# 3　情報通信実験第 2 課題 3(符号理論)

- 作成したプログラムは OCWi で提出し、課題中に求められた答えは紙のレポートで指定された提出日時に指定された提出場所に提出すること。
- 本質的に課題が解けていれば、入力ファイルを改編したり、プログラムのソースファイル内に埋め込んだりしても良い。
- 課題の中で【　】で示されたファイルはスタッフ用のプログラムです。気にしないでください。
- 例えば、学籍番号 17_55555 の学生が問題 1-2 を解答する場合は、17_55555-01-02 というプリフィックスの名前のファイルで提出すること。例：17_55555-01-02.c
- プログラム言語は何を利用してもよいが、実行できない場合には採点できないので、コンパイル方法と実行方法をプログラムの先頭に以下のようにコメントとして明記すること。

  //␣プログラミング言語：C
  //␣コンパイル方法：gcc␣-std=c11␣test.c␣-lm␣-o␣test.out
  //␣実行方法：ターミナル上で test.out を実行

  ␣は半角の空白を表します。プログラムが書かれているファイルがテキストでない場合には、readme.txt に上記の内容を書いて、プログラムと共に提出すること。
- 採点の間違いを避けるためにも、プログラムにはできるだけコメントを残すこと。
- プログラム内で定義した関数については必ず、それがどのような動作をするのか（何を入力として何を返すのか）を自分なりのコメントとして明記すること。コメントがない場合には減点対象となる場合があるので注意すること。
- 学生間で相談してもよいが、他の学生のファイルを写したりコピーしたりしてはいけない。自分なりのコメントを書いて回答すること。
- ☆ の数は難易度を表している。☆ が多いほど難しいので問題に取り組むための目安にするとよい。

  [難易度 ☆]：易しい（作業）

  [難易度 ☆☆]：普通（できる）

  [難易度 ☆☆☆]：少し難しい（できるはず）

  [難易度 ☆☆☆☆]：難しい（できてほしい）

  [難易度 ☆☆☆☆☆]：かなり難しい（できる人はいる）

[難易度 ☆☆☆☆☆☆] : 激むず（できたらすごい）

**3.1** ☆ 以下の問に答えよ。

(a) 以下の入出力からなるプログラムを作成せよ。
入力：ベクトルの長さ $n$、二つのベクトル $c_0, c_1 \in \mathbb{F}_2^n$
出力：ハミング距離 $d(c_0, c_1)$
例：

```
INPUT:
n=8
c0=11111001
c1=10101011
OUTPUT:
d=3
```

(b) ファイル `vec.txt` で与えられた入力に対応する出力を答えよ。

**3.2** ☆☆以下の問に答えよ。

(a) 【`code.c`】以下の入出力からなるプログラムを作成せよ。
入力：符号長 $n$、符号長 $n$ の 2 元非線形符号

$$C = \{c_0, \ldots, c_{M-1}\} \subset \mathbb{F}_2^n$$

要素数 $M := |C|$
出力：最小距離 $d(C)$
例：

```
INPUT:
n=12
M=4
C=
111011111110
010100001010
111001111000
110001110111
OUTPUT:
d_min=3
R=0.166667
```

(b) ファイル `code.txt` で与えられた入力に対応する出力を答えよ。

**3.3** ☆☆【code.c】以下の入出力からなるプログラムを作成せよ。
入力：符号長 $n$、符号長 $n$ の 2 元非線形符号

$$C = \{c_0, \ldots, c_{M-1}\} \subset \mathbb{F}_2^n$$

要素数 $M := |C|$
受信語 $r \in \mathbb{F}_2^n$
出力：最小距離復号による推定符号語 $\hat{c}^{(\mathrm{MD})}(r)$ と $\hat{c}^{(\mathrm{MD})}(r) = c_{i^{(\mathrm{MD})}}$ となる添字 $i^{(\mathrm{MD})}$, $0 \leq i^{(\mathrm{MD})} \leq M-1$
ファイル `r.txt` で与えられた入力に対応する出力を答えよ。

```
INPUT:
n=12
M=4
C=
111011111110
010100001010
111001111000
110001110111
r=
010101101010
OUTPUT:
hat_c=
010100001010
i_MD=1
```

**3.4** ☆☆☆ 2 元線形符号 $C$ に関して、以下の問に答えよ。

(a) 以下の入出力からなるプログラムを作成せよ。
入力：$C$ の符号長 $n$、次元 $k$、生成行列 $G \in \mathbb{F}_2^{k \times n}$
出力：符号語数 $M$、符号化率 $R$、最小距離 $d_{\min}$、標準形生成行列 $G'$、標準形パリティ検査行列 $H'$、$G(H')^T$、$G'(H')^T$
ただし、$G'$ を求める際に列の入れ替えが必要になる入力 $G$ は除外して良い。
例

```
INPUT:
n=10
k=5
G=
1010101101
```

```
0010011001
0001001110
0110111000
0010111110
OUTPUT:
M=32
R=0.5
d_min=3
G'=
1000010011
0100000110
0010011001
0001001110
0000100111
H'=
1010010000
0011001000
0101100100
1101100010
1010100001
G(H')^T=
00000
00000
00000
00000
00000
G'(H')^T=
00000
00000
00000
00000
00000
```

(b) ファイル `linearcode.txt` で与えられた入力に対応する出力を答えよ。

**3.5** 【`hakidashi.c`】☆☆☆☆以下の問に答えよ。

(a) 2 元線形符号 $C$ に対して、以下の入出力とするプログラムを作成せよ。
入力：符号長 $n$、次元 $k$、$C$ の生成行列 $G$

出力：重み分布 $(A_0, \ldots, A_n)$、$C^{\perp}$ の重み分布 $(B_0, \ldots, B_n)$。または等価的に

$$A(X,Y) := \sum_{w=0} A_w X^{n-w} Y^w,$$
$$B(X,Y) := \sum_{w=0} B_w X^{n-w} Y^w$$

例：

```
INPUT:
n=16
k=8
G=
0101101011100100
1111001001011000
0100000110101111
0000010101100101
1111100001110001
0101001011110111
0101010001110011
0111010001011011
OUTPUT:
```

$$\begin{aligned}
&A(X,Y) = \\
&+ X^{16} + X^{13}Y^3 + 7\,X^{12}Y^4 + 20\,X^{11}Y^5 \\
&+ 26\,X^{10}Y^6 + 44\,X^9Y^7 + 57\,X^8Y^8 \\
&+ 42\,X^7Y^9 + 30\,X^6Y^{10} + 19\,X^5Y^{11} \\
&+ 7\,X^4Y^{12} + 2\,X^3Y^{13} \\
&B(X,Y) = \\
&+ X^{16} + 2\,X^{13}Y^3 + 5\,X^{12}Y^4 + 17\,X^{11}Y^5 \\
&+ 30\,X^{10}Y^6 + 46\,X^9Y^7 + 57\,X^8Y^8 \\
&+ 44\,X^7Y^9 + 26\,X^6Y^{10} + 16\,X^5Y^{11} \\
&+ 9\,X^4Y^{12} + 3\,X^3Y^{13}
\end{aligned}$$

(b) ファイル `dual.txt` で与えられた入力に対する出力を答えよ。

ヒント：

$$
\begin{aligned}
&A(X,Y) = X^{64} + 3\,X^{41}Y^{23} + 3\,X^{40}Y^{24} + \cdots \\
&B(X,Y) = \\
&+ X^{64} + 10\,X^{62}Y^{2} \\
&+ 142\,X^{61}Y^{3} + 2457\,X^{60}Y^{4} \\
&+ 29775\,X^{59}Y^{5} + 292948\,X^{58}Y^{6} \\
&\vdots
\end{aligned}
$$

# 4　情報通信実験第 2 課題 4(符号理論)

**4.1** 【poly.c】以下の問に答えよ。

(a) 有限体 $\mathbb{F}_p$ の加減乗除表を出力するプログラムを作成せよ。以下の入出力からなるプログラムを作成せよ。
入力：素数 $p$
出力：$\mathbb{F}_p$ の加減乗除表
例：

```
INPUT:
p=5
OUTPUT:
ADD
  | 0 1 2 3 4
--+-----------
0 | 0 1 2 3 4
1 | 1 2 3 4 0
2 | 2 3 4 0 1
3 | 3 4 0 1 2
4 | 4 0 1 2 3
MUL
  | 0 1 2 3 4
--+-----------
0 | 0 0 0 0 0
1 | 0 1 2 3 4
2 | 0 2 4 1 3
3 | 0 3 1 4 2
4 | 0 4 3 2 1
SUB
  | 0 1 2 3 4
--+-----------
0 | 0 4 3 2 1
1 | 1 0 4 3 2
2 | 2 1 0 4 3
3 | 3 2 1 0 4
4 | 4 3 2 1 0
DIV
  | 0 1 2 3 4
--+-----------
0 | - 0 0 0 0
1 | - 1 3 2 4
2 | - 2 1 4 3
3 | - 3 4 1 2
4 | - 4 2 3 1
```

(b) $p = 7$ に対応する出力を答えよ。

**4.2** 【hakidashi_Fp.c】以下の問に答えよ。

(a) 以下の入出力からなる有限体 $\mathbb{F}_p$ 上の線形方程式を解くプログラムを作成せよ。
入力：素数 $p$、自然数 $n > 0$、正則行列 $A \in \mathbb{F}_p^{n \times n}$、$b \in \mathbb{F}_p^n$
出力：$Ax = b$ をみたす $x \in \mathbb{F}_p^n$
例：

```
INPUT:
p=5
n=3
```

```
A=
3 4 1
3 4 3
1 2 4
b=
2
3
4
OUTPUT:
x=
0
1
3
```

(b) ファイル `linear_equation_Fp.txt` で与えられる入力に対応する出力を答えよ。

**4.3** 【`poly.c`】以下の問に答えよ。

(a) 次数がそれぞれ $n, m > 0$ の多項式 $f(X), g(X) \in \mathbb{F}_2[X]$ の加減乗除

$$f(X) + g(X),$$
$$f(X) - g(X),$$
$$f(X) \times g(X),$$
$$f(X)/g(X) \text{ の商と余り}$$

を出力するプログラムを作成せよ。ただし、$g(X) \neq 0$ とする。
例：

```
INPUT:
n=13
m=9
f=[11001111100111]
g=[0011011111]
OUTPUT:
f+g=[11111000010111]
f-g=[11111000010111]
f*g=[0010111001100001011101]
f/g= 商 [01001] 剰余 [11010111]
```

(b) 以下またはファイル `poly.txt` で与えられる入力に対応する出力を答えよ。

**4.4** 【`poly.c`】以下の問に答えよ。

(a) 与えられた次数 $m$ の原始多項式 $f(X) \in \mathbb{F}_2[X]$ によって定義される有限体 $\mathbb{F}_{2^m}$ の加減乗除を計算するプログラムを作成せよ。
例：$f(X) = 1 + X + X^3$

```
INPUT:
m=3
f(X)=[1101]
OUTPUT:
ADD   | [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]

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

SUB   | [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]

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

(b) 以下の入力に対する、計算の結果を求めよ。

```
INPUT:
m=8
f(X)=[101011111]
OUTPUT:
[00100001]*[11111100]=?
[00010101]*[10101111]=?
[00111100]*[00111011]=?

[00000011]/[01110110]=?
[10100000]/[00110001]=?
[10111011]/[00010100]=?
```

**4.5** 【hakidashi_Fp.c】以下の問に答えよ。

(a) $\mathbb{F}_{2^m}$ は $m$ 次原始多項式 $f(X) \in \mathbb{F}_2[X]$ で定義されているとする。以下の入出力からなる有限体 $\mathbb{F}_{2^m}$ 上の線形方程式を解くプログラムを作成せよ。
入力：$m, n \in \mathbb{N}$、$m$ 次原始多項式 $f(X) \in \mathbb{F}_2[X]$、$A \in (\mathbb{F}_{2^m})^{n \times n}$、$b \in (\mathbb{F}_{2^m})^n$
出力：$Ax = b$ をみたす $x \in (\mathbb{F}_{2^m})^n$
例：$f(X) = 1 + X + X^3$

```
INPUT:
m=3
n=3
f(X)=[1101]
A=
[101][000][001]
[101][101][100]
[100][110][110]
b=
[010]
[001]
[001]
OUTPUT:
x=
[011]
[000]
[111]
```

(b) ファイル `linear_equation_F256.txt` で与えられる入力に対応する出力を答えよ。

**4.6** 【`poly.c`】原始多項式（既約多項式）$f(X) = [101011111]$ で定義される $\mathbb{F}_{256} := \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{254}\}$ 上の $(1, \alpha, \alpha^2, \ldots, \alpha^{254})$ で定義される長さ $n = 255$、次元 $k = 223$ の RS 符号に関して以下の問に答えよ。ここで、$\alpha := [X]$ である。

(a) 符号器 $u \in \mathbb{F}_{256}^k \to c \in \mathbb{F}_{256}^n$ のプログラムを作成せよ。
例：`RS256_encode_example.txt`

(b) 入力 `RS256_encode_problem.txt` に対応する符号器の出力 $c$ の初めの 4 シンボルを答えよ。
解答形式 `[????????][????????][????????][????????]`

(c) 復号器 $r \in \mathbb{F}_{256}^n \to \hat{u} \in \mathbb{F}_{256}^k$ のプログラムを作成せよ。
例：`RS256_decode_example.txt`

(d) 入力 `RS256_decode_problem.txt` に対応する復号器の出力 $\hat{u}$ の初めの 4 シンボルを答えよ。
解答形式 `[????????][????????][????????][????????]`