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。

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

答え：符号長は 5, 最小ハミング距離は 00000 と 00011 の間の 2, 符号化率は $\log_2(4)/5 = 0.4$.

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。

答え： C_2 は符号長 5，最小ハミング距離 2, 符号化率 $1/5$ を有する．C_1 と C_2 は符号長と最小ハミング距離が同じで符号化率は C_1 のほうが大きいから、C_1 のほうが望ましい。

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。

答え：

$$
\begin{aligned}
p(r_1r_2r_3|000) &= 0.3^{r_1+r_2+r_3}0.7^{3-r_1-r_2-r_3} \\
p(r_1r_2r_3|111) &= 0.8^{r_1+r_2+r_3}0.2^{3-r_1-r_2-r_3}
\end{aligned}
$$

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。

答え：

$r_1r_2r_3$	$p(r_1r_2r_3\|000)$	$p(r_1r_2r_3\|111)$	復号の結果
000	0.343	0.008	000
001 010 100	0.147	0.032	000
110 101 011	0.063	0.128	111
111	0.027	0.512	111

1.5 前問の最尤復号を最小距離復号に置き換えて解け。

答え：復号結果は受信ビット r_1, r_2, r_3 の中で 0 が 1 よりも多いときは 000 が送られたと判定し、そうでなければ 111 が送られたと判定する。したがって、復号の結果は同じになる。

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。

答え： 容器に A 個の球が入っているとする。このとき、各球から距離 r 以下の空間には、互いに交わりがない。したがって、ユニオン限界を等式で満たし、すべての球が占有する空間の体積は各球の体積の和に等しい。さらに、すべての球が占有する空間の体積は容器の容積を超えないので、

$$B \geq A\frac{4}{3}\pi r^3$$

を得る。最大の充填の場合にも上の議論は成り立つので、

$$B \geq A(B,r)\frac{4}{3}\pi r^3$$

を得る。

(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。

答え：$\mathbb{F}_2^n$ に入れるハミング球の球被覆限界の証明にしたがって、最大充填を与える球配置の各球を中心とする半径 r の仮想的な球の合併は容器を被覆すると主張する。そうでないと仮定して、以下のように矛盾を導くのが、球被覆限界の証明のストーリーであった。充填されていない点は他のどの仮想球からも距離 r だけ離れているので、その点を中心とする球を容器に追加することができる。これは、最大充填であることに矛盾する。しかし、被覆されていない部分の点を加えてもその点が容器の境界から距離 r 未満に位置していることがあるので、その点を中心とする球を加えることはできない。よって、この証明は破綻する。容器が 3 次元トーラス（2 次元だったらドラクエの世界地図のように南北と東西がそれぞれ隣接しているような空間です。地球はこうなっていないので注意しよう。）ならば加えることはできる。

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。

答え： 誤りの数つまり $d(\vec{Y}, \vec{x})$ を Z と書く。ハミング球の定義

$$B(\vec{c}, d) \stackrel{\text{def}}{=} \{\vec{x} \in \mathbb{F}_2^n \mid d(x, \vec{c}) \leq d\}$$

を思い出すと、以下の 2 つは同値である。

$$\vec{Y} \in B(\vec{x}, \lfloor qn \rfloor) \Longleftrightarrow Z \leq \lfloor qn \rfloor$$

大数の弱法則[1]から、任意の $\epsilon > 0$ に対して以下が成り立つ。

$$\lim_{n\to\infty} \Pr\{|Z - pn| \leq \epsilon n\} = 1 \tag{1.1}$$

以下の 2 つは等価である。

$$\begin{aligned} & |Z - pn| \leq \epsilon n \\ & \Longleftrightarrow \\ & (p - \epsilon)n \leq Z \leq (p + \epsilon)n \end{aligned} \tag{1.2}$$

[1] https://goo.gl/PSmcrs

$q - p > \epsilon > 0$ なる ϵ に対して $p + \epsilon < q$ なので、十分大きな n に対して、

$$(8) \Longrightarrow Z \leq \lfloor qn \rfloor$$

となる。したがって、

$$\Pr\{|Z - pn| \leq \epsilon n\} \leq \Pr\{\vec{y} \in B(\vec{x}, qn)\}$$

となる。これと (8) から、以下を得る。

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

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) $1 + 1$

答え：0

(b) $1/1$

答え：1

(c) $1(0110)$

答え：(0110)

(d) $0(0110)$

答え：(0000)

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

答え：010

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

答え：定義されていない

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

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

答え： $x_1 = 1, x_2 = 1, x_3 = 0, x_4 = 1$

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

答え：11 と 11 の和 00 が符号 C_1 に含まれないから C_1 は線形符号ではない。

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

答え： 線形符号であり、次元は 3、基底は $\{10110, 01101, 11111\}$ で、最小距離 1，符号化率 3/5,

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

答え：線形符号ではない。理由は零ベクトルが含まれていないから。

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。

答え：

$$G = \begin{pmatrix} 11111 \end{pmatrix}$$

$$H = \begin{pmatrix} 11000 \\ 01100 \\ 00110 \\ 00011 \end{pmatrix}$$

$$H = \begin{pmatrix} 11000 \\ 10100 \\ 10010 \\ 10001 \end{pmatrix}$$

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。

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

答え： H の任意 2 列は異なっているので、任意 2 列は線形独立である。最下行はすべて 1 なので、どの 3 列を足しても $(0000)^T$ になることはない。任意の 3 列以下は線形独立にな

る。したがって、$d(C) \geq 4$ である。H の上 3 行は $[7,4,3]$ ハミング符号の制約を表しているので、1 ビット付け加えられても各符号語の距離は減ることは無いので $d(C) \geq 3$ となる。第 4,5,6,7 列を加算すると $(0000)^T$ となるので $d(C) \leq 4$ となり、主張は証明された。

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。

答え：$s = 100$

(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。

答え：

コセット s に対応するコセットは、$Hy = s$ となる y からなる集合である。特殊解 y(例えば $y = 0111101$) を一つ求めて

$y_0 + x\,(x \in C)$ が一般解となる。コセット C_s は以下の要素からなる。

0000100 1000010 0100111 1100001
0010001 1010111 0110010 1110100
0001011 1001101 0101000 1101110
0011110 1011000 0111101 1111011

(c) C_s のコセット代表元を求めよ。

答え：C_s の要素のうち重みが最小のもの $y_s = 0000100$ がコセット代表元となる。

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.

答え：次のような手順で行ベクトルが線形独立になる生成行列 G を構成することを考えよう。符号 C から非ゼロ符号語を一つ選び G の第1行とする。$|C| = 2^k$ なので、$2^k - 1$ 通りの選び方がある。次に、第1行の行ベクトルではられる部分空間に含まれない符号語、つまり残りの $2^k - 2$ 個の非ゼロ符号語の中から一つ選び、G の第2行とする。さらに同様に考えて、第1行から第 $i-1$ 行の行ベクトルではられる部分空間に含まれない符号語を選び G の第 i 行とする。この G の第 i 行の選び方は $2^k - 2^{i-1}$ 通りある。このように生成行列 G を

構成することですべての $k \times n$ 生成行列が生成される。したがって、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 $\prod_{i=1}^{k}(2^k - 2^{i-1})$ 通りある。

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．

答え： k 個のベクトルからなる基底を作ると一つの $[n,k]$ 符号ができる．k 個の独立なベクトルの選び方は，

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

通りある．ひとつの $[n,k]$ 符号に対して，

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

通りの基底の取り方があるので，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．

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。

答え：

$$G' = \begin{pmatrix} 100\ 01 \\ 010\ 11 \\ 001\ 10 \end{pmatrix} \qquad H' = \begin{pmatrix} 011\ 10 \\ 110\ 01 \end{pmatrix}$$

$$G^\perp = \begin{pmatrix} 10\ 111 \\ 01\ 110 \end{pmatrix} \qquad H^\perp = \begin{pmatrix} 11\ 100 \\ 11\ 010 \\ 10\ 001 \end{pmatrix}$$

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**	00010	01110	01000	10000
0**1**000	0000**1**	00010	00001	01000	00100
00**1**00	0000**1**	00010	00010	01000	01000
000**1**0	0000**1**	00010	00100	10110	01101
0000**1**	0000**1**	00001	01101	11111	10101
00000	**1**0001	00011	01010	01001	11000
00000	0**1**001	00000	00110	00101	10010
00000	00**1**01	00000	01111	01010	01010
00000	0001**1**	00000	01001	00000	10010
00000	00000	**1**0001	00110	11101	10111
00000	00000	0**1**010	00110	01100	00110
00000	00000	00**1**10	00011	11000	00110
00000	00000	00000	**1**0010	10001	11110
00000	00000	00000	00000	00000	00000
00000	00000	00000	00000	00000	00000

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**

教員用メモ `program/encode/`

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

答え： $(0000)^T$ を除く 15 個の異なる長さ 4 の非ゼロベクトルを列として持つ 4×15 行列

(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。

答え： (000000000000000)

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。

答え：

$$A(X,Y) = X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7$$
$$A(X) = 1 + 7X^3 + 7X^4 + X^7$$

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

答え：

$$B(X,Y) = X^7 + 7X^3Y^4$$
$$B(X) = 1 + 7X^4$$

(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。

答え： $C^\perp$ の双対符号は C なので、$|C^\perp| = 8$ をもちいて、MacWilliams の恒等式

$$|C^\perp|A(X,Y) = B(X+Y, X-Y)$$

を確認する。代入して、以下の等式が成り立つことを確かめれば良い。

$$\begin{aligned}&(X+Y)^7 + 7(X+Y)^3(X-Y)^4 \\ &= 8(X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7)\end{aligned} \tag{3.1}$$

これらは 7 次の同時多項式なので、$Y = 1$ の時に一致することを示せば十分である。

$$\begin{aligned}&(X+1)^7 + 7(X+1)^3(X-1)^4\\&= 8(X^7 + 7X^4 + 7X^3 + 1)\end{aligned}$$

(2) の左辺を因数分解して、

$$\begin{aligned}&(X+1)^7 + 7(X+1)^3(X-1)^4\\&= 8(X+1)^3(X^4 - 3X^3 + 6X^2 - 3X + 1)\end{aligned}$$

となる。(2) の右辺を $(X+1)^3$ で割ると割り切れて、

$$\begin{aligned}&8(X^7 + 7X^4 + 7X^3 + 1)\\&= 8(X+1)^3(X^4 - 3X^3 + 6X^2 - 3X + 1)\end{aligned}$$

となる。MacWilliams の恒等式が成り立つことが確認できた。

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。

答え：(1100101)

(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。

答え：(1111111).

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．

答え：(1) 3回以上必要なことを説明すれば良い。つまり、1回と2回では不十分なことを言えば良い。3回で十分なことを説明しても意味ない。検出器の1回の使用の結果は検出するかしないかの2通りなので，検出器を N 回使用した時に得られる使用結果は 2^N 通りである．どのワインが毒ワインであるかは，毒ワインがない場合を含めて8通りである．$N = 1$ と $N = 2$ の場合では使用結果はそれぞれ2通りと4通りしか無いので，8通りの毒ワインのありかを分別することはできない．従って，使用結果から毒ワインを見つけるためには $N \geq 3$ でなければならない．

(2) 検出器の使用方法

1回目： W_1, W_2, W_4, W_5 を混ぜて入れる
2回目： W_1, W_2, W_3, W_6 を混ぜて入れる
3回目： W_1, W_3, W_4, W_7 を混ぜて入れる

1，2，3回目の測定の結果をそれぞれ、

$$s_1, s_2, s_3 \in \{0\text{: 検出しなかった, } 1\text{: 検出した }\}$$

とする．3回の測定の結果が全て0である場合には毒ワインはない。s_1, s_2, s_3 をシンドロームとしてハミング符号の復号を行う。シンドロームと一致する列の番号に対応するワインに毒が含まれていることがわかる。

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。

答え： まず、長さ7のハミング符号 C の16個の符号語を列挙し、A-Pの16文字を対応させる。例えば以下の通りである。

```
A 0000000 B 1000110
C 0100011 D 1100101
E 0010101 F 1010011
G 0110110 H 1110000
I 0001111 J 1001001
K 0101100 L 1101010
M 0011010 N 1011100
O 0111001 P 1111111
```

次に、各 $i = 1, \ldots, 7$ に対して第 i ビットが0である符号語に対応する文字の集合を $\mathcal{A}_i$ とする。

$$\mathcal{A}_1 = \{\mathrm{ACEGIKMO}\}$$
$$\mathcal{A}_2 = \{\mathrm{ABEFIJMN}\}$$
$$\vdots$$
$$\mathcal{A}_7 = \{\mathrm{ABGHKLMN}\}$$

第i回の質問を「その文字は$\mathcal{A}_i$に含まれますか」とする。YESの場合に$r_i = 0$、NOの場合には$r_i = 1$とする。$(r_1, \ldots, r_7)$を受信語としてハミング符号の復号法を実行し、復号結果の符号語に対応する文字を答える。

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。

答え：囚人 i は、$h_i = 1\,(0)$ としたときに h が長さ 3 の繰り返し符号の符号語 111(000) になるとき $a_i = 0\,(1)$ と答える。そうでないとき、棄権する。配置 h がハミング符号になっている時またその時に限って開放されない。符号語数は 2、総配置数は 8 なので、3/4(=1-2/8) の確率で解放される。

(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。

答え： 囚人 i は、$h_i = 1\,(0)$ としたときに h が長さ 7 のハミング符号の符号語になるとき $a_i = 0\,(1)$ と答える。そうでな

いとき、棄権する。配置 h がハミング符号になっている時またその時に限って開放されない。符号語数は 16 で総配置数は 128 なので、$1 - 16/128 = 7/8$ の確率で解放される。

(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。

答え： 任意に固定された戦略 $(a_i(h_{\sim i}))_{i=1}^7$ に対して、解放される帽子配置の集合を S、解放されない帽子配置の集合を S' と書く。S と S' に交わりはなく、合併はすべての配置集合に等しい。言い換えると、$S + S' = \{0,1\}^7$ である。帽子の総配置数は 2^7 なので、解放される確率は $|S|/2^7$ で与えられる[2]。

囚人 i の帽子の色を反転させる、言い換えると h の第 i ビットを反転させた帽子配置を $h' =: F_i(h)$ と書く。h' は戦略 $(a_i(h_{\sim i}))_{i=1}^7$ では解放されない。言い換えると、$h' =: F_i(h) \in S'$ である。

囚人 i の回答 $a_i(h_{\sim i})$ は帽子 h_i には依存していない。解放される帽子配置 $h \in S$ に対して、ある囚人 i が存在して、正しい色 $a_i(a_i = h_i)$ を答えるはずである。このような配置 h の集合を S_i と書く。$S_i \subset S$ である。$S_i \quad (i = 1, \ldots, 7)$ は交わりが無いとは限らないことに注意しよう。$h \in S_i$ に対して上の操作によって $F_i(h) = h' \in S'$ を作ることができる。

S_i $(i = 1, \ldots, 7)$ のうちサイズが最大のものを S_j とする。S_j のサイズ $|S_j|$ は $|S|/7$ 以上である。そうで無い、つまり

[2] $|S|$ は S のサイズを表す。

$|S_j| < |S|/7$ とすると、

$$\begin{aligned} |S| &\le |S_1| + \cdots + |S_7| \\ &\le |S_j| + \cdots + |S_j| \\ &= 7|S_j| \\ &< |S| \end{aligned}$$

となり、矛盾する。F_j は第 j ビットを反転させる操作なので 1 対 1 に対応し、$F_j(S_j)$ のサイズは S_j と一致する。

S と S_j は交わりがないので、$|S| + |S|/7 \le 128$ である。これを満たす $|S|$ の最大値は $|S| = 112$ となる。このことから、どんな戦略 $(a_i(h_{\sim i}))_{i=1}^{7}$ を用いても $112/128 = 7/8$ を超える確率で解放されることはないことがわかる。

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			

答え：

$\times$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

(b) 演算表が一意に定まることを証明せよ。

答え： 最上行と再左列は単位元の性質から自動的に決まる。$ab \neq a$ であることを示す。$ab = a$ だと仮定すると、両辺に左から a^{-1} をかけて $b = e$ となってしまい、元が 3 つかることに矛盾する。同様に考えて、$ab \neq b, ba \neq a, ba \neq b$ となり、結果 $ab = ba = e$ となる。逆元が一意に決まることから、各行各列は e, a, b の順序を入れ替えたものになっていなければならないので、残りの $aa = b, bb = a$ が分かる。

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。

答え：

(a) $f_i * f_j$ を合成関数

$$f_i \circ f_j \stackrel{\text{def}}{=} f_i(f_j(x))$$

として定義すれば良い。積 $(f_i * f_j)(x) = f_i(x) \times f_j(x)$ として定義するのは不正解。実際、$(f_1 * f_1)(x) = x^2$ となり、閉性が満たされない。

(b) 単位元は f_1 である。f_1, f_4, f_5, f_6 はそれぞれ自身が逆元となり、f_2 と f_3 は互いに逆元となっている。

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

$$\mathrm{F}, \mathrm{ꟻ}, \mathrm{ⅎ}, \mathrm{Ⅎ}, \mathrm{ꟼ}, \mathrm{Ⅎ}, \mathrm{Ⅎ}$$

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。

答え：$a^3 b$

(b) $(G, \times)$ は可換群でないことを示せ。

答え：$ab \neq ba = a^3 b$ となることから分かる。

(c) G の要素をすべて $a^i b^j$ の形で辞書順で列挙せよ。

答え：$e, a, a^2, a^3, a^3 b, a^2 b, ab, b$

(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。

答え：

$\times$	e	a	a^2	a^3	$a^3 b$	$a^2 b$	ab	b
e	e	a	a^2	a^3	$a^3 b$	$a^2 b$	ab	b
a	a	a^2	a^3	e	b	$a^3 b$	$a^2 b$	ab
a^2	a^2	a^3	e	a	ab	b	$a^3 b$	$a^2 b$
a^3	a^3	e	a	a^2	$a^2 b$	ab	b	$a^3 b$
$a^3 b$	$a^3 b$	$a^2 b$	ab	b	e	a	a^2	a^3
$a^2 b$	$a^2 b$	ab	b	$a^3 b$	a^3	e	a	a^2
ab	ab	b	$a^3 b$	$a^2 b$	a^2	a^3	e	a
b	b	$a^3 b$	$a^2 b$	ab	a	a^2	a^3	e

(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。

答え： ab を F に施した結果は␣となる。この結果に b を施すと␣ さらに a を施すと F にもどる。このことより、ab の逆元は ab となり、求める答えは $i = 1, j = 1$ となることがわ

かる。
詳細は https://goo.gl/4W3TM6 を参照。

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、

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

答え： まず、(a)⇔(b) を示す。(a) は定義より $\forall g \in G$ に対して $gN = Ng$ を言い換えたものである。これは、$gN \subset Ng, gN \supset Ng$ であり、さらに形式的に書くと、以下が成り立つことである。

$$\forall g \in G, \forall n \in N, \exists n' \in N, gn = n'g \tag{3.2}$$

$$\forall g \in G, \forall n \in N, \exists n' \in N gn' = ng \tag{3.3}$$

(b) は正確に書くと、$gNg^{-1} \subset N$, $gNg^{-1} \supset N$ であり、さらに形式的に書くと、それぞれ以下が成り立つことである。

$$\forall g \in G, \forall n \in N, \exists n' \in N, gng^{-1} = n' \tag{3.4}$$

$$\forall g \in G, \forall n \in N, \exists n' \in N gn'g^{-1} = n \tag{3.5}$$

$gn = n'g \Leftrightarrow gng^{-1} = n'$ なので、(10c) と (10c) は同値であることが分かる。$gn' = ng \Leftrightarrow gn'g^{-1} = n$ なので、(10c) と (10c) は同値であることが分かる。したがって、(a)⇔(b) を得る。

次に (a)⇔(c) を示す。(c) を形式的に書くと、以下が成り立つことである。

$$\forall n \in N, \forall g \in G, \exists n' \in N, gng^{-1} = n'$$

これは (10c) と同値である。$(a) \Rightarrow (c)$ を得た。g は任意なので g^{-1} とみなし $g^{-1}ng = n'$ から $n = gn'g^{-1}$ を得る。これは、(10c) と同値である。こうして $(c) \Rightarrow (a)$ が分かった。

3.11 $(G, \times)$ 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 準同型である、いいかえると

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

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

答え： 次に、 $\mathrm{Ker}(f)$ が G の正規部分群であることを示します。任意の $g \in G$ および $a \in \mathrm{Ker}(f)$ に対し て、共役元 gag^{-1} が $\mathrm{Ker}(f)$ に含まれることを確認します。f が準同型

であるため、

$$\begin{aligned} f\left(gag^{-1}\right) &= f(g)f(a)f(g)^{-1} \\ &= f(g)\cdot 1\cdot f(g)^{-1} \\ &= f(g)f(g)^{-1} = 1 \end{aligned}$$

となり、 $gag^{-1} \in \mathrm{Ker}(f)$ です。したがって、 $\mathrm{Ker}(f)$ は G の正規部分群です。

3.12 $f : G \to H$ を群の準同型とする．すなわち

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

を満たすとする．

このとき，f の像 $\mathrm{Im}(f)$ およびカーネル $\mathrm{Ker}(f)$ を

$$\mathrm{Ker}(f) := \{\, x \in G \mid f(x) = e_H \,\}, \mathrm{Im}(f) := \{\, f(x) \mid x \in G \,\}$$

と定める．

写像 $f : G \to H$ が **同型 (isomorphism)** であるとは，f が準同型であり，かつ全単射（1 対 1 対応）であるときにいう．このとき，G と H は同型であるといい，

$$G \cong H$$

と書く．

群の準同型 $f : G \to H$ に対して，$\mathrm{Ker}(f)$ は G の正規部分群であり，f によって定まる写像

$$\tilde{f} : G/\mathrm{Ker}(f) \to \mathrm{Im}(f), \qquad \tilde{f}(g\,\mathrm{Ker}(f)) = f(g)$$

は同型写像である．したがって

$$G/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$$

が成り立つことを示せ。

答え： (1) まず，$\mathrm{Ker}(f)$ が G の正規部分群であることはすでに示した.

(2) 写像

$$\tilde{f} : G/\mathrm{Ker}(f) \to \mathrm{Im}(f), \quad \tilde{f}(g\,\mathrm{Ker}(f)) = f(g)$$

を定める．この写像が well-defined（代表元の取り方に依存しない）であることを確認する．もし $g\,\mathrm{Ker}(f) = g'\,\mathrm{Ker}(f)$ ならば $g^{-1}g' \in \mathrm{Ker}(f)$ なので

$$f(g^{-1}g') = e_H \quad \Rightarrow \quad f(g') = f(g)f(g^{-1}g') = f(g)e_H = f(g)$$

であり，$\tilde{f}$ は well-defined である．

(3) 準同型性を確認する．任意の $g_1, g_2 \in G$ に対して，

$$\begin{aligned}
&\tilde{f}(g_1 \operatorname{Ker}(f)\, g_2 \operatorname{Ker}(f)) \\
&= \tilde{f}(g_1 g_2 \operatorname{Ker}(f)) \\
&= f(g_1 g_2) \\
&= f(g_1) f(g_2) \\
&= \tilde{f}(g_1 \operatorname{Ker}(f))\, \tilde{f}(g_2 \operatorname{Ker}(f)).
\end{aligned}$$

したがって，$\tilde{f}$ は群準同型である．

(4) 単射性を示す．$\tilde{f}(g \operatorname{Ker}(f)) = e_H$ ならば $f(g) = e_H$，すなわち $g \in \operatorname{Ker}(f)$．したがって $g \operatorname{Ker}(f) = \operatorname{Ker}(f)$ であり，$\tilde{f}$ は単射．

(5) 全射性を示す．任意の $y \in \operatorname{Im}(f)$ に対して，ある $g \in G$ が存在して $y = f(g)$．このとき

$$y = \tilde{f}(g \operatorname{Ker}(f))$$

であるから，$\tilde{f}$ は全射である．

(6) よって $\tilde{f}$ は全単射な群準同型であり，

$$G/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$$

が成り立つ．

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. 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。

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

答え：符号長は 12，最小ハミング距離は 6，符号化率は $\log_2(4)/12 = 1/6$.

(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。

答え：受信語 $\vec{r}$ から最もハミング距離の近い符号語を復号結果とする。正確に書くと下である。

$$\hat{\vec{c}}^{(\mathrm{MD})}(\vec{r}) = \operatorname*{argmin}_{\vec{c}\in C} d_H(\vec{r},\vec{c})$$

(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。

答え： 符号 C を用いて通信を行い受信語 $\vec{r}$ を受信した。$\vec{r}$ から距離 t の範囲に符号語が唯一存在すれば、言い換えると $d(\vec{c},\vec{r}) \le t$ となる符号語 $\vec{c}$ は複数存在しないならば、それを復号語 $\hat{\vec{c}}_t^{(\mathrm{BD})}(\vec{r})$ とし、見つからなければ復号誤りである error を宣言して復号を中止する。正確に述べると、

$$\hat{\vec{c}}_t^{(\mathrm{BD})}(\vec{r}) = \begin{cases} \vec{c}\in C, & d(\vec{c},\vec{r}) \le t \text{ となる符号語 } \vec{c} \text{ が} \\ & \text{唯一存在する} \\ \mathrm{error}, & \text{そんな符号語 } \vec{c} \text{ は存在しない} \end{cases}$$

である。この復号法を復号半径 t の限界距離復号法という。

(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、$d(\vec{c},\vec{r}) \le t$ 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。

答え： 異なる 2 つの符号語 $\vec{c}_1, \vec{c}_2 \in C$ の $d/2$ より小さい半径 t に共通して含まれる受信語 $\vec{r}$ が存在したと仮定すると、

$$\begin{aligned} d &\leq d(\vec{c}_1, \vec{c}_2) \,(d \text{ は } C \text{ の最小距離}) \\ &\leq d(\vec{c}_1, \vec{r}) + d(\vec{r}, \vec{c}_2) \;\; (\text{三角不等式}) \\ &< \frac{d}{2} + \frac{d}{2} = d \end{aligned}$$

で $d < d$ となり矛盾が導ける。

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。

答え：必要条件

(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。

答え：十分条件

(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。

答え：

$$B \geq A(B, r)\frac{4}{3}\pi r^3$$

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

答え：容器に A 個の球が入っているとする。このとき、各球から距離 r 以下の空間には、互いに交わりがない。したがって、ユニオン限界を等式で満たし、すべての球が占有する空間の体積は各球の体積の和に等しい。さらに、すべての球が占有する空間の体積は容器の容積を超えないので、

$$B \geq A\frac{4}{3}\pi r^3$$

を得る。最大の充填の場合にも上の議論は成り立つので、

$$B \geq A(B,r)\frac{4}{3}\pi r^3$$

を得る。

(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。

答え：

$$V_2(n,t) := \sum_{i=0}^{t} \binom{n}{i} \text{個}$$

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

答え：

$$2^n \geq A(n,t)|V_2(n,t)|$$

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

答え：充填された点の集合を X と書く。各点からハミング距離 t 以下のベクトル全体は、互いに交わりがない。 したがって、ユニオン限界を等式で満たし、

$$\begin{aligned}\#\bigcup_{\vec{x}\in X} B(\vec{x},t) &= \sum_{\vec{x}\in X} \#B(\vec{c},t)\\ &= |C|V_2(n,t)\end{aligned}$$

がなりたつ。左辺の集合は $\mathbb{F}_2^n$ に含まれるまたは等しいので、

$$2^n \geq A(n,t)|V_2(n,t)|$$

となる。

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。

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

答え：11 と 11 の和 00 が符号 C_1 に含まれないから C_1 は線形符号ではない。

$$\begin{aligned}C_2 = \{&00000, 10110, 01101, 11011,\\ &11111, 01001, 10010, 00100\}\end{aligned}$$

答え： 線形符号であり、次元は 3、基底は $\{10110, 01101, 11111\}$ となる。基底の選び方は任意性があるので、答えは一意ではない。生成行列は基底の要素を行ベクトルとして積み上げたもの。最小距離 1，符号化率 3/5,

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

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

答え：いくつかの基本行変形[3]により、

$$\begin{pmatrix} 1000|1 \\ 1011|0 \\ 1111|1 \\ 0001|0 \end{pmatrix} \overset{\text{前進消去}}{\longrightarrow} \begin{pmatrix} 1000|1 \\ 0111|0 \\ 0011|1 \\ 0001|0 \end{pmatrix}$$

$$\overset{\text{後退代入}}{\longrightarrow} \begin{pmatrix} 1000|1 \\ 0100|1 \\ 0010|1 \\ 0001|0 \end{pmatrix}.$$

となる。よって、$(x_1, \ldots, x_4) = (1110)$ である。

[3] https://ja.wikipedia.org/wiki/行列の基本変形

(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。

答え：

$$C^\perp = \{000, 011, 101, 110\}$$
$$C = \{000, 111\}$$

(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。

答え： $A(X,Y)$ の $A_w \neq 0$ となる $w > 0$ の最小値が C の最小距離 d である。MacWilliams の恒等式から $B(X,Y)$ を求めることができる。$B(X,Y)$ の $B_w \neq 0$ となる $w > 0$ の最小値が $C^\perp$ の最小距離 $d^\perp$ である。

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。

答え：

$$G = \begin{pmatrix} 1000\ 110 \\ 0100\ 011 \\ 0010\ 101 \\ 0001\ 111 \end{pmatrix}$$

(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。

答え：(1111111)

(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。

答え：(1111111).

(d) 符号語数、次元、符号化率を求めよ。

答え：16,4,4/7

(e) 最小距離が 3 以上であることを証明せよ。

答え：H の異なる 2 列は異なっていて線形独立だから、最小距離は 3 以上となる。

(f) 最小距離が 3 以下であることを証明せよ。

答え：H の第 1,2,3 列は線形従属なので、最小距離は 3 以下である。

(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。

答え：半径 1 のハミング球の要素数は $n+1$ である。各符号語の半径 1 のハミング球には交わりがない。なぜなら、交わりがあったと仮定するとその符号語間のハミング距離は 2 となり、最小距離が 3 であることに矛盾する。したがって、$t=1$ として次のユニオン限界を等式で満たす。

$$\#\bigcup_{\vec{x}\in C} B(\vec{x},t) \le \sum_{\vec{x}\in C} \#B(\vec{c},t)$$

$t=1$ に対して、

$$\begin{aligned}\sum_{\vec{x}\in C} \#B(\vec{c},t) &= |C|V_2(n,t)\\ &= 16\times(n+1) = 16\times 8 = 128\end{aligned}$$

となり、$\mathbb{F}_2^7$ の要素をすべて埋め尽くすことが分かる。

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

答え：群である。$e=0, -x$

ii. 非零実数の集合とその乗算

答え：群である。$e=1, x^{-1}$

iii. 2×2 実行列の集合と行列の乗算

答え：群でない。単位元は単位行列 I_2 となるが、非正則行列 X には乗じて $XY = YX = I_n$ となる行列は存在しない。

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

答え：群である。単位元は恒等写像である。写像 $x : X \to X$ に対して、x の逆元は $y \in X$ に対して $x(a) = y$ となる $a \in X$ を対応させる写像、つまり逆写像である。

(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。

答え： e, e' を単位元とする。e, e' が単位元であることから、単位元の存在より、

$$ee' = e',$$
$$ee' = e$$

を得る。よって、結局 $e' = e$ である。

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

答え： a', a'' を a の逆元とする。逆元の存在より

$$a'a = e$$

を得る。両辺 LHS, RHS に右から a'' をかけるとそれぞれ

$$(\mathrm{LHS})a'' = (a'a)a'' = a'(aa'') = a'e = a'$$
$$(\mathrm{RHS})a'' = ea'' = a''$$

となり、結局 $a' = a''$ である。

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. 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。

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

答え：符号長は 5, 最小ハミング距離は 11111 と 00111 の間の 2, 符号化率は $\log_2(4)/5 = 2/5 = 0.4$.

(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。

答え： C_2 は符号長 5，最小ハミング距離 2, 符号化率 1/5 を有する．C_1 と C_2 は符号長と最小ハミング距離が同じで符号化率は C_1 のほうが大きいから、C_1 のほうが望ましい。

(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。

答え：受信語 $\vec{r}$ から最もハミング距離の近い符号語を復号結果とする。正確に書くと下である。

$$\hat{\vec{c}}^{(\mathrm{MD})}(\vec{r}) = \operatorname*{argmin}_{\vec{c}\in C} d_H(\vec{r},\vec{c})$$

(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。

答え： 符号 C を用いて通信を行い受信語 $\vec{r}$ を受信した。$\vec{r}$ から距離 t の範囲に符号語が唯一存在すれば、言い換えると $d(\vec{c},\vec{r}) \le t$ となる符号語 $\vec{c}$ は複数存在しないならば、それを復号語 $\hat{\vec{c}}_t^{(\mathrm{BD})}(\vec{r})$ とし、見つからなければ復号誤りである error を宣言して復号を中止する。正確に述べると、

$$\hat{\vec{c}}_t^{(\mathrm{BD})}(\vec{r}) = \begin{cases} \vec{c}\in C, & d(\vec{c},\vec{r}) \le t \text{ となる符号語 } \vec{c} \text{ が} \\ & \text{唯一存在する} \\ \mathrm{error}, & \text{そんな符号語 } \vec{c} \text{ は存在しない} \end{cases}$$

である。この復号法を復号半径 t の限界距離復号法という。

(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。

答え： 異なる 2 つの符号語 $\vec{c}_1, \vec{c}_2 \in C$ の $d/2$ より小さい半径 t に共通して含まれる受信語 $\vec{r}$ が存在したと仮定すると、

$$\begin{aligned} d &\leq d(\vec{c}_1,\vec{c}_2)\,(d \text{ は } C \text{ の最小距離}) \\ &\leq d(\vec{c}_1,\vec{r}) + d(\vec{r},\vec{c}_2)\ \text{(三角不等式)} \\ &< \frac{d}{2} + \frac{d}{2} = d \end{aligned}$$

で $d < d$ となり矛盾が導ける。

(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。

答え：

$$\hat{\vec{c}}_1^{(\mathrm{BD})}(\vec{r}) = \text{error}$$
$$\hat{\vec{c}}^{(\mathrm{MD})}(\vec{r}) = 110001110111$$

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。

答え： (2),(3)

(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。

答え：

$$V_2(n, t) := \sum_{i=0}^{t} \binom{n}{i} \text{個}$$

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

$$2^n \geq A(n,t)|V_2(n,t)|$$

iii. $\big(t, n, A(n,t)\big)$ に関する球充填限界式を証明せよ。
答え：充填された点の集合を X と書く。各点からハミング距離 t 以下のベクトル全体は、互いに交わりがない。 したがって、ユニオン限界を等式で満たし、

$$\begin{aligned} \# \bigcup_{\vec{x} \in X} B(\vec{x}, t) &= \sum_{\vec{x} \in X} \# B(\vec{c}, t) \\ &= |C| V_2(n,t) \end{aligned}$$

がなりたつ。左辺の集合は $\mathbb{F}_2^n$ に含まれるまたは等しいので、

$$2^n \geq A(n,t)|V_2(n,t)|$$

となる。

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。

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

答え：11 と 11 の和 00 が符号 C_1 に含まれないから C_1 は線形符号ではない。

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

答え：　線形符号であり、次元は 3、基底は $\{10110, 01101, 11111\}$ となる。基底の選び方は任意性があるので、答えは一意ではない。生成行列は基底の要素を行ベクトルとして積み上げたもの。最小距離 1，符号化率 3/5,

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

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

答え：いくつかの基本行変形[4]により、

$$\begin{pmatrix} 1000|1 \\ 1011|0 \\ 1111|1 \\ 0001|0 \end{pmatrix} \overset{\text{前進消去}}{\longrightarrow} \begin{pmatrix} 1000|1 \\ 0111|0 \\ 0011|1 \\ 0001|0 \end{pmatrix}$$

$$\overset{\text{後退代入}}{\longrightarrow} \begin{pmatrix} 1000|1 \\ 0100|1 \\ 0010|1 \\ 0001|0 \end{pmatrix}.$$

となる。よって、$(x_1, \ldots, x_4) = (1110)$ である。

(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。

答え：

$$C^\perp = \{000, 011, 101, 110\}$$
$$C = \{000, 111\}$$

(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。

[4] https://ja.wikipedia.org/wiki/行列の基本変形

答え： $B(X,Y)$ の $B_w \neq 0$ となる $w > 0$ の最小値が $C^{\perp}$ の最小距離 $d^{\perp}$ である。MacWilliams の恒等式から双対符号の重み分布多項式 $A(X,Y)$ を求めることができる。$A(X,Y)$ の $A_w \neq 0$ となる $w > 0$ の最小値が C の最小距離 d である。

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。

答え：

$$G = \begin{pmatrix} 1000\ 110 \\ 0100\ 011 \\ 0010\ 101 \\ 0001\ 111 \end{pmatrix}$$

(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。

答え：(1010011)

(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。

答え：(1111111).

(d) 符号語数、次元、符号化率を求めよ。

答え：16,4,4/7

(e) 最小距離が 3 以上であることを証明せよ。

答え：H の異なる 2 列は異なっていて線形独立だから、最小距離は 3 以上となる。

(f) 最小距離が 3 以下であることを証明せよ。

答え：H の第 1,2,3 列は線形従属なので、最小距離は 3 以下である。

(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。

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

答え： H' のある 3 つの列 c_1, c_2, c_3 が線系従属であるとすると $c_1 + c_2 + c_3 = 0$ となる。しかしこの第 4 要素は 1 になるはずなので、矛盾する。ハミング符号の符号語を構成する列ベクトルに第 8 列を加えると、ゼロベクトルとなるので、これら 4 つの列ベクトルは線系従属となる。したがって、H' の最小ハミング距離は 4 である。

(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。

答え：半径 1 のハミング球の要素数は $n+1$ である。各符号語の半径 1 のハミング球には交わりがない。なぜなら、交わりがあったと仮定するとその符号語間のハミング距離は 2 となり、最小距離が 3 であることに矛盾する。したがって、$t=1$ として次のユニオン限界を等式で満たす。

$$\#\bigcup_{\vec{x}\in C} B(\vec{x},t) \le \sum_{\vec{x}\in C} \#B(\vec{c},t)$$

$t=1$ に対して、

$$\begin{aligned}\sum_{\vec{x}\in C} \#B(\vec{c},t) &= |C|V_2(n,t)\\ &= 16\times(n+1) = 16\times 8 = 128\end{aligned}$$

となり、$\mathbb{F}_2^7$ の要素をすべて埋め尽くすことが分かる。

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

答え：群である。$e=0, -x$

ii. 非零実数の集合とその乗算

答え：群である。$e=1, x^{-1}$

iii. 2×2 実行列の集合と行列の乗算

答え：群でない。単位元は単位行列 I_2 となるが、非正則行列 X には乗じて $XY = YX = I_n$ となる行列は存在しない。

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

答え：群である。単位元は恒等写像である。写像 $x : X \to X$ に対して、x の逆元は $y \in X$ に対して $x(a) = y$ となる $a \in X$ を対応させる写像、つまり逆写像である。

(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。

答え： e, e' を単位元とする。e, e' が単位元であることから、単位元の存在より、

$$ee' = e',$$
$$ee' = e$$

を得る。よって、結局 $e' = e$ である。

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

答え： a', a'' を a の逆元とする。逆元の存在より

$$a'a = e$$

を得る。両辺 LHS, RHS に右から a'' をかけるとそれぞれ

$$(\mathrm{LHS})a'' = (a'a)a'' = a'(aa'') = a'e = a'$$
$$(\mathrm{RHS})a'' = ea'' = a''$$

となり、結局 $a' = a''$ である。

(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。

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. 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。

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

答え：符号長は 12，最小ハミング距離は 6，符号化率は $\log_2(4)/12 = 1/6$.

(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。

答え： C_2 は符号長 5，最小ハミング距離 2, 符号化率 1/5 を有する．C_1 と C_2 は符号長と最小ハミング距離が同じで符号化率は C_1 のほうが大きいから、C_1 のほうが望ましい。

(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。

答え：受信語 $\vec{r}$ から最もハミング距離の近い符号語を復号結果とする。正確に書くと下である。

$$\hat{\vec{c}}^{(\mathrm{MD})}(\vec{r}) = \operatorname*{argmin}_{\vec{c}\in C} d_H(\vec{r}, \vec{c})$$

(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。

答え： 符号 C を用いて通信を行い受信語 $\vec{r}$ を受信した。$\vec{r}$ から距離 t の範囲に符号語が唯一存在すれば、言い換えると $d(\vec{c}, \vec{r}) \leq t$ となる符号語 $\vec{c}$ は複数存在しないならば、それを復号語 $\hat{\vec{c}}_t^{(\mathrm{BD})}(\vec{r})$ とし、見つからなければ復号誤りである error

を宣言して復号を中止する。正確に述べると、

$$\hat{\vec{c}}_t^{(\mathrm{BD})}(\vec{r}) = \begin{cases} \vec{c} \in C, & d(\vec{c},\vec{r}) \le t \text{ となる符号語 } \vec{c} \text{ が} \\ & \text{唯一存在する} \\ \text{error}, & \text{そんな符号語 } \vec{c} \text{ は存在しない} \end{cases}$$

である。この復号法を復号半径 t の限界距離復号法という。

(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、$d(\vec{c},\vec{r}) \le t$ 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。

答え： 異なる 2 つの符号語 $\vec{c}_1, \vec{c}_2 \in C$ の $d/2$ より小さい半径 t に共通して含まれる受信語 $\vec{r}$ が存在したと仮定すると、

$$\begin{aligned} d &\le d(\vec{c}_1,\vec{c}_2) \,(d \text{ は } C \text{ の最小距離}) \\ &\le d(\vec{c}_1,\vec{r}) + d(\vec{r},\vec{c}_2) \;(\text{三角不等式}) \\ &< \frac{d}{2} + \frac{d}{2} = d \end{aligned}$$

で $d < d$ となり矛盾が導ける。

(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。

答え：

$$\hat{\vec{c}}_1^{(\mathrm{BD})}(\vec{r}) = \mathrm{error}$$
$$\hat{\vec{c}}^{(\mathrm{MD})}(\vec{r}) = 110001110111$$

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。

答え： (2),(3)

(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。

答え：

$$V_2(n,t) := \sum_{i=0}^{t} \binom{n}{i} 個$$

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

答え：

$$2^n \geq A(n,t)|V_2(n,t)|$$

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

答え：充填された点の集合を X と書く。各点からハミング距離 t 以下のベクトル全体は、互いに交わりがない。 したがって、ユニオン限界を等式で満たし、

$$\begin{aligned} \# \bigcup_{\vec{x} \in X} B(\vec{x}, t) &= \sum_{\vec{x} \in X} \# B(\vec{c}, t) \\ &= |C| V_2(n,t) \end{aligned}$$

がなりたつ。左辺の集合は $\mathbb{F}_2^n$ に含まれるまたは等しいので、

$$2^n \geq A(n,t)|V_2(n,t)|$$

となる。

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。

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

答え：11 と 11 の和 00 が符号 C_1 に含まれないから C_1 は線形符号ではない。

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

答え：　線形符号であり、次元は 3、基底は $\{10110, 01101, 11111\}$ となる。基底の選び方は任意性があるので、答えは一意ではない。生成行列は基底の要素を行ベクトルとして積み上げたもの。最小距離 1，符号化率 3/5,

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

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

答え：いくつかの基本行変形[5]により、

$$\begin{pmatrix} 1000|1 \\ 1011|0 \\ 1111|1 \\ 0001|0 \end{pmatrix} \overset{\text{前進消去}}{\longrightarrow} \begin{pmatrix} 1000|1 \\ 0111|0 \\ 0011|1 \\ 0001|0 \end{pmatrix} \overset{\text{後退代入}}{\longrightarrow} \begin{pmatrix} 1000|1 \\ 0100|1 \\ 0010|1 \\ 0001|0 \end{pmatrix}.$$

となる。よって、$(x_1, \ldots, x_4) = (1110)$ である。

(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。

答え：

$$C = \{000, 011, 101, 110\}$$
$$C^\perp = \{000, 111\}$$

[5] https://ja.wikipedia.org/wiki/行列の基本変形

(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。

答え： $B(X,Y)$ の $B_w \neq 0$ となる $w > 0$ の最小値が $C^{\perp}$ の最小距離 $d^{\perp}$ である。MacWilliams の恒等式から双対符号の重み分布多項式 $A(X,Y)$ を求めることができる。$A(X,Y)$ の $A_w \neq 0$ となる $w > 0$ の最小値が C の最小距離 d である。

(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。

答え：

$$B(X,Y) = X^3 + 3XY^2$$

$$= \frac{1}{2}\boxed{\text{下の式を展開すれば確認できる}} \quad = \frac{1}{2}\big((X+Y)$$

$$= \frac{1}{|C|}A(X+Y, X-Y)$$

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。

答え：

$$G = \begin{pmatrix} 1000\ 110 \\ 0100\ 011 \\ 0010\ 101 \\ 0001\ 111 \end{pmatrix}$$

(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。

答え：(1010011)

(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。

答え：(1111111).

(d) 符号語数、次元、符号化率を求めよ。

答え：16,4,4/7

(e) 最小距離が 3 以上であることを証明せよ。

答え：H の異なる 2 列は異なっていて線形独立だから、最小距離は 3 以上となる。

(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。

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

答え： H' のある 3 つの列 c_1, c_2, c_3 が線系従属であるとすると $c_1 + c_2 + c_3 = 0$ となる。しかしこの第 4 要素は 1 になるはずなので、矛盾する。ハミング符号の符号語を構成する列ベクトルに第 8 列を加えると、ゼロベクトルとなるので、これら 4 つの列ベクトルは線系従属となる。したがって、H' の最小ハミング距離は 4 である。

(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.

答え：(1) ３回以上必要なことを説明すれば良い。つまり、１回と２回では不十分なことを言えば良い。３回で十分なことを説明しても意味ない。検出器の１回の使用の結果は検出するかしないかの２通りなので，検出器を N 回使用した時に得られる使用結果は 2^N 通りである．どのワインが毒ワインであるかは，毒ワインがない場合を含めて８通りである．$N = 1$ と $N = 2$ の場合では使用結果はそれぞれ２通りと４通りしか無いので，８通りの毒ワインのありかを分別することはできない．従って，使用結果から毒ワインを見つけるためには $N \geq 3$ でなければならない.

(2) 検出器の使用方法

１回目： W_1, W_2, W_4, W_5 を混ぜて入れる

２回目： W_1, W_2, W_3, W_6 を混ぜて入れる

３回目： W_1, W_3, W_4, W_7 を混ぜて入れる

１，２，３回目の測定の結果をそれぞれ、

$$s_1, s_2, s_3 \in \{0\text{: 検出しなかった}, 1\text{: 検出した}\}$$

とする．３回の測定の結果が全て０である場合には毒ワインはない。s_1, s_2, s_3 をシンドロームとしてハミング符号の復号を行う。シンドロームと一致する列の番号に対応するワインに毒が含まれていることがわかる。

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

答え：群である。$e = 0, -x$

ii. 非零実数の集合とその乗算

答え：群である。$e = 1, x^{-1}$

iii. 2×2 実行列の集合と行列の乗算

答え：群でない。単位元は単位行列 I_2 となるが、非正則行列 X には乗じて $XY = YX = I_n$ となる行列は存在しない。

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

答え：群である。単位元は恒等写像である。写像 $x : X \to X$ に対して、x の逆元は $y \in X$ に対して $x(a) = y$ となる $a \in X$ を対応させる写像、つまり逆写像である。

(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。

答え： e, e' を単位元とする。e, e' が単位元であることから、

単位元の存在より、

$$ee' = e',$$
$$ee' = e$$

を得る。よって、結局 $e' = e$ である。

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

答え： a', a'' を a の逆元とする。逆元の存在より

$$a'a = e$$

を得る。両辺 LHS, RHS に右から a'' をかけるとそれぞれ

$$(\mathrm{LHS})a'' = (a'a)a'' = a'(aa'') = a'e = a'$$
$$(\mathrm{RHS})a'' = ea'' = a''$$

となり、結局 $a' = a''$ である。

(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			

答え：

$\times$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

ii. 演算表が一意に定まることを証明せよ。

答え： 最上行と再左列は単位元の性質から自動的に決まる。$ab \neq a$ であることを示す。$ab = a$ だと仮定すると、両辺に左から a^{-1} をかけて $b = e$ となってしまい、元が 3 つかることに矛盾する。同様に考えて、$ab \neq b, ba \neq a, ba \neq b$ となり、結果 $ab = ba = e$ となる。逆元が一意に決まることから、各行各列は e, a, b の順序を入れ替えたものになっていなければならないので、残りの $aa = b, bb = a$ が分かる。

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. 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。

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

答え： 符号長は 8,
符号語数は 4,

最小ハミング距離は 3,
符号化率は $\log_2(4)/8 = 1/4 = 0.25$.

(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。

答え： C_2 は符号長 5, 最小ハミング距離 2, 符号化率 1/5 を有する. C_1 と C_2 は符号長と最小ハミング距離が同じで符号化率は C_1 のほうが大きいから、C_1 のほうが望ましい。

(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。

答え：受信語 $\vec{r}$ から最もハミング距離の近い符号語を復号結果とする。正確に書くと下である。

$$\hat{\vec{c}}^{(\mathrm{MD})}(\vec{r}) = \operatorname*{argmin}_{\vec{c}\in C} d_H(\vec{r}, \vec{c})$$

(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。

答え： 符号 C を用いて通信を行い受信語 $\vec{r}$ を受信した。$\vec{r}$ から距離 t の範囲に符号語が唯一存在すれば、言い換えると $d(\vec{c}, \vec{r}) \le t$ となる符号語 $\vec{c}$ は複数存在しないならば、それを

復号語 $\hat{\vec{c}}_t^{(\mathrm{BD})}(\vec{r})$ とし、見つからなければ復号誤りである error を宣言して復号を中止する。正確に述べると、

$$\hat{\vec{c}}_t^{(\mathrm{BD})}(\vec{r}) = \begin{cases} \vec{c} \in C, & d(\vec{c},\vec{r}) \le t \text{ となる符号語 } \vec{c} \text{ が} \\ & \text{唯一存在する} \\ \text{error}, & \text{そんな符号語 } \vec{c} \text{ は存在しない} \end{cases}$$

である。この復号法を復号半径 t の限界距離復号法という。

(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、$d(\vec{c},\vec{r}) \le t$ 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。

答え： 異なる 2 つの符号語 $\vec{c}_1, \vec{c}_2 \in C$ の $d/2$ より小さい半径 t に共通して含まれる受信語 $\vec{r}$ が存在したと仮定すると、

$$\begin{aligned} d &\le d(\vec{c}_1,\vec{c}_2) \,(d \text{ は } C \text{ の最小距離}) \\ &\le d(\vec{c}_1,\vec{r}) + d(\vec{r},\vec{c}_2) \;\; (\text{三角不等式}) \\ &< \frac{d}{2} + \frac{d}{2} = d \end{aligned}$$

で $d < d$ となり矛盾が導ける。

(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。

答え：

$$\hat{\vec{c}}_1^{(\mathrm{BD})}(\vec{r}) = \mathrm{error}$$
$$\hat{\vec{c}}^{(\mathrm{MD})}(\vec{r}) = 110001110111$$

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。

答え： (2),(3)

(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。

答え：

$$V_2(n,t) := \sum_{i=0}^{t} \binom{n}{i} 個$$

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

答え：

$$2^n \geq A(n,t)|V_2(n,t)|$$

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

答え：充填された点の集合を X と書く。各点からハミング距離 t 以下のベクトル全体は、互いに交わりがない。 したがって、ユニオン限界を等式で満たし、

$$\begin{aligned} \# \bigcup_{\vec{x} \in X} B(\vec{x}, t) &= \sum_{\vec{x} \in X} \# B(\vec{c}, t) \\ &= |C| V_2(n,t) \end{aligned}$$

がなりたつ。左辺の集合は $\mathbb{F}_2^n$ に含まれるまたは等しいので、

$$2^n \geq A(n,t)|V_2(n,t)|$$

となる。

(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. $1 + 1$

答え：0

ii. $1/1$

答え：1

iii. $1(0110)$

答え：(0110)

iv. $0(0110)$

答え：(0000)

v. $(011) + (001)$

答え：010

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

答え：定義されていない

(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。

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

答え： 0 符号語を含まないので、線形符号ではない。

(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
```

答え：次元 4, 最小距離 2

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

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

答え：0001

(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。

答え：

$$C = \{000, 011, 101, 110\}$$
$$C^{\perp} = \{000, 111\}$$

(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
```

答え：

$$A(X,Y) = X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7$$
$$B(X,Y) = X^7 + 7X^3Y^4$$

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。

答え：

$$G = \begin{pmatrix} 1000\ 110 \\ 0100\ 011 \\ 0010\ 101 \\ 0001\ 111 \end{pmatrix}$$

(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。

答え：(1010011)

(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。

答え：(1111111).

(d) 符号語数、次元、符号化率を求めよ。

答え：16,4,4/7

(e) 最小距離が 3 以上であることを証明せよ。

答え：H の異なる 2 列は異なっていて線形独立だから、最小距離は 3 以上となる。

(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。

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

答え： H' のある 3 つの列 c_1, c_2, c_3 が線系従属であるとすると $c_1 + c_2 + c_3 = 0$ となる。しかしこの第 4 要素は 1 になるはずなので、矛盾する。ハミング符号の符号語を構成する列ベクトルに第 8 列を加えると、ゼロベクトルとなるので、これら 4 つの列ベクトルは線系従属となる。したがって、H' の最小ハミング距離は 4 である。

(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。

答え：(1) 3回以上必要なことを説明すれば良い。つまり、1回と2回では不十分なことを言えば良い。3回で十分なことを説明しても意味ない。検出器の1回の使用の結果は検出するかしないかの2通りなので，検出器を N 回使用した時に得られる使用結果は 2^N 通りである．どのワインが毒ワインであるかは，毒ワインがない場合を含めて8通りである．$N = 1$ と $N = 2$ の場合では使用結果はそれぞれ2通りと4通りしか無いので，8通りの毒ワインのありかを分別することはできない．従って，使用結果から毒ワインを見つけるためには $N \geq 3$ でなければならない．

(2) 検出器の使用方法

1回目： W_1, W_2, W_4, W_5 を混ぜて入れる

2回目： W_1, W_2, W_3, W_6 を混ぜて入れる

3回目： W_1, W_3, W_4, W_7 を混ぜて入れる

1，2，3回目の測定の結果をそれぞれ、

$$s_1, s_2, s_3 \in \{0\text{: 検出しなかった}, 1\text{: 検出した}\}$$

とする．3回の測定の結果が全て0である場合には毒ワインはない。s_1, s_2, s_3 をシンドロームとしてハミング符号の復号を行う。シンドロームと一致する列の番号に対応するワインに毒が含まれていることがわかる。

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

答え：群である。$e = 0, -x$

ii. 無理数と 1 を含む集合とその乗算。

答え：群でない。$\sqrt{2}\sqrt{2} = 2$ となり無理数になっていないから。

iii. 非零実数の集合とその乗算

答え：群である。$e = 1, x^{-1}$

iv. 2×2 実行列の集合と行列の乗算

答え：群でない。単位元は単位行列 I_2 となるが、非正則行列 X には乗じて $XY = YX = I_n$ となる行列は存在しない。

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

答え：群である。単位元は恒等写像である。写像 $x : X \to X$ に対して、x の逆元は $y \in X$ に対して $x(a) = y$ となる $a \in X$ を対応させる写像、つまり逆写像である。

(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。

答え： e, e' を単位元とする。e, e' が単位元であることから、単位元の存在より、

$$ee' = e',$$
$$ee' = e$$

を得る。よって、結局 $e' = e$ である。

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

答え： a', a'' を a の逆元とする。逆元の存在より

$$a'a = e$$

を得る。両辺 LHS, RHS に右から a'' をかけるとそれぞれ

$$(\mathrm{LHS})a'' = (a'a)a'' = a'(aa'') = a'e = a'$$
$$(\mathrm{RHS})a'' = ea'' = a''$$

となり、結局 $a' = a''$ である。

(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			

答え：

$\times$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

ii. 演算表が一意に定まることを証明せよ。

答え： 最上行と再左列は単位元の性質から自動的に決まる。$ab \neq a$ であることを示す。$ab = a$ だと仮定すると、両辺に左から a^{-1} をかけて $b = e$ となってしまい、元が 3 つかることに矛盾する。同様に考えて、$ab \neq b, ba \neq a, ba \neq b$ となり、結果 $ab = ba = e$ となる。逆元が一意に決まることから、各行各列は e, a, b の順序を入れ替えたものになっていなければならないので、残りの $aa = b, bb = a$ が分かる。

(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 準同型である、いいかえると

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

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

答え： 次に、 $\mathrm{Ker}(f)$ が G の正規部分群であることを示します。任意の $g \in G$ および $a \in \mathrm{Ker}(f)$ に対し て、共役元 gag^{-1} が $\mathrm{Ker}(f)$ に含まれることを確認します。f が準同型

であるため、

$$\begin{aligned} f\left(gag^{-1}\right) &= f(g)f(a)f(g)^{-1} \\ &= f(g)\cdot 1\cdot f(g)^{-1} \\ &= f(g)f(g)^{-1} = 1 \end{aligned}$$

となり、 $gag^{-1} \in \mathrm{Ker}(f)$ です。したがって、 $\mathrm{Ker}(f)$ は G の正規部分群です。

代数系と符号理論 中間試験 (令和 7 年 10 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. 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) 次の 2 元符号の符号長、符号語数、最小距離、符号化率を答えよ。

$$C_0 = \{00000, 10101, 01010, 11111\}$$

答え：符号長は 5，符号語数は 4，最小ハミング距離は 2，符号化率は $\log_2(4)/5 = 0.4$。

(b) 受信語 $\boldsymbol{r}$ に対して半径 t の限界距離復号 $\hat{\boldsymbol{c}}_t^{(\mathrm{BD})}(\boldsymbol{r})$ の定義を述べよ。

答え：$\boldsymbol{r}$ から距離 t 以内に符号語がちょうど 1 つ存在するとき，それを復号結果とする。

$$\hat{\boldsymbol{c}}_t^{(\mathrm{BD})}(\boldsymbol{r}) = \begin{cases} \boldsymbol{c} \in C, & d(\boldsymbol{c}, \boldsymbol{r}) \le t \text{ となる符号語が唯一存在する} \\ \text{error}, & \text{そのような符号語が存在しないとき.} \end{cases}$$

(c) 最小距離 d の符号 C を用いて通信する。$2t < d$ のとき，任意の受信語 $\boldsymbol{r}$ に対して $d(\boldsymbol{c}, \boldsymbol{r}) \leq t$ を満たす符号語 $\boldsymbol{c}$ が存在するとしたら一意であることを示せ。

答え： 異なる 2 つの符号語 $\boldsymbol{c}_1, \boldsymbol{c}_2 \in C$ が存在し，同じ $\boldsymbol{r}$ がそれぞれ距離 t 以内にあると仮定すると，

$$d(\boldsymbol{c}_1, \boldsymbol{c}_2) \leq d(\boldsymbol{c}_1, \boldsymbol{r}) + d(\boldsymbol{r}, \boldsymbol{c}_2) \leq t + t < d,$$

となり矛盾。よってそのような $\boldsymbol{c}$ は一意である。

M.2 以下の問に答えよ。

(a) 次の生成行列 G で定義される符号 C の符号長 n と次元 k を答えよ。

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

答え：$n = 4, k = 2$.

(b) この符号 C のパリティ検査行列 H を求めよ。

答え： $H = [-P^T | I_2] = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$.

(c) 双対符号 $C^\perp$ の次元を求めよ。

答え：$n - k = 2$.

(d) 最小距離 $d = 3$、符号長 $n = 5$、次元 $k = 2$ である二元線形符号のパリティ検査行列 H を 1 つ与えよ. 最小距離が 3 であることと次元が 2 であることの確認も行うこと。

答え： 次の 3×5 行列は条件を満たすパリティ検査行列の一例である。

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

確認：H の列ベクトルを $h_1,\dots,h_5$ とすると、任意の 2 列は一次独立であり、$h_1+h_2+h_4=0$ が成り立つので 3 列が一次従属である。したがって最小距離は $d=3$。また $n-k=3$ より次元 $k=2$。

M.3 以下の問に答えよ。

(a) 訂正能力 t、符号長 n、サイズ M の 2 元符号 C に対して、球充填限界式を述べよ。

答え：$2^n\geq MV_2(n,t)$。

(b) $n=6,d=3$ のときハミング球の要素数 $V_2(n,t)$ を求めよ。t は訂正能力 $t=\left\lfloor\frac{d-1}{2}\right\rfloor$ である。

答え：$V_2(6,1)=\binom{6}{0}+\binom{6}{1}=7.$

(c) 符号長 $n=6$、訂正能力 $t=1$, 次元 $k=3$ の 2 元線形符号 C が球充填限界を等号で満たすかどうか確認せよ。

答え：$|C|V_2(6,1)=8\times7=56<2^6=64$ より等号は成り立たない。

(d) 次元 k で、最小距離 $d=3$ である、2 元線形符号 C が球充填限界が等号成立するとする。C の符号長 n を求めよ。

答え： $|C| = 2^k$ より、球充填限界の等号成立は

$$2^n = 2^k V_2(n,1) = 2^k(n+1)$$

となる。よって n は $2^{n-k} = n+1$ を満たす。これは $n = 2^m - 1, k = n - m$（m は正整数）のときに成り立つ。

M.4 以下の問に答えよ。

(a) 次のパリティ検査行列 H に対して，$y = (1010)$ のシンドローム $s(y) = Hy^T$ を求めよ。

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

答え：

$$s(y) = H \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1\cdot 1 + 0\cdot 0 + 1\cdot 1 + 1\cdot 0 \\ 0\cdot 1 + 1\cdot 0 + 1\cdot 1 + 0\cdot 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

よってシンドロームは $s(y) = (01)$。

(b) シンドロームを $s(x) = Hx^T$ と定める．2つの語 $x, y \in \mathbb{F}_2^n$ が同じシンドローム $s(x) = s(y)$ をもつとき，x と y が同じコセット（剰余類）に属する $(x - y \in C)$ ことを示せ．

答え： $s(x) = s(y) \iff Hx^T = Hy^T \iff H(x-y)^T = 0.$ よって $x - y \in C = \{z \mid Hz^T = 0\}$ となり，x と y は C に

よる同値関係で同じ剰余類（コセット） $x + C = y + C$ に属する.

(c) 最小距離 $d = 3$ の線形符号のパリティ検査行列を H とする。重み 1 の誤りベクトル e から、対応するシンドローム Hs^T への対応は、1 対 1 であることを証明せよ。

答え： もし異なる 2 つの重み 1 誤り e_i, e_j が同じシンドロームを与えるなら，$He_j^T = He_i^T$、したがって $H(e_i + e_j)^T = 0$ となり $e_i + e_j \in C$ である。しかし $e_i + e_j$ の重みは 2 なので，符号に重み 2 の語が存在することになる。これは最小距離 $d = 3$ に反する。したがって，重み 1 誤りのシンドロームは一意に対応する。

M.5 以下の問に答えよ。

(a) 群 $(G, \circ)$ の 4 つの性質 (1)-(4) について，A,B,C,D の中から適切なものを選びなさい。（選択肢）

(A) $e \circ a = a \circ e = a$,

(B) $a \circ b \in G$,

(C) $(a \circ b) \circ c = a \circ (b \circ c)$,

(D) $(a + b) \circ c = a \circ (b + c)$,

(E) $a \circ a^{-1} = a^{-1} \circ a = e$

(1) 集合 G が二項演算 $\circ$ に対して _____ であること。

(2) 任意の $a, b, c \in G$ に対して _____ が成り立つこと。

(3) 単位元 e が存在し，任意の $a \in G$ に対して $\_\_\_\_\_$ が成り立つこと。

(4) 任意の $a \in G$ に対して逆元 $a^{-1} \in G$ が存在し，$\_\_\_\_\_$ が成り立つこと。

答え：略

(b) 次の表で定義される集合 $S = \{a, b, c, d\}$ との二項演算 $\circ$ に対して、$(S, \circ)$ が群となるか判定せよ（単位元はどれか？各元に対する逆元はなにか？）。

$\circ$	d	a	b	c
d	d	a	b	c
a	a	d	c	b
b	b	c	d	a
c	c	b	a	d

答え： 単位元は e。逆元は $a^{-1} = a,\ b^{-1} = b,\ c^{-1} = c$。
結合法則も成り立つため，$(S, \circ)$ は群である。

(c) 上の群 $S = \{a, b, c, d\}$ において，部分群 $H = \{a, d\}$ が正規部分群であることを確認せよ。

答え： S の演算表より，
$dH = H,\ aH = H,\ bH = \{b, c\},\ cH = \{c, b\} = bH$。
よってすべての $s \in S$ について $sH = Hs$ が成り立つため，H は正規部分群である。

(d) 商群 S/H の元と演算表を求めよ。

答え： $S/H = \{H,\ bH\}$。

演算は

$\circ$	H	bH
H	H	bH
bH	bH	H

となり，商群 $S/H \simeq \mathbb{Z}_2$。

4　第4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。

4.1 $(R, +, \times)$ と $(S, +, \times)$ を可換環とする．写像 $f : R \to S$ が **環の準同型**，すなわち

$$\begin{aligned} &f(a+b) = f(a) + f(b), \\ &f(ab) = f(a)f(b), \\ &f(1_R) = 1_S \\ &\text{for all } a, b \in R \end{aligned}$$

を満たすとする．このとき，

$$\mathrm{Ker}(f) := \{\, a \in R \mid f(a) = 0 \,\}$$

が R のイデアルであることを示せ．

答え： (1) まず，$\mathrm{Ker}(f)$ が加法に関して部分群であることを示す．$a, b \in \mathrm{Ker}(f)$ のとき，

$$f(a+b) = f(a) + f(b) = 0 + 0 = 0$$

より $a+b \in \mathrm{Ker}(f)$．また $f(0) = 0$ より $0 \in \mathrm{Ker}(f)$ であり，

$$f(-a) = -f(a) = -0 = 0$$

なので $-a \in \mathrm{Ker}(f)$．したがって $\mathrm{Ker}(f)$ は加法に関して部分群である．

(2) 次にイデアル条件を示す．任意の $r \in R$ および $a \in \mathrm{Ker}(f)$ に対して，

$$f(ra) = f(r)f(a) = f(r) \cdot 0 = 0$$

よって $ra \in \mathrm{Ker}(f)$．R が可換であるため，同様に $ar = ra \in \mathrm{Ker}(f)$ も成り立つ．

(3) 以上より，$\mathrm{Ker}(f)$ は加法部分群であり，任意の $r \in R$ に対して $ra, ar \in \mathrm{Ker}(f)$ が成り立つので，$\mathrm{Ker}(f)$ は R のイデアルである．

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

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

答え：

$$\begin{aligned} &= (1-1) + (1-1)X + (0-1)X^2 + X^3 \\ &= 0 + 0X + (-1)X^2 + X^3 \\ &= -X^2 + X^3 \end{aligned}$$

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

答え：

$$\begin{aligned} &= (1 + X + X^2) + (X + X^2 + X^3) \\ &= 1 + (1+1)X + (1+1)X^2 + X^3 \\ &= 1 + 0X + 0X^2 + X^3 \\ &= 1 + X^3 \end{aligned}$$

(c) $1+X^2+X^5$ を $1+X$ で割った商と剰余。

答え：

$$1+X^2+X^5=(X^2-X^3+X^4)\times(1+X)+1$$

なので、

$$\begin{aligned}&(1+X^2+X^5)/(1+X)\\&=\text{商 } X^2-X^3+X^4\text{剰余 } 1\end{aligned}$$

4.3 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。

答え：例えば、(正則 n 次正方実行列の集合,$\times$)

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

答え：例えば、(n 次正方実行列の集合,$\{+,\times\}$)

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

答え：例えば、(n 次正方実行列の集合,$\{+,\times\}$)

4.4 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。

答え：

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\times$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

(b) $+, \times$ のそれぞれに関する単位元を答えよ。

答え：$[0]$,$[1]$

(c) 体でないことを確認せよ。

答え：$[2]$ の逆元、つまり $[2] \times [i] = [1]$ となる $[i] \in \mathbb{Z}/4\mathbb{Z}$ が存在しない。

4.5 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。

答え：

+	[00]	[10]	[01]	[11]
[00]	[00]	[10]	[01]	[11]
[10]	[10]	[00]	[11]	[01]
[01]	[01]	[11]	[00]	[10]
[11]	[11]	[01]	[10]	[00]

x	[00]	[10]	[01]	[11]
[00]	[00]	[00]	[00]	[00]
[10]	[00]	[10]	[01]	[11]
[01]	[00]	[01]	[01]	[00]
[11]	[00]	[11]	[00]	[11]

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。

答え：[00],[10]

(c) 体でないことを確認せよ。

答え：[01] の逆元が存在しない。

4.6 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。

答え：

$$
\begin{aligned}
&[a_1 + b_1X] + [a_2 + b_2X] \\
&[(a_1 + b_1X) + (a_2 + b_2X) \bmod 1 + X^2] \\
&= [(a_1 + a_2) + (b_1 + b_2)X \bmod 1 + X^2] \\
&= [(a_1 + a_2) + (b_1 + b_2)X]
\end{aligned}
$$

$$
\begin{aligned}
&[a_1 + b_1X] \times [a_2 + b_2X] \\
&[(a_1 + b_1X) \times (a_2 + b_2X) \bmod 1 + X^2] \\
&= [b_1b_2X^2 + (a_1b_2 + a_2b_1)X + a_1a_2 \\
&\quad \bmod 1 + X^2] \\
&= [(a_1b_2 + a_2b_1)X + a_1a_2 - b_1b_2] \\
&\in \mathbb{R}[X]/\langle 1 + X^2 \rangle
\end{aligned}
$$

となる。

(b) $+, \times$ のそれぞれに関する単位元を答えよ。

答え： [0],[1]

(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。

答え：

$$(a+bX)\frac{a-bX}{a^2+b^2} \bmod 1+X^2 = 1$$

より，$a+bX$ の逆元は

$$\Big(a+bX\Big)^{-1} = \frac{a-bX}{a^2+b^2} \in \mathbb{R}[X]/\langle 1+X^2\rangle$$

だと分かる．これらの乗算と乗法に関する逆元が複素数における乗算

$$\begin{aligned}&(a_1+b_1\sqrt{-1})(a_2+b_2\sqrt{-1})\\ &= (a_1b_2+a_2b_1)\sqrt{-1}+a_1a_2-b_1b_2 \in \mathbb{C}\end{aligned}$$

$$\Big(a+b\sqrt{-1}\Big)^{-1} = \frac{a-b\sqrt{-1}}{a^2+b^2} \in \mathbb{C}$$

とまったく同じになっていることがわかる。その他の演算 (加算，減算) も複素数における演算と同じなので、この例で構成される $\mathbb{R}[X]/\langle 1+X^2\rangle$ は実は複素数 $\mathbb{C}$ そのものである。高校ではこの X を $\sqrt{-1}$ と書いていたと考えることができる．

4.7 $X^3+X+1 \in \mathbb{F}_2[X]$ が既約多項式であることを証明せよ。

答え： ２次以下の多項式で割り切れないことを示せば良い。３次多項式が２次多項式で割り切れる時には１次多項式の因

数を含むので、1次多項式で割り切れないことを示せば十分である。$\mathbf{F}_2$ 上の一次の多項式は X と $X+1$ である。どちらで割っても X^3+X+1 の余りは 1 になる。したがって、X^3+X+1 を $\mathbf{F}_2$ 上の多項式と見たときに既約多項式であることがわかる。

4.8 $\mathbb{F}_7$ の加算、減算、乗算、除算に関する演算表を書け。

答え：

```
ADD
  | 0 1 2 3 4 5 6
--+---------------
0 | 0 1 2 3 4 5 6
1 | 1 2 3 4 5 6 0
2 | 2 3 4 5 6 0 1
3 | 3 4 5 6 0 1 2
4 | 4 5 6 0 1 2 3
5 | 5 6 0 1 2 3 4
6 | 6 0 1 2 3 4 5
MUL
  | 0 1 2 3 4 5 6
--+---------------
0 | 0 0 0 0 0 0 0
1 | 0 1 2 3 4 5 6
2 | 0 2 4 6 1 3 5
3 | 0 3 6 2 5 1 4
4 | 0 4 1 5 2 6 3
5 | 0 5 3 1 6 4 2
6 | 0 6 5 4 3 2 1
SUB
  | 0 1 2 3 4 5 6
--+---------------
0 | 0 6 5 4 3 2 1
1 | 1 0 6 5 4 3 2
2 | 2 1 0 6 5 4 3
3 | 3 2 1 0 6 5 4
```

```
4 | 4 3 2 1 0 6 5
5 | 5 4 3 2 1 0 6
6 | 6 5 4 3 2 1 0
DIV
  | 0 1 2 3 4 5 6
--+---------------
0 | - 0 0 0 0 0 0
1 | - 1 4 5 2 3 6
2 | - 2 1 3 4 6 5
3 | - 3 5 1 6 2 4
4 | - 4 2 6 1 5 3
5 | - 5 6 4 3 1 2
6 | - 6 3 2 5 4 1
```

4.9 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。

答え：

$$(1+X) \times (X+X^2) = X + X^2 + X^2 + X^3 = X + X^3$$

である。$X + X^3$ を $p(X)$ で割ると、

$$(X + X^3) \div p(X) = \text{商}\ 1\ \text{あまり}\ 1 + X + X^2$$

となる。このあまりをベクトル表示して、$[111]$ が答えとなる。

(b) 演算表を使って次の計算の答えを求めよ。

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

答え：乗算表から $[001]$ と分かる。

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

答え：$[010]$ と乗じて $[100]$ になるものなので、$[011]$

iii. $[011]/[010]$

答え：$[011]/[010] = [011] \times [010]^{-1} = [011] \times [011] = [110]$

(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。

答え： $\alpha_1 = [100], \alpha_2 = [011]$

4.10 $\mathbb{F}_{11}$ 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。

答え：符号長 5、次元 3、符号化率 3/5、最小距離 3

(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。

答え：[7][7][8][10][2]

(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。

答え：

```
G=
[1][1][1][1][1]
[0][1][2][3][4]
[0][1][4][9][5]
f=
[7][1][7]
c=
[7][4][4][7][2]
e=
[0][0][0][2][0]
r=
[7][4][4][9][2]
A=
[1][0][0][0][7][0]
[1][1][1][1][4][4]
```

```
[1][2][4][8][4][8]
[1][3][9][5][9][5]
[1][4][5][9][2][8]
A=
[1][0][0][0][7][0]
[0][1][1][1][8][4]
[0][0][1][3][7][0]
[0][0][0][1][4][8]
[0][0][0][0][1][3]
前進消去終了 rank=5
A=
[1][0][0][0][0][1]
[0][1][0][0][0][4]
[0][0][1][0][0][2]
[0][0][0][1][0][7]
[0][0][0][0][1][3]
後退代入終了 rank=5
q=
[10][7][9][4][8][1]
q0=
[10][7][9][4]
q1=
[8][1]
-q0/q1=
商
[7][1][7]
剰余
```

4.11 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。

答え： 符号長 5、次元 3、符号化率 3/5、最小距離 3

(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。

答え：[001][100][001][100][010]

(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。

答え：

```
G=
[100] [100] [100] [100] [100]
[000] [100] [010] [110] [001]
[000] [100] [001] [101] [111]
f=
[000] [000] [101]
c=
[000] [101] [110] [011] [100]
e=
[000] [000] [000] [000] [000]
r=
[000] [101] [110] [011] [100]
A=
[100] [000] [000] [000] [000] [000]
[100] [100] [100] [100] [101] [101]
[100] [010] [001] [101] [110] [011]
[100] [110] [101] [010] [011] [111]
```

```
[100][001][111][011][100][001]
A=
[100][000][000][000][000][000]
[000][100][100][100][101][101]
[000][000][100][110][101][010]
[000][000][000][100][000][101]
[000][000][000][000][000][000]
前進消去終了 rank=4
A=
[100][000][000][000][000][000]
[000][100][000][000][000][000]
[000][000][100][000][101][000]
[000][000][000][100][000][101]
[000][000][000][000][000][000]
後退代入終了 rank=4
q=
[000][000][101][101][100][100]
q0=
[000][000][101][101]
q1=
[100][100]
-q0/q1=
商
[000][000][101]
剰余
```

4.12 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。

答え：(i$\Longleftrightarrow$ii)：H を C のパリティ検査行列とする。C の最

小距離は d なので、H の $d-1$ 列は線型独立である。シングルトン限界から $d \leq n-k+1$ である。これから、$d = n-k+1$ と H の $n-k$ 列が線型独立であることが等価であることがわかる。したがって i$\Longleftrightarrow$ii である。

(iii$\Longrightarrow$i)：k 個の座標からなる集合

$$K \subset \{1, \ldots, n\}, |K| = k$$

に対して、ベクトル $\vec{c} \in \mathbb{F}^n$ の座標を K に限定した部分ベクトルを $\vec{c}_K$ と書く。同様に G を K に限定した部分行列 G_K を定義する。

任意の K と任意の符号語 $\vec{c} \in C$ に対して、$\vec{c}_K = \vec{0} \in \mathbb{F}^k$ ならば $\vec{c} = \vec{0} \in \mathbb{F}^n$ となることを示す。これが示されれば、重みが $n-k$ 以下の符号語は存在しないので、i を導くのに十分である。$\vec{c} \in C$ なので、$\vec{c} = \vec{u}G$ となる情報ベクトル $\vec{u} \in \mathbb{F}^k$ が存在する。

$$\vec{0} = \vec{c}_K = \vec{u}G_K$$

が成り立つ。仮定より、G_K は正則になるので、$\vec{u} = 0$ となり、結局 $\vec{c} = 0$ が導けた。

(i$\Longrightarrow$iii)：仮定より C は MDS 符号なので、H の $n-k$ 列は線型独立である。任意の K と $\vec{u} \in \mathbb{F}^k$ に対して、

$$\vec{u}G_K = \vec{0} \Longrightarrow \vec{u} = 0$$

を示す。これが示されれば、$\ker G_K = \{\vec{0}\}$ となり、次元定理より $\mathrm{rank} G_K = k$ つまり、G_K の列は線形独立、つまり iii であることが分かる。$\vec{c}_K = \vec{u}G_K = \vec{0}$ なので、$\vec{c}$ の重みは高々 $n-k$ である。i から最小距離は $n-k+1$ なので、$\vec{c} = \vec{0}$ となる。

(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。

答え： C の生成行列 G は $C^{\perp}$ のパリティ検査行列 $H^{\perp}$ になる。前問から、G、即ち $H^{\perp}$ の任意の k 列は線形独立である。したがって、$C^{\perp}$ の最小距離は $k+1$ 以上となり、シングルトン限界から逆の不等式も成り立つ。こうして、$C^{\perp}$ も MDS 符号であることが示された。

4.13 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。

5　第5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。

5.1 $\mathbb{F}_4 := \mathbb{F}_2[X]/\langle 1+X+X^2\rangle$ 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。

答え：$\beta^2 = [11], \beta^3 = [10]$ よりわかる。

(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。

答え：

$$\begin{aligned} c &= (f(\beta^0), f(\beta^1), f(\beta^2)) \\ &= (f([10]), f([01]), f([11])) \\ &= ([11] + [11] \times [10], \\ &\qquad [11] + [11] \times [01], [11] + [11] \times [11]) \\ &= ([11] + [11], [11] + [10], [11] + [01]) \\ &= ([00], [01], [10]) \end{aligned}$$

(c) 生成多項式 $g(X)$ を求めよ。

答え：次数が最小のモニック符号多項式なので、

$$g(X) = ([01][10]) \text{ または } g(X) = ([01][10][00])$$

(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。

答え：モニックな 1 次符号多項式は確かに一つしかない

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

(e) $g(X)$ が $X^n - 1$ を割り切ることを示せ。

答え： 以下の通り確かに割り切れる。

$$
\begin{aligned}
&X^3 - 1 \\
&= ([01] + [10]X)([11] + [01]X + [10]X^2)
\end{aligned}
$$

商と余りを示していたら正解。

(f) C の生成行列を一つ求めよ。

答え：

$$
\begin{pmatrix}
[01][10][00] \\
[00][01][10]
\end{pmatrix}
$$

(g) パリティ検査多項式 $h(X)$ を求めよ。

答え：

$$
\begin{aligned}
h(X) &= (X^3 - 1)/g(X) \\
&= ([11] + [01]X + [10]X^2)
\end{aligned}
$$

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

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

答え：

$$
\begin{aligned}
c(X) &= [01][00][11] \\
h(X) &= [11][01][10] \\
c(X)h(X) &= [10][11][00][10][11] \\
c(X)h(X)/(X^n-1) &= \text{商 } [10][11] \text{ 剰余 } [00]
\end{aligned}
$$

$c(X)h(X)$ と商が計算できていたら正解。

(i) C のパリティ検査行列を一つ求めよ。

答え：

$$\Big([10][01][11]\Big)$$

5.2 $\mathbb{F}_5 := \mathbb{Z}/5\mathbb{Z}$ 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。

答え： $\beta^2 = [4], \beta^3 = [3], \beta^4 = [1]$ となり確かめられた。

(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。

答え：

$$
\begin{aligned}
&(f(\beta^0), f(\beta^1), f(\beta^2), f(\beta^3)) \\
&= (f([1]), f([2]), f([4]), f([3]) \\
&= ([4] + [3][1]), [4] + [3][2], \\
&\qquad [4] + [3][4], [4] + [3][3]) \\
&= ([4] + [3]), [4] + [1], [4] + [2], [4] + [4]) \\
&= ([2]), [0], [1], [3])
\end{aligned}
$$

(c) 生成多項式 $g(X)$ を求めよ。

答え： $g(X) = ([3][4][1])$

(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。

答え：モニックな２次符号多項式は確かに一つしかない

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

(e) $g(X)$ が $X^n - 1$ を割り切ることを示せ。

答え：

$$
\begin{aligned}
&(X^n - 1)/g(X) \\
&= (X^4 - 1)/([3] + [4]X + X^2) \\
&= \text{商 } ([3] + [1]X + [1]X^2) \text{ 余り } [0]
\end{aligned}
$$

(f) C の生成行列を一つ求めよ。

答え：

$$\begin{pmatrix} [3][4][1][0] \\ [0][3][4][1] \end{pmatrix}$$

(g) パリティ検査多項式 $h(X)$ を求めよ。

答え：

$$\begin{aligned} h(X) &= (X^4 - 1)/g(X) \\ &= [3][1][1] \end{aligned}$$

(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。

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

答え：

$$\begin{aligned} c(X) &= [2][1][4][0] \\ h(X) &= [3][1][1] \\ X^n - 1 &= [4][0][0][0][1] \\ c(X)h(X) &= [1][0][0][0][4] \\ c(X)h(X)/(X^n - 1) &= \text{商 } [4] \text{ 剰余 } [0] \end{aligned}$$

$c(X)h(X)$ と商が計算できていたら正解。

(i) C のパリティ検査行列を一つ求めよ。

答え：

$$\begin{pmatrix} [1][1][3][0] \\ [0][1][1][3] \end{pmatrix}$$

(j) C の双対符号 $C^{\perp}$ の生成多項式を求めよ。

答え：

$$\begin{aligned} g^{\perp}(X) &= h_0^{-1}(h_k + h_{k-1}X + h_{k-2}X^2 \\ &\quad + \cdots + h_1X^{k-1} + h_0X^k) \\ &= [3]^{-1}([1] + [1]X + [3]X^2) \\ &= [2]([1] + [1]X + [3]X^2) \\ &= [2] + [2]X + [1]X^2 \end{aligned}$$

5.3 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。

答え：まず、C が線形符号であること、つまり $c(X), d(X) \in C$ に対して、$u(X), v(X) \in \mathbb{F}[X; k]$ が存在して、

$$\begin{aligned} c(X) &= u(X)g(X) \\ d(X) &= v(X)g(X) \end{aligned}$$

と書ける。$a, b \in \mathbb{F}$ に対して、

$$\begin{aligned} ac(X) + bd(X) &= au(X)g(X) + bv(X)g(X) \\ &(au(X) + bv(X))g(X) \\ &au(X) + bv(X) \in \mathbb{F}[X; k] \end{aligned}$$

となるので、$ac(X) + bd(X) \in C$ となる。

次に C が巡回性を満たすことを示す。右巡回シフトで閉じていること、言い換えると、$c(X) \in C$ に対して、$Xc(X) \bmod X^n - 1 \in C$ であることを示せば十分である。

$$\begin{aligned} & Xc(X) \\ & \equiv Xc(X) - c_{n-1}(X^n - 1) \quad (\mathrm{mod} X^n - 1) \\ & \equiv Xu(X)g(X) - c_{n-1}h(X)g(X) \quad (\mathrm{mod} X^n - 1) \\ & \equiv \big(Xu(X) - c_{n-1}h(X)\big)g(X) \quad (\mathrm{mod} X^n - 1) \end{aligned}$$

が成り立つ。ここで、$h(X)$ は C のパリティ検査多項式である。$Xu(X) - c_{n-1}h(X) \in \mathbb{F}[X; k]$ を示せば証明は完了する。$u(X) \in \mathbb{F}[X; k]$ であり、$h(X)$ は k 次のモニックな多項式なので、$Xu(X)$ の k 次の係数が c_{n-1} であることを示せば十分である。ここで、多項式 $f(X)$ の k 次の係数を

$$\mathrm{coef}(f(X); k)$$

と書くと、

$$\begin{aligned} & \mathrm{coef}(Xu(X); k) = u_{k-1} \\ & \mathrm{coef}(c_{n-1}h(X); k) = c_{n-1} = u_{k-1}g_{n-k} = u_{k-1} \end{aligned}$$

である。ここで、$h(X), g(X)$ はそれぞれ $k, n-k$ 次のモニック多項式であることを使った。こうして、

$$Xu(X) - c_{n-1}h(X) \in \mathbb{F}[X;k]$$

となる。これより、主張が導けた。

(別解)C が $\mathbb{F}[X]/\langle X^n-1\rangle$ のイデアルであることを示せば良い。$\mathbb{F}[X]/\langle X^n-1\rangle$ の $[g(X)]$ で生成されるイデアルを I と書く

$$\begin{aligned} I &= \{[f(X)][g(X)] : [f(X)] \in \mathbb{F}[X]/\langle X^n-1\rangle\} \\ &= \{[f(X)][g(X)] : f(X) \in \mathbb{F}[X]\} \end{aligned}$$

$$f(X)/h(X) = \text{商 } Q(X) \text{ 余り } R(X)$$

とする。$h(X)g(X) = X^n - 1$ であるから、以下が成り立つ。

$$\begin{aligned} I &= \{[f(X)][g(X)] - [Q(X)][h(X)][g(X)] \\ &\quad : f(X) \in \mathbb{F}[X]\} \\ &= \{[f(X) - Q(X)h(X)][g(X)] : f(X) \in \mathbb{F}[X]\} \\ &= \{[R(X)][g(X)] : f(X) \in \mathbb{F}[X]\} \\ &\overset{(a)}{=} \{[u(X)][g(X)] : u(X) \in \mathbb{F}[X;k]\} \\ &\overset{(b)}{=} \{u(X)g(X) \mid u(X) \in \mathbb{F}[X;k]\} \\ &= C \end{aligned}$$

(a) では $f(X) \mapsto [R(X)] \in \mathbb{F}[X;k]$ が全射であることを用いた。(b) では剰余類環 $\mathbb{F}[X]/\langle X^n - 1\rangle$ と多項式空間 $\mathbb{F}[X;n]$ を同一視した。

5.4 $\mathbb{F}$ 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。

答え： $g(X) \mid X^n - 1$ でなければならない。$X^3 - 1$ を素因数分解すると $X^3 - 1 = (1 + X)(1 + X + X^2)$ である。生成多項式を $g(X) = 1, g(X) = X^n - 1$ と選ぶと、それぞれ自明な巡回符号 $\mathbb{F}^n, \{0\}$ を生成する。答えは、$g(X) := 1 + X$ によって生成される $\{000, 110, 011, 101\}$ と、$g(X) := 1 + X + X^2$ によって生成される $\{000, 111\}$ である。

(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。

答え：$X^4 - 1$ を素因数分解すると $X^4 - 1 = (1 + X)^4$ である。自明なものを除くと、

i. $g(X) := 1 + X$ によって生成される長さ 4 の単一パリティ検査符号、

ii. $g(X) := (1 + X)^2 = 1 + X^2$ によって生成される $\{0000, 1010, 0101, 1111\}$

iii. $g(X) := (1+X)^3 = 1+X+X^2+X^3$ によって生成される長さ 4 の繰り返し符号 $\{0000, 1111\}$ である。

(c) $\mathbb{F}_2$ 上の符号長 $n = 5$ の巡回符号で非自明なものをすべて挙げよ。

答え：$X^5 - 1$ を素因数分解すると

$$X^5 - 1 = (1+X)(1+X+X^2+X^3+X^4)$$

である。自明なものを除くと、$g(X) := 1+X$ によって生成される長さ 5 の単一パリティ検査符号、$g(X) := 1+X+X^2+X^3+X^4$ によって生成される長さ 5 の繰り返し符号 $\{00000, 11111\}$ である。

5.5 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。

答え：https://youtu.be/YTvYIU1vdWo

5.6 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。

答え：

$$\begin{aligned}
\mathrm{ord}([0]) &= \text{定義されていない} \\
\mathrm{ord}([1]) &= 1 \\
\mathrm{ord}([2]) &= 3 \\
\mathrm{ord}([3]) &= 6 \\
\mathrm{ord}([4]) &= 3 \\
\mathrm{ord}([5]) &= 6 \\
\mathrm{ord}([6]) &= 2
\end{aligned}$$

(b) $\mathbb{F}_7$ の原始元をすべて挙げよ。

答え： [3],[5]

(c) $[3]^{999}$ を求めよ。

答え： [3] は原始元なので、位数は 6 であるから、$[3]^{999} = [3]^{999 \bmod 6} = [3]^3 = [27] = [6]$

5.7 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 $\mathbb{F}_8 := \left(\mathbb{F}_2[X]/\langle p(X)\rangle, \{+, \times\}\right)$ 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。

答え：

$$\begin{aligned}
\mathrm{ord}([000]) &= \text{定義されていない} \\
\mathrm{ord}([100]) &= 1 \\
\mathrm{ord}([010]) &= 7 \\
\mathrm{ord}([110]) &= 7 \\
\mathrm{ord}([001]) &= 7 \\
\mathrm{ord}([101]) &= 7 \\
\mathrm{ord}([011]) &= 7 \\
\mathrm{ord}([111]) &= 7
\end{aligned}$$

(b) $\mathbb{F}_8$ の原始元をすべて挙げよ。

答え：$[010], [110], [001], [101], [011], [111]$

(c) $[111]^{999}$ を求めよ。

答え： $[111]$ は原始元なので、位数は 7 であるから、

$$[111]^{999} = [111]^{999 \bmod 7} = [111]^5$$

であり、$[111]$ のべき乗を求めると、

$$[111] \overset{\times[111]}{\to} [110] \overset{\times[111]}{\to} [010] \overset{\times[111]}{\to} [101] \overset{\times[111]}{\to} [011]$$

となる。よって、

$$[111]^{999} = [111]^5 = [011]$$

が分かる。

5.8 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。

答え： 位数が有限でないと仮定する。すると、非ゼロ元列

$$\beta, \beta^2, \beta^3, \ldots \in \mathbb{F}_q$$

には、いつまで乗じても 1 は現れないことになる。有限体 $\mathbb{F}_q$ の非零元の数は $q-1$ 個なので、この最初の q 個 $\beta^1, \beta^2, \ldots, \beta^q$ の中に等しい 2 元 $\beta^{i_1} = \beta^{i_2}$ with $0 < i_1 < i_2 \leq q$ が存在するはずである。すると、

$$\beta^{i_2 - i_1} = 1 \text{ with } 0 < i_2 - i_1 < q$$

となり、1 が現れないことに矛盾する。

5.9 $[n, k]$ 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。

答え：$g_0 = 0$ と仮定する。$g(X)$ を左巡回シフトした $g(X)/X$ も符号語となるが、この符号語は $g(X)$ より低く、$g(X)$ が次数の最小の符号語であることに矛盾する。

5.10 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。

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 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。

答え：

$$\begin{aligned}
\alpha^0 &= (100) \\
\alpha^1 &= (010) \\
\alpha^2 &= (001) \\
\alpha^3 &= (110) \\
\alpha^4 &= (011) \\
\alpha^5 &= (111) \\
\alpha^6 &= (101)
\end{aligned}$$

(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。

答え：

$\times$	α^0	α^1	α^2	α^3	α^4	α^5	α^6
α^0	α^0	α^1	α^2	α^3	α^4	α^5	α^6
α^1	α^1	α^2	α^3	α^4	α^5	α^6	α^0
α^2	α^2	α^3	α^4	α^5	α^6	α^0	α^1
α^3	α^3	α^4	α^5	α^6	α^0	α^1	α^2
α^4	α^4	α^5	α^6	α^0	α^1	α^2	α^3
α^5	α^5	α^6	α^0	α^1	α^2	α^3	α^4
α^6	α^6	α^7	α^1	α^2	α^3	α^4	α^5

(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。

答え：

	[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]

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

答え：

$$\alpha^{50} = \alpha^{50 \bmod 7} = \alpha^1$$
$$\alpha^{100} = \alpha^{100 \bmod 7} = \alpha^2$$
$$\alpha^{50} + \alpha^{100} = \alpha + \alpha^2$$
$$= (010) + (001) = (011) = \alpha^4$$

6.2 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。

答え：

α^i	$m_i(X)$
α^0	$1 + X$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	$1 + X^3 + X^4$
$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$	$1 + X + X^2 + X^3 + X^4$
α^5, α^{10}	$1 + X + X^2$
$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$	$1 + X + X^4$

(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。

答え：

$$
\begin{aligned}
& g(X) \\
& \stackrel{\text{def}}{=} \operatorname{lcm}(m_1(X), m_2(X), \ldots, m_{2t}(X)) \\
& = \operatorname{lcm}(m_1(X), m_2(X), \ldots, m_4(X)) \\
& = \operatorname{lcm}(m_1(X), m_3(X)) \\
& = (1 + X^3 + X^4)(1 + X + X^2 + X^3 + X^4)
\end{aligned}
$$

(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。

答え：

$$
\begin{aligned}
& g(X) \\
& \stackrel{\text{def}}{=} \operatorname{lcm}(m_1(X), m_2(X), \ldots, m_{2t}(X)) \\
& = \operatorname{lcm}(m_1(X), m_2(X), \ldots, m_6(X)) \\
& = \operatorname{lcm}(m_1(X), m_3(X), m_5(X)) \\
& = (1 + X^3 + X^4)(1 + X + X^2 + X^3 + X^4) \\
& \quad \times (1 + X + X^2)
\end{aligned}
$$

6.3 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。

答え： $m(X) \in \mathbb{F}_p[X]$ を α の $\mathbb{F}_p$ 上の最小多項式とする。

$$f(X)/m(X) =: \text{商 } q(X) + \text{剰余 } r(X)$$

と書く。$\deg r(X) < \deg m(X)$ である。

$$f(X) = q(X)m(X) + r(X)$$

に $X := \alpha$ を代入して、

$$0 = r(\alpha)$$

となり、$r(X)$ は α を根に持つ。$r(X) = 0$ である場合、$f(X) = q(X)m(X) + r(X)$ すなわち、$\deg f(X) \geq m(X)$ となる。$q(X) = 1$ でないと仮定すると、$f(X)$ が既約であることに矛盾する。したがって、$f(X) = m(X)$ である。$r(X) \neq 0$ な場合、$r(X)$ を適当に $\mathbb{F}_p$ の非零元倍すると α を根に持つモニック多項式にすることができる。これは、$m(X)$ が最小多項式であることに矛盾する。

6.4 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。

答え：$(q-1)/n =$ 商 Q 余り R、言い換えると

$$q - 1 = Qn + R, 0 \leq R < n$$

とする。

$$1 = \alpha^{q-1} = \alpha^{Qn} \times \alpha^R = \alpha^R$$

となる。割り切れない、即ち $R \neq 0$ と仮定すると、位数 n の最小性に矛盾する。

(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。

答え：$f(X)$ の任意の根 β は、$\beta = \alpha^{p^i}$ with $0 \leq i < m$ の形をしている。

$$\mathrm{ord}(\beta) = n \tag{6.1}$$

であることを示せば十分である。$\mathrm{ord}(\alpha) = n$ より、

$$\begin{aligned} \mathrm{ord}(\beta) &= \mathrm{ord}(\alpha^{p^i}) \\ &= \mathrm{ord}(\alpha)/\gcd(\mathrm{ord}(\alpha), p^i) \\ &= n/\gcd(n, p^i) \end{aligned}$$

と計算できる。$n \mid p^m - 1$ である。

$$(p^m - 1)/p = \text{商 } p^{m-1}\text{余り } p - 1$$

となり割り切れないので、$\gcd(n, p^i) = 1$ となり、(4b) が示された。

6.5 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。

答え：$\mathbb{F}_q$ の原始元の一つを α とする。$\mathbb{F}_q$ に含まれる原始元の数 $A(q)$ は $\mathrm{ord}(\alpha^i) = q-1$ となる $i = 1, \ldots, q-1$ の数である。

$$\begin{aligned}\mathrm{ord}(\alpha^i) &= \mathrm{ord}(\alpha)/\gcd(\mathrm{ord}(\alpha), i) \\ &= (q-1)/\gcd(q-1, i)\end{aligned}$$

が成り立つから、$A(q)$ は $\gcd(\mathrm{ord}(\alpha) = q-1, i) = 1$ となる i の数と等しい。

(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。

答え： $A(q=64)$、$\gcd(63,i)=1$ となる i の数つまり $\varphi(63)$ である。

$$63 = 3^2 \times 7$$

となるから、

$$A(64) = \varphi(63) = 63(1-1/3)(1-1/7) = 36$$

である。

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. 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. $1+1$

答え：0

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

答え：$X+X^3$

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

答え：$1+X^2$

iv. $1+X^2+X^6$ を $1+X$ で割った商と剰余。

答え：

$$\begin{aligned}&1+X^2+X^6\\&=(X+X^5)\times(1+X)+1\end{aligned}$$

なので、

$$\begin{aligned}&(1+X^2+X^6)/(1+X)\\&=\text{商 } X+X^5\text{剰余 } 1\end{aligned}$$

(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. $[010]\times[010]$

答え：$[001]$

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

答え：$[011]$

C. $[011]/[010]$

答え：$[110]$

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。

答え： $\alpha_1 = [100], \alpha_2 = [011]$

(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。

答え：p は素数なので、最大公約数

$$\gcd(a, p) = 1$$

である。したがって、$y, z \in \mathbb{Z}$ が存在して、

$$ay + pz = 1$$

となる。両辺 $\mathrm{mod} p$ すると

$$ay \bmod p = 1 \bmod p$$

となるから、

$$[ay] = [a][y] = [1]$$

となり、この $[y] \in \mathbb{F}_p$ が $[a]$ の逆元となることを表す。

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。

答え：符号長 5、次元 3、符号化率 3/5、最小距離 3

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。

答え：$[4][0][2][3][3]$

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。

答え：

```
G=
[1][1][1][1][1]
[0][1][2][3][4]
[0][1][4][2][2]
f=
[1][4][0]
c=
[1][5][2][6][3]
e=
[6][0][0][0][0]
r=
[0][5][2][6][3]
A=
[1][0][0][0][0][0]
[1][1][1][1][5][5]
[1][2][4][1][2][4]
[1][3][2][6][6][4]
```

```
[1][4][2][1][3][5]
前進消去終了 rank=5
後退代入終了 rank=5
q=
[0][6][3][0][0][1]
q0=
[0][6][3]
q1=
[0][1]
-q0/q1=
商
[1][4]
剰余
[0]
```

(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。

答え： C の非ゼロ符号語は、

$$\vec{x}(f) = \big(f(\alpha_1), \ldots, f(\alpha_n)\big) \neq (0, \ldots, 0)$$
$$\text{with } f(X)(\neq 0) \in \mathbb{F}_q[X; k]$$

と書ける。

- 次数 k 未満の非ゼロ多項式 $f(X)$ の根の個数は k 未満であることと，
- $\alpha_1, \ldots, \alpha_n$ は全て異なることから，

$f(\alpha_i) = 0$ となる i $(1 \leq i \leq n)$ の個数は k 未満であることが分かる．言い換えると，$f(\alpha_i) \neq 0$ となる i $(1 \leq i \leq n)$ の個数は $n-k+1$ 以上である．こうして，$w_{\min}(\vec{x}) \geq n-k+1$ が

示せた。シングルトン限界より逆の不等式も成り立つので、$[n,k]$RS 符号の最小距離は $n-k+1$ となる。

(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。

答え：講義資料を見てください。

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.

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

答え： 巡回符号である。$k=3,n=4$

ii.

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

答え：巡回符号ではない。なぜなら、巡回性は満たされるが、

$$(1000) + (0100) = (1100) \notin C$$

であるからである。

(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。

答え： 0000,0101,1010,1111

(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。

答え：X^4-1 を素因数分解すると $X^4-1 = (1+X)^4$ である。

$$\begin{aligned} g(X) &:= 1 + X \\ g(X) &:= (1 + X)^2 = 1 + X^2 \\ g(X) &:= (1 + X)^3 = 1 + X + X^2 + X^3 \end{aligned}$$

(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

答え：$k = 2$

ii. 生成多項式 $g(X) \in \mathbb{F}_5[X]$

答え：$g(X) = ([2][3][1][0]) = [2] + [3]X + [1]X^2$

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

答え：$(X^n - 1)/g(X) = ([2][2][1][0]) = [2] + [2]X + [1]X^2$

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

答え：

$$\begin{aligned} g^\perp(X) &= h_0^{-1} X^k h(1/X) \\ &= h_0^{-1}(h_k + h_{k-1}X + h_{k-2}X^2 \\ &\quad + \cdots + h_1 X^{k-1} + h_0 X^k) \\ &= [2]^{-1}([1] + [2]X + [2]X^2) \\ &= [3]([1] + [2]X + [2]X^2) \\ &= [3] + [1]X + [1]X^2 \end{aligned}$$

```
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。

答え：演習問題 5.3 を見てください。

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 $0 \le i \le 6$ 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。

答え：

$$\begin{aligned}
\alpha^0 &= (100)\\
\alpha^1 &= (010)\\
\alpha^2 &= (001)\\
\alpha^3 &= (110)\\
\alpha^4 &= (011)\\
\alpha^5 &= (111)\\
\alpha^6 &= (101)
\end{aligned}$$

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

答え：

$$\alpha^{50} = \alpha^{50 \bmod 7} = \alpha^1$$
$$\alpha^{100} = \alpha^{100 \bmod 7} = \alpha^2$$
$$\alpha^{50} + \alpha^{100} = \alpha + \alpha^2$$
$$= (010) + (001) = (011) = \alpha^4$$

(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。

答え：講義資料 39.9 を見てください。

(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。

答え：講義資料 39.9 を見てください。

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	$1+X$
$\alpha^1, \boxed{\alpha^2}, \boxed{\alpha^4}, \boxed{\alpha^8}$	$\boxed{1+X+X^4}$
$\alpha^3, \boxed{\alpha^6}, \boxed{\alpha^{12}}, \boxed{\alpha^9}$	$1+X+X^2+X^3+X^4$
$\alpha^5, \boxed{\alpha^{10}}$	$\boxed{1+X+X^2}$
$\alpha^7, \boxed{\alpha^{14}}, \boxed{\alpha^{13}}, \boxed{\alpha^{11}}$	$\boxed{1+X^3+X^4}$

(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。

答え：$g(X)$ が $\alpha, \alpha^2, \alpha^3, \alpha^4$ を根に含むようにすればよい。

$$\begin{aligned} g(X) &= \mathrm{lcm}(m_1(X), m_2(X), m_3(X), m_4(X)) \\ &= \mathrm{lcm}(1+X+X^4, 1+X+X^4, \\ &\quad 1+X+X^2+X^3+X^4, 1+X+X^4) \\ &= (1+X+X^2+X^3+X^4)(1+X+X^4) \end{aligned}$$

(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。

答え：

$$\begin{aligned} g(X) =& \mathrm{lcm}(m_1(X), m_2(X), \ldots, m_6(X)) \\ =& (1+X+X^2+X^3+X^4)(1+X+X^4) \\ & (1+X+X^2) \end{aligned}$$

(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。

答え：講義資料 40.7 を見てください。

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。

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

答え：符号長は 12，最小ハミング距離は 6，符号化率は $\log_2(4)/12 = 1/6$.

(b) 次の長さ 12 の 4 つの行ベクトルからなる符号

$$C = \{\\ 111011111110\\ 010100001010\\ 111001111000\\ 110001110111\}$$

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。

答え：

$$\hat{c}_1^{(\mathrm{BD})}(\vec{r}) = \mathrm{error}$$
$$\hat{c}^{(\mathrm{MD})}(\vec{r}) = 110001110111$$

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。

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

答え：11 と 11 の和 00 が符号 C_1 に含まれないから C_1 は線形符号ではない。

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

答え： 線形符号であり、次元は 3、基底は $\{10110, 01101, 11111\}$ となる。基底の選び方は任意性があるので、答えは一意ではない。生成行列は基底の要素を行ベクトルとして積み上げたもの。最小距離 1，符号化率 3/5，

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

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

答え：いくつかの基本行変形[6]により、

$$\begin{pmatrix} 1000|1 \\ 1011|0 \\ 1111|1 \\ 0001|0 \end{pmatrix} \overset{\text{前進消去}}{\longrightarrow} \begin{pmatrix} 1000|1 \\ 0111|0 \\ 0011|1 \\ 0001|0 \end{pmatrix} \overset{\text{後退代入}}{\longrightarrow} \begin{pmatrix} 1000|1 \\ 0100|1 \\ 0010|1 \\ 0001|0 \end{pmatrix}.$$

となる。よって、$(x_1, \ldots, x_4) = (1110)$ である。

(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。

[6] https://ja.wikipedia.org/wiki/行列の基本変形

答え：

$$C^{\perp} = \{000, 011, 101, 110\}$$
$$C = \{000, 111\}$$

(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。

答え： $B(X,Y)$ の $B_w \neq 0$ となる $w > 0$ の最小値が $C^{\perp}$ の最小距離 $d^{\perp}$ である。MacWilliams の恒等式から双対符号の重み分布多項式 $A(X,Y)$ を求めることができる。$A(X,Y)$ の $A_w \neq 0$ となる $w > 0$ の最小値が C の最小距離 d である。

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。

答え：

$$G = \begin{pmatrix} 1000\ 110 \\ 0100\ 011 \\ 0010\ 101 \\ 0001\ 111 \end{pmatrix}$$

(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。

答え：(1010011)

(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。

答え：(1111111).

(d) 符号語数、次元、符号化率を求めよ。

答え：16,4,4/7

(e) 最小距離が 3 以上であることを証明せよ。

答え：H の異なる 2 列は異なっていて線形独立だから、最小距離は 3 以上となる。

(f) 最小距離が 3 以下であることを証明せよ。

答え：H の第 1,2,3 列は線形従属なので、最小距離は 3 以下である。

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

答え：群である。$e = 0, -x$

ii. 非零実数の集合とその乗算

答え：群である。$e = 1, x^{-1}$

iii. 2×2 実行列の集合と行列の乗算

答え：群でない。単位元は単位行列 I_2 となるが、非正則行列 X には乗じて $XY = YX = I_n$ となる行列は存在しない。

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。

答え：

```
99221=1*97343+1878
97343=51*1878+1565
1878=1*1565+313
1565=5*313+0
gcd=313=52*99221+-53*97343
x=52
y=-53
```

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. $1 + 1$

答え：0

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

答え：$X + X^3$

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

答え：$1+X^2$

iv. $1+X^2+X^6$ を $1+X$ で割った商と剰余。

答え：

$$\begin{aligned}&1+X^2+X^6\\&=(X^2+X^3+X^4+X^5)\times(1+X)+1\end{aligned}$$

なので、

$$\begin{aligned}&(1+X^2+X^6)/(1+X)\\&=\text{商}\ X^2+X^3+X^4+X^5\text{剰余}\ 1\end{aligned}$$

(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. $[010]\times[010]$

答え：$[001]$

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

答え：$[011]$

C. $[011]/[010]$

答え：$[110]$

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。
答え： $\alpha_1 = [100], \alpha_2 = [011]$

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。
答え：符号長 5、次元 3、符号化率 3/5、最小距離 3

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。

答え：[4][0][2][3][3]

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。

答え：

```
G=
[1][1][1][1][1]
[0][1][2][3][4]
[0][1][4][2][2]
f=
[1][4][0]
c=
[1][5][2][6][3]
e=
[6][0][0][0][0]
r=
[0][5][2][6][3]
A=
[1][0][0][0][0][0]
[1][1][1][1][5][5]
[1][2][4][1][2][4]
[1][3][2][6][6][4]
[1][4][2][1][3][5]
前進消去終了 rank=5
後退代入終了 rank=5
q=
[0][6][3][0][0][1]
q0=
[0][6][3]
q1=
[0][1]
```

```
-q0/q1=
商
[1][4]
剰余
[0]
```

(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。

答え： $\alpha_1, \ldots, \alpha_n$ を相異なる n 個の実数とする。情報多項式 $u(X) = \sum_{i=0}^{k-1} u_i X^i$ に対して、

$$(c_1, \ldots, c_n) = \big(u(\alpha_1), u(\alpha_2), \ldots, u(\alpha_n)\big) \in \mathbb{R}^n$$

に符号化する。

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。

答え：

$$\begin{aligned}\alpha^0 &= (100)\\ \alpha^1 &= (010)\\ \alpha^2 &= (001)\\ \alpha^3 &= (110)\\ \alpha^4 &= (011)\\ \alpha^5 &= (111)\\ \alpha^6 &= (101)\end{aligned}$$

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

答え：

$$\begin{aligned}&\alpha^{50} = \alpha^{50 \bmod 7} = \alpha^1\\ &\alpha^{100} = \alpha^{100 \bmod 7} = \alpha^2\\ &\alpha^{50} + \alpha^{100} = \alpha + \alpha^2\\ &= (010) + (001) = (011) = \alpha^4\end{aligned}$$

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	$1+X$
$\alpha^1, \boxed{\alpha^2}, \boxed{\alpha^4}, \boxed{\alpha^8}$	$\boxed{1+X^3+X^4}$
$\alpha^3, \boxed{\alpha^6}, \boxed{\alpha^{12}}, \boxed{\alpha^9}$	$1+X+X^2+X^3+X^4$
$\alpha^5, \boxed{\alpha^{10}}$	$\boxed{1+X+X^2}$
$\alpha^7, \boxed{\alpha^{14}}, \boxed{\alpha^{13}}, \boxed{\alpha^{11}}$	$\boxed{1+X^1+X^4}$

(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。

答え：$g(X)$ が $\alpha, \alpha^2, \alpha^3, \alpha^4$ を根に含むようにすればよい。

$$\begin{aligned} g(X) &= \mathrm{lcm}(m_1(X), m_2(X), m_3(X), m_4(X)) \\ &= (1+X+X^2+X^3+X^4)(1+X^3+X^4) \end{aligned}$$

(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。

答え：

$$\begin{aligned} g(X) =& \mathrm{lcm}(m_1(X), m_2(X), \ldots, m_6(X)) \\ =& (1+X+X^2+X^3+X^4)(1+X^3+X^4) \\ & (1+X+X^2) \end{aligned}$$

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. 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. $1+1$

答え：0

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

答え：$X+X^3$

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

答え：$1+X^6$

iv. $1+X^2+X^6$ を $1+X$ で割った商と剰余。

答え：

$$\begin{aligned}&1+X^2+X^6\\&=(X^2+X^3+X^4+X^5)\times(1+X)+1\end{aligned}$$

なので、

$$\begin{aligned}&(1+X^2+X^6)/(1+X)\\&=\text{商 } X^2+X^3+X^4+X^5\text{剰余 } 1\end{aligned}$$

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

答え：既約です。可約だと仮定すると、1 次の因子 $X-x$ with $x\in\mathbb{R}$ をもち、x は X^2+1 の根となるはずである。しかし、$x\in R$ に対して、$X:=x$ を代入しても 0 にならない。

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

答え：可約です。$X^2+1=(X+\sqrt{-1})(X-\sqrt{-1})$

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

答え：可約です。$X^2+1=(X+1)^2$

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

答え：既約です。この多項式は 3 次なので、可約だとしてたら、3 つの 1 次の因子または、2 次と 1 次の因子に分解できるはずである。どちらにしても根 $x \in \mathbb{F}_2$ を有するはずである。しかし、$0,1 \in \mathbb{F}_2$ のどちらを代入しても 0 とはならない。

(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. $[010] \times [010]$

答え：$[001]$

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

答え：$[101]$

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

答え：$[011]$

(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。

答え：$p(X)$ は既約なので、最大公約数

$$\gcd(a(X), p(X)) = 1$$

である。したがって、$y(X), z(X) \in \mathbb{F}[X]$ が存在して、

$$a(X)y(X) + p(X)z(X) = 1$$

となる。両辺 $\mathrm{mod} p(X)$ すると

$$a(X)y(X) \bmod p(X) = 1 \bmod p(X)$$

となるから、

$$[a(X)y(X)] = [a(X)][y(X)] = [1]$$

となり、この $[y(X)] \in \mathbb{F}[X]/\langle p(X)\rangle$ が $[a(X)]$ の逆元となる。

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。

答え：符号長 5、次元 3、符号化率 3/5、最小距離 3

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。

答え：[3][2][1][0][4]

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。

答え：

```
G=
[1][1][1][1][1]
[0][1][2][3][4]
[0][1][4][4][1]
f=
[3][1][2]
c=
[3][1][3][4][4]
e=
[0][2][0][0][0]
r=
[3][3][3][4][4]
A=
[1][0][0][0][3][0]
[1][1][1][1][3][3]
[1][2][4][3][3][1]
[1][3][4][2][4][2]
[1][4][1][4][4][1]
A=
[1][0][0][0][3][0]
[0][1][1][1][0][3]
[0][0][1][3][0][0]
[0][0][0][1][1][3]
[0][0][0][0][1][1]
前進消去終了 rank=5
A=
[1][0][0][0][0][2]
[0][1][0][0][0][2]
[0][0][1][0][0][4]
[0][0][0][1][0][2]
[0][0][0][0][1][1]
後退代入終了 rank=5
q=
[3][3][1][3][4][1]
q0=
[3][3][1][3]
q1=
[4][1]
-q0/q1=
商
```

[3][1][2]
剰余
[0]

(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。

答え： C の非ゼロ符号語は、

$$\vec{x}(f) = \big(f(\alpha_1),\ldots,f(\alpha_n)\big) \neq (0,\ldots,0)$$
$$\text{with } f(X)(\neq 0) \in \mathbb{F}_q[X;k]$$

と書ける。

- 次数 k 未満の非ゼロ多項式 $f(X)$ の根の個数は k 未満であることと，
- $\alpha_1,\ldots,\alpha_n$ は全て異なることから，

$f(\alpha_i)=0$ となる i $(1\le i\le n)$ の個数は k 未満であることが分かる．言い換えると，$f(\alpha_i)\neq 0$ となる i $(1\le i\le n)$ の個数は $n-k+1$ 以上である．こうして，$w_{\min}(\vec{x})\ge n-k+1$ が示せた。シングルトン限界より逆の不等式も成り立つので、$[n,k]$RS 符号の最小距離は $n-k+1$ となる。

(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。$t\le\lfloor\frac{n-k}{2}\rfloor$ 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。

答え： $\alpha_1, \ldots, \alpha_n$ を相異なる n 個の実数とする。情報多項式 $u(X) = \sum_{i=0}^{k-1} u_i X^i$ に対して、

$$(c_1, \ldots, c_n) = \big(u(\alpha_1), u(\alpha_2), \ldots, u(\alpha_n)\big) \in \mathbb{R}^n$$

に符号化する。

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.

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

答え： 巡回符号である。$k = 3, n = 4$

ii.

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

答え：巡回符号ではない。なぜなら、巡回性は満たされるが、

$$(1000) + (0100) = (1100) \notin C$$

であるからである。

(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。

答え： 0000,0101,1010,1111

(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。

答え：X^4-1 を素因数分解すると $X^4-1 = (1+X)^4$ である。

$$g(X) := 1 + X$$
$$g(X) := (1 + X)^2 = 1 + X^2$$
$$g(X) := (1 + X)^3 = 1 + X + X^2 + X^3$$

(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

答え：$k = 2$

ii. 生成多項式 $g(X) \in \mathbb{F}_5[X]$

答え：

$$g(X) = \underline{([2][3][1][0]) = [2] + [3]X + [1]X^2}$$

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

答え：

$$
\begin{aligned}
&(X^n - 1)/g(X) \\
&= \underline{([2][2][1][0]) = [2] + [2]X + [1]X^2}
\end{aligned}
$$

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

答え：

$$
\begin{aligned}
g^\perp(X) &= h_0^{-1} X^k h(1/X) \\
&= h_0^{-1}(h_k + h_{k-1}X + h_{k-2}X^2 \\
&\quad + \cdots + h_1 X^{k-1} + h_0 X^k) \\
&= [2]^{-1}([1] + [2]X + [2]X^2) \\
&= [3]([1] + [2]X + [2]X^2) \\
&= \underline{[3] + [1]X + [1]X^2}
\end{aligned}
$$

```
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。

答え：演習問題 5.3 を見てください。

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。

答え：

$$\begin{aligned}
\alpha^0 &= (100)\\
\alpha^1 &= (010)\\
\alpha^2 &= (001)\\
\alpha^3 &= (110)\\
\alpha^4 &= (011)\\
\alpha^5 &= (111)\\
\alpha^6 &= (101)
\end{aligned}$$

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

答え：

$$\alpha^{50} = \alpha^{50 \bmod 7} = \alpha^1$$
$$\alpha^{100} = \alpha^{100 \bmod 7} = \alpha^2$$
$$\alpha^{50} + \alpha^{100} = \alpha + \alpha^2$$
$$= (010) + (001) = (011) = \alpha^4$$

(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。

答え：講義資料 39.9 を見てください。

(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。

答え：講義資料 39.9 を見てください。

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	$1+X$
$\alpha^1, \boxed{\alpha^2}, \boxed{\alpha^4}, \boxed{\alpha^8}$	$\boxed{1+X^3+X^4}$
$\alpha^3, \boxed{\alpha^6}, \boxed{\alpha^{12}}, \boxed{\alpha^9}$	$1+X+X^2+X^3+X^4$
$\alpha^5, \boxed{\alpha^{10}}$	$\boxed{1+X+X^2}$
$\alpha^7, \boxed{\alpha^{14}}, \boxed{\alpha^{13}}, \boxed{\alpha^{11}}$	$\boxed{1+X^1+X^4}$

(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。

答え：$g(X)$ が $\alpha, \alpha^2, \alpha^3, \alpha^4$ を根に含むようにすればよい。

$$\begin{aligned} g(X) &= \mathrm{lcm}(m_1(X), m_2(X), m_3(X), m_4(X)) \\ &= (1+X+X^2+X^3+X^4)(1+X^3+X^4) \end{aligned}$$

(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。

答え：

$$\begin{aligned} g(X) =& \mathrm{lcm}(m_1(X), m_2(X), \ldots, m_6(X)) \\ =& (1+X+X^2+X^3+X^4)(1+X^3+X^4) \\ & (1+X+X^2) \end{aligned}$$

(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。

答え：講義資料 39.9 を見てください。

7　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. 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. $1+1$

答え：0

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

答え：$X+X^3$

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

答え：$1+X^6$

iv. $1+X^2+X^6$ を $1+X$ で割った商と剰余。

答え：

$$\begin{aligned}&1+X^2+X^6\\&=(X^2+X^3+X^4+X^5)\times(1+X)+1\end{aligned}$$

なので、

$$\begin{aligned}&(1+X^2+X^6)/(1+X)\\&=\text{商 } X^2+X^3+X^4+X^5\text{剰余 } 1\end{aligned}$$

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

答え：既約です。可約だと仮定すると、1 次の因子 $X-x$ with $x\in\mathbb{R}$ をもち、x は X^2+1 の根となるはずである。しかし、$x\in R$ に対して、$X:=x$ を代入しても 0 にならない。

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

答え：可約です。$X^2+1=(X+\sqrt{-1})(X-\sqrt{-1})$

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

答え：可約です。$X^2+1=(X+1)^2$

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

答え：既約です。この多項式は 3 次なので、可約だとしてたら、3 つの 1 次の因子または、2 次と 1 次の因子に分解できるはずである。どちらにしても根 $x \in \mathbb{F}_2$ を有するはずである。しかし、$0,1 \in \mathbb{F}_2$ のどちらを代入しても 0 とはならない。

(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. $[010] \times [010]$

答え：$[001]$

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

答え：$[101]$

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

答え：$[011]$

(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。

答え：$p(X)$ は既約なので、最大公約数

$$\gcd(a(X), p(X)) = 1$$

である。したがって、$y(X), z(X) \in \mathbb{F}[X]$ が存在して、

$$a(X)y(X) + p(X)z(X) = 1$$

となる。両辺 $\mathrm{mod} p(X)$ すると

$$a(X)y(X) \bmod p(X) = 1 \bmod p(X)$$

となるから、

$$[a(X)y(X)] = [a(X)][y(X)] = [1]$$

となり、この $[y(X)] \in \mathbb{F}[X]/\langle p(X)\rangle$ が $[a(X)]$ の逆元となる。

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。

答え：符号長 5、次元 3、符号化率 3/5、最小距離 3

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。

答え：[4][0][2][3][3]

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。

答え：

```
G=
[1][1][1][1][1]
[0][1][2][3][4]
[0][1][4][2][2]
f=
[1][4][0]
c=
[1][5][2][6][3]
e=
[6][0][0][0][0]
r=
[0][5][2][6][3]
A=
[1][0][0][0][0][0]
[1][1][1][1][5][5]
[1][2][4][1][2][4]
[1][3][2][6][6][4]
[1][4][2][1][3][5]
前進消去終了 rank=5
後退代入終了 rank=5
q=
[0][6][3][0][0][1]
q0=
[0][6][3]
q1=
[0][1]
-q0/q1=
商
[1][4]
剰余
[0]
```

(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。

答え： $g(X) = (X-\alpha)(X-\alpha^2)\cdots(X-\alpha^{n-k})$

(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。

答え： C の非ゼロ符号語は、

$$\vec{x}(f) = \big(f(\alpha_1), \ldots, f(\alpha_n)\big) \neq (0, \ldots, 0)$$
$$\text{with } f(X)(\neq 0) \in \mathbb{F}_q[X; k]$$

と書ける。

- 次数 k 未満の非ゼロ多項式 $f(X)$ の根の個数は k 未満であることと，
- $\alpha_1, \ldots, \alpha_n$ は全て異なることから，

$f(\alpha_i) = 0$ となる i $(1 \leq i \leq n)$ の個数は k 未満であることが分かる．言い換えると，$f(\alpha_i) \neq 0$ となる i $(1 \leq i \leq n)$ の個数は $n-k+1$ 以上である．こうして，$w_{\min}(\vec{x}) \geq n-k+1$ が示せた。シングルトン限界より逆の不等式も成り立つので、$[n, k]$RS 符号の最小距離は $n-k+1$ となる。

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

答え： 巡回符号である。(1) $n = 4$,(2) $k = 3$, (3) $1 + X$,(4) $1 + X + X^2 + X^3$

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

答え： 巡回符号ではない。なぜなら、巡回性は満たされるが、

$$(1000) + (0100) = (1100) \notin C$$

であるからである。

(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 $\{\overbrace{0 \cdots 0}^{n}\}$ 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。

答え：$X^4 - 1$ を素因数分解すると $X^4 - 1 = (1 + X)^4$ である。

$$g(X) := 1 + X$$
$$g(X) := (1 + X)^2 = 1 + X^2$$
$$g(X) := (1 + X)^3 = 1 + X + X^2 + X^3$$

(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

答え：$k = 2$

ii. 生成多項式 $g(X) \in \mathbb{F}_5[X]$

答え：

$$g(X) = \underline{([2][3][1][0]) = [2] + [3]X + [1]X^2}$$

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

答え：

$$
\begin{aligned}
&(X^n - 1)/g(X) \\
&= \underline{([2][2][1][0]) = [2] + [2]X + [1]X^2}
\end{aligned}
$$

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

答え：

$$
\begin{aligned}
g^\perp(X) &= h_0^{-1} X^k h(1/X) \\
&= h_0^{-1}(h_k + h_{k-1}X + h_{k-2}X^2 \\
&\quad + \cdots + h_1 X^{k-1} + h_0 X^k) \\
&= [2]^{-1}([1] + [2]X + [2]X^2) \\
&= [3]([1] + [2]X + [2]X^2) \\
&= \underline{[3] + [1]X + [1]X^2}
\end{aligned}
$$

```
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 $g(X) = g_0 + g_1 X + \cdots + g_{n-k-1}X^{n-k-1} + g_{n-k}X^{n-k}$ 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。

答え： ここで $g(X)$ を巡廻シフトした $g(X),\ Xg(X),\ \ldots,\ X^{k-1}g(X)$ に対応する k 個の符号語を考えると

$$\begin{aligned} g(X) &\leftrightarrow (g_0, g_1, \ldots, g_{n-k-1}, g_{n-k}, 0, \cdots, 0) \\ Xg(X) &\leftrightarrow (0, g_0, g_1, \ldots, g_{n-k-1}, g_{n-k}, 0, \cdots, 0) \\ &\vdots \\ X^{k-2}g(X) &\leftrightarrow (0, \ldots, 0, g_0, g_1, \ldots, g_{n-k-1}, g_{n-k}, 0) \\ X^{k-1}g(X) &\leftrightarrow (0, \ldots, \ldots, 0, g_0, g_1, \ldots, g_{n-k-1}, g_{n-k}) \end{aligned}$$

となり、これらは一番右にある非ゼロ成分 $g_{n-k} = 1$ の位置がすべて異なるから線形独立である。または、$g_0 \neq 0$ であること（証明は演習で行う）からも分かる。またベクトルの数 k は C の次元 k に等しいからこれらのベクトルは基底を構成している。従ってこれらのベクトルを縦に並べた $\mathbb{F}_q$ 値 $k \times n$ 行列

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

が C の生成行列になる。

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。

答え：

$$\begin{aligned}
\alpha^0 &= (100) \\
\alpha^1 &= (010) \\
\alpha^2 &= (001) \\
\alpha^3 &= (110) \\
\alpha^4 &= (011) \\
\alpha^5 &= (111) \\
\alpha^6 &= (101)
\end{aligned}$$

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

答え：

$$\begin{aligned}
&\alpha^{50} = \alpha^{50 \bmod 7} = \alpha^1 \\
&\alpha^{100} = \alpha^{100 \bmod 7} = \alpha^2 \\
&\alpha^{50} + \alpha^{100} = \alpha + \alpha^2 \\
&= (010) + (001) = (011) = \alpha^4
\end{aligned}$$

(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。

答え：講義資料 39.9 を見てください。

(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。

答え： $\mathbb{F}_q$ の原始元の一つを α とする。$\mathbb{F}_q$ に含まれる原始元の数 $A(q)$ は $\mathrm{ord}(\alpha^i) = q-1$ となる $i = 1, \ldots, q-1$ の数である。

$$\begin{aligned} \mathrm{ord}(\alpha^i) &= \mathrm{ord}(\alpha)/\gcd(\mathrm{ord}(\alpha), i) \\ &= (q-1)/\gcd(q-1, i) \end{aligned}$$

が成り立つから、$A(q)$ は $\gcd(\mathrm{ord}(\alpha) = q-1, i) = 1$ となる i の数と等しい。

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	$1+X$
$\alpha^1, \boxed{\alpha^2}, \boxed{\alpha^4}, \boxed{\alpha^8}$	$\boxed{1+X^3+X^4}$
$\alpha^3, \boxed{\alpha^6}, \boxed{\alpha^{12}}, \boxed{\alpha^9}$	$1+X+X^2+X^3+X^4$
$\alpha^5, \boxed{\alpha^{10}}$	$\boxed{1+X+X^2}$
$\alpha^7, \boxed{\alpha^{14}}, \boxed{\alpha^{13}}, \boxed{\alpha^{11}}$	$\boxed{1+X^1+X^4}$

(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。

答え：

$$\alpha, \alpha^2, \lll, \alpha^{\hat{d}-1} \in \mathbb{F}^q$$

を根とする、$\mathbb{F}_p$ 上の次数が最小のモニック多項式を $g(X)$ と書く。

(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。

答え： $1+X+X^2+X^3+X^4$

(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。

答え：$g(X)$ が $\alpha, \alpha^2, \alpha^3, \alpha^4$ を根に含むようにすればよい。

$$\begin{aligned} g(X) &= \mathrm{lcm}(m_1(X), m_2(X), m_3(X), m_4(X)) \\ &= (1+X+X^2+X^3+X^4)(1+X^3+X^4) \end{aligned}$$

(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。

答え：

$$\begin{aligned} g(X) =& \mathrm{lcm}(m_1(X), m_2(X), \ldots, m_6(X)) \\ =& (1+X+X^2+X^3+X^4)(1+X^3+X^4) \\ & (1+X+X^2) \end{aligned}$$

(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。

答え：講義資料 40.7 を見てください。

8　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. 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. $(1+X+X^2)(1+X)$

答え：$1+X^3$

ii. $1+X+X^2$ を $1+X$ で割った商と剰余。

答え：X+1 あまり X

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

答え：可約です。$X^2+1=(X+1)^2$

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

答え：既約です。この多項式は 3 次なので、可約だとしてたら、3 つの 1 次の因子または、2 次と 1 次の因子に分解できるはずである。どちらにしても根 $x \in \mathbb{F}_2$ を有するはずである。しかし、$0,1 \in \mathbb{F}_2$ のどちらを代入しても 0 とはならない。

(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 $\mathbb{F}_8 := \left(\mathbb{F}_2[X]/\langle p(X)\rangle, \{+,\times\}\right)$ に関して以下の問に答えよ。

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

答え：$[101]$

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

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

答え：$\alpha_1 = [100], \alpha_2 = [011]$

(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。

答え：p は素数なので、最大公約数

$$\gcd(a, p) = 1$$

である。したがって、$y, z \in \mathbb{Z}$ が存在して、

$$ay + pz = 1$$

となる。両辺 $\mathrm{mod} p$ すると

$$ay \bmod p = 1 \bmod p$$

となるから、

$$[ay] = [a][y] = [1]$$

となり、この $[y] \in \mathbb{F}_p$ が $[a]$ の逆元となることを表す。

(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。

答え： $\left(X^2+X+1\right)$

$$\left(X^2+X+1\right)\left(X^3+X^2+1\right)=X^5+X+1$$
$$\left(X^2+X+1\right)\left(X^3+X+1\right)=X^5+X^4+1$$

$$(x+1)\left(x^5+x+1\right)+(x)\left(x^5+x^4+1\right)=x^2+x+1$$
$$s(X)=X+1, t(X)=x$$

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、

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

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、

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

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。

答え：符号長 5、次元 3、符号化率 3/5、最小距離 3

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。

答え：[3][2][1][0][4]

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。

答え：

```
G=
[1][1][1][1][1]
[0][1][2][3][4]
[0][1][4][4][1]
f=
[3][1][2]
c=
[3][1][3][4][4]
e=
[0][2][0][0][0]
r=
[3][3][3][4][4]
A=
[1][0][0][0][3][0]
[1][1][1][1][3][3]
[1][2][4][3][3][1]
[1][3][4][2][4][2]
```

```
[1][4][1][4][4][1]
A=
[1][0][0][0][3][0]
[0][1][1][1][0][3]
[0][0][1][3][0][0]
[0][0][0][1][1][3]
[0][0][0][0][1][1]
前進消去終了 rank=5
A=
[1][0][0][0][0][2]
[0][1][0][0][0][2]
[0][0][1][0][0][4]
[0][0][0][1][0][2]
[0][0][0][0][1][1]
後退代入終了 rank=5
q=
[3][3][1][3][4][1]
q0=
[3][3][1][3]
q1=
[4][1]
-q0/q1=
商
[3][1][2]
剰余
[0]
```

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

答え： $g(X) = (X - \alpha)(X - \alpha^2) \cdots (X - \alpha^{n-k=q-1-k})$

(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。

答え： C の非ゼロ符号語は、

$$\vec{x}(f) = \big(f(\alpha_1), \ldots, f(\alpha_n)\big) \neq (0, \ldots, 0)$$
$$\text{with } f(X)(\neq 0) \in \mathbb{F}_q[X; k]$$

と書ける。

- 次数 k 未満の非ゼロ多項式 $f(X)$ の根の個数は k 未満であることと，
- $\alpha_1, \ldots, \alpha_n$ は全て異なることから，

$f(\alpha_i) = 0$ となる i $(1 \leq i \leq n)$ の個数は k 未満であることが分かる．言い換えると，$f(\alpha_i) \neq 0$ となる i $(1 \leq i \leq n)$ の個数は $n-k+1$ 以上である．こうして，$w_{\min}(\vec{x}) \geq n-k+1$ が示せた。シングルトン限界より逆の不等式も成り立つので、$[n, k]$RS 符号の最小距離は $n - k + 1$ となる。

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

答え： 巡回符号である。(1) $n = 4$,(2) $k = 3$, (3) $1 + X$,(4) $1 + X + X^2 + X^3$

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

答え：巡回符号ではない。なぜなら、巡回性は満たされるが、

$$(1000) + (0100) = (1100) \notin C$$

であるからである。

(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。

答え：$X^4 - 1$ を素因数分解すると $X^4 - 1 = (1+X)^4$ である。

$$\begin{aligned} g(X) &:= 1 + X \\ g(X) &:= (1+X)^2 = 1 + X^2 \\ g(X) &:= (1+X)^3 = 1 + X + X^2 + X^3 \end{aligned}$$

(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

答え：$k = 2$

ii. 生成多項式 $g(X) \in \mathbb{F}_5[X]$

答え：

$$g(X) = \underline{([2][3][1][0]) = [2] + [3]X + [1]X^2}$$

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

答え：

$$
\begin{aligned}
&(X^n-1)/g(X)\\
&=\underline{([2][2][1][0])=[2]+[2]X+[1]X^2}
\end{aligned}
$$

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

答え：

$$
\begin{aligned}
g^\perp(X)&=h_0^{-1}X^kh(1/X)\\
&=h_0^{-1}(h_k+h_{k-1}X+h_{k-2}X^2\\
&\quad+\cdots+h_1X^{k-1}+h_0X^k)\\
&=[2]^{-1}([1]+[2]X+[2]X^2)\\
&=[3]([1]+[2]X+[2]X^2)\\
&=\underline{[3]+[1]X+[1]X^2}
\end{aligned}
$$

```
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。
答え：

$$\begin{aligned}
\alpha^0 &= (100) \\
\alpha^1 &= (010) \\
\alpha^2 &= (001) \\
\alpha^3 &= (110) \\
\alpha^4 &= (011) \\
\alpha^5 &= (111) \\
\alpha^6 &= (101)
\end{aligned}$$

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

答え：

$$\alpha^{50} = \alpha^{50 \bmod 7} = \alpha^1$$
$$\alpha^{100} = \alpha^{100 \bmod 7} = \alpha^2$$
$$\alpha^{50} + \alpha^{100} = \alpha + \alpha^2$$
$$= (010) + (001) = (011) = \alpha^4$$

(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。

答え：講義資料 39.9 を見てください。

(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。

答え：$\mathbb{F}_q$ の原始元の一つを α とする。$\mathbb{F}_q$ に含まれる原始元の数 $A(q)$ は $\mathrm{ord}(\alpha^i) = q-1$ となる $i = 1, \ldots, q-1$ の数である。

$$\mathrm{ord}(\alpha^i) = \mathrm{ord}(\alpha)/\gcd(\mathrm{ord}(\alpha), i)$$
$$= (q-1)/\gcd(q-1, i)$$

が成り立つから、$A(q)$ は $\gcd(\mathrm{ord}(\alpha) = q-1, i) = 1$ となる i の数と等しい。

(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$\alpha$とする。各非零元$\alpha^i$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。

答え：$1 + X^3 + X^4$

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

答え：3,6,12,9

(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。

答え：$g(X)$が$\alpha, \alpha^2, \alpha^3, \alpha^4$を根に含むようにすればよい。

$$\begin{aligned} g(X) &= \mathrm{lcm}(m_1(X), m_2(X), m_3(X), m_4(X)) \\ &= (1 + X + X^2 + X^3 + X^4)(1 + X^3 + X^4) \end{aligned}$$

(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。

答え：講義資料 40.7 を見てください。

9　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 16 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
```

答え：110110001010

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。