2006年度 情報科学I　レポート6　学生用

学籍番号：　　　　　　　　　　　　氏名：

<u>下記の注意事項を守り</u>、次ページ以降の問いに答え、レポートを完成させなさい。

提出期限：2006年7月14日(金) 13:00まで
提出場所：理学部棟 正面玄関内に設置のレポートボックス

注意事項：

(1) このページを印刷し、必要事項を記入の上(学籍番号欄と氏名欄は2箇所あるので忘れずに記入すること)、レポートの表紙として提出すること。
(2) ~~文章処理ソフトウェアや図形処理ソフトウェア等を駆使してレポートを作成し~~(問→解答→問→解答→ ··· の順になるように記述すること)、A4サイズの用紙~~に印刷して提出すること(手書きは不可)。~~
(3) クラスメイトのレポートを参考にしたり、クラスメイトと協力してレポートを作成した場合は、教員控の協力者氏名欄にクラスメイトの氏名を記入すること。これらの場合も、自分の言葉で表現し直すこと。**コピー禁止**。
(4) 情報科学Iについて、あなたの声を聞かせてください(教員控の意見・質問欄に記入のこと)。気軽にどうぞ(成績には一切影響しません)。

出題者：幸山 直人
出題日：2006年7月12日(水)　＊7月5日(水)先行公開

得点：　　　　/6

－－－－－－－－－－－－－－－－－－－－－－－－－ 切り取り線 －－－－－－－－－－－－－－－－－－－－－－－－－

2006年度 情報科学I　レポート6　教員控

学籍番号：　　　　　　　　　　　　氏名：

協力者氏名：　　　　　　　　　　,　　　　　　　　　　,

レポート作成に要した時間：　　　　.　　　　時間

得点：　　　　/6

意見・質問：

問 1　[テキスト 60 ページの行列式の値 ($t=3$ の場合)]　GF(q) 上の 6×6 行列を

$$D=\begin{bmatrix} (\alpha^1)^{i_1} & (\alpha^1)^{i_2} & (\alpha^1)^{i_3} & (\alpha^1)^{i_4} & (\alpha^1)^{i_5} & (\alpha^1)^{i_6} \\ (\alpha^2)^{i_1} & (\alpha^2)^{i_2} & (\alpha^2)^{i_3} & (\alpha^2)^{i_4} & (\alpha^2)^{i_5} & (\alpha^2)^{i_6} \\ (\alpha^3)^{i_1} & (\alpha^3)^{i_2} & (\alpha^3)^{i_3} & (\alpha^3)^{i_4} & (\alpha^3)^{i_5} & (\alpha^3)^{i_6} \\ (\alpha^4)^{i_1} & (\alpha^4)^{i_2} & (\alpha^4)^{i_3} & (\alpha^4)^{i_4} & (\alpha^4)^{i_5} & (\alpha^4)^{i_6} \\ (\alpha^5)^{i_1} & (\alpha^5)^{i_2} & (\alpha^5)^{i_3} & (\alpha^5)^{i_4} & (\alpha^5)^{i_5} & (\alpha^5)^{i_6} \\ (\alpha^6)^{i_1} & (\alpha^6)^{i_2} & (\alpha^6)^{i_3} & (\alpha^6)^{i_4} & (\alpha^6)^{i_5} & (\alpha^6)^{i_6} \end{bmatrix}$$

とする。ただし、$i_1<i_2<i_3<i_4<i_5<i_6$ とする。このとき、行列 D の行列式の値が

$$\det D=\alpha^{i_1+i_2+i_3+i_4+i_5+i_6}\prod_{1\le k<l\le 6}(\alpha^{i_l}-\alpha^{i_k})$$

で与えられることを示しなさい。計算過程も記述すること。(2 点)

解答例　行列 D を $(a^i)^j=(a^j)^i$ に注意して以下のように書き換える。

$$D=\begin{bmatrix} (\alpha^{i_1})^1 & (\alpha^{i_2})^1 & (\alpha^{i_3})^1 & (\alpha^{i_4})^1 & (\alpha^{i_5})^1 & (\alpha^{i_6})^1 \\ (\alpha^{i_1})^2 & (\alpha^{i_2})^2 & (\alpha^{i_3})^2 & (\alpha^{i_4})^2 & (\alpha^{i_5})^2 & (\alpha^{i_6})^2 \\ (\alpha^{i_1})^3 & (\alpha^{i_2})^3 & (\alpha^{i_3})^3 & (\alpha^{i_4})^3 & (\alpha^{i_5})^3 & (\alpha^{i_6})^3 \\ (\alpha^{i_1})^4 & (\alpha^{i_2})^4 & (\alpha^{i_3})^4 & (\alpha^{i_4})^4 & (\alpha^{i_5})^4 & (\alpha^{i_6})^4 \\ (\alpha^{i_1})^5 & (\alpha^{i_2})^5 & (\alpha^{i_3})^5 & (\alpha^{i_4})^5 & (\alpha^{i_5})^5 & (\alpha^{i_6})^5 \\ (\alpha^{i_1})^6 & (\alpha^{i_2})^6 & (\alpha^{i_3})^6 & (\alpha^{i_4})^6 & (\alpha^{i_5})^6 & (\alpha^{i_6})^6 \end{bmatrix}$$

行列式の値は、各列を $\alpha^{i_1}, \alpha^{i_2}, \alpha^{i_3}, \alpha^{i_4}, \alpha^{i_5}, \alpha^{i_6}$ でくくると、

$$\det D \quad = \quad \alpha^{i_1+i_2+i_3+i_4+i_5+i_6}\begin{vmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \alpha^{i_3} & \alpha^{i_4} & \alpha^{i_5} & \alpha^{i_6} \\ (\alpha^{i_1})^2 & (\alpha^{i_2})^2 & (\alpha^{i_3})^2 & (\alpha^{i_4})^2 & (\alpha^{i_5})^2 & (\alpha^{i_6})^2 \\ (\alpha^{i_1})^3 & (\alpha^{i_2})^3 & (\alpha^{i_3})^3 & (\alpha^{i_4})^3 & (\alpha^{i_5})^3 & (\alpha^{i_6})^3 \\ (\alpha^{i_1})^4 & (\alpha^{i_2})^4 & (\alpha^{i_3})^4 & (\alpha^{i_4})^4 & (\alpha^{i_5})^4 & (\alpha^{i_6})^4 \\ (\alpha^{i_1})^5 & (\alpha^{i_2})^5 & (\alpha^{i_3})^5 & (\alpha^{i_4})^5 & (\alpha^{i_5})^5 & (\alpha^{i_6})^5 \end{vmatrix}$$

となる (上記の右側の行列式は線形代数学 I 演習 (2 行列式論 2.10.1 行列式の交代多重線形性 C(1-5)) で出題および解答済みです)。ここで、$x_k=\alpha^{i_k}$ ($k=1,2,3,4,5,6$) と置き、行列式を

$$\det D'=(\alpha^{i_1+i_2+i_3+i_4+i_5+i_6})^{-1}\det D$$

と書き直せば、

$$\det D'=\det D'^T=\begin{vmatrix} 1 & x_1 & x_1^2 & x_1^3 & x_1^4 & x_1^5 \\ 1 & x_2 & x_2^2 & x_2^3 & x_2^4 & x_2^5 \\ 1 & x_3 & x_3^2 & x_3^3 & x_3^4 & x_3^5 \\ 1 & x_4 & x_4^2 & x_4^3 & x_4^4 & x_4^5 \\ 1 & x_5 & x_5^2 & x_5^3 & x_5^4 & x_5^5 \\ 1 & x_6 & x_6^2 & x_6^3 & x_6^4 & x_6^5 \end{vmatrix}$$

$$
= \begin{vmatrix}
1 & x_1 & x_1^2 & x_1^3 & x_1^4 & x_1^5 \\
0 & x_2 - x_1 & x_2^2 - x_1^2 & x_2^3 - x_1^3 & x_2^4 - x_1^4 & x_2^5 - x_1^5 \\
0 & x_3 - x_1 & x_3^2 - x_1^2 & x_3^3 - x_1^3 & x_3^4 - x_1^4 & x_3^5 - x_1^5 \\
0 & x_4 - x_1 & x_4^2 - x_1^2 & x_4^3 - x_1^3 & x_4^4 - x_1^4 & x_4^5 - x_1^5 \\
0 & x_5 - x_1 & x_5^2 - x_1^2 & x_5^3 - x_1^3 & x_5^4 - x_1^4 & x_5^5 - x_1^5 \\
0 & x_6 - x_1 & x_6^2 - x_1^2 & x_6^3 - x_1^3 & x_6^4 - x_1^4 & x_6^5 - x_1^5
\end{vmatrix}
$$

$$
\Big(\text{第 2 行, 第 3 行, 第 4 行, 第 5 行, 第 6 行から第 1 行をそれぞれ引く.}\Big)
$$

$$
= \begin{vmatrix}
\underline{x_2 - x_1} & x_2^2 - x_1^2 & x_2^3 - x_1^3 & x_2^4 - x_1^4 & x_2^5 - x_1^5 \\
\underline{x_3 - x_1} & x_3^2 - x_1^2 & x_3^3 - x_1^3 & x_3^4 - x_1^4 & x_3^5 - x_1^5 \\
\underline{x_4 - x_1} & x_4^2 - x_1^2 & x_4^3 - x_1^3 & x_4^4 - x_1^4 & x_4^5 - x_1^5 \\
\underline{x_5 - x_1} & x_5^2 - x_1^2 & x_5^3 - x_1^3 & x_5^4 - x_1^4 & x_5^5 - x_1^5 \\
\underline{x_6 - x_1} & x_6^2 - x_1^2 & x_6^3 - x_1^3 & x_6^4 - x_1^4 & x_6^5 - x_1^5
\end{vmatrix}
\quad \Big(\text{第 1 列でラプラス展開.}\Big)
$$

$$
= (x_2 - x_1)(x_3 - x_1)(x_4 - x_1)(x_5 - x_1)(x_6 - x_1)
$$

$$
\times \begin{vmatrix}
1 & x_2 + x_1 & x_2^2 + x_2 x_1 + x_1^2 & x_2^3 + x_2^2 x_1 + x_2 x_1^2 + x_1^3 & x_2^4 + x_2^3 x_1 + x_2^2 x_1^2 + x_2 x_1^3 + x_1^4 \\
1 & x_3 + x_1 & x_3^2 + x_3 x_1 + x_1^2 & x_3^3 + x_3^2 x_1 + x_3 x_1^2 + x_1^3 & x_3^4 + x_3^3 x_1 + x_3^2 x_1^2 + x_3 x_1^3 + x_1^4 \\
1 & x_4 + x_1 & x_4^2 + x_4 x_1 + x_1^2 & x_4^3 + x_4^2 x_1 + x_4 x_1^2 + x_1^3 & x_4^4 + x_4^3 x_1 + x_4^2 x_1^2 + x_4 x_1^3 + x_1^4 \\
1 & x_5 + x_1 & x_5^2 + x_5 x_1 + x_1^2 & x_5^3 + x_5^2 x_1 + x_5 x_1^2 + x_1^3 & x_5^4 + x_5^3 x_1 + x_5^2 x_1^2 + x_5 x_1^3 + x_1^4 \\
1 & x_6 + x_1 & x_6^2 + x_6 x_1 + x_1^2 & x_6^3 + x_6^2 x_1 + x_6 x_1^2 + x_1^3 & x_6^4 + x_6^3 x_1 + x_6^2 x_1^2 + x_6 x_1^3 + x_1^4
\end{vmatrix}
$$

$$
\left(\begin{array}{l}
\text{第 1 行から } (x_2 - x_1)\text{, 第 2 行から } (x_3 - x_1)\text{, 第 3 行から } (x_4 - x_1)\text{,} \\
\text{第 4 行から } (x_5 - x_1)\text{, 第 5 行から } (x_6 - x_1) \text{ をそれぞれくくり出す.}
\end{array}\right)
$$

<u>以下、上記の手順を繰り返す.</u>

$$
= (x_2 - x_1)(x_3 - x_1)(x_4 - x_1)(x_5 - x_1)(x_6 - x_1)
$$

$$
\times \left|\begin{matrix}
1 & x_2 + x_1 & x_2^2 + x_2 x_1 + x_1^2 & x_2^3 + x_2^2 x_1 + x_2 x_1^2 + x_1^3 \\
0 & x_3 - x_2 & (x_3 - x_2)(x_3 + x_2 + x_1) & (x_3 - x_2)(x_3^2 + x_2^2 + x_1^2 + x_1 x_2 + x_1 x_3 + x_2 x_3) \\
0 & x_4 - x_2 & (x_4 - x_2)(x_4 + x_2 + x_1) & (x_4 - x_2)(x_4^2 + x_2^2 + x_1^2 + x_1 x_2 + x_1 x_4 + x_2 x_4) \\
0 & x_5 - x_2 & (x_5 - x_2)(x_5 + x_2 + x_1) & (x_5 - x_2)(x_5^2 + x_2^2 + x_1^2 + x_1 x_2 + x_1 x_5 + x_2 x_5) \\
0 & x_6 - x_2 & (x_6 - x_2)(x_6 + x_2 + x_1) & (x_6 - x_2)(x_6^2 + x_2^2 + x_1^2 + x_1 x_2 + x_1 x_6 + x_2 x_6)
\end{matrix}\right.
$$

$$
\left.\begin{matrix}
x_2^4 + x_2^3 x_1 + x_2^2 x_1^2 + x_2 x_1^3 + x_1^4 \\
(x_3 - x_2)\big((x_3^2 + x_2^2 + x_1^2)(x_1 + x_2 + x_3) + x_1 x_2 x_3\big) \\
(x_4 - x_2)\big((x_4^2 + x_2^2 + x_1^2)(x_1 + x_2 + x_4) + x_1 x_2 x_4\big) \\
(x_5 - x_2)\big((x_5^2 + x_2^2 + x_1^2)(x_1 + x_2 + x_5) + x_1 x_2 x_5\big) \\
(x_6 - x_2)\bigl((x_6^2 + x_2^2 + x_1^2)(x_1 + x_2 + x_6) + x_1 x_2 x_6 |
\end{matrix}\right|
$$

$$
\begin{aligned}
= \quad & (x_2-x_1)(x_3-x_1)(x_4-x_1)(x_5-x_1)(x_6-x_1) \\
\times & \left| \begin{array}{llll}
\underline{x_3-x_2} & (x_3-x_2)(x_3+x_2+x_1) & (x_3-x_2)(x_3^2+x_2^2+x_1^2+x_1x_2+x_1x_3+x_2x_3) & (x_3-x_2)\left((x_3^2+x_2^2+x_1^2)(x_1+x_2+x_3)+x_1x_2x_3\right) \\
\underline{x_4-x_2} & (x_4-x_2)(x_4+x_2+x_1) & (x_4-x_2)(x_4^2+x_2^2+x_1^2+x_1x_2+x_1x_4+x_2x_4) & (x_4-x_2)\left((x_4^2+x_2^2+x_1^2)(x_1+x_2+x_4)+x_1x_2x_4\right) \\
\underline{x_5-x_2} & (x_5-x_2)(x_5+x_2+x_1) & (x_5-x_2)(x_5^2+x_2^2+x_1^2+x_1x_2+x_1x_5+x_2x_5) & (x_5-x_2)\left((x_5^2+x_2^2+x_1^2)(x_1+x_2+x_5)+x_1x_2x_5\right) \\
\underline{x_6-x_2} & (x_6-x_2)(x_6+x_2+x_1) & (x_6-x_2)(x_6^2+x_2^2+x_1^2+x_1x_2+x_1x_6+x_2x_6) & (x_6-x_2)\left((x_6^2+x_2^2+x_1^2)(x_1+x_2+x_6)+x_1x_2x_6\right)
\end{array} \right|
\end{aligned}
$$

$$
\begin{aligned}
= \quad & (x_2-x_1)(x_3-x_1)(x_4-x_1)(x_5-x_1)(x_6-x_1) \\
& \times(x_3-x_2)(x_4-x_2)(x_5-x_2)(x_6-x_2) \\
\times & \left| \begin{array}{llll}
1 & x_3+x_2+x_1 & x_3^2+x_2^2+x_1^2+x_1x_2+x_1x_3+x_2x_3 & (x_3^2+x_2^2+x_1^2)(x_1+x_2+x_3)+x_1x_2x_3 \\
1 & x_4+x_2+x_1 & x_4^2+x_2^2+x_1^2+x_1x_2+x_1x_4+x_2x_4 & (x_4^2+x_2^2+x_1^2)(x_1+x_2+x_4)+x_1x_2x_4 \\
1 & x_5+x_2+x_1 & x_5^2+x_2^2+x_1^2+x_1x_2+x_1x_5+x_2x_5 & (x_5^2+x_2^2+x_1^2)(x_1+x_2+x_5)+x_1x_2x_5 \\
1 & x_6+x_2+x_1 & x_6^2+x_2^2+x_1^2+x_1x_2+x_1x_6+x_2x_6 & (x_6^2+x_2^2+x_1^2)(x_1+x_2+x_6)+x_1x_2x_6
\end{array} \right|
\end{aligned}
$$

$$
\begin{aligned}
= \quad & (x_2-x_1)(x_3-x_1)(x_4-x_1)(x_5-x_1)(x_6-x_1) \\
& \times(x_3-x_2)(x_4-x_2)(x_5-x_2)(x_6-x_2) \\
\times & \left| \begin{array}{cccc}
1 & x_3+x_2+x_1 & x_3^2+x_2^2+x_1^2+x_1x_2+x_1x_3+x_2x_3 & (x_3^2+x_2^2+x_1^2)(x_1+x_2+x_3)+x_1x_2x_3 \\
0 & x_4-x_3 & (x_4-x_3)(x_4+x_3+x_2+x_1) & (x_4-x_3)\left(x_4^2+x_3^2+x_2^2+x_1^2+x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4\right) \\
0 & x_5-x_3 & (x_5-x_3)(x_5+x_3+x_2+x_1) & (x_5-x_3)\left(x_5^2+x_3^2+x_2^2+x_1^2+x_1x_2+x_1x_3+x_1x_5+x_2x_3+x_2x_5+x_3x_5\right) \\
0 & x_6-x_3 & (x_6-x_3)(x_6+x_3+x_2+x_1) & (x_6-x_3)\left(x_6^2+x_3^2+x_2^2+x_1^2+x_1x_2+x_1x_3+x_1x_6+x_2x_3+x_2x_6+x_3x_6\right)
\end{array} \right|
\end{aligned}
$$

$$
\begin{aligned}
= \quad & (x_2-x_1)(x_3-x_1)(x_4-x_1)(x_5-x_1)(x_6-x_1) \\
& \times(x_3-x_2)(x_4-x_2)(x_5-x_2)(x_6-x_2)
\end{aligned}
$$

$$
\times \begin{vmatrix}
\underline{x_4-x_3} & (x_4-x_3)(x_4+x_3+x_2+x_1) & (x_4-x_3)\left(x_4^2+x_3^2+x_2^2+x_1^2+x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4\right) \\
\underline{x_5-x_3} & (x_5-x_3)(x_5+x_3+x_2+x_1) & (x_5-x_3)\left(x_5^2+x_3^2+x_2^2+x_1^2+x_1x_2+x_1x_3+x_1x_5+x_2x_3+x_2x_5+x_3x_5\right) \\
\underline{x_6-x_3} & (x_6-x_3)(x_6+x_3+x_2+x_1) & (x_6-x_3)\left(x_6^2+x_3^2+x_2^2+x_1^2+x_1x_2+x_1x_3+x_1x_6+x_2x_3+x_2x_6+x_3x_6\right)
\end{vmatrix}
$$

$$
\begin{aligned}
= \quad & (x_2-x_1)(x_3-x_1)(x_4-x_1)(x_5-x_1)(x_6-x_1) \\
& \times(x_3-x_2)(x_4-x_2)(x_5-x_2)(x_6-x_2) \\
& \times(x_4-x_3)(x_5-x_3)(x_6-x_3)
\end{aligned}
$$

$$
\times \begin{vmatrix}
1 & x_4+x_3+x_2+x_1 & x_4^2+x_3^2+x_2^2+x_1^2+x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4 \\
1 & x_5+x_3+x_2+x_1 & x_5^2+x_3^2+x_2^2+x_1^2+x_1x_2+x_1x_3+x_1x_5+x_2x_3+x_2x_5+x_3x_5 \\
1 & x_6+x_3+x_2+x_1 & x_6^2+x_3^2+x_2^2+x_1^2+x_1x_2+x_1x_3+x_1x_6+x_2x_3+x_2x_6+x_3x_6
\end{vmatrix}
$$

$$
\begin{aligned}
= \quad & (x_2-x_1)(x_3-x_1)(x_4-x_1)(x_5-x_1)(x_6-x_1) \\
& \times(x_3-x_2)(x_4-x_2)(x_5-x_2)(x_6-x_2) \\
& \times(x_4-x_3)(x_5-x_3)(x_6-x_3)
\end{aligned}
$$

$$
\times \begin{vmatrix}
1 & x_4+x_3+x_2+x_1 & x_4^2+x_3^2+x_2^2+x_1^2+x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4 \\
0 & x_5-x_4 & (x_5-x_4)(x_5+x_4+x_3+x_2+x_1) \\
0 & x_6-x_4 & (x_6-x_4)(x_6+x_4+x_3+x_2+x_1)
\end{vmatrix}
$$

$$
\begin{aligned}
= \quad & (x_2-x_1)(x_3-x_1)(x_4-x_1)(x_5-x_1)(x_6-x_1) \\
& \times(x_3-x_2)(x_4-x_2)(x_5-x_2)(x_6-x_2) \\
& \times(x_4-x_3)(x_5-x_3)(x_6-x_3)
\end{aligned}
$$

$$
\times \begin{vmatrix}
\underline{x_5-x_4} & (x_5-x_4)(x_5+x_4+x_3+x_2+x_1) \\
\underline{x_6-x_4} & (x_6-x_4)(x_6+x_4+x_3+x_2+x_1)
\end{vmatrix}
$$

$$
\begin{aligned}
= \quad & (x_2-x_1)(x_3-x_1)(x_4-x_1)(x_5-x_1)(x_6-x_1) \times \begin{vmatrix}
1 & x_5+x_4+x_3+x_2+x_1 \\
1 & x_6+x_4+x_3+x_2+x_1
\end{vmatrix} \\
& \times(x_3-x_2)(x_4-x_2)(x_5-x_2)(x_6-x_2) \\
& \times(x_4-x_3)(x_5-x_3)(x_6-x_3) \\
& \times(x_5-x_4)(x_6-x_4)
\end{aligned}
$$

$$
\begin{aligned}
= \quad & (x_2-x_1)(x_3-x_1)(x_4-x_1)(x_5-x_1)(x_6-x_1) \times \begin{vmatrix} 1 & x_5+x_4+x_3+x_2+x_1 \\ 0 & x_6-x_5 \end{vmatrix} \\
& \qquad \times(x_3-x_2)(x_4-x_2)(x_5-x_2)(x_6-x_2) \\
& \qquad\qquad \times(x_4-x_3)(x_5-x_3)(x_6-x_3) \\
& \qquad\qquad\qquad \times(x_5-x_4)(x_6-x_4)
\end{aligned}
$$

$$
\begin{aligned}
= \quad & (x_2-x_1)(x_3-x_1)(x_4-x_1)(x_5-x_1)(x_6-x_1) \\
& \qquad \times(x_3-x_2)(x_4-x_2)(x_5-x_2)(x_6-x_2) \\
& \qquad\qquad \times(x_4-x_3)(x_5-x_3)(x_6-x_3) \\
& \qquad\qquad\qquad \times(x_5-x_4)(x_6-x_4) \\
& \qquad\qquad\qquad\qquad \times(x_6-x_5)
\end{aligned}
$$

となる。従って、行列式の値

$$
\det D = \alpha^{i_1+i_2+i_3+i_4+i_5+i_6} \det D' = \alpha^{i_1+i_2+i_3+i_4+i_5+i_6} \prod_{1 \le k < l \le 6} (\alpha^{i_l} - \alpha^{i_k})
$$

を得る。

評価基準　解答例に準じた解答であれば 2 点。なお、$\alpha^{i_1+i_2+i_3+i_4+i_5+i_6}$ をくくり出せていれば部分点 1 点。計算が不十分な解答は減点 1 点。

問 2　3 個の誤りが訂正可能な [15,5]BCH 符号について、以下の (1)〜(3) の問いに答えなさい ($m=4$, $t=3$)。ただし、$\mathrm{GF}(2^4)$ の原始多項式を x^4+x+1 とし、α をその根とする。計算過程も記述すること。

(1) 生成多項式 $G(x)$ を求めなさい。ただし、展開した形で答えること。(1 点)
ヒント：$\alpha^{15}=1$ を上手に使う。

解答例　生成多項式は $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$ を根にもつから、

$$
\begin{aligned}
&\alpha^{1\cdot 2^0} = \alpha, && \alpha^{3\cdot 2^0} = \alpha^3, && \alpha^{5\cdot 2^0} = \alpha^5, \\
&\alpha^{1\cdot 2^1} = \alpha^2, && \alpha^{3\cdot 2^1} = \alpha^6, && \alpha^{5\cdot 2^1} = \alpha^{10}, \\
&\alpha^{1\cdot 2^2} = \alpha^4, && \alpha^{3\cdot 2^2} = \alpha^{12}, && \\
&\alpha^{1\cdot 2^3} = \alpha^8, && \alpha^{3\cdot 2^3} = \alpha^9 &&
\end{aligned}
$$

も根となる。したがって、$\alpha, \alpha^3, \alpha^5$ の最小多項式は

$$
\begin{aligned}
M_1(x) &= (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8) \\
M_3(x) &= (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9) \\
M_5(x) &= (x-\alpha^5)(x-\alpha^{10})
\end{aligned}
$$

となる。ゆえに、生成多項式は

$$
\begin{aligned}
G(x) &= \mathrm{LCM}[M_1(x), M_3(x), M_5(x)] \\
&= (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^5)(x-\alpha^6)(x-\alpha^8)(x-\alpha^9)(x-\alpha^{10})(x-\alpha^{12}) \\
&= (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)(x+\alpha^5)(x+\alpha^6)(x+\alpha^8)(x+\alpha^9)(x+\alpha^{10})(x+\alpha^{12})
\end{aligned}
$$

となる。生成多項式を計算する ($\alpha^4+\alpha+1=0$, $\alpha^{15}=1$)：

$$\begin{cases} (x+\alpha)(x+\alpha^4) &= x^2+(\alpha+\alpha^4)x+\alpha^5 \\ &= x^2+x+\alpha^5 \\ \\ (x+\alpha^2)(x+\alpha^8) &= x^2+(\alpha^2+\alpha^8)x+\alpha^{10} \\ &= x^2+x+\alpha^{10} \\ \\ (x+\alpha^6)(x+\alpha^9) &= x^2+(\alpha^6+\alpha^9)x+\alpha^{15} \\ &= x^2+\alpha^5 x+1 \\ \\ (x+\alpha^3)(x+\alpha^{12}) &= x^2+(\alpha^3+\alpha^{12})x+\alpha^{15} \\ &= x^2+\alpha^{10}x+1 \\ \\ (x+\alpha^5)(x+\alpha^{10}) &= x^2+(\alpha^5+\alpha^{10})x+\alpha^{15} \\ &= x^2+x+1 \end{cases}$$

$$\begin{cases} (x^2+x+\alpha^5)(x^2+x+\alpha^{10}) &= x^4+(1+1)x^3+(1+\alpha^5+\alpha^{10})x^2+(\alpha^5+\alpha^{10})x+1 \\ &= x^4+x+1 \\ \\ (x^2+\alpha^5 x+1)(x^2+\alpha^{10}x+1) &= x^4+(\alpha^5+\alpha^{10})x^3+(1+1+\alpha^{15})x^2+(\alpha^5+\alpha^{10})x+1 \\ &= x^4+x^3+x^2+x+1 \\ \\ x^2+x+1 \end{cases}$$

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

$$\begin{aligned} (x^6+x^4+x^3+x^2+1)(x^4+x+1) &= x^{10}+x^8+x^7+x^6+x^4 \\ &\quad +x^7+x^5+x^4+x^3+x \\ &\quad +x^6+x^4+x^3+x^2+1 \\ &= x^{10}+x^8+x^5+x^4+x^2+x+1. \end{aligned}$$

以上より、生成多項式

$$G(x)=1+x+x^2+x^4+x^5+x^8+x^{10}$$

を得る。

なお、GF(2^4) の元の演算は下記の表を使って行なった。

べき表現	展開
α^0	1
α^1	α
α^2	α^2
α^3	α^3
α^4	$1+\alpha$
α^5	$\alpha+\alpha^2$
α^6	$\alpha^2+\alpha^3$
α^7	$1+\alpha+\alpha^3$
α^8	$1+\alpha^2$
α^9	$\alpha+\alpha^3$
α^{10}	$1+\alpha+\alpha^2$
α^{11}	$\alpha+\alpha^2+\alpha^3$
α^{12}	$1+\alpha+\alpha^2+\alpha^3$
α^{13}	$1+\alpha^2+\alpha^3$
α^{14}	$1+\alpha^3$

$$\begin{aligned}
\alpha+\alpha^4 &= (\alpha)+(1+\alpha) = 1\\
\alpha^2+\alpha^8 &= (\alpha^2)+(1+\alpha^2) = 1\\
\alpha^6+\alpha^9 &= (\alpha^2+\alpha^3)+(\alpha+\alpha^3) = \alpha+\alpha^2 = \alpha^5\\
\alpha^3+\alpha^{12} &= (\alpha^3)+(1+\alpha+\alpha^2+\alpha^3) = 1+\alpha+\alpha^2 = \alpha^{10}\\
\alpha^5+\alpha^{10} &= (\alpha+\alpha^2)+(1+\alpha+\alpha^2) = 1
\end{aligned}$$

評価基準　解答例に準じた解答であれば 1 点。計算が不十分な解答は 0 点。

(2) 誤り位置を求めるための $\sigma_1, \sigma_2, \sigma_3$ を変数とする連立 1 次方程式を求めなさい。ただし、誤り位置多項式は

$$\sigma(x) = x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3$$

とする。(1 点)

解答例　[15,5]BCH 符号のシンドロームは

$$S_i = Y(\alpha^i) = y_0 + y_1 x + y_2 x^2 + \cdots + y_{14} x^{14}, \qquad (i = 1,2,3,4,5,6)$$

と定義できる。3 個の誤りが訂正可能であるから、k_1, k_2, k_3 成分に誤りがあったと仮定する。このとき、シンドロームは

$$\begin{cases}
S_1 = Y(\alpha^1) = (\alpha^{k_1})^1 + (\alpha^{k_2})^1 + (\alpha^{k_3})^1\\
S_2 = Y(\alpha^2) = (\alpha^{k_1})^2 + (\alpha^{k_2})^2 + (\alpha^{k_3})^2 = S_1^2\\
S_3 = Y(\alpha^3) = (\alpha^{k_1})^3 + (\alpha^{k_2})^3 + (\alpha^{k_3})^3\\
S_4 = Y(\alpha^4) = (\alpha^{k_1})^4 + (\alpha^{k_2})^4 + (\alpha^{k_3})^4 = S_2^2\\
S_5 = Y(\alpha^5) = (\alpha^{k_1})^5 + (\alpha^{k_2})^5 + (\alpha^{k_3})^5\\
S_6 = Y(\alpha^6) = (\alpha^{k_1})^6 + (\alpha^{k_2})^6 + (\alpha^{k_3})^6 = S_3^2
\end{cases}$$

となる。また、誤り位置多項式は

$$\begin{aligned}\sigma(x) &= (x-\alpha^{k_1})(x-\alpha^{k_2})(x-\alpha^{k_3}) \\ &= x^2-(\alpha^{k_1}+\alpha^{k_2}+\alpha^{k_3})x^2+(\alpha^{k_1}\alpha^{k_2}+\alpha^{k_2}\alpha^{k_3}+\alpha^{k_3}\alpha^{k_1})x-\alpha^{k_1}\alpha^{k_2}\alpha^{k_3} \\ &= x^2+(\alpha^{k_1}+\alpha^{k_2}+\alpha^{k_3})x^2+(\alpha^{k_1}\alpha^{k_2}+\alpha^{k_2}\alpha^{k_3}+\alpha^{k_3}\alpha^{k_1})x+\alpha^{k_1}\alpha^{k_2}\alpha^{k_3} \\ &= x^3+\sigma_1x^2+\sigma_2x+\sigma_3\end{aligned}$$

$$\Longleftrightarrow \qquad \begin{cases}\sigma_1=\alpha^{k_1}+\alpha^{k_2}+\alpha^{k_3} \\ \sigma_2=\alpha^{k_1}\alpha^{k_2}+\alpha^{k_2}\alpha^{k_3}+\alpha^{k_3}\alpha^{k_1} \\ \sigma_3=\alpha^{k_1}\alpha^{k_2}\alpha^{k_3}\end{cases}$$

であるから、関係式

$$S_1=\alpha^{k_1}+\alpha^{k_2}+\alpha^{k_3}=\sigma_1,$$

$$\begin{aligned}S_2\sigma_1 &= ((\alpha^{k_1})^2+(\alpha^{k_2})^2+(\alpha^{k_3})^2)(\alpha^{k_1}+\alpha^{k_2}+\alpha^{k_3}) \\ &= (\alpha^{k_1})^3+(\alpha^{k_2})^3+(\alpha^{k_3})^3 \\ &\quad +(\alpha^{k_1}+\alpha^{k_2}+\alpha^{k_3})(\alpha^{k_1}\alpha^{k_2}+\alpha^{k_2}\alpha^{k_3}+\alpha^{k_3}\alpha^{k_1})+\alpha^{k_1}\alpha^{k_2}\alpha^{k_3} \\ &= S_3+S_1\sigma_2+\sigma_3,\end{aligned}$$

$$\begin{aligned}S_4\sigma_1 &= ((\alpha^{k_1})^4+(\alpha^{k_2})^4+(\alpha^{k_3})^4)(\alpha^{k_1}+\alpha^{k_2}+\alpha^{k_3}) \\ &= (\alpha^{k_1})^5+(\alpha^{k_2})^5+(\alpha^{k_3})^5 \\ &\quad +((\alpha^{k_1})^3+(\alpha^{k_2})^3+(\alpha^{k_3})^3)(\alpha^{k_1}\alpha^{k_2}+\alpha^{k_2}\alpha^{k_3}+\alpha^{k_3}\alpha^{k_1}) \\ &\quad\quad +((\alpha^{k_1})^2+(\alpha^{k_2})^2+(\alpha^{k_3})^2)(\alpha^{k_1}\alpha^{k_2}\alpha^{k_3}) \\ &= S_5+S_3\sigma_2+S_2\sigma_3\end{aligned}$$

を満たす。よって、誤り位置を求めるための $\sigma_1, \sigma_2, \sigma_3$ の連立 1 次方程式は

$$\begin{cases}S_1+\sigma_1=0 \\ S_3+S_2\sigma_1+S_1\sigma_2+\sigma_3=0 \\ S_5+S_4\sigma_1+S_3\sigma_2+S_2\sigma_3=0\end{cases}$$

となる。

評価基準　解答例に準じた解答であれば 1 点。

(3) (2) を使って、受信語 $\boldsymbol{y}=(0,1,0,1,0,0,0,0,1,1,1,0,0,0,0)$ の誤りを訂正なさい。(2 点)
ヒント：誤り位置は α^{12}, α^{13} の 2 つ。

解答例　受信語 $\boldsymbol{y}$ の多項式表現は

$$Y(x)=x+x^3+x^8+x^9+x^{10}$$

であるから、シンドロームを計算すると、

$$\begin{cases}S_1=Y(\alpha^1)=\alpha+\alpha^3+\alpha^8+\alpha^9+\alpha^{10}=\alpha \\ S_2=Y(\alpha^2)=S_1^2=\alpha^2 \\ S_3=Y(\alpha^3)=(\alpha^3)+(\alpha^3)^3+(\alpha^3)^8+(\alpha^3)^9+(\alpha^3)^{10}=\alpha^5 \\ S_4=Y(\alpha^4)=S_2^2=\alpha^4 \\ S_5=Y(\alpha^5)=(\alpha^5)+(\alpha^5)^3+(\alpha^5)^8+(\alpha^5)^9+(\alpha^5)^{10}=\alpha^{10} \\ S_6=Y(\alpha^6)=S_3^2=\alpha^{10}\end{cases}$$

となる。従って、(2) で求めた連立 1 次方程式にこれらを代入すると、

$$\begin{cases} \alpha + \sigma_1 = 0 \\ \alpha^5 + \alpha^2\sigma_1 + \alpha\sigma_2 + \sigma_3 = 0 \\ \alpha^{10} + \alpha^4\sigma_1 + \alpha^5\sigma_2 + \alpha^2\sigma_3 = 0 \end{cases}$$

となり、これを解くと

$$\begin{cases} \sigma_1 = \alpha \\ \sigma_2 = \alpha^{10} \\ \sigma_3 = 0 \end{cases}$$

となる。ゆえに、誤り位置多項式は

$$\sigma(x) = x^3 + \alpha x^2 + \alpha^{10}x \qquad \leftarrow \text{誤りが 2 個であることがわかる}$$

となるので、GF(2^4) の元を順次代入し誤り位置を見つける：

$$\begin{aligned}
\sigma(\alpha^0) &= 1^3 + \alpha \cdot 1^2 + \alpha^{10} \cdot 1 = \alpha^2, \\
\sigma(\alpha^1) &= \alpha^3 + \alpha \cdot \alpha^2 + \alpha^{10} \cdot \alpha = \alpha^{11}, \\
\sigma(\alpha^2) &= (\alpha^2)^3 + \alpha(\alpha^2)^2 + \alpha^{10}(\alpha^2) = \alpha^8, \\
\sigma(\alpha^3) &= (\alpha^3)^3 + \alpha(\alpha^3)^2 + \alpha^{10}(\alpha^3) = \alpha^6, \\
\sigma(\alpha^4) &= (\alpha^4)^3 + \alpha(\alpha^4)^2 + \alpha^{10}(\alpha^4) = \alpha^6, \\
\sigma(\alpha^5) &= (\alpha^5)^3 + \alpha(\alpha^5)^2 + \alpha^{10}(\alpha^5) = \alpha^{11}, \\
\sigma(\alpha^6) &= (\alpha^6)^3 + \alpha(\alpha^6)^2 + \alpha^{10}(\alpha^6) = \alpha^{10}, \\
\sigma(\alpha^7) &= (\alpha^7)^3 + \alpha(\alpha^7)^2 + \alpha^{10}(\alpha^7) = \alpha^{14}, \\
\sigma(\alpha^8) &= (\alpha^8)^3 + \alpha(\alpha^8)^2 + \alpha^{10}(\alpha^8) = \alpha^5, \\
\sigma(\alpha^9) &= (\alpha^9)^3 + \alpha(\alpha^9)^2 + \alpha^{10}(\alpha^9) = \alpha^{12}, \\
\sigma(\alpha^{10}) &= (\alpha^{10})^3 + \alpha(\alpha^{10})^2 + \alpha^{10}(\alpha^{10}) = \alpha^7, \\
\sigma(\alpha^{11}) &= (\alpha^{11})^3 + \alpha(\alpha^{11})^2 + \alpha^{10}(\alpha^{11}) = 1, \\
\sigma(\alpha^{12}) &= (\alpha^{12})^3 + \alpha(\alpha^{12})^2 + \alpha^{10}(\alpha^{12}) = 0, \\
\sigma(\alpha^{13}) &= (\alpha^{13})^3 + \alpha(\alpha^{13})^2 + \alpha^{10}(\alpha^{13}) = 0, \\
\sigma(\alpha^{14}) &= (\alpha^{14})^3 + \alpha(\alpha^{14})^2 + \alpha^{10}(\alpha^{14}) = \alpha^6.
\end{aligned}$$

以上より、誤り位置が α^{12} および α^{13} であることがわかる。従って、0 から数えて 12 番目と 13 番目の成分の 0 と 1 を入れ替え、誤りを訂正する。すなわち、受信語 $\boldsymbol{y}$ の推定情報

$$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, \underline{1}, \underline{1}, 0)$$

が得られる。

評価基準　解答例に準じた解答であれば 2 点。連立方程式が正しく解けていれば部分点 1 点。