復習問題

1 Hamming 符号 $H(7,4)$ では，長さ 4 の情報ビット $a_1a_2a_3a_4$ $(a_i = 0, 1)$ に対し，検査ビット $c_1c_2c_3$ $(c_i = 0, 1)$ を次の式で定義して付け加え，符号語 $a_1a_2a_3a_4c_1c_2c_3$ を作るのであった．

$$\begin{cases} a_1 + a_2 + a_3 + c_1 \equiv 0 \pmod 2 \\ a_2 + a_3 + a_4 + c_2 \equiv 0 \pmod 2 \\ a_1 + a_2 + a_4 + c_3 \equiv 0 \pmod 2 \end{cases}$$

a) a_i, c_j を $\mathbb{F}_2$ の元とみなし，$\mathbb{F}_2$ 係数の行列 G（生成行列と呼ぶ）を次のように定義する．

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

情報ビット $a_1a_2a_3a_4$ に対応する列ベクトル $\vec{a} = {}^t(a_1, a_2, a_3, a_4)$ に G の転置行列 ${}^TG$ をかけ，${}^TG\vec{a}$ を計算すると符号語 $a_1a_2a_3a_4c_1c_2c_3$ に対応する列ベクトル $u = {}^t(a_1, a_2, a_3, a_4, c_1, c_2, c_3)$ が得られることを示せ．

b) 行列 H（パリティ検査行列と呼ぶ）を次のように定義する．

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

$H^TG = O$ であることを示し，7 次元列ベクトル $\vec{b} = {}^t(b_1, b_2, \ldots, b_7)$ が符号語に対応するならば，$H\vec{b} = \vec{0}$ であることを示せ．

c) $\vec{u}$ は符号語に対応する列ベクトルとするとき，これに雑音 $\vec{e}$ が加わり，$\vec{r} = \vec{u} + \vec{e}$ を受信したとする．いま，雑音は 1bit のみ，すなわち $\vec{e}$ は基本ベクトル（どれか 1 つの成分が 1 でそれ以外は 0）であると仮定する．このとき，$H\vec{r}$（シンドローム）と呼ぶ）は H の列ベクトルのいずれかと一致し，$H\vec{r}$ が第 j 列と一致するなら，$\vec{r}$ の第 j 成分が誤りであることを示せ．

2 $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$ を 3 元体とする．

a) $\mathbb{F}_3$ 上の 2 次のモニック（最高次係数が 1 である多項式）は全部でいくつあるか．そのうち，既約なものはいくつあるか．

b) $f(x) = x^2 + 2x + 2$ とおく．$f(x)$ は既約であることを示せ．

c) $\mathbb{F}_3$ の 2 次拡大 $\mathbb{F}_9 = \mathbb{F}_3[x]/(f(x))$ の生成元 $x \bmod f(x)$ を θ とおく．すなわち，θ を $\theta^2 + 2\theta + 2 = 0$ を満たす元とする．このとき，$\theta^8 = 1$ であることを示せ．また，$\{\theta^k \mid 0 \le k \le 7\} = \mathbb{F}_9^\times = \mathbb{F}_9 - \{0\}$ となることを示せ．

担当： 鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)