

2019 年度 情報数理特論 B 練習問題 3

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 4 日 (火)

問 1 集合 $\{a, b, c, d\}$ から成る符号について、符号語 $\mathbf{x} = (a, b, c, a, d, a, a, c, c, a, b, b, a, d, d)$ と $\mathbf{y} = (a, c, c, a, a, a, a, c, c, a, b, b, a, b, b)$ のハミング距離を求めなさい。

解答例 ハミング距離の定義より、各成分を比較し、異なれば 1、同じであれば 0 とし、その総和を取ればよい。したがって、ハミング距離は

$$d_H(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{15} \delta(x_i, y_i) = 0 + 1 + 0 + 0 + 1 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 1 + 1 = 4$$

となる。

問 2 α をガロア拡大体 $\text{GF}(2^4)$ の原始多項式 $x^4 + x + 1$ の 1 つの根 (原始元) とするとき、次の (1)~(2) の問いに答えなさい。ヒント: $\alpha^4 = \alpha + 1$, $\alpha^{15} = 1$ 。

(1) テキストの表 2.5 (p.43) に習って、以下のガロア拡大体 $\text{GF}(2^4)$ のべき表現とベクトル表現の表を完成しなさい。

解答

べき表現	展開	ベクトル表現
0	0	0000
1	1	0001
α	α	0010
α^2	α^2	0100
α^3	α^3	1000
α^4	$\alpha + 1$	0011
α^5	$\alpha^2 + \alpha$	0110
α^6	$\alpha^3 + \alpha^2$	1100
α^7	$\alpha^3 + \alpha + 1$	1011
α^8	$\alpha^2 + 1$	0101
α^9	$\alpha^3 + \alpha$	1010
α^{10}	$\alpha^2 + \alpha + 1$	0111
α^{11}	$\alpha^3 + \alpha^2 + \alpha$	1110
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$	1111
α^{13}	$\alpha^3 + \alpha^2 + 1$	1101
α^{14}	$\alpha^3 + 1$	1001

(2) 次の①～④を計算し、その値を (1) の表のべき表現で答えなさい。

$$\begin{aligned}
 \textcircled{1} \quad \alpha^5 + \alpha^{10} &= (\alpha^2 + \alpha) + (\alpha^2 + \alpha + 1) \\
 &= 2\alpha^2 + 2\alpha + 1 \quad \leftarrow \text{多項式の係数は } 2 \text{ を法とする} \\
 &= 1
 \end{aligned}$$

$$\begin{aligned}
 \textcircled{2} \quad \alpha^4 - \alpha^5 &= (\alpha + 1) + (\alpha^2 + \alpha) \quad \leftarrow 2 \text{ を法とするため加法と減法を同一視する} \\
 &= \alpha^2 + 2\alpha + 1 \quad \leftarrow \text{多項式の係数は } 2 \text{ を法とする} \\
 &= \alpha^2 + 1 \\
 &= \alpha^8
 \end{aligned}$$

$$\begin{aligned}
 \textcircled{3} \quad \alpha^9 \cdot \alpha^{10} &= \alpha^{19} \\
 &= \alpha^{15} \cdot \alpha^4 \quad \leftarrow \alpha^{15} = 1 \\
 &= \alpha^4
 \end{aligned}$$

$$\begin{aligned}
 \textcircled{4} \quad \alpha^7 / \alpha^{14} &= \alpha^{-7} \\
 &= \alpha^{-7} \cdot 1 \\
 &= \alpha^{-7} \cdot \alpha^{15} \quad \leftarrow \alpha^{15} = 1 \\
 &= \alpha^8
 \end{aligned}$$

問 3 α をガロア拡大体 $\text{GF}(2^8)$ の原始多項式 $x^8 + x^4 + x^3 + x^2 + 1$ の 1 つの根 (原始元) とするとき、 $\text{GF}(2^8)$ 上の多項式 $h(x) = \alpha^{122}x^3 + \alpha^2x^2 + \alpha^{15}x + \alpha^{201}$ を多項式 $g(x) = x^2 + \alpha^{167}x + \alpha^{98}$ で割り、剰余 $r(x)$ を求めなさい。ヒント：付録 A のガロア拡大体 $\text{GF}(2^8)$ の表を利用。

解答例 $h(x) \div g(x)$ を計算すると

$$\begin{array}{r}
 \alpha^{122}x + \alpha^{37} \\
 x^2 + \alpha^{167}x + \alpha^{98} \overline{) \alpha^{122}x^3 + \alpha^2x^2 + \alpha^{15}x + \alpha^{201}} \\
 \underline{\alpha^{122}x^3 + \alpha^{34}x^2 + \alpha^{220}x} \phantom{+ \alpha^{201}} \\
 \text{ステップ 1} \rightarrow \alpha^{37}x^2 + \alpha^{222}x + \alpha^{201} \\
 \underline{\alpha^{37}x^2 + \alpha^{204}x + \alpha^{135}} \\
 \text{ステップ 2} \rightarrow \alpha^{189}x + \alpha^{165}
 \end{array}$$

となる (例えば $\alpha^{289} = \alpha^{255} \cdot \alpha^{34} = 1 \cdot \alpha^{34} = \alpha^{35}$)。したがって、剰余 $r(x)$ は $\alpha^{189}x + \alpha^{165}$ である。