

2010 年度 情報数理 レポート 5

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 21 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： 2010 年 12 月 10 日 (金)

得点：

/6

----- 切り取り線 -----

2010 年度 情報数理 レポート 5

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 2 元符号 $\text{GF}(2) = \{0, 1\}$ 上の $G(x) = 1 + x + x^4 + x^5$ を生成多項式とする $[8, 3]$ 巡回符号について、次の (1)～(6) の問いに答えなさい。(1 点×6)

(1) この符号の検査多項式 $H(x)$ を求めなさい。

解答例 検査多項式を求めるには $H(x) = (x^8 - 1)/G(x) = (x^8 + 1)/G(x)$ を計算すればよいから、

$$\begin{array}{r}
 x^5 + x^4 + x + 1 \overline{) x^8 + x^4 + x^3 + x + 1} \\
 \underline{x^8 + x^7 + x^4 + x^3 + x + 1} \\
 x^7 + x^4 + x^3 + x + 1 \\
 \underline{x^7 + x^6 + x^3 + x^2 + 1} \\
 x^6 + x^4 + x^2 + 1 \\
 \underline{x^6 + x^5 + x^2 + x } \\
 x^5 + x^4 + x + 1 \\
 \underline{x^5 + x^4 + x + 1} \\
 0
 \end{array}$$

より、検査多項式は $H(x) = 1 + x + x^2 + x^3$ である。

評価基準 解答例に準じた解答であれば 1 点。

(2) この符号の検査行列 H を求めなさい。ヒント：テキスト (p.58) を参照のこと。

解答例 $[8, 3]$ 巡回符号であることから $n = 8$ および $k = 3$ である。したがって、

$$\begin{aligned}
 [x^5] \bmod G(x) &= 1 + x + x^4 \iff [1 \ 1 \ 0 \ 0 \ 1] \\
 [x^6] \bmod G(x) &= 1 + x^2 + x^4 \iff [1 \ 0 \ 1 \ 0 \ 1] \\
 [x^7] \bmod G(x) &= 1 + x^3 + x^4 \iff [1 \ 0 \ 0 \ 1 \ 1]
 \end{aligned}$$

となる。ゆえに、検査行列 H は

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

となる。

評価基準 解答例に準じた解答であれば 1 点。

(3) この符号の符号語 $\mathbf{x}_i = (x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7)$ を全て求めなさい。ヒント：全部で8個ある。

解答例 符号語 $\mathbf{x}_i$ が $\mathbf{x}_i H^T = \mathbf{0}$ を満たすことより、関係式

$$\begin{cases} x_0 + x_5 + x_6 + x_7 = 0 \\ x_1 + x_5 = 0 \\ x_2 + x_6 = 0 \\ x_3 + x_7 = 0 \\ x_4 + x_5 + x_6 + x_7 = 0 \end{cases} \iff \begin{cases} x_0 = x_5 + x_6 + x_7 \\ x_1 = x_5 \\ x_2 = x_6 \\ x_3 = x_7 \\ x_4 = x_5 + x_6 + x_7 \end{cases}$$

を得る。すなわち、 x_5, x_6, x_7 を変数 (パラメータ) として8個の符号語を求めればよい。

注意1：それぞれ0または1の値をとるため、8通りの解が存在する。

注意2：巡回符号と線形符号 (加法について閉じている) になっていることをチェックしておこう。

$$\begin{aligned} \mathbf{x}_0 &= (0, 0, 0, 0, 0, 0, 0, 0), & \mathbf{x}_1 &= (1, 0, 0, 1, 1, 0, 0, 1), & \mathbf{x}_2 &= (1, 0, 1, 0, 1, 0, 1, 0), \\ \mathbf{x}_3 &= (0, 0, 1, 1, 0, 0, 1, 1), & \mathbf{x}_4 &= (1, 1, 0, 0, 1, 1, 0, 0), & \mathbf{x}_5 &= (0, 1, 0, 1, 0, 1, 0, 1), \\ \mathbf{x}_6 &= (0, 1, 1, 0, 0, 1, 1, 0), & \mathbf{x}_7 &= (1, 1, 1, 1, 1, 1, 1, 1) \end{aligned}$$

評価基準 解答例に準じた解答であれば1点。

(4) この符号の生成行列 G を求めなさい。

解答例 (3) より、情報を $\mathbf{i}_i = (i_0, i_1, i_2)$ とし、 $x_5 = i_0, x_6 = i_1, x_7 = i_2$ とおく。このとき、

$$\begin{cases} x_0 = i_0 + i_1 + i_2 \\ x_1 = i_0 \\ x_2 = i_1 \\ x_3 = i_2 \\ x_4 = i_0 + i_1 + i_2 \\ x_5 = i_0 \\ x_6 = i_1 \\ x_7 = i_2 \end{cases} \iff \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} = \begin{bmatrix} i_0 + i_1 + i_2 \\ i_0 \\ i_1 \\ i_2 \\ i_0 + i_1 + i_2 \\ i_0 \\ i_1 \\ i_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} i_0 \\ i_1 \\ i_2 \end{bmatrix}$$

であるから、 $\mathbf{x}_i = \mathbf{i}_i G$ を考慮すると上記の式は $\mathbf{x}_i^T = (\mathbf{i}_i G)^T = G^T \mathbf{i}_i^T$ である。したがって、生成行列 G は

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

となる。

注意1： $GH^T = \mathbf{0}$ が成り立つか計算してみましょう。

注意2：生成行列 G はパラメータの取り方によって同値な行列が複数存在する。

評価基準 解答例に準じた解答であれば1点。

(5) この符号の最小距離 $d_{\min}$ を求めなさい。

解答例 1 テキストの 48 ページの「2 元符号の場合、2 つの異なる符号語間のハミング距離は、それら符号語の和 (排他的論理和) によって得られるベクトルに含まれる 1 の個数と一致します。さらに、線形符号では符号語の和は再び符号語になります。したがって、零ベクトルでない符号語に含まれる 1 の個数の最小値が最小距離に一致します。」より、符号語 $\mathbf{x}_i$ ($i = 1, 2, 3, 4, 5, 6, 7$) に含まれる 1 の個数はそれぞれ 4 個で最小となる。したがって、最小距離 $d_{\min} = 4$ である。

解答例 2 異なる符号語 $\mathbf{x}_i, \mathbf{x}_j$ ($i \neq j$) に対して、それぞれ $d_H(\mathbf{x}_i, \mathbf{x}_j)$ を求めると

d_H	$\mathbf{x}_0$	$\mathbf{x}_1$	$\mathbf{x}_2$	$\mathbf{x}_3$	$\mathbf{x}_4$	$\mathbf{x}_5$	$\mathbf{x}_6$	$\mathbf{x}_7$
$\mathbf{x}_0$		4	4	4	4	4	4	8
$\mathbf{x}_1$			4	4	4	4	8	4
$\mathbf{x}_2$				4	4	8	4	4
$\mathbf{x}_3$					8	4	4	4
$\mathbf{x}_4$						4	4	4
$\mathbf{x}_5$							4	4
$\mathbf{x}_6$								4
$\mathbf{x}_7$								

となる。したがって、最小距離 $d_{\min} = 4$ である。

注意 : 1 個の誤りであれば訂正可能であるが、2 個の誤りであれば検出のみ可能で訂正はできない。

評価基準 解答例に準じた解答であれば 1 点。

(6) この符号の受信語 $\mathbf{y} = (1, 1, 0, 0, 0, 0, 0, 0)$ のシンδροームを計算し、可能であれば推定情報 $\hat{\mathbf{i}}$ を求めなさい。

解答例 まず、(5) より最小距離 $d_{\min} = 4$ であることから誤り訂正可能な成分の個数 t_0 が 1 個 ($t_0 = [(d_{\min} - 1)/2] = 1$) であることに注意する。次に、シンδροーム $\mathbf{s}$ を計算すると

$$\mathbf{s} = \mathbf{x}H^T = [11000000] \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix} = [11000] \neq \mathbf{0}$$

となり、誤りを含んでいることが判る。ところが、シンδροーム $\mathbf{s}$ は転置した検査行列 H^T のいずれの行とも一致しない (誤り訂正可能な成分の個数が 1 個であることに矛盾する)。すなわち、2 個以上の誤りを含む。実際、例えば

$$\mathbf{s} = [10000] + [01000] = [11001] + [00001]$$

(第 1 行) (第 2 行) (第 6 行) (第 5 行)

のように 2 通りの誤り訂正が可能性がある。したがって、誤りの検出は可能であるが、誤りを訂正し推定情報を得ることはできない。

評価基準 解答例に準じた解答であれば 1 点。