代数系と符号理論 (O) 第5回板書プリント

制作：植松友彦

2014.5.13

第4回の復習

- シンドローム
- シンドローム復号法
- 標準配列の作り方
- Varshamov-Gilbert の下界式
- ハミング限界
- Singleton 限界

1　重み分布

線形符号の場合、A_w は任意の符号語から距離 w にある符号語の総数でもあることに注意しておく。

[例 **1**] 2 元 (7,4) 線形符号

$$\begin{aligned} C \quad = \quad & \{(0000000), (1101000), (0110100), (0011010), \\ & (0001101), (1011100), (1110010), (1100101), \\ & (0101110), (0111001), (0010111), (1000110), \\ & (1010001), (1111111), (0100011), (1001011)\} \end{aligned}$$

について、重み零の符号語と重み 7 の符号語がそれぞれ 1 個、重み 3 の符号語が 7 個、重み 4 の符号語が 7 個あるので、重み分布は

$$A_0 = 1,\ A_1 = A_2 = 0, A_3 = A_4 = 7,\ A_5 = A_6 = 0,\ A_7 = 1$$

である。従って、重み分布母関数は

$$A(z) = 1 + 7z^3 + 7z^4 + z^7$$

である。

[例 **2**]　例 1 の $(7,4)$ 線形符号を考えよう。この場合の重み分布母関数は、

$$A(z) = 1 + 7z^3 + 7z^4 + z^7$$

である。この符号の生成行列は、

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

であり、パリティ検査行列は

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

となり、双対符号の符号語は、

$$\begin{aligned} C^{\perp} &= \{(0000000), (1011100), (1110010), (0111001), \\ &\quad (0101110), (1100101), (1001011), (0010111)\} \end{aligned}$$

であり、双対符号の重み分布母関数は

$$B(z) = 1 + 7z^4$$

となる。MacWilliams の恒等式によれば、

$$\begin{aligned} 2^{-4}(1+z)^7 A\left(\frac{1-z}{1+z}\right) &= 2^{-4}(1+z)^7 \left\{1 + 7\left(\frac{1-z}{1+z}\right)^3 + 7\left(\frac{1-z}{1+z}\right)^4 + \left(\frac{1-z}{1+z}\right)^7\right\} \\ &= \frac{1}{16}\{(1+z)^7 + 7(1-z)^3(1+z)^4 + 7(1-z)^4(1+z)^3 + (1-z)^7\} \\ &= \frac{1}{16}\left\{16 + 112z^4\right\} \\ &= 1 + 7z^4 \\ &= B(z) \end{aligned}$$

となり、重み分布母関数 $A(z)$ から双対符号の重み分布母関数 $B(z)$ が求まることが分る。

2　群の例

[例 **3**] 有理数は加法 $(+)$ の元に群をなす。なぜならば、有理数は和について閉じており (G1)、結合法則が成り立ち (G2)、単位元は 0 であり (G3)、m/n の逆元は $-m/n$ である (G4)。

　また、非零の有理数は乗法 $(\times)$ の元に群をなす。なぜならば、有理数は乗法について閉じており (G1)、結合法則が成り立ち (G2)、単位元は 1 であり (G3)、非零の元 m/n の逆元は n/m である (G4)。

[例 **4**] 実数を係数とする 2×2 の正則行列の全体を $GL(2,R)$ とする。すなわち、

$$GL(2,R) = \{A : A \text{ は } 2 \times 2 \text{ の実行列}, \det A \neq 0\}$$

2 つの行列 A, B の演算 $A \cdot B$ を通常の行列の積と定める。このとき、行列の積に関して $GL(2, R)$ は閉じている (G1)。なぜなら、行列式の性質から

$$\det(A \cdot B) = \det(A) \times \det(B) \neq 0$$

が成り立つからである。行列の積なので結合法則がなりたつ (G2)。単位元は単位行列である (G3)。更に、行列 $A \in GL(2, R)$ の逆元は逆行列 A^{-1} である (G4)。従って、$GL(2, R)$ は行列の積に関して群をなす。

[例 **5**] 集合 $S = \{a, b, c\}$ の上での演算 $\circ_1, \circ_2, \circ_3$ を次の表で定義する。

$\circ_1$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

$\circ_2$	a	b	c
a	a	b	c
b	c	a	b
c	b	c	a

$\circ_3$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

演算 $\circ_1$ については、単位元は b であるが、a の逆元が存在しないので群ではない。尚、逆元の存在しないのは a だけであり、b の逆元は b であり、c の逆元は c である。

演算 $\circ_2$ については、任意の $x \in S$ について $a \circ_2 x = x$ が成り立つが、$b \circ_2 a = c$ なので、単位元が存在しない。

演算 $\circ_3$ について S は群をなす。なぜならば、表には S の元しか現れない (G1)。結合法則が成り立つ (G2)。単位元は a である (G3)。a の逆元は a、b の逆元は c、c の逆元は b である (G4)。

[例 **6**] 例 3 の有理数に関する群は無限群である。例 4 の $GL(2, R)$ も無限群である。例 5 の集合 S は演算 $\circ_3$ に関して有限群である。また、例 3 の有理数の群と例 5 の群は可換群であるが、例 4 の $GL(2, R)$ は非可換群である。例えば、

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 2 & 2 \end{pmatrix}$$
$$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & -2 \\ 1 & 2 \end{pmatrix}$$

である。

[例 **7**] 3 の倍数の集合 $\{0, \pm 3, \pm 6, \ldots\}$ は、整数の加法における群の部分群である。同様に、整数 a の倍数の集合は、整数の加法における群の部分群である。

[例 **8**] $GL(2, R)$ において、部分集合

$$SL(2, R) = \{A \in GL(2, R) : \det(A) = 1\}$$

は $GL(2, R)$ の部分群である。なぜならば、$A, B \in SL(2, R)$ ならば、

$$\det(A \cdot B) = \det(A) \det(B) = 1$$

なので、$A \cdot B \in SL(2, R)$ である (G1)。また、上の式で $B = A^{-1}$ とおくことで、

$$\det(A^{-1}) = \frac{1}{\det(A)} = 1$$

が得られ、$A^{-1} \in SL(2, R)$ である (G4)。

3　巡回群

[例 **9**] 複素数の積の演算について $G = \{1, -1, i, -i\}$ は i によって生成される巡回群である。なぜならば、

$$i^1 = i,\ i^2 = -1,\ i^3 = -i,\ i^4 = 1$$

が成り立つからである。また、G の生成元には i の他に $-i$ もある。

4　部分群による類別

[例 **10**] 整数の加法群 Z を考えよう。このとき、3 の倍数の集合

$$H = \{0, \pm 3, \pm 6, \cdots\}$$

は Z の部分群である。そこで H による類別を行うと

H	$\cdots, -9, -6, -3, 0, 3, 6, 9, \cdots$
$1 + H$	$\cdots, -8, -5, -2, 1, 4, 7, 10, \cdots$
$2 + H$	$\cdots, -7, -4, -1, 2, 5, 8, 11, \cdots$

が得られる。これは 3 で割った剰余による整数の分類に他ならない。

[例 **11**] 2 元体上の 2 元符号

$$C = \{(000000), (100110), (010101), (0010110), (110011), (101101), (011110), (111000)\}$$

による 2 元体上の 6 次元ベクトル空間 G の類別を考えよう。G は明らかにベクトルの加法について群をなす。また、C は G の部分群である。従って、部分群 C による類別を行うと、

C	(000000)	(100110)	(010101)	(001011)	(110011)	(101101)	(011110)	(111000)
$(100000) + C$	(100000)	(000110)	(110101)	(101011)	(010011)	(001101)	(111110)	(011000)
$(010000) + C$	(010000)	(110110)	(000101)	(011011)	(100011)	(111101)	(001110)	(101000)
$(001000) + C$	(001000)	(101110)	(011101)	(000011)	(111011)	(100101)	(010110)	(110000)
$(000100) + C$	(000100)	(100010)	(010001)	(001111)	(110111)	(101001)	(011010)	(111100)
$(000010) + C$	(000010)	(100100)	(010111)	(001001)	(110001)	(101111)	(011100)	(111010)
$(000001) + C$	(000001)	(100111)	(010100)	(001010)	(110010)	(101100)	(011111)	(111001)
$(100001) + C$	(100001)	(000111)	(110100)	(101010)	(010010)	(001100)	(111111)	(011001)

が得られる。これは、シンドローム復号法のときに用いたコセットの表に一致する。(第 4 回板書プリント p.3 参照)

[注意] G の位数の任意の約数の位数を持つ部分群が存在するか否かは G によって異なる。(群論の難しさ！)

5　同型写像と群の同型

[例 **12**] $GL(2,R)$ に対し、行列式を取る写像

$$f : GL(2,R) \to R^* = R - \{0\}, \quad A \mapsto \det(A)$$

は、非零の実数の乗法に関する群への準同型写像である。なぜならば、行列式の性質

$$\det(A \cdot B) = \det(A)\det(B)$$

から

$$f(A \cdot B) = f(A) \times f(B)$$

が成り立つからである。

J. L. Lagrange (1736-1813)　　N. H. Abel (1802-1829)

群論を創った人々(その 1)

代数方程式の解の公式と群論の発展

3 次方程式の解の公式 : カルダノ (伊) の公式 (1545)

4 次方程式の解の公式 : フェラーリ (伊) の公式 (1545)

解の公式の研究 : ラグランジュによる根の置換群 (対称群) の導入と方程式が解ける為の条件 (1770)

5 次以上の方程式には解の公式がない : ルフィニ (伊) の証明 (1799)

ルフィニの証明の欠陥の解決 : アーベルの証明 (1824)

代数方程式が代数的に解ける為の必要十分条件 : ガロアによるガロア群とガロア理論の発見 (1829)

代数方程式の解の公式について興味のある者は、「中村亨: “ガロアの群論–方程式はなぜ解けなかったのか”, ブルーバックス, 講談社」が良い入門書である。