2010 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 :　2010 年 12 月 8 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 :　2010 年 11 月 26 日 (金)

得点 :　　　/6

－－－－－－－－－－－－－－ 切り取り線 －－－－－－－－－－－－－－

2010 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 :

$\boxed{\textbf{問 1}}$ 集合 $\{a,b,c,d\}$ から成る符号について、符号語 $\boldsymbol{x} = (a,b,c,a,d,a,a,c,c,a,b,b,a,d,d)$ と $\boldsymbol{y} = (a,c,c,a,a,a,a,c,c,a,b,b,a,b,b)$ 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

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

となる。

評価基準 解答例に準じた解答であれば 1 点。

$\boxed{\textbf{問 2}}$ α をガロア拡大体 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 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	0 0 0 0
1	1	0 0 0 1
α	α	0 0 1 0
α^2	α^2	0 1 0 0
α^3	α^3	1 0 0 0
α^4	$\alpha+1$	0 0 1 1
α^5	$\alpha^2+\alpha$	0 1 1 0
α^6	$\alpha^3+\alpha^2$	1 1 0 0
α^7	$\alpha^3+\alpha+1$	1 0 1 1
α^8	α^2+1	0 1 0 1
α^9	$\alpha^3+\alpha$	1 0 1 0
α^{10}	$\alpha^2+\alpha+1$	0 1 1 1
α^{11}	$\alpha^3+\alpha^2+\alpha$	1 1 1 0
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1 1 1 1
α^{13}	$\alpha^3+\alpha^2+1$	1 1 0 1
α^{14}	α^3+1	1 0 0 1

評価基準 解答と同じであれば 1 点。

(2) 次の①〜④を計算し、その値をべき表現で答えなさい。(2 点)

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

$$\text{②}\quad \alpha^8-\alpha^3 = (\alpha^2+1) + (\alpha^3) \quad \leftarrow \text{2 を法とするため加法と減法を同一視する}$$
$$= \alpha^3+\alpha^2+1 = \alpha^{13}$$

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

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

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。

$\boxed{\textbf{問 3}}$　α をガロア拡大体 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、GF(2^8) 上の多項式 $h(x)=\alpha^{123}x^3+\alpha^2x^2+\alpha^{15}x+\alpha^{201}$ 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 GF(2^8) の表を利用。(2 点)

解答例　$h(x)\div g(x)$ を計算すると

$$\begin{array}{rr}
 & \alpha^{123}x + \alpha^{17} \\
x^2+\alpha^{167}x+\alpha^{98} \;) & \alpha^{123}x^3 + \alpha^2x^2 + \alpha^{15}x + \alpha^{201} \\
 & \alpha^{123}x^3 + \alpha^{35}x^2 + \alpha^{221}x \\
\text{ステップ 1} \rightarrow & \alpha^{17}x^2 + \alpha^{163}x + \alpha^{201} \\
 & \alpha^{17}x^2 + \alpha^{184}x + \alpha^{115} \\
\text{ステップ 2} \rightarrow & \alpha^{173}x + \alpha^{102}
\end{array}$$

となる (例えば $\alpha^{290}=\alpha^{255}\cdot\alpha^{35}=1\cdot\alpha^{35}=\alpha^{35}$)。したがって、剰余 $r(x)$ は $\alpha^{173}x+\alpha^{102}$ 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。