2019年度 情報数理特論B　練習問題4

学籍番号：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿　氏名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

問題の質問や不明な点は、授業終了後またはオフィスアワーを利用して、質問してください。

出題者： 幸山 直人

出題日： 2019年6月18日 (火)

$\boxed{\textbf{問 1}}$ 2 元符号 GF(2) $= \{0, 1\}$ 上の情報 $\boldsymbol{i} = (i_1, i_2, i_3)$ に対する検査ビット $(p_1, p_2, p_3, p_4, p_5)$ を関係式

$$\begin{cases} p_1 = i_1 + i_2 + i_3 \\ p_2 = i_1 \\ p_3 = \quad\;\; i_2 \\ p_4 = \qquad\quad i_3 \\ p_5 = i_1 + i_2 + i_3 \end{cases}$$

で与え、符号語が $\boldsymbol{x} = (i_1, i_2, i_3, p_1, p_2, p_3, p_4, p_5)$ となる [8,3] 線形符号を構成する。この線形符号について、次の (1)〜(5) の問いに答えなさい。

(1) この符号の生成行列 G および検査行列 H を求めなさい。

解答例 定義より、直ちに

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

を得る。

(2) 以下の空欄を埋め、この符号の符号語 $\boldsymbol{x}_j$ $(j = 0, 1, 2, 3, 4, 5, 6, 7)$ を全て求めなさい。

解答例 i_1, i_2, i_3 を変数 (パラメータ) とし、関係式

$$\begin{cases} p_1 = i_1 + i_2 + i_3 \\ p_2 = i_1 \\ p_3 = \quad\;\; i_2 \\ p_4 = \qquad\quad i_3 \\ p_5 = i_1 + i_2 + i_3 \end{cases}$$

を計算することで、直ちに符号語 $\boldsymbol{x}_j$ が得られる。

注意： i_1, i_2, i_3 は、それぞれ 0 または 1 の値をとる。

$\boldsymbol{x}_0 = (0, 0, 0, 0, 0, 0, 0, 0)$, $\boldsymbol{x}_1 = (0, 0, 1, 1, 0, 0, 1, 1)$, $\boldsymbol{x}_2 = (0, 1, 0, 1, 0, 1, 0, 1)$,
$\boldsymbol{x}_3 = (0, 1, 1, 0, 0, 1, 1, 0)$, $\boldsymbol{x}_4 = (1, 0, 0, 1, 1, 0, 0, 1)$, $\boldsymbol{x}_5 = (1, 0, 1, 0, 1, 0, 1, 0)$,
$\boldsymbol{x}_6 = (1, 1, 0, 0, 1, 1, 0, 0)$, $\boldsymbol{x}_7 = (1, 1, 1, 1, 1, 1, 1, 1)$

(3) この符号の最小距離 $d_{\min}$ を求めなさい。

解答例 1　テキストの 48 ページの「2 元符号の場合、2 つの異なる符号語間のハミング距離は、それら符号語の和 (排他的論理和) によって得られるベクトルに含まれる 1 の個数と一致します。さらに、線形符号では符号語の和は再び符号語になります。したがって、零ベクトルでない符号語に含まれる 1 の個数の最小値が最小距離に一致します。」より、符号語 $\boldsymbol{x}_j$ $(j = 1, 2, 3, 4, 5, 6, 7)$ に含まれる 1 の個数は 4 個が最小である。したがって、最小距離 $d_{\min} = 4$ である。

解答例 2　異なる符号語 $\boldsymbol{x}_j$, $\boldsymbol{x}_k$ $(j \neq k)$ に対して、それぞれ $d_H(\boldsymbol{x}_j, \boldsymbol{x}_k)$ を求めると

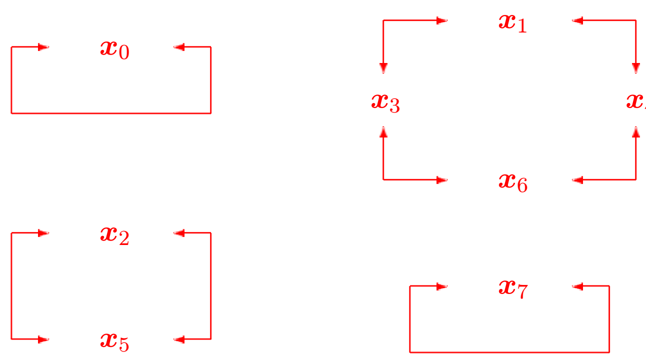
d_H	$\boldsymbol{x}_0$	$\boldsymbol{x}_1$	$\boldsymbol{x}_2$	$\boldsymbol{x}_3$	$\boldsymbol{x}_4$	$\boldsymbol{x}_5$	$\boldsymbol{x}_6$	$\boldsymbol{x}_7$
$\boldsymbol{x}_0$		4	4	4	4	4	4	8
$\boldsymbol{x}_1$			4	4	4	4	8	4
$\boldsymbol{x}_2$				4	4	8	4	4
$\boldsymbol{x}_3$					8	4	4	4
$\boldsymbol{x}_4$						4	4	4
$\boldsymbol{x}_5$							4	4
$\boldsymbol{x}_6$								4
$\boldsymbol{x}_7$								

となる。したがって、最小距離 $d_{\min} = 4$ である。

注意 : 1 個の誤りであれば訂正可能であるが、2 個の誤りであれば検出のみ可能で訂正はできない。

(4) この符号が巡回符号であることを示しなさい。

解答例　(2) で求めた符号語をそれぞれ巡回置換すると下図の関係が得られ、直ちに巡回符号であることが示される。



。

(5) この符号が $G(x)=1+x+x^4+x^5$ を生成多項式とする [8,3] 巡回符号と同値な符号であることを証明しなさい。

解答例　巡回符号の定義より、符号語 $\boldsymbol{x}'$ は

$$\boldsymbol{x}'=(p_0',p_1',p_2',p_3',p_4',i_0',i_1',i_2')$$

となり (テキストの 57 ページ)、検査行列 H' は

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

となる (テキストの 58 ページ)。このとき、符号語 $\boldsymbol{x}'$ は $\boldsymbol{x}'H'^T=\boldsymbol{0}$ を満たすから、関係式

$$\begin{cases}p_0'+i_0'+i_1'+i_2'=0\\p_1'+i_0'=0\\p_2'+i_1'=0\\p_3'+i_2'=0\\p_4'+i_0'+i_1'+i_2'=0\end{cases}\cdots(*1)\quad\Longleftrightarrow\quad\begin{cases}p_0'=i_0'+i_1'+i_2'\\p_1'=i_0'\\p_2'=i_1'\\p_3'=i_2'\\p_4'=i_0'+i_1'+i_2'\end{cases}\cdots(*2)$$

を得る。したがって、上記の関係式 $(*2)$ が [8,3] 線形符号の関係式と一致することより、この [8,3] 巡回符号は [8,3] 線形符号と同値な符号となる (p_k' は p_{k+1} で、i_j' は i_{j+1} で、それぞれ読み換える)。

注意 1 : 巡回符号の検査行列は線形符号の検査行列の列を入れ替えたもの (列に関する基本変形) だから、$(*1)$ より

$$\begin{cases}i_0'+i_1'+i_2'+p_0'=0\\i_0'+p_1'=0\\i_1'+p_2'=0\\i_2'+p_3'=0\\i_0'+i_1'+i_2'+p_4'=0\end{cases}\Longleftrightarrow\begin{bmatrix}1&1&1&1&0&0&0&0\\1&0&0&0&1&0&0&0\\0&1&0&0&0&1&0&0\\0&0&1&0&0&0&1&0\\1&1&1&0&0&0&0&1\end{bmatrix}\begin{bmatrix}i_0'\\i_1'\\i_2'\\p_0'\\p_1'\\p_2'\\p_3'\\p_4'\end{bmatrix}=\boldsymbol{0}$$

$$\left(\Longleftrightarrow\quad H\boldsymbol{x}'^T=\boldsymbol{0}\quad(H'\text{ではないことに注意})\quad\Longleftrightarrow\quad\left(H\boldsymbol{x}'^T\right)^T=\boldsymbol{0}^T\quad\Longleftrightarrow\quad\boldsymbol{x}'H^T=\boldsymbol{0}^T\right)$$

とし (上記のように並び順を変えて)、検査行列が一致することを示しても良い。
注意 2 : 巡回符号の検査行列 H' によって得られる解集合と線形符号の検査行列 H によって得られる解集合が一致することを示しても良い ($\boldsymbol{x}'H'^T=\boldsymbol{0}\iff\boldsymbol{x}'H^T=\boldsymbol{0}$)。
注意 3 : 巡回符号であれば必ず線形符号となるが、線形符号だからといって必ず巡回符号になるとは限らない。