

$$= u_{ghk} a_{g,hk} a_{h,k} x_g^{\sigma(hk)} y_h^{\sigma(k)} z_k$$

この単項関数の積を基にして，G上のσ値関数の積を定義すると，このような関数の全体は線形環となる。これを因子団$\{ a_{g.h} \}$についてのσのGによる接合積という。いうまでもなく$a_{g.h}=1$のときが本文の場合である。

以下この論文では因子団をもつ場合の接合積には言及しない。接合積については文献〔5〕，〔6〕，〔7〕参照のこと。

5　整数加群による接合積

Gが無限群のときには，線形環がトポロジーをもつ位相環でない限り，前節（＊＊＊）の無限和 $\sum_h x_{g\,k-1}^{\sigma(h)} y_h$ に意味をもたせることができず，したがって前節の定義のままで接合積$G\otimes_\sigma \sigma$をつくることはできない。しかし$G=\boldsymbol{Z}$（整数の加群）の場合には拡大環を構成する元にわずかの制限を課すことによって無限和を有限和に変え，有限群の場合ほとんどそのままに接合積を定義することができる。$\mathfrak{F}_\sigma(\boldsymbol{Z})$は群$\boldsymbol{Z}$上で定義され，線形環$\sigma$に値をとる関数$\sum_{n=-\infty}^{\infty} u_n x_n$の全体とし，$\mathfrak{F}_\sigma^o(\boldsymbol{Z})$は$\mathfrak{F}_\sigma(\boldsymbol{Z})$の関数のなかで条件

$$\exists n_o : n < n_o \longrightarrow x_n = 0$$

を満たすものの全体とする。$\mathfrak{F}_\sigma^o(\boldsymbol{Z})$の関数を$\sum_{n=n_o}^{\infty} u_n x_n$で表わす。$\mathfrak{F}_\sigma(\boldsymbol{Z})$が体$\boldsymbol{F}$上の線形空間となり，$\mathfrak{F}_\sigma^o(\boldsymbol{Z})$がその部分空間となることは前節とまったく同様であり，単項関数$u_g x_g$と$u_h y_h$の積も前節と同様に定義する。このとき$\mathfrak{F}_\sigma^o(\boldsymbol{Z})$に属する関数には前節（＊＊＊）によって積が定義できる。なぜなら

$$\sum_{n=n_0}^{\infty} u_n x_n,\quad \sum_{n=m_0}^{\infty} u_n y_n \in \mathfrak{F}_\sigma^0(\boldsymbol{Z})$$

に対して（＊＊＊）の項$x_{n-m}^{\sigma(m)} y_m$は$m_o \leqq m \leqq n-n_o$をを満たすmでだけ非零となりうるので

（無限和）$\sum_{m=-\infty}^{\infty} x_{n-m}^{\sigma(m)} y_m =$

$$\begin{cases} 0 & (n < n_0+m_0) \\ \text{（有限和）} \sum_{m=m_0}^{n-n_0} x_{n-m}^{\sigma(m)} y_m & (n \geqq n_0+m_0) \end{cases}$$

となり，積の定義式が意味をもち，$\sum_{n=n_o}^{\infty} u_n x_n \cdot \sum_{n=m_o}^{\infty} u_n y_n$は$\mathfrak{F}_\sigma^o(\boldsymbol{Z})$に属する。

このように積の定義された線形環$\mathfrak{F}_\sigma^o(\boldsymbol{Z})$を$\sigma$の$\boldsymbol{Z}$による接合積と呼び，$\boldsymbol{Z}\otimes_\sigma \sigma$で表わす。単項関数$u_o x_o$（$x_o \in \sigma$）の全体は$\sigma$と同型な$\boldsymbol{Z}\otimes_\sigma \sigma$の部分環となるから，$\boldsymbol{Z}\otimes_\sigma \sigma$は$\sigma$の拡大環である。

6　剰余多項式環$\boldsymbol{F}_n[X]$の自己同型写像

$\boldsymbol{F}_n[X]$はn次多項式X^n-1を法とする体$\boldsymbol{F}$上の剰余多項式環とする。$\boldsymbol{F}_n[X]$の元は次数$n-1$以下の多項式

$$x = a_0 X^{n-1} + a_1 X^{n-2} + \cdots + a_{n-1} \quad (a_i \in \boldsymbol{F})$$

である。πはnより小さい正整数とし，σは$\boldsymbol{F}_n[X]$より自分自身の中への写像

$$\sigma:\ x = a_0 X^{n-1} + a_1 X^{n-2} + \cdots + a_{n-1} \longrightarrow$$

$$x^\sigma = a_0 X^{(n-1)\pi} + \cdots + a_{n-1}$$

とすると

$$(x+y)^\sigma = x^\sigma + y^\sigma,\ (ax)^\sigma = ax^\sigma \quad (a \in \boldsymbol{F}),$$

$$(xy)^\sigma = x^\sigma y^\sigma$$

が成り立ち，σは準同型写像である。特に

補題　πとnが素のときかつそのときにのみσは$\boldsymbol{F}_n[X]$の自己同型写像である。

証明　$(\pi, n)=1$のとき整数r，sが存在して，$r\pi + sn = 1$となる。したがって$r\pi \equiv 1 \pmod{n}$，rはmod nでπの逆数となる。そこで正整数tに対して$t\pi \equiv 0 \pmod{n}$であれば$t \equiv 0 \pmod{n}$となる。

いま$o \leqq p$，$q \leqq n-1$に対して

$$X^{p\pi} \equiv X^{q\pi} \pmod{X^n - 1}$$

とすると，$(p-q)\pi \equiv 0 \pmod{n}$より$p=q$となる。したがって$p \gtrless q$のとき

$$X^{p\pi} \equiv X^{q\pi} \quad (\mathrm{mod}.\ X^n-1)$$

これはσが多項式xの係数の置換を惹き起すことを意味するから，σは1：1写像で，$\boldsymbol{F}_n[X]$の自己同型写像となる。逆にσが自己同型写像のときには$r\pi \equiv 1$（mod.n）となるrが存在するから$(\pi, n)=1$である。

σを上述のような整数πによって定義された線形環$\boldsymbol{F}_n[X]$の自己同型写像とすると，写像

$$\sigma:\ \text{整数}\ j \ \longrightarrow\ \sigma(j)=\sigma^j$$

は整数加群$\boldsymbol{Z}$から，群Aut（$\boldsymbol{F}_n[X]$）の中の，σを生成元とする巡回部分群への準同型写像となる。したがってこの準同型写像によって接合積$\boldsymbol{Z}\otimes_\sigma \boldsymbol{F}_n[X]$をつくることができる。Piretの巡回コードの記号と一致させるため$\boldsymbol{Z}\otimes_\sigma \boldsymbol{F}_n[X]$の単項関数を$u_n v_n(X)$の代りに$D^n v_n(X)$と表わすことにすると$\boldsymbol{Z}\otimes_\sigma \boldsymbol{F}_n[X]$の一般の元は$\sum_{j=n_0}^{\infty} D^j v_j(X)$と表わされ，これに単項関数$D^0X$を左乗すると

$$D^0X\cdot\sum_{j=n_0}^{\infty} D^j v_j(X)=\sum_{j=n_0}^{\infty} D^j X^{\sigma^j} v_j(X)$$
$$=\sum_{j=n_0}^{\infty} D^j X^{\pi^j} v_j(X)$$

となる。これはPiretが定義した巡回性にほかならない。また

$$\sum_{j=n_0}^{\infty} D^j v_j(X)\in \boldsymbol{C}(D) \ \longrightarrow$$
$$D\cdot\sum_{j=n_0}^{\infty} D^j v_j(X)=\sum_{j=n_0}^{\infty} D^{j+1} v_j(X)\in \boldsymbol{C}(D)$$

だから，$\boldsymbol{C}$（D）の元に$\boldsymbol{Z}\otimes_\sigma \boldsymbol{F}_n[X]$の任意の元を左剰すると，その積もまた$\boldsymbol{C}$（$D$）に属する。このことはPiretの巡回たたみ込み符号のコード単語列の全体$\boldsymbol{C}$（D）が接合積$\boldsymbol{Z}\otimes_\sigma \boldsymbol{F}_n[X]$の左イデアルであることを意味する。

7　正規たたみ込み符号

剰余多項式環$\boldsymbol{F}_n[X]$の2元の積は

$$\left(\sum_{i=0}^{n-1} a_i X^{n-i}\right)\cdot\left(\sum_{i=0}^{n-1} b_i X^{n-i}\right)=\sum_{i=0}^{n-1}\left(\sum_{k=0}^{n-1} a_k b_{i-k}\right)X^i$$

である。ここで係数a_i，b_jの添字i，jについての計算は常にnを法として行なわれるから，上式を位数nの巡回群，すなわちnを法とする整数の加群$\boldsymbol{Z}_n=\{0, 1, \cdots, n-1\}$で定義された関数についての積と解釈することができる。この見地より剰余多項式環$\boldsymbol{F}_n[X]$の構成は一般の有限群に対して以下のように一般化される。

Gは有限群とし，Gの元gで$a_g\in \boldsymbol{F}$を値にとる単項関数を$a_g X_g$，G上で定義され$\boldsymbol{F}$に値をとる一般の関数を単項関数の和$\Sigma_g a_g X_g$と表わすことにする。

$$x=\sum_g a_g X_g,\ y=\sum_g b_g X_g,\quad c\in \boldsymbol{F}$$

に対して，和，スカラー倍，積を

$$x+y=\sum_g (a_g+b_g)X_g,\ cx=\sum_g (ca_g)X_g,$$
$$x\cdot y=\sum_g\left(\sum_h a_h b_{gh^{-1}}\right)X_g$$

と定めると，$\boldsymbol{F}_n$（X）の場合と同様に，このような関数の集合$\mathfrak{F}_F(G)$は線形環となる。この線形環を群Gの群環という。群環は接合積の特別な場合，すなわち$\sigma=\boldsymbol{F}$，$\sigma(g)=\iota$の場合と見ることができる。

$\boldsymbol{F}_n[X]$の場合πをnと素な整数とし，

$$\sigma:\quad k \longrightarrow k\pi$$

によって群$\boldsymbol{Z}_n$の元の変換を定義すると，k，$h\in \boldsymbol{Z}_n$に対して

$$\sigma(k+h)=(k+h)\pi=k\pi+k\pi=\sigma(k)+\sigma(h)$$
$$k\neq h \longrightarrow \sigma(k)\neq\sigma(h)$$

が成り立ち，σは群$\boldsymbol{Z}_n$の自己同型置換となる。群$\boldsymbol{Z}_n$の自己同型置換σは前節で述べたように

$$\sigma:\ x=\sum_{i=0}^{n-1} a_i X^i \ \longrightarrow$$
$$x^\sigma=\sum_{i=0}^{n-1} a_i X^{\sigma(i)}=\sum_{i=0}^{n-1} a_i X^{i\pi}$$

によって群環$\boldsymbol{F}_n[X]$の自己同型写像にまで拡大される。この事実は一般の有限群Gの場合にもまったく同様である。σをGの自己同型置換とすると$\sigma(g\cdot h)=\sigma(g)\cdot\sigma(h)$を満たし，$\sigma^{-1}$が存在してこれも$G$の自己同型置換となる。このことから$\sigma$による群環$\mathfrak{F}_F(G)$の元の変換

$$x=\sum_g a_g X_g \ \longrightarrow\ x^\sigma=\sum_g a_g X_{\sigma(g)}$$

は群環の自己同型写像となる。実際Gでは逆置換σ^{-1}が存在するから，$\mathfrak{F}_F(G)$の変換σは1：1,写像であり，条件$(x\cdot y)^\sigma=x^\sigma\cdot y^\sigma$はつぎのように確められる。

$$x^{\sigma}\cdot y^{\sigma}=\sum_{g}a_{g}X_{\sigma(g)}\cdot\sum_{g}b_{g}X_{\sigma(g)}$$
$$=\sum_{g}a_{\sigma^{-1}(g)}X_{g}\cdot\sum_{g}b_{\sigma^{-1}(g)}X_{g}$$
$$=\sum_{g}(\sum_{h}a_{\sigma^{-1}(h)}b_{\sigma^{-1}(g)\sigma^{-1}(h^{-1})})X_{g}$$
$$=\sum_{g}\sum_{h}a_{h}b_{\sigma^{-1}(g)h^{-1}}X_{g}$$
$$=\sum_{g}(\sum_{h}a_{h}b_{gh^{-1}})X_{\sigma(g)}=(x\cdot y)^{\sigma}$$

群環の自己同型写像σが与えられると，$\sigma(i)=\sigma^{i}$として整数加群$\boldsymbol{Z}$から自己同型群Aut($\mathfrak{F}_{F}(G)$)への準同型写像が定義できるから，接合積$\boldsymbol{Z}\otimes_{\sigma}\mathfrak{F}_{F}(G)$がつくれる。コード単語列がこの接合積環のイデアルとなるたたみ込み符号は巡回たたみ込み符号の一般化となる。Delsarte－Piret〔3〕が正規たたみ込み符号と名づけたものはこのように構成された符号とちょうど一致する。

引　用　文　献

[1] Forney, G.D., Convolutional codes I : Algebraic structure *IEEE TRANS. Information Theory IT-16 (1970) 720-738*

[2] Piret, P., Structure and constructions of cyclic convolutional codes, *IEEE Trans. Information Theory IT-22 (1976) 147-155*

[3] Delsarte, P. -Piret, P., Semiregular convolutional codes : Definition, structure and examples, *Information and Control 33 (1977) 56-71*

[4] Piret, P., On a class of alternating cyclic convolutional codes, *IEEE Trans. Information Theory IT-21 (1975) 64-69*

[5] Artin, E. -Nesbitt, C. -Thrall, R., Rings with minimum condition, *Univ. of Michigan Press (1944)*

[6] Jacobson, N., Structure of rings, *American Mathematical Scoiety (1956)*

[7] 東屋五郎，単純環の理論，河出書房（1951）