1　第1回 演習 (ICT.209 代数系と符号理論)

- 少人数の履修者同士で協力して演習に取り組むことを推奨しています。

1.1 以下の符号の符号長、最小距離、符号化率を答えよ。

$$C_1 = \{00000, 10101, 00011, 11111\}$$

1.2 2 元対称通信路で符号を用いる場合、2 つの符号

$$C_1 = \{00000, 10101, 00011, 11111\}$$
$$C_2 = \{00000, 11000\}$$

のどちらが望ましいか理由と共に答えよ。

1.3 0 が 1 に反転する確率が 0.3 であり、1 が 0 に反転する確率が 0.2 の無記憶通信路において

$$p(r_1r_2r_3|000), p(r_1r_2r_3|111)$$

を求めよ。

1.4 前問と同じ通信路において符号 $C_5 = \{000, 111\}$ を用いたときに、8 種類の有り得るすべての受信語について、最尤復号の復号結果が 000 または 111 のどちらになるか答えよ。

1.5 前問の最尤復号を最小距離復号に置き換えて解け。

1.6 以下の QR コードを手持ちの携帯電話で読めることを確認したあと、ペンで少し汚してもまだ読めることを確認せよ。どこまで汚しても読めるか、限界を探ろう。

1.7 半径 r の球を体積 B の立方体の容器に充填する。充填可能な球の最大数を $A(B,r)$ と書く。

(a) 球充填限界に対応する、$\big(r, B, A(B,r)\big)$ に関する限界式を導出せよ。

(b) 球被覆限界に対応する、$\big(r, B, A(B,r)\big)$ に関する限界式を導出しようとして、同様の証明をしようとするとあるところで破綻してしまう。証明のどこで破綻するか説明せよ。

1.8 ある 2 元ベクトル $\vec{x} \in \mathbb{F}_2^n$ を反転確率 $p < 1/2$ の 2 元対称通信路に入力した。出力を $\vec{y} \in \mathbb{F}_2^n$ とする。このとき、$p < q$ に対して、以下が成り立つことを示せ。

$$\lim_{n\to\infty} \Pr\{\vec{Y} \in B(\vec{x}, \lfloor qn \rfloor)\} = 1$$

ヒント：誤りの数つまり $d(\vec{Y}, \vec{x})$ を Z と書いて、Z に関する大数の弱法則を使う。

1.9 これまで勉強したところで、分かりにくかったところ、配布資料の誤り、その他なんでもあったら教えて下さい。

2　第2回 演習 (ICT.209 代数系と符号理論)

- 少人数の履修者同士で協力して演習に取り組むことを推奨しています。

2.1 $\mathbb{F}_2$ 上の線形空間のスカラおよびベクトルに関して以下を計算せよ。

(a) $1 + 1$

(b) $1/1$

(c) $1(0110)$

(d) $0(0110)$

(e) $(011) + (001)$

(f) $(111)/(111)$

2.2 次を満たす $x_1, \ldots, x_4 \in \mathbb{F}_2$ を求めよ。

$$\begin{pmatrix} 1000 \\ 1011 \\ 1111 \\ 1001 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

2.3 以下の $\{0,1\}^2$ または $\{0,1\}^5$ の部分集合について、それが二元線形符号であるか否か述べ、二元線形符号でない場合にはその理由を述べよ。二元線形符号である場合にはその基底、次元、生成行列，最小距離，符号化率を述べよ。

(a) $C_1 = \{01, 10, 11\}$

(b) $C_2 = \{00000, 10110, 01101, 11011, 11111, 01001, 10010, 00100\}$

(c) $C_3 = \{01000, 00001, 10110, 01001, 11111, 11011, 01101, 10010\}$

2.4 $\mathbb{F}$ 上の長さ 5 の繰り返し符号の生成行列 G とパリティ検査行列 H を求めよ。

2.5 以下のパリティ検査行列で定義される二元線形符号 C の最小距離 $d(C)$ に対して、$d(C) = 4$ であることを示せ。

$$H = \begin{pmatrix} 1011\ 1000 \\ 1101\ 0100 \\ 0111\ 0010 \\ 1111\ 1111 \end{pmatrix}$$

2.6 次のパリティ検査行列 H で定義される $\mathbb{F}_2$ 上の線形符号を C と書く。

$$H = \begin{pmatrix} 1011\ 100 \\ 1101\ 010 \\ 0111\ 001 \end{pmatrix}$$

C は以下の行ベクトルを符号語として有する。

```
0000000 1000110 0100011 1100101
0010101 1010011 0110110 1110000
0001111 1001001 0101100 1101010
0011010 1011100 0111001 1111111
```

(a) $y = 0111101$ のシンドローム s を求めよ。

(b) 前項で求めたシンドローム s に対応するコセット C_s を求めよ。

(c) C_s のコセット代表元を求めよ。

2.7 ある $[n, k]$ 2元線形符号 C に対して異なる $k \times n$ 生成行列は

$$\prod_{i=1}^{k} (2^k - 2^{i-1})$$

個あることを示せ。ただし，$n > k$ である.

2.8 異なる $[n, k]$ 2元線形符号の個数は

$$\frac{(2^n - 1)(2^n - 2) \cdots (2^n - 2^{k-1})}{(2^k - 1)(2^k - 2) \cdots (2^k - 2^{k-1})}$$

個であることを示せ。ただし，$n > k$ である.

2.9 生成行列

$$G' = \begin{pmatrix} 10111 \\ 11100 \\ 00110 \end{pmatrix}$$

は線形符号 C を生成する。

(a) G' の標準形 G を求めよ。

(b) さらに、対応する標準型パリティ検査行列 H を求めよ。

(c) C の双対符号 $C^{\perp}$ の生成行列の標準形 $G^{\perp}$ を求めよ。

(d) さらに、対応する標準型パリティ検査行列 $H^{\perp}$ を求めよ。

2.10 符号長 n の線形符号 C のパリティ検査行列 H は、C の双対符号 $C^{\perp}$ の $m(:= \dim C)$ 個の基底ベクトルを行ベクトルとして並べた $m \times n$ 行列であった。基底は線形独立なので、H はフルランクになる。

ここでは、フルランクとは限らない 2 元 $m \times n$ 行列 A に対して、符号空間 $C_A \stackrel{\text{def}}{=} \{\underline{x} = (x_1, \ldots, x_n)^{\mathsf{T}} \in \mathbb{F}_2^n \mid A\underline{x} = \underline{0}\}$ を考えよう。線形符号 C_A に対して、生成行列 G を求めたい。言い換えると、C_A を生成する:

$$C_A = \{\underline{x} \in \mathbb{F}_2^n \mid \underline{x} = \underline{u}G, \underline{u} \in \mathbb{F}_2^k, k := \dim C_A\}$$

となる $k \times n$ 行列である G を求めたい。
与えられた行列 A に対して、生成行列 G を求めるプログラムを作成し、行列 A が下記の行列で与えられるとき、生成行列 G を求めよ。

```
00010 00100 00100 01000 00100 00001
00001 00010 10000 00010 00010 10000
```

```
01000 00001 00010 00001 01000 00100
10000 10000 00001 00100 00001 01000
00100 01000 01000 10000 10000 00010
10000 00010 01000 00001 00100 00100
01000 00001 00100 00010 10000 00010
00010 01000 00010 10000 00010 00001
00100 10000 00001 01000 00001 10000
00001 00100 10000 00100 01000 01000
00010 10000 10000 01000 00010 00010
00001 00100 00001 10000 00100 00001
01000 01000 01000 00001 00001 10000
10000 00010 00100 00100 10000 00100
00100 00001 00010 00010 01000 01000
```

この行列は各 5×5 部分行列が置換行列 (列重みと行重みが 1 である行列) となっているので、ランクはフルランクより少なくとも 2 落ちる。行基本変形により A を行簡約階段形 (reduced row echelon form) に変形する。全零行以外の行が

$C_A^{\perp}$ の基底を構成している。

10000	0000**1**	0001**0**	0**1**110	0**1**000	1**0**000
0**1**000	0000**1**	0001**0**	0**0**001	0**1**000	0**0**100
00**1**00	0000**1**	0001**0**	0**0**010	0**1**000	0**1**000
000**1**0	0000**1**	0001**0**	0**0**100	1**0**110	0**1**101
0000**1**	0000**1**	0000**1**	0**1**101	1**1**111	1**0**101
00000	**1**0001	00011	0**1**010	0**1**001	1**1**000
00000	0**1**001	00000	0**0**110	0**0**101	1**0**010
00000	00**1**01	00000	0**1**111	0**1**010	0**1**010
00000	0001**1**	00000	0**1**001	0**0**000	1**0**010
00000	00000	**1**0001	0**0**110	1**1**101	1**0**111
00000	00000	0**1**010	0**0**110	0**1**100	0**0**110
00000	00000	00**1**10	0**0**011	1**1**000	0**0**110
00000	00000	00000	**1**0010	1**0**001	1**1**110
00000	00000	00000	0**0**000	0**0**000	0**0**000
00000	00000	00000	0**0**000	0**0**000	0**0**000

底の 2 行が全 0 ベクトルなので、ランクはフルランクより 2 下がっていることがわかる。

部分単位行列を構成している列とそれ以外の列からなるものに分けて考えて、標準形のパリティ検査行列 $(I|P)$ から標準形の生成行列 $(P^{\mathsf{T}}|I)$ を作った方法（またはその逆の方法）と同様の考え方で、G を求める。

11111	1111**1**	00000	00000	00000	00000
11110	10000	0111**1**0	00000	00000	00000
00001	10000	1000**1**	00000	00000	00000
10001	10110	00000	0**1**000	00000	00000
10011	01100	11000	00**1**00	00000	00000
10100	11100	11100	10**1**0	00000	00000
01001	00110	00100	0000**1**	00000	00000
00011	00000	10100	10000	**1**0000	00000
11101	10100	11100	00000	0**1**000	00000
00011	01000	11000	00000	00**1**00	00000
00011	00100	00000	00000	000**1**0	00000
00001	11000	10000	10000	0000**1**	00000
10001	11010	10000	10000	00000	**1**0000
00110	10100	00000	10000	00000	0**1**000
01011	00000	11100	10000	00000	00**1**00
00000	01110	11100	10000	00000	000**1**0
00011	00000	10000	00000	00000	0000**1**

2.11 これまで勉強したところで、分かりにくかったところ、配布資料の誤り、その他なんでもあったら教えて下さい。

3　第3回 演習 (ICT.209 代数系と符号理論)

- 少人数の履修者同士で協力して演習に取り組むことを推奨しています。

3.1 長さ 15 のハミング符号に関して、以下の問に答えよ。

(a) パリティ検査行列を書け

(b) 長さ 15 のハミング符号を用いて (000000000000010) が受信されたときに、前問で解答したパリティ検査行列とともに復号手続きを実行して得られる符号語を書け。

3.2 $[7, 4, 3]$ ハミング符号は、以下の符号語を有する。

```
0000000 1000110 0100011 1100101
0010101 1010011 0110110 1110000
0001111 1001001 0101100 1101010
0011010 1011100 0111001 1111111
```

$[7, 4, 3]$ ハミング符号 C の双対符号 $C^{\perp}$ は、以下の符号語を有する。

```
0000000 1011100 1101010 0110110
0111001 1100101 1010011 0001111
```

(a) C の重み分布 $A(X), A(X, Y)$ を求めよ。

(b) $C^{\perp}$ の重み分布 $B(X), B(X,Y)$ を求めよ。

(c) $A(X,Y), B(X,Y)$ に関して MacWilliams の恒等式が成り立つことを確認せよ。

3.3 符号長 7 のハミング符号は以下のパリティ検査行列 H と生成行列 G で定義される二元線形符号である。

$$H = \begin{pmatrix} 1011\ 100 \\ 1101\ 010 \\ 0111\ 001 \end{pmatrix}, G = \begin{pmatrix} 1000\ 110 \\ 0100\ 011 \\ 0010\ 101 \\ 0001\ 111 \end{pmatrix}$$

長さ 7 のハミング符号に関して、以下の問に答えよ。

(a) 情報 (1100) を符号化して得られる符号語を求めよ。

(b) 受信語が (1110111) であったときに講義で説明した復号法を実施して得られる符号語を求めよ。

3.4 1 本以下の毒ワインを含む 7 本のワイン $W_1, \ldots, W_7$ がある．毒ワイン検出器を N 回使用して，毒ワインが存在しない場合には存在しないことを知り，毒ワインが存在する場合にはどのワインが毒ワインであるかを必ず特定する方法を考える．ただし，毒ワイン検出器の 1 回の使用の際に、複数本のワインを混ぜて使用してもよい。毒ワイン検出器の使用結果として，毒が含まれていたか含まれていなかったかのどちらかがわかる。さらに，はじめに毒ワイン検出器を使用

するより前に，毒ワイン検出器を使用する回数 N と、どのように 7 本のワインを混ぜて毒ワイン検出器を N 回使用するかを決めなければならない.

(1) 1 本以下の毒ワインを見つけるためには毒ワイン検出器を 3 回以上使用することが必要であることを証明せよ.

(2) 1 本以下の毒ワインを見つけることが可能な 3 回の毒ワイン検出器の使用方法と毒ワイン検出器の使用結果から毒ワインをみつける方法を示し、ハミング符号の復号法との関係を説明せよ.

3.5 A から P までの 16 文字のひとつが書かれた紙が私のポケットの中にある。あなたは私に YES/NO で答えられる質問を 7 回することができる。私はあなたに正直に回答するが、1 回または 0 回正しくない回答をする。7 回の質問と、その回答から紙に書いてある文字を正しく当てる方法を答えなさい。ただし、7 回の質問は 1 回目の質問をする前に決めなければならない。ただし、「第 7 の質問に正しく答えますか？」など、回答の正誤に関する質問はしてはならない。

3.6 n 人の囚人は独立に 1/2 の確率で白か黒の帽子のどちらかを着せられる。他の囚人の帽子を見ることはできるが自分の帽子を見ることはできない。それぞれの囚人は残りの囚人の帽子を見て、自分の帽子の色を決定的に（同じ帽子の色を配置であったときには同じ選択を答える）推測し、白、黒、棄権のうち一つを回答する。ただし、帽子を着させられる前

に、戦略（各囚人が、どのように他の囚人の帽子の色を見て、答えを回答するか）をどのようにするかを相談することはできるが、帽子を着させられた後には一切情報を交換することはできない。さらに、他の囚人の回答を知ることはできない。正しい色を答える囚人が少なくとも一人いて誤った色を答える囚人はひとりもいないとき、すべての囚人は解放される。そうでないとき、すべての囚人のおかずが一皿減らされる。

より形式的に述べる。帽子配置を

$$h = (h_1, \ldots, h_n) \in \{0,1\}^n$$

で表す。$\Pr(H = h) = 2^{-n}$ である。各囚人は、入力、白 (0)・黒 (1)・棄権 (-) のどれかを出力

$$a(h) = \big(a_1(h_{\sim 1}), \ldots, a_n(h_{\sim n})\big) \in \{0,1,\text{-}\}^n$$

する関数として見なすことができる。ここで、$h_{\sim i}$ は h から h_i を除いたものである。与えられた h に対して、$a_i(h_{\sim i}) = h_i$ なる $1 \leq i \leq n$ が存在し、$a_i = h'_i$ となる $1 \leq i \leq n$ が存在しないとき解放される。ここで、

$$h'_i = \begin{cases} 0 & (h_i = 1) \\ 1 & (h_i = 0) \end{cases}$$

である。

大学でハミング符号を習っていた囚人達は、大勢いれば（n が大きければ）高い確率で解放される希望の戦略を思いついた。

(a) $n = 3$ のとき 3/4(=1-2/8) の確率で解放される戦略を答えよ。その戦略によって、3/4 の確率で解放されることを説明せよ。

(b) $n = 7$ のとき 7/8(=1-16/128) の確率で解放される戦略を答え、ハミング符号との関係を説明せよ。その戦略によって、7/8 の確率で解放されることを説明せよ。

(c) $n = 7$ のとき、前問で答えた戦略が最適である、すなわちどんな戦略を用いても解放される確率は 7/8 以下で有ることを証明せよ。

3.7 3 つの元からなる群 $(G =: \{e, a, b\}, \times)$ に対して、演算表は一意に決まる。e は単位元である。

(a) 演算表を書け。

$\times$	e	a	b
e			
a			
b			

(b) 演算表が一意に定まることを証明せよ。

3.8 0 と 1 を除いた実数上で定義された次の 6 つの関数の集合 $\mathcal{F}$ を考える。

$$f_1(x) = x, f_2(x) = \frac{1}{1-x}, f_3(x) = \frac{x-1}{x},$$
$$f_4(x) = 1-x, f_5(x) = \frac{1}{x}, f_6(x) = \frac{x}{x-1},$$

(a) $(\mathcal{F}, *)$ が群となるためには、2 つの関数 f_i と f_j の間にどのような 2 項演算 $f_i * f_j$ を定義すればよいか答えよ。

(b) 定義した演算 $*$ に対して、演算表をつくり、単位元と $\mathcal{F}$ の各関数に対する逆元を求めよ。

3.9 紙に書かれた文字「F」を時計回りに 90 度回転させる操作を a と書き、紙の右が左に来るように裏返す操作を b と書く。何もしない操作を e と書く。操作 a のあとに操作 b を行う合成された操作を $b \times a$ と書く。この操作の合成を続けていくことにより生成される操作を考える。これらの操作によって生成される操作は、F を

$$\mathrm{F}, \exists, \mathrm{\Lambda}, \mathrm{\Gamma}, \mathrm{\Gamma}, \mathrm{E}, \mathrm{\Xi}$$

と見えるようにする紙への操作の 8 通りである。

すべてからなる集合

$$\begin{aligned} G &:= \{a, b\}^* \\ &:= \{e, a, b, ab, ba, aaa, aab, aba, baa, abb, bab, bba, \dots\} \end{aligned}$$

はある有限な群 $(G, \times)$ をなす。

(a) $ba = a^i b^j$ となる最も小さい $i, j \geq 0$ を求めよ。

(b) $(G, \times)$ は可換群でないことを示せ。

(c) G の要素をすべて $a^i b^j$ の形で辞書順で列挙せよ。

(d) G の演算表 $a^i b^j \times a^k b^l$ を作成せよ。表の行と列は辞書順で配置すること。

(e) $ab \in G$ の逆元を $a^i b^j$ と表したときの整数 i, j を求めよ。

3.10 群 $(G, \times)$ の正規部分群 N に対して、次は同値であることを証明せよ。

(a) $N \triangleleft G$ である。

(b) $\forall g \in G$ に対して、

$$gNg^{-1} = N$$

(c) $\forall n \in N, \forall g \in G$ に対して、

$$gng^{-1} \in N$$

代数系と符号理論 中間試験 (令和元年 10 月 31 日)

1. **１枚の解答用紙につき大問１つを回答すること**. 答案用紙には答えのみでなく、それを導く過程も記入すること。
2. **全ての答案用紙に名前と学籍番号を忘れず記入すること。**
3. 各大問は独立しており，特に断りのない限り大問間で設定や記号等は共有されない.
4. 試験開始 30 分までの退室と、試験終了 10 分前からの退室と、試験開始 30 分からの入室を禁ずる。
5. 答案を提出せずに退室することはできません。
6. 用紙が足りない場合は裏も使って良い。その場合には表面の右下に「裏面に続く」と書いてください。
7. 試験時間内にすべての問題に解答できるように作問されていない。
8. 各大問において小問は易しい順に並んでいる。
9. 易しい小問ほど配点が高い。
10. 変数 x の範囲を限定せずに命題 $P(x)$ を参照する場合には、命題 $P(x)$ が文脈上意味のある範囲で x の範囲が限定されているものとする。
11. 設定が不明な場合には、文脈上もっとも尤もらしい解釈で理解すること。
12. 設定に不備や矛盾がある場合には、文脈上もっとも尤もらしい修正を施して理解すること。

M.1 以下の問に答えよ。

(a) 以下の 2 元符号の符号長、最小距離、符号化率を答え

よ。

$$C = \{100001011001,\\ 111010001100,\\ 001101010010,\\ 110110110101\}$$

(b) 2元符号Cを用いて通信を行う。送信語$\vec{c}$が送信され、受信語$\vec{r}$を受信した。最小距離復号$\hat{\vec{c}}^{(\mathrm{MD})}(\vec{r})$の定義を述べよ。

(c) 2元符号Cを用いて通信を行う。送信語$\vec{c}$が送信され、受信語$\vec{r}$を受信した。半径tの限界距離復号$\hat{\vec{c}}_t^{(\mathrm{BD})}(\vec{r})$の定義を述べよ。復号エラーを出力することがあることに注意せよ。

(d) 最小ハミング距離がdである2元符号Cを用いて通信を行い受信語$\vec{r}$を受信した。$2t < d$となるtに対して、$d(\vec{c},\vec{r}) \leq t$となる符号語$\vec{c}$は存在するとしたら一意であることを示せ。

M.2 以下の問に答えよ。

(a) ハミング限界は(n, M, d)符号が存在するための十分条件と必要条件のどちらを与えますか。

(b) VG限界は(n, M, d)符号が存在するための十分条件と必要条件のどちらを与えますか。

(c) 半径rの球を体積Bの立方体の容器に充填する。充填可能な球の最大数を$A(B, r)$と書く。半径rの球の体積は$\frac{4}{3}\pi r^3$で与えられる。

i. $\big(r, B, A(B,r)\big)$ に関する球充填限界式を述べよ。

ii. $\big(r, B, A(B,r)\big)$ に関する球充填限界式を証明せよ。

(d) $\mathbb{F}_2^n$ に点を配置する。ただし、各点を中心とする半径 t のハミング球が交わらないように、各点は $\mathbb{F}_2^n$ に配置されなければならない。配置可能な点の最大数を $A(n,t)$ と書く。

i. $\mathbb{F}_2^n$ のある点を中心とする半径 t のハミング球に含まれる点の数を求めよ。

ii. $\big(t, n, A(n,t)\big)$ に関する球充填限界式を述べよ。

iii. $\big(t, n, A(n,t)\big)$ に関する球充填限界式を証明せよ。

M.3 (a) 以下の集合について、それが二元線形符号であるか否か述べ、二元線形符号でない場合にはその理由を述べよ。二元線形符号である場合にはその次元、生成行列，最小距離，符号化率を求めよ。

$$C_1 = \{01, 10, 11\}$$

$$C_2 = \{00000, 10110, 01101, 11011, \\ 11111, 01001, 10010, 00100\}$$

(b) 次を満たす $x_1, \ldots, x_4 \in \mathbb{F}_2$ を求めよ。

$$\begin{pmatrix} 1000 \\ 1011 \\ 1111 \\ 0001 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

(c) 以下で定義される、長さ n の 2 元符号 C を繰り返し符号という。

$$C = \{x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n \mid x_1 = \cdots = x_n\}$$

$n = 3$ のとき C とその双対符号 $C^\perp$ の符号語を列挙せよ。

(d) 2 元線形符号 C とその双対符号 $C^\perp$ の重み分布多項式をそれぞれ $A(X, Y)$ と $B(X, Y)$ と書く。C の最小距離 d と双対符号 $C^\perp$ の最小距離 $d^\perp$ を求める方法を述べよ。

M.4 符号長 7 のハミング符号 C は下の標準型パリティ検査行列 H で定義される二元線形符号である。

$$H = \begin{pmatrix} 1011\ 100 \\ 1101\ 010 \\ 0111\ 001 \end{pmatrix}$$

長さ 7 のハミング符号に関して、以下の問に答えよ。

(a) H に対応する標準型生成行列 G を求めよ。

(b) 前問で得られた生成行列 G を用いて情報ベクトル (1111) を符号化して得られる符号語を求めよ。

(c) 受信語が (1101111) であったときに講義で説明した復号法を実施して、推定符号語を求めよ。

(d) 符号語数、次元、符号化率を求めよ。

(e) 最小距離が 3 以上であることを証明せよ。

(f) 最小距離が 3 以下であることを証明せよ。

(g) 各符号語の半径 1 のハミング球の合併は $\mathbb{F}_2^7$ を埋め尽くすことを証明せよ。

M.5 以下の問に答えよ。

(a) 以下の集合と二項演算の組み合わせが，群であるための条件をすべて満たすか否か答えよ。群となる場合にはその単位元 e と元 x に対する逆元を明らかにし，群とならない場合にはその理由を述べよ.

i. 有理数の集合とその加算

ii. 非零実数の集合とその乗算

iii. 2×2 実行列の集合と行列の乗算

iv. 有限集合 X から X 自身への全単射の全体からなる集合 $S(X)$ と写像の合成

(b) 群 $(G, \times)$ に関して次を証明せよ。

i. 単位元 $e \in G$ は一意に存在する。

ii. $a \in G$ に対して、逆元 a^{-1} は一意に存在する。

代数系と符号理論 中間試験 (令和４年 11 月 10 日)

1. **１枚の解答用紙につき大問１つを回答すること**. 答案用紙には答えのみでなく、それを導く過程も記入すること。
2. **全ての答案用紙に名前と学籍番号を忘れず記入すること。**
3. 各大問は独立しており，特に断りのない限り大問間で設定や記号等は共有されない.
4. 試験開始 30 分までの退室と、試験終了 10 分前からの退室と、試験開始 30 分からの入室を禁ずる。
5. 答案を提出せずに退室することはできません。
6. 用紙が足りない場合は裏も使って良い。その場合には表面の右下に「裏面に続く」と書いてください。
7. 試験時間内にすべての問題に解答できるように作問されていない。
8. 各大問において小問は易しい順に並んでいる。
9. 易しい小問ほど配点が高い。
10. 変数 x の範囲を限定せずに命題 $P(x)$ を参照する場合には、命題 $P(x)$ が文脈上意味のある範囲で x の範囲が限定されているものとする。
11. 設定が不明な場合には、文脈上もっとも尤もらしい解釈で理解すること。
12. 設定に不備や矛盾がある場合には、文脈上もっとも尤もらしい修正を施して理解すること。

M.1 以下の問に答えよ。

(a) 以下の 2 元符号の符号長、最小距離、符号化率を答え

よ。

$$C = \{00000, 10101, 00111, 11111\}$$

(b) 2 元対称通信路で符号を用いる場合、 2 つの 2 元符号

$$C_1 = \{00000, 10101, 00011, 11111\}$$
$$C_2 = \{00000, 11000\}$$

のどちらが望ましいか理由と共に答えよ。

(c) 2 元符号 C を用いて通信を行う。送信語 $\vec{c}$ が送信され、受信語 $\vec{r}$ を受信した。最小距離復号 $\hat{\vec{c}}^{(\mathrm{MD})}(\vec{r})$ の定義を述べよ。

(d) 2 元符号 C を用いて通信を行う。送信語 $\vec{c}$ が送信され、受信語 $\vec{r}$ を受信した。半径 t の限界距離復号 $\hat{\vec{c}}_t^{(\mathrm{BD})}(\vec{r})$ の定義を述べよ。復号エラーを出力することがあることに注意せよ。

(e) 最小ハミング距離が d である 2 元符号 C を用いて通信を行い受信語 $\vec{r}$ を受信した。$2t < d$ となる t に対して、$d(\vec{c}, \vec{r}) \leq t$ となる符号語 $\vec{c}$ は存在するとしたら一意であることを示せ。

(f) 次の長さ 12 の 4 つの行ベクトルからなる符号 C

$C = \{$
111011111110
010100001010
111001111000

110001110111
}
と受信語 $\vec{r} = 010101111101$ に対して、最小距離復号の出力 $\hat{\vec{c}}^{(\mathrm{MD})}(\vec{r})$ と半径 $t := \lfloor \frac{d(C)-1}{2} \rfloor$ の限界距離復号の出力 $\hat{\vec{c}}_t^{(\mathrm{BD})}$ を求めよ。

M.2 以下の問に答えよ。

(a) 次のうち正しいものを選択しなさい。

(1) (n, M, d) に関するハミング限界が成り立てば、(n, M, d) 符号が存在する。

(2) (n, M, d) 符号が存在すれば、(n, M, d) に関するハミング限界が成り立つ。

(3) (n, M, d) に関して VG 限界が成り立てば、(n, M, d) 符号が存在する。

(4) (n, M, d) 符号が存在すれば、(n, M, d) に関して VG 限界が成り立つ。

(b) $\mathbb{F}_2^n$ に点を配置する。ただし、各点を中心とする半径 t のハミング球が交わらないように、各点は $\mathbb{F}_2^n$ に配置されなければならない。配置可能な点の最大数を $A(n, t)$ と書く。

i. $\mathbb{F}_2^n$ のある点を中心とする半径 t のハミング球に含まれる点の数を求めよ。

ii. $\big(t, n, A(n, t)\big)$ に関する球充填限界式を述べよ。

iii. $\big(t, n, A(n, t)\big)$ に関する球充填限界式を証明せよ。

M.3 (a) 以下の集合について、それが二元線形符号であるか否か述べ、二元線形符号でない場合にはその理由を述べよ。二元線形符号である場合にはその次元、生成行列，最小距離，符号化率を求めよ。

$$C_1 = \{01, 10, 11\}$$

$$C_2 = \{00000, 10110, 01101, 11011,$$
$$11111, 01001, 10010, 00100\}$$

(b) 次を満たす $x_1, \ldots, x_4 \in \mathbb{F}_2$ を求めよ。

$$\begin{pmatrix} 1000 \\ 1011 \\ 1111 \\ 0001 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

(c) 以下で定義される、長さ n の 2 元符号 C を繰り返し符号という。

$$C = \{x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n \mid x_1 = \cdots = x_n\}$$

$n = 3$ のとき C とその双対符号 $C^\perp$ の符号語を列挙せよ。

(d) 2 元線形符号 C の双対符号を $C^\perp$ とする。$C^\perp$ の重み分布多項式 $B(X, Y)$ から、C の最小距離 d と $C^\perp$ の最小距離 $d^\perp$ を求める方法を述べよ。

M.4 符号長 7 のハミング符号 C は下の標準型パリティ検査行列 H で定義される二元線形符号である。

$$H = \begin{pmatrix} 1011\ 100 \\ 1101\ 010 \\ 0111\ 001 \end{pmatrix}$$

長さ 7 のハミング符号に関して、以下の問に答えよ。

(a) H に対応する標準型生成行列 G を求めよ。

(b) 前問で得られた生成行列 G を用いて情報ベクトル (1010) を符号化して得られる符号語を求めよ。

(c) 受信語が (1111101) であったときに講義で説明した復号法を実施して、推定符号語を求めよ。

(d) 符号語数、次元、符号化率を求めよ。

(e) 最小距離が 3 以上であることを証明せよ。

(f) 最小距離が 3 以下であることを証明せよ。

(g) 下記の行列 H' は、H の右にすべて 0 の列を加えて、さらに下にすべて 1 の行を加えてたものである。H' を有する 2 元線系符号の最小距離は 4 であることを示せ。

$$H' = \begin{pmatrix} 10111000 \\ 11010100 \\ 01110010 \\ 11111111 \end{pmatrix}$$

(h) 各符号語の半径 1 のハミング球の合併は $\mathbb{F}_2^7$ を埋め尽くすことを証明せよ。

M.5 以下の問に答えよ。

(a) 以下の集合と二項演算の組み合わせが，群であるための条件をすべて満たすか否か答えよ。群となる場合にはその単位元 e と元 x に対する逆元を明らかにし，群とならない場合にはその理由を述べよ.

i. 有理数の集合とその加算

ii. 非零実数の集合とその乗算

iii. 2×2 実行列の集合と行列の乗算

iv. 有限集合 X から X 自身への全単射の全体からなる集合 $S(X)$ と写像の合成

(b) 群 $(G, \times)$ に関して次を証明せよ。

i. 単位元 $e \in G$ は一意に存在する。

ii. $a \in G$ に対して、逆元 a^{-1} は一意に存在する。

(c) 講義や演習で扱ってない自明でない群の例を挙げ、群となることを示せ。

4　代数系と符号理論 中間試験 (令和 5 年 11 月 6 日)

1. **１枚の解答用紙につき大問１つを回答すること**. 答案用紙には答えのみでなく、それを導く過程も記入すること。
2. **全ての答案用紙に名前と学籍番号を忘れず記入すること。**
3. 各大問は独立しており，特に断りのない限り大問間で設定や記号等は共有されない.
4. 試験開始 30 分までの退室と、試験終了 10 分前からの退室と、試験開始 30 分からの入室を禁ずる。
5. 答案を提出せずに退室することはできません。
6. 用紙が足りない場合は裏も使って良い。その場合には表面の右下に「裏面に続く」と書いてください。
7. 試験時間内にすべての問題に解答できるように作問されていない。
8. 各大問において小問は易しい順に並んでいる。
9. 易しい小問ほど配点が高い。
10. 変数 x の範囲を限定せずに命題 $P(x)$ を参照する場合には、命題 $P(x)$ が文脈上意味のある範囲で x の範囲が限定されているものとする。
11. 設定が不明な場合には、文脈上もっとも尤もらしい解釈で理解すること。
12. 設定に不備や矛盾がある場合には、文脈上もっとも尤もらしい修正を施して理解すること。

M.1 以下の問に答えよ。

(a) 以下の 2 元符号の符号長、最小距離、符号化率を答え

よ。

$$
\begin{aligned}
C = \{&001101010010,\\
&111010001100,\\
&100001011001,\\
&110110110101\}
\end{aligned}
$$

(b) 2 元対称通信路で符号を用いる場合、 2 つの 2 元符号

$$
\begin{aligned}
C_1 &= \{00000, 10101, 00011, 11111\}\\
C_2 &= \{00000, 11000\}
\end{aligned}
$$

のどちらが望ましいか理由と共に答えよ。

(c) 2 元符号 C を用いて通信を行う。送信語 $\vec{c}$ が送信され、受信語 $\vec{r}$ を受信した。最小距離復号 $\hat{\vec{c}}^{(\mathrm{MD})}(\vec{r})$ の定義を述べよ。

(d) 2 元符号 C を用いて通信を行う。送信語 $\vec{c}$ が送信され、受信語 $\vec{r}$ を受信した。半径 t の限界距離復号 $\tilde{\vec{c}}_t^{(\mathrm{BD})}(\vec{r})$ の定義を述べよ。復号エラーを出力することがあることに注意せよ。

(e) 最小ハミング距離が d である 2 元符号 C を用いて通信を行い受信語 $\vec{r}$ を受信した。$2t < d$ となる t に対して、$d(\vec{c}, \vec{r}) \leq t$ となる符号語 $\vec{c}$ は存在するとしたら一意であることを示せ。

(f) 次の長さ 12 の 4 つの行ベクトルからなる符号 C

$C = \{$

111011111110
010100001010
111001111000
110001110111
}
と受信語 $\vec{r} = 010101111101$ に対して、最小距離復号の出力 $\hat{\vec{c}}^{(\mathrm{MD})}(\vec{r})$ と半径 $t := \lfloor \frac{d(C)-1}{2} \rfloor$ の限界距離復号の出力 $\hat{\vec{c}}_t^{(\mathrm{BD})}$ を求めよ。

M.2 以下の問に答えよ。

(a) 次のうち正しいものを選択しなさい。

(1) (n, M, d) に関するハミング限界が成り立てば、(n, M, d) 符号が存在する。

(2) (n, M, d) 符号が存在すれば、(n, M, d) に関するハミング限界が成り立つ。

(3) (n, M, d) に関して VG 限界が成り立てば、(n, M, d) 符号が存在する。

(4) (n, M, d) 符号が存在すれば、(n, M, d) に関して VG 限界が成り立つ。

(b) $\mathbb{F}_2^n$ に点を配置する。ただし、各点を中心とする半径 t のハミング球が交わらないように、各点は $\mathbb{F}_2^n$ に配置されなければならない。配置可能な点の最大数を $A(n, t)$ と書く。

i. $\mathbb{F}_2^n$ のある点を中心とする半径 t のハミング球に含まれる点の数を求めよ。

ii. $\big(t, n, A(n,t)\big)$ に関する球充填限界式を述べよ。

iii. $\big(t, n, A(n,t)\big)$ に関する球充填限界式を証明せよ。

M.3 (a) 以下の集合について、それが二元線形符号であるか否か述べ、二元線形符号でない場合にはその理由を述べよ。二元線形符号である場合にはその次元、生成行列，最小距離，符号化率を求めよ。

$$C_1 = \{01, 10, 11\}$$

$$C_2 = \{00000, 10110, 01101, 11011,$$
$$11111, 01001, 10010, 00100\}$$

(b) 次を満たす $x_1, \ldots, x_4 \in \mathbb{F}_2$ を求めよ。

$$\begin{pmatrix} 1000 \\ 1011 \\ 1111 \\ 0001 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

(c) 以下で定義される、長さ n の 2 元符号 C を単一パリティ検査符号という。

$$C = \{x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n \mid \sum_{i=1}^{n} x_i = 0\}$$

$n = 3$ のとき C とその双対符号 $C^{\perp}$ の符号語を列挙せよ。

(d) 2 元線形符号 C の双対符号を $C^{\perp}$ とする。$C^{\perp}$ の重み分布多項式 $B(X,Y)$ から、C の最小距離 d と $C^{\perp}$ の最小距離 $d^{\perp}$ を求める方法を述べよ。

(e) 2 元線形符号 C の双対符号を $C^{\perp}$ とする。$C^{\perp}$ の重み分布多項式 $B(X,Y) = X^3+3XY^2$ から、C の重み分布 $A(X,Y)$ と最小距離 d を求めよ。

M.4 符号長 7 のハミング符号 C は下の標準型パリティ検査行列 H で定義される二元線形符号である。

$$H = \begin{pmatrix} 1011\ 100 \\ 1101\ 010 \\ 0111\ 001 \end{pmatrix}$$

長さ 7 のハミング符号に関して、以下の問に答えよ。

(a) H に対応する標準型生成行列 G を求めよ。

(b) 前問で得られた生成行列 G を用いて情報ベクトル (1010) を符号化して得られる符号語を求めよ。

(c) 受信語が (1111101) であったときに講義で説明した復号法を実施して、推定符号語を求めよ。

(d) 符号語数、次元、符号化率を求めよ。

(e) 最小距離が 3 以上であることを証明せよ。

(f) 下記の行列 H' は、H の右にすべて 0 の列を加えて、さらに下にすべて 1 の行を加えてたものである。H' を有す

る 2 元線系符号の最小距離は 4 であることを示せ。

$$H' = \begin{pmatrix} 10111000 \\ 11010100 \\ 01110010 \\ 11111111 \end{pmatrix}$$

(g) 1 本以下の毒ワインを含む 7 本のワイン $W_1, \ldots, W_7$ がある．毒ワイン検出器を N 回使用して，毒ワインが存在しない場合には存在しないことを知り，毒ワインが存在する場合にはどのワインが毒ワインであるかを必ず特定する方法を考える．ただし，毒ワイン検出器の 1 回の使用の際に、複数本のワインを混ぜて使用してもよい。毒ワイン検出器の使用結果として，毒が含まれていたか含まれていなかったかのどちらかがわかる。さらに，はじめに毒ワイン検出器を使用するより前に，毒ワイン検出器を使用する回数 N と、どのように 7 本のワインを混ぜて毒ワイン検出器を N 回使用するかを決めなければならない．

(1) 1 本以下の毒ワインを見つけるためには毒ワイン検出器を 3 回以上使用することが必要であることを証明せよ．

(2) 1 本以下の毒ワインを見つけることが可能な 3 回の毒ワイン検出器の使用方法と毒ワイン検出器の使用結果から毒ワインをみつける方法を示し、ハミング符号の復号法との関係を説明せよ．

M.5 以下の問に答えよ。

(a) 以下の集合と二項演算の組み合わせが，群であるための条件をすべて満たすか否か答えよ。群となる場合にはその単位元 e と元 x に対する逆元を明らかにし，群とならない場合にはその理由を述べよ.

i. 有理数の集合とその加算

ii. 非零実数の集合とその乗算

iii. 2×2 実行列の集合と行列の乗算

iv. 有限集合 X から X 自身への全単射の全体からなる集合 $S(X)$ と写像の合成

(b) 群 $(G, \times)$ に関して次を証明せよ。

i. 単位元 $e \in G$ は一意に存在する。

ii. $a \in G$ に対して、逆元 a^{-1} は一意に存在する。

(c) 3 つの元からなる群 $(G =: \{e, a, b\}, \times)$ に対して、演算表は一意に決まる。e は単位元である。

i. 演算表を書け。

$\times$	e	a	b
e			
a			
b			

ii. 演算表が一意に定まることを証明せよ。

5　代数系と符号理論 中間試験 (令和 6 年 10 月 31 日)

1. **１枚の解答用紙につき大問１つを回答すること**. 答案用紙には答えのみでなく、それを導く過程も記入すること。
2. **全ての答案用紙に名前と学籍番号を忘れず記入すること。**
3. 各大問は独立しており，特に断りのない限り大問間で設定や記号等は共有されない.
4. 試験開始 30 分までの退室と、試験終了 10 分前からの退室と、試験開始 30 分からの入室を禁ずる。
5. 答案を提出せずに退室することはできません。
6. 用紙が足りない場合は裏も使って良い。その場合には表面の右下に「裏面に続く」と書いてください。
7. 試験時間内にすべての問題に解答できるように作問されていない。
8. 各大問において小問は易しい順に並んでいる。
9. 易しい小問ほど配点が高い。
10. 変数 x の範囲を限定せずに命題 $P(x)$ を参照する場合には、命題 $P(x)$ が文脈上意味のある範囲で x の範囲が限定されているものとする。
11. 設定が不明な場合には、文脈上もっとも尤もらしい解釈で理解すること。
12. 設定に不備や矛盾がある場合には、文脈上もっとも尤もらしい修正を施して理解すること。

M.1 以下の問に答えよ。

(a) 以下の 2 元符号の符号長、符号語数、最小距離、符号

化率を答えよ。

$$C = \{11110010,\\ 00011110,\\ 10001100,\\ 01110111\}$$

(b) 2 元対称通信路で符号を用いる場合、 2 つの 2 元符号

$$C_1 = \{00000, 10101, 00011, 11111\}$$
$$C_2 = \{00000, 11000\}$$

のどちらが望ましいか理由と共に答えよ。

(c) 2 元符号 C を用いて通信を行う。送信語 $\vec{c}$ が送信され、受信語 $\vec{r}$ を受信した。最小距離復号 $\hat{\vec{c}}^{(\mathrm{MD})}(\vec{r})$ の定義を述べよ。

(d) 2 元符号 C を用いて通信を行う。送信語 $\vec{c}$ が送信され、受信語 $\vec{r}$ を受信した。半径 t の限界距離復号 $\hat{\vec{c}}_t^{(\mathrm{BD})}(\vec{r})$ の定義を述べよ。復号エラーを出力することがあることに注意せよ。

(e) 最小ハミング距離が d である 2 元符号 C を用いて通信を行い受信語 $\vec{r}$ を受信した。$2t < d$ となる t に対して、$d(\vec{c}, \vec{r}) \leq t$ となる符号語 $\vec{c}$ は存在するとしたら一意であることを示せ。

(f) 次の長さ 12 の 4 つの行ベクトルからなる符号 C
$C = \{$

111011111110
010100001010
111001111000
110001110111
}
と受信語 $\vec{r} = 010101111101$ に対して、最小距離復号の出力 $\hat{\vec{c}}^{(\mathrm{MD})}(\vec{r})$ と半径 $t := \lfloor \frac{d(C)-1}{2} \rfloor$ の限界距離復号の出力 $\hat{\vec{c}}_t^{(\mathrm{BD})}$ を求めよ。

M.2 以下の問に答えよ。

(a) 次のうち正しいものを選択しなさい。

(1) (n, M, d) に関するハミング限界が成り立てば、(n, M, d) 符号が存在する。

(2) (n, M, d) 符号が存在すれば、(n, M, d) に関するハミング限界が成り立つ。

(3) (n, M, d) に関して VG 限界が成り立てば、(n, M, d) 符号が存在する。

(4) (n, M, d) 符号が存在すれば、(n, M, d) に関して VG 限界が成り立つ。

(b) $\mathbb{F}_2^n$ に点を配置する。ただし、各点を中心とする半径 t のハミング球が交わらないように、各点は $\mathbb{F}_2^n$ に配置されなければならない。配置可能な点の最大数を $A(n, t)$ と書く。

i. $\mathbb{F}_2^n$ のある点を中心とする半径 t のハミング球に含まれる点の数を求めよ。

ii. $\big(t, n, A(n,t)\big)$ に関する球充填限界式を述べよ。

iii. $\big(t, n, A(n,t)\big)$ に関する球充填限界式を証明せよ。

(c) 符号長 n、最小距離 d、訂正能力が $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ である q 元符号 $C \subset \mathbb{F}_q^n$ に対して、次が成り立つことを示せ。

$$|C| \cdot \sum_{i=0}^{t} \binom{n}{i} \cdot (q-1)^i \leq q^n$$

M.3 (a) $\mathbb{F}_2$ 上の線形空間のスカラおよびベクトルに関して以下を計算せよ。

i. $1 + 1$

ii. $1/1$

iii. $1(0110)$

iv. $0(0110)$

v. $(011) + (001)$

vi. $(101) \times (011)$

(b) 以下の集合について、それが二元線形符号であるか否か述べ、二元線形符号でない場合にはその理由を述べよ。

$$C = \{ \quad 10110, 01101, 11011,$$
$$11111, 01001, 10010, 00100\}$$

(c) 次の 16 個の 2 元ベクトルの集合 C は長さ 8 の線形符号になっている。次元と最小距離を求めよ。

```
00000000 11101101 11100111 00001010
00101000 11000101 11001111 00100010
10110001 01011100 01010110 10111011
10011001 01110100 01111110 10010011
```

(d) 次を満たす $x_1, \ldots, x_4 \in \mathbb{F}_2$ を求めよ。

$$\begin{pmatrix} 0111 \\ 1100 \\ 1001 \\ 1011 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

(e) 以下で定義される、長さ n の 2 元符号 C を単一パリティ検査符号という。

$$C = \{x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n \mid \sum_{i=1}^{n} x_i = 0\}$$

$n = 3$ のとき C とその双対符号 $C^\perp$ の符号語を列挙せよ。

(f) 下記の長さ 7 の 16 個の符号語を有する 2 元線形符号 C の重み分布 $A(X, Y)$ と双対符号 $C^\perp$ の重み分布 $B(X, Y)$ を求めよ。

```
0000000  1000110  0100011  1100101
0010101  1010011  0110110  1110000
0001111  1001001  0101100  1101010
0011010  1011100  0111001  1111111
```

M.4 符号長 7 のハミング符号 C は下の標準型パリティ検査行列 H で定義される二元線形符号である。

$$H = \begin{pmatrix} 1011\ 100 \\ 1101\ 010 \\ 0111\ 001 \end{pmatrix}$$

長さ 7 のハミング符号に関して、以下の問に答えよ。

(a) H に対応する標準型生成行列 G を求めよ。

(b) 前問で得られた生成行列 G を用いて情報ベクトル (1010) を符号化して得られる符号語を求めよ。

(c) 受信語が (1111101) であったときに講義で説明した復号法を実施して、推定符号語を求めよ。

(d) 符号語数、次元、符号化率を求めよ。

(e) 最小距離が 3 以上であることを証明せよ。

(f) 下記の行列 H' は、H の右にすべて 0 の列を加えて、さらに下にすべて 1 の行を加えてたものである。H' を有する 2 元線系符号の最小距離は 4 であることを示せ。

$$H' = \begin{pmatrix} 10111000 \\ 11010100 \\ 01110010 \\ 11111111 \end{pmatrix}$$

(g) 1本以下の毒ワインを含む7本のワイン $W_1, \ldots, W_7$ がある．毒ワイン検出器を N 回使用して，毒ワインが存在しない場合には存在しないことを知り，毒ワインが存在する場合にはどのワインが毒ワインであるかを必ず特定する方法を考える．ただし，毒ワイン検出器の1回の使用の際に、複数本のワインを混ぜて使用してもよい。毒ワイン検出器の使用結果として，毒が含まれていたか含まれていなかったかのどちらかがわかる。さらに，はじめに毒ワイン検出器を使用するより前に，毒ワイン検出器を使用する回数 N と、どのように7本のワインを混ぜて毒ワイン検出器を N 回使用するかを決めなければならない．

(1) 1本以下の毒ワインを見つけるためには毒ワイン検出器を3回以上使用することが必要であることを証明せよ．

(2) 1本以下の毒ワインを見つけることが可能な3回の毒ワイン検出器の使用方法と毒ワイン検出器の使用結果から毒ワインをみつける方法を与えよ。

M.5 以下の問に答えよ。

(a) 以下の集合と二項演算の組み合わせが，群であるための条件をすべて満たすか否か答えよ。群となる場合にはその単位元 e と元 x に対する逆元を明らかにし，群とならない場合にはその理由を述べよ．

i. 有理数の集合とその加算

ii. 無理数と 1 を含む集合とその乗算。

iii. 非零実数の集合とその乗算

iv. 2×2 実行列の集合と行列の乗算

v. 有限集合 X から X 自身への全単射の全体からなる集合 $S(X)$ と写像の合成

(b) 群 $(G, \times)$ に関して次を証明せよ。

i. 単位元 $e \in G$ は一意に存在する。

ii. $a \in G$ に対して、逆元 a^{-1} は一意に存在する。

(c) 3 つの元からなる群 $(G =: \{e, a, b\}, \times)$ に対して、演算表は一意に決まる。e は単位元である。

i. 演算表を書け。

$\times$	e	a	b
e			
a			
b			

ii. 演算表が一意に定まることを証明せよ。

(d) $(G, \times)$ と $(H, \times)$ をそれぞれ単位元 e_G, e_H を有する群とする。写像 $f : G \to H$ が

$$f(xy) = f(x)f(y) \text{ for all } x, y \in G$$

を満たすとする。このとき、$K := \{x \in G \mid f(x) = e_H\}$ が $(G, \times)$ の正規部分群となることを示せ。

6　第6回 演習 (ICT.209 代数系と符号理論)

- 少人数の履修者同士で協力して演習に取り組むことを推奨しています。

6.1 以下の $\mathbb{F}_2[X]$ の多項式に関する計算を求めよ。

(a) $(1 + X + X^3) - (1 + X + X^2)$

(b) $(1 + X + X^2) \times (1 + X)$

(c) $1 + X^2 + X^5$ を $1 + X$ で割った商と剰余。

6.2 次の問に答えよ。

(a) 群ではあるが可換群ではない代数系 $(A, \circ)$ を挙げよ。

(b) 環ではあるが可換環ではない代数系 $(A, \{+, \times\})$ を挙げよ。

(c) 環ではあるが体ではない代数系 $(A, \{+, \times\})$ を挙げよ。

6.3 可換剰余環

$$\Big(\mathbb{Z}/4\mathbb{Z} = \{[0], [1], [2], [3]\}, \{+, \times\}\Big)$$

に関して、以下に答えよ。

(a) $+, \times$ のそれぞれに関する演算表を書け。

(b) $+, \times$ のそれぞれに関する単位元を答えよ。

(c) 体でないことを確認せよ。

6.4 可換剰余環

$$\begin{aligned}&\mathbb{F}_2[X]/\langle X+X^2\rangle\\&=\{[0],[1],[X],[1+X]\}\\&=\{[00],[10],[01],[11]\}\\&\Big(\mathbb{F}_2[X]/\langle X+X^2\rangle,\{+,\times\}\Big)\end{aligned}$$

に関して以下に答えよ。

(a) 演算表を書け。

例えば、$[11]\times[11]=[11]$ であることは以下のように確かめることができる。

$$\begin{aligned}[11]^2&=(1+X)^2=1+X^2\\&=1+X \bmod X+X^2=[11]\end{aligned}$$

(b) $+,\times$ のそれぞれに関する単位元を答えよ。

(c) 体でないことを確認せよ。

6.5 可換剰余環

$$\Big(\mathbb{R}[X]/\langle 1+X^2\rangle:=\big\{[a+bX]\mid a,b\in\mathbb{R}\big\},\{+,\times\}\Big)$$

に関して、以下に答えよ。

(a) $[a_1+b_1X],[a_2+b_2X]$ の和と積を $[a+bX]$ with $a,b\in\mathbb{R}$ の形で表せ。

(b) $+, \times$ のそれぞれに関する単位元を答えよ。

(c) $\mathbb{R}[X]/\langle 1+X^2\rangle$ は体をなす。非零元

$$[a+bX] \in \mathbb{R}[X]/\langle 1+X^2\rangle$$

の加法と乗法それぞれに関する逆元を求めよ。この体は複素数体と呼ばれている。

6.6 $X^3+X+1 \in \mathbb{F}_2[X]$ が既約多項式であることを証明せよ。

6.7 $\mathbb{F}_7$ の加算、減算、乗算、除算に関する演算表を書け。

6.8 既約多項式 $p(X) := 1+X^2+X^3 \in \mathbb{F}_2[X]$ で生成された有限体 $\mathbb{F}_8 := \Big(\mathbb{F}_2[X]/\langle p(X)\rangle, \{+,\times\}\Big)$ の演算表を示した。以下の問に答えよ。

+	[000]	[100]	[010]	[110]	[001]	[101]	[011]	[111]
[000]	[000]	[100]	[010]	[110]	[001]	[101]	[011]	[111]
[100]	[100]	[000]	[110]	[010]	[101]	[001]	[111]	[011]
[010]	[010]	[110]	[000]	[100]	[011]	[111]	[001]	[101]
[110]	[110]	[010]	[100]	[000]	[111]	[011]	[101]	[001]
[001]	[001]	[101]	[011]	[111]	[000]	[100]	[010]	[110]
[101]	[101]	[001]	[111]	[011]	[100]	[000]	[110]	[010]
[011]	[011]	[111]	[001]	[101]	[010]	[110]	[000]	[100]
[111]	[111]	[011]	[101]	[001]	[110]	[010]	[100]	[000]

x	[000]	[100]	[010]	[110]	[001]	[101]	[011]	[111]
[000]	[000]	[000]	[000]	[000]	[000]	[000]	[000]	[000]
[100]	[000]	[100]	[010]	[110]	[001]	[101]	[011]	[111]
[010]	[000]	[010]	[001]	[011]	[101]	[111]	[100]	[110]

```
[110] | [000] [110] [011] [101] [100] [010] [111] [001]
[001] | [000] [001] [101] [100] [111] [110] [010] [011]
[101] | [000] [101] [111] [010] [110] [011] [001] [100]
[011] | [000] [011] [100] [111] [010] [001] [110] [101]
[111] | [000] [111] [110] [001] [011] [100] [101] [010]
```

(a) $[110] \times [011] = [111]$ となること定義に基づいて説明せよ。

(b) 演算表を使って次の計算の答えを求めよ。

i. $[010] \times [010]$

ii. $[010]^{-1}$

iii. $[011]/[010]$

(c)

$$\begin{pmatrix} [100] & [011] \\ [100] & [101] \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} [010] \\ [101] \end{pmatrix}$$

となる $\alpha_1, \alpha_2 \in \mathbb{F}_8$ を求めよ。

6.9 $\mathbb{F}_{11}$ 上の $[n = 5, k = 3]$RS 符号 C を用いてある符号語を送信して、受信語 $r = [7][4][4][9][2]$ を受信した。以下の問に答えよ。ただし、$\alpha_1 = [0], \ldots, \alpha_5 = [4]$ と選ぶ。

(a) 符号長、次元、符号化率、最小距離を求めよ。

(b) 生成行列 G を求めよ。

(c) 情報ベクトル $[7][5][6]$ を符号化して、符号語を求めよ。

(d) 復号行列 A を求めよ。

(e) 補完多項式 $Q_0(X), Q_1(X)$ を求めよ。

(f) 推定情報ベクトル $\hat{f}$ を求めよ。

6.10 既約多項式 $p(X) := 1 + X^2 + X^3 \in \mathbb{F}_2[X]$ で生成された有限体 $\mathbb{F}_8 := \left(\mathbb{F}_2[X]/\langle p(X)\rangle, \{+, \times\}\right)$ に対して、$\mathbb{F}_8$ 上の $[n = 5, k = 3]$RS 符号 C を用いてある符号語を送信して、受信語 $r = [000][101][110][011][100]$ を受信した。以下の問に答えよ。ただし、

$$(\alpha_1, \ldots, \alpha_5) = ([000], [100], [010], [110], [001])$$

と選ぶ。

(a) 符号長、次元、符号化率、最小距離を求めよ。

(b) 生成行列 G を求めよ。

(c) 情報ベクトル $[001][011][110]$ を符号化して符号語を求めよ。

(d) 復号行列 A を求めよ。

(e) 補完多項式 $Q_0(X), Q_1(X)$ を求めよ。

(f) 推定情報ベクトル $\hat{f}$ を求めよ。

6.11 有限体 $\mathbb{F}$ 上の $[n, k, d]$ 符号はパリティ検査行列 H と生成行列 G を有する。

(a) 以下は等価であることを示せ。

i. C は MDS 符号、即ち $[n, k, n-k+1]$ 符号である。

ii. H の任意の $n-k$ 列は線形独立である。

iii. G の任意の k 列は線形独立である。

(b) 有限体 $\mathbb{F}$ 上の $[n, k, n-k+1]$ 符号 C の双対符号は $[n, n-k, k+1]$ 符号 $C^{\perp}$ となることを示せ。これは MDS 符号の双対符号は MDS 符号になることを表している。

6.12 これまで勉強したところで、分かりにくかったところ、配布資料の誤り、その他なんでもあったら教えて下さい。

7　第7回 演習 (ICT.209 代数系と符号理論)

- 少人数の履修者同士で協力して演習に取り組むことを推奨しています。

7.1 $\mathbb{F}_4 := \mathbb{F}_2[X]/\langle 1+X+X^2\rangle$ に対して、$\beta := [01] \in \mathbb{F}_4$ は3乗するとはじめて $[10]$ になる。β によって定義される $\mathbb{F}_4$ 上の $[n=3,k=2,d=2]$RS 符号を考える。

$$\begin{aligned} C &:= \{(f(\beta^0), f(\beta^1), f(\beta^2) \mid f(X) \in \mathbb{F}_4[X;2]\} \\ &= \{(f([10]), f([01]), f([11])) \mid f(X) \in \mathbb{F}_4[X;2]\} \end{aligned}$$

16通りの情報多項式 $f(X) \in \mathbb{F}_4[X;2]$ に対して、符号多項式 $c(X)$ は以下の対応で与えられる。

```
f=([00][00]),c=([00][00][00])
f=([10][00]),c=([10][10][10])
f=([01][00]),c=([01][01][01])
f=([11][00]),c=([11][11][11])
f=([00][10]),c=([10][01][11])
f=([10][10]),c=([00][11][01])
f=([01][10]),c=([11][00][10])
f=([11][10]),c=([01][10][00])
f=([00][01]),c=([01][11][10])
f=([10][01]),c=([11][01][00])
f=([01][01]),c=([00][10][11])
f=([11][01]),c=([10][00][01])
f=([00][11]),c=([11][10][01])
f=([10][11]),c=([01][00][11])
f=([01][11]),c=([10][11][00])
f=([11][11]),c=([00][01][10])
```

(a) $\beta := [01] \in \mathbb{F}_4$ は3乗するとはじめて $[10]$ になることを示せ。

(b) 対応 `f=([11][11]),c=([00][01][10])` が正しいことを定義にしたがって示せ。

(c) 生成多項式 $g(X)$ を求めよ。

(d) 生成多項式 $g(X)$ と同じ次数の符号語を挙げて、モニックなものは1つしかないことを確認せよ。

(e) $g(X)$ が $X^n - 1$ を割り切ることを示せ。

(f) C の生成行列を一つ求めよ。

(g) パリティ検査多項式 $h(X)$ を求めよ。

(h) 符号語 `c=([01][00][11])` に対して、以下が成り立つことを示せ。

$$c(X)h(X) \bmod X^n - 1 = 0$$

(i) C のパリティ検査行列を一つ求めよ。

7.2 $\mathbb{F}_5 := \mathbb{Z}/5\mathbb{Z}$ に対して、$\beta := [2] \in \mathbb{F}_5$ は4乗するとはじめて $[1]$ になる。β によって定義される $\mathbb{F}_5$ 上の $[n = 4, k = 2, d = 3]$RS 符号を考える。

$$\begin{aligned} C &:= \{(f(\beta^0), f(\beta^1), f(\beta^2), f(\beta^3)) \mid f(X) \in \mathbb{F}_5[X; 2]\} \\ &= \{(f([1]), f([2]), f([4]), f([3])) \mid f(X) \in \mathbb{F}_5[X; 2]\} \end{aligned}$$

25通りの情報多項式 $f(X) \in \mathbb{F}_5[X; 2]$ に対して、符号多項式 $c(X)$ は以下の通り与えられる。

```
f=([0][0]),c=([0][0][0][0])
f=([1][0]),c=([1][1][1][1])
f=([2][0]),c=([2][2][2][2])
f=([3][0]),c=([3][3][3][3])
f=([4][0]),c=([4][4][4][4])
f=([0][1]),c=([1][2][4][3])
f=([1][1]),c=([2][3][0][4])
f=([2][1]),c=([3][4][1][0])
f=([3][1]),c=([4][0][2][1])
f=([4][1]),c=([0][1][3][2])
f=([0][2]),c=([2][4][3][1])
f=([1][2]),c=([3][0][4][2])
f=([2][2]),c=([4][1][0][3])
f=([3][2]),c=([0][2][1][4])
f=([4][2]),c=([1][3][2][0])
f=([0][3]),c=([3][1][2][4])
f=([1][3]),c=([4][2][3][0])
f=([2][3]),c=([0][3][4][1])
f=([3][3]),c=([1][4][0][2])
f=([4][3]),c=([2][0][1][3])
f=([0][4]),c=([4][3][1][2])
f=([1][4]),c=([0][4][2][3])
f=([2][4]),c=([1][0][3][4])
f=([3][4]),c=([2][1][4][0])
f=([4][4]),c=([3][2][0][1])
```

(a) $\beta := [2] \in \mathbb{F}_5$ は 4 乗するとはじめて 1 になることを示せ。

(b) 対応 `f=[4][3],c=[2][0][1][3]` が正しいことを定義にしたがって示せ。

(c) 生成多項式 $g(X)$ を求めよ。

(d) 生成多項式 $g(X)$ と同じ次数の符号語を挙げて、モニックなものは 1 つしかないことを確認せよ。

(e) $g(X)$ が $X^n - 1$ を割り切ることを示せ。

(f) C の生成行列を一つ求めよ。

(g) パリティ検査多項式 $h(X)$ を求めよ。

(h) 符号語 `c=([2][1][4][0])` に対して、以下が成り立つことを示せ。

$$c(X)h(X) \bmod X^n - 1 = 0$$

(i) C のパリティ検査行列を一つ求めよ。

(j) C の双対符号 $C^\perp$ の生成多項式を求めよ。

7.3 有限体 $\mathbb{F}$ に対して、$g(X) \mid X^n - 1, \deg g(X) = n - k$ を満たすモニックな非零多項式 $g(X) \in \mathbb{F}[X]$ を用いて定義される

$$C = \{u(X)g(X) \mid u(X) \in \mathbb{F}[X;k]\} \subset \mathbb{F}[X;n]$$

は、$\mathbb{F}$ 上の $[n,k]$ 巡回符号となることを示せ。

7.4 $\mathbb{F}$ 上の長さ n の巡回符号のうち、零ベクトルだけからなる符号 $\{\overbrace{0\cdots0}^{n}\}$ と全ベクトルからなる符号 $\mathbb{F}^n$ は自明であるという。

(a) $\mathbb{F}_2$ 上の符号長 $n = 3$ の巡回符号で非自明なものをすべて挙げよ。

(b) $\mathbb{F}_2$ 上の符号長 $n = 4$ の巡回符号で非自明なものをすべて挙げよ。

7.5 集合 $(i),(j),(k),(m)$ に対して、$(i) \subset (j) \cup (k), (i) \cap (j) \subset (m)$ ならば、$(i) \setminus (m) \subset (k)$ となることをベン図で確かめよ。

7.6 有限体 $\mathbb{F}_7 := \mathbb{Z}/7\mathbb{Z}$ について以下の問に答えよ。

(a) $\mathbb{F}_7$ の各元の位数を求めよ。

(b) $\mathbb{F}_7$ の原始元をすべて挙げよ。

(c) $[3]^{999}$ を求めよ。

7.7 既約多項式 $p(X) := 1 + X + X^3 \in \mathbb{F}_2[X]$ で生成された有限体 $\mathbb{F}_8 := \Big(\mathbb{F}_2[X]/\langle p(X)\rangle, \{+, \times\}\Big)$ について以下の問に答えよ。

(a) $\mathbb{F}_8$ の各元の位数を求めよ。

(b) $\mathbb{F}_8$ の原始元をすべて挙げよ。

(c) $[111]^{999}$ を求めよ。

7.8 有限体 $\mathbb{F}_q$ の非零元 β に対して、$\mathrm{ord}(\beta)$ は有限であることを示せ。

7.9 $[n,k]$ 巡回符号 C の生成符号 $g(X) = \sum_{i=0}^{n-k} g_i X^i$ に対して、$g_0 \neq 0$ であることを証明せよ。

7.10 これまで勉強したところで、分かりにくかったところ、配布資料の誤り、その他なんでもあったら教えて下さい。

8　第8回 演習 (ICT.209 代数系と符号理論)

- 少人数の履修者同士で協力して演習に取り組むことを推奨しています。

8.1 原始多項式 $1 + X + X^3 \in \mathbb{F}_2[X]$ の根 α を用いて定義される $\mathbb{F}_8$ に対して、$\mathbb{F}_8$ の元の冪表現 α^i with $0 \leq i \leq 6$ と $\mathbb{F}_8$ の元の多項式表現

$$(f_0\ f_1\ f_2) = f_0 + f_1\alpha + f_2\alpha^2 \text{ with } f_0, f_1, f_2 \in \mathbb{F}_2$$

について、以下の問に答えよ。

(a) $\mathbb{F}_8$ の元の冪表現に対応する多項式表現を求めよ。

(b) $\mathbb{F}_8$ の非零元の冪表現を各行と各列として、積の演算表を書け。

(c) $\mathbb{F}_8$ の元の多項式表現を各行各列として、和の演算表を書け。

(d) $\alpha^{50} + \alpha^{100}$ の冪表現とベクトル表現を求めよ。

8.2 原始多項式 $1 + X^3 + X^4 \in \mathbb{F}_2[X]$ によって定義される $\mathbb{F}_{16}$ の原始元を α とする。以下の問に答えよ。

(a) 各非零元 α^i の $\mathbb{F}_2$ 上の最小多項式 $m_i(X)$ を求めよ。

(b) $t = 2$ ビットまでの誤りを訂正可能な設計距離 $2t+1 = 5$、符号長 15 の BCH 符号の生成多項式 $g(X) \in \mathbb{F}_2[X]$ を構成せよ。

(c) $t = 3$ ビットまでの誤りを訂正可能な設計距離 $2t+1 = 7$、符号長 15 の BCH 符号の生成多項式 $g(X) \in \mathbb{F}_2[X]$ を構成せよ。

8.3 素数 p に対して、$q = p^m$ とする。モニック既約多項式 $f(X) \in \mathbb{F}_p[X]$ に対して、$\alpha \in \mathbb{F}_q$ が $f(X)$ の根ならば、$f(X)$ は α の $\mathbb{F}_p$ 上の最小多項式であることを示せ。

8.4 素数 p に対して、$q = p^m$ とする。位数 n の元を $\alpha \in \mathbb{F}_q$ とする。

(a) $n \mid p^m - 1$ であることを示せ。

(b) 最小多項式 $M(X)$ の根はすべて同じ位数 n を有することを示せ。

8.5 各正の整数 n に対して、1 から n までの自然数のうち n と互いに素なものの個数を $\phi(n)$ と書き、オイラー関数と呼ぶ。素数 p に対して、$q = p^m$ とする。原始元を $\alpha \in \mathbb{F}_q$ とする。以下の問に答えよ。

(a) $\mathbb{F}_q$ に含まれる原始元の数は $\varphi(q-1)$ であることを示せ。

(b) n の素因数分解が次のように

$$n = \prod_{k=1}^{d} {p_k}^{e_k}$$

と与えられているならば、

$$\varphi(n) = \prod_{k=1}^{d} \left({p_k}^{e_k} - {p_k}^{e_k - 1} \right) = n \prod_{k=1}^{d} \left(1 - \frac{1}{p_k} \right)$$

によって $\varphi(n)$ を計算することができる。$\mathbb{F}_{64}$ に含まれる原始元の数を求めよ。

代数系と符号理論 期末試験 (令和元年 11 月 25 日)

1. **１枚の解答用紙につき大問１つを回答すること**. 答案用紙には答えのみでなく、それを導く過程も記入すること。
2. **全ての答案用紙に名前と学籍番号を忘れず記入すること。**
3. 各大問は独立しており，特に断りのない限り大問間で設定や記号等は共有されない.
4. 試験開始 30 分までの退室と、試験終了 10 分前からの退室と、試験開始 30 分からの入室を禁ずる。
5. 答案を提出せずに退室することはできません。
6. 用紙が足りない場合は裏も使って良い。その場合には表面の右下に「裏面に続く」と書いてください。
7. 試験時間内にすべての問題に解答できるように作問されていない。
8. 各大問において小問は易しい順に並んでいる。
9. 易しい小問ほど配点が高い。
10. 変数 x の範囲を限定せずに命題 $P(x)$ を参照する場合には、命題 $P(x)$ が文脈上意味のある範囲で x の範囲が限定されているものとする。
11. 設定が不明な場合には、文脈上もっとも尤もらしい解釈で理解すること。
12. 設定に不備や矛盾がある場合には、文脈上もっとも尤もらしい修正を施して理解すること。

F.1 (a) 以下の $\mathbb{F}_2[X]$ の多項式に関する計算を求めよ。

i. $1+1$

ii. $(1+X^2+X^3)+(1+X+X^2)$

iii. $(1+X)(1-X)$

iv. $1+X^2+X^6$ を $1+X$ で割った商と剰余。

(b) 既約多項式 $p(X) := 1+X^2+X^3 \in \mathbb{F}_2[X]$ で生成された有限体 $\mathbb{F}_8 := \Big(\mathbb{F}_2[X]/\langle p(X)\rangle, \{+,\times\}\Big)$ に関して以下の問に答えよ。

i. 次の計算の答えを求めよ。

A. $[010]\times[010]$

B. $[010]^{-1}$

C. $[011]/[010]$

ii.

$$\begin{pmatrix}[100] & [011]\\ [100] & [101]\end{pmatrix}\begin{pmatrix}\alpha_1\\ \alpha_2\end{pmatrix} = \begin{pmatrix}[010]\\ [101]\end{pmatrix}$$

となる $\alpha_1, \alpha_2 \in \mathbb{F}_8$ を求めよ。

(c) p を素数とする。剰余類環

$$\mathbb{F}_p := \Big(\mathbb{Z}/p\mathbb{Z}, \{+,\times\}\Big)$$

は $[1] \in \mathbb{F}_p$ を乗法単位元とする単位的可換環になる。任意の非零元

$$[a] \in \mathbb{F}_p$$

に対して乗法に関する逆元が存在することを示せ。

F.2 $\alpha_1, \ldots, \alpha_n$ を互いに異なる $\mathbb{F}_q$ の元とする．このため、$n \leq q$ となる。$\mathbb{F}_q[X;k]$ は $\mathbb{F}_q$ を係数とする次数が k 未満の多項式

$$f(X) = \sum_{i=0}^{k-1} f_i X^i$$

の集合である。情報多項式 $f(x) \in \mathbb{F}_q[X;k]$ に対して、

$$\vec{c}(f) := \big(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)\big) \in \mathbb{F}_q^n$$

を符号語とする符号空間を、$\mathbb{F}_q$ 上の $[n,k]$RS 符号という。正確に書くと、

$$\Big\{\vec{c}(f) \in \mathbb{F}_q^n \mid f(X) \in \mathbb{F}_q[X;k]\Big\}$$

として定義される。

以下の問に答えよ。

(a) $\mathbb{F}_7$ 上の $[n=5, k=3]$RS 符号 C を用いた通信を考える。ただし、$\alpha_1 = [0], \ldots, \alpha_5 = [4]$ と選ぶ。

i. 符号長、次元、符号化率、最小距離を求めよ。

ii. 生成行列 G を求めよ。

iii. 情報ベクトル $[4][0][3]$ を符号化して、符号語を求めよ。

iv. ある符号語を送信して、受信語 $r = [0][5][2][6][3]$ を受信した。講義で学習した RS 符号の復号法に関して、以下の問に答えよ。復号行列 A を求めよ。

v. 前問の設定で、補完多項式 $Q_0(X), Q_1(X)$ を求めよ。

vi. 前問の設定で、推定情報ベクトル $\hat{f}$ を求めよ。

(b) 有限体 $\mathbb{F}$ 上の $[n,k]$RS 符号 C の最小重みまたは最小距離が $n-k+1$ であることを示せ。

(c) $\mathbb{F}_q$ の非ゼロ要素 β が n 乗して始めて 1 に等しくなるとする。このとき、n は $q-1$ を割り切る様に選ばなければならない。$\beta^0, \ldots, \beta^{n-1}$ によって定義された $\mathbb{F}_q$ 上の $[n,k]$RS 符号

$$C = \left\{ \vec{c}(f) \mid f(X) \in \mathbb{F}_q[X;k] \right\}$$
$$\vec{c}(f) := \left(f(\beta^0), f(\beta^1), \ldots, f(\beta^{n-1}) \right)$$

は巡回符号となることを示せ。線形性は示さなくて良い。

F.3 以下の問に答えよ。

(a) 下記の $\mathbb{F}_2$ 上の符号 C が巡回符号である場合には、その次元と符号長を答えよ。そうでない場合にはその理由を答えよ。

i.

$$C = \{(0000), (1001), (0011), (0110),$$
$$(1100), (1010), (0101), (1111)\}$$

ii.

$$C = \{(0000), (1000), (0100), (0010), (0001)\}$$

(b) $g(X) = 1+X^2 \in \mathbb{F}_2[X]$ によって生成される長さ $n = 4$ の $\mathbb{F}_2$ 上の巡回符号の符号語を列挙せよ。

(c) $\mathbb{F}_2$ 上の長さ n の巡回符号のうち、零ベクトルだけからなる符号 $\{\overbrace{0\cdots0}^{n}\}$ と全ベクトルからなる符号 $\mathbb{F}_2^n$ は自明であるという。$\mathbb{F}_2$ 上の符号長 $n = 4$ の非自明な巡回符号の生成多項式をすべて挙げよ。

(d) 下記の $\mathbb{F}_5$ 上の符号 C は巡回符号である。C に関する以下の値を求めよ。

i. 次元 k

ii. 生成多項式 $g(X) \in \mathbb{F}_5[X]$

iii. パリティ検査多項式 $h(X) \in \mathbb{F}_5[X]$

iv. C の双対符号 $C^\perp$ の生成多項式 $g^\perp(X) \in \mathbb{F}_5[X]$

```
C={
   ([0][0][0][0]),([1][1][1][1]),([2][2][2][2]),
   ([3][3][3][3]),([4][4][4][4]),([1][3][4][2]),
   ([2][4][0][3]),([3][0][1][4]),([4][1][2][0]),
   ([0][2][3][1]),([2][1][3][4]),([3][2][4][0]),
   ([4][3][0][1]),([0][4][1][2]),([1][0][2][3]),
   ([3][4][2][1]),([4][0][3][2]),([0][1][4][3]),
   ([1][2][0][4]),([2][3][1][0]),([4][2][1][3]),
   ([0][3][2][4]),([1][4][3][0]),([2][0][4][1]),
   ([3][1][0][2])
}
```

(e) 有限体 $\mathbb{F}$ に対して、$g(X) \mid X^n - 1, \deg g(X) = n - k$ を満たすモニックな非零多項式 $g(X) \in \mathbb{F}[X]$ を用いて定義される

$$C = \{u(X)g(X) \mid u(X) \in \mathbb{F}[X; k]\} \subset \mathbb{F}[X; n]$$

は、$\mathbb{F}$ 上の $[n, k]$ 巡回符号となることを示せ。ただし線形性は示さなくて良い。

F.4 以下の問に答えよ。

(a) 原始多項式 $1 + X + X^3 \in \mathbb{F}_2[X]$ の根 α を用いて定義される $\mathbb{F}_8$ に対して、$\mathbb{F}_8$ の元の冪表現 α^i with $0 \leq i \leq 6$ と $\mathbb{F}_8$ の元の多項式表現 $f_0 + f_1\alpha + f_2\alpha^2$ with $f_0, f_1, f_2 \in \mathbb{F}_2$ のベクトル表現を

$$(f_0\ f_1\ f_2)$$

と書くこととする。以下の問に答えよ。

i. $\mathbb{F}_8$ の非零元の冪表現に対応する多項式表現を求めよ。

ii. $\alpha^{50} + \alpha^{100}$ の冪表現とベクトル表現を求めよ。

(b) 素数 p に対して $q = p^m$ とする。 $\alpha \in \mathbb{F}_q$ の $\mathbb{F}_p$ 上の最小多項式 $M(X)$ に対して、$M(X)$ は存在すれば唯一であることを示せ。

(c) 素数 p に対して $q = p^m$ とする。 $\alpha \in \mathbb{F}_q$ の $\mathbb{F}_p$ 上の最小多項式 $M(X)$ に対して、$M(X)$ は存在すれば既約であることを示せ。

F.5 原始多項式 $1 + X + X^4 \in \mathbb{F}_2[X]$ によって定義される $\mathbb{F}_{16}$ の原始元を α とする。各非零元 α^i の $\mathbb{F}_2$ 上の最小多項式 $m_i(X)$ は以下の通りである。

α^i	$m_i(X)$
α^0	$1 + X$
α^1, (1), (2), (3)	(11)
α^3, (4), (5), (6)	$1 + X + X^2 + X^3 + X^4$
α^5, (7)	(12)
α^7, (8), (9), (10)	(13)

(a) 空欄を埋めよ。

(b) $t = 2$ ビットまでの誤りを訂正可能な設計距離 $2t+1 = 5$、符号長 $n = 15$ の BCH 符号の生成多項式 $g(X)$ を求めよ。

(c) $t = 3$ ビットまでの誤りを訂正可能な設計距離 $2t+1 = 7$、符号長 $n = 15$ の BCH 符号の生成多項式 $g(X)$ を求めよ。

(d) 設計距離 $2t + 1$ の BCH 符号の最小距離が $2t + 1$ 以上になることを示せ。ただし、ヴァンデルモンド行列の性質を証明無しで用いて良い。

代数系と符号理論 課題 (令和３年度)

1. この課題の出来不出来は、成績に支配的に影響します。

2. 解の導出過程を書くこと。

3. 少人数の履修者同士で協力して課題に取り組むことを推奨しています。ただし、答案を書き写させること、および書き写すことをしてはいけません。

4. 証明ができていないのに証明できたように装って回答することは、不正行為とみなされることがあります。分からないときには、分かっているように振舞わずに、「私は＊＊が分かりません」と宣言してください。分からないことを宣言して考察すると、加点されることがあります。

5. 答案の上部に、氏名、学籍番号、科目コード（ICT.C209)、[協力者および被協力者の氏名]を記入すること。

6. 全ての提出用紙に名前と学籍番号を忘れず記入すること。

7. 各大問は独立しており，特に断りのない限り大問間で設定や記号等は共有されない.

8. １枚の解答用紙につき大問を２問以上回答してはいけない。

9. 用紙が足りない場合は２枚以上に渡って大問一問を回答しても良い。その場合には最終ページ以外のページの右下に「次ページに続く」と書いてください。

10. 各大問において小問は易しい順に並んでいる。

11. 易しい小問ほど配点が高い。

12. 変数 x の範囲を限定せずに命題 $P(x)$ を参照する場合には、命題 $P(x)$ が文脈上意味のある範囲で x の範囲が限定されているものとする。

13. 設定が不明な場合には、文脈上もっとも尤もらしい解釈で理解すること。

14. 設定に不備や矛盾がある場合には、文脈上もっとも尤もらしい修正を施して理解すること。

15. 証明問題に対して、講義資料の証明や、宿題の例解は、そのまま書き写しても正解とならないことがあります。

K.1 以下の問に答えよ。

(a) 以下の 2 元符号の符号長、最小距離、符号化率を答えよ。

$$
\begin{aligned}
C = \{&100001011001,\\
&111010001100,\\
&001101010010,\\
&110110110101\}
\end{aligned}
$$

(b) 次の長さ 12 の 4 つの行ベクトルからなる符号

$$
\begin{aligned}
C = \{&\\
&111011111110\\
&010100001010\\
&111001111000\\
&110001110111\}
\end{aligned}
$$

を用いた通信における受信語 $\vec{r} = 010101111101$ に対して、最小距離復号の出力 $\hat{c}^{(\mathrm{MD})}(\vec{r})$ と、半径 $t := \lfloor \frac{d(C)-1}{2} \rfloor$ の限界距離復号の出力 $\hat{c}_t^{(\mathrm{BD})}$ を求めよ。

K.2 (a) 以下の集合について、それが二元線形符号であるか否か述べ、二元線形符号でない場合にはその理由を述べよ。二元線形符号である場合にはその次元、生成行列，最小距離，符号化率を求めよ。

$$C_1 = \{01, 10, 11\}$$

$$C_2 = \{00000, 10110, 01101, 11011, \\ 11111, 01001, 10010, 00100\}$$

(b) 次を満たす $x_1, \ldots, x_4 \in \mathbb{F}_2$ を求めよ。

$$\begin{pmatrix} 1000 \\ 1011 \\ 1111 \\ 0001 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

(c) 以下で定義される、長さ n の 2 元符号 C を繰り返し符号という。

$$C = \{x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n \mid x_1 = \cdots = x_n\}$$

$n = 3$ のとき C とその双対符号 $C^\perp$ の符号語を列挙せよ。

(d) 2 元線形符号 C の双対符号を $C^{\perp}$ とする。$C^{\perp}$ の重み分布多項式 $B(X,Y)$ から、C の最小距離 d と $C^{\perp}$ の最小距離 $d^{\perp}$ を求める方法を述べよ。

K.3 符号長 7 のハミング符号 C は下の標準型パリティ検査行列 H で定義される二元線形符号である。

$$H = \begin{pmatrix} 1011\ 100 \\ 1101\ 010 \\ 0111\ 001 \end{pmatrix}$$

長さ 7 のハミング符号に関して、以下の問に答えよ。

(a) H に対応する標準型生成行列 G を求めよ。

(b) 前問で得られた生成行列 G を用いて情報ベクトル (1010) を符号化して得られる符号語を求めよ。

(c) 受信語が (1111101) であったときに講義で説明した復号法を実施して、推定符号語を求めよ。

(d) 符号語数、次元、符号化率を求めよ。

(e) 最小距離が 3 以上であることを証明せよ。

(f) 最小距離が 3 以下であることを証明せよ。

K.4 以下の問に答えよ。

(a) 以下の集合と二項演算の組み合わせが，群であるための条件をすべて満たすか否か答えよ。群となる場合にはその

単位元 e と元 x に対する逆元を明らかにし，群とならない場合にはその理由を述べよ．

i. 有理数の集合とその加算

ii. 非零実数の集合とその乗算

iii. 2×2 実行列の集合と行列の乗算

iv. 授業で扱ってない群の例を挙げ、群となることを示せ。

(b) 99221 と 97343 の最大公約数を g とする。拡張ユークリッドの互除法を用いて、$g = 99221x + 97343y$ となる整数 x, y を求めよ。

K.5 (a) 以下の $\mathbb{F}_2[X]$ の多項式に関する計算を求めよ。

i. $1 + 1$

ii. $(1 + X^2 + X^3) + (1 + X + X^2)$

iii. $(1 + X)(1 - X)$

iv. $1 + X^2 + X^6$ を $1 + X$ で割った商と剰余。

(b) 既約多項式 $p(X) := 1 + X^2 + X^3 \in \mathbb{F}_2[X]$ で生成された有限体 $\mathbb{F}_8 := \left(\mathbb{F}_2[X]/\langle p(X)\rangle, \{+, \times\}\right)$ に関して以下の問に答えよ。

i. 次の計算の答えを求めよ。

A. $[010] \times [010]$

B. $[010]^{-1}$

C. $[011]/[010]$

ii.

$$\begin{pmatrix} [100] & [011] \\ [100] & [101] \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} [010] \\ [101] \end{pmatrix}$$

となる $\alpha_1, \alpha_2 \in \mathbb{F}_8$ を求めよ。

K.6 $\alpha_1, \ldots, \alpha_n$ を互いに異なる $\mathbb{F}_q$ の元とする．このため、$n \leq q$ となる。$\mathbb{F}_q[X;k]$ は $\mathbb{F}_q$ を係数とする次数が k 未満の多項式

$$f(X) = \sum_{i=0}^{k-1} f_i X^i$$

の集合である。情報多項式 $f(x) \in \mathbb{F}_q[X;k]$ に対して、

$$\vec{c}(f) := \big(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)\big) \in \mathbb{F}_q^n$$

を符号語とする符号空間を、$\mathbb{F}_q$ 上の $[n,k]$RS 符号という。正確に書くと、

$$\Big\{ \vec{c}(f) \in \mathbb{F}_q^n \mid f(X) \in \mathbb{F}_q[X;k] \Big\}$$

として定義される。

以下の問に答えよ。

(a) $\mathbb{F}_7$ 上の $[n=5, k=3]$RS 符号 C を用いた通信を考える。ただし、$\alpha_1 = [0], \ldots, \alpha_5 = [4]$ と選ぶ。

i. 符号長、次元、符号化率、最小距離を求めよ。

ii. 生成行列 G を求めよ。

iii. 情報ベクトル $[4][0][3]$ を符号化して、符号語を求めよ。

iv. ある符号語を送信して、受信語 $r = [0][5][2][6][3]$ を受信した。講義で学習した RS 符号の復号法に関して、以下の問に答えよ。復号行列 A を求めよ。

v. 前問の設定で、補完多項式 $Q_0(X), Q_1(X)$ を求めよ。

vi. 前問の設定で、推定情報ベクトル $\hat{f}$ を求めよ。

(b) n 個の実数 $c_1, \ldots, c_n \in \mathbb{R}$ を入力すると、t 個の入力を誤って出力する通信路を考える。この通信路を介して、k 個の情報 $u_0, \ldots, u_{k-1} \in \mathbb{R}$ を、誤り無く伝えたい。$t \leq \lfloor \frac{n-k}{2} \rfloor$ 個までの誤りを訂正可能な、符号化法

$$(u_0, \ldots, u_{k-1}) \mapsto (c_1, \ldots, c_n)$$

を答えよ。

K.7 以下の問に答えよ。

(a) 原始多項式 $1 + X + X^3 \in \mathbb{F}_2[X]$ の根 α を用いて定義される $\mathbb{F}_8$ に対して、$\mathbb{F}_8$ の元の冪表現 α^i with $0 \leq i \leq 6$ と $\mathbb{F}_8$ の元の多項式表現 $f_0 + f_1\alpha + f_2\alpha^2$ with $f_0, f_1, f_2 \in \mathbb{F}_2$ のベクトル表現を

$$(f_0\ f_1\ f_2)$$

と書くこととする。以下の問に答えよ。

i. $\mathbb{F}_8$ の非零元の冪表現に対応する多項式表現とベクトル表現を求めよ。

ii. $\alpha^{50} + \alpha^{100}$ の冪表現とベクトル表現を求めよ。

K.8 原始多項式 $1 + X^3 + X^4 \in \mathbb{F}_2[X]$ によって定義される $\mathbb{F}_{16}$ の原始元を α とする。各非零元 α^i の $\mathbb{F}_2$ 上の最小多項式 $m_i(X)$ は以下の通りである。

α^i	$m_i(X)$
α^0	$1 + X$
$\alpha^1, \boxed{(1)}, \boxed{(2)}, \boxed{(3)}$	$\boxed{(11)}$
$\alpha^3, \boxed{(4)}, \boxed{(5)}, \boxed{(6)}$	$1 + X + X^2 + X^3 + X^4$
$\alpha^5, \boxed{(7)}$	$\boxed{(12)}$
$\alpha^7, \boxed{(8)}, \boxed{(9)}, \boxed{(10)}$	$\boxed{(13)}$

(a) 空欄を埋めよ。

(b) $t = 2$ ビットまでの誤りを訂正可能な設計距離 $2t+1 = 5$、符号長 $n = 15$ の BCH 符号の生成多項式 $g(X)$ を求めよ。

(c) $t = 3$ ビットまでの誤りを訂正可能な設計距離 $2t+1 = 7$、符号長 $n = 15$ の BCH 符号の生成多項式 $g(X)$ を求めよ。

K.9 次の問題を解け。

(a) 出題範囲をこの講義全体とする試験問題を作問しなさい。（良い問題は来年以降の講義で使用する場合があります。

使用されることを希望しない場合にはその旨を書いておいてください。）

(b) (a) で作問した問題を解け。

(c) (a) で作問した問題の出題意図を解説せよ。

代数系と符号理論 期末試験 (令和 4 年 12 月 1 日)

1. **１枚の解答用紙につき大問１つを回答すること**. 答案用紙には答えのみでなく、それを導く過程も記入すること。
2. **全ての答案用紙に名前と学籍番号を忘れず記入すること。**
3. 各大問は独立しており，特に断りのない限り大問間で設定や記号等は共有されない.
4. 試験開始 30 分までの退室と、試験終了 10 分前からの退室と、試験開始 30 分からの入室を禁ずる。
5. 答案を提出せずに退室することはできません。
6. 用紙が足りない場合は裏も使って良い。その場合には表面の右下に「裏面に続く」と書いてください。
7. 試験時間内にすべての問題に解答できるように作問されていない。
8. 各大問において小問は易しい順に並んでいる。
9. 易しい小問ほど配点が高い。
10. 変数 x の範囲を限定せずに命題 $P(x)$ を参照する場合には、命題 $P(x)$ が文脈上意味のある範囲で x の範囲が限定されているものとする。
11. 設定が不明な場合には、文脈上もっとも尤もらしい解釈で理解すること。
12. 設定に不備や矛盾がある場合には、文脈上もっとも尤もらしい修正を施して理解すること。

F.1 (a) 以下の $\mathbb{F}_2[X]$ の多項式に関する計算を求めよ。

i. $1+1$

ii. $(1+X^2+X^3)+(1+X+X^2)$

iii. $(1+X+X^2+X^3+X^4+X^5)(1+X)$

iv. $1+X^2+X^6$ を $1+X$ で割った商と剰余。

v. 次の多項式が、既約であるか可約であるか答えよ。既約である場合にはその理由を答え、可約である場合にはその因数分解を答えよ。

A. $X^2+1 \in \mathbb{R}[X]$

B. $X^2+1 \in \mathbb{C}[X]$

C. $X^2+1 \in \mathbb{F}_2[X]$

D. $X^3+X+1 \in \mathbb{F}_2[X]$

(b) 既約多項式 $p(X) := 1+X^2+X^3 \in \mathbb{F}_2[X]$ で生成された有限体 $\mathbb{F}_8 := \Big(\mathbb{F}_2[X]/\langle p(X)\rangle, \{+,\times\}\Big)$ に関して以下の問に答えよ。

i. 次の計算の答えを求めよ。

A. $[010]\times[010]$

B. $[001]\times[010]$

C. $[010]^{-1}$

(c) 体 $\mathbb{F}$ を係数とする次数 $m \geq 1$ のモニック既約多項式 $p(X) \in \mathbb{F}[X]$ に対して、イデアル $\langle p(X)\rangle$ を法とする剰余類環

$$\Big(\mathbb{F}[X]/\langle p(X)\rangle, \{+,\times\}\Big)$$

は $[1] \in \mathbb{F}[X]/\langle p(X)\rangle$ を乗法単位元とする単位的可換環になる。任意の非零元

$$[a(X)](\neq [0]) \in \mathbb{F}[X]/\langle p(X)\rangle$$

に対して乗法に関する逆元が存在することを示せ。

F.2 $\alpha_1, \ldots, \alpha_n$ を互いに異なる $\mathbb{F}_q$ の元とする．このため、$n \leq q$ となる。$\mathbb{F}_q[X;k]$ は $\mathbb{F}_q$ を係数とする次数が k 未満の多項式

$$f(X) = \sum_{i=0}^{k-1} f_i X^i$$

の集合である。情報多項式 $f(x) \in \mathbb{F}_q[X;k]$ に対して、

$$\vec{c}(f) := \big(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)\big) \in \mathbb{F}_q^n$$

を符号語とする符号空間を、$\mathbb{F}_q$ 上の $[n,k]$RS 符号という。正確に書くと、

$$\Big\{\vec{c}(f) \in \mathbb{F}_q^n \mid f(X) \in \mathbb{F}_q[X;k]\Big\}$$

として定義される。

以下の問に答えよ。

(a) $\mathbb{F}_5$ 上の $[n=5, k=3]$RS 符号 C を用いた通信を考える。ただし、$\alpha_1 = [0], \ldots, \alpha_5 = [4]$ と選ぶ。

i. 符号長、次元、符号化率、最小距離を求めよ。

ii. 生成行列 G を求めよ。

iii. 情報ベクトル [3][4][0] を符号化して、符号語を求めよ。

iv. ある符号語を送信して、受信語 $r = [3][3][3][4][4]$ を受信した。講義で学習した RS 符号の復号法に関して、以下の問に答えよ。復号行列 A を求めよ。

v. 前問の設定で、補完多項式 $Q_0(X), Q_1(X)$ を求めよ。

vi. 前問の設定で、推定情報ベクトル $\hat{f}$ を求めよ。

(b) 有限体 $\mathbb{F}$ 上の $[n, k]$RS 符号 C の最小重みまたは最小距離が $n - k + 1$ であることを示せ。

(c) n 個の複素数 $c_1, \ldots, c_n \in \mathbb{C}$ を入力すると、t 個の入力を誤って出力する通信路を考える。この通信路を介して、k 個の情報 $u_0, \ldots, u_{k-1} \in \mathbb{C}$ を、誤り無く伝えたい。$\alpha_1, \ldots, \alpha_n$ を相異なる n 個の複素数とする。$t \leq \lfloor \frac{n-k}{2} \rfloor$ 個までの誤りを訂正可能な、符号化法

$$(u_0, \ldots, u_{k-1}) \mapsto (c_1, \ldots, c_n)$$

を $\alpha_1, \ldots, \alpha_n$ を用いて具体的に答えよ。

F.3 以下の問に答えよ。

(a) 下記の $\mathbb{F}_2$ 上の符号 C が巡回符号である場合には、その次元と符号長を答えよ。そうでない場合にはその理由を答えよ。

i.

$$C = \{(0000), (1001), (0011), (0110),$$
$$(1100), (1010), (0101), (1111)\}$$

ii.

$$C = \{(0000), (1000), (0100), (0010), (0001)\}$$

(b) $g(X) = 1+X^2 \in \mathbb{F}_2[X]$ によって生成される長さ $n = 4$ の $\mathbb{F}_2$ 上の巡回符号の符号語を列挙せよ。

(c) $\mathbb{F}_2$ 上の長さ n の巡回符号のうち、零ベクトルだけからなる符号 $\{\overbrace{0\cdots0}^{n}\}$ と全ベクトルからなる符号 $\mathbb{F}_2^n$ は自明であるという。$\mathbb{F}_2$ 上の符号長 $n = 4$ の非自明な巡回符号の生成多項式をすべて挙げよ。

(d) 下記の $\mathbb{F}_5$ 上の符号 C は巡回符号である。C に関する以下の値を求めよ。

i. 次元 k

ii. 生成多項式 $g(X) \in \mathbb{F}_5[X]$

iii. パリティ検査多項式 $h(X) \in \mathbb{F}_5[X]$

iv. C の双対符号 $C^\perp$ の生成多項式 $g^\perp(X) \in \mathbb{F}_5[X]$

```
C={
   ([0][0][0][0]),([1][1][1][1]),([2][2][2][2]),
   ([3][3][3][3]),([4][4][4][4]),([1][3][4][2]),
   ([2][4][0][3]),([3][0][1][4]),([4][1][2][0]),
```

```
   ([0][2][3][1]),([2][1][3][4]),([3][2][4][0]),
   ([4][3][0][1]),([0][4][1][2]),([1][0][2][3]),
   ([3][4][2][1]),([4][0][3][2]),([0][1][4][3]),
   ([1][2][0][4]),([2][3][1][0]),([4][2][1][3]),
   ([0][3][2][4]),([1][4][3][0]),([2][0][4][1]),
   ([3][1][0][2])
}
```

(e) 有限体 $\mathbb{F}$ に対して、$g(X) \mid X^n - 1, \deg g(X) = n - k$ を満たすモニックな非零多項式 $g(X) \in \mathbb{F}[X]$ を用いて定義される

$$C = \{u(X)g(X) \mid u(X) \in \mathbb{F}[X; k]\} \subset \mathbb{F}[X; n]$$

は、$\mathbb{F}$ 上の $[n, k]$ 巡回符号となることを示せ。ただし線形性は示さなくて良い。

F.4 以下の問に答えよ。

(a) 原始多項式 $1 + X + X^3 \in \mathbb{F}_2[X]$ の根 α を用いて定義される $\mathbb{F}_8$ に対して、$\mathbb{F}_8$ の元の冪表現 α^i with $0 \leq i \leq 6$ と $\mathbb{F}_8$ の元の多項式表現

$$(f_0\ f_1\ f_2) = f_0 + f_1\alpha + f_2\alpha^2 \text{ with } f_0, f_1, f_2 \in \mathbb{F}_2$$

について、以下の問に答えよ。

i. $\mathbb{F}_8$ の非零元の冪表現に対応する多項式表現を求めよ。

ii. $\alpha^{50} + \alpha^{100}$ の冪表現とベクトル表現を求めよ。

(b) 素数 p に対して $q = p^m$ とする。 $\alpha \in \mathbb{F}_q$ の $\mathbb{F}_p$ 上の最小多項式 $M(X)$ に対して、$M(X)$ は存在すれば唯一であることを示せ。

(c) 素数 p に対して $q = p^m$ とする。 $\alpha \in \mathbb{F}_q$ の $\mathbb{F}_p$ 上の最小多項式 $M(X)$ に対して、$M(X)$ は存在すれば既約であることを示せ。

F.5 原始多項式 $1 + X^3 + X^4 \in \mathbb{F}_2[X]$ によって定義される $\mathbb{F}_{16}$ の原始元を α とする。各非零元 α^i の $\mathbb{F}_2$ 上の最小多項式 $m_i(X)$ は以下の通りである。

α^i	$m_i(X)$
α^0	$1 + X$
$\alpha^1, \boxed{(1)}, \boxed{(2)}, \boxed{(3)}$	$\boxed{(11)}$
$\alpha^3, \boxed{(4)}, \boxed{(5)}, \boxed{(6)}$	$1 + X + X^2 + X^3 + X^4$
$\alpha^5, \boxed{(7)}$	$\boxed{(12)}$
$\alpha^7, \boxed{(8)}, \boxed{(9)}, \boxed{(10)}$	$\boxed{(13)}$

(a) 空欄を埋めよ。

(b) $t = 2$ ビットまでの誤りを訂正可能な設計距離 $2t+1 = 5$、符号長 $n = 15$ の BCH 符号の生成多項式 $g(X)$ を求めよ。

(c) $t = 3$ ビットまでの誤りを訂正可能な設計距離 $2t+1 = 7$、符号長 $n = 15$ の BCH 符号の生成多項式 $g(X)$ を求めよ。

(d) 設計距離 $\hat{d}$ の BCH 符号の最小距離が $\hat{d}$ 以上になることを示せ。ただし、ヴァンデルモンド行列の性質を証明無しで用いて良い。

9　代数系と符号理論 期末試験 (令和 5 年 11 月 30 日)

1. **１枚の解答用紙につき大問１つを回答すること**．答案用紙には答えのみでなく、それを導く過程も記入すること。

2. **全ての答案用紙に名前と学籍番号を忘れず記入すること。**

3. 各大問は独立しており，特に断りのない限り大問間で設定や記号等は共有されない．

4. 試験開始 30 分までの退室と、試験終了 10 分前からの退室と、試験開始 30 分からの入室を禁ずる。

5. 答案を提出せずに退室することはできません。

6. 用紙が足りない場合は裏も使って良い。その場合には表面の右下に「裏面に続く」と書いてください。

7. 試験時間内にすべての問題に解答できるように作問されていない。

8. 各大問において小問は易しい順に並んでいる。

9. 易しい小問ほど配点が高い。

10. 変数 x の範囲を限定せずに命題 $P(x)$ を参照する場合には、命題 $P(x)$ が文脈上意味のある範囲で x の範囲が限定されているものとする。

11. 設定が不明な場合には、文脈上もっとも尤もらしい解釈で理解すること。

12. 設定に不備や矛盾がある場合には、文脈上もっとも尤もらしい修正を施して理解すること。

F.1 (a) 以下の $\mathbb{F}_2[X]$ の多項式に関する計算を求めよ。

i. $1+1$

ii. $(1+X^2+X^3)+(1+X+X^2)$

iii. $(1+X+X^2+X^3+X^4+X^5)(1+X)$

iv. $1+X^2+X^6$ を $1+X$ で割った商と剰余。

v. 次の多項式が、既約であるか可約であるか答えよ。既約である場合にはその理由を答え、可約である場合にはその因数分解を答えよ。

A. $X^2+1 \in \mathbb{R}[X]$

B. $X^2+1 \in \mathbb{C}[X]$

C. $X^2+1 \in \mathbb{F}_2[X]$

D. $X^3+X+1 \in \mathbb{F}_2[X]$

(b) 既約多項式 $p(X) := 1+X^2+X^3 \in \mathbb{F}_2[X]$ で生成された有限体 $\mathbb{F}_8 := \Big(\mathbb{F}_2[X]/\langle p(X)\rangle, \{+,\times\}\Big)$ に関して以下の問に答えよ。

i. 次の計算の答えを求めよ。

A. $[010]\times[010]$

B. $[001]\times[010]$

C. $[010]^{-1}$

(c) 体 $\mathbb{F}$ を係数とする次数 $m \geq 1$ のモニック既約多項式 $p(X) \in \mathbb{F}[X]$ に対して、イデアル $\langle p(X)\rangle$ を法とする剰余類環

$$\Big(\mathbb{F}[X]/\langle p(X)\rangle, \{+,\times\}\Big)$$

は $[1] \in \mathbb{F}[X]/\langle p(X)\rangle$ を乗法単位元とする単位的可換環になる。任意の非零元

$$[a(X)](\neq [0]) \in \mathbb{F}[X]/\langle p(X)\rangle$$

に対して乗法に関する逆元が存在することを示せ。

F.2 $\alpha_1, \ldots, \alpha_n$ を互いに異なる $\mathbb{F}_q$ の元とする．このため、$n \leq q$ となる。$\mathbb{F}_q[X;k]$ は $\mathbb{F}_q$ を係数とする次数が k 未満の多項式

$$f(X) = \sum_{i=0}^{k-1} f_i X^i$$

の集合である。情報多項式 $f(x) \in \mathbb{F}_q[X;k]$ に対して、

$$\vec{c}(f) := \big(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)\big) \in \mathbb{F}_q^n$$

を符号語とする符号空間を、$\mathbb{F}_q$ 上の $[n,k]$RS 符号という。正確に書くと、

$$\Big\{\vec{c}(f) \in \mathbb{F}_q^n \mid f(X) \in \mathbb{F}_q[X;k]\Big\}$$

として定義される。

以下の問に答えよ。

(a) $\mathbb{F}_7$ 上の $[n=5, k=3]$RS 符号 C を用いた通信を考える。ただし、$\alpha_1 = [0], \ldots, \alpha_5 = [4]$ と選ぶ。

i. 符号長、次元、符号化率、最小距離を求めよ。

ii. 生成行列 G を求めよ。

iii. 情報ベクトル $[4][0][3]$ を符号化して、符号語を求めよ。

iv. ある符号語を送信して、受信語 $r = [0][5][2][6][3]$ を受信した。講義で学習した RS 符号の復号法に関して、以下の問に答えよ。復号行列 A を求めよ。

v. 前問の設定で、補完多項式 $Q_0(X), Q_1(X)$ を求めよ。

vi. 前問の設定で、推定情報ベクトル $\hat{f}$ を求めよ。

(b) $\mathbb{F}_q$ の原始元 α を用いて、符号長が $q-1$ で次元が k の巡回 RS 符号の生成多項式を答えよ。

(c) 有限体 $\mathbb{F}$ 上の $[n,k]$RS 符号 C の最小重みまたは最小距離が $n-k+1$ であることを示せ。

(d) RS 符号のパリティ検査行列 H の任意の $n-k$ 列はフルランクになることを示せ。

F.3 以下の問に答えよ。

(a) 下記の $\mathbb{F}_2$ 上の符号 C が巡回符号である場合には、その (1) 符号長と (2) 次元と (3) 生成多項式と (4) パリティ検査多項式を答えよ。そうでない場合にはその理由を答えよ。

i. $C = \{(0000), (1001), (0011), (0110), (1100), (1010), (0101), (1111)$

ii. $C = \{(0000), (1000), (0100), (0010), (0001)\}$

(b) $\mathbb{F}_2$ 上の長さ n の巡回符号のうち、零ベクトルだけからなる符号 $\{\overbrace{0\cdots0}^{n}\}$ と全ベクトルからなる符号 $\mathbb{F}_2^n$ は自明であるという。$\mathbb{F}_2$ 上の符号長 $n=4$ の非自明な巡回符号の生成多項式をすべて挙げよ。

(c) 下記の $\mathbb{F}_5$ 上の符号 C は巡回符号である。C に関する以下の値を求めよ。

i. 次元 k

ii. 生成多項式 $g(X) \in \mathbb{F}_5[X]$

iii. パリティ検査多項式 $h(X) \in \mathbb{F}_5[X]$

iv. C の双対符号 $C^{\perp}$ の生成多項式 $g^{\perp}(X) \in \mathbb{F}_5[X]$

```
C={
   ([0][0][0][0]),([1][1][1][1]),([2][2][2][2]),
   ([3][3][3][3]),([4][4][4][4]),([1][3][4][2]),
   ([2][4][0][3]),([3][0][1][4]),([4][1][2][0]),
   ([0][2][3][1]),([2][1][3][4]),([3][2][4][0]),
   ([4][3][0][1]),([0][4][1][2]),([1][0][2][3]),
   ([3][4][2][1]),([4][0][3][2]),([0][1][4][3]),
   ([1][2][0][4]),([2][3][1][0]),([4][2][1][3]),
   ([0][3][2][4]),([1][4][3][0]),([2][0][4][1]),
   ([3][1][0][2])
}
```

(d) $\mathbb{F}_q$ 上の $[n,k]$ 巡回符号 C の生成多項式が $g(X)=g_0+g_1X+\cdots+g_{n-k-1}X^{n-k-1}+g_{n-k}X^{n-k}$ で与えられるとす

る。$\mathbb{F}_q$ 値 $k \times n$ 行列 $G =$

$$\begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0 \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & 0 \\ 0 & \cdots & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} \end{pmatrix}$$

は C の生成行列になることを示せ。

F.4 以下の問に答えよ。

(a) 原始多項式 $1 + X + X^3 \in \mathbb{F}_2[X]$ の根 α を用いて定義される $\mathbb{F}_8$ に対して、$\mathbb{F}_8$ の元の冪表現 α^i with $0 \leq i \leq 6$ と $\mathbb{F}_8$ の元の多項式表現

$$(f_0\ f_1\ f_2) = f_0 + f_1\alpha + f_2\alpha^2 \text{ with } f_0, f_1, f_2 \in \mathbb{F}_2$$

について、以下の問に答えよ。

i. $\mathbb{F}_8$ の非零元の冪表現に対応する多項式表現を求めよ。

ii. $\alpha^{50} + \alpha^{100}$ の冪表現とベクトル表現を求めよ。

(b) 素数 p に対して $q = p^m$ とする。 $\alpha \in \mathbb{F}_q$ の $\mathbb{F}_p$ 上の最小多項式 $M(X)$ に対して、$M(X)$ は存在すれば唯一であることを示せ。

(c) 正の整数 n に対して、1 から n までの自然数のうち n と互いに素なものの個数を $\phi(n)$ と書き、オイラー関数と呼ぶ。原始元を $\alpha \in \mathbb{F}_q$ とする。$\mathbb{F}_q$ に含まれる原始元の数を $A(q)$ と書く。$A(q)$ は $\varphi(q-1)$ と等しいことを示せ。

F.5 原始多項式 $1+X^3+X^4 \in \mathbb{F}_2[X]$ によって定義される $\mathbb{F}_{16}$ の原始元を α とする。各非零元 α^i の $\mathbb{F}_2$ 上の最小多項式 $m_i(X)$ は以下の通りである。

α^i	$m_i(X)$
α^0	$1+X$
$\alpha^1, \boxed{(1)}, \boxed{(2)}, \boxed{(3)}$	$\boxed{(11)}$
$\alpha^3, \boxed{(4)}, \boxed{(5)}, \boxed{(6)}$	$1+X+X^2+X^3+X^4$
$\alpha^5, \boxed{(7)}$	$\boxed{(12)}$
$\alpha^7, \boxed{(8)}, \boxed{(9)}, \boxed{(10)}$	$\boxed{(13)}$

(a) 空欄を埋めよ。

(b) p を素数とする。$n := q-1 := p^m-1$ とする。$\alpha \in \mathbb{F}_q$ を原始元とする。$\hat{d} \leq q-1$ なる $\hat{d}$ に対して、符号長 n、設計距離 $\hat{d}$ の BCH 符号の生成多項式 $g(X) \in \mathbb{F}_p[X]$ の定義を答えよ。

(c) $X^{15}-1$ を 4 つの多項式の積 $(1+X)\times(11)\times(12)\times(13)$ で割った商と余りと求めよ。

(d) $t=2$ ビットまでの誤りを訂正可能な設計距離 $2t+1=5$、符号長 $n=15$ の BCH 符号の生成多項式 $g(X)$ を求めよ。

(e) $t=3$ ビットまでの誤りを訂正可能な設計距離 $2t+1=7$、符号長 $n=15$ の BCH 符号の生成多項式 $g(X)$ を求めよ。

(f) 設計距離 $\hat{d}$ の BCH 符号の最小距離が $\hat{d}$ 以上になることを示せ。ただし、ヴァンデルモンド行列の性質を証明無しで用いて良い。

10　代数系と符号理論 期末試験 (令和 6 年 12 月 02 日)

1. **１枚の解答用紙につき大問１つを回答すること**．答案用紙には答えのみでなく、それを導く過程も記入すること。

2. **全ての答案用紙に名前と学籍番号を忘れず記入すること。**

3. 各大問は独立しており，特に断りのない限り大問間で設定や記号等は共有されない．

4. 試験開始 30 分までの退室と、試験終了 10 分前からの退室と、試験開始 30 分からの入室を禁ずる。

5. 答案を提出せずに退室することはできません。

6. 用紙が足りない場合は裏も使って良い。その場合には表面の右下に「裏面に続く」と書いてください。

7. 試験時間内にすべての問題に解答できるように作問されていない。

8. 各大問において小問は易しい順に並んでいる。

9. 易しい小問ほど配点が高い。

10. 変数 x の範囲を限定せずに命題 $P(x)$ を参照する場合には、命題 $P(x)$ が文脈上意味のある範囲で x の範囲が限定されているものとする。

11. 設定が不明な場合には、文脈上もっとも尤もらしい解釈で理解すること。

12. 設定に不備や矛盾がある場合には、文脈上もっとも尤もらしい修正を施して理解すること。

F.1 (a) 以下の $\mathbb{F}_2[X]$ の多項式に関する計算を求めよ。

i. $(1+X+X^2)(1+X)$

ii. $1+X+X^2$ を $1+X$ で割った商と剰余。

(b) 次の多項式が、既約であるか可約であるか答えよ。既約である場合にはその理由を答え、可約である場合にはその因数分解を答えよ。

i. $X^2+1 \in \mathbb{F}_2[X]$

ii. $X^3+X+1 \in \mathbb{F}_2[X]$

(c) 既約多項式 $p(X) := 1+X^2+X^3 \in \mathbb{F}_2[X]$ で生成された有限体 $\mathbb{F}_8 := \Big(\mathbb{F}_2[X]/\langle p(X)\rangle, \{+,\times\}\Big)$ に関して以下の問に答えよ。

i. $[001]\times[010]$

ii. 次を満たす $\alpha_1, \alpha_2 \in \mathbb{F}_8$ を求めよ。

$$\begin{pmatrix}[100] & [011]\\ [100] & [101]\end{pmatrix}\begin{pmatrix}\alpha_1\\ \alpha_2\end{pmatrix} = \begin{pmatrix}[010]\\ [101]\end{pmatrix}$$

(d) p を素数とする。剰余類環

$$\mathbb{F}_p := \Big(\mathbb{Z}/p\mathbb{Z}, \{+,\times\}\Big)$$

は $[1] \in \mathbb{F}_p$ を乗法単位元とする単位的可換環になる。任意の非零元 $[a] \in \mathbb{F}_p$ に対して乗法に関する逆元が存在することを示せ。

(e) 2つの多項式 $a(X) = X^5 + X + 1, b(X) = X^5 + X^4 + 1 \in \mathbb{F}_2[X]$ の最大公約多項式を $d(X)$ とする。$s(X)a(X) + t(X)b(X) = d(X)$ を満たす $s(X), t(X) \in \mathbb{F}_2[X]$ を求めよ。

F.2 $\alpha_1, \ldots, \alpha_n$ を互いに異なる $\mathbb{F}_q$ の元とする．このため、$n \leq q$ となる。$\mathbb{F}_q[X; k]$ は $\mathbb{F}_q$ を係数とする次数が k 未満の多項式

$$f(X) = \sum_{i=0}^{k-1} f_i X^i$$

の集合である。情報多項式 $f(x) \in \mathbb{F}_q[X; k]$ に対して、

$$\vec{c}(f) := \big(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)\big) \in \mathbb{F}_q^n$$

を符号語とする符号空間を、$\mathbb{F}_q$ 上の $[n, k]$RS 符号という。正確に書くと、

$$\Big\{\vec{c}(f) \in \mathbb{F}_q^n \mid f(X) \in \mathbb{F}_q[X; k]\Big\}$$

として定義される。

以下の問に答えよ。

(a) $\mathbb{F}_5$ 上の $[n = 5, k = 3]$RS 符号 C を用いた通信を考える。ただし、$\alpha_1 = [0], \ldots, \alpha_5 = [4]$ と選ぶ。

i. 符号長、次元、符号化率、最小距離を求めよ。

ii. 生成行列 G を求めよ。

iii. 情報ベクトル [3][4][0] を符号化して、符号語を求めよ。

iv. ある符号語を送信して、受信語 $r = [3][3][3][4][4]$ を受信した。講義で学習した RS 符号の復号法に関して、以下の問に答えよ。復号行列 A を求めよ。

v. 前問の設定で、補完多項式 $Q_0(X), Q_1(X)$ を求めよ。

vi. 前問の設定で、推定情報ベクトル $\hat{f}$ を求めよ。

(b) $\mathbb{F}_q$ の原始元 α を用いて、符号長が $q-1$ で次元が k の巡回 RS 符号の生成多項式を答えよ。

(c) 有限体 $\mathbb{F}$ 上の $[n,k]$RS 符号 C の最小重みまたは最小距離が $n-k+1$ であることを示せ。

F.3 以下の問に答えよ。

(a) 下記の $\mathbb{F}_2$ 上の符号 C が巡回符号である場合には、その (1) 符号長と (2) 次元と (3) 生成多項式と (4) パリティ検査多項式を答えよ。そうでない場合にはその理由を答えよ。

i. $C = \{(0000), (1001), (0011), (0110), (1100), (1010), (0101), (1111)$

ii. $C = \{(0000), (1000), (0100), (0010), (0001)\}$

(b) $\mathbb{F}_2$ 上の長さ n の巡回符号のうち、零ベクトルだけからなる符号 $\{\overbrace{0\cdots0}^{n}\}$ と全ベクトルからなる符号 $\mathbb{F}_2^n$ は自明であるという。$\mathbb{F}_2$ 上の符号長 $n=4$ の非自明な巡回符号の生成多項式をすべて挙げよ。

(c) 下記の $\mathbb{F}_5$ 上の符号 C は巡回符号である。C に関する以下の値を求めよ。

i. 次元 k

ii. 生成多項式 $g(X) \in \mathbb{F}_5[X]$

iii. パリティ検査多項式 $h(X) \in \mathbb{F}_5[X]$

iv. C の双対符号 $C^{\perp}$ の生成多項式 $g^{\perp}(X) \in \mathbb{F}_5[X]$

```
C={
   ([0][0][0][0]),([1][1][1][1]),([2][2][2][2]),
   ([3][3][3][3]),([4][4][4][4]),([1][3][4][2]),
   ([2][4][0][3]),([3][0][1][4]),([4][1][2][0]),
   ([0][2][3][1]),([2][1][3][4]),([3][2][4][0]),
   ([4][3][0][1]),([0][4][1][2]),([1][0][2][3]),
   ([3][4][2][1]),([4][0][3][2]),([0][1][4][3]),
   ([1][2][0][4]),([2][3][1][0]),([4][2][1][3]),
   ([0][3][2][4]),([1][4][3][0]),([2][0][4][1]),
   ([3][1][0][2])
}
```

(d) $\mathbb{F}$ を体とする。多項式環 $\mathbb{F}[X]$ の非自明なイデアル $I \neq \{0\}$ は単項生成であること、つまり次が成り立つことを示せ。$g(X) \in I$ が存在して、

$$I = \{f(x)g(X) \mid f(X) \in \mathbb{F}[X]\}$$

となる。

F.4 以下の問に答えよ。

(a) 原始多項式 $1 + X + X^3 \in \mathbb{F}_2[X]$ の根 α を用いて定義される $\mathbb{F}_8$ に対して、$\mathbb{F}_8$ の元の冪表現 α^i with $0 \leq i \leq 6$ と

$\mathbb{F}_8$ の元の多項式表現

$$(f_0\ f_1\ f_2) = f_0 + f_1\alpha + f_2\alpha^2 \text{ with } f_0, f_1, f_2 \in \mathbb{F}_2$$

について、以下の問に答えよ。

i. $\mathbb{F}_8$ の非零元の冪表現に対応する多項式表現を求めよ。

ii. $\alpha^{50} + \alpha^{100}$ の冪表現とベクトル表現を求めよ。

(b) 素数 p に対して $q = p^m$ とする。 $\alpha \in \mathbb{F}_q$ の $\mathbb{F}_p$ 上の最小多項式 $M(X)$ に対して、$M(X)$ は存在すれば既約であることを示せ。

(c) 正の整数 n に対して、1 から n までの自然数のうち n と互いに素なものの個数を $\phi(n)$ と書き、オイラー関数と呼ぶ。原始元を $\alpha \in \mathbb{F}_q$ とする。$\mathbb{F}_q$ に含まれる原始元の数を $A(q)$ と書く。$A(q)$ は $\varphi(q-1)$ と等しいことを示せ。

(d) 非ゼロ元 $\beta \in \mathbb{F}_q$ に対して、最小多項式 $M_\beta(X) \in \mathbb{F}_p[X]$ の根の集合を $[\beta]$ と書く。異なる $[\beta], [\beta']$ は互いに素であることを示せ。

F.5 原始多項式 $1 + X^3 + X^4 \in \mathbb{F}_2[X]$ によって定義される $\mathbb{F}_{16}$ の原始元を α とする。各非零元 α^i の $\mathbb{F}_2$ 上の最小多項式を $m_i(X)$ と書く。

(a) $m_1(X)$ を求めよ。

(b) $m_3(X) = m_i(X)$ となる $0 \le i \le 14$ をすべて求めよ。

(c) $t = 2$ ビットまでの誤りを訂正可能な設計距離 $2t+1 = 5$、符号長 $n = 15$ の BCH 符号の生成多項式 $g(X)$ を求めよ。

(d) 前項の BCH 符号の次元 k を求めよ。また、情報多項式 $1 + X^2$ を符号化せよ。

(e) 設計距離 $\hat{d}$ の BCH 符号の最小距離が $\hat{d}$ 以上になることを示せ。ただし、ヴァンデルモンド行列の性質を証明無しで用いて良い。

11　研究プロジェクトのプロジェクト案

P.1 LDPC 符号のパリティ検査行列を生成するプログラムを作成する。

P.2 この資料のページ 10 の演習 2.10 のプログラムを作成する。

P.3 Sum-Product アルゴリズムの導出を理解してまとめる。

P.4 Sum-Product 復号 (対数領域) の導出を理解してまとめる。mct の 2.5.2. Simplification of Message-Passing Rules for Bit-wise MAP Decoding を読む。

P.5 Sum-Product 復号 (確率領域または対数領域) のプログラムを書く。

P.6 パリティ検査行列 H を下記の 9×12 行列とする。

```
0  1  1  0  0  0  0  1  0  0  1  0
0  0  1  1  0  0  1  0  1  0  0  0
0  0  0  0  0  0  0  0  1  1  1  1
0  0  0  0  1  1  0  1  1  0  0  0
1  0  1  0  1  0  0  0  0  0  0  1
0  1  0  0  1  0  1  0  0  1  0  0
1  0  0  1  0  0  0  1  0  1  0  0
0  1  0  1  0  1  0  0  0  0  0  1
1  0  0  0  0  1  1  0  0  0  1  0
```

反転確率 $p = 0.1$ のビット反転通信路を介して通信した受信語を

V=111110100000

としたときに推定符号語を求めるプログラムを作成する。次の設定では、繰り返し５回で復号に成功するはずです。

送信符号語 U
受信後　　V
ノイズ　　Z
U=110110001010 V=111110100000 Z=001000101010

非ゼロ要素に次のような番号をつけました.

```
    [00][01]                [02]        [03]
        [04][05]        [06]    [07]
                                [08][09][10][11]
                [12][13]    [14][15]
[16]    [17]    [18]                        [19]
    [20]        [21]    [22]        [23]
[24]        [25]            [26]    [27]
    [28]    [29]    [30]                    [31]
[32]                [33][34]            [35]
```

次のようにメッセージは計算されます.

```
VtoC: 変数ノードからチェックノードへのメッセージ
CtoV: チェックノードから変数ノードへのメッセージ
U=110110001010 V=111110100000 Z=001000101010
 iteration=0<20
VtoC=
[ 0](.100,.900)[ 1](.100,.900)[ 2](.900,.100)[ 3](.900,.100)
[ 4](.100,.900)[ 5](.100,.900)[ 6](.100,.900)[ 7](.900,.100)
[ 8](.900,.100)[ 9](.900,.100)[10](.900,.100)[11](.900,.100)
[12](.100,.900)[13](.900,.100)[14](.900,.100)[15](.900,.100)
```

```
[16](.100,.900)[17](.100,.900)[18](.100,.900)[19](.900,.100)
[20](.100,.900)[21](.100,.900)[22](.100,.900)[23](.900,.100)
[24](.100,.900)[25](.100,.900)[26](.900,.100)[27](.900,.100)
[28](.100,.900)[29](.100,.900)[30](.900,.100)[31](.900,.100)
[32](.100,.900)[33](.900,.100)[34](.100,.900)[35](.900,.100)
CtoV=
[ 0](.244,.756)[ 1](.244,.756)[ 2](.756,.244)[ 3](.756,.244)
[ 4](.756,.244)[ 5](.756,.244)[ 6](.756,.244)[ 7](.244,.756)
[ 8](.756,.244)[ 9](.756,.244)[10](.756,.244)[11](.756,.244)
[12](.756,.244)[13](.244,.756)[14](.244,.756)[15](.244,.756)
[16](.756,.244)[17](.756,.244)[18](.756,.244)[19](.244,.756)
[20](.756,.244)[21](.756,.244)[22](.756,.244)[23](.244,.756)
[24](.244,.756)[25](.244,.756)[26](.756,.244)[27](.756,.244)
[28](.244,.756)[29](.244,.756)[30](.756,.244)[31](.756,.244)
[32](.244,.756)[33](.756,.244)[34](.244,.756)[35](.756,.244)
 iteration=1<20
VtoC=
[ 0](.100,.900)[ 1](.516,.484)[ 2](.900,.100)[ 3](.989,.011)
[ 4](.100,.900)[ 5](.011,.989)[ 6](.100,.900)[ 7](.900,.100)
[ 8](.484,.516)[ 9](.900,.100)[10](.989,.011)[11](.900,.100)
[12](.516,.484)[13](.989,.011)[14](.989,.011)[15](.900,.100)
[16](.011,.989)[17](.100,.900)[18](.516,.484)[19](.989,.011)
[20](.011,.989)[21](.516,.484)[22](.100,.900)[23](.989,.011)
[24](.100,.900)[25](.100,.900)[26](.900,.100)[27](.900,.100)
[28](.100,.900)[29](.100,.900)[30](.900,.100)[31](.900,.100)
[32](.100,.900)[33](.900,.100)[34](.516,.484)[35](.989,.011)
CtoV=
[ 0](.513,.487)[ 1](.187,.813)[ 2](.487,.513)[ 3](.490,.510)
[ 4](.813,.187)[ 5](.756,.244)[ 6](.813,.187)[ 7](.187,.813)
[ 8](.813,.187)[ 9](.487,.513)[10](.490,.510)[11](.487,.513)
[12](.882,.118)[13](.513,.487)[14](.513,.487)[15](.515,.485)
[16](.487,.513)[17](.485,.515)[18](.882,.118)[19](.513,.487)
[20](.487,.513)[21](.882,.118)[22](.485,.515)[23](.513,.487)
[24](.244,.756)[25](.244,.756)[26](.756,.244)[27](.756,.244)
[28](.244,.756)[29](.244,.756)[30](.756,.244)[31](.756,.244)
[32](.513,.487)[33](.487,.513)[34](.187,.813)[35](.490,.510)
 iteration=2<20
VtoC=
[ 0](.033,.967)[ 1](.312,.688)[ 2](.967,.033)[ 3](.892,.108)
[ 4](.024,.976)[ 5](.011,.989)[ 6](.024,.976)[ 7](.976,.024)
```

```
[ 8](.688,.312)[ 9](.967,.033)[10](.892,.108)[11](.967,.033)
[12](.861,.139)[13](.964,.036)[14](.964,.036)[15](.900,.100)
[16](.036,.964)[17](.100,.900)[18](.861,.139)[19](.964,.036)
[20](.036,.964)[21](.861,.139)[22](.100,.900)[23](.964,.036)
[24](.100,.900)[25](.100,.900)[26](.900,.100)[27](.900,.100)
[28](.100,.900)[29](.100,.900)[30](.900,.100)[31](.900,.100)
[32](.033,.967)[33](.967,.033)[34](.312,.688)[35](.892,.108)
CtoV=
[ 0](.362,.638)[ 1](.158,.842)[ 2](.638,.362)[ 3](.664,.336)
[ 4](.944,.056)[ 5](.933,.067)[ 6](.944,.056)[ 7](.056,.944)
[ 8](.842,.158)[ 9](.638,.362)[10](.664,.336)[11](.638,.362)
[12](.844,.156)[13](.768,.232)[14](.768,.232)[15](.810,.190)
[16](.232,.768)[17](.190,.810)[18](.844,.156)[19](.768,.232)
[20](.232,.768)[21](.844,.156)[22](.190,.810)[23](.768,.232)
[24](.244,.756)[25](.244,.756)[26](.756,.244)[27](.756,.244)
[28](.244,.756)[29](.244,.756)[30](.756,.244)[31](.756,.244)
[32](.362,.638)[33](.638,.362)[34](.158,.842)[35](.664,.336)
 iteration=3<20
VtoC=
[ 0](.011,.989)[ 1](.303,.697)[ 2](.989,.011)[ 3](.972,.028)
[ 4](.005,.995)[ 5](.011,.989)[ 6](.005,.995)[ 7](.995,.005)
[ 8](.697,.303)[ 9](.989,.011)[10](.972,.028)[11](.989,.011)
[12](.765,.235)[13](.980,.020)[14](.980,.020)[15](.741,.259)
[16](.020,.980)[17](.259,.741)[18](.765,.235)[19](.980,.020)
[20](.020,.980)[21](.765,.235)[22](.259,.741)[23](.980,.020)
[24](.019,.981)[25](.332,.668)[26](.981,.019)[27](.981,.019)
[28](.019,.981)[29](.332,.668)[30](.981,.019)[31](.981,.019)
[32](.011,.989)[33](.989,.011)[34](.303,.697)[35](.972,.028)
CtoV=
[ 0](.318,.682)[ 1](.048,.952)[ 2](.682,.318)[ 3](.688,.312)
[ 4](.979,.021)[ 5](.986,.014)[ 6](.979,.021)[ 7](.021,.979)
[ 8](.952,.048)[ 9](.682,.318)[10](.688,.312)[11](.682,.318)
[12](.723,.277)[13](.623,.377)[14](.623,.377)[15](.744,.256)
[16](.377,.623)[17](.256,.744)[18](.723,.277)[19](.623,.377)
[20](.377,.623)[21](.723,.277)[22](.256,.744)[23](.623,.377)
[24](.344,.656)[25](.054,.946)[26](.656,.344)[27](.656,.344)
[28](.344,.656)[29](.054,.946)[30](.656,.344)[31](.656,.344)
[32](.318,.682)[33](.682,.318)[34](.048,.952)[35](.688,.312)
 iteration=4<20
VtoC=
```

```
[ 0](.034,.966)[ 1](.642,.358)[ 2](.966,.034)[ 3](.978,.022)
[ 4](.002,.998)[ 5](.000,1.000)[ 6](.002,.998)[ 7](.998,.002)
[ 8](.358,.642)[ 9](.966,.034)[10](.978,.022)[11](.966,.034)
[12](.430,.570)[13](.973,.027)[14](.973,.027)[15](.793,.207)
[16](.027,.973)[17](.207,.793)[18](.430,.570)[19](.973,.027)
[20](.027,.973)[21](.430,.570)[22](.207,.793)[23](.973,.027)
[24](.030,.970)[25](.303,.697)[26](.970,.030)[27](.970,.030)
[28](.030,.970)[29](.303,.697)[30](.970,.030)[31](.970,.030)
[32](.034,.966)[33](.966,.034)[34](.642,.358)[35](.978,.022)
CtoV=
[ 0](.627,.373)[ 1](.085,.915)[ 2](.373,.627)[ 3](.377,.623)
[ 4](.996,.004)[ 5](.994,.006)[ 6](.996,.004)[ 7](.004,.996)
[ 8](.915,.085)[ 9](.373,.627)[10](.377,.623)[11](.373,.627)
[12](.763,.237)[13](.461,.539)[14](.461,.539)[15](.437,.563)
[16](.539,.461)[17](.563,.437)[18](.763,.237)[19](.461,.539)
[20](.539,.461)[21](.763,.237)[22](.563,.437)[23](.461,.539)
[24](.326,.674)[25](.086,.914)[26](.674,.326)[27](.674,.326)
[28](.326,.674)[29](.086,.914)[30](.674,.326)[31](.674,.326)
[32](.627,.373)[33](.373,.627)[34](.085,.915)[35](.377,.623)
 iteration=5<20
VtoC=
[ 0](.059,.941)[ 1](.972,.028)[ 2](.941,.059)[ 3](.767,.233)
[ 4](.013,.987)[ 5](.001,.999)[ 6](.013,.987)[ 7](.987,.013)
[ 8](.028,.972)[ 9](.941,.059)[10](.767,.233)[11](.941,.059)
[12](.534,.466)[13](.917,.083)[14](.917,.083)[15](.288,.712)
[16](.083,.917)[17](.712,.288)[18](.534,.466)[19](.917,.083)
[20](.083,.917)[21](.534,.466)[22](.712,.288)[23](.917,.083)
[24](.179,.821)[25](.645,.355)[26](.821,.179)[27](.821,.179)
[28](.179,.821)[29](.645,.355)[30](.821,.179)[31](.821,.179)
[32](.059,.941)[33](.941,.059)[34](.972,.028)[35](.767,.233)
CtoV=
[ 0](.722,.278)[ 1](.293,.707)[ 2](.278,.722)[ 3](.134,.866)
[ 4](.973,.027)[ 5](.962,.038)[ 6](.973,.027)[ 7](.027,.973)
[ 8](.707,.293)[ 9](.278,.722)[10](.134,.866)[11](.278,.722)
[12](.352,.648)[13](.488,.512)[14](.488,.512)[15](.524,.476)
[16](.512,.488)[17](.476,.524)[18](.352,.648)[19](.488,.512)
[20](.512,.488)[21](.352,.648)[22](.476,.524)[23](.488,.512)
[24](.560,.440)[25](.368,.632)[26](.440,.560)[27](.440,.560)
[28](.560,.440)[29](.368,.632)[30](.440,.560)[31](.440,.560)
[32](.722,.278)[33](.278,.722)[34](.293,.707)[35](.134,.866)
```

教員用メモ

```
cd ./program/naive_encode_nb/
./naive_encode 20 ../construct/34REGULAR_n12_N12_M9_GF2_gcy6_gss6_hss
```

例として，メッセージ (0.244,0.756) の第 1 要素 0.244 は次のように計算された.

```
+[1](0)*[2](0)*[3](0)
+[1](1)*[2](1)*[3](0)
+[1](0)*[2](1)*[3](1)
+[1](1)*[2](0)*[3](1)
=
+0.1*0.9*0.9
+0.9*0.1*0.9
+0.1*0.1*0.1
+0.9*0.9*0.1
= 0.244
```

P.7 LDPC 符号の符号化アルゴリズムを理解してまとめる。mct の Encoding Low-Density Parity-Check Codes の章を読む。

P.8 LDPC 符号の符号化アルゴリズムのプログラムを作成する。