実施：2024 年 8 月 17 日 (水) 9:10-10:40, 場所：E-202

2024 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．

$\boxed{\mathbf{1}}$ (20 点) 検査行列 H が

$$H = \begin{bmatrix} 1 & 0 & 4 & 6 \\ 0 & 1 & 2 & 3 \end{bmatrix} \in \mathrm{Mat}(4, 2, \mathbb{F}_7)$$

で与へられる $\mathbb{F}_3$ 上の線形符号 $C \subset \mathbb{F}_7{}^{-4}$ について, 次の (1) 〜 (3) に答へよ.

(1) C の生成行列 G を求めよ.

(2) C の最小距離 d を求めよ.

(3) $\boldsymbol{v} = [2\ 1\ 1\ 1]$ は 1 箇所のみ誤送信されてゐるが, その箇所を特定でき得ないことを説明せよ.

解 (1) 方程式 $H^t\boldsymbol{x} = \mathbf{0}$ 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

$$G = \begin{bmatrix} -4 & -2 & 1 & 0 \\ -6 & -3 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 5 & 1 & 0 \\ 1 & 4 & 0 & 1 \end{bmatrix} \in \mathrm{Mat}(4, 2, \mathbb{F}_7).$$

(2) H に対して, **定理 5.1** を使ふと $d = 2$ であることがわかる.

第 3 列を 3 倍すると第 4 列に一致することに注意.

<u>別解</u> **命題 3.9**（2024 年 6 月 6 日付けの text）による．つまり C の $\mathbf{0}$ 以外の元の重さ $\omega(\boldsymbol{w})$ を見れば, それらはすべて 2 である．よつて, 答は 2.

(3)

$$H^t\boldsymbol{v} = \begin{bmatrix} 5 \\ 6 \end{bmatrix}$$

であるが

$$\begin{bmatrix} 5 \\ 6 \end{bmatrix} = 3\begin{bmatrix} 4 \\ 2 \end{bmatrix} = 2\begin{bmatrix} 6 \\ 3 \end{bmatrix}$$

であるから, 第 3 成分の誤りなのか, 第 4 成分の誤りなのかを特定できない.

<u>別解</u> $d(C) \geqq 2t + k + 1$ を利用すれば説明できる.

学籍番号	

$\boxed{\mathbf{2}}$ (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) $[1\ 1\ 1\ 0]$ 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) $[1\ 1\ 1\ 1\ 0\ 0\ 1]$, $[1\ 1\ 0\ 0\ 0\ 1\ 0]$ を元語化せよ.

解. (1)

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

(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

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

であるが, これは H の第 1 列に他ならないから, そこの修正を入れて

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

とわかる. よつて, 正しい符号語は

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

である. これに対応する単語 $\boldsymbol{w}$ は

$$\boldsymbol{w}G = [1\ 0\ 1\ 1\ 0\ 1\ 1]$$

を満たす. これを解いて

$$\boldsymbol{w} = [0\ 1\ 0\ 1] \quad \cdots\cdots\cdot \ \text{Ans.}$$

である. もう一つについても

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

から, 正しい符号語は

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

である. これに対応する単語は上と同じ様に考へて

$$[1\ 0\ 1\ 0] \quad \cdots\cdots\cdot \ \text{Ans.}$$

である.

学籍番号	

$\boxed{\mathbf{3}}$ (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

$$H = \begin{bmatrix} 1+\alpha & \alpha & 1 & 1 \\ \alpha & 1+\alpha & 0 & 1 \end{bmatrix} \in \mathrm{Mat}(2, 4, \mathbb{F}_4)$$

で定義される線形符号 C に対し,

(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 $[1\ \ \alpha]$ を符号化せよ.
(5) C が 1 誤り訂正符号であることを踏まへて, 受信語 $[0\ \ \alpha\ \ \alpha\ \ \alpha]$ を元語化せよ.

解

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

(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:

$$\begin{array}{cccc|l} \hline 1+\alpha & \alpha & 1 & 1 & \\ \alpha & 1+\alpha & 0 & 1 & \\ \hline 1 & 1 & 1 & 0 & ① - ② \\ \alpha & 1+\alpha & 0 & 1 & \\ \hline 1 & 1 & 1 & 0 & \\ 0 & 1 & \alpha & 1 & ② - ① \times \alpha \\ \hline 1 & 0 & 1+\alpha & 1 & ① - ② \\ 0 & 1 & \alpha & 1 & \end{array}$$

よつて

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

(4)

$$[1\ \ \alpha]\,G = [1\ \ 0\ \ 1\ \ \alpha].$$

(5) 与へられた受信語の syndrome は

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

この syndrome を持つ様な 1 誤りは

$$[0\ \ 0\ \ 0\ \ 1+\alpha]$$

に他ならない. よつて復号は

$$[0\ \ \alpha\ \ \alpha\ \ \alpha] + [0\ \ 0\ \ 0\ \ 1+\alpha] = [0\ \ \alpha\ \ \alpha\ \ 1]$$

となる. これの元語化は $\boxed{2}$ と同様にして計算すれば

$$[\alpha\ \ 1]$$

とわかる. □

2024 年度 「計算機科学 7」 定期試験

学籍番号	

$\boxed{\mathbf{4}}$ (15 点) $\mathbb{F}_2[x]/(x^7-1)$ の ideals を全て求めよ.
(Hint : $x(x^7-1) = x^{2^3} - x$ の分解体は $\mathbb{F}_2$ の 3 次拡大であるから, 既約因数 (式) の次数は 3 の約数.)

解 $\mathbb{F}_2$ 上で

$$x^7 - 1 = (x+1)(x^3+x+1)(x^3+x^2+1).$$

よつて, ideals は,

$$(x+1)^a(x^3+x+1)^b(x^3+x^2+1)^c.$$

で a, b, $c \in \{0,1\}$ なる 8 個の多項式をそれぞれ生成元とする 8 個である. $\square$

5 (15 点) $g(x) = 1 + 4x + x^2 \in \mathbb{F}_5[x]$ は周期 6 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 6）.
これの生成する巡回符号 $C \subset {\mathbb{F}_5}^{-6}$, つまり

$$\mathbb{F}_5\, g(x) + \mathbb{F}_5\, xg(x) + \mathbb{F}_5\, x^2 g(x) + \mathbb{F}_5\, x^3 g(x)$$

の係数を昇冪の順に拾つてできる ${\mathbb{F}_5}^{-6}$ 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) $\boldsymbol{u} = [\,4\ 2\ 1\ 2\ 4\ 3\,]$ は符号語であるか否か. 理由を付けて答えよ.
(3) $\boldsymbol{v} = [\,1\ 2\ 4\ 3\ 0\ 1\,]$ は符号語であるか否か. 理由を付けて答えよ.

略解. (1)

$$h(x) = 4 + 4x + x^3 + x^4.$$

(2) $\boldsymbol{u}$ に対応する多項式

$$u(x) = \mathrm{rep}(\boldsymbol{u}, x) = 4 + 2x + x^2 + 2x^3 + 4x^4 + 3x^5$$

について

$$u(x) \equiv 4 + x \mod g(x)$$

であり $g(x) \nmid u(x)$ であるから $\boldsymbol{u}$ は符号語ではない.

(3) $\boldsymbol{v}$ に対応する多項式

$$v(x) = \mathrm{rep}(\boldsymbol{v}, x) = x + 2x + 4x^2 + 3x^3 + x^5$$

について

$$v(x)/g(x) = 1 + 3x + x^2 + x^3$$

と割り切れるので $\boldsymbol{u}$ は符号語である.

$\boxed{\mathbf{6}}$ (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．

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

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 $h(x)$ を記せ．

(3) $(\boldsymbol{g}_0 + 2\boldsymbol{g}_5)^{\sigma^2}$ 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）

略解． （以下すべて $\mathbb{F}_3$ 上での計算である．）

(1)

$$g(x) = 2 + 2x + x^2 + 2x^3 + x^5.$$

(2)

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

(3) $(\boldsymbol{g}_0 + 2\boldsymbol{g}_5)^{\sigma^2}$ は $\mathrm{rep}(\quad, x)$ で $(x^2 + 2x^7)g \mod (x^{11} - 1)$ に対応するのであるが，

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

を使つて x^6 より次数の高い項を消去すれば

$$\begin{aligned} x^2 + 2x^7 &= x^2 - 2x(1 + 2x + 2x^2 + 2x^3 + x^4) \mod h(x) \\ &= x^2 - 2x(1 + 2x + 2x^2 + 2x^3 + x^4) \mod h(x) \\ &= x + 2x^3 + 2x^4 + x^5 \mod h(x) \end{aligned}$$

であるから $(x + 2x^3 + 2x^4 + x^5)g(x)$ に対応する．ゆゑに，

$$(x^2 + 2x^7)g(x) \equiv (x + 2x^3 + 2x^4 + x^5)g(x) \mod h(x)g(x), \quad \text{つまり,}$$
$$(x^2 + 2x^7)g(x) \equiv (x + 2x^3 + 2x^4 + x^5)g(x) \mod (x^{11} - 1).$$

ゆゑに

$$(\boldsymbol{g}_0 + 2\boldsymbol{g}_5)^{\sigma^2} = 0\,\boldsymbol{g}_0 + \boldsymbol{g}_1 + 0\,\boldsymbol{g}_2 + 2\,\boldsymbol{g}_3 + 2\,\boldsymbol{g}_4 + \boldsymbol{g}_5$$

である．