2008 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：2008 年 11 月 25 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：2008 年 11 月 13 日 (木)

得点：　／6

－－－－－－－－－－－－－－－－－－－－－－－－ 切り取り線 －－－－－－－－－－－－－－－－－－－－－－－－

2008 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 $\boldsymbol{x} = (a, b, c, a, d, d, a, c, c, a, b, b, a, d, d, a)$ と $\boldsymbol{y} = (a, c, c, a, a, a, a, c, c, a, b, b, a, b, b, d)$ 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。したがて、

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

であるから、その総和を取ればハミング距離は、

$$d_H(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^{16} \delta(x_i, y_i) = 0+1+0+0+1+1+0+0+0+0+0+0+0+0+1+1+1 = 6$$

となる。

評価基準　解答例に準じた解答であれば 1 点。

問 2　GF(2) 上の多項式 $x^3 + x^2 + x + 1$ が **3 次既約多項式でない**ことを示しなさい。(1 点)

解答例　既約でないなら、多項式 $x^3 + x^2 + x + 1$ は 2 次以下の多項式の積として表せる。ここで、

$$
\begin{aligned}
(x+1)(x+1)(x+1) &= x^3 + 3x^2 + 3x + 1 \\
&\equiv x^3 + x^2 + x + 1 \pmod 2
\end{aligned}
$$

であるから、GF(2) 上の多項式 $x^3 + x^2 + x + 1$ は 3 次既約多項式でないことが示された。　■

【参考】GF(2) 上の 3 次既約多項式には、多項式 $x^3 + x + 1$ と $x^3 + x^2 + 1$ の 2 つが存在します (テキストでは多項式 $x^3 + x + 1$ を 3 次既約多項式として採用しています)。4 次既約多項式や 5 次既約多項式についても調べておきましょう。

	既約多項式	既約多項式でない
1 次	$x + 1$	
2 次	$x^2 + x + 1$	$x^2 + 1,\ x^2 + x$
3 次	$x^3 + x + 1,\ x^3 + x^2 + 1$	$x^3 + 1,\ x^3 + x,\ x^3 + x^2,$ $x^3 + x^2 + x,\ x^3 + x^2 + x + 1$

評価基準　解答例に準じた解答であれば 1 点。

問 3　α をガロア拡大体 GF(2^3) の原始多項式 x^3+x+1 の 1 つの根 (原始元) とするとき、ガロア拡大体 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　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 $h(x)=\alpha^3x^3+\alpha x^2+\alpha^6x+\alpha^{19}$ 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

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

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。