

2007 年度 情報数理 レポート 4

学生用

学籍番号： _____

氏名： _____

下記の注意事項を守り、次ページ以降の問いに答え、レポートを完成させなさい。

提出期限： 2007 年 12 月 18 日 (火) 13:00 まで

提出場所： 理学部棟 正面玄関内に設置のレポートボックス

注意事項：

- (1) このページを印刷し、必要事項を記入の上 (学籍番号欄と氏名欄は 2 箇所あるので忘れずに記入すること)、レポートの表紙として提出すること。
- (2) ~~文章処理ソフトウェアや図形処理ソフトウェア等を駆使してレポートを作成し (問→解答→問→解答→… の順になるように記述すること)、A4 サイズの用紙に印刷して提出すること (手書きは不可)。~~
- (3) クラスメイトのレポートを参考にしたり、クラスメイトと協力してレポートを作成した場合は、教員控の協力者氏名欄にクラスメイトの氏名を記入すること。これらの場合も、自分の言葉で表現し直すこと。**コピー禁止。**
- (4) 情報数理について、あなたの声を聞かせてください (教員控の意見・質問欄に記入のこと)。気軽にどうぞ (成績には一切影響しません)。

出題者： 幸山 直人

出題日： 2007 年 12 月 5 日 (水)

得点：

/6

----- 切り取り線 -----

2007 年度 情報数理 レポート 4

教員控

学籍番号： _____

氏名： _____

協力者氏名： _____ , _____ , _____

レポート作成に要した時間： _____ . _____ 時間

得点：

/6

意見・質問：

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

解答例 ハミング距離の定義より、各成分ごとに比較し、異なれば 1、同じであれば 0 として、その総和を取ればよい。したがて、

$$\begin{array}{cccccccccccccccc} \mathbf{x} & = & (& a, & b, & c, & a, & d, & d, & a, & c, & c, & a, & b, & b, & a, & d, & d, & d &) \\ \mathbf{y} & = & (& a, & c, & c, & a, & a, & a, & a, & c, & c, & a, & b, & b, & a, & b, & b, & d &) \\ & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{array}$$

であるから、その総和を取ればハミング距離は、

$$d_H(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{16} \delta(x_i, y_i) = 0 + 1 + 0 + 0 + 1 + 1 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 1 + 1 + 0 = 5$$

となる。

評価基準 解答例に準じた解答であれば 1 点。

問 2 ガロア体 $\text{GF}(11)$ の各元 x に対する乗法に関する逆元 x^{-1} をそれぞれ求めなさい。(1 点)

解答例 ガロア体 $\text{GF}(11) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ の各元は以下の通りである。ただし、零元 0 に対する乗法に関する逆元は存在しない。

$$\begin{array}{ll} 1^{-1} = 1 & (\because 1 \cdot 1 = 1 \equiv 1 \pmod{11}) \\ 2^{-1} = 6 & (\because 2 \cdot 6 = 12 = 11 + 1 \equiv 1 \pmod{11}) \\ 3^{-1} = 4 & (\because 3 \cdot 4 = 12 = 11 + 1 \equiv 1 \pmod{11}) \\ 4^{-1} = 3 & (\because 4 \cdot 3 = 12 = 11 + 1 \equiv 1 \pmod{11}) \\ 5^{-1} = 9 & (\because 5 \cdot 9 = 45 = 44 + 1 \equiv 1 \pmod{11}) \\ 6^{-1} = 2 & (\because 6 \cdot 2 = 12 = 11 + 1 \equiv 1 \pmod{11}) \\ 7^{-1} = 8 & (\because 7 \cdot 8 = 56 = 55 + 1 \equiv 1 \pmod{11}) \\ 8^{-1} = 7 & (\because 8 \cdot 7 = 56 = 55 + 1 \equiv 1 \pmod{11}) \\ 9^{-1} = 5 & (\because 9 \cdot 5 = 45 = 44 + 1 \equiv 1 \pmod{11}) \\ 10^{-1} = 10 & (\because 10 \cdot 10 = 100 = 99 + 1 \equiv 1 \pmod{11}) \end{array}$$

評価基準 解答例に準じた解答であれば 1 点。

問 3 原始多項式 $x^3 + x + 1$ の 1 つの根 α をガロア拡大体 $\text{GF}(2^3)$ の原始元とするとき、ガロア拡大体 $\text{GF}(2^3)$ の加法表を完成しなさい。ただし、値はべき表現で記述すること。(2 点)

解答

+	0	1	α	α^2	α^3	α^4	α^5	α^6
0	0	1	α	α^2	α^3	α^4	α^5	α^6
1	1	0	α^3	α^6	α	α^5	α^4	α^2
α	α	α^3	0	α^4	1	α^2	α^6	α^5
α^2	α^2	α^6	α^4	0	α^5	α	α^3	1
α^3	α^3	α	1	α^5	0	α^6	α^2	α^4
α^4	α^4	α^5	α^2	α	α^6	0	1	α^3
α^5	α^5	α^4	α^6	α^3	α^2	1	0	α
α^6	α^6	α^2	α^5	1	α^4	α^3	α	0

評価基準 解答例に準じた解答であれば 2 点。

問 4 原始多項式 $x^8 + x^4 + x^3 + x^2 + 1$ の 1 つの根 α をガロア拡大体 $\text{GF}(2^8)$ の原始元とするとき、多項式 $h(x) = \alpha^3 x^3 + \alpha x^2 + \alpha^6 x + \alpha^{19}$ を多項式 $g(x) = x^2 + \alpha^{17} x + \alpha^{200}$ で割った余り (剰余) $r(x)$ を求めなさい。(2 点)

解答例 $h(x) \div g(x)$ を計算すると

$$\begin{array}{r}
 \alpha^3 x + \alpha^{93} \\
 x^2 + \alpha^{17} x + \alpha^{200} \overline{) \alpha^3 x^3 + \alpha x^2 + \alpha^6 x + \alpha^{19}} \\
 \underline{\alpha^3 x^3 + \alpha^{20} x^2 + \alpha^{203} x} \phantom{+ \alpha^{19}} \\
 \text{ステップ 1} \rightarrow \alpha^{93} x^2 + \alpha^{55} x + \alpha^{19} \\
 \underline{\alpha^{93} x^2 + \alpha^{110} x + \alpha^{38}} \\
 \text{ステップ 2} \rightarrow \alpha^{118} x + \alpha^{111}
 \end{array}$$

となる ($\alpha^{293} = \alpha^{255} \cdot \alpha^{38} = 1 \cdot \alpha^{38} = \alpha^{38}$)。従って、剰余 $r(x)$ は $\alpha^{118} x + \alpha^{111}$ である。

評価基準 ステップ 1 まで正しければ 1 点。ステップ 2 まで正しければ更に 1 点。