2012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： 2012年12月5日(水) 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サイズの内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： 2012年11月22日(木)

得点： /6

----- 切り取り線 -----

2012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 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。(1点)

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

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

となる。

評価基準 解答例に準じた解答であれば1点。

問 2 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。(1点)

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

評価基準 解答と同じであれば1点。

(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。(2点)

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

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

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

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

評価基準 解答例に準じた解答であれば2点。なお、1問間違えるごとに減点1点。

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。(2点)

解答例 $h(x) \div g(x)$ を計算すると

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

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。

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。