BCH 符号と RS 符号 (I)

正会員 金子敏信*

1. ま え が き

今回と次の2回にわたり、応用上重要な符号である BCH 符号と RS 符号(リードソロモン符号)を紹介する。これらは、ガロア体上の多項式の根の性質を使って構成される。2章では、数学的準備として、多項式と根の関係を述べ符号の根の考え方を紹介する。これをもとに3章で、2重誤り訂正 BCH 符号を導く。さらに次回に一般の BCH 符号、その特別な場合として RS 符号を説明する。

2. 多項式の根と符号の根

前回の5章において巡回ハミング符号の復号法を説明した。復号の際に使用するシンドロームは、受信多項式を $Y(x)$ として、

$$s = Y(\alpha) \quad (1)$$

である。この α は、ハミング符号の生成多項式として使用した原始多項式の根である。

このように巡回符号の復号の際に、生成多項式の根が重要な役割を果たす。今回の議論の数学的準備として、ガロア体 $GF(2)$ 上の多項式の根についていくつかの性質を述べよう*。

2.1 1 の n 乗根

最初に $GF(2^m)$ の元の性質といくつかの用語を説明する。表1に $GF(2^4)$ の16個の元を示す。以下、具体例として、この表を使うことにする。

〈位 数〉

$GF(2^m)$ の任意の元 $a(a \neq 0)$ を $a^1, a^2, \dots$ と順次べき

表1 $GF(2^4)$ の元 (mod $a^4 + a + 1$)

べき表示	ベクトル表示				べき表示	ベクトル表示			
	a^3	a^2	a	1		a^3	a^2	a	1
0	0	0	0	0	a^7	1	0	1	1
$a^0=1$	0	0	0	1	a^8	0	1	0	1
a	0	0	1	0	a^9	1	0	1	0
a^2	0	1	0	0	a^{10}	0	1	1	1
a^3	1	0	0	0	a^{11}	1	1	1	0
a^4	0	0	1	1	a^{12}	1	1	1	1
a^5	0	1	1	0	a^{13}	1	1	0	1
a^6	1	1	0	0	a^{14}	1	0	0	1

乗して、 n 乗で初めて $a^n=1$ となったとき n を a の“位数”(order)という。

(例 1. a)

表1の α は原始元であるから、当然、位数は $2^4-1=15$ (第4回5章)である。 $a=a^3$ は、 $a^2=a^6, a^3=a^9=1, a^4=a^{12}, a^5=a^{15}=1$ であるので a^3 の位数は5である。

〈1 の n 乗根〉

位数が n の元 a は $a^n=1$ であるから、多項式 $F(x)=x^n-1$ とすれば、

$$F(a)=a^n-1=0 \quad (2)$$

であり $F(x)$ の根である。 x^n-1 の根であるから、この a を“1 の n 乗根”という。

(例 1. b)

a^3 の位数は5である。したがって a^3 は x^5-1 の根であり、1の5乗根である。

〈 $GF(2^m)$ の元〉

$GF(2^4)$ の零以外の任意の元 $a=a^i \neq 0$ は、15 乗すると1となる。

$$a^{15}=(a^i)^{15}=(a^{15})^i=(1)^i=1 \quad (3)$$

したがって、 $F(x)=x^{15}-1$ とすれば、

$$F(a)=a^{15}-1=1-1=0 \quad (4)$$

であり、 a は $x^{15}-1$ の根となる。よって、 $GF(2^4)$ の

* 東京理科大学 理工学部

“Introduction to Coding Theory (6); BCH Code and RS Code (I)” by Toshinobu Kaneko (Faculty of Engineering, Science University of Tokyo, Noda)

* 一般のガロア体 $GF(q)$ 上の多項式に関し、ここに述べるのと同種の性質が成り立つ。詳しく知りたい読者は、第4回の参考文献参照のこと。

零以外の元 a は 1 の 15 乗根である。いい替えれば、1 の 15 乗根は、 $a^0=1, a^1, a^2, \dots, a^{14}$ の 15 個である。一般に $GF(2^m)$ の零以外の 2^m-1 個の元は 1 の (2^m-1) 乗根である。

2.2 共役根

$GF(2)$ 上の多項式の 2 乗を考えてみよう。例えば $F(x)=f_2x^2+f_1x+f_0$ を 2 乗すれば、

$$\begin{aligned} (F(x))^2 &= (f_2x^2+f_1x+f_0)^2 \\ &= f_2^2x^4+f_1^2x^2+f_0^2 \\ &\quad + 2(f_2f_1x^3+f_2f_0x^2+f_1f_0x) \end{aligned} \quad (5)$$

である。各項の 2 乗と、 $2 * (2 \text{ つの項の積})$ の和となる。しかし、多項式の係数は $GF(2)$ で計算されるので $(2=0 \bmod 2)$ であるから第 2 項は 0 である。また、 f_2, f_1, f_0 は $GF(2)$ の元であるから 0 または 1 であり、 $f_2^2=f_2, f_1^2=f_1, f_0^2=f_0$ となるので、結局、

$$\begin{aligned} (F(x))^2 &= f_2x^4+f_1x^2+f_0 \\ \therefore (F(x))^2 &= F(x^2) \end{aligned} \quad (6)$$

となる。この関係は $GF(2)$ 上の任意の多項式 $F(x)$ に対して成立する。したがって、 a が $F(x)$ の根であれば、 $F(a)=0$ であるから、

$$\therefore (F(a))^2 = F(a^2) = 0 \quad (7)$$

となるので a^2 も根である。これをさらに繰り返せば、 $a^{2^2}, a^{2^3}, \dots, a^{2^{d-1}}$ も根であることがいえる。ただし d は $a^{2^d}=a$ となる最小の正整数である。このような根 $\{a, a^2, a^{2^2}, \dots, a^{2^{d-1}}\}$ を a の“共役根” (conjugate root) という。

(例 2.a)

表 1 の原始元 a の共役根を求めよう。原始元であるから $a^{15}=1$ である。順次 2 乗を繰り返せば $a, a^2, a^4, a^8, a^{16}=a$ となるから、共役根は $\{a, a^2, a^4, a^8\}$ の 4 つである。したがって原始多項式

$$F(x)=x^4+x+1 \quad (8)$$

は、この 4 つの根を持つ。例えば、 a^8 が $F(x)$ の根であることを、表 1 のベクトル表示で確認しよう。

$$\begin{aligned} F(a^8) &= (a^8)^4 + a^8 + 1 \\ &= a^{32} + a^8 + 1 \\ &= a^2 + a^8 + 1 \quad (\because a^{15}=1) \\ &= (0100) + (0101) + (0001) \\ &= (0000) = 0 \end{aligned} \quad (9)$$

(例 2.b)

元 a^3 の共役根を求めてみる。

$$\begin{aligned} a^3, (a^3)^2 &= a^6, (a^3)^{2^2} = a^{12}, \\ (a^3)^{2^3} &= a^{24} = a^9, (a^3)^{2^4} = a^{48} = a^3 \end{aligned} \quad (10)$$

であるから

$$\{a^3, a^6, a^{12}, a^9\} \quad (11)$$

の 4 つが a^3 の共役根である。

2.3 最小多項式

表 1 に示されている 16 個の $GF(2^4)$ の元のうち $1=a^0$ は多項式

$$M_0(x)=x+1 \quad (12)$$

の根であり、 $\{a^1, a^2, a^4, a^8\}$ は、例 2.a のように原始多項式

$$M_1(x)=x^4+x+1 \quad (13)$$

の根である。残りはどのような $GF(2)$ 上の多項式の根であろうか。 a^3 を根とする多項式は、(11) 式の共役根を持つ。そこで、

$$M_3(x)=(x-a^3)(x-a^6)(x-a^{12})(x-a^9) \quad (14)$$

なる多項式を考えよう。この式を展開し、 $a^{15}=1$ に注意しながら表 1 を使って整理すると、 $GF(2)$ 上の多項式

$$M_3(x)=x^4+x^3+x^2+x+1 \quad (15)$$

が得られる。 a^3 を根に持つ $GF(2)$ 上の多項式は、(11) 式の共役根を持たねばならないことから、この式は a^3 を根に持つ $GF(2)$ 上の多項式のうちで次数が最小のものである。そこで、この式を a^3 の最小多項式と呼ぶ。

[定義] 最小多項式

$GF(2^m)$ の任意の元 a が与えられたとき、それを根に持つ $GF(2)$ 上の多項式で次数が最小のものを a の $GF(2)$ 上の“最小多項式” (minimal polynomial) という。

a^3 の最小多項式を求めたのと同じ方法で、任意の元 a の $GF(2)$ 上の最小多項式が求められる。すなわち、 a の共役根

$$\{a, a^2, a^{2^2}, \dots, a^{2^{d-1}}\} \quad (16)$$

を求めれば、これより a の最小多項式 $M(x)$ は、

$$M(x)=(x-a)(x-a^2)\cdots(x-a^{2^{d-1}}) \quad (17)$$

で与えられる。

$GF(2^4)$ のすべての元の最小多項式を表 2 に示す。

<最小多項式の性質>

$GF(2^m)$ の任意の元 $a=a^i$ の $GF(2)$ 上の最小多項式 $M_i(x)$ に対し次の性質 (1)~(5) が成り立つ。証

表 2 $GF(2^4)$ の元の最小多項式 (a は x^4+x+1 の根)

$GF(2^4)$ の元 (共役根)	最小多項式 $M(x)$	位数
0	x	—
1	$x+1$	1
a, a^2, a^4, a^8	x^4+x+1	15
a^3, a^6, a^{12}, a^9	$x^4+x^3+x^2+x+1$	5
a^5, a^{10}	x^2+x+1	3
$a^7, a^{14}, a^{13}, a^{11}$	x^4+x^3+1	15

明は付録に述べるが、ここでは表2を例として性質を確認する。

- (1) $M_i(x)$ は既約多項式である。
 (2) $GF(2)$ 上の多項式 $F(x)$ が $F(a)=0$ であれば、 $F(x)$ は、 $M_i(x)$ で割り切れる。

例えば、 $F(x)=x^2+1$ は $F(1)=0$ であり、 $x^2+1=(x+1)^2$ であるので、確かに $M_0(x)=(x+1)$ で割り切れる。

- (3) a の位数を n とすると、 $M_i(x)$ は多項式 x^n-1 を割り切る。この n は $M_i(x)$ で割り切れる多項式 x^n-1 における、最小の n である。この n を $M_i(x)$ の位数という。

例えば、 $GF(2^4)$ の元 $a=a^5$ とする。 $a^2=a^{10}$, $a^3=a^{15}=1$, であるから、 a^5 の位数は3である。最小多項式 $M_5(x)=x^2+x+1$ は $x^3-1=(x+1)(x^2+x+1)$ より、 x^3-1 を割り切る。しかし、 $M_5(x)$ は、 x^2-1 や $x-1$ を割り切らない。 $M_5(x)$ で、割り切れる多項式 x^n-1 における最小の n は3であり、 $M_5(x)$ の位数は3である。表2第3列に各最小多項式の位数を示す。

- (4) $M_i(x)$ の次数は m 次以下である。

例えば、 $GF(2^4)$ の元の最小多項式の次数は表2のようにすべて4次以下である。

- (5) 2つの最小多項式 $M_i(x)$ と $M_j(x)$ の最小公倍多項式 $G(x)$ は、

$$G(x)=M_i(x)M_j(x) \quad (18)$$

($M_i(x) \neq M_j(x)$ の時)

または、

$$G(x)=M_i(x) \quad (19)$$

($M_i(x)=M_j(x)$ の時)

である。

例えば、表2より $M_1(x)$ と $M_3(x)$ の最小公倍多項式は、それぞれの共役根を持たなければならないので、

$$G(x)=M_1(x)M_3(x) \quad (20)$$

となる。また、 $M_1(x)$ と $M_2(x)$ の最小公倍多項式は、 $M_1(x)=M_2(x)$ であり、次式となる。

$$G(x)=M_1(x) \quad (21)$$

前回、既約多項式を説明に用いた。既約多項式と最小多項式の関係を確認する。性質(1)のように最小多項式は、 $GF(2^m)$ の元 a を根に持つ既約多項式である。逆に $GF(2^m)$ の元 a を根に持つ規約多項式は、ただ1つであり、これが a の最小多項式である。したがって、既約多項式に対し、元 a の…と名前を付けたものが最小多項式である、と理解してよい。

2.4 符号の根

巡回ハミング符号において、符号多項式 $W(x)$ に対して(1)式のシンドロームを計算すれば、

$$s=W(a)=0 \quad (22)$$

となる。なぜかという、符号多項式 $W(x)$ は生成多項式 $G(x)$ の多項式倍

$$W(x)=A(x)G(x) \quad (23)$$

であり、 $G(x)$ が原始元 a を根としているため、

$$G(a)=0 \quad (24)$$

が成り立つからである。

また、SEC-DED ハミング符号は、単純パリティ検査符号の生成多項式 $M_0(x)=x+1$ と巡回ハミング符号の生成多項式 $M_1(x)$ の最小公倍多項式 $G(x)=M_0(x)M_1(x)$ を生成多項式としている。この符号の復号は、シンドローム

$$\begin{aligned} s_0 &= Y(1) \\ s_1 &= Y(a) \end{aligned} \quad (25)$$

を使用して行える(前回5.3節)。この符号では1, a が、それぞれ $M_0(x)$, $M_1(x)$ の根であり、生成多項式 $G(x)$ の根になっている。したがって、符号多項式 $W(x)$ に対して、

$$\begin{aligned} s_0 &= W(1)=0 \\ s_1 &= W(a)=0 \end{aligned} \quad (26)$$

が成り立つ。この関係は逆も成り立つ。もし(25)式のシンドロームが0であるならば、最小多項式の性質(2)により、1および、 a の最小多項式である $M_0(x)$, $M_1(x)$ で割り切れる。したがって $G(x)$ で割り切れるので符号多項式となっている。多項式の根を使って考えれば、このような根拠により、(25)式のシンドロームが0であるか否かで、符号多項式であるか否かが判断できるわけである。

一般の場合としてまとめよう。 $GF(2)$ 上の m 次の生成多項式 $G(x)$ の根は m 個あり、これらを $a_1, a_2, \dots, a_m$ とする。

$$G(a_i)=0 \quad i=1, 2, \dots, m \quad (27)$$

$a_1, a_2, \dots, a_m$ は適当な拡大体 (2^m) の元である。符号多項式 $W(x)$ は、 $G(x)$ の多項式倍であるから、 $W(x)$ も $a_1, a_2, \dots, a_m$ を根として持つ。

$$W(a_i)=0 \quad i=1, 2, \dots, m \quad (28)$$

このため生成多項式 $G(x)$ の根を“符号の根”(root)と呼ぶ。

(例3.)

生成多項式が、

$$\begin{aligned} G(x) &= M_0(x)M_1(x) \\ &= (x+1)(x^4+x+1) \end{aligned} \quad (29)$$

の(15, 10) SEC-DED ハミング符号を考える(前回例

2.c). $M_0(x)$ は根 $x=1$ を持つ. $M_1(x)$ は原始多項式であり, 根は $\alpha, \alpha^2, \alpha^4, \alpha^8$ の4個である. したがって, この符号は $1=\alpha^0, \alpha, \alpha^2, \alpha^4, \alpha^8$ の5個の根を持つ.

3. 2重誤り訂正 BCH 符号

3.1 誤りロケータ

巡回ハミング符号を基に2重誤り訂正符号を作ろう. 例として(15, 11)巡回ハミング符号を用いる. 生成多項式 $G(x)$ は4次の原始多項式

$$G(x)=x^4+x+1 \quad (30)$$

である. 巡回ハミング符号で1重誤りが訂正できるのは, すべての1重誤りの誤りパターン多項式に対するシンドロームが非零で相異なっているからである(前回5.2節). 符号長15ビット中 i 番目のビットに誤りがあるならば, 誤りパターン多項式 $E(x)$ は,

$$E(x)=x^i \quad (31)$$

であり, このときシンドローム s は,

$$s=Y(a)=W(a)+E(a)=E(a)=\alpha^i \quad (32)$$

であり, シンドローム $s=\alpha^i$ が計算されたならば, すぐに i 番目のビットが誤っていることがわかる.

α^i が得られたならば i 番目のビット位置というのは煩わしいので, i 番目のビットの位置を α^i 番目の位置と呼ぶことにする(図1). 0番目, 1番目, 2番目という代わりに, α^0 番目, α^1 番目, α^2 番目...と呼ぶ. ビットの位置は0番目から14番目, α^i も表1のように α^0 から α^{14} まであって, すべて異なっているから一向に差し支えない. このように, α^i で表した誤りの位置を“誤りロケータ”(error locator)という. 2元符号の場合, 誤りの訂正は誤りロケータがわかれば行えるから, 復号器の役割は, シンドロームより未知の誤りロケータ α^i を推定することである. 1重誤りだけを考えるならば, (32)式のシンドローム s からすぐに未知の誤りロケータが求められる(s そのものが誤りロケータである).

3.2 2重誤りを訂正するために

それでは, この符号で α^i と α^j 番目の2重誤りが起きたらどうなるか? (図2). 誤りパターン多項式は,

$$E(x)=x^i+x^j \quad (33)$$

である. このとき得られるシンドロームは,

$$s=Y(a)=E(a)=\alpha^i+\alpha^j \quad (34)$$

である. このままでは, 使用できる式が1個しかなく, 未知数 α^i と α^j は確定できない. 2個の未知数を決めるには, 独立な方程式が2つ必要である. 未知数 α^i と α^j を含み, 受信多項式 $Y(x)$ から計算される別のシンドロームが必要である. 巡回ハミング符号は根 α を持つので, (1)式のシンドロームが使えた. それ

$$\begin{array}{cccccccccccccccc} E(x)= & & & & & & x^i & & & & & & & & & \text{誤りパターン多項式} \\ e= & (0 & \cdots & 0 & 1 & 0 & \cdots & 0 & 0) & \text{誤りパターン} \\ & \uparrow & & & \uparrow & & & & \uparrow & \uparrow & & & & & & \\ \text{誤りの位置} & n-1 & \cdots & i & \cdots & 1 & 0 & \text{番目} \\ \text{誤りロケータ} & \alpha^{n-1} & \cdots & \alpha^i & \cdots & \alpha^0 & \alpha^i & \text{番目} \end{array}$$

図1 誤りロケータ

$$\begin{array}{cccccccccccccccc} e=(0 & \cdots & 0 & 1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0) \\ & & & \uparrow & & & & \uparrow & & & & & & & \\ & & & \alpha^i & & & & \alpha^j & & & & & & & \text{番目} \end{array}$$

図2 2重誤りパターン

では, 別の符号の根 a も持つようにして, その根を受信多項式に代入した

$$s'=Y(a) \quad (35)$$

をシンドロームとして, 併せ使ってみよう. $GF(2^4)$ の零でない元は表1のように $0, 1, \alpha, \dots, \alpha^{14}$ と16種類ある. $a=0$ と選ぶと(35)式は常に零となり, 誤りの訂正・検出の役には立たない. $a=1$ とすると,

$$s'=Y(1)=E(1)=0 \quad (36)$$

であって, 未知数 α^i, α^j を含んでいないので, やはり2重誤りの場所を確定することができない. この(36)式と(1)式の2つのシンドロームを使用して誤り検出・訂正を行うのがSED-DEDハミング符号であるが, 前回に述べたように訂正できる誤りは, 単一誤りまでである.

$a=\alpha^2$ としたらどうであろうか? 受信多項式 $Y(x)$ は $GF(2)$ の上の多項式であるから, (7)式のように

$$Y(x^2)=\{Y(x)\}^2 \quad (37)$$

が成り立つので,

$$\begin{aligned} s' &= Y(\alpha^2)=\{Y(\alpha)\}^2=s^2 \\ &= \{\alpha^i+\alpha^j\}^2=\alpha^{2i}+\alpha^{2j} \end{aligned} \quad (38)$$

となり, s がわかれば s' は計算でき, 誤りロケータに関し新たな情報を与えるものではない.

実は $a=\alpha^3$ とするとうまくいく. (34)式と(35)式の s および s' を改めて s_1, s_3 と置くならば, 受信多項式 $Y(x)$ から計算されたこれらシンドロームと誤りロケータの間には,

$$\begin{aligned} s_1 &= Y(\alpha)=\alpha^i+\alpha^j \\ s_3 &= Y(\alpha^3)=(\alpha^i)^3+(\alpha^j)^3 \end{aligned} \quad (39)$$

の関係があり, この連立方程式を解くことで誤りロケータが求められる. α^i, α^j がガロア体の元であり自由に加減乗除を行ってよいから, このような連立方程式が解けるのである. 得られた誤りロケータに対し α^i および α^j 番目のビットを誤りとして反転すれば, 誤

図3 (15, 7) 2重誤り訂正 BCH 符号の符号器
 $G(x)=x^8+x^7+x^6+x^4+1$

りの訂正が行える。

3.3 2重誤り訂正 BCH 符号の生成多項式

この符号の生成多項式はどうなるか？ この符号は α および α^3 を根とする符号である。巡回ハミング符号の生成多項式 ((30)式) は例2.aのように $\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$ を根に持つ。さらに根 α^3 を持つために α^3 の最小多項式 $M_3(x)$ を追加し、 $M_1(x)$ と $M_3(x)$ の最小公倍多項式

$$\begin{aligned} G(x) &= LCM(M_1(x), M_3(x)) \\ &= M_1(x)M_3(x) \\ &= (x^4+x+1)(x^4+x^3+x^2+x+1) \\ &= x^8+x^7+x^6+x^4+1 \end{aligned} \quad (40)$$

を生成多項式とすればよい。

この符号の符号長を考えよう。 $G(x)$ で割り切れる多項式 x^n-1 における最小の n が符号長である。表2より、この $M_1(x), M_3(x)$ の位数はそれぞれ 15, 5 である。よって求める n は、

$$n = LCM(15, 5) = 15 \quad (41)$$

であり、符号長は 15 となる。また、生成多項式 $G(x)$ の次数 $m=8$ であるから、この符号の情報点数 $k=n-m=7$ となる。よって、この符号は (15, 7) 2重誤り訂正 BCH 符号である。生成多項式が (40) 式であるから、符号器は図3となる。

ここでは (15, 11) ハミング符号をもとに考えて来たが、一般に $GF(2^m)$ 上の原始元 α を根に持つハミング符号をもとに同様に α, α^3 を根に持つ符号として 2重誤り訂正符号が導かれ、その生成多項式は、

$$G(x) = M_1(x)M_3(x) \quad (42)$$

ただし $M_1(x), M_3(x)$ は α, α^3 の最小多項式であり、符号長は、

$$n = 2^m - 1 \quad (43)$$

となる。このような生成多項式を持つ符号が 2重誤り訂正 BCH (Bose-Chaudhuri-Hocquenghem code) 符号である。

3.4 シンドローム計算回路

(39) 式のシンドローム s_1, s_3 を使ってこの符号は 2

(a) $GF(2)$ 上の多項式割り算回路

(b) $GF(2^4)$ 上の多項式割り算回路

図4 シンドローム s_1 計算回路

重誤りを訂正する。シンドロームを計算する回路を考えよう。前回の SEC-DED ハミング符号は 2つの LFSR 回路で (25) 式のシンドロームを計算している。これと同じように、2つの LFSR 回路を用意すれば s_1, s_3 が計算できる。

s_1 は $Y(\alpha)$ であり、巡回ハミング符号のシンドロームであるから、前回と同じく図4(a)の

$$M_1(x) = x^4 + x + 1 \quad (44)$$

による割り算回路でも計算できる。別の観点から見てみよう。受信多項式を、

$$Y(x) = y_{14}x^{14} + y_{13}x^{13} + \dots + y_0 \quad (45)$$

y_i は $GF(2)$ の元

とする。 $Y(x)$ を $M_1(x)$ で割り算し、余りを $S(x)$ とすれば、次式である。

$$Y(x) = Q(x)M_1(x) + S(x) \quad (46)$$

$M_1(x)$ は根 α を持つことに注意して、上式に $x=\alpha$ を代入しよう。

$$Y(\alpha) = Q(\alpha)M_1(\alpha) + S(\alpha) = S(\alpha) \quad (47)$$

これがシンドローム s_1 である。ところで、 $Y(x)$ は係数が 0 または 1 すなわち $GF(2)$ 上の多項式であるが、0, 1 は $GF(2^4)$ の元でもある。多項式の係数の計算を $GF(2^4)$ で行って、 $Y(x)$ を (2^4) 上の 1 次式 $(x-\alpha)$ で割り算し、余りを S_1 とする。

$$Y(x) = Q'(x)(x - \alpha) + S_1 \quad (48)$$

1 次式で割り算したから、余り S_1 は $GF(2^4)$ 上の定数である。この式に $x = \alpha$ を代入すれば、

$$Y(\alpha) = S_1 \quad (49)$$

となり、これもシンドローム s_1 である。したがって、多項式 $Y(x)$ を $(x - \alpha)$ で割り算し、余りを求めてもシンドローム s_1 が得られる。多項式 $x - \alpha$ による割り算回路としてシンドローム s_1 の計算回路を示せば図 4(b) である。この回路に $Y(x)$ の係数を高次項 y_{14} より順番に入れ、 y_0 まで入力し終わった段階でレジスタに残るのが余り、すなわち s_1 である。この回路は、第 4 回 3.1 節で述べた割り算回路と基本的考えは全く同一のシフトレジスタ回路である。割り算されるのが $GF(2^4)$ 上の多項式であるから以下の点が拡張されている。

- ① 回は $GF(2^4)$ の元を蓄積する記憶素子
- ② $\bigcirc$ は α 倍する回路 (正確には $-\alpha$ 倍するのだが、 $GF(2^m)$ では $-\alpha = \alpha$ である)。
- ③ $\oplus$ は $GF(2^4)$ の加算回路

第 4 回 5.3 節に述べたように、拡大体の計算の実現法は何通りもある。 $GF(2^4)$ の元を表 1 の 4 ビットのベクトルで表し、 α 倍する計算を第 4 回 (58) 式の随伴行列 T の掛け算で行うとすれば、図の

- ① 回は 4 ビットのレジスタ
- ② $\bigcirc$ は行列 T の掛け算
- ③ $\oplus$ は 4 ビットのビット毎の exOR

と考えればよい。このシフトレジスタ回路は 4 ビットの並列データを 1 つの単位として取り扱っている $GF(2^4)$ の上の LFSR であるので、誤解のないよう図の信号線は太い $\Rightarrow$ で表してある。蛇足であるが、多項式 $Y(x)$ の係数の y_i は 1 または 0 であるが、この回路に入るときは 4 ビットの並列データであり、それぞれ表 1 の $\alpha^0 = (0001)$, $0 = (0000)$ として扱われる。

同様に考えれば、シンドローム $s_3 = Y(\alpha^3)$ は (47), (48) 式で α を α^3 で置き換えればよく、 $x - \alpha^3$ による割り算回路で計算できる。したがって、用意すべき 2 つ目の LFSR も $GF(2^4)$ の上の LFSR であり、 $x - \alpha^3$ による割り算回路として、図 5 となる。

3.5 誤り位置多項式

シンドローム s_1, s_3 が計算されたならば、(39) 式の連立方程式より、誤りロケータ α^i, α^j を求める。その手段として、 $GF(2^4)$ 上の次のような多項式 $\sigma(z)$ を考える。

$$\sigma(z) = (1 - \alpha^i z)(1 - \alpha^j z) \quad (50)$$

$$= 1 + \sigma_1 z + \sigma_2 z^2 \quad (51)$$

この多項式は誤りロケータの逆数 α^{-i}, α^{-j} を根に持つ

図 5 シンドローム s_3 計算回路 ($GF(2^4)$ 上の多項式割り算回路)

ものである。この $\sigma(z)$ のように、誤りロケータの逆数を根に持つ多項式を“誤り位置多項式” (error locator polynomial) という。

シンドローム s_1, s_3 からこの $\sigma(z)$ (の係数 σ_1, σ_2) が定まれば、その根として誤りロケータの逆数が求まり、誤りロケータがわかることになる。(51) 式を展開し、

$$\sigma(z) = 1 - (\alpha^i + \alpha^j)z + \alpha^i \alpha^j z^2$$

とすれば、(39), (51) 式と比較して、

$$\sigma_1 = -(\alpha^i + \alpha^j) = -s_1 = s_1$$

$$\sigma_2 = \alpha^i \alpha^j = (s_1^3 - s_3) / 3s_1 = (s_1^3 + s_3) / s_1 \quad (52)$$

$$\begin{aligned} \therefore s_1^3 &= (\alpha^i + \alpha^j)^3 \\ &= \alpha^{3i} + 3\alpha^{2i}\alpha^j + 3\alpha^i\alpha^{2j} + \alpha^{3j} \\ &= \alpha^{3i} + \alpha^i\alpha^j(\alpha^i + \alpha^j) + \alpha^{3j} \end{aligned}$$

となる。

このようにしてシンドローム s_1, s_3 から誤り位置多項式 $\sigma(z)$ を求めることができる。この $\sigma(z)$ は 2 次方程式であるが、実数体の方程式のように、根の公式で解くわけにはいかない。 α^{-i} ($i=0, 1, 2, \dots, 14$) を順次 $\sigma(z)$ に代入し、 $\sigma(\alpha^i)$ が 0 かどうかを調べることで誤りロケータを求めることになる。しかし、この方法は時間がかかるので、2 重誤り訂正符号では、誤り位置多項式の係数 (またはシンドローム) と根の関係を表で用意しておき、この表を索くことで誤りロケータを求めて誤り訂正を行うことが普通である。

3.6 2 重誤り訂正 BCH 符号の復号法

2 重誤り以外の誤りが生じたときどうなるかを考察して、この符号の復号法としてまとめよう。

α^i 番目のみの単一誤りであった場合、

$$\begin{aligned} s_1 &= \alpha^i \\ s_3 &= \alpha^{3i} \end{aligned} \quad (53)$$

であるから、(52) 式より誤り位置多項式は、

$$\sigma(z) = 1 - s_1 z + 0z^2 = 1 - \alpha^i z \quad (54)$$

の 1 次式となる。その根は $z = \alpha^{-i}$ の 1 つである。この場合、誤り位置多項式の根の数が 1 つとなるだけで、正しい誤りロケータが得られる。

(39) 式の s_1 は巡回ハミング符号のシンドロームである。巡回ハミング符号は、最小距離が 3 であるから、3 重以上の誤りに対してのみ $s_1 = 0$ となることから、

図 6 2重誤り訂正 BCH 符号の復号手順

ある。この時(52)式において、0で割り算することになり、 σ_2 が求まらない。また、誤り位置多項式 $\sigma(z)$ が求められても、 $\alpha^0, \dots, \alpha^{n-1}$ までの範囲に根がない場合もある。しかし2重以下の誤りに対しては、このようなことは起きないので、誤り位置多項式の係数や、その根が求められなかった場合は3重以上の誤りと考えればよい。

以上をまとめれば、復号法として次のようになる。これを図示すれば図6となる。

- (1) 受信多項式 $Y(x)$ から(39)式によりシンδροーム s_1, s_3 を計算する (図4(b), 図5)。
- (2) $s_1 = s_3 = 0$ ならば誤りなしと判定する。
- (3) 誤り位置多項式 $\sigma(z)$ の係数を(52)式により計算する。
- (4) $\sigma(z)$ の次数に等しい個数の根 α^{-i}, α^{-j} を求める。
- (5) i 番目と j 番目のビットを反転し、訂正を行う。ただし、(3), (4)において $\sigma(z)$ や、その根が求まらない場合は、3重以上の誤りが起きたと判断する。

なお、この復号法は(15, 7) BCH 符号以外であっても、根として $GF(2^m)$ 上の α と α^3 を持つ任意の符号に適用可能である。

(例 4.)

ここで考えている2重誤り訂正 BCH 符号で誤り訂正の例を見てみよう。受信語を、

$$\mathbf{y} = (0000001000000001) \quad (55)$$

とする。受信多項式は、

$$Y(x) = x^9 + 1 \quad (56)$$

である。シンδροームは、表1を見て計算すると、

$$\begin{aligned} s_1 &= Y(\alpha) = \alpha^9 + 1 = (1010) + (0001) = \alpha^7 \\ s_3 &= Y(\alpha^3) = \alpha^{27} + 1 = \alpha^{12} + 1 \\ &= (1111) + (0001) = \alpha^{11} \end{aligned} \quad (57)$$

である。誤り位置多項式の係数は、

$$\begin{aligned} \sigma_1 &= s_1 = \alpha^7 \\ \sigma_2 &= (s_1^3 + s_3) / s_1 = (\alpha^{21} + \alpha^{11}) / \alpha^7 \\ &= (\alpha^6 + \alpha^{11}) / \alpha^7 = \alpha / \alpha^7 = \alpha^{-6} = \alpha^9 \end{aligned} \quad (58)$$

である。誤り位置多項式

$$\sigma(z) = 1 + \alpha^7 z + \alpha^9 z^2 \quad (57)$$

に $z = \alpha^i$ ($i = 0, 1, \dots, 14$) を順次代入して根を求めれば、 $\sigma(\alpha^0) = 0$ がまず求められる。このまま代入を続けるか、または求められた根 α^0 を使って $\sigma(z) / (1 - \alpha^0 z) = (1 - \alpha^9 z)$ と計算すれば、誤りロケータ、 α^0 と α^9 が得られる。 $\mathbf{y}$ に対し、この位置を訂正すれば送信語 $\mathbf{w}$ は、

$$\mathbf{w} = (0000000000000000) \quad (60)$$

と推定される。

4. む す び

今回は BCH 符号と RS 符号(その1)として、これら符号のより所である、多項式の根の性質を説明し、それをもとに2重誤り訂正 BCH 符号を導いた。次の準備のために主要事項をまとめておく。

- 最小多項式： $GF(2^m)$ の元 a を根に持つ最小次数の $GF(2)$ の多項式を a の最小多項式という。
- 符号の根：巡回符号の生成多項式 $G(x)$ の根。符号の根 α_i 、受信多項式 $Y(x)$ に対し、シンδροーム $Y(\alpha_i)$ が零か否かで、符号語か否かがわかる。
- 2重誤り訂正 BCH 符号： α を $GF(2^m)$ の原始元として符号の根 α, α^n をもつ巡回符号。生式多項式は α, α^3 の最小多項式を用いて与えられる。
- 誤りロケータ：誤りの位置を拡大体 $GF(2^m)$ の元で表したものの。 i 番目の誤りならば、誤りロケータ α_i の誤りという。
- 2重誤り BCH 符号のシンδροーム：符号の根 α, α^3 に対しシンδροーム $s_1 = Y(\alpha), s_3 = Y(\alpha^3)$ である。これらは、 $GF(2^m)$ 上の多項式の割り算

回路で計算できる。

- ・誤り位置多項式 $\sigma(z)$: 誤りロケータの逆数を根に持つ多項式, シンドロームから誤りロケータ (誤りの位置) を求める際の手段として使用する。

〈付録〉 最小多項式の性質の証明

(1) [証明]

$M_i(x)=A(x)B(x)$ と因数分解できるとすると, $M_i(a)=A(a)B(a)=0$ であり, $A(a)=0$ または $B(a)=0$ となる. $M_i(x)$ より次数の低い多項式 $A(x)$ または $B(x)$ が a を根に持つことになり $M_i(x)$ が最小多項式であることに矛盾する。

(2) [証明]

$F(x)$ が $M_i(x)$ で割り切れないとする. すなわち $M_i(x)$ で割り算を行って

$$F(x)=Q(x)M_i(x)+R(x) \quad (\text{A } 1)$$

なる余り $R(x)$ が残るとする. この式で $x=a$ とおけば次式となり $R(x)$ は a を根に持つ。

$$0=F(a)=Q(a)M_i(a)+R(a)=R(a) \quad (\text{A } 2)$$

$R(x)$ は余りであるから, $M_i(x)$ より次数が低い多項式であり, これも $M_i(x)$ が最小多項式であることに矛盾する。

(3) [証明]

a の位数が n であることより, $F(x)=x^n-1$ に対し $F(a)=0$ である. この $F(x)$ に (2) の性質を適用すれば (3) の前半は成立する. $n'<n$ として $M_i(x)$ が $x^{n'}-1$ を割り切るならば a は $x^{n'}-1$ の根である. すなわち $a^{n'}-1=0$ であり, これは a の位数が n であることに矛盾する。

(4) [証明]

拡大体 $GF(2^m)$ の元は m 次元ベクトルで表される. $1, a, a^2, \dots, a^m$ なる $m+1$ 個のベクトルを考えれば, 線形従属である. すなわち, すべてが 0 ではない $GF(2)$ の元 $c_0, c_1, \dots, c_m$ で次式を満たすものが存在する。

$$c_0 1 + c_1 a + c_2 a^2 + \dots + c_m a^m = 0 \quad (\text{A } 3)$$

この $c_0, c_1, \dots, c_m$ を使って, m 次多項式

$$F(x)=c_0+c_1x+c_2x^2+\dots+c_mx^m \quad (\text{A } 4)$$

を考えれば $F(a)=0$ である. 性質 (2) より $M_i(x)$ はこの $F(x)$ を割り切るので, $M_i(x)$ の次数は m 次以下である。

(5) [証明]

$M_i(x)$ と $M_j(x)$ が 1 つの根 b を共通に持つとする. $M_i(b)=M_j(b)=0$ である. b の最小多項式を $M_b(x)$ とすれば, 性質 (2) より, $M_i(x), M_j(x)$ は $M_b(x)$ で割り切れる. 最小多項式は既約多項式であるので, 次数の低い他の多項式で割り切れることはない. それ故, この 3 つの多項式は非零の定数倍の違いを除いて一致する. $GF(2)$ の非零の元は 1 であり結局 $M_i(x)=M_j(x)=M_b(x)$ となり, $M(x)$ と $M_j(x)$ はすべての根を共通に持つことになる. したがって $M_i(x)$ と $M_j(x)$ は根を完全に共有するか, または全く異なる根を持つかのいずれかである. 前者の場合, 最小公倍多項式は (19) 式となり, 後者の場合が (18) 式となる。

金子 敏信 (かね こしゆん) 昭和 51 年, 東京大学大学院博士課程修了. 同年, 東京理科大学講師, 53 年, 同助教授となり, 現在, 同大学理工学部電気工学科に勤務. 符号理論, 通信方式, 情報セキュリティの研究に従事. 工学博士. 正会員.