

2006 年度 情報科学 I 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：2006 年 6 月 27 日 (火) 15:00 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) 情報科学 I 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：2006 年 6 月 14 日 (水)

得点：

/6

----- 切り取り線 -----

2006 年度 情報科学 I 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 記号 $\{a, b, c, d, e\}$ からなる 5 元符号の 10 次元ベクトル $\mathbf{x} = (b, a, c, d, b, a, c, d, e, a)$ と $\mathbf{y} = (b, e, b, d, b, a, c, c, c, a)$ のハミング距離を定義に従って求めなさい。(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、その総和をとればよい。従って、

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

であるから、その総和をとればハミング距離は

$$d_H(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{10} \delta(x_i, y_i) = 0 + 1 + 1 + 0 + 0 + 0 + 0 + 1 + 1 + 0 = 4$$

となる。

評価基準 解答例に準じた解答であれば 1 点。

問 2 7 を法とするガロア体 $\text{GF}(7)$ の元 x の乗法に関する逆元 (x^{-1}) を全て求めなさい。(1 点)

解答例 各元の乗法に関する逆元は

$$\begin{aligned} (1^{-1}) &= 1 \iff \because 1 \cdot 1 = 1 \equiv 1 \pmod{7} \\ (2^{-1}) &= 4 \iff \because 4 \cdot 2 = 8 \equiv 1 \pmod{7} \\ (3^{-1}) &= 5 \iff \because 5 \cdot 3 = 15 \equiv 1 \pmod{7} \\ (4^{-1}) &= 2 \iff \because 2 \cdot 4 = 8 \equiv 1 \pmod{7} \\ (5^{-1}) &= 3 \iff \because 3 \cdot 5 = 15 \equiv 1 \pmod{7} \\ (6^{-1}) &= 6 \iff \because 6 \cdot 6 = 36 \equiv 1 \pmod{7} \end{aligned}$$

となる。

評価基準 解答例に準じた解答であれば 1 点。乗法表を作成し、表から読み取ってもよい。

問 3 下記 (テキストの 42 ページ) のガロア拡大体 $\text{GF}(2^3)$ の加法表を完成しなさい。ただし、解答はべき表現で記述すること。(2 点; 2 箇所間違えるごとに 1 点減点)

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 α を原始多項式 $x^8 + x^4 + x^3 + x^2 + 1$ の 1 つの根とすると、すなわち α をガロア拡大体 $\text{GF}(2^8)$ の原始元とすると、多項式 $h(x) = \alpha^4 x^5 + \alpha^{26} x^4 + \alpha^3 x^3 + \alpha x^2 + \alpha^6 x + \alpha^{19}$ を多項式 $g(x) = x^4 + \alpha^{113} x^3 + \alpha^{199} x^2 + \alpha^{17} x + \alpha^{200}$ 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

$$\begin{array}{r}
 x^4 + \alpha^{113} x^3 + \alpha^{199} x^2 + \alpha^{17} x + \alpha^{200} \quad \overline{\alpha^4 x + \alpha^{235}} \\
 \hline
 \alpha^4 x^5 + \alpha^{26} x^4 + \alpha^3 x^3 + \alpha x^2 + \alpha^6 x + \alpha^{19} \\
 \text{ステップ 1} \rightarrow \quad \underline{\alpha^4 x^5 + \alpha^{117} x^4 + \alpha^{203} x^3 + \alpha^{21} x^2 + \alpha^{204} x} \\
 \alpha^{235} x^4 + \alpha^{11} x^3 + \alpha^{43} x^2 + \alpha^{32} x + \alpha^{19} \\
 \text{ステップ 2} \rightarrow \quad \underline{\alpha^{235} x^4 + \alpha^{93} x^3 + \alpha^{179} x^2 + \alpha^{252} x + \alpha^{180}} \\
 \alpha^{70} x^3 + \alpha^{77} x^2 + \alpha^{29} x + \alpha^{127}
 \end{array}$$

となる。従って、剰余 $r(x)$ は $\alpha^{70} x^3 + \alpha^{77} x^2 + \alpha^{29} x + \alpha^{127}$ 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。