実施：2025 年 7 月 23 日 (水) 9:10-10:40, 場所：E-702

2025 年度 **前期 定期試験** (問題 兼 解答用紙)

開講学部	評点小計
理工学部	

評　点

問題枚数	両面印刷	別紙解答用紙	試験時間	試 験 科 目 名	出 題 者
1/6	有	なし	80 分	計算機科学 7　水曜 1 時限, 教科書：Original	大西 良博

持込許可物	所属学部	所属学科	学年	クラス	学籍番号 (9 桁)	氏　名
なし	理工学部	学科	年			

注意 1. 最終的な答に至る途中の説明をできるだけ詳しく書くこと. 最終結果だけでは得点できない.
注意 2. 途中退出し試験を完了できるのは 10:10 の時点のみとする.

1 (20 点) $\mathbb{F}_3$ 上の検査行列 H が

$$H = \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 2 \end{bmatrix} \in \mathrm{Mat}(4, 2, \mathbb{F}_3)$$

で与へられた線形符号 C に対し, 次の (1) 〜 (3) に答へよ.

(1) C の生成行列 G および C の符号語をすべて求めよ.

(2) C の最小距離 d を求めよ.

(3) C の標準配列および対応する syndromes を求めよ.
　但し, 最左欄はできるだけ重さが小さい符号が並ぶ様にせよ.

解 (1) 方程式 $H{}^t\boldsymbol{x} = \boldsymbol{0}$ の解空間が C であり, その基底を行 vectors とする行列が G であつて

$$G = \begin{bmatrix} 2 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \in \mathrm{Mat}(4, 2, \mathbb{F}_3).$$

また, G の行 vectors の 1 次結合の全体が C であるから,

$$C = \{\, c_1[2\ 1\ 1\ 0] + c_2[1\ 1\ 0\ 1] \,|\, c_1,\ c_2 \in \mathbb{F}_3 \,\}$$

これを書き出せばよいが, 具体的に書くことは省略する.

(2) H に対して, **定理 5.1**（2024 年 6 月 6 日以降版の text）を使ふと $d = 3$ であることがわかる. 別解 **命題 3.10** による. つまり C の $\boldsymbol{0}$ 以外の元（9 個）の重さ $\omega(\boldsymbol{w})$ を見れば, それらはすべて 3 以上である. よつて, 答は 3.

(3) $G = \begin{bmatrix} \boldsymbol{a} \\ \boldsymbol{b} \end{bmatrix}$ とすれば, 以下の様になる：

$\boldsymbol{e}$	$\boldsymbol{e}+\boldsymbol{a}$	$\boldsymbol{e}+2\boldsymbol{a}$	$\boldsymbol{e}+\boldsymbol{b}$	$\boldsymbol{e}+2\boldsymbol{b}$	$\boldsymbol{e}+\boldsymbol{a}+\boldsymbol{b}$	$\boldsymbol{e}+2\boldsymbol{a}+\boldsymbol{b}$	$\boldsymbol{e}+\boldsymbol{a}+2\boldsymbol{b}$	$\boldsymbol{e}+2\boldsymbol{a}+2\boldsymbol{b}$	$\boldsymbol{e}{}^tH$
0000	1101	2202	2110	0211	1012	1220	2021	0122	00
0001	1102	2200							22
0002	1100	2201							11
0010	1111	2212							12
0020	1121	2222							21
0100	1201	2102							01
0200	1001	2202							02
1000	2101	0202							10
2000	0101	1202							20

$\boldsymbol{e}$ ····· coset leaders

$\boldsymbol{e}{}^tH$ ····· syndrome

この表（標準配列）の作り方

Coset leaders の Hamming 重さがなるべく小さくなる様にしてみた.

そのためには, 第 1 列に Hamming 重さ 1 の 0001, 0001, 0010, 0020, 0100, 0200, 1000, 2000 を入れて syndrome を計算する. この場合は, 0000 とこの 8 個とで丁度 syndromes のすべてが現れる.

2025 年度 「計算機科学 7」 定期試験

学籍番号	

2 (20 点) 次の行列 G は $(7,4)$ Hamming 符号の生成行列である.

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

(但し, ここでは巡回符号として記述してある.) これについて以下に答へよ.

(1) $[1\,0\,1\,0]$ を符号化せよ.

(2) 検査行列 H を簡約化された形で求めよ.

(3) $[1\,0\,1\,0\,1\,1\,0]$, $[0\,1\,0\,0\,0\,0\,1]$ を元語化せよ.

解. (1)

$$[1\,0\,1\,0]G = [1\,1\,1\,0\,0\,1\,0] \quad \cdots\cdots \text{ Ans.}$$

(2) G を反転簡約化すると

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

よつて, 検査行列は,

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

である. これは簡約化されてゐる.

(3) Syndrome を計算すると

$$\boldsymbol{e} = H\,{}^t[1\,0\,1\,0\,1\,1\,0] = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

であるが, これは H の第 3 列に他ならないから, そこの修正を入れて

$$\boldsymbol{e} = [1\,0\,1\,0\,1\,1\,0] - [0\,0\,1\,0\,0\,0\,0] = [1\,0\,0\,0\,1\,1\,0]$$

と復号される. これの元語化 $[x\ y\ z\ w]$ とは

$$(\star) \qquad [x\ y\ z\ w]G = [1\,0\,0\,0\,1\,1\,0]$$

を満たすもののことであるから, これを解けばよい. まづ G の第 1, 6, 7 列に対応する成分に注目して,

$$x = 1, \quad z = 1, \quad w = 0$$

である. さらに G の第 2 列に対応する成分を見れば

$$1 + y = 0$$

から $y = 1$ である. つまり元語化は $\boxed{[1\ \ 1\ \ 1\ \ 0]}$ である. もう一つについても

$$\boldsymbol{e} = H\,{}^t[0\,1\,0\,0\,0\,0\,1] = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

から, 正しい符号語は

$$[0\,1\,0\,0\,0\,0\,1] - [0\,0\,0\,0\,0\,1\,0] = [0\,1\,0\,0\,0\,1\,1]$$

である. こちらに元語化についても, 同様に考へて

$$[0\ \ y\ \ 1\ \ 1]$$

の形であるが, やはり, G の第 2 列を見ることで $y = 1$ がわかり $\boxed{[0\ \ 1\ \ 1\ \ 1]}$ が元語化である.

2025 年度 「計算機科学 7」 定期試験

学籍番号	

3 (15 点) $\mathbb{F}_4 = \mathbb{F}_{2^2} = \mathbb{F}_2[\alpha] = \{0,\ 1,\ \alpha,\ 1+\alpha\}$ (但し $\alpha^2 = 1+\alpha$) 上の検査行列

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

で定義される線形符号 C に対し, 次の問に答へよ.

(1) C の最小距離 $d(C)$ を求めよ.

(2) C が 1 誤り訂正符号であることを示せ.

(3) C の生成行列を反転簡約行列の形で求めよ. それを G とする.

(4) 通報 $[\alpha\ \ 1]$ を符号化せよ.

(5) C が 1 誤り符号であることを踏まへて, 受信語 $[0\ \ 1\ \ 1{+}\alpha\ \ \alpha]$ を復号せよ.

解

(1) どの 2 列も 1 次独立で, どの 3 列も 1 次従属なので, $d(C) = \boxed{3}$.

(2) $d(C) = 2t+1$ なる最大の t は 1 なので 1 誤り符号である.

(3) まづ, H を簡約化する :

α	$1+\alpha$	1	1	
$1+\alpha$	α	0	1	
α	$1+\alpha$	1	1	
1	1	1	0	② − ①
0	1	$1+\alpha$	1	① − ② × α
1	1	1	0	
0	1	$1+\alpha$	1	
1	0	α	1	② − ①
1	0	α	1	②
0	1	$1+\alpha$	1	①

よつて

$$G = \boxed{\begin{bmatrix} \alpha & 1+\alpha & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}}.$$

(4)

$$[\alpha\ \ 1]\,G = \boxed{[\alpha\ \ 0\ \ \alpha\ \ 1]}.$$

(5) 与へられた受信語の syndrome は

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

この syndrome を持つ様な 1 誤りは

$$[0\ \ 0\ \ \alpha\ \ 0]$$

に他ならない. よつて求める復号は

$$[0\ \ 1\ \ 1+\alpha\ \ \alpha] - [0\ \ 0\ \ \alpha\ \ 0] = \boxed{[0\ \ 1\ \ 1\ \ \alpha]} \cdots\cdots\cdots \text{Ans.}$$

である. ちなみに, これの元語化 $[x\ \ y]$ は

$$[x\ \ y]\,G = [0\ \ 1\ \ 1\ \ \alpha]$$

を解けばよく, $[x\ \ y] = [1\ \ \alpha]$ である. □

2025 年度 「計算機科学 7」 定期試験

学籍番号	

4 (15 点) 可換環 $\mathbb{F}_5[x]/(x^{124}-1)$ の ideals はいくつあるか.

(Hint : $x(x^{124}-1) = x^{5^3} - x$ の分解体は $\mathbb{F}_5$ の 3 次拡大であるから, 既約因数 (式) の次数は 3 の約数.
また, この多項式は分離的 (重複根を持たない).)
(答には具体的に ideal を書く必要はないし, 求める個数は自然数の冪乗を使つた形でよい.)

解 $x(x^{124}-1) = x^{5^3} - x$ の分解体は $\mathbb{F}_5$ の 3 次拡大であるから, 既約因数 (式) の次数は 3 の約数.
また, この多項式は分離的 (重複根を持たない) である. ゆゑに, $\mathbb{F}_5$ 上で $x^{124}-1$ を因数分解すれば

$$x^{124}-1 = (x-1)(x-2)(x-3)(x-4) \times (\text{異なる } \tfrac{124-4}{3} = 40 \text{ 種類の 3 次既約多項式の積})$$

ここで, 異なる $\frac{124-4}{3} = 40$ 種類の 3 次既約多項式を $f_1(x), \cdots, f_{40}(x)$ とおくと, よつて求める ideals は,

$$(x-1)^a(x-2)^b(x-3)^c(x-4)^d \prod_{j=1}^{40} f_j(x)^{e_j}$$

を生成元とする. 但し, $a, b, c, d, e_j \in \{0, 1\}$ である. その様な多項式を生成元とする ideals は

$$\boxed{2^{44}} (= 17592186044416) \text{ 個}$$

ある. □

2025 年度 「計算機科学 7」 定期試験

学籍番号	

5 (15 点) $g(x) = 2 + 2x + x^3 \in \mathbb{F}_3[x]$ は周期 13 の多項式である.
(つまり $g(x) | x^n - 1$ なる最小の $n \in \mathbb{N}$ は 13).
これの生成する巡回符号 $C \subset {\mathbb{F}_3}^{-13}$, つまり

$$\mathbb{F}_3\, g(x) + \mathbb{F}_3\, xg(x) + \cdots + \mathbb{F}_3\, x^9 g(x)$$

の係数を昇冪の順に拾つてできる ${\mathbb{F}_3}^{-13}$ 内の vectors の全体のなす部分空間, について以下に答へよ.

(1) C の検査多項式 $h(x)$ を求めよ.

(2) $\boldsymbol{u} = [2\,1\,1\,0\,1\,1\,2\,2\,1\,1\,0\,1\,0]$ は符号語であるか否か. 理由を付けて答えよ.

(3) C は 1 誤り訂正可能である. これを既知として $\boldsymbol{v} = [2\,1\,2\,0\,0\,1\,1\,1\,1\,0\,1\,0\,1]$ を複号せよ.
その際, 下記の syndrome の表を用ゐてよい.

error	syndrome
1	1
2	2
x	x
$2x$	$2x$
x^2	x^2
$2x^2$	$2x^2$
x^3	$1+x$
$2x^3$	$2+2x$
x^4	$x+x^2$
$2x^4$	$2x+2x^2$
x^5	$1+x+x^2$
$2x^5$	$2+2x+2x^2$
x^6	$1+2x+x^2$
$2x^6$	$2+x+2x^2$
x^7	$1+2x+2x^2$
$2x^7$	$2+x+x^2$
x^8	$2+2x^2$
$2x^8$	$1+x^2$
x^9	$2+x$
$2x^9$	$1+2x$
x^{10}	$2x+x^2$
$2x^{10}$	$x+2x^2$
x^{11}	$1+x+2x^2$
$2x^{11}$	$2+2x+x^2$
x^{12}	$2+x^2$
$2x^{12}$	$1+2x^2$

略解. (1)

$$h(x) = \frac{x^{13}-1}{g(x)} = \boxed{1 + 2x + x^2 + 2x^4 + 2x^5 + x^6 + x^7 + x^8 + x^{10}}.$$

(2) $\boldsymbol{u}$ に対応する多項式 $u(x) = 2 + x + x^2 + x^4 + x^5 + 2x^6 + 2x^7 + x^8 + x^9 + x^{11}$ について

$$u(x) \equiv x + x^2 \bmod g(x)$$

なので $\boldsymbol{u}$ は符号語でない.

(3) $\boldsymbol{v}$ に対応する多項式 $\boldsymbol{v}$ に対応する多項式 $v(x) = 2 + x + 2x^2 + x^5 + x^6 + x^7 + x^8 + x^{10} + x^{12}$ について

$$g(x) \equiv 2x + x^2 \bmod g(x)$$

であるから $\boldsymbol{v}$ は, 表の syndrome $2x + x^2$ に対応する誤り x^{10} を含むと推測できる. よつて

$$\begin{aligned}&[2\,1\,2\,0\,0\,1\,1\,1\,1\,0\,1\,0\,1] - [0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0]\\ &= [2\,1\,2\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1]\end{aligned}$$

と複号される.

2025 年度 「計算機科学 7」 定期試験

学籍番号	

6 (15 点) 次の行列 G を生成行列とする $\mathbb{F}_3$ 上の線形符号 $C \subset {\mathbb{F}_3}^{11}$ は巡回符号である.

$$G = \begin{bmatrix} \boldsymbol{g}_0 \\ \boldsymbol{g}_1 \\ \boldsymbol{g}_2 \\ \boldsymbol{g}_3 \\ \boldsymbol{g}_4 \\ \boldsymbol{g}_5 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 1 & 2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 2 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 1 & 2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 2 & 1 & 1 \end{bmatrix} \in \mathrm{Mat}(6, 11, \mathbb{F}_3).$$

これについて以下に答へよ.

(1) 生成多項式 $g(x)$ を記せ.

(2) 検査多項式 $h(x)$ を求めよ.

(3) $\boldsymbol{g}_0 + {\boldsymbol{g}_5}^{\sigma}$ を $\boldsymbol{g}_0, \cdots, \boldsymbol{g}_5$ の $\mathbb{F}_3$ 上の 1 次結合で表せ. (σ は右 shift を意味する)

解 (1) 生成多項式は $g(x) = 2 + 0x + x^2 + 2x^3 + x^4 + x^5$.

(2) 検査多項式は

$$h(x) = \frac{x^{11} - 1}{g(x)} = x^6 + 2x^5 + 2x^4 + 2x^3 + x^2 + 1$$

${\boldsymbol{g}_5}^{\sigma}$ は $x^6\, g(x)$ に対応するが,

$$x^6 = h(x) - 2x^5 - 2x^4 - 2x^3 - x^2 - 1$$

$$\begin{aligned} g(x) + x^6 g(x) &= g(x) + \big(h(x) - 2x^5 - 2x^4 - 2x^3 - x^2 - 1\big)\, g(x) \\ &\equiv g(x) + (2 + 2x^2 + x^3 + x^4 + x^5) g(x) \mod x^{11} - 1. \end{aligned}$$

よつて

$$\boldsymbol{g}_0 + {\boldsymbol{g}_5}^{\sigma} = 0\boldsymbol{g}_0 + 0\boldsymbol{g}_1 + 2\boldsymbol{g}_2 + \boldsymbol{g}_3 + \boldsymbol{g}_4 + \boldsymbol{g}_5 \quad \cdots\cdots \text{ Ans.}$$

□