レポート課題 (の主な例) (7/10 配布)

- 暗号理論・計算量の理論の内容については、来週配布のプリントを参照のこと。

5. 概論 (必修課題)

問 5–1. 以下の問の中から 1 つ以上について調べて記せ。但し、参考にした文献 (書籍・ネット上の情報) があれば、それを明記すること。

(1) 実際に使われている符号化・データ圧縮の方式について調べ、その特徴・性質や、何に用いられている／用いるのが適しているか、述べよ。
(2) 実際に使われている誤り訂正符号の方式について調べ、その特徴・性質や、何に用いられている／用いるのが適しているか、述べよ。
(3) 実際に使われている暗号化の方式について調べ、その特徴・性質や、何に用いられている／用いるのが適しているか、述べよ。
(4) その他、高度な情報処理に利用されている数理現象について調べ、その特徴・性質や、何に用いられている／用いるのが適しているか、述べよ。

6. 代数系の基礎事項 (数学領域以外の理工学専攻の受講者のみ)

問 6–1. 本講義内容に表れた代数系 (群・環・体・加群・線型空間など) の基礎事項について、自分で学習したことをまとめよ。

7. 情報理論 (情報源符号化)

問 7–1. 一意符号ではあるが瞬時符号ではないような符号の例を構成し、それと同じ符号語長列を持つ瞬時符号を (なるべく systematic に) 構成せよ。

問 7–2. 瞬時符号であることと語頭符号であることが同値であることを示せ。

問 7–3. 情報源 $\mathcal{S} = (S, P)$ に対し、2 元 Huffman 符号 $\mathcal{C} : S \longrightarrow \{0,1\}^+$ が最適符号であることを、情報源 alphabet の個数 $\#S$ に関する帰納法を用いて、以下の手順で示せ。

(1) 2 元瞬時符号では、最長の符号語は $x0, x1$ ($x \in \{0,1\}^*$) の形で組になって現れる。
(2) 2 元最適符号 $\mathcal{D}$ で、出現確率が最小とその次 (等しいこともある) の 2 つの S の元 s_i, s_j に対して、$\mathcal{D}(s_i) = x0, \mathcal{D}(s_j) = x1$ となるものが存在する。
(3) s_i, s_j をまとめて s' とした情報源 $\mathcal{S}' = (S', P')$ を定式化せよ。(s_i, s_j を縮退させた情報源と呼ぶ。)
(4) $\mathcal{S}'$ の符号 $\mathcal{D}'$ を $\mathcal{D}'(s') = x, \mathcal{D}'|_{S \setminus \{s_i, s_j\}} = \mathcal{D}|_{S \setminus \{s_i, s_j\}}$ で定めるとき、$L(\mathcal{D}) - L(\mathcal{D}') = P(s_i) + P(s_j)$ となる。
(5) $\mathcal{S}$ の Huffman 符号 $\mathcal{C}$ について、$\mathcal{C}(s_i) = y0, \mathcal{C}(s_j) = y1$ ($y \in \{0,1\}^*$) となっているとして一般性を失わない。これより同様に $\mathcal{S}'$ の符号 $\mathcal{C}'$ を構成するとき、$\mathcal{C}'$ は $\mathcal{S}'$ の Huffman 符号である。従って、帰納法の仮定により $\mathcal{S}'$ の最適符号である。
(6) $L(\mathcal{C}) - L(\mathcal{C}') = P(s_i) + P(s_j)$ となる。このことから $L(\mathcal{C}) = L(\mathcal{D})$ となり、$\mathcal{C}$ は $\mathcal{S}$ の最適符号である。

問 7–4. 英文の alphabet の出現頻度の統計を何処かで調べ、それに従って 2 元 Huffman 符号化の符号化関数 $\mathcal{C} : \{a, b, \ldots, z\} \longrightarrow \{0,1\}^+$ を構成せよ。

問 7–5. 関数 $y = p \log \dfrac{1}{p}$ $(0 < p < 1)$、及び 2 値エントロピー関数 $y = H(p) = p \log \dfrac{1}{p} + \overline{p} \log \dfrac{1}{\overline{p}}$ (ここに $\overline{p} := 1 - p$) のグラフの概形を描き、最大値をとる p とその時の値を求めよ。

問 7–6. $\dfrac{1}{2} < p < 1$ である適当な p と幾つかの小さい n (または適当な系列に属する n) とについて、$S = \{a, b\}, P(a) = p$ である情報源 $\mathcal{S} = (S, P)$ に対し、$\mathcal{S}$ の n 次の拡大情報源 $\mathcal{S}^n$ の Huffman 符号 $\mathcal{C}^n$ を構成し、その平均符号長 $L(\mathcal{C}^n)$ と情報源 $\mathcal{S}$ のエントロピー $H(\mathcal{S}) = H(p)$ とを比較してみよ。

8. 符号理論 (誤り訂正符号)

問 8–1. 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 8–2. 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 8–3. $V = \boldsymbol{F}_q^n$ 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 8–4. 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 8–5. 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 8–6. 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 8–7. $l \equiv \pm 1 \pmod 8$ 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 $e_Q(X), e_N(X)$ 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、$\alpha \in Q$ に対し $e_Q(\alpha) = 0$ 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 8–8. 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 8–9. 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 8–10. 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。