数理解析研究所講究録
第82巻 1970年 52-62

ガロア拡大体の工学的一応用について

大阪府大　工学部　　田中　初一

§1. 序

データ伝送における誤り制御のために，誤り訂正符号が用いられる．能力の高い複雑な機構を有する誤り訂正符号の構成に際して，ガロア拡大体の理論が用いられている．独立な多重の誤りを訂正できるBose-Chaudhuri-Hocquenghem符号は，この一例である．ガロア拡大体の理論を適用した符号は，訂正能力の点では，きわめてすぐれているが，一般に構成が複雑で，実用化に乏しい．しかし，近い将来において，貴重なデータを伝送するために，信頼性の高いデータ伝送システムが必要となるであろうから，複雑な機構を有する能力の高い符号を容易に実用化のできる方向へ努力することが要求される．

筆者らは，ガロア拡大体の理論を用いて構成される，きわめてすぐれた能力を有する符号が，その復号化の複雑さのゆ

えに実用性を欠乏していることに着眼し，ガロア拡大体の上の演算を，シフトレジスタを用いて容易に行なうことを目的とし，そのシフトレジスタの結線を数学的に決定する理論を明らかにしている．

§2. ガロア拡大体

理論の展開において適用する代数系は，標数2の基礎体，GF(2)の上のm次拡大体である．基礎体の要素を0および1で示し，要素間の演算を表1に示す．

表1. GF(2)の演算

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

つぎに，GF(2)の上のm次原始多項式を$f(X)$とし，$f(X)=0$の一つの原始根をαとおく．αをGF(2)に付加することにより，ガロア拡大体$GF(2^m)$が構成される．

一例として，GF(2)の上の4次の原

表2. $GF(2^4)$ $(\alpha^4+\alpha+1=0)$

$0=0$	(0000)	} GF(2)
$\alpha^0=1$	(1000)	
$\alpha^1=\alpha$	(0100)	
$\alpha^2=\alpha^2$	(0010)	
$\alpha^3=\alpha^3$	(0001)	
$\alpha^4=1+\alpha$	(1100)	
$\alpha^5=\alpha+\alpha^2$	(0110)	
$\alpha^6=\alpha^2+\alpha^3$	(0011)	
$\alpha^7=1+\alpha+\alpha^3$	(1101)	} $GF(2^4)$
$\alpha^8=1+\alpha^2$	(1010)	
$\alpha^9=\alpha+\alpha^3$	(0101)	
$\alpha^{10}=1+\alpha+\alpha^2$	(1110)	
$\alpha^{11}=\alpha+\alpha^2+\alpha^3$	(0111)	
$\alpha^{12}=1+\alpha+\alpha^2+\alpha^3$	(1111)	
$\alpha^{13}=1+\alpha^2+\alpha^3$	(1011)	
$\alpha^{14}=1+\alpha^3$	(1001)	

始多項式, $f(X)=1+X+X^4$ を用いると, 表2に示すような GF(24) を構成できる. 以下の理論の展開において, この拡大体 GF(24) を簡単な実例として利用する.

§3. 結線行列

3.1 定義

基礎体 GF(2) の上の m 次原始多項式を

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots\cdots + a_{m-1}X^{m-1} + X^m \quad (1)$$

$$a_i \ (0 \leqq i \leqq m-1) \in GF(2)$$

とする. $f(X)$ の係数 a_i を要素として含む, つぎに示す m 行 m 列の行列を F 行列と定義する。

$$F = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots\cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots\cdots & 0 \\ \vdots & & & & & \vdots \\ & & & & & 0 \\ 0 & 0 & \cdots\cdots & & 0 & 1 \\ a_0 & a_1 & \cdots\cdots & & & a_{m-1} \end{bmatrix} \quad (2)$$

3.2 F行列の諸性質

行列 F の特性多項式 $h(\lambda)$ は次式で与えられる.

$$h(\lambda) = |\lambda E - F| . \quad (3)$$

ここに, E は m 行 m 列の単位行列である. $h(\lambda)$ に関し, 次の補題が成立する.

補題1. $h(\lambda) = f(\lambda)$. (4)

証明： つぎに示すような行列 Λ を導入する.

$$\Lambda = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ \lambda & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \lambda^{m-1} & \lambda^{m-2} & \cdots & \lambda & 1 \end{bmatrix} \qquad |\Lambda| = 1. \tag{5}$$

$(\lambda E - F)$ に Λ を乗ずることにより，次式を得る.

$$\begin{bmatrix} \lambda & -1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda & -1 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & \lambda & -1 \\ -a_0 & -a_1 & \cdots & \cdots & & (\lambda - a_{m-1}) \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ \lambda & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \lambda^{m-1} & \cdots & & \lambda & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ f_0 & f_1 & \cdots & \cdots & f_{m-1} \end{bmatrix}. \tag{6}$$

ここで f_i $(0 \leqq i \leqq m-1)$ は λ の多項式であり，時に，

$$f_0(\lambda) = -a_0 - a_1\lambda - \cdots - a_{m-1}\lambda^{m-1} + \lambda^m$$

となる．さらに，GF(2) の上で考えているので，$f_0(\lambda) = f(\lambda)$ である．式(5)および(6)を用いて，

$$h(\lambda) = |\lambda E - F| = |\lambda E - F||\Lambda| = |(\lambda E - F)\Lambda| = f_0(\lambda) = f(\lambda).$$

Q.E.D.

つぎに，二つの行列 F_1 と F_2 との和を，F_1 と F_2 との対応する要素間の mod 2 加算と定義し，$F_1 \oplus F_2$ で示す．この時，次の補題が成立する.

補題2. $f(F) = 0$. (7)

証明： 補題1より，

$f(F)=h(F)=|FE-F|=|F-F|=0$. Q.E.D.

基礎体 GF(2)の上の変数Fの多項式を考える． $f(X)$ が原始的で $f(\alpha)=0$ であり，補題2より $f(F)=0$ であることから，つぎの補題3が得られる．

補題3． $f(F)$ を法とする GF(2) の上のFの多項式より構成される多元環 $\Omega(F)$ は，$GF(2^m)$ と同型である．

$GF(2^m)$ のすべての要素が，$\alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{m-1}$ の線型結合により表現できて，かつ $\Omega(F)$ が $GF(2^m)$ に同型であるので，つぎの補題4が得られる．

補題4． F^n は $F^0=E, F^1, F^2, \cdots, F^{m-1}$ の線型結合として表現され，F^n を $f(F)$ で割り算を行ない，その剰余として与えられる．

3.3 F行列とシフトレジスタとの対応

行列Fおよびそのべき乗は，0または1のみを要素として含むから，1を結線ありと考え，0を結線なしと考えると，F行列とシフトレジスタとの1対1の対応づけが可能である．すなわち，行列の第 i 行第 j 列の要素1は，第 i 番目のフリップ・フロップの出力端子から，第 j 番目のフリップ・フロップの入力端子に結線されていると考える．このような対応の下に，行列Fおよびそのべき乗は，それに対応するシフト

レジスタの結線行列となる．たとえば，§2の例として用いた多項式 $f(X)=1+X+X^4$ に対応する行列は，式(8)に示すようになり，対応するシフトレジスタは，図1のようになる．

$$F=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&1&0&0\end{bmatrix} \quad (8)$$

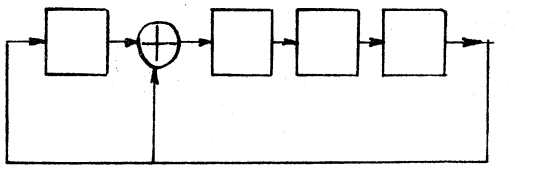

図1.式(8)のF行列に対応するフィードバック・シフトレジスタ

§4. 積演算回路

ガロア拡大体 $GF(2^m)$ の要素間の積の回路は，符号理論の見地から興味がある．この節では，$GF(2^m)$ の上の積演算回路をシフトレジスタで構成する場合の結線決定方法についてのべる．

[定理1] $\alpha^i\cdot\alpha^j=\alpha^{i+j}$ ($\alpha^i, \alpha^j, \alpha^{i+j}\in GF(2^m)$) なる演算は，初期状態が α^i で結線行列が F^j であるシフトレジスタを1回シフトすることにより実行される．ただし，

$$F^j=g_0E\oplus g_1F\oplus g_2F^2\oplus\cdots\oplus g_{m-1}F^{m-1} \quad (9)$$

であり，g_i ($0\leqq i\leqq m-1$) は，α^j を $\alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{m-1}$ の線型結合として表示した場合の結合係数である．

上述の定理は，補題1～4を考察し，$GF(2^m)$ の任意の要

素を，α^n 倍するシフトレジスタの結線行列が F^n で与えられることより明らかとなる．

一例として，§2 でのべたガロア拡大体 $GF(2^4)$ の上で，α^3 を α^5 倍する回路の結線を決定する．補題3および補題4と表2より，$F^5 = F \oplus F^2$ である．ここで，

$$F = \begin{bmatrix} 0100 \\ 0010 \\ 0001 \\ 1100 \end{bmatrix}, \quad F^2 = \begin{bmatrix} 0010 \\ 0001 \\ 1100 \\ 0110 \end{bmatrix}$$

であるから，F^5 は

$$F^5 = \begin{bmatrix} 0100 \\ 0010 \\ 0001 \\ 1100 \end{bmatrix} \oplus \begin{bmatrix} 0010 \\ 0001 \\ 1100 \\ 0110 \end{bmatrix} = \begin{bmatrix} 0110 \\ 0011 \\ 1101 \\ 1010 \end{bmatrix}$$

と決定される．F^5 に対応するシフトレジスタを図2に示す．

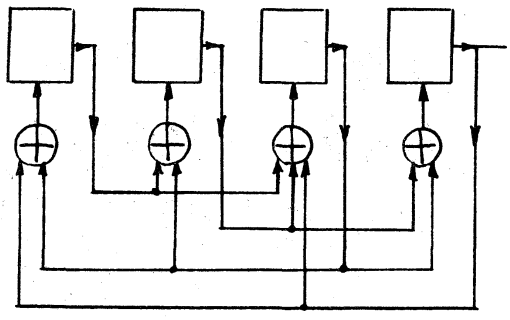

図2．F^5 に対応するシフトレジスタ

このシフトレジスタの初期値を $\alpha^3 = (0001)$ とおき，1回シフトすると，

$$(0001)\begin{bmatrix} 0110 \\ 0011 \\ 1101 \\ 1010 \end{bmatrix} = (1010)$$

となり，$(1010) = \alpha^8$ であるから，$\alpha^3 \cdot \alpha^5 = \alpha^8$ なる演算が実行されることがわかる．

§5. べき乗演算回路

ガロア拡大体 $GF(2^m)$ の要素をべき乗するためのシフトレジスタの結線は，つぎの定理を適用することにより決定される．

［定理2］ $GF(2^m)$ の任意の要素 α^i を n 乗する回路は，結線行列が次式で与えられるフィードバック・シフトレジスタとして決定される．

$$(F^{n-1})^i = (g_0 E \oplus g_1 F \oplus \cdots \oplus g_{m-1} F^{m-1})^{n-1} \quad (10)$$

ただし，g_i $(0 \leq i \leq m-1)$ は，$\alpha^0, \alpha^1, \cdots, \alpha^{m-1}$ の線型結合として α^i を表示したときの係数により決定される．

証明： 定理1により，

$$\alpha^i (F^{n-1})^i = \alpha^i F^{(n-1)i} = \alpha^i \cdot \alpha^{(n-1)i} = \alpha^{ni} = (\alpha^i)^n.$$

Q.E.D.

系： $n = 2^p + 1$ のとき，結線行列 (10) は

$$(F^{n-1})^i = (F^{2^p})^i = g_0 E \oplus g_1 F^{2^p} \oplus \cdots \oplus g_{m-1} F^{2^p(m-1)} \quad (11)$$

で与えられる．ただし，p は正の整数である．

上の定理2で決定される演算回路で，$GF(2^m)$ の要素は，1ビットタイムで n 乗される．しかし，シフトレジスタの構成に際して，べき乗される要素とべき数の両方に依存することに注意する必要がある．

一例として，前述の $GF(2^4)$ の上で α^4 を6乗する回路は，

つぎのようにして決定される．定理2により結線行列は，

$$(F^{6-1})^4 = (F^5)^4 = F^{20} = F^5 = F \oplus F^2$$

で与えられる．この結線行列に対応するシフトレジスタは，すでに図2で示したものと同じである．レジスタの初期値として，$\alpha^4 = (1100)$を代入し，1回シフトすると．

$$(1100)\begin{bmatrix} 0110 \\ 0011 \\ 1101 \\ 1010 \end{bmatrix} = (0101)$$

となり，$(0101) = \alpha^9$であるから，$(\alpha^4)^6 = \alpha^{24} = \alpha^9$の演算が実行されたことを検証できる．

§6. 応用例

[例題] GF(2^4) の上の多項式

$$G(X) = \alpha^2 + \alpha^8 X + X^3 \qquad (12)$$

に対応するフィードバック・シフトレジスタを，2値のフリップ・フロップとmod 2 加算器で構成せよ．

[解] GF(2^4)の上のフリップ・フロップは，2値のフリップ・フロップを4個1組として構成する．同様に，mod 2 加算器を4個並列に並べて，GF(2^4) の上の加算器を構成できる．最後にGF(2^4)の要素を，α^2およびα^8倍する乗算器は，定理1を適用することにより得られた結線行列をmod 2 加算器

で構成することにより得られる．式(12)に対応するフィードバック・シフトレジスタを図3に示す．

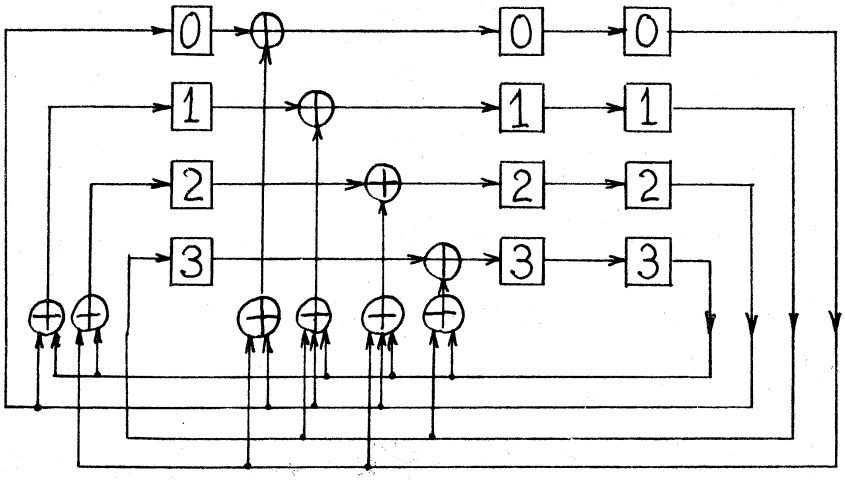

図3．$G(X)=\alpha^2+\alpha^8X+X^3$ に対応する
フィードバック・シフトレジスタ

§7．結言

ガロア拡大体の上の演算を行なう回路を，シフトレジスタで構成する場合，その結線を理論的に決定する方法を明らかにした．この理論によれば，ガロア拡大体の上の積演算およびべき乗演算を行なう回路を，シフトレジスタにより簡単に構成でき，Bose-Chaudhuri-Hocquenghem 符号および Reed-Solomon 符号等の復号化回路として，きわめて有効に利用できる．

謝辞　本研究において有益な御教示をいただいた、大阪大学工学部の笠原芳郎教授、手塚慶一助教授，笠原正雄助手ならびに京都大学数理工学教室の長谷川利治助教授に、厚くお礼を申し上げる．

参考文献

(1) W.W.Peterson, "Error Correcting Codes", MIT Press. Cambridge Massachusetts, (1961).
(2) S.W.Golomb, "Digital Communications", Prentice Hall, Englewood Cliffs, New Jersey, (1964).
(3) B.Elspas, "The theory of autonomous linear sequential networks", I.R.E. Trans. Comm. Theory 6, 45-60, (1965).
(4) M.Postonikov, 日野寛三訳, "ガロアの理論", (1964, 東京図書).
(5) 遠山啓, "行列論" (1965, 共立出版).