代数系と符号理論 (O) 第 1 回宿題
提出期限 5 月 13 日 (火) 講義終了時

制作：植松友彦

宿題専用のノートを１冊用意し、
問題の解答をそのノートに書き、
自己採点した後、ノートを提出せよ

[問題 **1**] 次の 2 元体上のベクトルの集合 S が線形独立かどうか調べよ。もし、線形独立でないならば、線形従属になっている部分集合を一つ示せ。

(a) $S = \{(1101), (1110), (1011)\}$

(b) $S = \{(101), (011), (110), (010)\}$

(c) $S = \{(1000), (1100), (1110), (1111)\}$

(d) $S = \{(1101), (0111), (1100), (0011)\}$

(e) $S = \{(1000), (0100), (0010), (0001)\}$

(f) $S = \{(1100), (1010), (1001), (0101)\}$

[問題 **2**] 2 元線形符号の生成行列が

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

であるとき、次の情報ベクトルを符号化せよ。

(a) $\boldsymbol{u} = (000)$ (b) $\boldsymbol{u} = (100)$ (c) $\boldsymbol{u} = (111)$

[問題 **3**] 2 元線形符号 C が次の生成行列 G を有するとき、パリティ検査行列 H を求めよ。

(a)

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

(b)

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

(c)

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

[**問題 4**] 次の符号に対して、生成行列とパリティ検査行列をそれぞれ 1 つ求めよ。

(a) $C = \{(0000), (1001), (0110), (1111)\}$

(b) $C = \{(00000), (11111)\}$

(c) $C = \{(00000), (11110), (01111), (10001)\}$

(d) $C = \{(000000), (101010), (010101), (111111)\}$

(e) $C = \{(000), (001), (010), (011)\}$

(f) $C = \{(00000), (11100), (00111), (11011)\}$

[**問題 5**] 次のベクトルの線形結合全体の集合によって定める線形符号の生成行列とパリティ検査行列をそれぞれ 1 つ求めよ。

(a) $\{(11111111), (11110000), (11001100), (10101010)\}$

(b) $\{(11111100), (11110011), (11001111), (00111111)\}$

(c) $\{(100100100), (010010010), (001001001), (111111111)\}$

(d) $\{(10101), (01010), (11111), (00011), (10110)\}$

(e) $\{(1010), (0101), (1111)\}$

(f) $\{(101101), (011010), (110111), (000111), (110000)\}$

(g) $\{(1001011), (0101010), (1001100), (0011001), (0000111)\}$

[**問題 6**] 2 元符号 C の双対符号 $C^{\perp}$ の基底が $\{(11110000), (00001111), (10000001)\}$ であるとき、C の次元と符号語の総数を求めよ。
[**問題 7**] 2 元符号 C の生成行列が

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

で与えられるとき、次の問いに答えよ。

(1) 符号 C の符号長と次元を求めよ。

(2) 符号 C の $[I_3\ P]$ の形をした生成行列を求めよ。

(3) 符号 C のパリティ検査行列を求めよ。

(4) 双対符号 $C^{\perp}$ の生成行列とパリティ検査行列を求めよ。

(5) 符号 C の最小距離を求めよ。

[問題 **8**] 符号 C をパリティ検査行列

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

によって定まる 2 元線形符号とする。

(1) 定理 3.3 を用いて、この符号の最小距離を求めよ。

(2) この符号の全ての符号語を求めて、定理 2.1 が成立していることを確認せよ。

[問題 **9**]

(1) $m = 3, 4, 5, 6$ の場合に対する 2 元ハミング符号のパラメータ (符号長、次元、最小距離) を求めよ。また、$m = 4$ の場合についてパリティ検査行列を示せ。

(2) $m = 3, 4, 5, 6$ の場合に対する 2 元拡大ハミング符号のパラメータ (符号長、次元、最小距離) を求めよ。また、$m = 4$ の場合についてパリティ検査行列を示せ。

[問題 **10**] $m = 3$ の場合の 2 元ハミング符号の双対符号について次の問いに答えよ。

(1) 生成行列 G を求めよ。

(2) この符号の全ての符号語を求めよ。

(3) どの 2 つの符号語も同じ距離を有することを示せ。

(4) 一般的な 2 元ハミング符号の双対符号について、その最小距離を求めよ。

[問題 **11**] 次の 2 元線形符号 C について標準配列を作れ。

(1) $C = \{(0000), (1001), (0101), (1100)\}$

(2) $C = \{(00000), (10100), (01011), (11111)\}$

(3) $C = \{(0000), (1111)\}$

[問題 **12**] 次のパリティ検査行列 H を有する 2 元線形符号 C について標準配列を作れ。また、与えられた受信語をシンドローム復号法によって復号せよ。

(1)

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

受信語 (1100)

(2)

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

受信語 (111010)

[問題 **13**]

(1) Varshamov-Gilbert 限界を用いて、最小距離 3 を持つ 2 元 $(15,k)$ 符号が存在するような k の値の下界を求めよ。

(2) ハミング限界を用いて、最小距離 3 を持つ 2 元 $(15,k)$ 符号が存在するような k の値の上界を求めよ。

(3) Singleton 限界を用いて、最小距離 3 を持つ 2 元 $(15,k)$ 符号が存在するような k の値の上界を求めよ。

解答

[問題 **1**]

(a) 線形独立

(b) $(101)+(011)=(110)$ から線形従属

(c) 線形独立

(d) 線形独立

(e) 線形独立

(f) $(1100)+(1001)=(0101)$ から線形従属

[問題 **2**]

(a) (0000000)　(b) (1000111)　(c) (1110001)

[問題 **3**] H 行列の 1 つを示す。この他に、(1) 行ベクトルが線形独立で、(2)$GH^T=O$ が成り立つ行列 H ならば良い。

(a)

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

(b)

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

(c)

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

[問題 **4**] 生成行列 G とパリティ検査行列 H の一例を示す。

(a)

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

(b)

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

(c)

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

(d)

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

(e)

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

(f)

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

[問題 5] 生成行列 G とパリティ検査行列 H の一例を示す。

(a)

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

(b)

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

(c)

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

(d)

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

(e)

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

(f)

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

(g)

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

[問題 **6**] $C^{\perp}$ の生成行列 G とパリティ検査行列 H は、

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

である。従って、C の生成行列は H に等しいので、次元は 5 であり、符号語の総数は $2^5 = 32$ である。

[問題 **7**]

(1) 符号長は 6 で、次元は 3。

(2)

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

(3)

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

(4)

$$G^{\perp} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \quad H^{\perp} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

(5) 最小距離は 3。

[問題 **8**]

(1) $d_{min} = 3$

(2) この符号の生成行列は

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

であるから、全ての符号語は (00000), (10110), (01011), (11101) の 4 つである。これから、非零の最小重みは 3 であり、定理 2.1 の成立が分る。

[問題 **9**]

(1)

m	符号長	次元	最小距離
3	7	4	3
4	15	11	3
5	31	26	3
6	63	57	3

$m = 4$ のパリティ検査行列は、

$$H = \begin{bmatrix} 101010101010101 \\ 011001100110011 \\ 000111100001111 \\ 000000011111111 \end{bmatrix}$$

となる。

(2)

m	符号長	次元	最小距離
3	8	4	4
4	16	11	4
5	32	26	4
6	64	57	4

$m = 4$ のパリティ検査行列は、

$$H = \begin{bmatrix} 1010101010101010 \\ 0110011001100110 \\ 0001111000011110 \\ 0000000111111110 \\ 1111111111111111 \end{bmatrix}$$

となる。

[問題 **10**]

(1)

$$G = \begin{bmatrix} 1010101 \\ 0110011 \\ 0001111 \end{bmatrix}$$

(2)

$$\{(0000000), (1010101), (0110011), (0001111), (1100110), (1011010), (0111100), (1101001)\}$$

(3) 非零の全ての符号語の重みが全て 4 なので、どの 2 つの符号語の距離は 4 である。

(4) $d_{min} = 2^{(m-1)}$

[問題 **11**] 次の 2 元線形符号 C について標準配列を作れ。

(1)

(00)	(0000)	(1001)	(0101)	(1100)
(01)	(1000)	(0001)	(1101)	(0100)
(10)	(0010)	(1011)	(0111)	(1110)
(11)	(0011)	(1010)	(0110)	(1111)

(2)

(000)	(00000)	(10100)	(01011)	(11111)
(100)	(10000)	(00100)	(11011)	(01111)
(011)	(01000)	(11100)	(00011)	(10111)
(010)	(00010)	(10110)	(01001)	(11101)
(001)	(00001)	(10101)	(01010)	(11110)
(110)	(00110)	(10010)	(01101)	(11001)
(101)	(00101)	(10001)	(01110)	(11010)
(111)	(11000)	(01100)	(10011)	(00111)

(3)

(000)	(0000)	(1111)
(111)	(1000)	(0111)
(100)	(0100)	(1011)
(010)	(0010)	(1101)
(001)	(0001)	(1110)
(110)	(0110)	(1001)
(101)	(0101)	(1010)
(011)	(0011)	(1100)

[問題 **12**] 次のパリティ検査行列 H を有する 2 元線形符号 C について標準配列を作れ。また、与えられた受信語をシンドローム復号法によって復号せよ。

(1)

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

(00)	(0000)	(1010)	(0111)	(1101)
(10)	(1000)	(0010)	(1111)	(0101)
(11)	(0100)	(1110)	(0011)	(1001)
(01)	(0001)	(1011)	(0110)	(1100)

受信語 (1100) に対応するシンドロームは (01) なので、誤りベクトルは (0001) となり、受信語は (1101) に復号される。

(2)

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

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

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

受信語 (111010) のシンドロームは (010) なので、対応する誤りベクトルは (000010) となり、受信語は (111000) に復号される。

[問題 **13**]

(1) Varshamov-Gilbert 限界より、

$$\begin{aligned} 1 + \binom{14}{1} &= 1 + 14 \\ &= 15 \\ &< 2^4 \\ &= 2^{15-11} \end{aligned}$$

を得る。従って、k の下界は 11 である。

(2) $q=2$、$n=15$ である。また最小距離は 3 なので、定理 3.1 より、$\lfloor\frac{3-1}{2}\rfloor=1$ 個以下のすべての誤りを訂正可能である。従って、$t=1$ とすれば、ハミング限界より、

$$2^k\sum_{j=0}^{1}\binom{15}{j} \quad\leq\quad 2^{15}$$

を得る。さらに、左辺を式変形していけば、

$$\begin{aligned}2^k\sum_{j=0}^{1}\binom{15}{j}\leq 2^{15} \quad&\Longleftrightarrow\quad 2^k\left(\binom{15}{0}+\binom{15}{1}\right)\leq 2^{15}\\ &\Longleftrightarrow\quad 2^k16\leq 2^{15}\\ &\Longleftrightarrow\quad 2^{k+4}\leq 2^{15}\end{aligned}$$

を得る。従って、k の上界は 11 である。

(3) Singleton 限界より、

$$3\leq 15-k+1 \quad\Longleftrightarrow\quad 3\leq 16-k$$

を得る。従って、k の上界は 13 である。