

2008 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： 2008 年 12 月 9 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 27 日 (木)

得点：

/6

----- 切り取り線 -----

2008 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 $\text{GF}(2) = \{0, 1\}$ 上の情報 $\mathbf{i} = (i_1, i_2)$ に対する検査ビット (p_1, p_2, p_3) を関係式

$$\begin{cases} p_1 = i_1 + i_2 \\ p_2 = i_1 \\ p_3 = i_2 \end{cases}$$

で与え、符号語が $\mathbf{x} = (i_1, i_2, p_1, p_2, p_3)$ となる $[5, 2]$ 線形符号を構成する。この線形符号について、次の (1)~(4) の問いに答えなさい。(1 点 $\times 4$)

(1) 生成行列 G および検査行列 H を求めなさい。

解答例 定義より、

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}, \quad H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

(2) 符号語 $\mathbf{x}$ を全てリストアップしなさい。

解答例 1 (Im G として求める) 4 通りの情報 $\mathbf{i} = (i_1, i_2)$ に対して、符号語 $\mathbf{x} = \mathbf{i}G$ をそれぞれ求めればよい (関数 $p_1 = i_1 + i_2$, $p_2 = i_1$, $p_3 = i_2$ に代入しても同じ)。従って、

情報 $(0, 0)$ に対する符号語 $[0 \ 0]G$ は $(0, 0, 0, 0, 0)$,

情報 $(0, 1)$ に対する符号語 $[0 \ 1]G$ は $(0, 1, 1, 0, 1)$,

情報 $(1, 0)$ に対する符号語 $[1 \ 0]G$ は $(1, 0, 1, 1, 0)$,

情報 $(1, 1)$ に対する符号語 $[1 \ 1]G$ は $(1, 1, 0, 1, 1)$

となる。

解答例 2 (Ker H として求める) 符号語 $\mathbf{x}$ は $\mathbf{x}H^T = \mathbf{0}$ を満たすから、方程式

$$[x_1 \ x_2 \ x_3 \ x_4 \ x_5] \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [0 \ 0 \ 0] \iff \begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1 + x_4 = 0 \\ x_2 + x_5 = 0 \end{cases}$$

を解けばよい。それぞれ $x_3 = x_1 + x_2$, $x_4 = x_1$, $x_5 = x_2$ だから、 x_1 および x_2 をパラメータとして符号語を求めれば、

$x_1 = 0$ かつ $x_2 = 0$ のとき符号語は $(0, 0, 0, 0, 0)$,

$x_1 = 0$ かつ $x_2 = 1$ のとき符号語は $(0, 1, 1, 0, 1)$,

$x_1 = 1$ かつ $x_2 = 0$ のとき符号語は $(1, 0, 1, 1, 0)$,

$x_1 = 1$ かつ $x_2 = 1$ のとき符号語は $(1, 1, 0, 1, 1)$

となる ($x_i = i_1$, $x_2 = i_2$, $x_3 = p_1$, $x_4 = p_2$, $x_5 = p_3$ と置き直せば解答例 1 と全く同じ計算をしていることがわかる $\iff \text{Im } G = \text{Ker } H$)。

(3) 最小距離 $d_{\min}$ を求めなさい。

解答例 1 検査行列 H の ある 1 つの列ベクトルは他の列ベクトルのスカラー倍となっていない ことから、任意の 2 つの縦ベクトルは 1 次独立である。従って、各符号語間のハミング距離は $2+1$ 以上であることがわかる ($\text{GF}(2)$ のときはスカラーとして取れるのは 1 だけであるから、同じものを含まなければよい)。逆に、例えば、検査行列 H の第 1 列は第 3 列と第 4 列の 1 次結合

$$\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

と書けるから、ある符号語間のハミング距離が $2+1$ となるものが存在する。ゆえに、最小距離 $d_{\min}$ は 3 となる (一般に、最小距離が検査行列 H の階数 (ランク) に 1 を足したものの以下であることはわかるが、列ベクトルの行数が多くなると実際に書き出してみないと 1 次独立な最小の組を見つけることはできない)。

解答例 2 (2) で求めた符号語をそれぞれ

$$x_1 = (0, 0, 0, 0, 0), \quad x_2 = (0, 1, 1, 0, 1), \quad x_3 = (1, 0, 1, 1, 0), \quad x_4 = (1, 1, 0, 1, 1)$$

とおく。各符号語間のハミング距離を求めると以下ようになる (注意: $d_H(u, v) = d_H(v, u)$)。

d_H	x_1	x_2	x_3	x_4
x_1	—	3	3	4
x_2	—	—	4	3
x_3	—	—	—	3
x_4	—	—	—	—

従って、最小距離 $d_{\min}$ は 3 となる (符号語が少ない場合は直接求めた方が楽かも?)。

解答例 3 (2) で求めた符号語をそれぞれ

$$x_1 = (0, 0, 0, 0, 0), \quad x_2 = (0, 1, 1, 0, 1), \quad x_3 = (1, 0, 1, 1, 0), \quad x_4 = (1, 1, 0, 1, 1)$$

とおく。このとき、最小重みは

$$\begin{aligned} (\text{最小重み}) &= \min\{ \text{“}x_1\text{以外の各符号語の 1 の個数を数える”} \} \\ &= \min\{ d_H(x_1, x_2), d_H(x_1, x_3), d_H(x_1, x_4) \} \\ &= \min\{ 3, 3, 4 \} \\ &= 3 \end{aligned}$$

となる。したがって、最小重みは最小距離と一致するから、最小距離 $d_{\min}$ は 3 となる。

* 線形符号の符号語は加法群を成す (符号語に符号語を加えたものは再び符号語となる) から、ある符号語とそれ以外の符号語のハミング距離の集合は、全体の符号語に対して各符号語間のハミング距離の集合と一致する。言い換えれば、最小重みが相対的なハミング距離の最小値であるのに対して、最小距離は絶対的なハミング距離の最小値である。

(4) 誤りの検出が可能、かつ、誤り訂正が不可能な受信語 y を全てリストアップしなさい。

解答例 (3) より、誤りが訂正可能な数は $1 (= [3 - 1]/2)$ であるから、1 個の符号語につき誤り訂正可能な受信語が 5 個ある。また、受信語 y は全部で $32 (= 2^5)$ 個あるから、誤りの検出しかできない受信語は $8 (= 32 - (1 + 5) \times 4)$ 個である。従って、全ての受信語から符号語および訂正可能な受信語を消去し、誤りの検出が可能、かつ、誤り訂正が不可能な受信語を見つける。

符号語	(0, 0, 0, 0, 0)	1	(0, 0, 0, 0, 0)	1
	(<u>1</u> , 0, 0, 0, 0)	2	(0, 0, 0, 0, 1)	6
	(0, <u>1</u> , 0, 0, 0)	3	(0, 0, 0, 1, 0)	5
	(0, 0, <u>1</u> , 0, 0)	4	(0, 0, 0, 1, 1)	
	(0, 0, 0, <u>1</u> , 0)	5	(0, 0, 1, 0, 0)	4
	(0, 0, 0, 0, <u>1</u>)	6	(0, 0, 1, 0, 1)	9
			(0, 0, 1, 1, 0)	14
符号語	(0, 1, 1, 0, 1)	7	(0, 0, 1, 1, 1)	
	(<u>1</u> , 1, 1, 0, 1)	8	(0, 1, 0, 0, 0)	3
	(0, <u>0</u> , 1, 0, 1)	9	(0, 1, 0, 0, 1)	10
	(0, 1, <u>0</u> , 0, 1)	10	(0, 1, 0, 1, 0)	
	(0, 1, 1, <u>1</u> , 1)	11	(0, 1, 0, 1, 1)	20
	(0, 1, 1, 0, <u>0</u>)	12	(0, 1, 1, 0, 0)	12
			(0, 1, 1, 0, 1)	7
符号語	(1, 0, 1, 1, 0)	13	(0, 1, 1, 1, 0)	
	(<u>0</u> , 0, 1, 1, 0)	14	(0, 1, 1, 1, 1)	11
	(1, <u>1</u> , 1, 1, 0)	15	(1, 0, 0, 0, 0)	2
	(1, 0, <u>0</u> , 1, 0)	16	(1, 0, 0, 0, 1)	
	(1, 0, 1, <u>0</u> , 0)	17	(1, 0, 0, 1, 0)	16
	(1, 0, 1, 1, <u>1</u>)	18	(1, 0, 0, 1, 1)	21
			(1, 0, 1, 0, 0)	17
符号語	(1, 1, 0, 1, 1)	19	(1, 0, 1, 0, 1)	
	(<u>0</u> , 1, 0, 1, 1)	20	(1, 0, 1, 1, 0)	13
	(1, <u>0</u> , 0, 1, 1)	21	(1, 0, 1, 1, 1)	18
	(1, 1, <u>1</u> , 1, 1)	22	(1, 1, 0, 0, 0)	
	(1, 1, 0, <u>0</u> , 1)	23	(1, 1, 0, 0, 1)	23
	(1, 1, 0, 1, <u>0</u>)	24	(1, 1, 0, 1, 0)	24
			(1, 1, 0, 1, 1)	19
			(1, 1, 1, 0, 0)	
			(1, 1, 1, 0, 1)	8
			(1, 1, 1, 1, 0)	15
			(1, 1, 1, 1, 1)	22

* 下線部が符号語に対する誤り部分

従って、誤りの検出が可能、かつ、誤り訂正が不可能な受信語は

(0, 0, 0, 1, 1), (0, 0, 1, 1, 1), (0, 1, 0, 1, 0), (0, 1, 1, 1, 0),
(1, 0, 0, 0, 1), (1, 0, 1, 0, 1), (1, 1, 0, 0, 0), (1, 1, 1, 0, 0)

の合計 8 個である (いずれの符号語からも 2 以上 (2 または 3) のハミング距離を持っている)。

評価基準 解答例に準じた解答であれば各 1 点。

問 2 非 2 元符号 $\text{GF}(3) = \{0, 1, 2\}$ 上の 1 つの誤りが訂正可能な線形符号の検査行列 H を以下の書式に合うように 1 つ作りなさい。(2 点)

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

解答例 検査行列 H の階数 (ランク) が 3 であることから、 $\{0, 1, 2\}$ の全ての組み合わせ 3^3 個の列ベクトルを作ると以下になる。

$$\begin{aligned} & \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 2 \\ 2 \end{bmatrix}, \\ & \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix}, \\ & \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \\ 2 \end{bmatrix} \end{aligned}$$

まず、零ベクトル $\mathbf{0}$ は不適切なので除く (零ベクトル自身で 1 次従属となる; 符号語そのものである; ハミング距離が 0 である)。従って、 $3^3 - 1$ 個の列ベクトルが候補として残る。次に、例えば、

$$\begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix} = 2 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix} = 2 \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}$$

などのようにスカラー倍 (1 または 2; 0 は除く) になっているものは 1 次従属なので一方を除く。ただし、書式に合うように第 1 行が 0 または 1 となるものを残す。従って、以下の $(3^3 - 1)/(3 - 1)$ 個の列ベクトルが残る (これが非 2 元符号の符号長となる; テキストの 50 ページも参照)。

$$\begin{aligned} & \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \left(\text{or } \begin{bmatrix} 0 \\ 2 \\ 2 \end{bmatrix} \right), \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} \left(\text{or } \begin{bmatrix} 0 \\ 2 \\ 1 \end{bmatrix} \right), \\ & \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix} \end{aligned}$$

以上より、書式に合わせて検査行列 H を記述すれば、例えば

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ \boxed{2} & \boxed{2} & \boxed{1} & \boxed{1} & \boxed{1} & \boxed{2} & \boxed{0} & \boxed{0} & \boxed{1} & \boxed{1} & 0 & 1 & 0 \\ \boxed{1} & \boxed{2} & \boxed{1} & \boxed{2} & \boxed{0} & \boxed{0} & \boxed{1} & \boxed{2} & \boxed{1} & \boxed{2} & 0 & 0 & 1 \end{bmatrix}$$

となる。

評価基準 解答例に準じた解答であれば 2 点。ただし、スカラー倍が 1 次従属であることに気づいたと思われる解答には部分点 1 点。