環境数理モデル特論A（符号理論）

2016年８月８‐９日　於岡山大学環境理工学部

渡辺宏太郎　防衛大学校情報工学科教授

符号理論

通信路符号化定理は送信系列の長さを十分大きくとると，符号化率が通信路容量をオーバーしなければ復号誤り率を0に近づけることができるというものであった．

誤り訂正符号の理論は，上記のような符号の発見を目指している理論ともいえる．実際，ターボ符号，LDPC符号ごく最近ではポーラ符号などは上記の性質を近似的に備えている符号と言える（とはいえ復号法の問題などいろいろと問題は残っている）．

ここでは簡単な例から始めて最後にLDPC符号について触れてみたいと思います．

さて，誤り検出，誤り訂正符号を具体的に構成するために必要となる方法を与えるのが符号理論である．通信路上で，誤りの生じた受信系列から誤りを見出し，正しいデータを復元することを誤り訂正という．これに対して，受信系列に誤りが生じていることだけを検知することを誤り検出とよんでいる．

誤り訂正符号の研究は様々な数学が使われ面白い．この講義でも線形代数代数学で勉強する有限体，最短路問題等を解くために使われる動的計画法（ダイナミックプログラミング）が使われ，そのことの一端を感じることができるのではなかろうか．

線形符号

<u>定義</u>　$F=\{0,1\}$ とする．

符号$\mathcal{C}$　が線形符号　$\Leftrightarrow$　$\mathcal{C}$ が $V=F^n$ の k 次元線形部分空間のとき，
すなわち，任意の $a,b\in F$ に対して $au+bv\in\mathcal{C}$ のとき

ここでFは2元体で和と積が次をみたすものとする．
kは情報ビットの次元でnは符号長である．よって
符号化率R=k/nである．このような符号を(n, k)線形符号
という．　(n, k)線形符号は

$\mathbf{w}=\mathbf{a}G$と書ける．ここで$\mathbf{a}$は情報ビット系列，
$\mathbf{w}$はその符号化である．具体的には

$$(w_1,\ \cdots\ w_n)=(a_1,\cdots,a_k)\underbrace{\begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & & \vdots \\ g_{k1} & \cdots & g_{kn} \end{pmatrix}}_{G}$$

Gを生成行列という

となる．

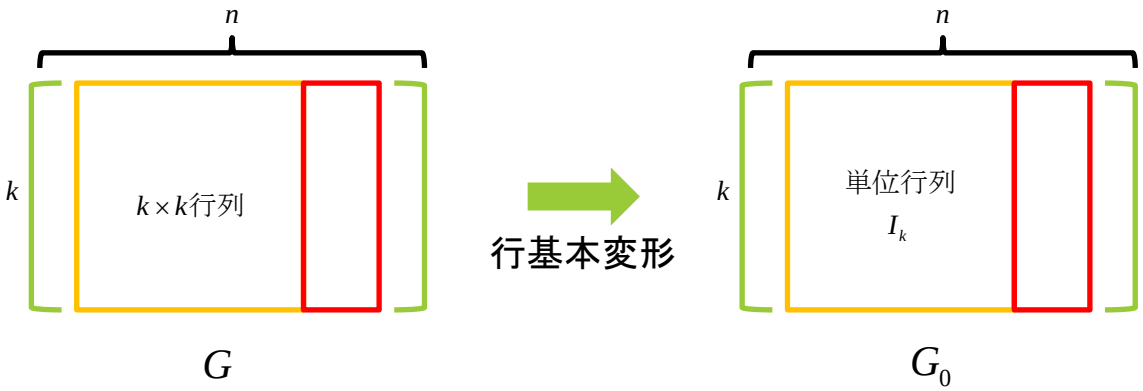
a	b	a+b	a･b
0	0	0	0
0	1	1	0
1	0	0	0
1	1	0	1

問24 符号長5の線形符号の生成行列を

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

とする．Gによって生成される線形符号$\mathcal{C}$を求めよ．

（答）　$\mathcal{C} = \{00000, 11000, 01101, 10110, 10101, 01110, 11011, 00011\}$



$$G=\begin{pmatrix}1&1&0&1&0&1\\0&1&1&0&1&0\\1&0&1&1&0&1\\1&1&1&0&1&1\end{pmatrix}\xrightarrow[\text{第4行に第1行を足す}]{\text{第3行に第1行を足す}}\begin{pmatrix}1&1&0&1&0&1\\0&1&1&0&1&0\\0&1&1&0&0&0\\0&0&1&1&1&0\end{pmatrix}\xrightarrow{\text{略}}\begin{pmatrix}1&0&0&0&0&1\\0&1&0&0&1&0\\0&0&1&0&1&0\\0&0&0&1&0&0\end{pmatrix}=G_0$$

第3行に第1行を足す行基本変形を表す行列をL_1，　第4行に第1行を足す行基本変形を表す行列をL_2とする．

$$L_1=\begin{pmatrix}1&&&\\&1&&\\1&&1&\\&&&1\end{pmatrix},\quad L_2=\begin{pmatrix}1&&&\\&1&&\\&&1&\\1&&&1\end{pmatrix},\quad L_1L_2=\begin{pmatrix}1&&&\\&1&&\\1&&1&\\1&&&1\end{pmatrix}$$ である．したがって

$$\mathbf{a}L_1L_2G=\mathbf{a}\begin{pmatrix}1&1&0&1&0&1\\0&1&1&0&1&0\\0&1&1&0&0&0\\0&0&1&1&1&0\end{pmatrix}$$ となり，$\mathbf{b}=\mathbf{a}L_1L_2$とおけばGと $\begin{pmatrix}1&1&0&1&0&1\\0&1&1&0&1&0\\0&1&1&0&0&0\\0&0&1&1&1&0\end{pmatrix}$

の生成する符号は同一ということがわかる．よってGとG_0の生成する符号も同一である．

線形代数の次元定理より $\boxed{F^n = \{0,1\}^n = \mathrm{Im}\,G \oplus \mathrm{Ker}G^T}$

ここで $\mathrm{Im}\,G = \left\{\mathbf{a}G \mid \mathbf{a} \in \{0,1\}^k\right\}$ （Gの像空間），$\mathrm{Ker}G^T = \left\{\mathbf{b} \in \{0,1\}^n \mid \mathbf{b}G^T = \mathbf{0}^k\right\}$

であり, $\mathrm{Im}\,G$と$\mathrm{Ker}G^T$はF^nの内積で直交する（$\mathbb{R}^n$や$\mathbb{C}^n$の場合と変わらない）

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$ の場合ならば $\mathrm{Im}\,G$は$(110101),(011010),(101101),(111011)$

の4つのGの行ベクトルで張られる4次元部分空間である．$\mathrm{Ker}G^T$は$n-k=2$次元の部分空間をなす．$\mathrm{Ker}G^T$の$n-k$次元分の基底を並べてできる行列をHと書きパリティチェック行列という．定義から$HG^T = \mathbf{O}$（$(n-k)\times k$零行列）

また$GH^T = \mathbf{O}$ （$k\times(n-k)$零行列）．

$G = G_0$の場合はHを求めることは簡単である．というのは$k\times(n-k)$行列Pを用いて

$$GH^T = \begin{pmatrix} I_k & P \end{pmatrix}\begin{pmatrix} P \\ I_{n-k} \end{pmatrix} = P + P = \mathbf{O}$$ （各成分の加算は2元体上のものだから）

よって$H = \begin{pmatrix} P^T & I_{n-k} \end{pmatrix}$

問25 (7,3) 線形符号の生成行列を

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

とする．Hを求めよ．

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

ハミング距離

定義　$\mathbf{a}=(a_1,\cdots,a_n)$, $\mathbf{b}=(b_1,\cdots,b_n)$とする．ここで$a_i,b_i\in\{0,1\}$, $(i=1,\cdots,n)$
$\mathbf{a}$と$\mathbf{b}$のハミング距離$d_H(\mathbf{a},\mathbf{b})$を成分毎に比較したとき，異なる箇所の数とする．

定義　（最小ハミング距離）2^k個の任意の2つの符号語$\mathbf{a}_i$と$\mathbf{a}_j$ $(i\neq j)$のハミング距離の最小値を最小距離d_{min}という．すなわち

$$d_{min}=\min_{i,j(i\neq j)} d_H(\mathbf{a}_i,\mathbf{a}_j)\ \ (\mathbf{a}_i,\mathbf{a}_j\in\mathcal{C})$$

このような符号$\mathcal{C}$を(n,k,d)符号という．

問26　$\mathcal{C}$の最小距離 ＝ $\mathcal{C}$の非零の符号語の最小重みが成り立つことを示せ．

問27　$\mathcal{C}$={0000, 00101, 00011, 00110, 11000, 11101, 11011, 11110}のとき最小距離を求めよ．

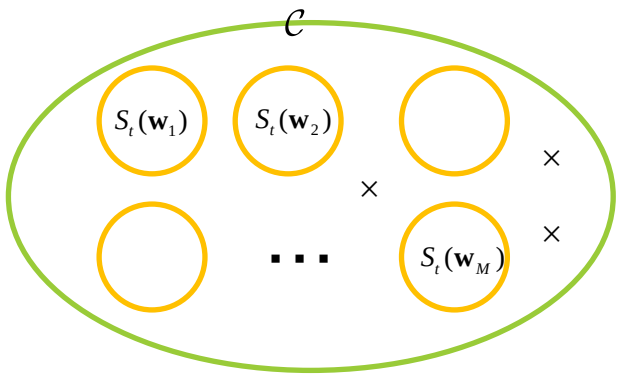
（8×7/2=28回計算しなくても済む）

限界距離復号法

$1 \le t \le \left\lfloor \dfrac{d_{min}-1}{2} \right\rfloor$とする．符号語$\mathbf{w}_i$を中心とする半径 t の球（ハミング球）を考える．

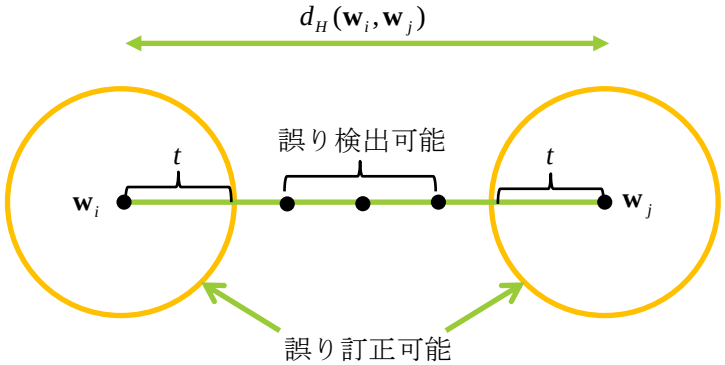
$$S_t(\mathbf{w}_i) := \left\{ \mathbf{x} \in \{0,1\}^n \mid d_H(\mathbf{w}_i, \mathbf{x}) \le t \right\} \ (i = 1, \cdots, M)$$

このとき，受信語$\mathbf{r}$が$S_t(\mathbf{w}_i)$に属していれば$\mathbf{w}_\mathbf{i}$に復号することにする．



×:どの$\mathbf{w}_\mathbf{i}$にも復号できない受信語

この訂正法を限界距離復号法という．またt個の誤りを訂正できることからt重誤り訂正という．限界距離復号法では一般にどの符号語にも復号できない受信語が存在する．それに対し最尤復号はハミング距離が最小となる符号語に復号するのでそのようなことは起こらない．



ハミング符号（1）

ハミング符号のパリティチェック行列は次の形をとる．

$$H = \overbrace{\begin{pmatrix} P^T & I_{n-k} \end{pmatrix}}^{\text{n}} \Big\updownarrow \text{n-k}$$

Hには全零以外の全てのn-k次元列ベクトルが現れるようにする．

$(n,k,d)=(7,4,3)$ならば

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

Hの列には全零以外の$(n-k)$次元ベクトルが現れるから$\mathbf{h_i}+\mathbf{h}_j+\mathbf{h_k}=\mathbf{0}$となるような3列が必ず存在する．よって最小ハミング重みは3，つまり最小距離=3となり1誤り訂正符号である．

ハミング符号（2）

ハミング符号は1誤り訂正符号である．$\mathbf{w}$を符号語，$\mathbf{e}$を（通信路における）エラー受信を$\mathbf{r}$とする．したがって$\mathbf{r}=\mathbf{w}+\mathbf{e}$が成り立つ．$GH^T=\mathbf{O}$が成り立っていたことを思い出そう．$\mathbf{a}$を情報ビット系列とすると$\mathbf{w}=\mathbf{a}G$であった．よって

$$\mathbf{w}H^T=\mathbf{a}GH^T=\mathbf{0}=(0,\cdots,0)\ \ (n-k\text{次元})$$

が成り立つ．したがって

$$\mathbf{r}H^T=(\mathbf{w}+\mathbf{e})H^T=\mathbf{w}H^T+\mathbf{e}H^T=\mathbf{0}+\mathbf{e}H^T=\mathbf{e}H^T$$

ここでエラーベクトル$\mathbf{e}$が$\mathbf{e}=\mathbf{e}_i=(0,\cdots,0,1,0,\cdots,0)$ (iビット目のみ1) という形をとるとしよう．このとき

$$\mathbf{r}H^T=\mathbf{e}H^T=\mathbf{e}_iH^T=(0,\cdots,0,1,0,\cdots,0)\begin{pmatrix}\mathbf{h}_1{}^T\\ \vdots\\ \mathbf{h}_n{}^T\end{pmatrix}=\mathbf{h}_i{}^T$$

$\mathbf{s}=\mathbf{h}_i{}^T$をシンドロームという．つまりHの$\mathbf{s}^T$とパターンマッチする列を探しそれが第i列であったら，$\mathbf{r}$に$\mathbf{e}_\mathbf{i}$を加えて$\mathbf{r}+\mathbf{e}_i=\mathbf{w}+\mathbf{e}_i+\mathbf{e}_i=\mathbf{w}$となって正しい符号語に訂正できる．

例 パリティ検査行列を

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

とする$(n,k,d)=(7,4,3)$ハミング符号を考える．

(1)情報ビット系列(1010)を符号化せよ．

(2)受信語=(1011011)であった．誤りがあれば訂正せよ．

(1)生成行列Gは

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

であるから$(1010)G=(1010011)$である．

(2) $\mathbf{s}=\mathbf{r}H^T=(1,1,1)$となり$H$の4列目の転置と一致する．よって$\mathbf{e}=\mathbf{e}_4=(0001000)$

したがって$\mathbf{w}=(1011011)+(0001000)=(1010011)$となり訂正により(1)の送信語が復号された．

問28 パリティ検査行列を

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

とする$(n,k,d)=(15,11,3)$ハミング符号を考える．

(1) 情報ビット系列(10100000000)を符号化せよ．

(2) 受信語=(101010000000101)であった．誤りがあれば訂正せよ．

短縮ハミング符号(1)

ハミング符号の符号語のうち特定のビットを削除した符号を短縮ハミング符号という．特にHの偶数重みをもつ列に対応するビットを削除すれば，符号語の最小重みは4以上となる．H中には奇数重みをもつ列しかないから奇数個の列を選んで足し合わせても**0**ベクトルにはできないからである．よって，そのような符号は1誤り訂正2誤り検出(SEC/DED符号，Single Error Correction/Double Error Detection)となる．サーバー機などのメモリにはこうしたSEC/DED符号が使われている．*ECC*メモリとよばれていて普通のメモリより少し値段が高い．誤り訂正能力が低いので通信路における符号としては使えないが復号遅延が少ないのでメモリの保護に使用される．

短縮ハミング符号（2）

問29　パリティ検査行列を

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

とする$(n,k,d)=(15,11,3)$ハミング符号の奇数重みをもつ列を除いてできた符号のパリティチェック行列を求めよ．できた符号は$(n,k,d)=(8,4,4)$符号になる．

ガロア体（有限体）（1）

巡回符号（BCH符号）の理解のためにはガロア体（有限体）の理解が必要である．加減乗除ができる数の集合を体という．有理数体，実数体，複素数体などは，要素数が無限であるが，要素数が有限の体（有限体）が情報分野では重要である．

体($Field$)の定義　$a,b,c \in F$とする．

(1)　$a+b \in F,\ a \cdot b \in F$

(2)　加法に関する性質（加法に関し可換群をなす）

(i) $a+(b+c)=(a+b)+c$　（結合法則), (ii) $a+0=0+a=a$となる$0 \in F$が存在（零元の存在）

(iii)　$a+(-a)=(-a)+a=0$となる$(-a)$の存在（加法についての逆元の存在）

(iv)　可換性　$a+b=b+a$

(3) 乗法に関する性質（$F \setminus \{0\}$は乗法に関し群をなす）

(i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$　（結合法則）,(ii) $1 \cdot a = a \cdot 1$となる$1 \in F$の存在（単位元の存在）

(iii) $a \neq 0$のとき，$a^{-1} \cdot a = a \cdot a^{-1} = 1$となる$a^{-1} \in F$の存在（乗法についての逆元の存在）

(iv)　可換性　$a \cdot b = b \cdot a$

(4) $(a+b) \cdot c = a \cdot c + b \cdot c,\ a \cdot (b+c) = a \cdot b + a \cdot c$　（分配法則）

ガロア体（有限体）（2）

2元体$GF(2)=\{0, 1\}$は表の演算で体となる位数（要素の数）最小の体である．$GF(p)$をpを法とする剰余がなす整数の集合とする．このときpが素数の場合には剰余がなす整数の集合は確かに体になるがpが合成数のときはそうはならない（下記の問題を参照）．そこで，規約なm次多項式の根を用いて$m = p^k$の場合は体（拡大体）$GF(p^k)$をつくるのである．

a	b	a+b	a･b
0	0	0	0
0	1	1	0
1	0	0	0
1	1	0	1

GF(2)の演算

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

･	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

GF(3)の演算

問30 4を法とする剰余ではガロア体はつくれないことを示せ．

既約多項式

F上のn次多項式

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \quad (a_n \neq 0)$$

が自分自身および1以外の多項式で割れないとき$f(x)$はF上で既約であるという．このような多項式を既約多項式という．

例　$f(x) = 2x^3 + x^2 + x - 1$ は有理数体$\mathbb{Q}$上既約でない．$f(x) = 2x^3 + x^2 + x - 1 = (2x-1)(x^2+x+1)$と因数分解できてしまうからである．

例　$f(x) = x^3 + x + 1$は$GF(2)$上既約である．$f(0) = 1, f(1) = 1$なので$x, (x-1)$を因数にもつことはない．

ガロア拡大体（1）

$f(x)=x^2-3$は[redacted]

とすると$\mathbb{Q}(\sqrt{3})=\left\{a+b\sqrt{3}\mid a,b\in\mathbb{Q}\right\}$となる．例えば$a+b\sqrt{3}$の逆元の存在は

$$\frac{1}{a+b\sqrt{3}}=\frac{b\sqrt{3}-a}{3b^2-a^2}=-\frac{a}{3b^2-a^2}+\frac{b}{3b^2-a^2}\sqrt{3}\in\mathbb{Q}(\sqrt{3})$$となるから保証される．

このように，ある体上の既約多項式の根を付加して得られる最小の体を拡大体という．

$GF(2)$上の既約多項式x^2+x+1の根αを$GF(2)$へ付加した拡大体を考える．これを$GF(2^2)$と書き，$GF(2)$の2次（ガロア）拡大体とよぶ.2次というのは，既約多項式の次数が2次だからである．

ガロア拡大体（2）

$GF(2)$上の既約多項式x^2+x+1の根αを$GF(2)$へ付加した拡大体を考える．これを$GF(2^2)$と書き，$GF(2)$の2次（ガロア）拡大体とよぶ.2次というのは，既約多項式の次数が2次だからである．

$GF(2^2)=\{a+b\alpha \mid a,b\in GF(2)\}=\{0,1,\alpha,1+\alpha\}$となる.$1+\alpha=\alpha^2$だから$GF(2^2)=\{0,1,\alpha,\alpha^2\}$と表すことができる．$GF(2^2)$の乗算と加算は表のようになっており乗算と加算について閉じていて，それぞれの演算の逆元の存在もわかるから確かに$GF(2^2)$は体になっている．例えばα^2の乗法に関する逆元はαである．

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

$\cdot$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

$GF(2^2)$の加算と乗算

ガロア拡大体（3）

$GF(2)$上の既約多項式x^3+x+1の根αを$GF(2)$へ付加した拡大体$GF(2^3)$を考える．

$GF(2^3)=\{0,1,\alpha,1+\alpha,\alpha^2,\alpha^2+1,\alpha^2+\alpha,\alpha^2+\alpha+1\}$である．しかし，$\alpha^3=\alpha+1,\alpha^4=\alpha^2+\alpha,$

$\alpha^5=\alpha^3+\alpha^2=\alpha^2+\alpha+1,\alpha^6=\alpha^2+1,\alpha^7=1$だから$GF(2^3)=\{0,1,\alpha,\alpha^3,\alpha^2,\alpha^6,\alpha^4,\alpha^5\}$と全て$\alpha$のべきで表すことができる．これを用いると$GF(2^3)$の乗算，加算表は次のようになり，やはり体になることがわかる．

$+$	0	1	α	α^2	α^3	α^4	α^5	α^6
0	0	1	α	α^2	α^3	α^4	α^5	α^6
1	1	0	α^3	α^6	α	α^5	α^4	α^2
α	α	α^3	0	α^4	1	α^2	α^6	α^5
α^2	α^2	α^6	α^4	0	α^5	α	α^3	1
α^3	α^3	α	1	α^5	0	α^6	α^2	α^4
α^4	α^4	α^5	α^2	α	α^6	0	1	α^3
α^5	α^5	α^4	α^6	α^3	α^2	1	0	α
α^6	α^6	α^2	α^5	1	α^4	α^3	α	0

$\cdot$	0	1	α	α^2	α^3	α^4	α^5	α^6
0	0	0	0	0	0	0	0	0
1	0	1	α	α^2	α^3	α^4	α^5	α^6
α	0	α	α^2	α^3	α^4	α^5	α^6	1
α^2	0	α^2	α^3	α^4	α^5	α^6	1	α
α^3	0	α^3	α^4	α^5	α^6	1	α	α^2
α^4	0	α^4	α^5	α^6	1	α	α^2	α^3
α^5	0	α^5	α^6	1	α	α^2	α^3	α^4
α^6	0	α^6	1	α	α^2	α^3	α^4	α^5

$GF(2^3)$の加算と乗算

原始既約多項式

$GF(2)$上の既約多項式x^2+x+1の根αを$GF(2)$へ付加した拡大体，$GF(2)$上の既約多項式x^3+x+1の根αを$GF(2)$へ付加した拡大体の例では拡大体の要素が全てαのべきで表されている．これは，既約多項式の根αを$GF(2)$へ付加した拡大体では必ず成立することなのだろうか？実はこれは正しくない．$f(x)=x^4+x^3+x^2+x+1$は$GF(2)$上の既約多項式であるがαを$f(x)=0$の根としたとき$\alpha^5=\alpha\cdot\alpha^4=\alpha\cdot(\alpha^3+\alpha^2+\alpha+1)=\alpha^4+\alpha^3+\alpha^2+\alpha=1$なので$\alpha^{2^4-1}=\alpha^{15}$にたどりつく前に1となって巡回してしまう．よって$GF(2^4)$の全ての要素を$\alpha$のべきで表すことはできない．

$\alpha^k=1$となるような最小の整数kをαの位数という．前の例では$\alpha^5=1$で初めて1になったからαの位数は5である．

$GF(2)$上の既約多項式x^2+x+1の根αを$GF(2)$へ付加した拡大体のように拡大体の全ての要素がαのべきで書けるとき，そのような既約多項式を原始既約多項式といい，αをその原始元という．$f(x)=x^4+x^3+x^2+x+1$を用いて$GF(2^4)$を構成することはできるが，$f(x)$は原始既約多項式でないので，逆元の計算をするときなど使い勝手が悪い．
$f(x)=x^4+x+1$は原始既約多項式となり，こちらを用いて$GF(2^4)$を構成する方がよい．

原始元と原始既約多項式の存在（1）

補題A　Gを有限可換群とする．Gの要素の位数の最大値をmとする．このときGの任意の要素aの位数order(a)はmを割り切る．可換群とは$a \cdot b = b \cdot a$ $(\forall a, b \in G)$が成り立つ群をいう．

（証明）加群の構造定理を用いる（代数学か線形代数学の授業で学習されることになるのではないかと思います．初等的な証明があれば，レポートにしてください．評価します）
（問31　レ）

補題B　Gをn個の要素を持つ可換群とする．$\forall a \in G$に対して$a^n = 1$が成り立つ．

（証明）$G = \{a_1, \cdots, a_n\}$とする．群の性質より$\{aa_1, \cdots, aa_n\} = \{a_1, \cdots, a_n\} = G$が成り立つ．
（何故か？もし等号が成り立たないならば$aa_i = aa_j$なる要素が存在しなければならないが）
可換性を使って

$$aa_1 aa_2 \cdots aa_n = a^n a_1 \cdots a_n = a_1 \cdots a_n$$

が成り立つ．$a^n a_1 \cdots a_n = a_1 \cdots a_n$の両辺に逆元$(a_1 \cdots a_n)^{(-1)} = a_n{}^{-1} \cdots a_1{}^{-1}$をかけて
$a^n = 1$を得る．

原始元と原始既約多項式の存在（2）

<u>定理</u>　有限体Fの乗法群$K = F \setminus \{0\}$には原始元が存在する．

（証明）$K=\{\alpha_1,\cdots,\alpha_M\}$とする．これらの要素の位数の最大値を$e$とする（当然そのような元は存在）
補題Bより$\mathrm{e} \le M$．一方，補題Aよりこれらのどの要素の位数もeの約数である．すなわち
Kの全ての元aに対して$a^e = 1$．つまりKの全ての元aは方程式$x^e - 1 = 0$の根である．
よって$M \le e$．ゆえに$M = e$．

<u>定理</u>　有限体Fの乗法群$K = F \setminus \{0\}$の原始元αを根にもつ既約多項式（原始既約多項式）が存在する．

（証明）　少し，目的としているところと外れるので省略します．興味のある人は
「符号と暗号の数理」，神保雅一，藤原良　著 p. 57-59を参考に証明を試みてください．
レポートにしてくれれば，評価します（問32　レ）．

共役元

<u>定義</u>　　αが$GF(2)$上のn次多項式

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \quad (a_n = 1)$$

の根であるとする．このとき$\alpha^2, \alpha^4, \cdots, \alpha^{2^{n-1}}$も根となる．なぜならば

$$f(\alpha^2) = \left(f(\alpha)\right)^2 = 0,\ f(\alpha^4) = \left(f(\alpha)\right)^4, \cdots$$

となるからである．$\alpha^2, \alpha^4, \cdots, \alpha^{2^{n-1}}$を$\alpha$の共役元（または共役根）という．

巡回符号（1）

定義 [redacted]

巡回符号であるという．巡回符号では符号語$\mathbf{w} = a_0 a_1 \cdots a_{n-1} \quad a_i \in \{0,1\}$に対して多項式

$$w(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

を対応させる．ここで

$$xw(x) = a_0 x + a_1 x^2 + \cdots a_{n-2} x^{n-1} + a_{n-1} x^n = a_{n-1} + a_0 x + a_1 x^2 + \cdots a_{n-2} x^{n-1} + a_{n-1}(x^n - 1)$$

$$\equiv a_{n-1} + a_0 x + a_1 x^2 + \cdots a_{n-2} x^{n-1} \pmod{x^n - 1}$$

となり$xw(x)$は$(\mathrm{mod}\, x^n - 1)$で巡回シフトした$a_1 \cdots a_{n-1} a_0$に対応した符号多項式となる．さらに$\mathrm{x}^l w(x) \quad (l = 1, 2, \cdots)$も$l$回巡回シフトした符号語に対応する符号多項式となる．$\mathcal{C}$は線形符号だからこれらの線形結合も$\mathcal{C}$の元とならねばならない．すなわち

$$b(x) = b_0 + b_1 x + \cdots + b_{n-1} \text{に対して} b(x)w(x) = (b_0 + b_1 x + \cdots + b_{n-1}) w(x) \in \mathcal{C}$$

である．

巡回符号（2）

命題A　$\mathcal{C}$を巡回符号とする．$g(x)$を0と異なる最小次数の符号多項式とすると任意の符号多項式は$w(x)=a(x)g(x)$の形をとる．

（証明）$a(x)g(x)$の形に表せない符号多項式$w(x)$が存在すると仮定する．$w(x)$を$g(x)$で割った余りを$r(x)$とおく．すなわち$w(x)=q(x)g(x)+r(x)$．$w(x), q(x)g(x)\in\mathcal{C}$だから
$r(x)=w(x)-q(x)g(x)\in\mathcal{C}$の符号多項式．$\deg(r(x))<\deg(g(x))$だから$g(x)$が最小次数の符号多項式であることに矛盾する．

定義　$g(x)$を$\mathcal{C}$の生成多項式といい，$a(x)$を情報多項式という．情報ビットがkの場合，
$a(x)=a_0+a_1x+\cdots a_{k-1}x^{k-1}$，　$g(x)=g_0+g_1x+\cdots+g_{n-k}x^{n-k}$
となる．

命題B　$\mathcal{C}$の生成多項式$g(x)$はx^n-1を割り切る．

（証明）$x^kg(x)=g_0x^k+g_1x^{k+1}+\cdots+g_{n-k}x^n=g_{n-k}+g_0x^k+g_1x^{k+1}+\cdots+g_{n-k-1}x^{n-1}+g_{n-k}(x^n-1)$
ここで定義から$g_{n-k}=1$だから
$(x^n-1)=x^kg(x)-\left(g_{n-k}+g_0x^k+g_1x^{k+1}+\cdots+g_{n-k-1}x^{n-1}\right)\in\mathcal{C}$．よって右辺は$q(x)g(x)$と書ける．

例　符号長3の巡回符号の生成多項式$g(x)$を求め，巡回符号を作成せよ．情報ビット長は3でないものとする．

命題より$g(x)$はx^3-1の因数である．$x^3-1=(x+1)(x^2+x+1)$だから$g(x)=x+1$または$g(x)=x^2+x+1$.

(i) $g(x)=x+1$のとき．$\mathcal{C}=\left\{(a_0+a_1x)(x+1)\mid a_0,a_1\in\{0,1\}\right\}=\left\{0,x+1,x(x+1),(x+1)^2\right\}$

$=\left\{0,1+x,x+x^2,1+x^2\right\}=\left\{000,110,011,101\right\}$

この符号の最小距離は2だから誤り訂正はできないが，誤り検出はできる．

(ii) $g(x)=x^2+x+1$のとき．$\mathcal{C}=\left\{a_0(x^2+x+1)\mid a_0\in\{0,1\}\right\}=\left\{0,x^2+x+1\right\}=\left\{000,111\right\}$

この符号の最小距離は3だから1誤り訂正できる．

巡回符号の生成行列

<u>定義</u>　$g(x)$を$\mathcal{C}$の生成多項式，$a(x)$を情報多項式としたとき

$$a(x) = a_0 + a_1 x + \cdots a_{k-1} x^{k-1}, \quad g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$$

とすると

$$a(x)g(x) = a_0 g(x) + a_1 x g(x) + \cdots + a_{k-1} x^{k-1} g(x)$$

である．ここで

$g(x), xg(x), \cdots, x^{k-1} g(x)$をベクトルで表現すると

$(g_0, g_1, \cdots, g_{n-k}, 0, \cdots \quad, 0)$

$(0, g_0, g_1, \cdots, g_{n-k}, 0, \cdots, 0)$

$\vdots$

$(0, \quad \cdots, 0, g_0, g_1, \cdots, g_{n-k})$

となる．よって $a(x)g(x) = a_0 g(x) + a_1 x g(x) + \cdots + a_{k-1} x^{k-1} g(x) =$

$$(a_0, \cdots, a_{k-1}) \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & & & \\ & g_0 & g_1 & g_2 & \cdots & g_{n-k} & & \\ & \ddots & \ddots & & & & \ddots & \\ & & & g_0 & g_1 & g_2 & \cdots & g_{n-k} \end{pmatrix} = (a_0, \cdots, a_{k-1}) G$$

となり，生成行列はGとなる．

巡回符号のパリティチェック行列

<u>定義</u>　命題Bより$g(x)$はx^n-1の因数であるから

$$h(x)=(x^n-1)/g(x)$$

が定義できる．$h(x)=h_kx^k+\cdots+h_1x+h_0$とおいたとき$G$のパリティチェック行列は

$$H=\begin{pmatrix} & & & h_k & h_{k-1} & \cdots & h_0 \\ & & h_k & h_{k-1} & \cdots & h_0 & \\ & \iddots & \iddots & & \iddots & & \\ h_k & h_{k-1} & \cdots & h_0 & & & \end{pmatrix}$$

となる．

<u>例</u>　$n=7, g(x)=1+x^2+x^3$の生成行列Gを求めてみる．$k=4$だから

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

$$h(x)=(x^7-1)/g(x)=x^4+x^3+x^2+1$$

である．よって

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

となる．

<u>問33</u>　例において$GH^T=O$が成り立っていることを確かめよ．

<u>問34（レ）</u>　一般に$GH^T=O$が成り立つことを示せ．

巡回符号の最小距離（1）

$$A=\begin{pmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{pmatrix}$$

とする．ヴァンデルモンデ行列式 $\det A = bc^2 + ab^2 + a^2c - a^2b - ac^2 - b^2c$

$= (c-b)a^2 + (b^2-c^2)a + bc(c-b)$

$= (c-b)\left(a^2 - (b+c)a + bc\right) = (c-b)(a-b)(a-c) = (b-a)(c-b)(a-c)$

一般に

$$A=\begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1{}^2 & a_2{}^2 & \cdots & a_n{}^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} & a_2{}^{n-1} & \cdots & a_n{}^{n-1} \end{pmatrix}$$

ならば $\det A = \prod_{1<i<j\le n} (a_j - a_i)$ となる．したがって A は正則（逆行列をもつ）である．

巡回符号の最小距離（2）

今，生成多項式g(x)の中にh個連続した根$\alpha^{tq(\mathrm{w}},\alpha^{t+1},\cdots,\alpha^{t+h-1}\in GF(2^m)$があるものとしよう．例えば$g(x)=(x^4+x+1)(x^4+x^3+x^2+x+1)$は$(x^4+x+1)=0$は$\alpha,\alpha^2,\alpha^4$を根にもち,$(x^4+x^3+x^2+x+1)=0$は$\alpha^3,\alpha^6,\alpha^{12},\alpha^{24}=\alpha^9$を根にもつから$\alpha,\alpha^2,\alpha^3,\alpha^4$という連続した4根をもつ.

符号多項式$w(x)=w_0+w_1x+\cdots+w_{n-1}x^{n-1}$に連続根$\alpha^t,\alpha^{t+1},\cdots,\alpha^{t+h-1}$を代入すると

$$\begin{pmatrix} 1 & \alpha^t & \cdots & \alpha^{t(n-1)} \\ 1 & \alpha^{t+1} & \cdots & \alpha^{(t+1)(n-1)} \\ 1 & \alpha^{t+2} & \cdots & \alpha^{(t+2)(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{t+h-1} & \cdots & \alpha^{(t+h-1)(n-1)} \end{pmatrix}\begin{pmatrix} w_0 \\ w_1 \\ w_2 \\ \vdots \\ w_{n-1} \end{pmatrix}=\begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

ここで$H=\begin{pmatrix} 1 & \alpha^t & \cdots & \alpha^{t(n-1)} \\ 1 & \alpha^{t+1} & \cdots & \alpha^{(t+1)(n-1)} \\ 1 & \alpha^{t+2} & \cdots & \alpha^{(t+2)(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{t+h-1} & \cdots & \alpha^{(t+h-1)(n-1)} \end{pmatrix}$とし，

Hの任意のh行を選びその$h\times h$行列Aを書くと

$$A=\begin{pmatrix} \alpha^{s_1t} & \alpha^{s_2t} & \cdots & \alpha^{s_ht} \\ \alpha^{s_1(t+1)} & \alpha^{s_2(t+1)} & \cdots & \alpha^{s_h(t+1)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{s_1(t+h-1)} & \alpha^{s_2(t+h-1)} & \cdots & \alpha^{s_h(t+h-1)} \end{pmatrix}$$

となり$\det A=\alpha^{s_1t}\alpha^{s_2t}\cdots\alpha^{s_ht}\det\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{s_1} & \alpha^{s_2} & \cdots & \alpha^{s_h} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{s_1(h-1)} & \alpha^{s_2(h-1)} & \cdots & \alpha^{s_h(h-1)} \end{pmatrix}$

となり，Aは正則．よって$(w_0,w_1,\cdots,w_{n-1})=(0,0,\cdots,0)$．すなわち$(w_0,w_1,\cdots,w_{n-1})$からどのような$h$組の変数を選んでもその変数は0となる．従って符号語のハミング重みは$h+1$以上となる．

BCH符号（1）(Bose-Chaudhuri-Hocquenghem Code)

$\alpha : GF(2^{m+z})$の原始元，$M_i(x) : \alpha^i$を$M_i(x)=0$の根とする最小多項式（最小多項式とは次数最小の多項式という意味）

$g(t)=\mathrm{LCM}\{M_1(x), M_2(x), \cdots, M_{2t}(x)\}$とする．このとき$g(x)$を生成多項式とする巡回符号（BCH符号）の最小距離は$2t+1$，したがってt重誤り訂正可能である．

例　$\alpha : GF(2^4)$の原始元とする．$x^{2^4-1}-1$を因数分解すると

$$x^{15}-1=(x+1)(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x^4+x^3+1)$$

x^4+x+1，x^4+x^3+1は原始既約多項式なので特にαは$x^4+x+1=0$の根とする．α^i　$(i=1,\cdots,15)$はp. 22の補題Bより全て$x^{15}-1$の根なので各因数多項式はαのべきを必ず根のもつ．また，その共役元も根にもつ．具体的には各因数多項式は次のように分解される．

$$M_1(x)=x^4+x+1=(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$$

$$M_3(x)=x^4+x^3+x^2+x+1=(x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9)$$

$$M_5(x)=x^2+x+1=(x-\alpha^5)(x-\alpha^{10})$$

$$M_7(x)=x^4+x^3+1=(x-\alpha^7)(x-\alpha^{14})(x-\alpha^{13})(x-\alpha^{11})$$

BCH符号（2）(Bose-Chaudhuri-Hocquenghem Code)

例　$\alpha : GF(2^4)$の原始元とする．αは$x^4+x+1=0$の根とする．

$M_1(x)=x^4+x+1=(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$

$M_3(x)=x^4+x^3+x^2+x+1=(x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9)$

$M_5(x)=x^2+x+1=(x-\alpha^5)(x-\alpha^{10})$

$M_7(x)=x^4+x^3+1=(x-\alpha^7)(x-\alpha^{14})(x-\alpha^{13})(x-\alpha^{11})$

$t=1$のとき（単一誤り訂正）

$g(x)=\mathrm{LCM}\{M_1(x),M_2(x)\}=M_1(x)=x^4+x+1.$　よって$n=15, n-k=4, k=11.$

$t=2$のとき（２重誤り訂正）

$g(x)=\mathrm{LCM}\{M_1(x),M_2(x),M_3(x),M_4(x)\}=M_1(x)M_3(x)=(x^4+x+1)(x^4+x^3+x^2+x+1).$

よって$n=15, n-k=8, k=7.$

$t=3$のとき（３重誤り訂正）

$g(x)=\mathrm{LCM}\{M_1(x),M_2(x),M_3(x),M_4(x),M_5(x),M_6(x)\}=M_1(x)M_3(x)M_5(x)$

$=(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1).$　よって$n=15, n-k=10, k=5.$

$g(x)=(x^4+x+1)(x^4+x^3+x^2+x+1)=x^8+x^7+x^6+x^4+1$のとき，情報ビット系列1010001を符号化する．

$(1+x^2+x^6)(x^8+x^7+x^6+x^4+1)=x^{14}+x^{13}+x^{12}+x^9+x^7+x^6+x^4+x^2+1$

よって符号化は101010110100111である．

BCH符号の復号（直接法（1））

$\alpha : GF(2^m)$の原始元，符号長$n = 2^m - 1$とする．BCH符号の生成多項式は連続根$\alpha, \cdots, \alpha^{2t}$をもつこととする．

受信多項式を$v(x)$,誤り多項式を$e(x)$とする．今$(i+1)$ビット目と$(j+1)$ビット目に誤りがあるものとすると

$$e(x) = x^i + x^j$$

$$\begin{cases} S_1 = v(\alpha) = (a(\alpha)g(\alpha) + e(\alpha)) = e(\alpha) = \alpha^i + \alpha^j \\ S_3 = v(\alpha^3) = (a(\alpha^3)g(\alpha^3) + e(\alpha^3)) = e(\alpha^3) = \alpha^{3i} + \alpha^{3j} \end{cases}$$

が成り立つ．上式より

$\alpha^i + \alpha^j = S_1$,また$S_1^3 = S_3 + \alpha^i\alpha^j(\alpha^i + \alpha^j) = S_3 + S_1\alpha^i\alpha^j$．よって$\alpha^i\alpha^j = S_1^2 + S_3 / S_1$が成り立つ．

誤り位置多項式を次で定義する．

$$\sigma(z) = (1 - \alpha^i z)(1 - \alpha^j z)$$

$\sigma(z)$はα^{-i}, α^{-j}を根に持つので逆数をとれば誤り位置が特定できる．$\sigma(z)$が具体的に書けなければ意味はないが

$$\sigma(z) = (1 - \alpha^i z)(1 - \alpha^j z) = 1 + (\alpha^i + \alpha^j)z + \alpha^i\alpha^j z^2 = 1 + S_1 z + (S_1^2 + S_3 / S_1)z^2$$

なので$\sigma(z)$は具体的に表現できる．

BCH符号の復号（直接法（2））

例　$\alpha : GF(2^4)$の原始元とする．αは$x^4+x+1=0$の根とする．$g(x)=M_1(x)M_3(x)$とする．

$g(x)=\mathrm{LCM}\{M_1(x),M_2(x),M_3(x),M_4(x)\}=M_1(x)M_3(x)=(x^4+x+1)(x^4+x^3+x^2+x+1).$

$n=15, n-k=8, k=7$で2重誤り訂正可能である．この符号において110100101101110を受信した．以下のように誤り訂正は行われる．

$v(x)=1+x+x^3+x^6+x^8+x^9+x^{11}+x^{12}+x^{13}$

$\alpha^4=\alpha+1, \alpha^5=\alpha^2+\alpha, \alpha^6=\alpha^3+\alpha^2, \alpha^7=\alpha^3+\alpha+1, \alpha^8=\alpha^2+1, \alpha^9=\alpha^3+\alpha, \alpha^{10}=\alpha^2+\alpha+1,$

$\alpha^{11}=\alpha^3+\alpha^2+\alpha, \alpha^{12}=\alpha^3+\alpha^2+\alpha+1, \alpha^{13}=\alpha^3+\alpha^2+1, \alpha^{14}=\alpha^3+1, \alpha^{15}=1$なので

$S_1=v(\alpha)=\alpha^2, S_3=v(\alpha^3)=0$

よって$\sigma(z)=1+\alpha^2 z+\alpha^4 z^2.z=1,\alpha,\cdots,\alpha^{14}$まで代入して$\sigma(z)=0$なる根を求めると$z=\alpha^3,\alpha^8$

$\alpha^{-3}=\alpha^{12}, \alpha^{-8}=\alpha^7$なので誤り位置は8ビット目と13ビット目．

110100111101010に訂正される．

BCH符号の復号（ピーターソン法（1））

ハワイ大学マノア校情報科学部教授
1924 - 2009

授賞理由

ウェスレイ･ピーターソン博士は現在の情報技術に基本的な役割を果たしつつあるデジタル技術の分野において、その最も重要な要素である符号理論に関する先駆的研究を行い、極めて顕著な成果を挙げた。

すなわち、同博士は、現在のデジタル通信、デジタル放送、デジタル記録の高信頼化にとって不可欠なものとなっている誤り訂正 符号（誤り検出符号を含む）の基礎理論を確立するとともに、その実用化への道を拓く数々の提案･発明を行い、デジタル技術の進歩に決定的な影響を与えた。

誤り訂正符号の基礎理論である代数的符号理論は、1961年に出版されたピーターソン博士の名著「誤り訂正符号」によって創 始されたということができる。同博士は、この著書により、誤り訂正符号に関する用語や概念を確立し、現代代数学を基礎とする代数的符号理論の枠組みを構築 するとともに、誤り訂正符号の符号化法や復号法、装置化法の体系を確立した。

符号理論の研究者にとってバイブルともいわれるこの著書は、多くの国の言語に翻訳され、「代数的符号理論の創始者」としての 同博士の名を不動のものとしている。電気工学、情報科学のカリキュラムに現代代数学が取り入れられることになったのも同博士の著書によるところが大きい。 かつては、工学の分野でほとんど関心を持たれることの無かった現代代数学が、この著書により、誤り訂正符号の工学的応用に極めて有用であることが示され、 現在で、符号理論、暗号理論、有限状態機械の理論などの基礎となっている。

同書の内容はピーターソン博士の多くの独創的な研究成果を柱として構成されているが、その主要なものを挙げると次の通りであ る。現在のほとんど全てのデジタル通信システムやあらゆるコンピュータディスクには誤り検出のためにピーターソン博士の提案によって巡回冗長検査が用いら れてきたが、さらに最近では、同博士が創始した代数概念を基礎とするさらに進歩した誤り検出･訂正システムに変わってきている。また、今日、コンパクト ディスクの誤り訂正をはじめ広く実用に供されているリードソロモン符号はBCH符号と呼ばれる誤り訂正符号の一種であるが、同博士はBCH符号の実際的な 復号法の最初の発明者でもある。さらに同博士は巡回符号の符号化や復号のための実用的なシフトレジスタ回路をも発明した。これらの発明は、誤り訂正符号の 産業応用に 決定的な貢献をしている。

このように、今日のデジタル通信、デジタル放送、デジタル記録にはピーターソン博士の研究成果が欠くべからざるものとして広く利用されており、その卓越した学術的ならびに技術的功績は日本国際賞の受賞者として誠にふさわしいものである。

BCH符号の復号（ピーターソン法（2））

ピーターソン法と直接法の違いは誤り位置多項式の導出の方法のみである．しかし，それを導入したことがすばらしいことと言えよう．

$\alpha : GF(2^m)$の原始元，符号長$n = 2^m - 1$とする．BCH符号の生成多項式は連続根$\alpha, \cdots, \alpha^{2t}$をもつこととする．$t = 3$とし，3重誤りの場合を考える．

$$e(x) = x^i + x^j + x^k$$

このとき次が成り立つ．

$$S_m = v(\alpha^m) = (a(\alpha^m)g(\alpha^m) + e(\alpha^m)) = e(\alpha^m) = \alpha^{mi} + \alpha^{mj} + \alpha^{mk} \quad (1 \le m \le 6)$$

$$\sigma(z) = (1 - \alpha^i z)(1 - \alpha^j z)(1 - \alpha^k z) = 1 + \sigma_1 z + \sigma_2 z^2 + \sigma_3 z^3$$

ここで$z = \alpha^{-i}, z = \alpha^{-j}, z = \alpha^{-k}$は根なので

$$\begin{cases} 1 + \sigma_1 \alpha^{-i} + \sigma_2 \alpha^{-2i} + \sigma_3 \alpha^{-3i} = 0, \\ 1 + \sigma_1 \alpha^{-j} + \sigma_2 \alpha^{-2j} + \sigma_3 \alpha^{-3j} = 0, \\ 1 + \sigma_1 \alpha^{-k} + \sigma_2 \alpha^{-2k} + \sigma_3 \alpha^{-3k} = 0 \end{cases} \qquad \text{（A）}$$

が成り立つ．

上式にそれぞれ$\alpha^{4i}, \alpha^{4j}, \alpha^{4k}$をかけると

$$\begin{cases} \alpha^{4i} + \sigma_1 \alpha^{3i} + \sigma_2 \alpha^{2i} + \sigma_3 \alpha^{i} = 0, \\ \alpha^{4j} + \sigma_1 \alpha^{3j} + \sigma_2 \alpha^{2j} + \sigma_3 \alpha^{j} = 0, \\ \alpha^{4k} + \sigma_1 \alpha^{3k} + \sigma_2 \alpha^{2k} + \sigma_3 \alpha^{k} = 0 \end{cases} \qquad \text{（B）}$$

BCH符号の復号(ピーターソン法(2))

式(B)を辺々加えることにより

$$S_4+\sigma_1 S_3+\sigma_2 S_2+\sigma_3 S_1=0$$

同様に式(A)の両辺に$\alpha^{5i},\alpha^{5j},\alpha^{5k}$および$\alpha^{6i},\alpha^{6j},\alpha^{6k}$をかけ辺々加えることにより

$$S_5+\sigma_1 S_4+\sigma_2 S_3+\sigma_3 S_2=0,\quad S_6+\sigma_1 S_5+\sigma_2 S_4+\sigma_3 S_3=0$$

これらを行列で表現すると

問35（レ）　(C)を確かめよ.

$$\begin{pmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{pmatrix}\begin{pmatrix} \sigma_3 \\ \sigma_2 \\ \sigma_3 \end{pmatrix}=S\begin{pmatrix} \sigma_3 \\ \sigma_2 \\ \sigma_3 \end{pmatrix}=\begin{pmatrix} S_4 \\ S_5 \\ S_6 \end{pmatrix}$$

となる．行列Sが正則な時はこれを解いて($\sigma_1,\sigma_2,\sigma_3$)を得る．実際$S$は正則である．

$$\begin{pmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{pmatrix}=\begin{pmatrix} 1 & 1 & 1 \\ \alpha^i & \alpha^j & \alpha^k \\ \alpha^{2i} & \alpha^{2j} & \alpha^{2k} \end{pmatrix}\begin{pmatrix} \alpha^i & 0 & 0 \\ 0 & \alpha^j & 0 \\ 0 & 0 & \alpha^k \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 \\ \alpha^i & \alpha^j & \alpha^k \\ \alpha^{2i} & \alpha^{2j} & \alpha^{2k} \end{pmatrix}^T \qquad \text{(C)}$$

が成り立つのでヴァンデルモンデ行列式よりSは正則である．

誤りの個数が2個の場合は，例えば(C)の右辺の中央の行列は

$\begin{pmatrix} \alpha^i & 0 & 0 \\ 0 & \alpha^j & 0 \\ 0 & 0 & 0 \end{pmatrix}$となり正則でなくなる．よって$S$は正則でなくなる．これにより誤りの個数が

3個未満であることが判断できる．

BCH符号の復号（ピーターソン法（3））

例　$\alpha : GF(2^4)$の原始元とする．αは$x^4+x+1=0$の根とする．$g(x)=M_1(x)M_3(x)$とする．

$g(x)=\mathrm{LCM}\{M_1(x),M_2(x),M_3(x),M_4(x)\}=M_1(x)M_3(x)=(x^4+x+1)(x^4+x^3+x^2+x+1).$

$n=15, n-k=8, k=7$で2重誤り訂正可能である．この符号において110100101101110を受信した．以下のように誤り訂正は行われる．

$v(x)=1+x+x^3+x^6+x^8+x^9+x^{11}+x^{12}+x^{13}, \sigma(z)=(1-\alpha^i z)(1-a^j z)=1+\sigma_1 z+\sigma_2 z^2$とおく．

$z=\alpha^{-i}, z=\alpha^{-j}$を代入すると

$1+\sigma_1\alpha^{-i}+\sigma_2\alpha^{-2i}=0,\quad 1+\sigma_1\alpha^{-j}+\sigma_2\alpha^{-2j}=0$を得る．前のスライドと同様にして

$$\begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix}\begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix}=\begin{pmatrix} S_3 \\ S_4 \end{pmatrix}$$

が成り立つ．

$\alpha^4=\alpha+1, \alpha^5=\alpha^2+\alpha, \alpha^6=\alpha^3+\alpha^2, \alpha^7=\alpha^3+\alpha+1, \alpha^8=\alpha^2+1, \alpha^9=\alpha^3+\alpha, \alpha^{10}=\alpha^2+\alpha+1,$

$\alpha^{11}=\alpha^3+\alpha^2+\alpha, \alpha^{12}=\alpha^3+\alpha^2+\alpha+1, \alpha^{13}=\alpha^3+\alpha^2+1, \alpha^{14}=\alpha^3+1, \alpha^{15}=1$なので

$S_1=v(\alpha)=\alpha^2, S_2=v(\alpha^2)=v(\alpha)^2=\alpha^4, S_3=v(\alpha^3)=0, S_4=v(\alpha^4)=v(\alpha^2)^2=\alpha^8$

よって $\begin{pmatrix} \alpha^2 & \alpha^4 \\ \alpha^4 & 0 \end{pmatrix}\begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix}=\begin{pmatrix} 0 \\ \alpha^8 \end{pmatrix}.$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}=\dfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$なので $\begin{pmatrix} \alpha^2 & \alpha^4 \\ \alpha^4 & 0 \end{pmatrix}^{-1}=\dfrac{1}{\alpha^8}\begin{pmatrix} 0 & \alpha^4 \\ \alpha^4 & \alpha^2 \end{pmatrix}=\begin{pmatrix} 0 & \alpha^{-4} \\ \alpha^{-4} & \alpha^{-6} \end{pmatrix}$

よって$\begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix}=\begin{pmatrix} 0 & \alpha^{-4} \\ \alpha^{-4} & \alpha^{-6} \end{pmatrix}\begin{pmatrix} 0 \\ \alpha^8 \end{pmatrix}$.従って$\sigma_2=\alpha^4, \sigma_1=\alpha^2.$

$\sigma(z)=1+\alpha^2 z+\alpha^4 z^2. z=1,\alpha,\cdots,\alpha^{14}$まで代入して$\sigma(z)=0$なる根を求めると$z=\alpha^3,\alpha^8$

$\alpha^{-3}=\alpha^{12}, \alpha^{-8}=\alpha^7$なので誤り位置は8ビット目と13ビット目．

110100111101010に訂正される．

問36(レ)　前のスライドと同様にしての部分を確かめよ．

拡張ユークリッドアルゴリズム（互除法）

杉山，笠原，平澤，滑川によるユークリッド復号法を紹介するために簡単に拡張ユークリッドアルゴリズムについて復習しておこう．

ユークリッド互除法では $\gcd(72,56)=\gcd(56,16)=\gcd(16,8)=\gcd(8,0)$ から72と56の最大公約数が8であることを示す．
ここで等号それぞれでの計算を見てゆくと $72=1\times 56+16,$ $\boxed{56=3\times 16+8,}$ $16=2\times 8+0$ という計算を行っていることがわかる．

ここで終わりから1つ前の式 $56=3\times 16+8$ を変形して $8=56-3\times 16$ としてみる．さらに1番目の式を使って $16=72-1\times 56$ より16を消去すると $8=-3\times 72+4\times 56$ が成り立つことがわかる．すなわち

$$\gcd(a,b)=\text{適当な整数}\times a+\text{適当な整数}\times b$$

が成り立っていてこれは正しい（何らかの講義で聞いたことがあるでしょうか？特にaとbが互いに素なとき，$\mathrm{mod}(b)$でのaの逆元の計算に用います）．このアルゴリズムは多項式$a(x)$と$b(x)$の最大公約多項式を求める際にも成り立つことが知られている．
すなわち $a_0(x)=a(x),\quad a_1(x)=b(x)\quad \deg(a_0(x))>\deg(a_1(x))$ としたとき

$$\begin{cases} a_0(x)=q_1(x)a_1(x)+a_2(x) \\ a_1(x)=q_2(x)a_2(x)+a_3(x) \\ a_2(x)=q_3(x)a_3(x)+a_4(x) \\ \qquad\vdots \\ a_{n-2}(x)=q_{n-1}(x)a_{n-1}(x)+a_n(x) \\ a_{n-1}(x)=q_n(x)a_n(x) \end{cases}$$

最大公約多項式$a_n(x)$の場合を含め，

$$\boxed{a_i(x)=\gcd(a(x),b(x))=\phi_i(x)a(x)+\psi_i(x)b(x)}\quad (i=2,\cdots,n)$$

と表すことができる（ここで$\phi_i(x),\psi_i(x)$はiに依存する多項式）．

ユークリッド復号法

「ユークリッド復号法」，平澤茂一，笠原正雄著
IEEE Fundamental Review Vol.4 No.3
より抜粋

3.1 ユークリッド復号法，発見への道

1967 年秋からの 2 年間，笠原は米国ベル電話研究所（以後単にベル研究所，通常 Bell Lab. と呼ばれている）のホルムデル研究所で 400Mbit/s の超高速パルス通信の開発研究に携わっていた．

1965 年に大阪大学大学院工学研究科通信工学専攻博士課程を修了して「誤りを検出または訂正できる符号に関する研究」という今から考えると非常に大雑把な題名のもとに工学博士の学位を授与されていたので，ベル研究所所員になってからも余暇を見つけては誤り訂正符号の研究を続けていた．

こんなことから，同じベル研究所のマレーヒル研究所「符号理論研究グループ」の若き逸材，E. R. Berlekamp 博士と電話を通してお話をしていた．この交流が契機となって，出版直前の彼の著書 *Algebraic Coding Theory* の原稿全体のコピーを社内便で送ってもらった．図画はすべて手書き，それも走り書きという生々しい原稿であった．27 歳の若さでこんなすごい本を書くのか! カルチャーショックという表現を超えた驚きであった．秀逸そして斬新な内容に，笠原は世界のレベルの高さを身近に，強く感じた．

帰国後，三菱電機在職中の平澤，故杉山博士とともに，土日祝日を利用しての勉強会が笠原の自宅で始まった．輪講のテーマはベル研究所で衝撃的な印象を受けたあの Berlekamp 博士の著書 *Algebraic Coding Theory* である．内容についての徹底的討論のスタートである．

厳しい輪講の中で得た結論の一つは “Srivastava 符号に大きな可能性あり” であった．

私たちの期待どおり，Srivastava 符号は幾つかの新しい発見をもたらしてくれた．例えば，その成果の一つは 1975 年に *IEEE IT Transaction* に掲載されている．

Srivastava 符号に大きな可能性があることを，私たちは Berlekamp 博士に伝えていたが，このことに対する回答が上記論文執筆中にあった．手紙には “ゴッパ符号により大きな可能性あり．ゴッパ符号を研究されよ” とあるではないか．

欧米の研究者の中で，いち早くゴッパ符号の秀逸性に気付いた人，その人こそ Berlekamp 博士であることを，後ほど知ることとなったが，私たちはそのときはこのことに気付かぬまま，Berlekamp 博士のアドバイスを素直に受け入れた．そして Berlekamp 博士から送ってもらったゴッパ符号についてのロシア語の論文を字引片手に読破した．そしてこのことがユークリッド復号法の誕生に結び付くこととなった．

3.2 ユークリッド復号法の誕生

3.2.1 ユークリッド復号法と Berlekamp 博士

ユークリッド復号法が土日勉強会の中で誕生したとき，実は喜びよりも不安の方がはるかに大きかった．“こんな簡単なアイデア，世界のどこかで既に発表されているのではないか?” という不安の方が大きかった．とにかくどこかの研究会で発表してみることも考えてみたけれど，“周知の考えとして，もの笑いになるかもしれない … ”，こんな心配が付きまとった．余りにも単純な考えであったからである．

しかし，とりあえず英文論文の形にまとめてみよう．私たちは数か月を費やして論文にまとめる作業をしていた．しかし，周知のことかもしれないという不安は解消されない．こんな悩みを払拭するために，書き上げた英文論文をそっくり Berlekamp 博士に送付するという選択を私たちは選んだ．

間を置かずに頂いた Berlekamp 博士からの手紙には，

“素晴らしい独創的なアイデアだ！ 実は自分は現在 *Information and Control* という雑誌の編集者を務めているが，編集者としての権限で即採録としたい．ただし *Information and Control* の発行部数は *IEEE IT Transaction* には及ばないので，IEEE への投稿を選択されてもよい．しかし，この場合は新たに査読者の選定作業等が入るので，世の中に出るタイミングが 1〜2 年遅れるでしょうね”

とあった．私たちは Berlekamp 博士の御好意に感謝するとともに，迷うことなく “*Information and Control* への掲載を希望する” という内容の手紙を送った．発行部数よりも早く世界に出した方がよい．私たちの選択である．

Berlekamp–Massey 復号法の考案者でもある Berlekamp 博士自身から，独創的な素晴らしいアイデアという最高の賛辞を頂いたこと，そして即採録という特段の御配慮を頂いたことは終生忘れることのできない記憶として残ることとなった．

3.2.2 ユークリッド復号法と嵩先生，そして Goppa 博士

符号理論の世界的権威，嵩先生とはキャンパスは異なるけれど同じ大阪大学ということで常に連絡を取り合っていたが，ある日，嵩先生から一通の手紙を受け取った．Goppa 博士の手紙のコピーが同封されていたと記憶するが，嵩先生直筆の字で，

“Goppa 博士からユークリッド互除法を用いた簡明な復号法を考えている，との手紙を受け取ったが，御提案の方法は日本人グループで発見され，既に周知のこととなっている，という回答をしておいた”

という内容の文章がつづられていた．

Goppa 博士は，嵩先生が符号理論の分野でのスーパースターであったからこそ，アイデアを思いついた瞬間に，このことを告げる手紙を送ったのである．これに対し嵩先生は間を置かず Goppa 博士に手紙を送って下さり，かつまた Goppa 博士はこの手紙を見てフェアプレーの精神で発表することを断念してくれた．このことによってユークリッド復号法についての先陣争いという日本人研究者には不利な戦場（いくさば）に駆り出されなくて済んだと思う．嵩先生の迅速な対応，Goppa 博士の寛大な判断によって救われたのである．

仮に Goppa 博士が嵩先生に手紙を送ることなく，また私たちの研究成果を知ることもなく，ロシア国内あるいはヨーロッパのどこかで発表していたなら，例え 1〜2 年こちらが早かったというしっかりした証拠が残っていたとしても，私たちのユークリッド復号法の先駆性を日本，アジアを含めた世界に認めさすためには耐え難い労力と長い年月の努力を強いられたことになったと思う．他の分野での幾つかの経験に基づくが，この戦場（いくさば）は研究とは全く無縁な余りにもつらい，過酷な世界である．

ユークリッド復号法

$\alpha : GF(2^m)$の原始元，符号長$n = 2^m - 1$とする．BCH符号の生成多項式は連続根$\alpha, \cdots, \alpha^{2t}$をもつこととする．

$e(x) = x^{i_1} + x^{i_2} +$ [redacted]

ここでシンドローム多項式$S(z)$を定義する．

$$S(z) = S_1 + S_2 z + \cdots + S_{2t} z^{2t-1} = \sum_{k=1}^{s} \sum_{j=1}^{2t} (\alpha^{i_k})^j z^{j-1}$$

$\sum_{j=1}^{\infty} (\alpha^{i_k})^j z^{j-1} = \dfrac{\alpha^{i_k}}{1-\alpha^{i_k} z}$だから　$\sum_{j=1}^{2t} (\alpha^{i_k})^j z^{j-1} = \dfrac{\alpha^{i_k}}{1-\alpha^{i_k} z} \pmod{z^{2t}}$　と書ける．

よって　$S(z) = \sum_{k=1}^{s} \dfrac{\alpha^{i_k}}{1-\alpha^{i_k} z} \pmod{z^{2t}}$　となる．これより

$$S(z)\sigma(z) = (1-\alpha^{i_1} z)(1-\alpha^{i_2} z)\cdots(1-\alpha^{i_s} z) \sum_{k=1}^{s} \frac{\alpha^{i_k}}{1-\alpha^{i_k} z} \pmod{z^{2t}}$$

$$= (1-\alpha^{i_2} z)\cdots(1-\alpha^{i_s} z)\alpha^{i_1} + (1-\alpha^{i_1} z)(1-\alpha^{i_3} z)\cdots(1-\alpha^{i_s} z)\alpha^{i_2} + \cdots + (1-\alpha^{i_1} z)(1-\alpha^{i_2} z)\cdots(1-\alpha^{i_{s-1}} z)\alpha^{i_s} \pmod{z^{2t}}$$

と書ける．右辺はzの多項式になっているから$\eta(z)$と書くことができる．

すなわち　$$\eta(z) = \sigma(z)S(z) + \gamma(z)z^{2t} \qquad \text{(A)}$$

ここで$S(z)$とz^{2t}は既知だから($S(z)$はシンドローム多項式で具体的に計算できる）拡張ユークリッドアルゴリズムで$a(z) = \eta(z)$, $b(z) = S(z)$として適用する．（$\deg(a_i(z)) < t-1$となった時点の$a_i(z)$を使う．$\eta(z)$は$t-1$次以下だから）

$$a_i(z) = \phi_i(z)S(z) + \psi_i(x)z^{2t} \qquad \text{(B)}$$

と書ける．(A), (B)を比較して$\sigma(z) = \phi_i(z)$, $\eta(z) = a_i(z)$を得る．

問37（レ）　上の証明の最後の部分に怪しさを感じた人も多いと思います．神保，藤原著補題7.51または，先名著付録IIを参照して証明を試みよ．

ユークリッド復号法

例　$\alpha : GF(2^4)$の原始元とする．αは$x^4+x+1=0$の根とする．$g(x)=M_1(x)M_3(x)$とする．

$g(x)=\mathrm{LCM}\{M_1(x),M_2(x),M_3(x),M_4(x)\}=M_1(x)M_3(x)=(x^4+x+1)(x^4+x^3+x^2+x+1).$

$n=15, n-k=8, k=7$で2重誤り訂正可能である．この符号において110100101101110を受信した．以下のように誤り訂正は行われる．

$S_1=v(\alpha)=\alpha^2, S_2=v(\alpha^2)=v(\alpha)^2=\alpha^4, S_3=v(\alpha^3)=0, S_4=v(\alpha^4)=v(\alpha^2)^2=\alpha^8$だから

$S(z)=\alpha^2+\alpha^4 z+\alpha^8 z^3$

$$\begin{cases} z^4=\alpha^7 z(\alpha^8 z^3+\alpha^4 z+\alpha^2)+\alpha^{11}z^2+\alpha^9 z \\ \alpha^8 z^3+\alpha^4 z+\alpha^2=(\alpha^{12}z+\alpha^{10})(\alpha^{11}z^2+\alpha^9)+\alpha^2 \end{cases}$$

よって

$$\alpha^2=S(z)+(\alpha^{12}z+\alpha^{10})(\alpha^{11}z^2+\alpha^9)=S(z)+(\alpha^{12}z+\alpha^{10})\left(z^4+\alpha^7 zS(z)\right)$$

$$=(\alpha^4 z^2+\alpha^2 z+1)S(z)+(\alpha^{12}z+\alpha^{10})z^4$$

よって　$\sigma(z)=\alpha^4 z^2+\alpha^2 z+1$

$z=1,\alpha,\cdots,\alpha^{14}$まで代入して$\sigma(z)=0$なる根を求めると$z=\alpha^3,\alpha^8$

$\alpha^{-3}=\alpha^{12}, \alpha^{-8}=\alpha^7$なので誤り位置は8ビット目と13ビット目．

110100111101010に訂正される．