4. 符号理論 (誤り訂正符号)

問 4–1. Hamming 距離の定義を述べ、距離の公理を満たすことを確かめよ。

問 4–2. Hamming の球充填上界:

$$q \text{ 元 } (n, M, 2t+1)\text{-符号について、} M \cdot \sum_{s=0}^{t} \binom{n}{s} (q-1)^s \leq q^n$$

について、

(1) これを示せ。
(2) 等号が成り立つような (q, n, M, t) の組を幾つか見付けよ。
(3) 等号を実現する符号を構成せよ (完全符号という)。

問 4–3. $V = \boldsymbol{F}_q^n$ を Hamming 距離 d による距離つき線型空間と見る。等距離自己同型群 $G := \mathrm{Aut}(V, d)$ が、次の 2 種の自己同型で生成されることを示せ。

- 成分の置換
- 或る成分の非零定数倍

問 4–4. 線型 $[n, k, d]$-符号 $\mathcal{C}$ に関する "singleton bound" $k + d \leq n + 1$ を示し、Hamming の球充填上界などと比較せよ。

問 4–5. 奇素数 l に対し、次を示せ。

(1) -1 が mod$l$ で平方剰余 $\iff l \equiv 1 \pmod 4$ (平方剰余の第 1 補助法則)
(2) 2 が mod$l$ で平方剰余 $\iff l \equiv \pm 1 \pmod 8$ (平方剰余の第 2 補助法則)

問 4–6. q を素数冪、l を q と互いに素な素数とし、$R := \boldsymbol{F}_q[X]/(X^l - 1)$ と置く。$\boldsymbol{F}_q$ の代数閉包 $\overline{\boldsymbol{F}_q}$ 内の 1 の原始 l 乗根 $\zeta_l \in \overline{\boldsymbol{F}_q}$ を一つ取って固定し、$F := \boldsymbol{F}_q(\zeta_l)$ と置く。

(1) $f \in R$ に対し、"f に α を代入した値" $f(\alpha) \in \overline{\boldsymbol{F}_q}$ が well-defined に定まるのは、$\alpha = \zeta_l^a$ $(a = 0, 1, \ldots, l-1)$ の時に限る。
(2) $R \otimes_{\boldsymbol{F}_q} F \simeq F^l$ となる。この同型写像を構成せよ。
(3) $f, g \in R$ に対し、$f = g \iff \forall a = 0, 1, \ldots, l-1 : f(\zeta_l^a) = g(\zeta_l^a)$ が成り立つ。

問 4–7. $l \equiv \pm 1 \pmod 8$ である奇素数 l (従って、2 : mod$l$ で平方剰余) に対して、$Q := \boldsymbol{F}_l^{\times 2}, N := \boldsymbol{F}_l^{\times} \smallsetminus \boldsymbol{F}_l^{\times 2}$ と置き、

$$f_Q(X) = \prod_{a \in Q} (X - \zeta_l^a), \qquad f_N(X) = \prod_{a \in N} (X - \zeta_l^a)$$

とする。また、$e_Q, e_N \in R = \boldsymbol{F}_2[X]/(X^l - 1)$ を次で定める:

$$e_Q(X) = \sum_{a \in Q} X^a, \qquad e_N(X) = \sum_{a \in N} X^a.$$

(1) $f_Q(X), f_N(X) \in \boldsymbol{F}_2[X]$ となり、$\boldsymbol{F}_2$ 上で ($\boldsymbol{F}_2[X]$ 内で) $X^l - 1 = (X-1) f_Q(X) f_N(X)$ と分解する。
(2) $e_Q(X), e_N(X)$ が R の直交冪等元 $(e_Q^2 = e_Q, e_N^2 = e_N, e_Q e_N = 0)$ である。
(3) Q, N 上で $e_Q(\zeta_l^a), e_N(\zeta_l^a)$ がそれぞれ 0 または 1 の一定値を取る。(どちらであるかは ζ_l の取り方に依る。)

以下では、$a \in Q$ に対し $e_Q(\zeta_l^a) = 0$ となるように、$\zeta_l \in \overline{\boldsymbol{F}_2}$ が選んであるものとする。

(4) $l \equiv -1 \pmod 8$ のとき、R の ideal として、$(e_Q) = (f_Q), (e_N) = ((X-1) f_N)$ となる。
(5) $l \equiv 1 \pmod 8$ のときはどうなるか。適切に修正せよ。

問 4–8. 平方剰余符号 $\mathcal{Q} := (e_Q) \subset R \simeq (\boldsymbol{F}_2)^l$ に対し、パリティ検査 bit を加えて延長した符号 $\widetilde{\mathcal{Q}} \subset (\boldsymbol{F}_2)^{l+1}$ を考える。成分の添字集合 $\{0, 1, \ldots, l-1\} \sqcup \{\infty\}$ を $\mathbf{P}^1(\boldsymbol{F}_l)$ と同一視するとき、$\mathrm{Aut}(\widetilde{\mathcal{Q}}) \supset \mathrm{PSL}(2, \boldsymbol{F}_l)$ となる。特に、$\mathrm{Aut}(\widetilde{\mathcal{Q}})$ は可移である。

問 4–9. 平方剰余符号 $\mathcal{Q} \subset R$ の最小距離 d について

(1) d が奇数であることを示せ。
(2) "square root bound" $d \geq \sqrt{l}$ を示せ。

問 4–10. 適当な誤り訂正符号について、受信ベクトルの誤りを検出して訂正するプログラムを作れ。