1章の演習問題の解答

[演習 **1.1**]

1) 2元符号なので、任意の符号語のスカラー倍 (0倍か1倍) は零ベクトルかその符号語自身であり、同一符号語どうしを加えると零ベクトルになる。従って、どの2つの符号語の和も符号語になっているものが線形符号である。

   (a) 零ベクトルがないため線形符号ではない。

   (b) どの2つの符号語の和も符号語であるので、C は $(3,2)$ 線形符号である。また、その基底の一つは、$\{(001),(010)\}$ である。

   (c) $(0001)+(1110)=(1111)\notin C$ なので、C は線形符号ではない。

   (d) どの2つの符号語の和も符号語であるので、C は $(5,2)$ 線形符号である。また、その基底の一つは $\{(11110),(01111)\}$ である。

   (e) $(11100)+(00111)=(11011)\notin C$ なので、C は線形符号ではない。

2) 線形空間 V の部分集合である $C=\{c_1,c_2,\cdots,c_m\}$ の元の線形結合の全体を

$$C' \triangleq \{a_1c_1+a_2c_2+\cdots+a_mc_m : a_i\in\mathbb{F}_2\}$$

   によって定義する。このとき、C' は C を含む線形空間 V の部分空間となる。従って、C には含まれていないが C' には含まれている符号語を C に追加すれば線形符号となる。

   (a) $C'=\{(000),(001),(010),(011),(100),(101),(110),(111)\}$ であり、$(000),(001),(010),(100),(110)$ を C に追加すればよい。

   (c) $C'=\{(0000),(0001),(1110),(1111)\}$ であり、(1111) を C に追加すればよい。

   (e) $C'=\{(00000),(00011),(00100),(00111),(11000),(11011),(11100),(11111)\}$ であり、$(00011),(00100),(11011),(11111)$ を C に追加すればよい。

3) (a) C' の中から一次独立な3つのベクトルを選べば良いので、例えば、$\{(001),(010),(100)\}$。

   (c) C' の中から一次独立な2つのベクトルを選べば良いので、例えば、$\{(0001),(1110)\}$。

   (e) C' の中から一次独立な3つのベクトルを選べば良いので、例えば、$\{(11100),(00111),(11000)\}$。

[演習 **1.2**]

(a) $(0011)=0(1000)+1(1100)+0(1110)+1(1111)$

(b) $(1010)=1(1000)+1(1100)+1(1110)+0(1111)$

(c) $(0111)=1(1000)+0(1100)+0(1110)+1(1111)$

(d) $(0001)=0(1000)+0(1100)+1(1110)+1(1111)$

(e) $(0000)=0(1000)+0(1100)+0(1110)+0(1111)$

2 章の演習問題の解答

[演習 **2.1**]

(1) 線形符号の場合、最小距離と非零の符号語の最小重みが等しいので (定理 2.1)、C の最小距離は 1 である。また、基底の一つは $\{(100), (010)\}$ なので、次元は 2 であり、生成行列の定義 (定義 2.1) より、

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

である。このとき、$G = [I_2\ P]$ とみなせば、式 (2.4) から

$$H = [-P^T\ I_1] = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}$$

を得る。

(2) C の最小距離は 2 である。また、C の基底の一つは $\{(1001), (0110)\}$ なので、次元は 2 であり、

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

である。また、

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

である。

(3) C の最小距離は 3 である。また、基底の一つは $\{(100110), (010101), (001011)\}$ なので、次元は 3 であり、

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

である。また、

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

である。

[演習 **2.2**] $S = \{\boldsymbol{s}_1, \boldsymbol{s}_2, \cdots, \boldsymbol{s}_m\}$ に属する符号語の線形結合で定まる符号 C は、行ベクトルが S の要素である行列 A を用いて、

$$C = \{\boldsymbol{x}A : \forall \boldsymbol{x} \in \mathbb{F}^m\}$$

と表現できる。また、A に対して行基本操作を行い、行に現れるすべての零ベクトルを取り除いて得られる $k \times n$ 行列 G を用いても、

$$C = \{\boldsymbol{u}G : \forall \boldsymbol{u} \in \mathbb{F}^k\}$$

と表現できる。このとき、G の作り方から、G の行ベクトルは線形独立であり、任意の $\boldsymbol{c} \in C$ がある $\boldsymbol{u} \in \mathbb{F}^k$ を用いて $\boldsymbol{c} = \boldsymbol{u}G$ と書けるため、G の行ベクトルは C の基底である。従って、G は C の生成行列の一つに他ならず、C の符号長は n、次元は k であることが分る。

(1) S に属するベクトルは線形独立なので、行ベクトルが S の要素である A がそのまま生成行列 G となる。従って、C の符号長は 4、次元は 2 である。また、

$$\begin{aligned} C &= \left\{ \boldsymbol{u} \begin{bmatrix} 1010 \\ 0101 \end{bmatrix} : \forall \boldsymbol{u} \in \mathbb{F}^2 \right\} \\ &= \{(0000), (1010), (0101), (1111)\} \end{aligned}$$

から、C の最小距離が 2 であることがわかる。

(2) 行ベクトルが S の要素である行列 A に対して行基本操作を行うと、

$$A = \begin{bmatrix} 10101 \\ 01010 \\ 11111 \\ 00011 \\ 10110 \end{bmatrix} \xrightarrow{\text{1 行目と 2 行目を 3 行目に加える}} \begin{bmatrix} 10101 \\ 01010 \\ 00000 \\ 00011 \\ 10110 \end{bmatrix} \xrightarrow{\text{1 行目と 4 行目を 5 行目に加える}} \begin{bmatrix} 10101 \\ 01010 \\ 00000 \\ 00011 \\ 00000 \end{bmatrix}$$

従って、

$$G = \begin{bmatrix} 10101 \\ 01010 \\ 00011 \end{bmatrix}$$

であり、符号長は 4、次元は 3 である。また、

$$\begin{aligned} C &= \left\{ \boldsymbol{u} \begin{bmatrix} 10101 \\ 01010 \\ 00011 \end{bmatrix} : \forall \boldsymbol{u} \in \mathbb{F}^3 \right\} \\ &= \{(0000), (10101), (01010), (11111), (00011), (10110), (01001), (11100)\} \end{aligned}$$

から、最小距離は 2 である。

(3) S のベクトルは線形独立なので、A がそのまま生成行列 G となる。従って、C の符号長は 8、

次元は 4 である。また、

$$
\begin{aligned}
C &= \left\{ \boldsymbol{u} \begin{bmatrix} 11111111 \\ 11110000 \\ 11001100 \\ 10101010 \end{bmatrix} : \forall \boldsymbol{u} \in \mathbb{F}^4 \right\} \\
&= \{(00000000), (11111111), (11110000), (00001111), (11001100), (00110011), \\
&\quad (00111100), (11000011), (10101010), (01010101), (01011010), \\
&\quad (10100101), (01100110), (10011001), (10010110), (01101001)\}
\end{aligned}
$$

から、最小距離は 4 である。

(4) S のベクトルは線形独立なので C の符号長は 8、次元は 4 である。また、A は簡単な行基本操作で、

$$
A = \begin{bmatrix} 11111100 \\ 11110011 \\ 11001111 \\ 00111111 \end{bmatrix} \longrightarrow \begin{bmatrix} 11000000 \\ 00110000 \\ 00001100 \\ 00000011 \end{bmatrix}
$$

とできる。また、

$$
\begin{aligned}
C &= \left\{ \boldsymbol{u} \begin{bmatrix} 11000000 \\ 00110000 \\ 00001100 \\ 00000011 \end{bmatrix} : \forall \boldsymbol{u} \in \mathbb{F}^4 \right\} \\
&= \{(00000000), (11000000), (00110000), (11110000), (00001100), (11001100), \\
&\quad (00111100), (11111100), (00000011), (11000011), (00110011), \\
&\quad (11110011), (00001111), (11001111), (00111111), (11111111)\}
\end{aligned}
$$

から、最小距離は 2 である。

3章の演習問題の解答

[演習 **3.1**]

(1) H の列は零ベクトルを含まず、全ての列ベクトルは異なっているので最小距離は 3 以上である。他方、H の 1,4,5,6 列を加えると零ベクトルとなる。以上から、H の任意の 3 つの列ベクトルは線形独立であり、4 つの列ベクトルの中には線形従属なものがあることが分るので、定理 3.3 から最小距離は 4 以上である。更に、

$$(100111)H^T = \mathbf{0}$$

であり、線形符号においては最小距離と最小重みが等しいことに注意すれば、(100111) は最小ハミング重みを有する符号語である。

(2) H の列は零ベクトルを含まず、全てのの列ベクトルは異なっているので最小距離は 3 以上である。ところが、任意の 3 つの列ベクトルは線形独立であるので、定理 3.3 から最小距離は 4 以上である。しかも、

$$(10001110)H^T = \mathbf{0}$$

であるので、(10001110) は最小ハミング重みを有する符号語であり、最小距離は 4 である。

(3) H の列は零ベクトルを含まず、全ての列ベクトルは異なっているので最小距離は 3 以上である。ところが、任意の 3 つの列ベクトルは線形独立であるので、定理 3.3 から最小距離は 4 以上である。しかも、

$$(0011110)H^T = \mathbf{0}$$

であるので、(0011110) は最小ハミング重みを有する符号語であり、最小距離は 4 である。

[演習 **3.2**]　パリティ検査行列 H を計算し、定理 3.3 を用いる。

(1) $G = [I_4\ P]$ と見なせば、

$$H = [-P^T\ I_3] = \begin{bmatrix} 1110100 \\ 1101010 \\ 1011001 \end{bmatrix}$$

となる。このとき、H の列は零ベクトルを含まず、全ての列ベクトルは異なっているので最小距離は 3 以上である。他方、

$$(0100110)H^T = \mathbf{0}$$

から、(0100110) は符号語なので、最小距離は 3 である。

(2) G に行基本操作を施したものもまた C の生成行列になっているので、

$$G = \begin{bmatrix} 111000000 \\ 000111000 \\ 111111111 \end{bmatrix} \overset{\text{1 行目と 2 行目を 3 行目に加える}}{\longrightarrow} \begin{bmatrix} 111000000 \\ 000111000 \\ 000000111 \end{bmatrix}$$

によって得られた行列 G' もまた C の生成行列である。更に、列の入れ替えを行うと、

$$G' = \begin{bmatrix} 111000000 \\ 000111000 \\ 000000111 \end{bmatrix} \overset{\substack{\text{2 列目と 4 列目、} \\ \text{3 列目と 7 列目を入れ替え}}}{\longrightarrow} \begin{bmatrix} 100100100 \\ 010011000 \\ 001000011 \end{bmatrix}$$

が得られる。この行列を $[I_3\ P]$ とみなせば、

$$[-P^T\ I_6] = \begin{bmatrix} 100100000 \\ 010010000 \\ 010001000 \\ 100000100 \\ 001000010 \\ 001000001 \end{bmatrix}$$

となる。このとき、$[I_3\ P] \cdot [-P^T\ I_6]^T = O$ であることから、列の入れ替えを行う前の生成行列 G' に対応するパリティ検査行列は、$[-P^T\ I_6]$ の 2 列目と 4 列目、3 列目と 7 列目を入れ替えた行列となる。すなわち、

$$H = \begin{bmatrix} 110000000 \\ 000110000 \\ 000101000 \\ 101000000 \\ 000000110 \\ 000000101 \end{bmatrix}$$

となる。ここで、H の列は零ベクトルを含まず、全ての列ベクトルは異なっているので最小距離は 3 以上である。他方、

$$(111000000)H^T = \mathbf{0}$$

であるので、(111000000) は符号語であり、最小距離は 3 である。

4章の演習問題の解答

[演習 **4.1**] G に対して次のような基本行操作を施す。

$$G = \begin{bmatrix}110100\\011010\\001101\end{bmatrix} \overset{\text{3 行目を 2 行目に加える}}{\longrightarrow} \begin{bmatrix}110100\\010111\\001101\end{bmatrix} \overset{\text{2 行目を 1 行目に加える}}{\longrightarrow} \begin{bmatrix}100011\\010111\\001101\end{bmatrix}$$

これから、パリティ検査行列 H は

$$H = \begin{bmatrix}011100\\110010\\111001\end{bmatrix}$$

であることが分る。

次に、標準配列を次のようにして作る。

(1) 先頭を零ベクトルとして、全ての符号を一行に書く (紙面の都合で解答では、行を折り返している)。

シンドローム	コセット			
(000)	(000000)	(110100)	(011010)	(101110)
	(001101)	(111001)	(010111)	(100011)

(2) 1 行目に出現しなかった 2 元ベクトルで重みが最小なものとして、(100000) を選び、1 行目のベクトルに (100000) を加えたものを 2 行目に書く。

シンドローム	コセット			
(000)	(000000)	(110100)	(011010)	(101110)
	(001101)	(111001)	(010111)	(100011)
(011)	(100000)	(010100)	(111010)	(001110)
	(101101)	(011001)	(110111)	(000011)

(3) これまでに出現しなかった 2 元ベクトルで重みが最小なものとして、(010000) を選び、1 行目のベクトルに (010000) を加えたものを 3 行目に書く。

シンドローム	コセット			
(000)	(000000)	(110100)	(011010)	(101110)
	(001101)	(111001)	(010111)	(100011)
(011)	(100000)	(010100)	(111010)	(001110)
	(101101)	(011001)	(110111)	(000011)
(111)	(010000)	(100100)	(001010)	(111110)
	(011101)	(101001)	(000111)	(110011)

(4) 上記の操作を繰り返せば、例えば次の表を得る。ただし、8 行目のコセット代表元として (000110) を用いた。

シンドローム	コセット			
(000)	(000000)	(110100)	(011010)	(101110)
	(001101)	(111001)	(010111)	(100011)
(011)	(100000)	(010100)	(111010)	(001110)
	(101101)	(011001)	(110111)	(000011)
(111)	(010000)	(100100)	(001010)	(111110)
	(011101)	(101001)	(000111)	(110011)
(101)	(001000)	(111100)	(010010)	(100110)
	(000101)	(110001)	(011111)	(101011)
(100)	(000100)	(110000)	(011110)	(101010)
	(001001)	(111101)	(010011)	(100111)
(010)	(000010)	(110110)	(011000)	(101100)
	(001111)	(111011)	(010101)	(100001)
(001)	(000001)	(110101)	(011011)	(101111)
	(001100)	(111000)	(010110)	(100010)
(110)	(000110)	(110010)	(011100)	(101000)
	(001011)	(111111)	(010001)	(100101)

これから、シンドロームとコセット代表元との対応表を作ると次の表が得られる。

シンドローム	コセット代表元
(000)	(000000)
(011)	(100000)
(111)	(010000)
(101)	(001000)
(100)	(000100)
(010)	(000010)
(001)	(000001)
(110)	(000110)

この表をもとにシンドローム復号法によって各受信語を復号する。

(a)

$$\boldsymbol{s} = (000100)H^T = (100)$$

であり、このシンドロームに対応するコセット代表元は、$\boldsymbol{e} = (000100)$ なので、受信語 $\boldsymbol{r}$ は

$$\boldsymbol{r} - \boldsymbol{e} = (000000)$$

に復号される。

(b)

$$\boldsymbol{s} = (011110)H^T = (100)$$

であり、このシンドロームに対応するコセット代表元は、$\boldsymbol{e} = (000100)$ なので、受信語 $\boldsymbol{r}$ は

$$\boldsymbol{r} - \boldsymbol{e} = (011010)$$

に復号される。

(c)

$$\boldsymbol{s} = (110011)H^T = (111)$$

であり、このシンドロームに対応するコセット代表元は、$\boldsymbol{e} = (010000)$ なので、受信語 $\boldsymbol{r}$ は

$$\boldsymbol{r} - \boldsymbol{e} = (100011)$$

に復号される。

[演習 **4.2**]

(1) Varshamov-Gilbert 限界において、$n = 15$, $d = 5$ とすることで、

$$\begin{aligned} 1 + \binom{14}{1} + \binom{14}{2} + \binom{14}{3} &= 1 + 14 + 91 + 364 \\ &= 470 \\ &< 2^9 \\ &= 2^{15-6} \end{aligned}$$

が得られる。従って、k は 6 以上である。

(2) $q = 2$、$n = 15$ である。また最小距離は 5 なので、定理 3.1 より、$\lfloor \frac{5-1}{2} \rfloor = 2$ 個以下のすべての誤りを訂正可能である。従って、$t = 2$ とすれば、ハミング限界より、

$$\begin{aligned} 2^k \sum_{j=0}^{2} \binom{15}{j} &= 2^k \left(\binom{15}{0} + \binom{15}{1} + \binom{15}{2} \right) \\ &= 2^k (1 + 15 + 105) \\ &= 2^k 121 \\ &< 2^k 2^7 \\ &= 2^{k+7} = 2^{15} \end{aligned}$$

を満たさねばならない。従って、k の上界は 8 である。

(3) Singleton 限界より、

$$\begin{aligned} 5 &\leq 15 - k + 1 \\ &\leq 16 - k \end{aligned}$$

を得る。従って、k の上界は 11 である。

5 章の演習問題の解答

[演習 **5.1**]

(1) 生成行列 G を用いて、C の全ての符号語を求めると、

$$\begin{aligned} C &= \left\{ \boldsymbol{u} \begin{bmatrix} 111100 \\ 000011 \end{bmatrix} : \forall \boldsymbol{u} \in \mathbb{F}_2^2 \right\} \\ &= \{(000000), (111100), (000011), (111111)\} \end{aligned}$$

となる。

(2) 重みが 0、2、4 と 6 の符号語がそれぞれ 1 個あるので、重み分布関数は

$$A(z) = 1 + z^2 + z^4 + z^6 \tag{1}$$

となる。

(3) G の 2 列目と 5 列目を交換すると、

$$\begin{bmatrix} 101110 \\ 010001 \end{bmatrix}$$

を得る。この行列を $[I_2 P]$ とみなせば、

$$[-P^T I_4] = \begin{bmatrix} 101000 \\ 100100 \\ 100010 \\ 010001 \end{bmatrix}$$

であり、$[I_2 P] \cdot [-P^T I_4]^T = O$ から、$[-P^T I_4]$ の 2 列目と 5 列目を交換した行列がパリティ検査行列 H である。すなわち、

$$H = \begin{bmatrix} 101000 \\ 100100 \\ 110000 \\ 000011 \end{bmatrix}$$

である。従って、双対符号 $C^\perp$ の全ての符号語を求めると、

$$\begin{aligned} C^\perp &= \left\{ \boldsymbol{u} \begin{bmatrix} 101000 \\ 100100 \\ 110000 \\ 000011 \end{bmatrix} : \forall \boldsymbol{u} \in \mathbb{F}_2^4 \right\} \\ &= \{(000000), (110000), (011000), (101000), (001100), (111100), \\ &\quad (010100), (100100), (000011), (110011), (011011), \\ &\quad (101011), (001111), (111111), (010111), (100111)\} \end{aligned}$$

となる。

(4) 双対符号 $C^{\perp}$ には、重み零の符号語が 1 個、重み 2 の符号語が 7 個、重み 4 の符号語が 7 個、重み 6 の符号語が 1 個あるので、双対符号の重み分布関数は

$$B(z) = 1 + 7z^2 + 7z^4 + z^6 \tag{2}$$

となる。

(5) Macwilliams の恒等式より、

$$B(z) = 2^{-2}(1+z)^6 A\left(\frac{1-z}{1+z}\right)$$

が成り立つ。この式の右辺に式 (1) を代入すれば、

$$\begin{aligned}
& 2^{-2}(1+z)^6 A\left(\frac{1-z}{1+z}\right) \\
&= 2^{-2}(1+z)^6 \left\{1 + \left(\frac{1-z}{1+z}\right)^2 + \left(\frac{1-z}{1+z}\right)^4 + \left(\frac{1-z}{1+z}\right)^6\right\} \\
&= 2^{-2}\left\{(1+z)^6 + (1+z)^4(1-z)^2 + (1+z)^2(1-z)^4 + (1-z)^6\right\} \\
&= 1 + 7z^2 + 7z^4 + z^6
\end{aligned}$$

となる。これは式 (2) と一致し、MacWilliams の恒等式が成り立つことが確認される。

6 章の演習問題の解答

[演習 **6.1**]　まず、3 つの要素を持つ群は全て同一の群であることを示す。

　定理 6.1 より、群は唯一の単位元 e を含み、群の任意の要素に対して逆元が唯一つ決まる。そこで、3 つの要素を持つ群を $\{e, a, b\}$ とおくと、b は a の逆元となる。なぜなら、

$$a \circ b = a \tag{1}$$
$$a \circ b = b \tag{2}$$
$$a \circ b = e \tag{3}$$

のいずれかが成り立つが、式 (1) の両辺に左から a の逆元を乗じると

$$b = e$$

であり、式 (2) の両辺に右から b の逆元を乗じると、

$$a = e$$

であるので、式 (1) と式 (2) は a と b が単位元 e ではないことに矛盾し、矛盾無く成り立つのは式 (3) のみだからである。従って、3 つの要素を持つ全ての群は、単位元 e とある要素 a とその要素の逆元 a^{-1} という構造になっており、それらには元の表し方以外に相違は無く、全て同一である。

　次に、3 つの要素を持つ群は可換であることを示す。いま、3 つの要素を持つ群を $G = \{e, a, a^{-1}\}$ とする。このとき、

$$\begin{aligned} e \circ a &= a = a \circ e \\ e \circ a^{-1} &= a^{-1} = a^{-1} \circ e \\ a \circ a^{-1} &= e = a^{-1} \circ a \end{aligned}$$

が成り立つ。従って、3 つの要素を持つ群は可換である。

[演習 **6.2**]

(1) G は可換、すなわち全ての $a, b \in G$ について $ab = ba$。

(2) 全ての $a, b \in G$ と全ての正整数 n について $(ab)^n = a^n b^n$。

が同値であることを示す。

　(1) $\Rightarrow$ (2) を示す。G が可換のとき、 $x_1, \ldots, x_n \in G$ として、

$$\begin{aligned} x_1 x_2 \cdots x_{n-2} x_{n-1} \underline{x_n} &= x_1 x_2 \cdots x_{n-2} \underline{x_n} x_{n-1} \\ &= x_1 x_2 \cdots \underline{x_n} x_{n-2} x_{n-1} \\ &\vdots \\ &= \underline{x_n} x_1 \cdots x_{n-1} \end{aligned}$$

が成り立ち、各要素の順番を任意に入れ換えることができる。このことを用いると

$$\begin{aligned}(ab)^n &= abab\cdots ab \\ &= a\cdots ab\cdots b \\ &= a^n b^n\end{aligned}$$

である。

(2) ⇒ (1) を示す。任意の $a, b \in G$ について

$$abab = (ab)(ab) = (ab)^2 = a^2b^2 = aabb$$

が成り立つ。両辺に左から a^{-1}、 右から b^{-1} を作用させると $ba = ab$ である。

以上より (1) と (2) が同値であることが示された。

7章の演習問題の解答

[演習 **7.1**]

加法表:

$+$	0	a	b
0	0	a	b
a	a	b	0
b	b	0	a

乗法表:

$\times$	0	a	b
0	0	0	0
a	0	a	b
b	0	b	a

または

$\times$	0	a	b
0	0	0	0
a	0	b	a
b	0	a	b

または

$\times$	0	a	b
0	0	0	0
a	0	0	0
b	0	0	0

これらの表の作り方について述べる。

[加法表について]

0 が加法に関する単位元であることと、可換であることから、$a+b=b+a$、 $a+a$、$b+b$ を定めればよい。

$a+b=a$ と仮定すると、両辺に a の逆元を加えることで $b=0$ となり矛盾。$a+b=b$ と仮定しても、同様に $a=0$ となり矛盾する。従って、$a+b=b+a=0$ でなければならない。

次に、$a+a=0$ と仮定すると $a+b=0$ の両辺に a を加えることで $b=a$ が得られ矛盾。$a+a=a$ とすると両辺に a の逆元を加えることで $a=0$ が得られ矛盾。従って、$a+a=b$ でなければならず、両辺に b を加えて $a=b+b$ を得る。

[乗法表について]

まず、環 R の任意の元 x に対して、$x\cdot 0=0\cdot x=0$ である。次に、加法表から $a=-b$、 $b=-a$ であることと、環 R の任意の元 x、y に対して、$x\cdot(-y)=(-x)\cdot y$ であることから、

$$a\cdot a=a\cdot(-b)=(-a)\cdot b=b\cdot b \quad \text{かつ} \quad a\cdot b=a\cdot(-a)=(-a)\cdot a=b\cdot a$$

となる。更に $x\cdot(-y)=-(x\cdot y)$ であるから

$$a\cdot b=a\cdot(-a)=-(a\cdot a)$$

となる。従って、$a\cdot a$ を決めれば乗法表が定まることになる。

[演習 **7.2**]

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

上記乗算表の各行 (または各列) は、イデアルの定義 I 2 から、あるイデアルの部分集合となる。従って定義 I 2 を満たす Z_6 の部分集合は $\{0\},\{0,3\},\{0,2,4\},\{0,1,2,3,4,5\}=Z_6$ の四つである。このどれもが定義 I 1 を満たすので、Z_6 の全てのイデアルは $\{0\},\{0,3\},\{0,2,4\},Z_6$ となる。

8章の演習問題の解答

[演習 **8.1**]

1. 7 は素数なので、剰余類環 Z_7 における加法と乗法の定義を用いて、加算表と乗算表を作ると、次の表が得られる。

加算表

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

乗算表

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

2. 位数は 6 を割り切るので、$1, 2, 3, 6$ のべき乗だけ調べればよい。乗算表から、

$$
\begin{aligned}
&1^1 \bmod 7 = 1 \\
&2^1 \bmod 7 = 2,\ 2^2 \bmod 7 = 4,\ 2^3 \bmod 7 = 1 \\
&3^1 \bmod 7 = 3,\ 3^2 \bmod 7 = 2,\ 3^3 \bmod 7 = 6,\ 3^6 \bmod 7 = 1 \\
&4^1 \bmod 7 = 4,\ 4^2 \bmod 7 = 2,\ 4^3 \bmod 7 = 1 \\
&5^1 \bmod 7 = 5,\ 5^2 \bmod 7 = 4,\ 5^3 \bmod 7 = 6,\ 5^6 \bmod 7 = 1 \\
&6^1 \bmod 7 = 6,\ 6^2 \bmod 7 = 1
\end{aligned}
$$

   を得る。従って、

$$
\begin{aligned}
&\mathrm{ord}(1) = 1, \quad \mathrm{ord}(2) = 3, \quad \mathrm{ord}(3) = 6 \\
&\mathrm{ord}(4) = 3, \quad \mathrm{ord}(5) = 6, \quad \mathrm{ord}(6) = 2
\end{aligned}
$$

   である。

3. 2. より、原始元は 3 と 5 である。

[演習 **8.2**]

1. 加算表と乗算表は次ページの表に示す。

2. 位数は $2^3 - 1 = 7$ を割り切るので、1 か 7 となる。元を 1 乗して 1 となるのは 1 だけなので、それ以外の元は全て位数が 7 である。

3. 2. より、原始元は 0 と 1 以外の全ての元、すなわち、$x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$ である。

表 1: 加算表

$+$	0	1	x	$x+1$	x^2
0	0	1	x	$x+1$	x^2
1	1	0	$x+1$	x	x^2+1
x	x	$x+1$	0	1	x^2+x
$x+1$	$x+1$	x	1	0	x^2+x+1
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$

$+$	x^2+1	x^2+x	x^2+x+1
0	x^2+1	x^2+x	x^2+x+1
1	x^2	x^2+x+1	x^2+x
x	x^2+x+1	x^2	x^2+1
$x+1$	x^2+x	x^2+1	x^2
x^2	1	x	$x+1$
x^2+1	0	$x+1$	x
x^2+x	$x+1$	0	1
x^2+x+1	x	1	0

表 2: 乗算表

$\cdot$	0	1	x	$x+1$	x^2
0	0	0	0	0	0
1	0	1	x	$x+1$	x^2
x	0	x	x^2	x^2+x	$x+1$
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x
x^2+1	0	x^2+1	1	x^2	x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1
x^2+x+1	0	x^2+x+1	x^2+1	x	1

$\cdot$	x^2+1	x^2+x	x^2+x+1
0	0	0	0
1	x^2+1	x^2+x	x^2+x+1
x	1	x^2+x+1	x^2+1
$x+1$	x^2	1	x
x^2	x	x^2+1	1
x^2+1	x^2+x+1	$x+1$	x^2+x
x^2+x	$x+1$	x	x^2
x^2+x+1	x^2+x	x^2	$x+1$

9 章の演習演習の解答

[演習 **9.1**]

1. 定理 9.2 より、$\mathbb{F}_{2^4}$ の部分体は $\mathbb{F}_2$、$\mathbb{F}_{2^2}$ と $\mathbb{F}_{2^4}$ の 3 つである。

2. $\alpha^4 = \alpha + 1$ を利用すれば、べき表示と多項式表示の対応表は次のようになる。

べき表示	多項式表示
α	α
α^2	α^2
α^3	α^3
α^4	$\alpha+1$
α^5	$\alpha^2+\alpha$
α^6	$\alpha^3+\alpha^2$
α^7	$\alpha^3+\alpha+1$
α^8	α^2+1

べき表示	多項式表示
α^9	$\alpha^3+\alpha$
α^{10}	$\alpha^2+\alpha+1$
α^{11}	$\alpha^3+\alpha^2+\alpha$
α^{12}	$\alpha^3+\alpha^2+\alpha+1$
α^{13}	$\alpha^3+\alpha^2+1$
α^{14}	α^3+1
α^{15}	1
—	—

3. 非零の各元の位数は次の通り。

元	位数
1	1
α	15
α^2	15
α^3	5
α^4	15
α^5	3
α^6	5
α^7	15

元	位数
α^8	15
α^9	5
α^{10}	3
α^{11}	15
α^{12}	5
α^{13}	15
α^{14}	15
—	—

4. $p(x)$ の根は原始元 α なので、α の最小多項式 (原始多項式) は x^4+x+1 である。$m_3(x)$ を α^3 の最小多項式と表すことにすれば、定理 14.2 より、

$$m_3(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9)$$

である。これを展開することで、最小多項式

$$\begin{aligned}
m_3(x) &= (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9) \\
&= (x-\alpha^3)(x-\alpha^{12})(x-\alpha^6)(x-\alpha^9) \\
&= (x^2-(\alpha^3+\alpha^{12})x+\alpha^{15})(x^2-(\alpha^6+\alpha^9)x+\alpha^{15}) \\
&= (x^2-\alpha^{10}x+1)(x^2-\alpha^5x+1) \\
&= (x^2+1)^2-(\alpha^{10}+\alpha^5)x(x^2+1)+\alpha^{15}x^2 \\
&= x^4+x^3+x^2+x+1
\end{aligned}$$

を得る。

[演習 **9.2**]

1. $\alpha^5 = \alpha^2 + 1$ を利用すれば、べき表示と多項式表示の対応表は次のようになる。

べき表示	多項式表示
α	α
α^2	α^2
α^3	α^3
α^4	α^4
α^5	α^2+1
α^6	$\alpha^3+\alpha$
α^7	$\alpha^4+\alpha^2$
α^8	$\alpha^3+\alpha^2+1$
α^9	$\alpha^4+\alpha^3+\alpha$
α^{10}	α^4+1
α^{11}	$\alpha^2+\alpha+1$
α^{12}	$\alpha^3+\alpha^2+\alpha$
α^{13}	$\alpha^4+\alpha^3+\alpha^2$
α^{14}	$\alpha^4+\alpha^3+\alpha^2+1$
α^{15}	$\alpha^4+\alpha^3+\alpha^2+\alpha+1$
α^{16}	$\alpha^4+\alpha^3+\alpha+1$

べき表示	多項式表示
α^{17}	$\alpha^4+\alpha+1$
α^{18}	$\alpha+1$
α^{19}	$\alpha^2+\alpha$
α^{20}	$\alpha^3+\alpha^2$
α^{21}	$\alpha^4+\alpha^3$
α^{22}	$\alpha^4+\alpha^2+1$
α^{23}	$\alpha^3+\alpha^2+\alpha+1$
α^{24}	$\alpha^4+\alpha^3+\alpha^2+\alpha$
α^{25}	$\alpha^4+\alpha^3+1$
α^{26}	$\alpha^4+\alpha^2+\alpha+1$
α^{27}	$\alpha^3+\alpha+1$
α^{28}	$\alpha^4+\alpha^2+\alpha$
α^{29}	α^3+1
α^{30}	$\alpha^4+\alpha$
α^{31}	1
—	—

2. 系 8.1 から、有限体 $\mathbb{F}_{2^5}$ の任意の非零元の位数は $2^5-1=31$ を割り切る。31 は素数なので、非零の全ての元の位数は 1 か 31 である。位数 1 の元は単位元だけなので、1 以外の非零の元の位数は全て 31 となり、原始元であることが分る。

3. $m_i(x)$ によって α^i の最小多項式を表すことにすれば、定理 14.3 より、

$$\begin{aligned}
m_1(x) &= (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)(x-\alpha^{16}) \\
m_3(x) &= (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^{24})(x-\alpha^{17}) \\
m_5(x) &= (x-\alpha^5)(x-\alpha^{10})(x-\alpha^{20})(x-\alpha^9)(x-\alpha^{18}) \\
m_7(x) &= (x-\alpha^7)(x-\alpha^{14})(x-\alpha^{28})(x-\alpha^{25})(x-\alpha^{19}) \\
m_{11}(x) &= (x-\alpha^{11})(x-\alpha^{22})(x-\alpha^{13})(x-\alpha^{26})(x-\alpha^{21}) \\
m_{15}(x) &= (x-\alpha^{15})(x-\alpha^{30})(x-\alpha^{29})(x-\alpha^{27})(x-\alpha^{23})
\end{aligned}$$

を得る。これらを展開することで、次の最小多項式が得られる。

$$\begin{aligned}
m_1(x) &= m_2(x) = m_4(x) = m_8(x) = m_{16}(x) = x^5+x^2+1 \\
m_3(x) &= m_6(x) = m_{12}(x) = m_{24}(x) = m_{17}(x) = x^5+x^4+x^3+x^2+1 \\
m_5(x) &= m_{10}(x) = m_{20}(x) = m_9(x) = m_{18}(x) = x^5+x^4+x^2+x+1 \\
m_7(x) &= m_{14}(x) = m_{28}(x) = m_{25}(x) = m_{19}(x) = x^5+x^3+x^2+x+1 \\
m_{11}(x) &= m_{22}(x) = m_{13}(x) = m_{26}(x) = m_{21}(x) = x^5+x^4+x^3+x+1 \\
m_{15}(x) &= m_{30}(x) = m_{29}(x) = m_{27}(x) = m_{23}(x) = x^5+x^3+1
\end{aligned}$$

10章の演習問題の解答

[演習 **10.1**] $\alpha^3 = \alpha + 1$ を利用すると、$\mathbb{F}_8$ のべき表示と多項式表示の対応は次の表で与えられる。

べき表示	多項式表示
α	α
α^2	α^2
α^3	$\alpha+1$
α^4	$\alpha^2+\alpha$
α^5	$\alpha^2+\alpha+1$
α^6	α^2+1
α^7	1

1. 多項式 1、x、x^2、x^3 はそれぞれ、

$$\begin{aligned} 1 &\rightarrow (1,1,1,1,1,1) \\ x &\rightarrow (1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5) \\ x^2 &\rightarrow (1,\alpha^2,\alpha^4,\alpha^6,\alpha^8,\alpha^{10}) = (1,\alpha^2,\alpha^4,\alpha^6,\alpha,\alpha^3) \\ x^3 &\rightarrow (1,\alpha^3,\alpha^6,\alpha^9,\alpha^{12},\alpha^{15}) = (1,\alpha^3,\alpha^6,\alpha^2,\alpha^5,\alpha) \end{aligned}$$

に符号化される。また、多項式 $i_0 + i_1 x + i_2 x^2 + i_3 x^3$ は

$$\begin{aligned} &(i_0+i_1+i_2+i_3,\ i_0+i_1\alpha+i_2\alpha^2+i_3\alpha^3,\ i_0+i_1\alpha^2+i_2\alpha^4+i_3\alpha^6, \\ &\qquad i_0+i_1\alpha^3+i_2\alpha^6+i_3\alpha^2,\ i_0+i_1\alpha^4+i_2\alpha+i_3\alpha^5,\ i_0+i_1\alpha^5+i_2\alpha^3+i_3\alpha) \\ &= i_0(1,1,1,1,1,1)+i_1(1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5) \\ &\qquad +i_2(1,\alpha^2,\alpha^4,\alpha^6,\alpha,\alpha^3)+i_3(1,\alpha^3,\alpha^6,\alpha^2,\alpha^5,\alpha) \end{aligned}$$

に符号化される。従って、生成行列は

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha \end{bmatrix}$$

である。

2. 1. の生成行列に対してべき表示と多項式表示の対応表を利用して行基本変形を行うと

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha \end{bmatrix} \xrightarrow{\text{1 行目をそれ以外の行に加える}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \alpha^3 & \alpha^6 & \alpha & \alpha^5 & \alpha^4 \\ 0 & \alpha^6 & \alpha^5 & \alpha^2 & \alpha^3 & \alpha \\ 0 & \alpha & \alpha^2 & \alpha^6 & \alpha^4 & \alpha^3 \end{bmatrix}$$

$$\xrightarrow{\text{2 行目を } \alpha^4 \text{ 倍}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & \alpha^3 & \alpha^5 & \alpha^2 & \alpha \\ 0 & \alpha^6 & \alpha^5 & \alpha^2 & \alpha^3 & \alpha \\ 0 & \alpha & \alpha^2 & \alpha^6 & \alpha^4 & \alpha^3 \end{bmatrix} \xrightarrow{\substack{\text{2 行目をそれ以外の行の 2 列目が} \\ \text{零になるように適当な元を乗じて加える}}} \begin{bmatrix} 1 & 0 & \alpha & \alpha^4 & \alpha^6 & \alpha^3 \\ 0 & 1 & \alpha^3 & \alpha^5 & \alpha^2 & \alpha \\ 0 & 0 & \alpha^3 & \alpha & 1 & \alpha^3 \\ 0 & 0 & \alpha & 0 & \alpha^6 & \alpha^5 \end{bmatrix}$$

$$\xrightarrow{\text{3 行目を } \alpha^4 \text{ 倍}} \begin{bmatrix} 1 & 0 & \alpha & \alpha^4 & \alpha^6 & \alpha^3 \\ 0 & 1 & \alpha^3 & \alpha^5 & \alpha^2 & \alpha \\ 0 & 0 & 1 & \alpha^5 & \alpha^4 & 1 \\ 0 & 0 & \alpha & 0 & \alpha^6 & \alpha^5 \end{bmatrix} \xrightarrow{\substack{\text{3 行目をそれ以外の行の 3 列目が} \\ \text{零になるように適当な元を乗じて加える}}} \begin{bmatrix} 1 & 0 & 0 & \alpha^3 & \alpha & 1 \\ 0 & 1 & 0 & \alpha^6 & \alpha^6 & 1 \\ 0 & 0 & 1 & \alpha^5 & \alpha^4 & 1 \\ 0 & 0 & 0 & \alpha^6 & \alpha & \alpha^6 \end{bmatrix}$$

$$\xrightarrow{\text{4 行目を } \alpha \text{ 倍}} \begin{bmatrix} 1 & 0 & 0 & \alpha^3 & \alpha & 1 \\ 0 & 1 & 0 & \alpha^6 & \alpha^6 & 1 \\ 0 & 0 & 1 & \alpha^5 & \alpha^4 & 1 \\ 0 & 0 & 0 & 1 & \alpha^2 & 1 \end{bmatrix} \xrightarrow{\substack{\text{4 行目をそれ以外の行の 4 列目が} \\ \text{零になるように適当な元を乗じて加える}}} \begin{bmatrix} 1 & 0 & 0 & 0 & \alpha^6 & \alpha \\ 0 & 1 & 0 & 0 & \alpha^5 & \alpha^2 \\ 0 & 0 & 1 & 0 & \alpha^5 & \alpha^4 \\ 0 & 0 & 0 & 1 & \alpha^2 & 1 \end{bmatrix}$$

が得られる。この行列が組織符号の生成行列となる。

3. 定理 10.1 より、RS$(6,4)$ 符号の最小距離は $n-k+1=6-4+1=3$ である。

4. $f(x)=x^3+x$ の場合、

$$\begin{aligned} f(1) &= 1+1=0 \\ f(\alpha) &= \alpha^3+\alpha=1 \\ f(\alpha^2) &= \alpha^6+\alpha^2=1 \\ f(\alpha^3) &= \alpha^9+\alpha^3=\alpha^2+\alpha^3=\alpha^5 \\ f(\alpha^4) &= \alpha^{12}+\alpha^4=\alpha^5+\alpha^4=1 \\ f(\alpha^5) &= \alpha^{15}+\alpha^5=\alpha+\alpha^5=\alpha^6 \end{aligned}$$

なので、符号語は

$$(f(1), f(\alpha), f(\alpha^2), f(\alpha^3), f(\alpha^4), f(\alpha^5)) = (0, 1, 1, \alpha^5, 1, \alpha^6)$$

である。

5. $(0,1,1,\alpha^5,1,\alpha^6)+(0,\alpha,0,0,0,0)=(0,\alpha^3,1,\alpha^5,1,\alpha^6)$ であり、$t=\lfloor\frac{6-4}{2}\rfloor=1$ なので、連立方程式の係数行列は、

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^3 & \alpha^4 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & 1 & \alpha^2 \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^5 & \alpha^8 \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha^{16} & 1 & \alpha^4 \\ 1 & \alpha^5 & \alpha^{10} & \alpha^{15} & \alpha^{20} & \alpha^6 & \alpha^{11} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^3 & \alpha^4 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & 1 & \alpha^2 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^5 & \alpha \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & 1 & \alpha^4 \\ 1 & \alpha^5 & \alpha^3 & \alpha & \alpha^6 & \alpha^6 & \alpha^4 \end{bmatrix}$$

となる。この行列に対して行基本操作をすると、

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^3 & \alpha^4 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & 1 & \alpha^2 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^5 & \alpha \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & 1 & \alpha^4 \\ 1 & \alpha^5 & \alpha^3 & \alpha & \alpha^6 & \alpha^6 & \alpha^4 \end{bmatrix} \xrightarrow{1\text{ 行目をそれ以外の行に加える}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & \alpha^3 & \alpha^6 & \alpha & \alpha^5 & \alpha^3 & \alpha^4 \\ 0 & \alpha^6 & \alpha^5 & \alpha^2 & \alpha^3 & 1 & \alpha^2 \\ 0 & \alpha & \alpha^2 & \alpha^6 & \alpha^4 & \alpha^5 & \alpha \\ 0 & \alpha^5 & \alpha^3 & \alpha^4 & \alpha^6 & 1 & \alpha^4 \\ 0 & \alpha^4 & \alpha & \alpha^3 & \alpha^2 & \alpha^6 & \alpha^4 \end{bmatrix}$$

$$\xrightarrow{2\text{ 行目を }\alpha^4\text{ 倍}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & \alpha^3 & \alpha^5 & \alpha^2 & 1 & \alpha \\ 0 & \alpha^6 & \alpha^5 & \alpha^2 & \alpha^3 & 1 & \alpha^2 \\ 0 & \alpha & \alpha^2 & \alpha^6 & \alpha^4 & \alpha^5 & \alpha \\ 0 & \alpha^5 & \alpha^3 & \alpha^4 & \alpha^6 & 1 & \alpha^4 \\ 0 & \alpha^4 & \alpha & \alpha^3 & \alpha^2 & \alpha^6 & \alpha^4 \end{bmatrix} \xrightarrow{\begin{array}{c}2\text{ 行目に適当な元を乗じて} \\ 2\text{ 行目以降の }2\text{ 列目を零にする}\end{array}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & \alpha^3 & \alpha^5 & \alpha^2 & 1 & \alpha \\ 0 & 0 & \alpha^3 & \alpha & 1 & \alpha^2 & \alpha^6 \\ 0 & 0 & \alpha & 0 & \alpha^6 & \alpha^6 & \alpha^4 \\ 0 & 0 & 1 & \alpha^6 & \alpha^2 & \alpha^4 & \alpha^3 \\ 0 & 0 & \alpha^3 & \alpha^5 & 1 & \alpha^3 & 1 \end{bmatrix}$$

$$\xrightarrow{3\text{ 行目を }\alpha^4\text{ 倍}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & \alpha^3 & \alpha^5 & \alpha^2 & 1 & \alpha \\ 0 & 0 & 1 & \alpha^5 & \alpha^4 & \alpha^6 & \alpha^3 \\ 0 & 0 & \alpha & 0 & \alpha^6 & \alpha^6 & \alpha^4 \\ 0 & 0 & 1 & \alpha^6 & \alpha^2 & \alpha^4 & \alpha^3 \\ 0 & 0 & \alpha^3 & \alpha^5 & 1 & \alpha^3 & 1 \end{bmatrix} \xrightarrow{\begin{array}{c}3\text{ 行目に適当な元を乗じて} \\ 3\text{ 行目以降の }3\text{ 列目を零にする}\end{array}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & \alpha^3 & \alpha^5 & \alpha^2 & 1 & \alpha \\ 0 & 0 & 1 & \alpha^5 & \alpha^4 & \alpha^6 & \alpha^3 \\ 0 & 0 & 0 & \alpha^6 & \alpha & \alpha^2 & 0 \\ 0 & 0 & 0 & \alpha & \alpha & \alpha^3 & 0 \\ 0 & 0 & 0 & \alpha^6 & 0 & \alpha^5 & \alpha^2 \end{bmatrix}$$

$$\xrightarrow{4\text{ 行目を }\alpha\text{ 倍}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & \alpha^3 & \alpha^5 & \alpha^2 & 1 & \alpha \\ 0 & 0 & 1 & \alpha^5 & \alpha^4 & \alpha^6 & \alpha^3 \\ 0 & 0 & 0 & 1 & \alpha^2 & \alpha^3 & 0 \\ 0 & 0 & 0 & \alpha & \alpha & \alpha^3 & 0 \\ 0 & 0 & 0 & \alpha^6 & 0 & \alpha^5 & \alpha^2 \end{bmatrix} \xrightarrow{\begin{array}{c}4\text{ 行目に適当な元を乗じて} \\ 4\text{ 行目以降の }4\text{ 列目を零にする}\end{array}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & \alpha^3 & \alpha^5 & \alpha^2 & 1 & \alpha \\ 0 & 0 & 1 & \alpha^5 & \alpha^4 & \alpha^6 & \alpha^3 \\ 0 & 0 & 0 & 1 & \alpha^2 & \alpha^3 & 0 \\ 0 & 0 & 0 & 0 & 1 & \alpha^6 & 0 \\ 0 & 0 & 0 & 0 & \alpha & \alpha^3 & \alpha^2 \end{bmatrix}$$

$$\xrightarrow{\begin{array}{c}5\text{ 行目に適当な元を乗じて} \\ 5\text{ 行目以降の }5\text{ 列目を零にする}\end{array}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & \alpha^3 & \alpha^5 & \alpha^2 & 1 & \alpha \\ 0 & 0 & 1 & \alpha^5 & \alpha^4 & \alpha^6 & \alpha^3 \\ 0 & 0 & 0 & 1 & \alpha^2 & \alpha^3 & 0 \\ 0 & 0 & 0 & 0 & 1 & \alpha^6 & 0 \\ 0 & 0 & 0 & 0 & 0 & \alpha & \alpha^2 \end{bmatrix} \xrightarrow{6\text{ 行目を }\alpha^6\text{ 倍}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & \alpha^3 & \alpha^5 & \alpha^2 & 1 & \alpha \\ 0 & 0 & 1 & \alpha^5 & \alpha^4 & \alpha^6 & \alpha^3 \\ 0 & 0 & 0 & 1 & \alpha^2 & \alpha^3 & 0 \\ 0 & 0 & 0 & 0 & 1 & \alpha^6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & \alpha \end{bmatrix}$$

が得られる。従って、連立方程式

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & \alpha^3 & \alpha^5 & \alpha^2 & 1 & \alpha \\ 0 & 0 & 1 & \alpha^5 & \alpha^4 & \alpha^6 & \alpha^3 \\ 0 & 0 & 0 & 1 & \alpha^2 & \alpha^3 & 0 \\ 0 & 0 & 0 & 0 & 1 & \alpha^6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & \alpha \end{bmatrix} \begin{bmatrix} Q_{0,0} \\ Q_{0,1} \\ Q_{0,2} \\ Q_{0,3} \\ Q_{0,4} \\ Q_{1,0} \\ Q_{1,1} \end{bmatrix} = \mathbf{0}$$

を解けばよい。この方程式の非自明な解は、$Q_{1,1} = 1$ と置けば、

$$
\begin{aligned}
Q_{1,0} &= -\alpha Q_{1,1} = \alpha \\
Q_{0,4} &= -\alpha^6 Q_{1,0} = 1 \\
Q_{0,3} &= -\alpha^2 Q_{0,4} - \alpha^3 Q_{1,0} = \alpha \\
Q_{0,2} &= -\alpha^5 Q_{0,3} - \alpha^4 Q_{0,4} - \alpha^6 Q_{1,0} - \alpha^3 Q_{1,1} = 1 \\
Q_{0,1} &= -\alpha^3 Q_{0,2} - \alpha^5 Q_{0,3} - \alpha^2 Q_{0,4} - Q_{1,0} - \alpha Q_{1,1} = \alpha \\
Q_{0,0} &= -Q_{0,1} - Q_{0,2} - Q_{0,3} - Q_{0,4} = 0
\end{aligned}
$$

となる。従って、

$$
\begin{aligned}
Q_0(x) &= x^4 + \alpha x^3 + x^2 + \alpha x \\
Q_1(x) &= x + \alpha
\end{aligned}
$$

が得られる。$Q_0(x)$ と $Q_1(x)$ から情報多項式を求めると

$$
g(x) = -\frac{Q_0(x)}{Q_1(x)} = \frac{x^4 + \alpha x^3 + x^2 + \alpha x}{x + \alpha} = x^3 + x
$$

となり、送信符号語は、

$$
(g(1), g(\alpha), g(\alpha^2), g(\alpha^3), g(\alpha^4), g(\alpha^5)) = (0, 1, 1, \alpha^5, 1, \alpha^6)
$$

となる。

11章の演習演習の解答

[演習 **11.1**] $\alpha^3 = \alpha + 1$ を利用すると、$\mathbb{F}_8$ のべき表示と多項式表示の対応は次の表で与えられる。

べき表示	多項式表示
α	α
α^2	α^2
α^3	$\alpha+1$
α^4	$\alpha^2+\alpha$
α^5	$\alpha^2+\alpha+1$
α^6	α^2+1
α^7	1

1.

$i=1:\ g_0(x,y)=1,\ g_1(x,y)=y$ から、

$$\Delta_0 = g_0(1,\alpha) = 1, \quad \Delta_1 = g_1(1,\alpha) = \alpha,$$

であるので、$J=\{0,1\}$ となる。$1 \prec y$ から、$j^*=0$ となり、$f(x,y)=g_0(x,y)=1$, $\Delta=\Delta_0=1$ として、

$$\begin{aligned} g_0(x,y) &:= (x-1)g_0(x,y) = x+1 \\ g_1(x,y) &:= g_1(x,y) - \alpha f(x,y) = y+\alpha \end{aligned}$$

が得られる。

$i=2:\ g_0(x,y)=x+1,\ g_1(x,y)=y+\alpha$ から、

$$\Delta_0 = g_0(\alpha,\alpha^3) = \alpha^3, \quad \Delta_1 = g_1(\alpha,\alpha^3) = 1$$

であるので、$J=\{0,1\}$ となる。$x \prec y$ から、$j^*=0$ となり、$f(x,y)=g_0(x,y)=x+1$, $\Delta=\Delta_0=\alpha^3$ として、

$$\begin{aligned} g_0(x,y) &:= (x-\alpha)g_0(x,y) = (x+\alpha)(x+1) \\ &= x^2+\alpha^3 x+\alpha \\ g_1(x,y) &:= \alpha^3 g_1(x,y) - f(x,y) = \alpha^3(y+\alpha)+(x+1) \\ &= \alpha^3 y + x + \alpha^5 \end{aligned}$$

が得られる。

$i=3:\ g_0(x,y)=x^2+\alpha^3 x+\alpha,\ g_1(x,y)=\alpha^3 y+x+\alpha^5$ から、

$$\Delta_0 = g_0(\alpha^2,\alpha^6) = \alpha^3, \quad \Delta_1 = g_1(\alpha^2,\alpha^6) = \alpha^5$$

であるので、$J=\{0,1\}$ となる。$y \prec x^2$ から、$j^*=1$ となり、$f(x,y)=g_1(x,y)=\alpha^3 y+x+\alpha^5$, $\Delta=\Delta_1=\alpha^5$ として、

$$\begin{aligned} g_0(x,y) &:= \alpha^5 g_0(x,y)-\alpha^3 f(x,y)=\alpha^5(x^2+\alpha^3 x+\alpha)-\alpha^3(\alpha^3 y+x+\alpha^5) \\ &= \alpha^5 x^2+x+\alpha^6 y+\alpha^5 \\ g_1(x,y) &:= (x-\alpha^2)g_1(x,y)=(x+\alpha^2)(\alpha^3 y+x+\alpha^5) \\ &= (\alpha^3 x+\alpha^5)y+x^2+\alpha^3 x+1 \end{aligned}$$

が得られる。

$i=4:\ g_0(x,y)=\alpha^5 x^2+x+\alpha^6 y+\alpha^5$、$g_1(x,y)=(\alpha^3 x+\alpha^5)y+x^2+\alpha^3 x+1$ から、

$$\Delta_0=g_0(\alpha^3,\alpha)=\alpha^3, \quad \Delta_1=g_1(\alpha^3,\alpha)=\alpha^6$$

であるので、$J=\{0,1\}$ となる。$x^2 \prec xy$ から、$j^*=0$ となり、$f(x,y)=g_0(x,y)=\alpha^5 x^2+x+\alpha^6 y+\alpha^5$, $\Delta=\Delta_0=\alpha^3$ として、

$$\begin{aligned} g_0(x,y) &:= (x-\alpha^3)g_0(x,y)=(x+\alpha^3)(\alpha^5 x^2+x+\alpha^6 y+\alpha^5) \\ &= \alpha^5 x^3+\alpha^3 x^2+\alpha^2 x+\alpha^6 xy+\alpha^2 y+\alpha \\ g_1(x,y) &:= \alpha^3 g_1(x,y)-\alpha^6 f(x,y) \\ &= \alpha^3((\alpha^3 x+\alpha^5)y+x^2+\alpha^3 x+1)-\alpha^6(\alpha^5 x^2+x+\alpha^6 y+\alpha^5) \\ &= (\alpha^6 x+\alpha^6)y+\alpha^6 x^2+\alpha^6 \end{aligned}$$

が得られる。

以上から、$xy \prec x^3$ に注意すれば、補間多項式

$$Q(x,y)=(\alpha^6 x+\alpha^6)y+\alpha^6 x^2+\alpha^6$$

が得られる。

2. $Q(x,y)=Q_1(x)y+Q_0(x)$ とすると、

$$\begin{aligned} Q_0(x) &= \alpha^6 x^2+\alpha^6 \\ Q_1(x) &= \alpha^6 x+\alpha^6 \end{aligned}$$

が得られる。$Q_0(x)$ を $Q_1(x)$ で割ると、商 $q(x)=x+1$ と余り $r(x)=0$ となり、余りが零なので送信符号語に対応する多項式は $x+1$ となる。また、これに対応する符号語は $(0,\alpha^3,\alpha^6,\alpha)$ となる。

[演習 **11.2**]

1. α は $\mathbb{F}_8$ の原始元なので、RS(n,k) 符号の生成行列は、

$$G=\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \end{bmatrix}$$

となる。

2. 定理 11.2 において $A = G$、$s = 3$ とおけば、

$$H = B = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \end{bmatrix}$$

が得られる。

3. 符号多項式の性質から

$$\begin{aligned} r(\alpha) &= c(\alpha) + e_i\alpha^i = e_i\alpha^i \\ r(\alpha^2) &= c(\alpha^2) + e_i(\alpha^2)^i = e_i(\alpha^i)^2 \\ r(\alpha^3) &= c(\alpha^3) + e_i(\alpha^3)^i = e_i(\alpha^i)^3 \end{aligned}$$

が成り立つ。従って、$r(\alpha)$、$r(\alpha^2)$、$r(\alpha^3)$ は受信語に対するシンドロームを表している。単一誤りの場合、これらのシンドロームを用いて、

$$\frac{r(\alpha^2)}{r(\alpha)} = \frac{e_i(\alpha^i)^2}{e_i(\alpha^i)} = \alpha^i$$

から誤り位置 i を、また

$$\frac{r(\alpha) \cdot r(\alpha^2)}{r(\alpha^3)} = \frac{e_i(\alpha)^i \cdot e_i(\alpha^2)^i}{e_i(\alpha^3)^i} = e_i$$

から誤り値 e_i を求め、受信多項式から誤り多項式 $e_i x^i$ を減ずれば、送信された符号多項式が得られる。

12章の演習問題の解答

[演習 **12.1**] $\alpha^4 = \alpha + 1$ を利用すると、$\mathbb{F}_{16}$ のべき表示と多項式表示の対応は次の表で与えられる。

べき表示	多項式表示	べき表示	多項式表示
α	α	α^9	$\alpha^3 + \alpha$
α^2	α^2	α^{10}	$\alpha^2 + \alpha + 1$
α^3	α^3	α^{11}	$\alpha^3 + \alpha^2 + \alpha$
α^4	$\alpha + 1$	α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$
α^5	$\alpha^2 + \alpha$	α^{13}	$\alpha^3 + \alpha^2 + 1$
α^6	$\alpha^3 + \alpha^2$	α^{14}	$\alpha^3 + 1$
α^7	$\alpha^3 + \alpha + 1$	α^{15}	1
α^8	$\alpha^2 + 1$	—	—

1. 定理 10.1 より、RS$(15, 11)$ 符号の最小距離は $15 - 11 + 1 = 5$ である。
2. 定理 3.1 と 1. より、RS$(15, 11)$ 符号は $\lfloor \frac{15-11}{2} \rfloor = 2$ 個までの誤りを訂正できる。
3. まず、シンドロームを計算すると、

$$
\begin{aligned}
S_1 = r(\alpha) &= \alpha^{10} + \alpha^{11} + \alpha^6 = \alpha^8 \\
S_2 = r(\alpha^2) &= \alpha^{10} + \alpha^{12} + \alpha^9 = \alpha \\
S_3 = r(\alpha^3) &= \alpha^{10} + \alpha^{13} + \alpha^{12} = \alpha^8 \\
S_4 = r(\alpha^4) &= \alpha^{10} + \alpha^{14} + \alpha^{15} = \alpha^{12}
\end{aligned}
$$

が得られ、誤り位置多項式の係数を定める連立方程式

$$
\begin{bmatrix} \alpha^8 & \alpha & \alpha^8 \\ \alpha & \alpha^8 & \alpha^{12} \end{bmatrix} \begin{bmatrix} Q_{1,0} \\ Q_{1,1} \\ Q_{1,2} \end{bmatrix} = \mathbf{0}
$$

となる。この方程式を解くため、左辺の行列に対して行基本変形を行うと

$$
\begin{bmatrix} 1 & \alpha^8 & 1 \\ 0 & 1 & \alpha \end{bmatrix} \begin{bmatrix} Q_{1,0} \\ Q_{1,1} \\ Q_{1,2} \end{bmatrix} = \mathbf{0}
$$

が得られる。ここで、左辺の行列の階数は 2 なので、最小次数の多項式 $Q_1(x)$ は 2 次であり、$Q_{1,2} = 1$ として、$Q_{1,1}$、$Q_{1,0}$ の順で解を求めればよく、

$$
\begin{aligned}
Q_{1,2} &= 1 \\
Q_{1,1} &= -\alpha Q_{1,2} = \alpha \\
Q_{1,0} &= -\alpha^8 Q_{1,1} - Q_{1,2} = \alpha^9 + 1 = \alpha^7
\end{aligned}
$$

となる。これから、誤り位置多項式

$$Q_1(x) = x^2 + \alpha x + \alpha^7$$

が得られる。

次に、誤り位置多項式の根を求めると、

$$Q_1(\alpha^2) = \alpha^4 + \alpha^3 + \alpha^7 = 0$$
$$Q_1(\alpha^5) = \alpha^{10} + \alpha^6 + \alpha^7 = 0$$

なので、α^2 と α^5 が根となり、その指数部が 2 と 5 であることから誤り多項式は、

$$e(x) = e_2 x^2 + e_5 x^5$$

と書ける。

最後に、連立不等式

$$\begin{bmatrix} \alpha^2 & \alpha^5 \\ \alpha^4 & \alpha^{10} \end{bmatrix} \begin{bmatrix} e_2 \\ e_5 \end{bmatrix} = \begin{bmatrix} \alpha^8 \\ \alpha \end{bmatrix}$$

を解いて、誤りの値 e_2, e_5 を求めると

$$\begin{bmatrix} e_2 \\ e_5 \end{bmatrix} = \begin{bmatrix} \alpha^2 & \alpha^{12} \\ \alpha^{11} & \alpha^9 \end{bmatrix} \begin{bmatrix} \alpha^8 \\ \alpha \end{bmatrix} = \begin{bmatrix} \alpha^9 \\ \alpha^2 \end{bmatrix}$$

となり、誤り多項式は

$$e(x) = \alpha^9 x^2 + \alpha^2 x^5$$

となる。これから、送信符号語 $c(x)$ は、

$$c(x) = r(x) - e(x) = \alpha^{10} + \alpha^{10} x + \alpha^9 x^2 + \alpha^3 x^3 + \alpha^2 x^5$$

となる。

13 章の演習問題の解答

[演習 **13.1**]

1. x^7-1 を既約多項式の積に因数分解すれば、

$$x^7-1=(x-1)(x^3+x+1)(x^3+x^2+1)$$

となり、x^7-1 は $g(x)$ で割り切れることが分る。

2. 多項式 $i(x)$ に対応する符号多項式は $i(x)g(x)$ によって与えられるので、$1+x^3$,x,$x+x^2+x^3$ に対応する符号多項式は、それぞれ、

$$\begin{aligned}(1+x^3)(1+x^2+x^3) &= 1+x^2+x^5+x^6\\ x(1+x^2+x^3) &= x+x^3+x^4\\ (x+x^2+x^3)(1+x^2+x^3) &= x+x^2+x^6\end{aligned}$$

である。

3. 符号語多項式に対応する情報多項式を得るには、符号多項式を $g(x)$ で割って得られる商を求めればよい。従って、$x^2+x^4+x^5$,$1+x+x^2+x^4$,$x^2+x^3+x^4+x^6$ に対応する多項式は、それぞれ

$$\begin{aligned}(x^2+x^4+x^5)\div(1+x^2+x^3) &= x^2\\ (1+x+x^2+x^4)\div(1+x^2+x^3) &= 1+x\\ (x^2+x^3+x^4+x^6)\div(1+x^2+x^3) &= x^2+x^3\end{aligned}$$

である。

[演習 **13.2**]

1. $x^{15}-1$ を既約多項式の積に因数分解すると、

$$x^{15}-1=(x-1)(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x^4+x^3+1) \qquad (1)$$

となる。

2. 符号長 15 の 2 元巡回符号の生成多項式 $g(x)$ は $x^{15}-1$ の因子であるので 2^5 個ある。従って、巡回符号は 32 種類ある。しかしながら、$g(x)=1$ から生成される巡回符号は $\mathbb{F}_2^{15}$ そのものであり $g(x)=x^{15}-1$ から生成される巡回符号は零ベクトルだけから成る符号である。従って、巡回符号として意味のあるもの (非自明なもの) は 30 個である。

3. 定理 13.1 より、次元 11 の巡回符号の生成多項式の次数は、$\deg g(x)=15-11=4$ である。従って、次元 11 の巡回符号の生成多項式は、式 (1) の因数の中から、その積の次数が 4 になるものを選べばよいから、

$$x^4+x+1,\quad x^4+x^3+x^2+x+1,\quad x^4+x^3+1$$

である。

4. 構成可能な生成多項式の $g(x)$ の次数は、$0, 1, \cdots, 14$ なので、巡回符号が構成可能な次元は $1, \cdots, 15$ である。

14 章の演習問題の解答

[演習 **14.1**]

1. $h(x) = \frac{x^{15}-1}{g(x)}$ とおくと、

$$h(x) = \frac{x^{15}-1}{x^4+x+1} = x^{11}+x^8+x^7+x^5+x^3+x^2+x+1$$

を得る。従って、13.2 節の議論から、パリティ検査行列は

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

となる。

2. 生成多項式 $g(x) = x^4+x+1$ は原始既約多項式であるので、根 $\alpha, \alpha^2, \alpha^4, \alpha^8$ をもつ。但し、α は $g(\alpha) = 0$ を満足する原始元である。従って、生成多項式は 2 つの連続した根 α, α^2 を持つので、定理 14.4 より最小距離は 3 以上であることが分かる。また、 生成多項式 $g(x)$ の項の数が 3 であるので、 符号 C は重み 3 の符号語を持つ。 以上のことから、最小距離は 3 である。

3. 1. で求めたパリティ検査行列を見ると、$\mathbb{F}_2^4$ に属する非零の全ての 4 次元ベクトルが列に現れている。従って、 この符号は 2 元ハミング符号であることが分かる。

4. 定理 14.1 と $h(x)$ より、双対符号の生成多項式は

$$g^{\perp}(x) = 1+x^3+x^4+x^6+x^8+x^9+x^{10}+x^{11}$$

である。従って、定理 13.1 より、次元は $15 - \deg g^{\perp}(x) = 15-11 = 4$ である。

演習 **14.2**

1. 2 個の誤りを訂正可能な BCH 符号の最小距離 d は、定理 3.1 より、$d \geq 2\cdot 2+1 = 5$ を満たす。従って、$t = 2$ とおき、BCH 符号の生成多項式 $g(x)$ を

$$g(x) = \mathrm{LCM}\{m_1(x), m_2(x), m_3(x), m_4(x)\}$$

によって定めれば、2 個の誤りを訂正可能となる。但し、$m_i(x)$ は $\alpha^i \in \mathbb{F}_{2^4}$ の $\mathbb{F}_2$ 上の最小多項式であり、α は $\mathbb{F}_{2^4}$ の原始元である。特に、$g(x)$ は $\mathbb{F}_2$ 上の多項式なので、

$$g(x) = \mathrm{LCM}\{m_1(x), m_3(x)\}$$

である。従って、原始元 α の満たす最小多項式が x^4+x+1 の場合は

$$g(x) = (x^4+x+1)(x^4+x^3+x^2+x+1)$$

であり、原始元 α の満たす最小多項式が $x^4 + x^3 + 1$ の場合は

$$g(x) = (x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$$

である。

2. $\deg g(x) = 8$ なので、定理 13.1 より、符号の次元は 7 である。

15 章の演習問題の解答

[演習 **15.1**]

(a) 符号長は $15 = 2^4 - 1$ であり、設計距離 $3 = 2t + 1$ から、$t = 1$ を得るので、表 15.1 と表 15.3 から、BCH 符号の生成多項式、次元、ならびに最小距離の下限は、

$$\text{生成多項式} : m_1(x) = x^4 + x + 1, \quad \text{次元} : 11, \quad \text{最小距離} : 3$$

となる。

(b) 設計距離 $5 = 2t + 1$ から、$t = 2$ を得るので、BCH 符号の生成多項式、次元、ならびに最小距離の下限は、

$$\text{生成多項式} : m_1(x)m_3(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1),$$
$$\text{次元} : 7, \quad \text{最小距離} : 5$$

となる。

(c) 設計距離 $7 = 2t + 1$ から、$t = 3$ を得るので、BCH 符号の生成多項式、次元、ならびに最小距離の下限は、

$$\text{生成多項式} : m_1(x)m_3(x)m_5(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1),$$
$$\text{次元} : 3, \quad \text{最小距離} : 7$$

となる。

(d) 設計距離 $9 = 2t + 1$ から、$t = 4$ を得るので、BCH 符号の生成多項式、次元、ならびに最小距離の下限は、

$$\text{生成多項式} : m_1(x)m_3(x)m_5(x)m_7(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) \times (x^2 + x + 1)(x^4 + x^3 + 1),$$
$$\text{次元} : 1, \quad \text{最小距離} : 15$$

となる。

[演習 **15.2**] $\alpha^4 = \alpha + 1$ を利用すると、$\mathbb{F}_{16}$ のべき表示と多項式表示の対応は次のようになる。

べき表示	多項式表示	べき表示	多項式表示
α	α	α^9	$\alpha^3 + \alpha$
α^2	α^2	α^{10}	$\alpha^2 + \alpha + 1$
α^3	α^3	α^{11}	$\alpha^3 + \alpha^2 + \alpha$
α^4	$\alpha + 1$	α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$
α^5	$\alpha^2 + \alpha$	α^{13}	$\alpha^3 + \alpha^2 + 1$
α^6	$\alpha^3 + \alpha^2$	α^{14}	$\alpha^3 + 1$
α^7	$\alpha^3 + \alpha + 1$	α^{15}	1
α^8	$\alpha^2 + 1$	—	—

1. 生成多項式 $\mathbb{F}_2$ 上の原始多項式なので、

$$g(x) = m_1(x)m_3(x)m_{2\cdot 3-1}(x)$$

と考えれば、$t = 3$ であり、設計距離は $2t + 1 = 7$ であることがわかる。

2. 定理 14.4 と、生成多項式 $g(x)$ の重みが 7 であることから、この符号の最小距離は 7 である。従って、6 個のシンドロームを計算する。

$$\begin{aligned}
S_1 &= r(\alpha) = 1 + \alpha^2 + \alpha^7 + \alpha^8 + \alpha^{11} = \alpha^8 \\
S_2 &= r(\alpha^2) = r(\alpha)^2 = \alpha \\
S_3 &= r(\alpha^3) = 1 + \alpha^6 + \alpha^6 + \alpha^9 + \alpha^3 = \alpha^4 \\
S_4 &= r(\alpha^4) = r(\alpha^2)^2 = \alpha^2 \\
S_5 &= r(\alpha^5) = 1 + \alpha^5 + \alpha^{10} = 0 \\
S_6 &= r(\alpha^6) = r(\alpha^3)^2 = \alpha^8
\end{aligned}$$

3. 誤り位置多項式を求めるために、次の連立方程式を解く。

$$\begin{bmatrix} \alpha^8 & \alpha & \alpha^4 & \alpha^2 \\ \alpha & \alpha^4 & \alpha^2 & 0 \\ \alpha^4 & \alpha^2 & 0 & \alpha^8 \end{bmatrix} \begin{bmatrix} Q_{1,0} \\ Q_{1,1} \\ Q_{1,2} \\ Q_{1,3} \end{bmatrix} = \mathbf{0}$$

行基本変形を行うと、

$$\begin{bmatrix} 1 & \alpha^8 & \alpha^{11} & \alpha^9 \\ 0 & 1 & \alpha^8 & \alpha^{11} \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} Q_{1,0} \\ Q_{1,1} \\ Q_{1,2} \\ Q_{1,3} \end{bmatrix} = \mathbf{0}$$

を得る。左辺の行列の階数は 2 なので、最小次数の多項式 $Q_1(x)$ は 2 次であり、$Q_{1,3} = 0$、$Q_{1,2} = 1$ として、

$$\begin{aligned}
Q_{1,1} &= -\alpha^8 Q_{1,2} - \alpha^{11} Q_{1,3} = \alpha^8 \\
Q_{1,0} &= -\alpha^8 Q_{1,1} - \alpha^{11} Q_{1,2} - \alpha^9 Q_{1,3} = \alpha^6
\end{aligned}$$

となる。これから、誤り位置多項式

$$Q_1(x) = x^2 + \alpha^8 x + \alpha^6$$

を得る。

4. $Q_1(x) = 0$ の根は、α^9 と α^{12} である。従って、誤り多項式は

$$e(x) = x^9 + x^{12}$$

である。

5. 受信多項式から誤り多項式を減ずることで、送信語は

$$c(x) = r(x) - e(x) = 1 + x^2 + x^7 + x^8 + x^9 + x^{11} + x^{12}$$

であることが分る。