情報理論・符号理論の基礎

大阪大学情報科学研究科　渡辺　尚

講義資料（講師版）

2023/ 6/22

改訂履歴

2022/4/26	第１０版
2023/6/22	第１１版

謝辞

広島市立大学小林真博士、大阪大学藤橋卓也博士、元函館工業高等専門学校藤原孝洋博士には、内容の詳細について議論していただいた。ここに記して謝意を表す。

目　次

補足資料１　第２定理の証明　（資料ファイル番号 410）

第５章　誤り訂正符号

５．１　基礎

５．１．１　誤り訂正の方法
５．１．２　組織符号
５．１．３　パリティ符号
５．１．４　ハミング距離と最小ハミング距離
５．１．５　よい(n,k)符号

５．２　ハミング符号

５．２．１　概要
５．２．２　ハミング符号の具体例

５．３　線形符号

５．３．１　符号理論のための群、環、体
５．３．２　ベクトル空間と符号
５．３．３　生成行列と検査行列
５．３．４　ハミング(7,4)符号の例

５．４　ハミング符号詳細－ハミング(7,4)符号を例に－

５．５　線形符号のさらなる議論

５．５．１　最小距離と最小重み
５．５．２　最小距離の求め方
５．５．３　復号の基礎

５．６　積符号・拡張ハミング・短縮ハミング

５．６．１　積符号
５．６．２　拡張ハミング(Extended Hamming Code)
５．６．３　短縮ハミング(Shortened Hamming Code)

補足資料１　ハミング符号詳細　（資料ファイル番号 510）
補足資料２　検査行列と生成行列（零空間の基底）　（資料ファイル番号 521）
補足資料３　検査行列と生成行列　（資料ファイル番号 530）

第６章　誤り訂正符号２（符号の多項式表現と巡回符号）

６．１　基礎

６．２　多項式表現

６．２．１　符号の多項式表現
６．２．２　生成多項式
６．２．３　送信・受信の手順

６．３　巡回符号

６．３．１　巡回符号
６．３．２　巡回符号の生成多項式
６．３．３　割り算回路
６．３．４　巡回符号の符号語の求め方、生成多項式と生成行列、検査行列
６．３．５　巡回ハミングと非巡回ハミング
６．３．６　巡回ハミング符号から BCH 符号への拡張

補足資料１　符号体系、巡回ハミングと非巡回ハミング　（資料ファイル番号 610）

第７章　誤り訂正符号３（BCH, RS, Goppa）

７．１　BCH 符号

７．１．１　概要
７．１．２　拡大体
７．１．３　BCH 詳細
補足資料１　符号語のフーリエ変換と BCH 限界の証明　（資料ファイル番号 710）

７．２　リードソロモン符号

７．２．１　概要
７．２．２　リード・ソロモン符号　具体的な例
７．２．３　ＲＳ詳細（発展）
７．２．４　リードソロモン符号の誤り訂正
７．２．５　BCH と RS のまとめ　　<<――――　　配布はここまで
７．２．６　リード・ソロモン符号の追加例と計算方法　<<-2020 年は授業後 up
７．２．７　３誤り訂正の例１
７．２．８　３誤り訂正の例２
７．２．９　岩垂教科書より
７．２．１０　３次の例１，４次の例１の unb サイトでの確認

７．３　Goppa 符号

７．３．１　概要
７．３．２　定義
７．３．３　ゴッパ符号のパラメータ(n, k, d)
７．３．４　検査行列と生成行列 G
７．３．５　例
７．３．６　McEliece 暗号
７．３．７　発展　　<<―――配布はここまで
７．３．８　Goppa 例の追加（例３、４，５，６）
７．３．９　McEliece 暗号と復号例

７．３．１０　Goppa 符号の復号

７．４　その他の話題

７．４．１　実際に使われている符号

７．４．２　RS とフーリエ変換

７．４．３　BCH 符号、RS 符号の初期値 l

補足資料２　BCH, RS の練習問題　　（資料ファイル番号 721）

補足資料３　ガロア体 GF(3)と原始多項式　（資料ファイル番号 731）

第８章　誤り訂正符号４（たたみ込み符号）

８．１　基礎

８．２　例

８．３　その他

第９章　復号方式

９．１　復号方式

９．１．１　復号の基礎

９．１．２　MAP 復号　最大事後確率復号（maximum a posterior probability decoding）

９．１．３　MLD 復号　最尤復号（maximum likelihood decoding）

９．１．４　MDD 復号　最小距離復号（minimum distance decoding）

９．１．５　BDD 復号　限界距離復号（bounded distance decoding）

９．１．６　いくつかの議論

１）最尤復号 MLD、限界距離復号法 BDD の比較

２）計算複雑度

９．２　符号の限界式（発展）

９．２．１　概要と準備

９．２．２　ハミング限界(Hamming bound)

９．２．３　プロトキン限界(Plotkin bound)

９．２．４　シングルトン限界(Singleton bound)

９．２．５　バルシャモフ-ギルバート限界（Varshamov-Gilbert bound）

第１０章　近年の話題

１０．１　符号理論の近年の話題

１０．１．１　概要

１０．１．２　ターボ符号（turbo code）

情報通信基礎Ⅰ　第１章　情報とエントロピー

2022/ 4/28　情シス　渡辺

ポイント

・情報量の定義

・情報源とは

・情報量、平均情報量、エントロピー

参考書：島田良作、木内陽介、大松繁著「わかる情報理論」　日新出版

１．１　情報量

（１）情報を数量として扱う

情報理論：情報を確率論にもとづいて理論的にあつかう方法

確率：多数の出来事（事象、イベント、通報）が発生する

　　人の心理などは考えない

情報の数量

　情報量(bit)、エントロピー、通信路容量(bps)、真に伝わる情報量（相互情報量）

　情報源符号化定理、通信路符号化定理

情報科学分野で幅広く応用されている

無線伝送路設計、情報記憶、情報検索、データ圧縮、最適符号化、環境観測、時系列予測

通信路を介して送信者と受信者が接続されているモデル

情報源が離散値をとる場合：

　情報源符号化定理

　符号化方式

　　シャノン符号、ハフマン符号

　通信路符号化定理

　　伝送速度と歪の関係を示す。ネットワーク設計の際に重要

情報源が連続値をとる場合：

　情報量の定義、通信路容量の定義

　標本化定理：

　　連続的情報を離散的情報に変換するための定理

　　音声認識やＰＣＭ通信などで活用

（２）情報量

２つの通報を考える。

Ａ：沖縄に雪が降る	ニュースになる
Ｂ：北海道に雪が降る	驚かない

この差は何か。驚きの量が情報量

cf. 真の情報量は周囲の状況によって異なる

聞く人、時間、場所、人の心理状態、etc.

今、情報量を I とする。

①通報の起きる確率（出現確率）を p とするとき、

p 大　　情報量I　少

p 小　　情報量I　多

よって、$I(p)$ は p の単調減少関数である。

②通報A による情報量を I_A とする。

A の内容が、独立な２つの通報BとC の内容の和であるならば、Aによる情報量I_Aは、Bによる情報量I_BとCによる情報量I_Cの和と考えてよい。

$$I_A = I_B + I_C \qquad I(p_A) = I(p_B * p_C) = I(p_B) + I(p_C)$$

すなわち、Iは加法性が成り立つ。

例

A:「沖縄に雪が降り大谷選手がホームランを打った」

B:「沖縄に雪がふる」 C:「大谷選手がホームランを打った」

Aの情報量=B の情報量+C の情報量

③確実に起きることからは情報は得られない。

$$I(p = 1) = 0$$

①②③を満たす関数は、以下の対数関数となる。

$$I = K\ log_a(\frac{1}{p}) \text{ ただし、} K > 0, a > 1$$

【レポート課題】証明せよ

$K = 1$　と決める。

$a = 2$ のとき、$I = log_2\left(\frac{1}{p}\right) = -log_2 p$　　単位は bit (binary unit)

$a = e$ のとき、$I = log_e\left(\frac{1}{p}\right) = -log_e p$　　単位は nat (natural unit)

例：256 本のくじ、１本が当り。当たった時の情報量は？

$$I = -log_2\left(\frac{1}{256}\right) = 8 \text{ bit}$$

年末ジャンボ宝くじが当たった時の情報量は？

１．２　情報源

ある情報源Xがある。この情報源から、n個の通報$s_1, s_2, , , s_n$が、$P_1, P_2, , , P_n$の確率で生起する。この情報源Xを

$$X = \begin{pmatrix} S_1 & S_2 & \cdots & S_n \\ P_1 & P_2 & \cdots & P_n \end{pmatrix} \qquad \sum_{i=1}^{n} P_i = 1$$

と表現する。
（注：これは、iid 情報源の場合であり、より複雑な場合はこれでは表現できない）

例）サイコロ

$$X = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} \end{pmatrix}$$

情報を確率でとらえる＝＞情報源から、通報が多数回繰り返して発生する。

１．３　エントロピー

ある単純な情報源

$X = \begin{pmatrix} S_1 & S_2 \\ P_1 & P_2 \end{pmatrix}$　$(P_1 + P_2 = 1)$を考える。

S_iに対する情報量は、$I_i = -logP_i$ である。これらの平均を取る。すなわち、

$$H = P_1 * I_1 + P_2 * I_2 = \sum_{i=1}^{2} P_i * I_i = -\sum_{i=1}^{2} P_i * logP_i \ \text{(bit)}$$

を、情報源Xの平均情報量、または、エントロピーと言う。
通報の数がn個の一般的な場合は、

$X = \begin{pmatrix} S_1 & S_2 & \cdots & S_n \\ P_1 & P_2 & \cdots & P_n \end{pmatrix}$　　$\sum_i P_i = 1$　に対して、

$H = -\sum_{i=1}^{n} P_i * logP_i$　(bit)
となる。

情報量は、個別の通報が生起したときの量を表現しているのに対し、エントロピーは情報源X全体の量を表現している。

何回も繰り返す。１回毎ではなく全体としてどの程度の情報量があるか＝エントロピー

例１）ある地方１の天気

$$X_1 = \begin{pmatrix} 晴れ & くもり & 雨 & 雪 \\ \frac{1}{2} & \frac{1}{4} & \frac{1}{8} & \frac{1}{8} \end{pmatrix}$$

$I(晴れ) = -\log\left(\frac{1}{2}\right) = 1$　$I(くもり) = -\log\left(\frac{1}{4}\right) = 2$　$I(雨) = I(雪) = -\log\left(\frac{1}{8}\right) = 3$

エントロピー

$$H_1 = P(晴れ) * I(晴れ) + P(くもり) * I(くもり) + P(雨) * I(雨) + P(雪) * I(雪)$$

$= 7/4(\text{bit})$

例２）ある地方２の天気

$$X_2 = \begin{pmatrix} \textit{晴れ} & \textit{くもり} & \textit{雨} & \textit{雪} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \end{pmatrix} \qquad H_2 = I\left(\textit{晴れ}\right) = 2\ (bit)$$

考察　$H_1 < H_2$　の原因は何か？　確率の偏り

確率が偏っている－＞予想が立てやすい－＞エントロピーが小さい

例３）ある地方３の天気

$$X_3 = \begin{pmatrix} \textit{晴れ} & \textit{くもり} & \textit{雨} & \textit{雪} \\ 1 & 0 & 0 & 0 \end{pmatrix} \qquad H_3 = 0\ (bit)$$

完全に予想が立つ。ただし、$\lim_{x\to 0} x\log x = 0$

例４）くじ　２５６本

$$X_4 = \begin{pmatrix} \textit{1等} & \textit{2等} & \textit{3等} & \textit{4等} \\ \frac{1}{256} & \frac{2}{256} & \frac{4}{256} & \frac{249}{256} \end{pmatrix} \quad H_4 = \frac{46+9.96}{256} = 0.22\ (bit)$$

一等が当たったときは大きいが、全体の平均の情報量（エントロピー）は小さい。つまり、ほとんどはずれる、という予測が立つ。

例５）アルファベット文字の生起確率

表1-1　英語のアルファベットにおける文字の生起確率

文字	生起確率	文字	生起確率	文字	生起確率
スペース	0.1859	H	0.0467	G	0.0152
E	0.1031	L	0.0321	P	0.0152
T	0.0796	D	0.0317	B	0.0127
A	0.0642	U	0.0228	V	0.0083
O	0.0632	C	0.0218	K	0.0049
I	0.0575	F	0.0208	X	0.0013
N	0.0574	M	0.0198	J	0.0008
S	0.0514	W	0.0175	Q	0.0008
R	0.0484	Y	0.0164	Z	0.0005

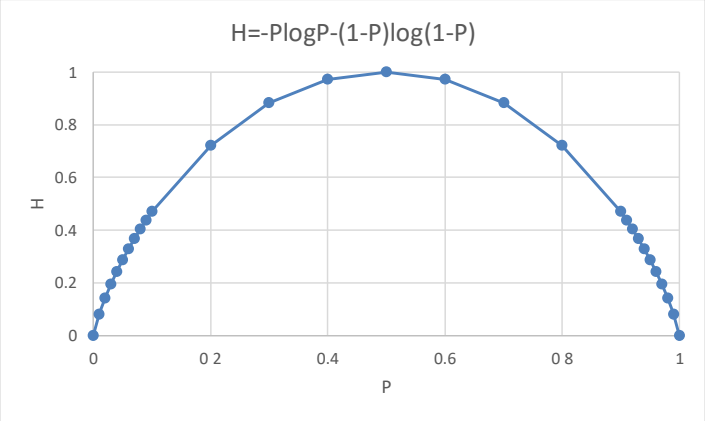
島田他:「わかる情報理論」より

１．４　エントロピーの最大値、最小値

最も単純な２元情報源を考える。

$$X = \begin{pmatrix} S_1 & S_2 \\ P & 1-P \end{pmatrix} \qquad H = -PlogP - (1-P)\log(1-P)$$

【図】グラフ　横軸 P, 縦軸 H



（課題　このグラフを考察せよ）

通報の数がn個の情報源を　$X=\begin{pmatrix}S_1 & S_2 & \cdots & S_n\\ P_1 & P_2 & \cdots & P_n\end{pmatrix}$　$\sum_i P_i=1$

とする時、エントロピーHが最大となるのは、$P_i=\frac{1}{n}$の時である。
（課題　上記を証明せよ。）

【証明】Lagrange の未定定数法を用いる。（P. 7 参照）

$f(x)=-\sum x_i lnx_i$の最大値を$|X|=1$のの条件下で求める。ただし、Xは、
$X=(x_1,x_2,,,,x_n)0\le x_i\le 1$の確率ベクトルである。

制約条件を　$g(X)=\sum x_i-1=0$　として、
関数　$F(X,\lambda)=f(X)+\lambda g(X)=-\sum x_i lnx_i+\lambda(\sum x_i-1)$　を考える。

$$\frac{\partial F(X,\lambda)}{\partial x_i}=-[x_i lnx_i]'+\lambda[x_i]'=-\left(lnx_i+\frac{x_i}{x_i}\right)+\lambda=-lnx_i-1+\lambda=0$$

$\therefore x_i=e^{\lambda-1}$　この値は、iには無関係なので$g(X)=0$より、$x_i=\frac{1}{n}$

以上より、$x_i=\frac{1}{n}$の時、$f(x)=-\sum x_i lnx_i$は最大となる。
上記の議論は、底が e の場合である。底が 2 の場合については、定数倍すれば同等の議論ができる。

１．５　典型的系列（typical sequence）

代表的系列とも言う。

エントロピーHの情報源Xから次々と文字が生起する。

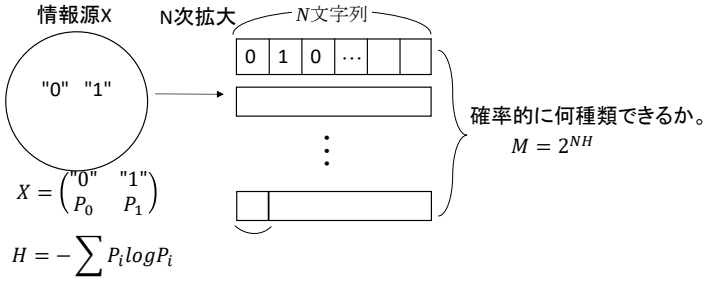
文字をN 個連ねて文字系列を作成する。これをN文字系列と表現する。

Nが十分大きい場合、ほぼ典型的な文字系列だけが生成される。

典型的なN文字系列の種類は、$M = 2^{NH}$　である。

【図】（簡略証明）

典型的系列



①一文字あたりの情報量　H

一文字列あたりの情報量　NH (1)　（N文字は独立に生起する）

②Nが十分大きいので、P0, P1の偏りは、一文字列の中の0と1の個数にのみ反映する。つまり、M個の文字列の出現頻度は等しいと考えてよい。$(1/M)$

よって一文字列あたりの情報量は、$-logp = -log\frac{1}{M} = logM$ (2)

③（1）＝（2）だから　$NH = logM$　　$M = 2^{NH}$

例１）$P_0 = P_1 = \frac{1}{2}$の時、$H = 1$。よって$M = 2^{NH} = 2^N$　　：全組合せが発生する

例２）$P_0 = 1,\ P_1 = 0$の時、$H = 0$。よって$M = 2^{NH} = 1$　　：１種類しかできない

典型的系列の議論は、情報源がn元の$X = \begin{pmatrix} S_1 & S_2 & \cdots & S_n \\ P_1 & P_2 & \cdots & P_n \end{pmatrix}$の場合も成立する。

例　$X = \begin{pmatrix} S_1 & S_2 & S_3 \\ P_1 & P_2 & P_3 \end{pmatrix}$ $P_1 = P_2 = P_3 = \frac{1}{3}$の時、$H = log3$。よって$M = 2^{NH} = 2^{Nlog3} = 3^N$

情報通信基礎Ⅰ　第１章　ラグランジェの未定乗数法

ラグランジェの未定乗数法　Lagrange's method of indeterminate co-efficiency
(Method of Lagrange Multipliers)

２変数x, yの関数$f(x,y)$を制約条件$g(x,y)=0$の元で、最大化する。

$F(x,y,\lambda)=f(x,y)+\lambda g(x,y)$ と置き、

$\frac{\partial F}{\partial x}=0$　$\frac{\partial F}{\partial y}=0$　$\frac{\partial F}{\partial \lambda}=0$

で得られる連立方程式を満たす$\hat{x}$, $\hat{y}$　が$f(x,y)$の最大値を与える。

情報通信基礎Ⅰ　第１章

レポート課題１

情報量$I(P)$は、以下の性質を持つ。

① $I(P)$は、Pの単調減少関数

② $I(P)$は、加法性が成立する。すなわち、$I(P_1 \cdot P_2) = I(P_1) + I(P_2)$

③ $I(1) = 0$

このとき、

$I(P) = K \log_a \frac{1}{P}$　ただし、$K > 0 \quad a > 1$　　（１）

である。

【証明のヒント】

１）十分性の証明

（１）－＞①②③　　自明

２）必要性の証明

$\frac{I(P)-I(P-\varepsilon P)}{\varepsilon P}$ を考える。ただし、εは、$0 < \varepsilon < 1$の任意の小さい数

$$I(P - \varepsilon P) = I(P) + I(1 - \varepsilon)$$

$$\lim_{\varepsilon \to +0} \frac{I(P) - I(P - \varepsilon P)}{\varepsilon P} = I'(P)$$

この微分方程式を③の境界条件で解く。なお、$\lim_{\varepsilon \to +0} \frac{I(1-\varepsilon)}{\varepsilon} = 定数$　とする。

情報通信基礎Ⅰ　第２章　相互情報量

情シス　渡辺

ポイント

・情報源が複数

・結合エントロピー、条件付きエントロピー、相互情報量

参考書：島田良作、木内陽介、大松繁著「わかる情報理論」　日新出版

２．１　結合エントロピー

情報源XとYを考える。すなわち、

$$X=\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ P(x_1) & P(x_2) & \cdots & P(x_n) \end{pmatrix} \qquad \sum_{i=1}^{n} P(x_i)=1$$

$$Y=\begin{pmatrix} y_1 & y_2 & \cdots & y_m \\ P(y_1) & P(y_2) & \cdots & P(y_m) \end{pmatrix} \qquad \sum_{j=1}^{m} P(y_j)=1$$

XとYを組み合わせた情報源$X\cdot Y$（結合情報源）を考える。(x_1,y_1)などを結合事象と呼ぶ。

$$X\cdot Y=\begin{pmatrix} (x_1,y_1) & (x_1,y_2) & \cdots & (x_2,y_1) & (x_2,y_2) & \cdots & (x_n,y_m) \\ P(x_1,y_1) & P(x_1,y_2) & \cdots & P(x_2,y_1) & P(x_2,y_2) & \cdots & P(x_n,y_m) \end{pmatrix}$$

$$\sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i,y_j)=1$$

情報源$X\cdot Y$のエントロピーは、

$$H(X,Y)=-\sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i,y_j)*\log P(x_i,y_j)$$

となる。これを結合エントロピーと呼ぶ。単位は bit。

例２．１）コインを２回投げる

$$X\cdot Y=\begin{pmatrix} (H,H) & (H,T) & (T,H) & (T,T) \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \end{pmatrix}$$

$$H(X,Y)=\left(-\frac{1}{4}\log\frac{1}{4}\right)*4=2 \ \text{(bit)}$$

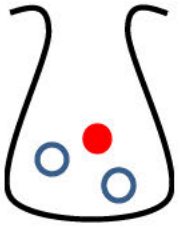
ちなみに、1 回目のコイン投げを X とし、2 回目のコイン投げを Y と表現すると、

$$X=\begin{pmatrix} H & T \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \quad H(X)=\left(-\frac{1}{2}\log\frac{1}{2}\right)*2=1$$

$$Y=\begin{pmatrix} H & T \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \quad H(Y)=\left(-\frac{1}{2}\log\frac{1}{2}\right)*2=1$$

よって、この例では、$H(X,Y)=H(X)+H(Y)$が成立している。（後に見るように常に等号が成立するわけではない。）

例２．２）赤玉１個と白玉２個が袋に入っている。１回目の玉の色をＸ、２回目の玉の色をＹとする。ただし、１回目の玉は戻さない。ＸとＹからなる結合情報源のエントロピーを求めたい。



まず、以下の表のように結合確率を求める。(玉の色を赤R，白Wと表現し、一回目に赤が出て２回目に赤が出る結合確率を $P(X=R,Y=R)$と表現する。)

【表】

	Y=R	Y=W	周辺分布
X=R	$\frac{1}{3}\times\frac{0}{2}=0$	$\frac{1}{3}\times\frac{2}{2}=\frac{1}{3}$	$0+\frac{1}{3}=\frac{1}{3}$
X=W	$\frac{2}{3}\times\frac{1}{2}=\frac{1}{3}$	$\frac{2}{3}\times\frac{1}{2}=\frac{1}{3}$	$\frac{1}{3}+\frac{1}{3}=\frac{2}{3}$
周辺分布	$0+\frac{1}{3}=\frac{1}{3}$	$\frac{1}{3}+\frac{1}{3}=\frac{2}{3}$	

$$H(X,Y)=-0log0-\frac{1}{3}log\frac{1}{3}-\frac{1}{3}log\frac{1}{3}-\frac{1}{3}log\frac{1}{3}=-log\frac{1}{3}=log3\ \approx 1.58$$

ちなみに、

$$H(X)=-\frac{1}{3}log\frac{1}{3}-\frac{2}{3}log\frac{2}{3}=log3-\frac{2}{3}$$
$$H(Y)=-\frac{1}{3}log\frac{1}{3}-\frac{2}{3}log\frac{2}{3}=log3-\frac{2}{3}$$
$$H(X)+H(Y)=2log3-4/3 \qquad \approx 1.83$$

２．２　条件付きエントロピー

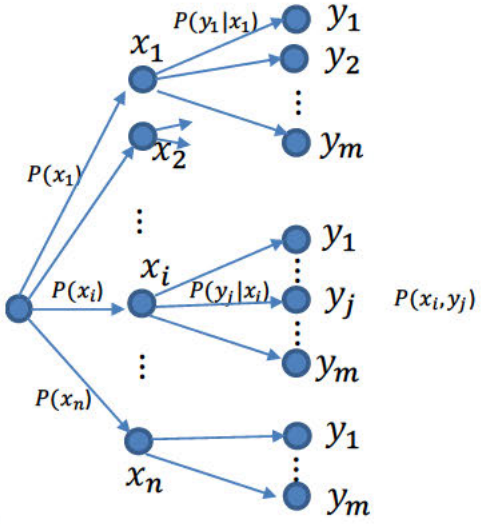
情報源XとYを考える。

$$X=\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ P(x_1) & P(x_2) & \cdots & P(x_n)\end{pmatrix} \qquad \sum_{i=1}^{n}P(x_i)=1$$

$$Y=\begin{pmatrix} y_1 & y_2 & \cdots & y_m \\ P(y_1) & P(y_2) & \cdots & P(y_m)\end{pmatrix} \qquad \sum_{j=1}^{m}P(y_j)=1$$

今情報源Xでx_iが生起したことを知った上で、情報源Yで生起する事象を考える。図のような分岐図を書くことができる。

【図】分岐図



x_iが分かったとき、Yに関してどの程度情報が分かるか。

もし、XとYが無関係（独立）

x_iが分かっても、Yに関して何も情報が得られない。

もし、XとYが関係あり（従属）

x_iが分かると、Yに関して何か情報が得られる。すなわち、曖昧さが減って予想が立ちやすくなる。

準備

１）ベイズ則

$$\mathrm{P}(x_i, y_j) = \mathrm{P}(y_j|x_i)P(x_i)$$

２）周辺分布

$$\mathrm{P}(x_i) = \sum_j \mathrm{P}(x_i, y_j)$$

ここで、x_iが出た条件の下での情報源$Y|x_i$を考える。

$$Y|x_i = \begin{pmatrix} (y_1|x_i) & (y_2|x_i) & \cdots & (y_j|x_i) & \cdots & (y_m|x_i) \\ P(y_1|x_i) & P(y_2|x_i) & \cdots & P(y_j|x_i) & \cdots & P(y_m|x_i) \end{pmatrix}$$

ただし、$\sum_j P(y_j|x_i) = 1$

このエントロピーは、

$$H(Y|x_i) = -\sum_j P(y_j|x_i) log P(y_j|x_i)$$

である。（x_iが生起したと言う条件の下での、Yの予想の立てにくさ）

これをXについても平均する。

$$H(Y|X) = \sum_{i=1}^{n} P(x_i)H(Y|x_i) = -\sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i)P(y_j|x_i) log P(y_j|x_i)$$
$$= -\sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i, y_j) log P(y_j|x_i)$$

これを条件付きエントロピーと呼ぶ。

同様に、

$$H(X|Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i, y_j) log P(x_i|y_j)$$

例２．２では、２回目の玉の色から１回目の玉の色に関する情報量を考えていることになる。時間に逆行している。しかし、情報通信では重要。

例２．３）例２．２）と同様に、赤玉１個と白玉２個が袋に入っている。１回目の玉の色をX、２回目の玉の色をYとする。ただし、１回目の玉は戻さない。条件付きエントロピーを求めたい。

$$H(Y|X) = -\sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i, y_j) log P(y_j|x_i)$$

$P(Y = R|X = R) = \frac{0}{2}$　$P(Y = W|X = R) = \frac{2}{2} = 1$

$P(Y = R|X = W) = \frac{1}{2}$　$P(Y = W|X = W) = \frac{1}{2}$

$H(Y|X) = -0 \cdot \log\frac{0}{2} - \frac{1}{3} \cdot \log 1 - \frac{1}{3} \cdot \log\frac{1}{2} - \frac{1}{3} \cdot \log\frac{1}{2} = \frac{2}{3} = 0.67$ (bit)

$H(Y) = \log 3 - \frac{2}{3} = 0.92$

$H(Y) > H(Y|X)$　　この差は何か。

注意　この例では、$H(X) = H(Y)$　$H(Y|X) = H(X|Y)$ であるが、常に成立するわけではない。演習問題２．１参照。

２．３　エントロピーの性質

① $H(X,Y) = H(X) + H(Y|X)$

左辺：XとYを結合した情報源のエントロピー（曖昧さ、予想の立てにくさ）

右辺第一項：Xのエントロピー（曖昧さ、予想の立てにくさ）

右辺第二項：Xに関して分かったときのYのエントロピー（曖昧さ、予想の立てにくさ）

証明　　数式で解ける

② $H(X,Y) = H(Y) + H(X|Y)$

③ $H(Y) \geq H(Y|X)$

シャノンの不等式と呼ぶ。

左辺：Yの曖昧さ

右辺：Xに関して分かったときのYの曖昧さ

同様に、$H(X) \geq H(X|Y)$

④ $H(X) + H(Y) \geq H(X,Y)$

証明は、①と③より自明。

２．４　相互情報量

シャノンの不等式の差分、すなわち

$$I(X;Y) = H(X) - H(X|Y) = \sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i, y_j) log \frac{P(x_i, y_j)}{P(x_i)P(y_j)}$$

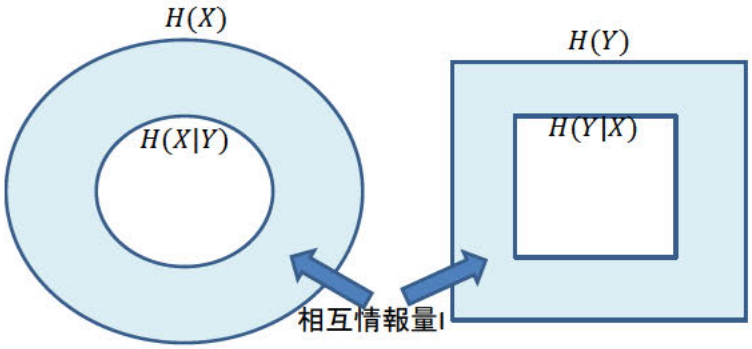
を相互情報量と呼ぶ。

$I(X;Y) = H(X) - H(X|Y)$

Yを知ることによって、どの程度Xの曖昧さが減ったか。どの程度予想が立てやすくなったか。つまり、Yから間接的にXについて得られる情報量。

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = H(X) + H(Y) - H(X,Y) = I(Y;X)$$

【図】



（課題　演習問題２．１～２．３）

例２．４）試験の出来具合と表情

表情から試験の出来具合を予想できるか。

A 君

	にこにこy_1	しずんでいるy_2	無表情y_3	周辺分布
できたx_1	0.45	0	0.05	0.50
できないx_2	0	0.45	0.05	0.50
周辺分布	0.45	0.45	0.10	

$H(X) = -\frac{1}{2}log\frac{1}{2} - \frac{1}{2}log\frac{1}{2} = 1$ (bit)

$P(x_1|y_1) = \frac{P(x1,y1)}{P(y1)} = \frac{0.45}{0.45} = 1$　$P(x_1|y_2) = 0$　$P(x_1|y_3) = \frac{0.05}{0.10} = 0.5$

$P(x_2|y_1) = 0$　$P(x_2|y_2) = \frac{0.45}{0.45} = 1$　$P(x_2|y_3) = \frac{0.05}{0.10} = 0.5$

$$H(X|Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i, y_j) log P(x_i|y_j)$$

$= -0.45log1 - 0log0 - 0.05log0.5 - 0log0 - 0.45log1 - 0.05log0.5 = 0.1$ (bit)

$I(X;Y) = H(X) - H(X|Y) = 0.9$ (bit)表情Yから試験の出来具合Xに関して得られた情報量

表情を見るとできたかおおよそ分かる。

B 君

	にこにこy_1	しずんでいるy_2	無表情y_3	周辺分布
できたx_1	0	0	0.50	0.50
できないx_2	0	0	0.50	0.50
周辺分布	0	0	1	

$H(X) = 1$　$H(X|Y) = 1$　$I(X;Y) = H(X) - H(X|Y) = 0$　　表情を見ても分からない。

C 君

	にこにこy_1	しずんでいるy_2	無表情y_3	周辺分布
できたx_1	0.50	0	0	0.50
できないx_2	0	0.50	0	0.50
周辺分布	0.50	0.50	0	

$H(X)=1$　$H(X|Y)=0$　　$I(X;Y)=H(X)-H(X|Y)=1$　　表情を見ると完全に分かる。

２．５　離散的情報源の種類

２．５．１　記憶のない情報源 Memoryless Information Source （IS)

情報源からの記号の発生が独立に生じる。

２．５．２　定常情報源　Stationary IS

時刻 t における記号の発生と、時刻 t+α における記号の発生が不偏（確率分布が同一）

２．５．３　記憶のない定常情報源　Independently and identically distributed IS (i.i.d.)

２．５．１＋２．５．２

２．５．４　エルゴード情報源 Ergodic IS

エルゴード性を持つ IS　【図】

十分長い系列に統計的な性質が完全に含まれている。

２．５．５　拡大情報源

$$X=\begin{pmatrix} S_1 & S_2 & S_3 \\ P_1 & P_2 & P_3 \end{pmatrix}$$

$$X^2=\begin{pmatrix} S_1S_1 & S_1S_2 & \cdots & S_3S_3 \\ P_1P_1 & P_1P_2 & \cdots & P_3P_3 \end{pmatrix}$$

２次拡大情報源　（課題　演習問題３．３）

２．５．６　マルコフ情報源

２．６　マルコフ情報源

情報源から、１秒に１回文字が生起することとする。ある時刻tに生起する文字が、時刻$t-1$，$t-2$,,, $t-M$に生起した文字に依存するとき、M 重マルコフ情報源という。

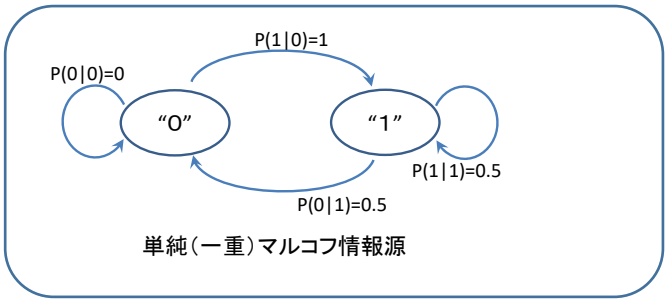
M=0　過去の文字に依存しない場合　０重マルコフ情報源、無記憶情報源

M=1　過去の１文字に依存する場合　１重マルコフ情報源、単純マルコフ情報源

例）英語のアルファベット

例２．５）１重マルコフ情報源X_1

【図】



このエントロピーH_1を求める方法

①$P(0), P(1)$の定常状態確率を求める。

定常状態方程式 $\vec{\pi} = \vec{\pi}\boldsymbol{P} \quad |\vec{\pi}| = 1$

$\vec{\pi}$：定常状態確率ベクトル　$\vec{\pi} = [\pi_1, \pi_2, , , \pi_n]$　　π_i：状態iの定常状態確率

$\boldsymbol{P}$：遷移確率行列　$\boldsymbol{P} = [P(j|i)]$ 状態iから状態jに遷移する確率

上記の例では、$\vec{\pi} = [\pi_1, \pi_2] = [P(0), P(1)] \quad \boldsymbol{P} = \begin{bmatrix} P(0|0) & P(1|0) \\ P(0|1) & P(1|1) \end{bmatrix}$

$$P(0) = P(0)P(0|0) + P(1)P(0|1)$$
$$P(1) = P(0)P(1|0) + P(1)P(1|1)$$
$$P(0) + P(1) = 1$$

これを解くと　$P(0) = \frac{1}{3} \quad P(1) = \frac{2}{3}$

②エントロピーH_1は、

$$H_1 = -\sum_{i=1}^{n}\sum_{j=1}^{m} P(x_1, x_2) log P(x_2|x_1) = -\frac{1}{3}(0log0 + 1log1) - \frac{2}{3}\left(\frac{1}{2}log\frac{1}{2} + \frac{1}{2}log\frac{1}{2}\right) = \frac{2}{3}$$
$$= 0.67$$

参考）０と１がそれぞれ$P(0), P(1)$の確率で無記憶で発生する情報源X_0

$$X_0 = \begin{pmatrix} 0 & 1 \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix}$$

$$H_0 = -\sum \quad P_i * log P_i = -\frac{1}{3}log\frac{1}{3} - \frac{2}{3}log\frac{2}{3} = log3 - \frac{2}{3} = 0.918$$

よって、$H_1 < H_0$

１重マルコフ情報源X_1の方が予想が立てやすい。例えば、０の次は必ず１であるから。

（発展　２重マルコフ情報源について調べよ。さらに、M 重マルコフ情報源のエントロピーを求める方法を調べよ。）

情報通信基礎Ⅰ　第３章　情報源符号化

情シス　渡辺

ポイント

・情報源符号化の定理（シャノンの第一定理）

・ハフマン符号化、シャノン符号化

同じ情報量を送るなら少ない文字数の方がいい！　どうしたらよいか。

我々が日常で行っていることは何か？

スマートホンー＞スマホ

パーソナルコンピューターー＞パソコン

情報源符号化定理ー＞情報源符号化定理　情定とは言わない。なぜか？

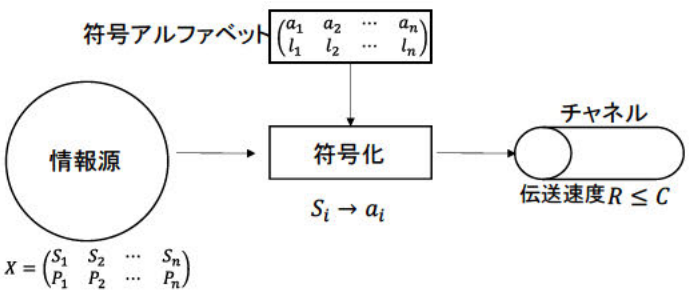
一方で、それに潜む危険は何か。ー＞第４章に

参考書：島田良作、木内陽介、大松繁著「わかる情報理論」　日新出版

３．１　基礎

【図３．１】

符号化の概念（１）



符号化：S_iを別のa_iに一対一に割り当てる。

符号アルファベットa_i　の例【図３．２】

（０，１）、（アナログ信号）、（日本語のあいうえお）、（モールス信号）等（補足資料２）

情報源Xのエントロピーは、

$H(X) = -\sum_{i=1}^{n} P_i * \log P_i$　である。

一方で、一符号語の平均長（時間；平均符号語長）Lは、$\sum_{i=1}^{n} P_i * l_i$

従って、情報伝送速度Rは、（１符号語の持つ情報量）/（１符号語の伝送時間）であり、以下で表現できる。

$$R = \frac{H}{L}$$

単位は、(bit/sec)。

Rは、大きいほどよい。　つまり、

$$R = \frac{H}{L} = \frac{-\sum_{i=1}^{n} P_i * \log P_i}{\sum_{i=1}^{n} P_i * l_i}$$

を最大化するにはどうしたらよいかを考える。

アプローチ１）l_i　が与えられたとき、Rを最大化するP_iを求める。

［定理３．１］

Rの最大値Cは、

$$\sum_{i=1}^{n} 2^{-Cl_i} = 1$$

の正の根で与えられる。

このとき、

$$P_i = 2^{-Cl_i}$$

となる。

（課題　証明せよ）

ヒント

ラグランジュの未定乗数法を用いる。

$F(P_1, P_2, , , P_n, \lambda) = R(P_1, P_2, , , , P_n) + \lambda(\sum P_i - 1)$　　として、これを各変数で偏微分して、

$\frac{\partial F}{\partial P_i} = 0$　$\frac{\partial F}{\partial \lambda} = 0$　　を解く。

C:　通信路に誤りがない場合には、Rの最大値Cはそのまま通信路の最大伝送速度になる。このためCは通信路容量と呼ばれる。

例３．１）　符号アルファベット集合が$\begin{pmatrix} a & b & c \\ 1 & 2 & 2 \end{pmatrix}$のときの通信路容量を求めよ。

$$\sum_{i=1}^{n} 2^{-Cl_i} = 2^{-C} + 2^{-2C} + 2^{-2C} = 1$$

$x = 2^{-C} > 0$ とすると、$x + x^2 + x^2 = 1$

これを解いて、$x = \frac{1}{2}$、$C = 1$を得る。よって、

$P_a = 2^{-C} = \frac{1}{2}$　$P_b = 2^{-2C} = \frac{1}{4}$　$P_c = 2^{-2C} = \frac{1}{4}$

とすれば、Rは最大値Cをとる。

この例からも分かるように、小さいl_iの符号アルファベットには、大きなP_i　のS_iを割り当てることがポイントである。

アプローチ２）P_i　が与えられたとき、Rを最大化するl_iを求める。

l_iを変化させ、$P_i = 2^{-Cl_i}$　を満足するように決める。

例３．２）

$X = \begin{pmatrix} S_1 & S_2 & S_3 & S_4 \\ \frac{1}{2} & \frac{1}{4} & \frac{1}{8} & \frac{1}{8} \end{pmatrix}$ のとき、

$S_1 \to a_1$　　0　$l_1 = 1$

$S_2 \to a_2$　　１０　$l_2 = 2$

$S_3 \to a_3$　１１０　$l_3 = 3$

$S_4 \to a_4$　１１１　$l_4 = 3$

と符号化すると、

$\sum_{i=1}^{n} 2^{-Cl_i} = 2^{-C} + 2^{-2C} + 2^{-3C} + 2^{-3C} = 1$　より、

$C = 1$　であり、$P_i = 2^{-Cl_i}$　とうまく一致している。

アプローチ３）実際には、l_i　や　P_i には制約があって、必ずしも満足させることができない。

例えば、① P_i やl_iが何らかの理由で固定の場合、② l_iが０，１の個数で決定される離散値の場合、など。どうしたらよいか。

cf.　　アプローチ１、２は、

S_i, P_i　→　a_i, l_i のように一対一で対応させている。

$S_1S_2S_2 \to a_1a_5a_6a_8$　などとまとめて符号化する。

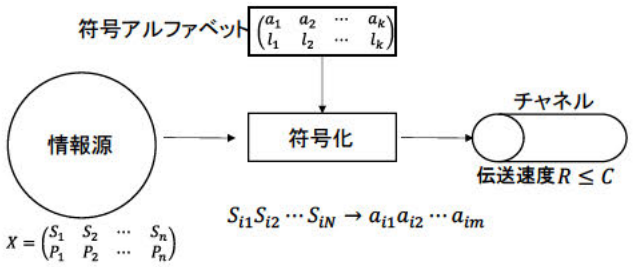
（確率$P_1P_2P_2$で生起する事象に、$l_1 + l_5 + l_6 + l_8$の長さの符号を割り当てる。）

つまり、

S_iの文字列をa_jの文字列に対応させ、$\prod P_i = 2^{-C\sum l_j}$ として自由度を上げれば、Rを最大化できる可能性がある。

３．２　情報源符号化の定理

【図３．３】　　符号化の概念（２）



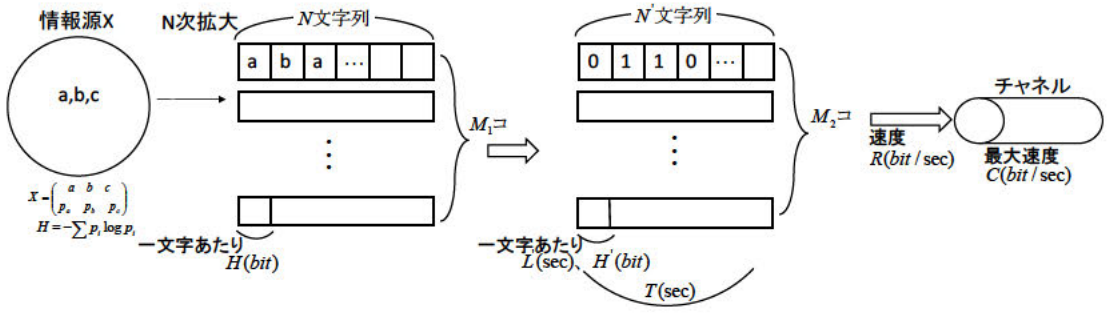
［シャノン第１定理（情報源符号化定理）］

情報源のエントロピーをH(bit)、通信路容量をC(bit/sec)とするとき、

$\frac{C}{H}(1-\varepsilon)$個/sec で伝送可能な符号が存在する。εは、任意に小さい正数。

（別形式　今井秀樹著「情報理論」昭晃堂 p.76）平均符号語長を$\bar{m}$とするとき、$H \le \bar{m} < H + \varepsilon$　となる符号化が存在する。（クラフトの不等式を満たす２元可分符号の場合）補足資料１

【図３．４】シャノン第１定理の証明



① $M_1 = 2^{NH}$

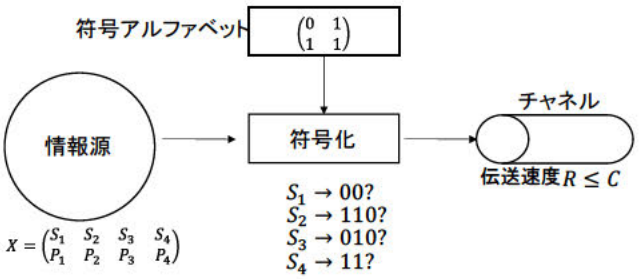
②チャネル側から見ると $M_2 = 2^{N'H'} = 2^{\frac{T}{L}H'} = 2^{T\frac{H'}{L}} = 2^{CT}$ $\because \frac{H'}{L'} = \frac{\text{一文字当たりの情報量}}{\text{一文字を送る時間}} = R = C(\text{最大の時})$

③原理的には、$M_1 = M_2$かつ1対1に対応すればよい。①=② $NH = CT$

④実際には $\frac{N}{T} = \frac{C}{H}$は常には実現できないから、$\frac{N}{T} = \frac{C}{H}(1-\varepsilon)$ 左辺：一秒当たりに送れる文字数（個／秒）

３．３　符号の性質

【図３．５】　符号の性質



３．３．１　一意に復号可能、瞬時に復号可能

a)符号化方法１

$S_1 \to$　０　　$m_1 = 1$（符号語長）

$S_2 \to$　１０　　$m_2 = 2$

$S_3 \to$　１１０　　$m_3 = 3$

$S_4 \to$　１１１０　$m_4 = 4$

このとき、０１０１１０１０・・を受信した。復号できるか。

０　１０　１１０　１０・・・

S_1　S_2　S_3　・・・

一意に復号可能

b)符号化方法２

$S_1 \to$　０　　$m_1 = 1$（符号語長）

$S_2 \to$　１０　　$m_2 = 2$

$S_3 \to$　１１　　$m_3 = 2$

$S_4 \to$　１１０　　$m_4 = 3$

このとき、０１０１１０１０・・を受信した。復号できるか。

０　１０　１１０　１０・・・

S_1　S_2　$S_3?S_4?$　・・・

一意に復号不可能

c)符号化方法３

$S_1 \rightarrow$　０　　$m_1 = 1$（符号語長）

$S_2 \rightarrow$　０１　　$m_2 = 2$

$S_3 \rightarrow$　０１１　　$m_3 = 3$

$S_4 \rightarrow$　０１１１　$m_4 = 4$

このとき、０１０１１０１０・・を受信した。復号できるか。

０１　０１１　０１　０・・・

S_2---↑　S_3---↑S_2---↑・・・

一意に復号可能　ただし、瞬時に復号は不可能

Kraft の不等式

一意に復号可能な条件

情報源Xを以下とする。

$$X = \begin{pmatrix} S_1 & S_2 & \cdots & S_n \\ P_1 & P_2 & \cdots & P_n \end{pmatrix} \qquad \sum_{i=1}^{n} P_i = 1$$

S_iに割り当てられた符号語の長さをm_iとする。

符号アルファベットがk個（k進）の場合、一意に復号可能な符号化は、以下の不等式を満たす。

$$\sum_{i=1}^{n} k^{-m_i} \leq 1$$

（課題：証明せよ。ヒント符号木において、すべての符号語を木の終端節点に対応するように構成する。）

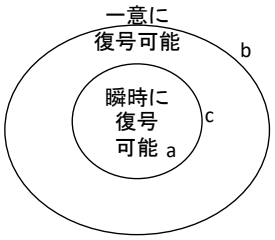
a) c)の場合、

$$\sum_{i=1}^{n} 2^{-m_i} = 2^{-1} + 2^{-2} + 2^{-3} + 2^{-4} = 15 \cdot 2^{-4} = \frac{15}{16} \leq 1$$

b)の場合、

$$\sum_{i=1}^{n} 2^{-m_i} = 2^{-1} + 2^{-2} + 2^{-2} + 2^{-3} = 9 \cdot 2^{-3} > 1$$

【図３．６】一意に復号可能、瞬時に復号可能



（発展　一意性、瞬時性に関しては、マクミランの不等式、サーディナスパターソン定理など）

３．３．２　平均符号語長

情報源$X=\begin{pmatrix}S_1 & S_2 & \cdots & S_n\\ P_1 & P_2 & \cdots & P_n\end{pmatrix}$から生起する文字列が、符号アルファベットの集合

$\begin{pmatrix}a_1 & a_2 & \cdots & a_n\\ m_1 & m_2 & \cdots & m_n\end{pmatrix}$を用いて一対一に符号化される時、符号語長の平均（平均符号語長）$\bar{m}$は、以下で計算される。

$$\bar{m}=\sum_{i=1}^{n}P_i m_i$$

（簡単のため、符号化の概念（１）と同じ条件としたが、符号化の概念（２）でも同様の議論ができる。）

平均符号語長$\bar{m}$　は、小さいほどよい。

［定理３．２］

Kraft の不等式を満たす符号は、

$$H\le \bar{m}\cdot logk < H+logk$$

を満たす。（課題　証明せよ。）

証明中　　$-log_k P_i \le m_i < -log_k P_i+1$　　－＞シャノンの符号化

［定理３．２］の解釈（$k=2$ とすると）

・$\bar{m}$をHより小さくはできない。

・$\bar{m}$を$H+1$以下にはできる。

a)符号化方法１の場合

$S_1\rightarrow$　０　　$m_1=1$　　$P_1=\frac{1}{2}$

$S_2\rightarrow$　１０　　$m_2=2$　　$P_2=\frac{1}{4}$

$S_3\rightarrow$　１１０　　$m_3=3$　　$P_3=\frac{1}{8}$

$S_4\rightarrow$　１１１０　　$m_4=4$　　$P_4=\frac{1}{8}$

$\bar{m}=\frac{1}{2}\cdot 1+\frac{1}{4}\cdot 2+\frac{1}{8}\cdot 3+\frac{1}{8}\cdot 4=\frac{15}{8}$　　$H=\frac{14}{8}$　　$\therefore H<\bar{m}<H+1$

d)符号化方法４

$S_1\rightarrow$　０　　$m_1=1$　　$P_1=\frac{1}{2}$

$S_2\rightarrow$　１０　　$m_2=2$　　$P_2=\frac{1}{4}$

$S_3\rightarrow$　１１０　　$m_3=3$　　$P_3=\frac{1}{8}$

$S_4 \rightarrow$　　１１１　　$m_4 = 3$　　$P_4 = \frac{1}{8}$

一意に復号可能、瞬時に復号可能

$\bar{m} = \frac{1}{2} \cdot 1 + \frac{1}{4} \cdot 2 + \frac{1}{8} \cdot 3 + \frac{1}{8} \cdot 3 = \frac{14}{8}$　　$H = \frac{14}{8}$　　$\therefore H = \bar{m}$　非常によい符号化

３．４　具体的な符号化方法

１）シャノンの符号化

（１）生起確率P_iの高い順に上から並べる。

（２）累積確率 $q_i = \sum_{j=1}^{i-1} P_j$　　$(i \geq 2)$　を求める。

（３）$-log\ \ P_i \leq m_i < -log\ \ P_i + 1$　となるm_iを求める。

（４）q_iの２進数展開の小数点以下m_i桁を取る。

２）ハフマンの符号化

（１）生起確率の高い順に上から並べる。

（２）下から２つ（すなわち最も生起確率の小さいもの２つ）を１グループとした枝にした木を作る。それらの確率を加算してそのグループの生起確率とする。

（３）新たなグループも含めて生起確率の高い順に上から並べる。

（４）グループが１つになる、すなわち生起確率が１になるまで、（２）（３）を繰り返す。

（５）全確率（=1）のルートから木をたどり分岐に対して０と１を割り付ける

例

１）シャノンの符号化

S_i	P_i	q_i　二進数展開		m_i
S_1	$\frac{5}{16}$	$0 = 0.0000$	$-log\frac{5}{16} = 1.68$	2
S_2	$\frac{4}{16}$	$\frac{5}{16} = 0.0101$	$-log\frac{4}{16} = 2$	2
S_3	$\frac{3}{16}$	$\frac{9}{16} = 0.1001$	$-log\frac{3}{16} = 4 - \log 3$	3
S_4	$\frac{2}{16}$	$\frac{12}{16} = 0.1100$	$-log\frac{2}{16}$	3
S_5	$\frac{1}{16}$	$\frac{14}{16} = 0.1110$	$-log\frac{1}{16}$	4
S_6	$\frac{1}{16}$	$\frac{15}{16} = 0.1111$	$-log\frac{1}{16}$	4

以上より、

$S_1 \rightarrow$　００

$S_2 \rightarrow$　０１

$S_3 \rightarrow$　１００

$S_4 \rightarrow$　１１０

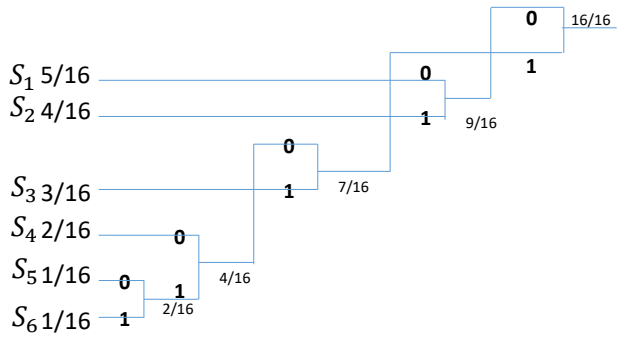
$S_5 \rightarrow$　１１１０

$S_6 \rightarrow$　１１１１

シャノン符号の平均符号語長

$\bar{m}_s = 2 * \frac{5}{16} + 2 * \frac{4}{16} + 3 * \frac{3}{16} + 3 * \frac{2}{16} + 4 * \frac{1}{16} + 4 * \frac{1}{16} = \frac{41}{16} = 2.56$

２）ハフマンの符号化



以上より、

$S_1 \rightarrow$　００

$S_2 \rightarrow$　０１

$S_3 \rightarrow$　１１

$S_4 \rightarrow$　１００

$S_5 \rightarrow$　１０１０

$S_6 \rightarrow$　１０１１

ハフマン符号の平均符号語長

$$\bar{m}_h = 2*\frac{5}{16}+2*\frac{4}{16}+2*\frac{3}{16}+3*\frac{2}{16}+4*\frac{1}{16}+4*\frac{1}{16}=\frac{38}{16}=2.38$$

$$H=\frac{5}{16}(4-log5)+\frac{4}{16}(2)+\frac{3}{16}(4-log3)+\frac{2}{16}(3)+\frac{1}{16}(4)+\frac{1}{16}(4)$$

$$=\frac{1}{16}(20+8+12+6+4+4-5log5-3log3)=\frac{1}{16}(54-11.6-4.75)$$

$$=2.35$$

$$H<\bar{m}_h<\bar{m}_s$$

ハフマン符号の注意点

・分岐（葉）に割り付ける０，１は、任意（上から０，１でも上から１，０でもよい。分岐毎に変えてもよい。）

・平均符号語長$\bar{m}$を最小にするという意味でコンパクト符号と呼ばれる。

・接頭符号(Prefix code)

（課題　ハフマン符号をコンピュータで実現するアルゴリズムを考えよ。データ構造を定義し、フローチャートを作成せよ。実際のプログラミングは行わなくてもよい。）

（発展）

・k 進のハフマン符号化はどのようにしたら実現するか。

・ハフマン符号のコンパクト性の証明

・ハフマン符号は、末端の葉（つまり最小の確率を持つ点）から開始した。逆に根（つまり全確率１）からほぼ等確率（２進の場合は１／２）になるように割り付ける符号化（ファノ符号）がある。

情報通信基礎Ⅰ　第３章　補足資料１　平均符号語長の範囲

k個の要素からなる情報源XのエントロピーをH、平均符号語長を$\bar{m}$とするとき、

$H \le \bar{m} \cdot logk < H + logk$　が成立する。

【証明】

１）任意の２つの確率ベクトルℙ, ℚ

$\mathbb{P} = (P_1, P_2, , , P_n)$　　$\sum_i P_i = 1$　　$0 \le P_i \le 1$

$\mathbb{Q} = (Q_1, Q_2, , , Q_n)$　　$\sum_i Q_i = 1$　　$0 < Q_i \le 1$

に対して、$-\sum P_i logP_i \le -\sum P_i logQ_i$ が成立する。（ギブスの不等式より）

２）$Q_i = \frac{k^{-m_i}}{\sum_{j=1}^{n} k^{-m_j}}$　とする。

３）以下の式展開を行う。

$H = -\sum_i P_i logP_i \le -\sum_i P_i logQ_i = -\sum_i P_i log \frac{k^{-m_i}}{\sum_{j=1}^{n} k^{-m_j}} = -\sum_i P_i logk^{-m_i} +$

$\sum_i P_i \log\left(\sum_j k^{-m_j}\right) = -\sum_i P_i(-m_i)logk + \left(\sum_i P_i\right)\log\left(\sum_j k^{-m_j}\right) = (logk) \cdot \left(\sum_i P_i m_i\right) +$
$\log\left(\sum_j k^{-m_j}\right) = \bar{m}logk + log\alpha$　　ただし、$\alpha = \sum_j k^{-m_j} \le 1$。

$0 < \alpha \le 1$より、$log\alpha \le 0$。よって、

$$H \le \bar{m}logk$$

が成立する。

４）等号が成立する時が最も効率がよいと判断される。等号が成立するのは、以下の時でありその時に限る。iff=if and only if

①$log\alpha = 0$ つまり、Kraft の不等式の等号が成立するとき

かつ

②$P_i = Q_i = \frac{k^{-m_i}}{\sum_{j=1}^{n} k^{-m_j}} = k^{-m_i}$　つまり、$m_i = -log_k P_i$

m_iは整数であるので、

$$\therefore -log_k P_i \le m_i < -log_k P_i + 1$$

式全体にP_iをかけて、

$$-P_i log_k P_i \le P_i m_i < P_i(-log_k P_i + 1)$$

iに関して加算して、

$$-\sum_i P_i log_k P_i \le \sum_i P_i m_i < \sum_i P_i(-log_k P_i + 1)$$

変形すると、

$$\frac{H}{logk} \le \bar{m} < \frac{H}{logk} + 1$$

----------補題　ギブスの不等式とその証明----------

任意の２つの確率ベクトル $\mathbf{P}$，$\mathbf{Q}$

$$\mathbf{P}=(P_1,P_2,\cdots,P_n),\ \sum_i P_i=1 \quad 0\le P_i\le 1$$

$$\mathbf{Q}=(Q_1,Q_2,\cdots,Q_n),\ \sum_i Q_i=1 \quad 0\le Q_i\le 1,\quad Q_i\neq 0$$

に対して、$-\sum P_i\log P_i\le -\sum P_i\log Q_i$ が成立する。これをギブスの不等式(Gibbs' inequality)と呼ぶ。

【証明】

まず簡単のため、$\mathbf{P}$ に 0 の要素が存在しない（すべての i に対して $P_i\neq 0$）場合を考える。

$$-\sum P_i\log P_i+\sum P_i\log Q_i=\sum P_i\log\frac{Q_i}{P_i}\le\sum P_i(\frac{Q_i}{P_i}-1)\log e=[\sum(Q_i-P_i)]\log e=(\sum Q_i-\sum P_i)\log e=0$$

よって、$-\sum P_i\log P_i\le -\sum P_i\log Q_i$

ただし、$\ln x\le x-1$　より　$\log x\le(x-1)\log e$　を用いている。

$\mathbf{P}$ に 0 の要素が存在するときは、0 の要素と 0 以外の要素を分離して扱う。

$$-\sum P_i\log P_i+\sum P_i\log Q_i=-\sum_{i,s\,t\ P_i\neq 0}P_i\log P_i+\sum_{i,s\,t\ P_i\neq 0}P_i\log Q_i-\sum_{i,s\,t\ P_i=0}P_i(\log P_i)+\sum_{i,s\,t\ P_i=0}P_i(\log Q_i)$$

$$\le\sum_{i,s\,t\ P_i\neq 0}P_i(\frac{Q_i}{P_i}-1)\log e=(\sum_{i,s\,t\ P_i\neq 0}Q_i-\sum_{i,s\,t\ P_i\neq 0}P_i)\log e=[(1-\sum_{i,s\,t\ P_i=0}Q_i)-1]\log e=-(\sum_{i,s\,t\ P_i=0}Q_i)\log e\le 0$$

となり、証明できる。ただし、$\lim_{P_i\to 0}P_i\log P_i=0$ を用いている。

また、$i,s.t.P_i\neq 0$ とは、「$P_i\neq 0$ である i」の意味である。(s.t.は such that の略)

等号は $P_i=Q_i$ の時に成立する。

このほかに Jensen の不等式を用いた証明などがある。

情報通信基礎Ⅰ　第３章　補足資料２　情報源符号化の具体例

情シス　渡辺

３．９　情報源符号化の具体例

冗長度削除のメリット

・データ削減

・通信時間の削減

・データ保管の効率向上

３．９．１　モールス信号

1.1.1 Letters

	a	.−	i	..	r	.−.
	b	−...	j	.−−−	s	...
	c	−.−.	k	−.−	t	−
	d	−..	l	.−..	u	..−
	e	.	m	−−	v	...−
accented	e	..−..	n	−.	w	.−−
	f	..−.	o	−−−	x	−..−
	g	−−.	p	.−−.	y	−.−−
	h	....	q	−−.−	z	−−..

1.1.2 Figures

1	.−−−−	6	−....
2	..−−−	7	−−...
3	...−−	8	−−−..
4	....−	9	−−−−.
5	.....	0	−−−−−

International Morse code Recommendation ITU-R M.1677-1, https://www.itu.int/rec/R-REC-M.1677-1-200910-I/

表1･1　英語のアルファベットにおける文字の生起確率

文字	生起確率	文字	生起確率	文字	生起確率
スペース	0.1859	H	0.0467	G	0.0152
E	0.1031	L	0.0321	P	0.0152
T	0.0796	D	0.0317	B	0.0127
A	0.0642	U	0.0228	V	0.0083
O	0.0632	C	0.0218	K	0.0049
I	0.0575	F	0.0208	X	0.0013
N	0.0574	M	0.0198	J	0.0008
S	0.0514	W	0.0175	Q	0.0008
R	0.0484	Y	0.0164	Z	0.0005

島田、木内、大松：「わかる情報理論」より

３．９．２　データ圧縮

１）圧縮技術の分類

・無圧縮

・圧縮

　・可逆圧縮　Lossless compression

　・非可逆圧縮　Lossy compression

２）無圧縮

・ラスタ画像（ビットマップ画像）　ペイント系　　－＞これが今回の議論の焦点

その他に、ベクトル画像があるが、ここでは対象外とする。

（ドロー系　　－＞点、線、面を数式のパラメータで表現する。）

２－１）ラスタ画像の表現方法

・RGB 画像

画素（ピクセル）ごとに R, G, B の濃淡を持たせる

濃淡の表現段階数　8bit なら 256 段階

2^(8x3)=1677 万色

・より進んだ色表現

人間の目はもっと複雑。

明るさの変化に敏感、色の変化に鈍感、高周波成分に鈍感

色空間、表色系

色を定量的に表す体系。通常は３要素で表現される。

混色系（英: color mixing system)、顕色系（英: color appearance system)

・原則は３要素である。３要素の取り方が種々ある。また、実用性などの観点から２要素、４要素以上を用いる色空間もある。

・多くの場合、ある色空間から別の色空間への変換が行えるが、必ずしも変換が行えるとは限らない。

・表色系の例

・RGB 表色系　CIE 1931　（CIE: 国際照明学会）

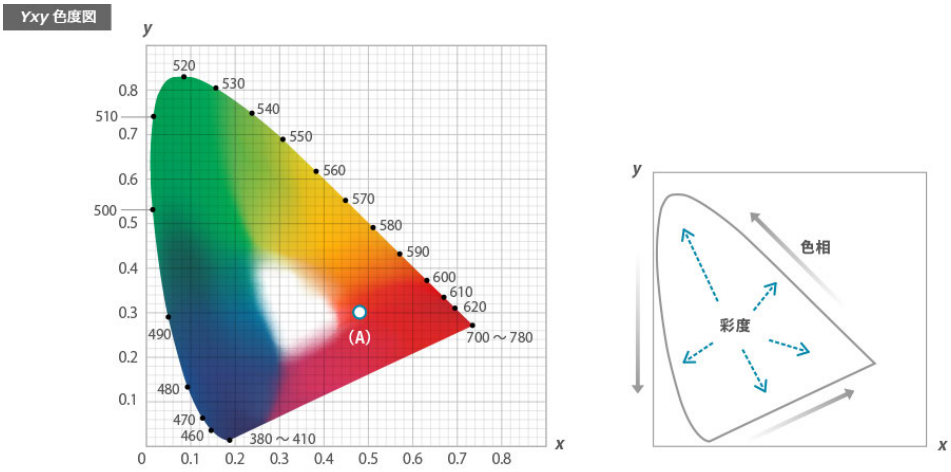
原色を R（赤、700nm)、G（緑、546.1nm)、B（青、435.8nm）で表現する。

・XYZ 表色系

CIE 1931 XYZ 色空間

・xyY 表色系　Y 反射率（明度)、xy 色度　（図）

XYZ 表色系から絶対的な色合いを表現する



Yxy 表色系コニカミノルタ https://www.konicaminolta.jp/instruments/knowledge/color/section2/03.html　より

・Ｌ*ｕ*ｖ*表色系（CIE1976Ｌ*ｕ*ｖ*色空間）

・Ｌ*ａ*ｂ*表色系（CIE1976Ｌ*ａ*ｂ*色空間）

・マンセル表色系（マンセル･カラーオーダー･システム）

・オストワルト表色系

・ＰＣＣＳ（日本色研配色体系）

・ＮＣＳ（ナチュラル･カラー･システム）

・ＡＢＣトーンシステム

・YUV、YCbCr、YPbPr

輝度信号 Y と、2 つの色差信号を使って表現される色空間。

・RAW, BMP, TIFF（圧縮も選択可能）

３）可逆圧縮　Lossless compression

圧縮・展開の処理を経たデータが圧縮前のデータと完全に一致する。

・データの冗長性を排除する。文字数を少なくすることにより、一文字当たりの情報量を大きくする（エントロピーが増大）

・データの偏りや法則性を利用する。

人間の扱うデータは何らかの法則性を持っている

（逆に言えば完全にランダムで法則性のないホワイトガウス雑音は圧縮できない）

・非可逆圧縮に比べてサイズが大きい。

・データの冗長性を的確にかつ高速に処理できるかが評価基準

圧縮率と圧縮時間のトレードオフ

・圧縮率の目安　1/2

・エントロピー符号化と関連

・ハフマン符号、ランレングス法、LZ 法

・PNG, GIF, TIFF

４）非可逆圧縮 Lossy compression

・サイズが小さい

・静止画、動画など画像系に用いられる

・圧縮率の目安　1/10-1/100

・JPEG, MPEG, Wavelet 変換　(PICT; ラスタ+ベクトル)など

５）情報源符号化が用いられている圧縮　－＞　可逆圧縮

５－１）ランレングス圧縮（連長圧縮；Run Length Encoding(RLE)）

データの多くは繰り返される。

文字の繰返回数+その文字のコード　で表現する。

例　AAAAA　-> A5

繰返回数が少ないとかえってサイズが大きくなる。

例えば、繰返回数１バイト、文字１バイトで表現すると

X　->　00000001 01011000　　圧縮率　8/16=1/2　圧縮前より悪い

Packbits

RLE と非圧縮を併用する。最上位ビットで区別する。

YXXXXXXXX　->　01011001 10001000 01011000 圧縮率 72/24=3

[Y]　^　8 回　[X]

５－２）Lempel-Ziv 圧縮

・ユニバーサル符号化（Universal Source Coding）の一種

ユニバーサル符号化：記号の出現頻度が不明な場合に符号化する技術

・同一の文字列を記憶するテーブル（辞書）を作成して圧縮する（辞書圧縮）

・LZ77, LZ78 等

例：https://www.ibm.com/developerworks/library/l-compr/index.html　より

ある地域の電話番号

772-7628 772-8601 772-0113 772-0429 772-9833 773-4319 772-3920 772-0893 772-9934

初期テーブル

index	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	・・
value	0	1	2	3	4	5	6	7	8	9	x	x	x	x	x	x	x	x	x	x	・・

出力データ　5 ビット　　0-9 は通常の数値 10-31 はインデックス番号

時刻	入力	テーブル参照結果	テーブルアクション	出力
1	7	7 found	nothing to add	なし
2	7	77 not found	set 77 in [10]	[7]=00111
3	2	72 not found	set 72 in [11]	[7]=00111
4	7	27 not found	set 27 in [12]	[2]=00010
5	6	76 not found	set 76 in [13]	[7]=00111
6	2	62 not found	set 62 in [14]	[6]=00110
7	8	28 not found	set 28 in [15]	[2]=00010
8	7	87 not found	set 87 in [16]	[8]=01000
9	7	77 found	nothing to add	なし
10	2	772 not found	set 772 in [17]	[10]=01010
11	8	28 found	nothing to add	なし
12	6	286 not found	set 286 in [18]	[15]=01111

時刻１２でのテーブル

index	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	・・
value	0	1	2	3	4	5	6	7	8	9	77	72	27	76	62	28	87	772	286		・・

・時刻 10 と 12 では、2 文字を一度に出力している。ここまでの圧縮率=45/4*11
　これ以降、772 が出ると[17]を出力する。つまり 3 文字を 5bit で表現可能。
　最終的には、インデックス 10 以降のテーブルも出力する。
・一般にハフマン符号やランレングス法よりも圧縮率が高い。
・メモリ上で大きなテーブルを扱う可能性がある。
・PNG は、Lempel-Ziv(LZ77)と Huffman を組み合わせている。

拡張方式 LZW

　That algorithm is very simple, ... algorithm.....algorithm.....alrogrithm....
　That algorithm is very simple, ... 6,9.....6,9.....6,9....
　　6,9 は既出の「6 バイト目から 9 バイト分同一」の意
　GIF に用いられている。

---時刻 13 以降

13	0	60 not found	set 60 in [19]	[6]=00110
14	1	01 not found	set 01 in [20]	[0]=00000
15	7	17 not found	set 17 in [21]	[1]=00001
16	7	77 found	nothing to add	なし
17	2	772 found	nothing to add	なし
18	0	7720 not found	set 7720 in [22]	[17]=10001
19	1	01 found	nothing to add	なし
20	1	011 not found	set 011 in [23]	[20]=10100
21	3	13 not found	set 13 in [24]	[1]=00001
22	7	37 not found	set 37 in [25]	[3]=00011
23	7	77 found	nothing to add	なし
24	2	772 found	nothing to add	なし
25	0	7720 found	nothing to add	なし
26	4	77204 not found	set 77204 in [26]	[22]=10110
27	2	42 not found	set 42 in [27]	[4]=00100
28	9	29 not found	set 29 in [28]	[2]=00010
29	7	97 not found	set 97 in [29]	[2]=00010
30	7	77 found	nothing to add	なし
31	2	772 found	nothing to add	なし
32	9	7729 not found	set 7729 in [30]	[17]=10001
33	8	98 not found	set 98 in [31]	[9]=01001<-テーブル溢れ

情報通信基礎Ⅰ　第４章　通信路符号化

ポイント

・第３章では、平均符号語長$\bar{m}$をできるだけHに近づけた。（冗長度をなくす）
　データ圧縮、誤りのない通信路での通信

・第４章では、雑音がある通信路で誤ったとしても正しく復号できる符号化を考える。
　（冗長度を加える）

・通信路符号化の定理（シャノンの第二定理）

誤りがある場合、我々はどうしているのだろうか？

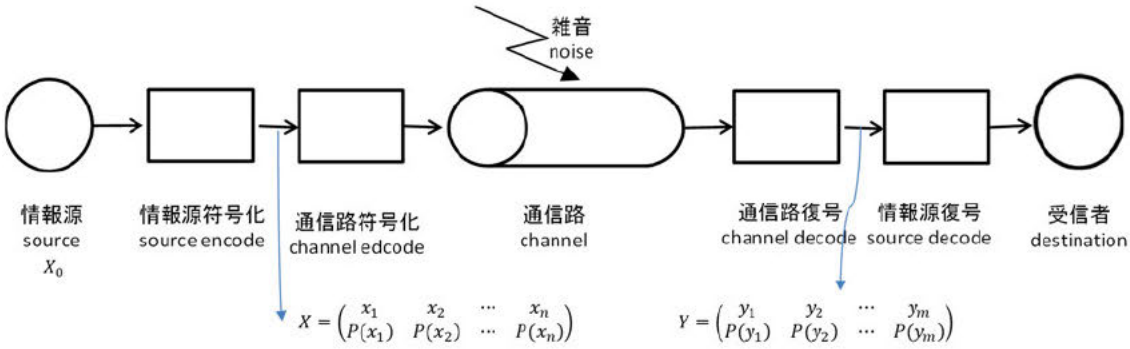
単純に繰り返したのでは時間がかかる。

想像を働かせて訂正する。一つの言葉が別の意味に解釈されるのを防ぐ。異なる語や言葉が同一の意味に解釈されるのを防ぐ。l と１、o と 0、れとわ。

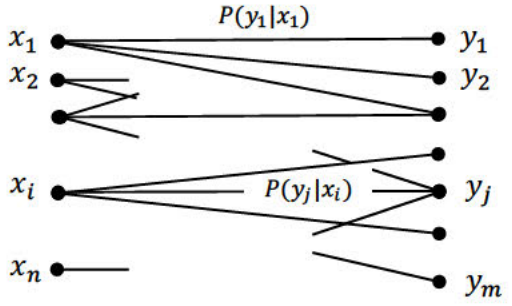
参考書：島田良作、木内陽介、大松繁著「わかる情報理論」　日新出版

４．１　基礎

【図４．１】



【図４．２】

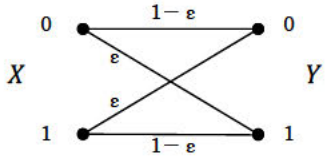


x_iを送るとy_jが受信される確率は条件付き確率　$P(y_j|x_i)$　で表現される。これを行列として並べたℙを通信路行列と呼ぶ。通信路行列は、通信路の誤りやすさの性質を表している。

$$\mathbb{P}=\begin{bmatrix} P(y_1|x_1) & P(y_2|x_1) & \cdots & P(y_m|x_1) \\ P(y_1|x_2) & \cdots & \cdots & P(y_m|x_2) \\ \vdots & \cdots & \cdots & \vdots \\ P(y_1|x_n) & \cdots & \cdots & P(y_m|x_n) \end{bmatrix}$$

例４．１　二元対称通信路(BSC; binary symmetric channel)

【図４．３】



$$\mathbb{P} = \begin{bmatrix} 1-\varepsilon & \varepsilon \\ \varepsilon & 1-\varepsilon \end{bmatrix}$$

４．２　通信誤り

【図４．４】　アナログ信号の誤り　ビットエラー率 BER (Bit Error Rate)

わ；　BER：　衛星10^{-3}程度　無線10^{-6}程度　　光ファイバ10^{-8}

４．３　情報伝送速度

図４．１に示したように、チャネルへの入力を情報源X、チャネルからの出力を情報源Yと考える。すなわち、

$$X = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ P(x_1) & P(x_2) & \cdots & P(x_n) \end{pmatrix} \qquad \sum_{i=1}^{n} P(x_i) = 1$$

$$Y = \begin{pmatrix} y_1 & y_2 & \cdots & y_m \\ P(y_1) & P(y_2) & \cdots & P(y_m) \end{pmatrix} \qquad \sum_{j=1}^{m} P(y_j) = 1$$

Yを情報「源」と呼ぶには抵抗感があるかもしれないが、十分長い時間Yを観測すれば、y_jの確率を計測でき情報「源」のように書ける。つまり、情報源と見なせる。

入力側から送られるエントロピー（一文字あたりの情報量）は、

$$H(X) = -\sum_{i}^{n} P(x_i) log P(x_i)$$

出力側に現れるエントロピーは、

$$H(Y) = -\sum_{j}^{m} P(y_j) log P(y_j)$$

である。XについてYから間接的に得られる情報量、すなわち相互情報量は、

$$I(X;Y) = H(Y) - H(Y|X) = \sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i, y_j) log \frac{P(x_i, y_j)}{P(x_i)P(y_j)} = H(X) - H(X|Y)$$

で表現される。(送信側では$H(X)$の情報量を送っているが途中で誤るので$H(X|Y)$だけ曖昧さの減少量が減る。（情報量が減る。))

一文字あたりの伝送時間をlとすると、情報伝送速度Rは、$R = \frac{I(X;Y)}{l}$ であり、Rの最大値をC（通信路容量）と呼ぶ。すなわち、

$$C = max \frac{I(X;Y)}{l}$$

である。今簡単のため、lを定数とすると、

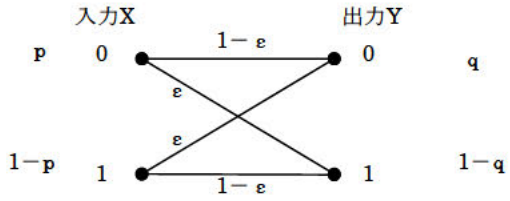
$$lC = max\, I(X;Y) = \max\{H(Y) - H(Y|X)\}$$

となる。これを最大化するには、以下が考えられる。

- $H(Y)$を大きくする。
- $H(Y|X)$を小さくする。

例４．２　二元対称通信路の通信路容量

【図４．５】



$$\mathbb{P} = \begin{bmatrix} 1-\varepsilon & \varepsilon \\ \varepsilon & 1-\varepsilon \end{bmatrix}$$

$$X = \begin{pmatrix} 0 & 1 \\ p & 1-p \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & 1 \\ q & 1-q \end{pmatrix}$$

わ　$q = p(1-\varepsilon) + (1-p)\varepsilon$であるが、敢えて$q$とする。

$$I(X;Y) = H(Y) - H(Y|X) \qquad (式4-1)$$

$$H(Y) = -qlogq - (1-q)\log(1-q) \qquad (式4-2)$$

$$H(Y|X) = -\sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i, y_j) * \log P(y_j|x_i) = -\sum_{i=1}^{n} P(x_i) \sum_{j=1}^{m} P(y_j|x_i) * \log P(y_j|x_i)$$

$$= -p\{(1-\varepsilon)log(1-\varepsilon) + \varepsilon log\varepsilon\} - (1-p)\{\varepsilon log\varepsilon + (1-\varepsilon)log(1-\varepsilon)\}$$

$$= -\varepsilon log\varepsilon - (1-\varepsilon)log(1-\varepsilon) \qquad (式4-3)$$

すなわち、$H(Y|X)$は、p，qに無関係。使う通信路によって決定される。

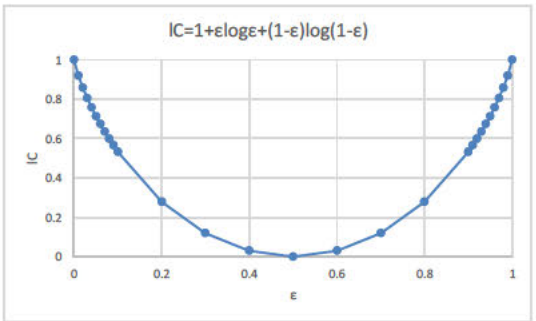
従って、（通信路が固定でεは変更できないとすると、）XについてYから間接的に得られる情報量、すなわち相互情報量$I(X;Y) = H(Y) - H(Y|X)$　が最大となるのは、$H(Y)$が最大になるとき、すなわち、$q = \frac{1}{2}$の時である。

よって、

$$lC = H(Y)_{|q=\frac{1}{2}} - H(Y|X) = -\frac{1}{2}log\frac{1}{2} - \frac{1}{2}log\frac{1}{2} + \varepsilon log\varepsilon + (1-\varepsilon)log(1-\varepsilon)$$

$$= 1 + \varepsilon log\varepsilon + (1-\varepsilon)log(1-\varepsilon) \qquad (式4-4)$$

【図４．６】縦軸lc、横軸ε



$\varepsilon = 0.5$ の時、実質的な通信が全く行えない。

（より詳細な計算１）$I(X;Y)=H(Y)-H(Y|X)$で計算する場合

$P(Y=0)=P(X=0)P(Y=0|X=0)+P(X=1)P(Y=0|X=1)=p(1-\varepsilon)+(1-p)\varepsilon$

$P(Y=1)=P(X=0)P(Y=1|X=0)+P(X=1)P(Y=1|X=1)=p\varepsilon+(1-p)(1-\varepsilon)$

$$H(Y)=-\sum_{j=1}^{m}P(y_j)logP(y_j)$$

$$=-[\{\mathrm{p}(1-\varepsilon)+(1-p)\varepsilon\}\log\{p(1-\varepsilon)+(1-p)\varepsilon\}$$

$$+\{p\varepsilon+(1-p)(1-\varepsilon)\log\{p\varepsilon+(1-p)(1-\varepsilon)\}] \quad (式4-5)$$

$P(X=0,Y=0)=P(X=0)P(Y=0|X=0)=p(1-\varepsilon)$　　$P(X=0,Y=1)=P(X=0)P(Y=1|X=0)=p\varepsilon$

$P(X=1,Y=0)=P(X=1)P(Y=0|X=1)=(1-p)\varepsilon$　　$P(X=1,Y=1)=P(X=1)P(Y=1|X=1)=(1-p)(1-\varepsilon)$

$$H(Y|X)=-\sum_{i=1}^{n}\sum_{j=1}^{m}P(x_i,y_j)*\log P(y_j|x_i)=-p(1-\varepsilon)\log(1-\varepsilon)-p\varepsilon log\varepsilon-(1-p)\varepsilon log\varepsilon-(1-p)(1-\varepsilon)log(1-\varepsilon)$$

$$=-\varepsilon log\varepsilon-(1-\varepsilon)log(1-\varepsilon) \quad (式4-6)$$

以上より、

$$I(X;Y)=H(Y)-H(Y|X)$$

$$=-\{\mathrm{p}(1-\varepsilon)+(1-p)\varepsilon\}\log\{p(1-\varepsilon)+(1-p)\varepsilon\}-\{p\varepsilon+(1-p)(1-\varepsilon)\log\{p\varepsilon+(1-p)(1-\varepsilon)\}$$

$$+\varepsilon log\varepsilon+(1-\varepsilon)log(1-\varepsilon) \quad 式(4-7)$$

（より詳細な計算２）　$I(X;Y)=H(X)-H(X|Y)$で計算する場合

$P(X=0|Y=0)=\frac{P(X=0,Y=0)}{P(Y=0)}=\frac{p(1-\varepsilon)}{p(1-\varepsilon)+(1-p)\varepsilon}$　　$P(X=0|Y=1)=\frac{P(X=0,Y=1)}{P(Y=1)}=\frac{p\varepsilon}{p\varepsilon+(1-p)(1-\varepsilon)}$

$P(X=1|Y=0)=\frac{P(X=1,Y=0)}{P(Y=0)}=\frac{(1-p)\varepsilon}{p(1-\varepsilon)+(1-p)\varepsilon}$　　$P(X=1|Y=1)=\frac{P(X=1,Y=1)}{P(Y=1)}=\frac{(1-p)(1-\varepsilon)}{p\varepsilon+(1-p)(1-\varepsilon)}$

$$H(X|Y)=-\sum_{i=1}^{n}\sum_{j=1}^{m}P(x_i,y_j)*\log P(x_i|y_j)$$

$$=-[P(X=0,Y=0)logP(X=0|Y=0)+P(X=0,Y=1)logP(X=0|Y=1)$$

$$+P(X=1,Y=0)logP(X=1|Y=0)+P(X=1,Y=1)logP(X=1|Y=1)]$$

$$=-p(1-\varepsilon)\log\frac{p(1-\varepsilon)}{p(1-\varepsilon)+(1-p)\varepsilon}-p\varepsilon\log\frac{p\varepsilon}{p\varepsilon+(1-p)(1-\varepsilon)}-(1-p)\varepsilon\log\frac{(1-p)\varepsilon}{p(1-\varepsilon)+(1-p)\varepsilon}$$

$$-(1-p)(1-\varepsilon)\log\frac{(1-p)(1-\varepsilon)}{p\varepsilon+(1-p)(1-\varepsilon)}$$

$H(X)=-plogp-(1-p)\log(1-p)$

以上より、

$$I(X;Y)=H(X)-H(X|Y)=\cdots$$

$$=-\{\mathrm{p}(1-\varepsilon)+(1-p)\varepsilon\}\log\{p(1-\varepsilon)+(1-p)\varepsilon\}-\{p\varepsilon+(1-p)(1-\varepsilon)\log\{p\varepsilon+(1-p)(1-\varepsilon)\}$$

$$+\varepsilon log\varepsilon+(1-\varepsilon)log(1-\varepsilon) \quad 式(4-7)と同じ$$

case 1)　$\varepsilon=0$の場合（誤りがない場合）

$$\mathbb{P}=\begin{bmatrix}1.0 & 0\\ 0 & 1.0\end{bmatrix}$$

式４－５より、

$$H(Y) = -\{\mathrm{p}(1-\varepsilon) + (1-p)\varepsilon\}\log\{p(1-\varepsilon) + (1-p)\varepsilon\} - \{p\varepsilon + (1-p)(1-\varepsilon)\log\{p\varepsilon + (1-p)(1-\varepsilon)\} = -plogp - (1-p)\log(1-p) = H(X)$$

式４－６より、$H(Y|X) = -\varepsilon log\varepsilon - (1-\varepsilon)log(1-\varepsilon) = 0$

よって、$I(X;Y) = H(Y) - H(Y|X) = H(X)$

つまり、完全にXの情報量を送っていることになる。

case 2)　$\varepsilon = 0.5$の場合

$$\mathbb{P} = \begin{bmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{bmatrix}$$

式４－５より、

$$H(Y) = -\{\mathrm{p}(1-\varepsilon) + (1-p)\varepsilon\}\log\{p(1-\varepsilon) + (1-p)\varepsilon\} - \{p\varepsilon + (1-p)(1-\varepsilon)\log\{p\varepsilon + (1-p)(1-\varepsilon)\}$$

$$= -\left\{\frac{1}{2}p + \frac{1}{2}(1-p)\right\}\log\left\{\frac{1}{2}p + \frac{1}{2}(1-p)\right\}$$

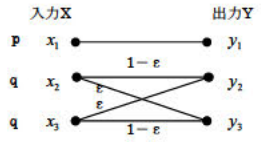
$$-\left\{\frac{1}{2}p + \frac{1}{2}(1-p)\right\}\log\left\{\frac{1}{2}p + \frac{1}{2}(1-p)\right\} = -\frac{1}{2}log\frac{1}{2} - \frac{1}{2}log\frac{1}{2} = 1$$

式４－６より、

$$H(Y|X) = -\varepsilon log\varepsilon - (1-\varepsilon)log(1-\varepsilon) = -\frac{1}{2}log\frac{1}{2} - \frac{1}{2}log\frac{1}{2} = 1$$

であり、$I(X;Y) = H(Y) - H(Y|X) = 0$、つまり実質的には通信できない。

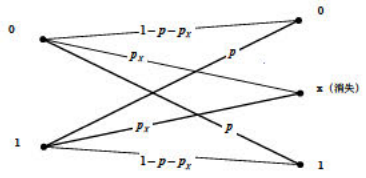
例４．３　以下の通信路の通信路容量を求めよ。



（演習問題４．７）

例４．４　以下の二元対称消失通信路の通信路容量を求めよ。

【図４．７】



入力アルファベットよりも出力アルファベットを多くする。軟判定復号（Soft decision decoding）とも呼ばれる。（演習問題４．３）

４．４　通信路符号化

誤りを下げる方法

（１）εを小さくする。　S/N を上げる。

（２）冗長度を増す。

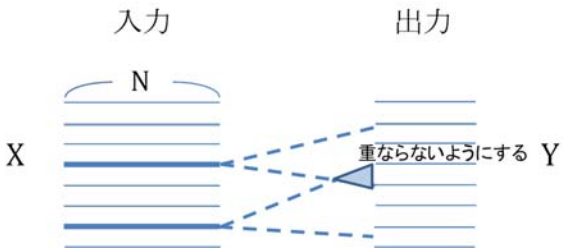
・繰り返す　　－＞単純に繰り返したのでは通信速度が下がる

・符号化に工夫をする　－＞通信速度を下げずに冗長度を増す方法がある（シャノンの第２定理）

（繰返す方法）繰返し回数に対して、誤り率が低下するが、情報伝送速度Ｒも低下する。

実質的に誤りのない通信方法：送信符号語が誤ったとしても隣の領域に入らないようにする。すなわち、下図の領域が重ならないようにする。

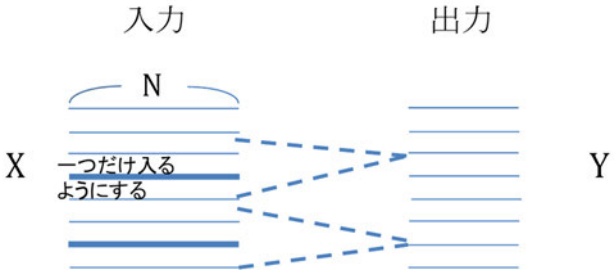
【図４．８】



では、重ならないようにするには？

Xのすべての符号語を使うのではなく、まばらに使う。

逆に、出力から類推される入力が１つになるようにする。



［通信路符号化の定理］（シャノンの第２定理）

通信路容量がCの時、情報伝送速度Rが$R < C$であれば、任意の正の数εに対し、符号誤り率P_eが$P_e < \varepsilon$となる符号化が存在する。

（証明）　略　（補足資料１）

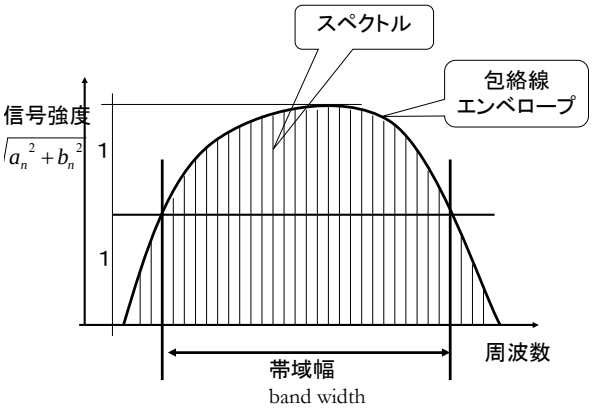
４．５　その他の関連する話題

［シャノン-ハートレーの定理］

伝送路の帯域幅をH(Hz)、受信信号電力をS(W)、雑音電力をN(W)とすると、達成可能な最大伝送速度R(bit/sec)は、以下で表される。

$$R = H \log_2 \left(1 + \frac{S}{N}\right)$$

これをシャノン容量、あるいはシャノンの定理と表現することもある。



具体的な帯域幅

無線 LAN 20MHz-80MHz

LTE　5MHz、10MHz、15MHz、20MHz

光ファイバ　4-10THz

情報通信基礎Ⅰ　第４章　補足資料１　通信路符号化定理の簡略証明

１　情報源SとN文字列を考える。ただし、Nは十分大きいものとする。
典型的系列の数$M_S(N)$は、$M_S(N) = 2^{H(S)N}$　（図１）

２　$H(X_0) > H(S)$なる情報源X_0を考える（ex. 0, 1 が等確率で生起する情報源）（図２）

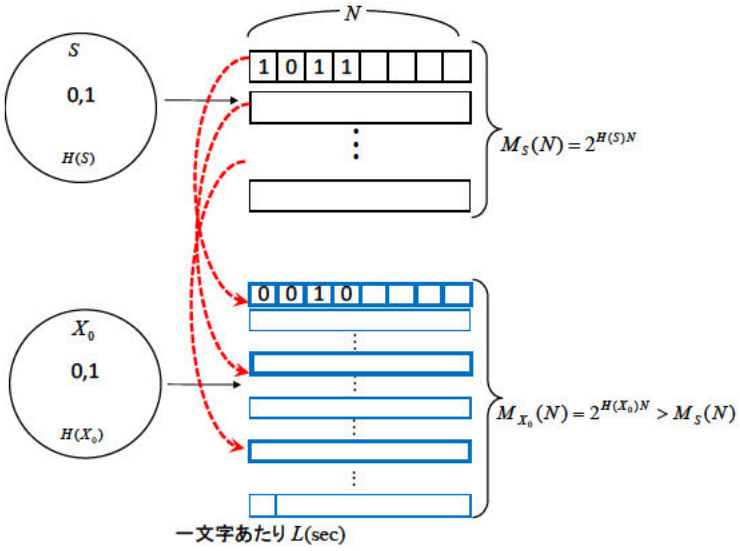


図１

図２

３　情報源Sの$M_S(N)$個の文字列に対して、情報源X_0の$M_{X_0}(N)$個の文字列をランダムに対応させる（図１、図２の間の赤破線）。対応させた文字列（図２の青太線の箱、図３の青線）だけを通信に用いる。

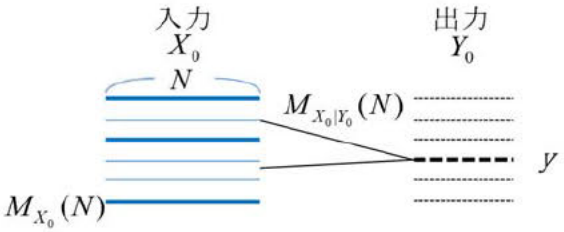


図３

４　図３のように出力側も考える。１つの出力yに対する入力の文字列の数$M_{X_0|Y_0}(N)$は、$M_{X_0|Y_0}(N) = 2^{H(X_0|Y_0)N}$である。

５　１つの出力yを受けた時、それに対応する$M_{X_0|Y_0}(N)$個の入力の中に、本当に使われた文字列（図３の青太線）が１つだけなら、完全に復号できる。

図３の左の中で青太線となる確率は、$\frac{M_S(N)}{M_{X_0}(N)}$

従って、使われない文字列（青細線）となる確率は、$1-\frac{M_S(N)}{M_{X_0}(N)}$

正しい通信が行われる確率P_cは、$M_{X_0|Y_0}(N)-1$個が細線となっていればよいので、

$$P_c=\left(1-\frac{M_S(N)}{M_{X_0}(N)}\right)^{M_{X_0|Y_0}(N)-1}\approx\left(1-\frac{M_S(N)}{M_{X_0}(N)}\right)^{M_{X_0|Y_0}(N)}$$

（Nが十分大きいので、$M_{X_0|Y_0}(N)>>1$）

$(1+x)^n\approx 1+nx$より、（$x=\frac{M_S(N)}{M_{X_0}(N)}<<1$）

$$P_c=1-M_{X_0|Y_0}(N)\bullet\frac{M_S(N)}{M_{X_0}(N)}=1-2^{H(X_0|Y_0)N}\bullet 2^{H(S)N}\bullet 2^{-H(X_0)N}=1-2^{\{H(X_0|Y_0)+H(S)-H(X_0)\}N}$$

一方、$C=\frac{I(X_0;Y_0)}{L}=\frac{1}{L}\{H(X_0)-H(X_0|Y_0)\}$であり、実質的な伝送速度は$R=\frac{H(S)}{L}$であるので、

$P_c=1-2^{\{R-C\}NL}$、誤り率P_eは$P_e=1-P_c=2^{\{R-C\}NL}$となる。

6　以上より、

$R-C<0$　なら　$N\to\infty$で$P_e\to 0$

$R-C>0$　なら　$P_e>>1$で不可

7　ポイント

・Nを十分大きくとれば、Rを確保しつつP_eを小さくできる。

（繰り返す方法だと、$R\to 0$）

情報通信基礎Ⅰ　第５章　誤り訂正符号

情シス　渡辺

ポイント

・第４章で論じた通信路符号化の具体的な手法を学ぶ。ポイントは多くの符号語を用意しそのうちの一部（何らかの条件を満たす符号語）を使うことである。（冗長度を増す）

・符号語をベクトルとして扱う方法（第５章）、符号語を多項式で扱う方法（第６章）を学ぶ。

・パリティ符号、ハミング符号

５．１　基礎

５．１．１　誤り訂正の方法

１）連送方式：同じ符号語を繰り返して送る

２）返送照合方式：受信した符号語を送信側に返送して送信側で照合する。誤りがあれば再送する。

３）自動再送要求方式（ARQ; Automatic Repeat reQuest）受信側で誤りを「検出」し、誤りがあれば再送を要求する。

ACK 方式：送信側は送信後タイマを起動する。受信側は、正しく受信できた場合はACK(acknowledgement)を送る。誤った場合は何も送らない。送信側は、ACK が来たら次の符号語を送る。タイマが切れたら再度符号語を送信する。

NAK 方式：受信側は、正しく受信できた場合は何も送らない。誤っていた場合はNAK(Negative ACK)を送る。送信側は NAK を受け取らない限り次の符号語を送る。NAK が来たら再送する。

ACK と NAK の併用等より深い考察が必要。インターネットは Selective ACK 方式。

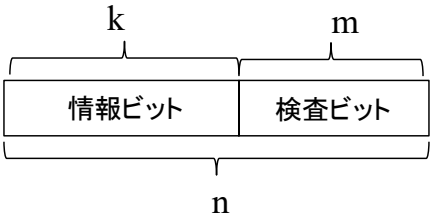
４）FEC（Forward Error Correction）

誤り訂正符号によって、受信側が「訂正」する。

５）混成などその他

５．１．２　組織符号

右図のような構造をもった符号を組織符号と呼ぶ。



【図５．１】(n,k)符号

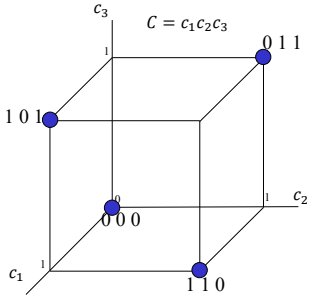
符号長n、情報ビットk、検査ビット$m=n-k$

また、組織符号の中で固定長のものをブロック符号と呼ぶ。

例５．１　(3,2)符号　最も簡単なパリティ符号

符号$\mathbb{C}$＝符号語Cの集合　$\mathbb{C}=\{000,011,101,110\}$

【図５．２】



符号語$C=c_1c_2c_3$ とすると、$c_3=c_1+c_2$となっている。

+は排他的論理和(XOR)

$0+0=0$　$0+1=1$　$1+0=1$　$1+1=0$

これを法２に関する加算　とも呼ぶ。

（今後+は、特に断らない限り排他的論理和を表すこととする）

$c_3=c_1+c_2$は、$c_1+c_2+c_3=0$と等価である。

５．１．３　パリティ符号

例５．１の情報ビットを増やして拡張する。

ここでは、情報ビット$a_5\ a_4\ a_3\ a_2$　に１個の検査記号a_1を付加した符号長５の符号を考える。各符号語の記号１の数が偶数になるように構成する。すなわち、

$$a_5+a_4+a_3+a_2+a_1=0$$

となるように、a_1と定める。これをパリティと呼ぶ。

すべての符号語は、【表５．１】となる。

（発展　検査記号を複数に拡張するとどうなるか。－＞ハミング符号）

表5・1　単一誤り検出(5,4)符号の例

	a_5	a_4	a_3	a_2	a_1		a_5	a_4	a_3	a_2	a_1
1つ1つが符号語	0	0	0	0	0		1	0	0	0	1
	0	0	0	1	1		1	0	0	1	0
	0	0	1	0	1		1	0	1	0	0
	0	0	1	1	0		1	0	1	1	1
	0	1	0	0	1		1	1	0	0	0
	0	1	0	1	0		1	1	0	1	1
	0	1	1	0	0		1	1	1	0	1
	0	1	1	1	1		1	1	1	1	0

全体が符号　16符号語からなる符号

$(b_5\ b_4\ b_3\ b_2\ b_1)=(1\,0\,0\,1\,1)$を受信したとする。

$b_5+b_4+b_3+b_2+b_1\neq 0$　誤り検出可能。

１ビット誤り検出可能。２ビット誤りは検出不可能。

５．１．４　ハミング距離と最小ハミング距離

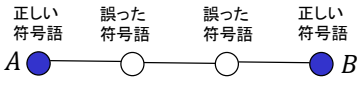
今、２つの符号語、$A=(a_1a_2a_3\ldots a_n)$　と$B=(b_1b_2b_3\ldots b_n)$　を考える。

各ビット毎の差を加算したものをハミング距離と呼ぶ。

$d=\sum_{i=1}^{n}|a_i-b_i|$　　ただし、ここでの加算は排他的論理和ではなく算術加算である。

例）$A=(0\,0\,0\,1\,1)$、$B=(0\,1\,1\,0\,1)$　$d=0\dotplus 1\dotplus 1\dotplus 1\dotplus 0=3$　　ここで、$\dotplus$は通常の算術加算を示す。

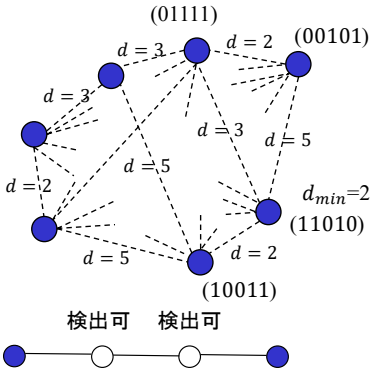
【図５．３】



$d=3$

符号に含まれるすべての符号語間のハミング距離のうち、最小のものを最小ハミング距離（最小距離）と呼ぶ。

【図５．４】



一般に、

・最小距離$d_{min}\geq d\dotplus 1$　のとき、d以下の誤り検出が可能。

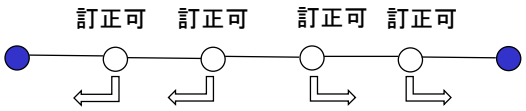
【図５．５】ex）$d_{min}=3$　$d=2$　d:detect の意味

２以下の誤り検出可能

・最小距離$d_{min} \geq 2t+1$ のとき、t以下の誤り訂正が可能。

【図５．６】ex) $d_{min}=5$ $t=2$

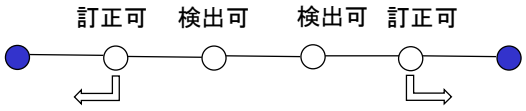
２以下の誤り訂正可能



・最小距離$d_{min} \geq t+d+1$ $(d>t)$ のとき、t以下の誤り訂正とd以下の誤り検出が可能。

【図５．７】ex) $d_{min}=5$ $d=3$ $t=1$

１誤り訂正可能、２・３誤り検出可能



５．１．５　よい(n,k)符号

・符号能率　$\frac{k}{n}$　が大きい

・誤り検出、訂正の能力が高い。　最小距離が大きい。

・誤り検出、訂正の処理が容易。

５．２　ハミング符号

５．２．１　概要

・1950 年にベル研 Richard Hamming によって発案された。

・パリティ検査を拡張。検査記号を複数にし、単一誤り訂正を可能とする。

・符号長　$n=2^m-1$

・検査ビット数　m

・情報ビット　$k=n-m$

・最小距離　3　（単一誤り訂正可能）

・数学的構造が明確。処理が容易。ハードウエア化。

・(3,1)符号、 (7, 4)符号、 (15, 11)符号、 (31, 26)符号　等

・計算機メモリ用 ECC

$m=7$ (127, 120)->1 ビット拡大化-> (128, 120)–>短縮化->(72, 64)8 バイト単位で扱う。

５．２．２　ハミング符号の具体例

【表５．２】　ハミング(7, 4)符号

情報ビットa_7 a_6 a_5 a_3

検査ビットa_4 a_2 a_1

表5･2 単一誤り訂正ハミング(7,4)符号の例

a_7	a_6	a_5	a_4	a_3	a_2	a_1		a_7	a_6	a_5	a_4	a_3	a_2	a_1
0	0	0	0	0	0	0		1	0	0	1	0	1	1
0	0	0	0	1	1	1		1	0	0	1	1	0	0
0	0	1	1	0	0	1		1	0	1	0	0	1	0
0	0	1	1	1	1	0		1	0	1	0	1	0	1
0	1	0	1	0	1	0		1	1	0	0	0	0	1
0	1	0	1	1	0	1		1	1	0	0	1	1	0
0	1	1	0	0	1	1		1	1	1	1	0	0	0
0	1	1	0	1	0	0		1	1	1	1	1	1	1

符号化規則

$$a_7+a_6+a_5+a_4 = 0$$
$$a_7+a_6+a_3+a_2 = 0$$
$$a_7+a_5+a_3+a_1 = 0$$

上の式を、$u=(a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1)$として、以下のように記述できる。

$$(a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1)\begin{pmatrix}1&1&1\\1&1&0\\1&0&1\\1&0&0\\0&1&1\\0&1&0\\0&0&1\end{pmatrix}=u\cdot H^T=0$$

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

符号語=(0 0 0 0 1 1 1)　ベクトルと考える。
符号　符号語の集合　　ベクトル空間

$u=(a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1)=(0\,0\,1\,1\,0\,0\,1)$　を　送　信　し　、　$v=(b_7\ b_6\ b_5\ b_4\ b_3\ b_2\ b_1)=(0\,1\,1\,1\,0\,0\,1)$を受信したとする。符号化規則に照らして以下を計算する。

$$\begin{aligned}s_4&=b_7+b_6+b_5+b_4&&&&=1\\s_2&=b_7+b_6&&+b_3+b_2&&=1\\s_1&=b_7&+b_5&+b_3&+b_1&=0\end{aligned}$$

上の式を、以下のように記述することもできる。

$$s=(s_4\ s_2\ s_1)=v\cdot H^T=(b_7\ b_6\ b_5\ b_4\ b_3\ b_2\ b_1)\cdot H^T=(1\,1\,0)$$

符号化規則によれば、vが正しい符号語ならば、$s=(s_4\ s_2\ s_1)=(0\,0\,0)$となるはずである。しかし、そうはならない。従って、誤りがあることがわかる。s をシンドロームと呼ぶ。また、Hは、誤りがあるかどうかを検査する行列であるため、検査行列と呼ばれる。
（この例では、$s=(s_4\ s_2\ s_1)=(1\,1\,0)=6$であり、$b_6$が誤りであることを決定できるがここでは置いておく）

５．３　線形符号

５．３．１　符号理論のための群、環、体

集合Ｇ、Ｒ、Ｆを考える。

１）群 group

・ある集合Ｇの元に対して、一つの演算○が定義されている
・以下の条件を満たす時、Ｇを群と言う。
Ｇ１（閉塞性）：Ｇの任意の元 a, b に対して、a○b はＧの元である。
Ｇ２（結合則）：Ｇの任意の元 a, b, c に対して、(a○b)○c=a○(b○c)を満たす。
Ｇ３（恒等元）：Ｇの任意の元 a に対して、a○I=I○a=a なるＩ（恒等元）がＧにある。
Ｇ４（逆元）：　Ｇの全ての元 a に対して、a○a’=a’○a=I となる a’（逆元）がＧにある。

１－１）加法群

・群Ｇの演算が＋であったとき、加法群と呼ぶ。
・恒等元 I=0, 逆元 a’=－a と表現する。

１－２）アーベル群

・群ＧがＧ５を満たす時、アーベル群、あるいは可換群と呼ぶ。

Ｇ５（交換則）：Ｇの任意の元 a, b に対して、a○b=b○a を満たす。

１－３）例

・実数すべての集合、すべての整数の集合は加法群でありアーベル群である。

・G={0 1}は、以下の演算＋（これを法２の元の加法と呼ぶ）の元でアーベル群である。

0+0=0　0+1=1　1+0=1　1+1=0

２）環 ring

・ある集合Ｒの元に対して、二つの演算（加法＋　乗法・）が定義されている。

・以下の条件を満たす時、Ｒを環と言う。

Ｒ１（加法群）：Ｒは加法の元でアーベル群である。

Ｒ２（閉塞性）：Ｒの任意の元 a, b に対し、a・b はＲの元である。

Ｒ３（結合則）：Ｒの任意の元 a, b, c に対し、(a・b)・c=a・(b・c)が成り立つ。

Ｒ４（分配則）：Ｒの任意の元 a, b, c に対し、a・(b＋c)=a・b＋a・c および

(a＋b)・c=a・c＋b・c が成り立つ。

２－１）可換環

・環ＲがＲ５を満たす時、可換環と呼ぶ。

Ｒ５（乗法に関する交換則）：Ｒの任意の元 a,b に対して、a・b=b・a を満たす。

２－２）剰余環

・正の整数 r に対して、法 r に関する整数の剰余集合（{0 1 2 ,,, r-1}）は、法 r に関する加法と乗法のもとに環をなす。これを剰余環と呼ぶ。

２－３）例

・R={0 1}は、以下の演算＋

0+0=0　0+1=1　1+0=1　1+1=0

および以下の乗法の元で可換環である。

0・0=0　0・1=0　1・0=0　1・1=1

R は法 2 の剰余環と考えることもできる。

補足２－４）イデアル

・環Ｒの部分集合 J が加法のもとにＲの部分群であり、J の任意の元 a とＲの任意の元 r の積 a・r が J の元であるとき、 J をＲのイデアルと呼ぶ。

３）体 field

・ある集合Ｆが以下の条件を満たす時、Ｆを体と言う。

Ｆ１：Ｆは可換環である。

Ｆ２：Ｆの０以外の元の集合が乗法群をなす。

・有限集合の体を有限体またはガロア体(Galois Field; GF)と呼ぶ。

３－１）例

・有理数全ての集合、実数すべての集合、複素数すべての集合はそれぞれ体である。

・F={0 1}は、以下の加法+

0+0=0　0+1=1　1+0=1　1+1=0

+	0	1
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

および以下の乗法・

0・0=0　0・1=0　1・0=0　1・1=1

の元で、体となる。これをガロア体 GF(2)と呼ぶ。

・p を素数とするとき、法 p に関する整数の剰余の集合$\{0, 1, 2, , , , p-1\}$は、法 p に関する加法と乗法の元に体 GF(p)をなす。

５．３．２　ベクトル空間と符号

GF(2)上の元a_i　$a_i \in GF(2)$　＜ー要は、{0, 1} と　＋　・の演算

GF(2)上の元のn記号列　$\mathbb{a} = (a_n\ a_{n-1}\ \cdots\ a_1)$　$a_i \in GF(2)$

この記号列をベクトルと呼ぶ。

記号列は2^n個ある。これらを要素とする集合をベクトル空間と呼びここではUと表現する。

【図５．８】

$\mathbb{a} \in U$　$\mathbb{b} \in U$　$c \in GF(2)$を考える。

$\mathbb{a} = (a_n\ a_{n-1}\ \cdots\ a_1)$　$a_i \in GF(2)$

$\mathbb{b} = (b_n\ b_{n-1}\ \cdots\ b_1)$　$b_i \in GF(2)$

ここで、積と和を以下のように定義する。

積　$c\mathbb{a} = c(a_n\ a_{n-1}\ \cdots\ a_1) = (ca_n\ ca_{n-1}\ \cdots\ ca_1)$

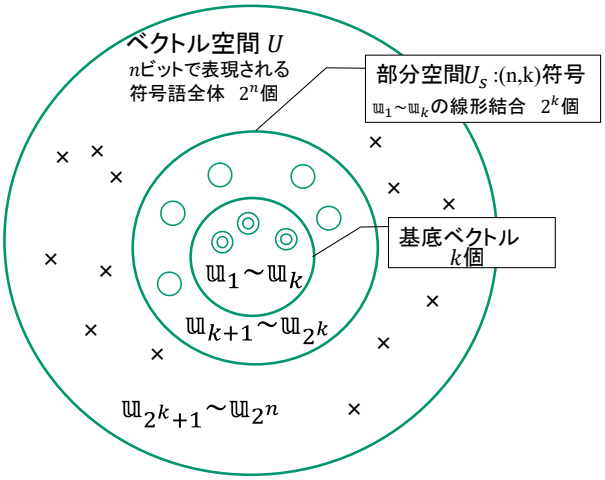
和　$\mathbb{a} + \mathbb{b} = (a_n\ a_{n-1}\ \cdots\ a_1) + (b_n\ b_{n-1}\ \cdots\ b_1) = (a_n + b_n\ a_{n-1} + b_{n-1}\ \cdots\ a_1 + b_1)$

ベクトル$\mathbb{u}$が線形結合、すなわち、$\mathbb{u} = c_1\mathbb{u}_1 + c_2\mathbb{u}_2 + \cdots + c_k\mathbb{u}_k$　であるとき、

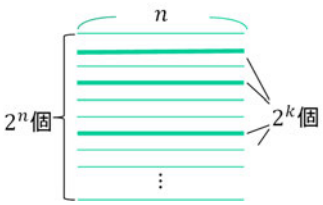
c_1~c_kがすべて０　$\Leftrightarrow$　$\mathbb{u} = 0$

ならば、$\mathbb{u}_1$~$\mathbb{u}_k$は独立であるという。また、$\mathbb{u}_1$~$\mathbb{u}_k$を基底ベクトルという。

(n,k)符号は、nビットの符号語のうち、k個の基底ベクトルの線形結合で表された符号語を用いる。すなわち、2^n個のnビットの符号語のうち、2^k個だけを用いる。



【図５．９】



$\mathbb{u}_1$～$\mathbb{u}_k$の線形結合によって部分空間U_sが生成されることを、基底ベクトル$\mathbb{u}_1$～$\mathbb{u}_k$が部分空間U_sを張る、と表現する。

注意：今後は、ベクトル$\mathbb{u}_1$などをu_1と表現する。

５．３．３　生成行列と検査行列

送信側は、送るべき情報ビットxに生成行列Gをかけて、送信符号語uを求める。

$$u = x \cdot G$$

一方、受信側は受信した符号語vに検査行列Hを使ってシンドロームsを求め、sが０であるかを調べる。

$$s = v \cdot H^T$$

$s = 0$ならば誤りがない。（$u \cdot H^T = 0$である）

$s \neq 0$ならば誤りがある。（さらにこれを用いて誤りを訂正できる可能性がある）

５．３．４　ハミング$(7,4)$符号の例

１）　表５．２から独立な４行を選びベクトルとする。（選び方は一通りではない）

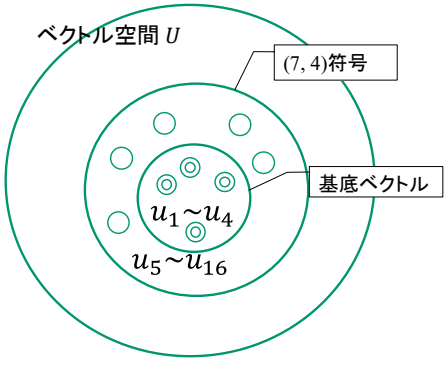
$u_1 = (1\,0\,0\,1\,0\,1\,1)$

$u_2 = (0\,1\,0\,1\,0\,1\,0)$

$u_3 = (0\,0\,1\,1\,0\,0\,1)$

$u_4 = (0\,0\,0\,0\,1\,1\,1)$

他の符号語は、u_1～u_4の線形結合で表現が可能。また、u_1～u_4は独立であり、u_1～u_4は基底ベクトルである。u_1～u_4を線形結合した符号語の集合U_sは、$(7,4)$符号を構成する。【図５．１０】



２）送信側

基底ベクトルを並べた行列が生成行列となる。上記の例のハミング$(7,4)$符号の生成行列Gは、以下となる。

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

情報ビット$x=(x_4\,x_3\,x_2\,x_1)$を送るとき、送るべき符号語uを、$u=x\cdot G$で生成する。

例）$x=(1\,0\,1\,1)$

$$u=x\cdot G=(1\,0\,1\,1)\cdot\begin{pmatrix}1&0&0&1&0&1&1\\0&1&0&1&0&1&0\\0&0&1&1&0&0&1\\0&0&0&0&1&1&1\end{pmatrix}=(1\,0\,1\,0\,1\,0\,1)=u_1+u_3+u_4$$

３）受信側

表５．２の符号化規則から、検査行列Hは以下である。

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

vを受信すると、$s=v\cdot H^T$によりシンドロームを求める。

例　$v=(1\,1\,1\,0\,1\,0\,1)$の時

$$s=v\cdot H^T=(1\,1\,1\,0\,1\,0\,1)\cdot\begin{pmatrix}1&1&1\\1&1&0\\1&0&1\\1&0&0\\0&1&1\\0&1&0\\0&0&1\end{pmatrix}=\quad(1\,1\,0)\quad\neq 0$$

従って、誤りがあることが分かる。

４）生成行列Gと検査行列Hの関係

もし、誤りが起こらず、送信語uと受信語vが一致していれば

$$s=v\cdot H^T=u\cdot H^T=(x\cdot G)H^T=x\cdot(G\cdot H^T)=0\ for\ any\ x$$

となる。従って$G\cdot H^T=0$となるようにG、Hを構成する。

（一般的には、HからGを求める場合は、Hを行基本変形し Reduced Row Echelon Form を求め、零空間の基底ベクトルからGを定める。$H=(A|I)$［Iは単位行列］の形式の場合はより簡単に求められる。補足資料２（補足資料１を読んだ後の方が理解しやすい））

５．４　ハミング符号詳細－ハミング(7,4)符号を例に－

別紙　補足資料１

５．５　線形符号のさらなる議論

５．５．１　最小距離と最小重み

１）ハミング重みω

符号語を$u=(a_n\,a_{n-1}\cdots a_1)$　とするとき、0 ではないa_iの数をハミング重みという。

２）最小重みω_{min}

符号Uの全符号語（すべて 0 の語以外）で、最小のハミング重みをUの最小重みという。

例）表５．２のハミング(7,4)符号の最小重みは３

３）ハミング距離dとハミング重みω

u_1とu_2のハミング距離は、u_1-u_2のハミング重みに等しい

例　$u_1=(100)$、$u_2=(001)$　距離は２。$u_1-u_2=(101)$、重みは２。

４）最小距離d_{min}と最小重みω_{min}

ベクトル空間Uの符号語間の最小距離をd_{min}、Uの最小重みをω_{min}とすると、

$d_{min}=\omega_{min}$

である。

（課題　４）を証明せよ。）

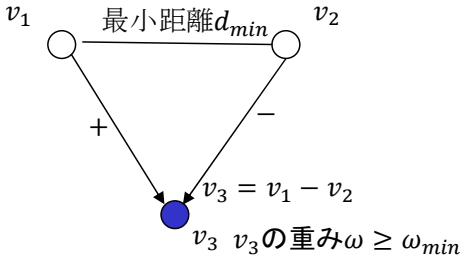
０）準備

Uの基底ベクトルをu_1~u_kとする。Uの符号語v_iは、以下のように表現できる。

$$v_i=c_{i_1}u_1+c_{i_2}u_2+\cdots+c_{i_k}u_k=\sum_{m=1}^{k}c_{i_m}u_m\in U$$

また、Uの２つの符号語v_iとv_jの差はまたUの符号語である。すなわち、　$v_i-v_j\in U$

１）今、v_1とv_2を最小距離d_{min}離れている符号語とする。



$$d_{min}=|v_1-v_2|=\left|\sum c_{1_m}u_m-\sum c_{2_m}u_m\right|$$

$$=\left|\sum(c_{1_m}-c_{2_m})u_m\right|$$

$$=\sum(c_{1_m}-c_{2_m})$$

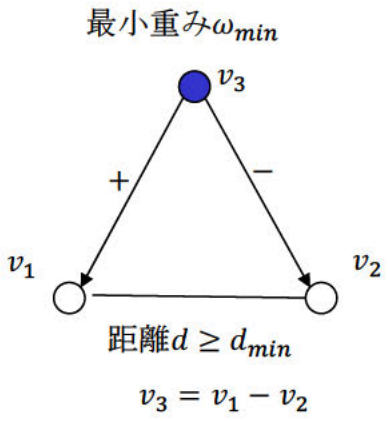
$v_3=v_1-v_2$　とすると、$v_3\in U$であるから、$v_3=\sum_{m=1}^{k}c_{3_m}u_m$と表現できる。

$$v_3=\sum_{m=1}^{k}c_{3_m}u_m=\sum_{m=1}^{k}c_{1_m}u_m-\sum_{m=1}^{k}c_{2_m}u_m=\sum_{m=1}^{k}(c_{1_m}-c_{2_m})u_m$$

v_3の重みは、

$$\omega=\sum_{m=1}^{k}c_{3_m}=\sum_{m=1}^{k}(c_{1_m}-c_{2_m})=d_{min}$$

ωはω_{min}以上であるので、$d_{min} = \omega \geq \omega_{min}$
すなわち、$d_{min} \geq \omega_{min}$



2）v_3は最小重みω_{min}を持つ符号語とする。ただし、$v_3 \neq 0$

$$v_3 = \sum_{m=1}^{k} c_{3_m} u_m$$

とすれば、$\omega_{min} = \sum_{m=1}^{k} c_{3_m}$　である。
一方、$v_3 = v_1 - v_2$　となるv_1，v_2が存在する。
すなわち、

$$v_3 = \sum_{m=1}^{k} c_{3_m} u_m = \sum_{m=1}^{k} c_{1_m} u_m - \sum_{m=1}^{k} c_{2_m} u_m = \sum_{m=1}^{k} (c_{1_m} - c_{2_m}) u_m$$

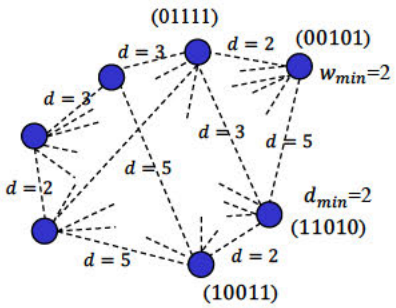
よって、

$$c_{3_m} = c_{1_m} - c_{2_m}$$

v_1とv_2の距離 d　は、

$$d = |v_1 - v_2| = \left| \sum c_{1_m} u_m - \sum c_{2_m} u_m \right| = \left| \sum (c_{1_m} - c_{2_m}) u_m \right| = \sum c_{3_m} = \omega_{min}$$

dは、d_{min}以上であるので、$d_{min} \leq d = \omega_{min}$
すなわち、$d_{min} \leq \omega_{min}$



3）1）2）より、$d_{min} = \omega_{min}$

5．5．2　最小距離の求め方

1）生成行列Gから求める。
$d_{min} = \omega_{min}$　より、ω_{min}　から求められる。
ただし、Gの中にω_{min}の符号語があるように線形結合で求める。

2）検査行列Hから求める。
Hの列ベクトルで独立な物の数から求める。
Hの列ベクトル（n個あるとする）を考える。

(1)　全列ベクトルの中から　d_m個の列ベクトルを取り出す。この全組み合わせ（$\binom{n}{d_m}$通り）の中に線形従属なものがあれば、　$d_{min} \leq d_m$

(2)　全列ベクトルの中から　$d_m - 1$個の列ベクトルを取り出す。この全組み合わせ（$\binom{n}{d_m - 1}$通り）がすべて独立ならば、　$d_{min} \geq d_m$

(3) (1)(2)よりこのようなd_mを見つけられれば、　$d_{min} = d_m$

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

(1) 7つある列ベクトルから、$d_m=3$　個の列ベクトルを取り出す。

$\begin{bmatrix}0\\1\\1\end{bmatrix}+\begin{bmatrix}0\\1\\0\end{bmatrix}+\begin{bmatrix}0\\0\\1\end{bmatrix}=0$

よってこの3つの列ベクトルは従属。従って、$d_{min}\leq 3$

(2) $d_m-1=2$　個を取り出す。

どの2つの列ベクトルをとっても独立。

例えば、$c_1\begin{bmatrix}1\\1\\1\end{bmatrix}+c_2\begin{bmatrix}1\\1\\0\end{bmatrix}=0$　　となるためには、　$c_1=0$、$c_2=0$

従って、$d_{min}\geq 3$

(3)(1)(2)より、$d_{min}=3$

５．５．３　復号の基礎

復号については後にまとめて説明することとして、ここでは、キーワードだけを列挙しておく。

復号法

最大事後確率復号法（MAP）　と　最尤復号法（MLD）

最小距離復号法（MDD）　と　限界距離復号法（BDD）

誤り訂正能力

シングルトン限界と最大距離分離符号

ハミングの限界式と完全符号

バルシャモフ＝ギルバート限界式

５．６　積符号・拡張ハミング・短縮ハミング

５．６．１　積符号

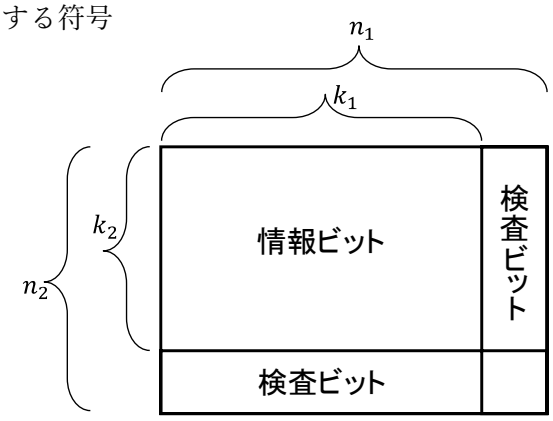
(n_1,k_1)符号と(n_2,k_2)符号を2次元に配列する符号

情報ビット数　k_1k_2

検査ビット数　$n_1n_2-k_1k_2$

符号長　n_1n_2

最小距離　$d_{min_1}+d_{min_2}$



ただし、d_{min_1}、d_{min_2}は、それぞれ(n_1, k_1)符号、(n_2, k_2)符号の最小距離

例　水平垂直パリティ符号　（積符号の一種）

x_1	x_2	c_1
x_3	x_4	c_2
c_3	c_4	c_5

例 1 (9,4) 符号　　演習問題５．２も参照のこと

２つの (3,2) 符号の組み合わせ

符号語 $u = (x_1\ x_2\ x_3\ x_4\ c_1\ c_2\ c_3\ c_4\ c_5)$

情報ビット数 2×2=4　検査ビット数 3×3-2×2=5　符号長 3×3=9

検査規則は、以下である。

$$
\begin{aligned}
x_1 + x_2 \qquad\quad + c_1 \qquad\qquad\quad &= 0 \\
\qquad x_3 + x_4 \qquad + c_2 \qquad\quad &= 0 \\
x_1 \qquad + x_3 \qquad\quad + c_3 \qquad\quad &= 0 \\
\qquad x_2 \qquad + x_4 \qquad\quad + c_4 \qquad &= 0 \\
x_1 + x_2 + x_3 + x_4 \qquad\quad + c_5 &= 0
\end{aligned}
$$

従って、検査行列は以下となる。

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

(3,2) 符号の最小距離は、２であるので、最小距離 4。

従って、１誤り訂正と２誤り検出が可能。

例 2 (35,24) 符号　　HDLC で実用化された

(5,4) 符号と (7,6) 符号の組み合わせ

情報ビット数 4×6=24

検査ビット数 5×7-4×6=11　符号長 5×7=35

(5,4) 符号、(7,6) 符号の最小距離は、

ともに２であるので、最小距離 4。

x_1	x_2	x_3	x_4	c_1
x_5	x_6	x_7	x_8	c_2
x_9	x_{10}	x_{11}	x_{12}	c_3
x_{13}	x_{14}	x_{15}	x_{16}	c_4
x_{17}	x_{18}	x_{19}	x_{20}	c_5
x_{21}	x_{22}	x_{23}	x_{24}	c_6
c_7	c_8	c_9	c_{10}	c_{11}

５．６．２　拡張ハミング(Extended Hamming Code)

拡大ハミングとも呼ぶ。

例えば、ハミング (7,4) 符号にさらに１個のパリティを加えて、(8, 4)符号を作る。

つまり、ハミング (7,4) 符号の符号語を$(a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1)$とするとき、

$a_7 + a_6 + a_5 + a_4 + a_3 + a_2 + a_1 + a_0 = 0$　となるようにa_0を定める。

$(a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1\ a_0)$で構成された符号を拡張ハミング (8,4) 符号と言う。

ハミング (7,4) 符号の最小距離は３であるのに対し、(8,4) 符号の最小距離は４となる。

５．６．３　短縮ハミング(Shortened Hamming Code)

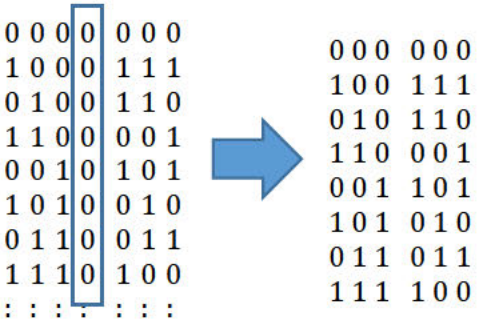
短縮化ハミングとも呼ぶ。

ハミング(n,k)符号からl個の情報記号がすべて 0 である符号語を取り出し、l個の 0 を除く。これによって構成される$(n-l,k-l)$符号を短縮化ハミング符号と呼ぶ。

最小重みは変わらない。

例　短縮ハミング(6,3)符号　$l=1$

ハミング(7,4)符号　　短縮ハミング(6,3)符号



元のハミング(7, 4)符号

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

短縮ハミング(6, 3)符号

$$H_S=\begin{pmatrix}1&1&1&1&0&0\\1&1&0&0&1&0\\1&0&1&0&0&1\end{pmatrix}\quad G_S=\begin{pmatrix}1&0&0&1&1&1\\0&1&0&1&1&0\\0&0&1&1&0&1\end{pmatrix}$$

５．４　ハミング符号詳細－ハミング(7,4)符号を例に－

５．４．１　検査行列

ハミング(7,4)符号の検査行列H

$$H=\begin{pmatrix}\circ & \circ & \circ & \circ & \circ & \circ & \circ\\ \circ & \circ & \circ & \circ & \circ & \circ & \circ\\ \circ & \circ & \circ & \circ & \circ & \circ & \circ\end{pmatrix}$$

条件

・全ての列要素がゼロではない

・全ての列要素が異なる

（課題:なぜこの条件か。ヒント:すべてのビットの単一誤りをチェックするためには？）

列の数 7、3 ビットの組み合わせ$2^3=8$

従って、0 以外の全パターンが必ずHの列として入る。ただし入り方は任意である。例えば、

$$H_1=\begin{pmatrix}1 & 1 & 1 & 0 & 0 & 1 & 0\\ 1 & 1 & 0 & 1 & 1 & 0 & 0\\ 0 & 1 & 1 & 1 & 0 & 0 & 1\end{pmatrix}\quad H_2=\begin{pmatrix}1 & 1 & 1 & 0 & 0 & 1 & 0\\ 1 & 1 & 0 & 1 & 1 & 0 & 0\\ 1 & 0 & 1 & 1 & 0 & 0 & 1\end{pmatrix}$$

などが考えられる。典型的な作成方法として、以下の２種類（ここでは、①単位行列法、②ビットパターン法と呼ぶ）を挙げる。

５．４．２　単位行列法

１）検査行列H

検査行列Hを

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

のように後半を単位行列とする。例えば、

$$H_1=\begin{pmatrix}1 & 0 & 1 & 1 & 1 & 0 & 0\\ 1 & 1 & 0 & 1 & 0 & 1 & 0\\ 0 & 1 & 1 & 1 & 0 & 0 & 1\end{pmatrix}\quad H_2=\begin{pmatrix}1 & 1 & 1 & 0 & 1 & 0 & 0\\ 0 & 1 & 1 & 1 & 0 & 1 & 0\\ 1 & 1 & 0 & 1 & 0 & 0 & 1\end{pmatrix}$$

以下では、H_1で説明する。符号語を$u=(a_7,a_6,a_5,a_4,a_3,a_2,a_1)$とすると、$H_1$は、

$$\begin{aligned}a_7 \quad &+a_5+a_4+a_3 \quad &&=0\\ a_7+a_6 \quad &+a_4 \quad &+a_2 \quad &=0\\ a_6+a_5+a_4 \quad &&+a_1 \quad &=0\end{aligned}$$

の符号化規則（ルール）を表現している。

２）生成行列G

生成行列Gは、$G \cdot H^T = 0$より

$$\begin{pmatrix} ○ & ○ & ○ & ○ & ○ & ○ & ○ \\ ○ & ○ & ○ & ○ & ○ & ○ & ○ \\ ○ & ○ & ○ & ○ & ○ & ○ & ○ \\ ○ & ○ & ○ & ○ & ○ & ○ & ○ \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

4×7　　7×3　　4×3

を解いて求められる。

Gには 28 個の変数がある。一方$G \cdot H^T = 0$で立てられた方程式は、12 本。よって 16 個は任意となる。Gの前部 16 個を単位行列とする方法がある。（既約標準形、既約梯陣形と呼ぶ：いつもこの形にできるとは限らない）。

$$G \cdot H^T = \begin{pmatrix} 1 & 0 & 0 & 0 & g_{15} & g_{16} & g_{17} \\ 0 & 1 & 0 & 0 & g_{25} & g_{26} & g_{27} \\ 0 & 0 & 1 & 0 & g_{35} & g_{36} & g_{37} \\ 0 & 0 & 0 & 1 & g_{45} & g_{46} & g_{47} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 0$$

ただし、最終行０はすべての要素が０の行列を意味している。これを解くと、（課題：実際に解け）その結果、

$$G = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

が得られる。G の後半部は、Hの前半部（単位行列より前の部分）の転置となっていることに注意せよ。（課題：$H = (A|I)$、$G = (I|B)$となる時、$B = A^T$　となることを証明せよ。）

３）符号語の生成

符号化したい情報ビットを$x = (x_7\ x_6\ x_5\ x_4)$とすると、符号語uは、$u = x \cdot G$で生成される。

例）$x = (1\ 0\ 1\ 1)$

$$x \cdot G = (1\ 0\ 1\ 1) \cdot \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) = (1\ 0\ 1\ 1\ 1\ 0\ 0)$$

この方法では、符号語の前半に情報ビットが現れる。（課題：すべての符号語を求めよ。）

４）誤り訂正

vを受信すると、$s = v \cdot H^T$によりシンドロームを求める。

今、$u = (a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1) = (1\ 0\ 1\ 1\ 1\ 0\ 0)$を送信し、

$v = (b_7\ b_6\ b_5\ b_4\ b_3\ b_2\ b_1) = (1\ 1\ 1\ 1\ 1\ 0\ 0)$を受信したとすると、

$$s = (1\,1\,1\,1\,1\,0\,0) \cdot \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (0\,1\,1) = (s_3\ s_2\ s_1)$$

となる。シンドローム$(0\,1\,1)$は、H^Tの下から６行目（上から２行目）に一致する。このため、誤りのあるビットはb_6であり、誤りが訂正できる。

（証明：今、$u = (a_n\ a_{n-1}\ \cdots\ a_1)$を送信し、下位ビットから$i$ビット目が誤った$v$を受信したとする。下位ビットから$i$番目のビットだけが 1 のベクトル（単一誤りベクトル）を$e_i = (0\,0\ \cdots\ 1\ \cdots\ 0)$とすると、$v = u + e_i$と表現できる。

$$v \cdot H^T = (u + e_i) \cdot H^T = u \cdot H^T + e_i \cdot H^T = e_i \cdot H^T = (0\,0\ \cdots\ 1\ \cdots\ 0) \cdot \begin{pmatrix} [h_n] \\ \vdots \\ \vdots \\ [h_i] \\ \vdots \\ \vdots \\ [h_1] \end{pmatrix} = [h_i]$$

（$[h_i]$はH^Tの下からi行目である。）

５．４．３　ビットパターン法

１）検査行列H

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

Hの各列を、１から 7 の 2 進数の順に並べる。

このとき、符号語を$u = (a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1)$とすると、$H$は、

$$\begin{array}{llll} a_7 + a_6 + a_5 + a_4 + & & & = 0 \\ a_7 + a_6 & + a_3 + a_2 & & = 0 \\ a_7 & + a_5 & + a_3 + a_1 & = 0 \end{array}$$

の符号化規則を表現している。

２）生成行列G

Hに対するG は、以下となる。

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

（課題：G を求めよ。一種類ではない。）

３）符号語の生成

符号化したい情報ビットを$x = (a_7\ a_6\ a_5\ a_4)$とすると、符号語uは、$u = x \cdot G$で生成される。

例）$x = (1\,0\,1\,1)$

$$x \cdot G = (1\,0\,1\,1) \cdot \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} = (1\,0\,1\,0\,1\,0\,1)$$

４）誤り訂正

今、$u = (a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1) = (1\,0\,1\,0\,1\,0\,1)$を送信し、

$v = (b_7\ b_6\ b_5\ b_4\ b_3\ b_2\ b_1) = (1\,1\,1\,0\,1\,0\,1)$を受信したとすると、

$$s = (1\,1\,1\,0\,1\,0\,1) \cdot \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (\,1\,1\,0\,) = (s_3\ s_2\ s_1)$$

となる。単位行列法と同様に、シンドローム$(\,1\,1\,0\,)$は、H^Tの下から６行目に一致する。このように誤りが訂正できる。しかし、

$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$の各行は２進数で行番号を表現しているので、$(1\,1\,0)$を１０進数で読んだ６は、$b_6$を直接表現している。単位行列法ではパターン検索が必要だが、ビットパターン法では省ける。

５）補足

Hの各行が２進数を表現していることは、

$$\begin{array}{lllllll} 2^2 & a_7 + a_6 + a_5 + a_4 & & & & & = 0 \\ 2^1 & a_7 + a_6 & & + a_3 + a_2 & & & = 0 \\ 2^0 & a_7 & + a_5 & & + a_3 & + a_1 & = 0 \end{array}$$

のようにシンドロームの要素に２のべき乗の重みがついていることと等価である。これは、例えば、b_6 に誤りがあるかどうかを、$6 = 4 + 2 = 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$ と分解して検査しているとも言える。

情報通信基礎Ⅰ　第５章　補足資料２　検査行列と生成行列

情シス　渡辺

ここでは、検査行列と生成行列の関係を議論する。まず、零空間の基底について述べる。その後、一方が分かったときにもう一方を求める方法について述べる。

１．零空間と基底

検査行列Hと生成行列Gは、$GH^T = 0$　あるいは、$HG^T = 0$ の関係がある。これは、線形代数の零空間の基底の概念が関係する。

連立一次方程式を以下の行列で表現する。

$$Ax = b \qquad (eq.1-1)$$

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & & \\ a_{31} & & & & \\ \vdots & & & \ddots & \\ a_{m1} & & & & a_{mn} \end{pmatrix} \quad x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \quad b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

Aは$m \times n$行列、xはn次元列ベクトル、bはm次元列ベクトルである。最も簡単な例は、$m = n$かつAがランクnの正方行列の場合である。

$m \times n$の行列Aに対して、行空間（row space）、列空間（column space）、零空間（null space）、左零空間（left null space）の４つの部分空間が定義される。このうち、零空間とは、$b = 0$すなわち、

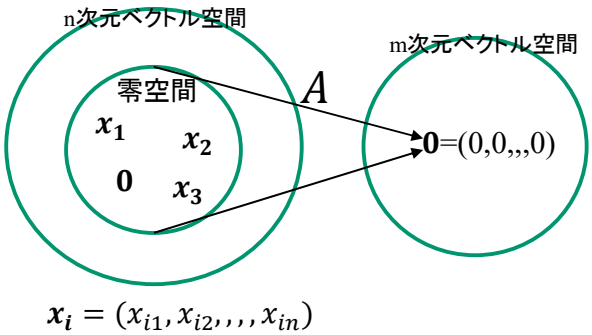
$$Ax = \mathbf{0} \qquad (eq.1-2)$$

となるベクトルxの集合をさす。eq. 1-2 は、

$$Ax = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & & \\ a_{31} & & & & \\ \vdots & & & \ddots & \\ a_{m1} & & & & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

であるので、これを満たす各xはAのすべての行との内積が０である、すなわち、直交している。つまり、零空間とは、Aのすべての行ベクトルと直交する列ベクトルの集合と言える。

また、$Ax = 0$とは、図のように、零空間に属するどのベクトルもAで写像すると０ベクトルとなることを意味している。従って、零空間を核（kernel）とも呼ぶ。なお、要素がすべて０のベクトルも零空間に属していることを注意しておく。



$$\boldsymbol{x_i} = (x_{i1}, x_{i2}, , , , x_{in})$$

零空間には複数のベクトルが存在するが、それらはいくつかの基本ベクトル（基底ベクトル）の線形結合によって作り出せる。すなわち基底ベクトル（の集合）を求められれば零空間を曖昧性なく表現することができる。これを零空間の基底と呼ぶ。

検査行列と生成行列について考える。例えば検査行列Hから生成行列Gを求めるには、$Hx = 0$ となる列ベクトルxの必要十分な集合、すなわちHの零空間の基底ベクトル（の集合）を求めればよい。

（Hは$m \times n$、符号長n、情報ビット数k、冗長ビット数$m = n - k$ 、$n \geq m$）

２．検査行列や生成行列の求め方

一方が分かったときにもう一方を求める方法としては、１）零空間の基底より求める方法、２）標準形より求める方法、３）列交換による方法、４）行基本変形による方法がある。

A．方法１　零空間の基底より求める方法

（１）原理は、１．で述べた通りである。この方法は、どんな検査行列と生成行列にも適用できる。

（２）例

以下の(6, 3)符号を例として取り上げる。（後で述べるようにこの例では、生成行列Gを簡単に求められるが、敢えて零空間の基底を求める方法を述べる）

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \qquad (eq.2-1)$$

（ステップ１）ガウスージョルダン消去法を用いてHの RREF（Reduced Row Echelon Form）を求める。

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} \mathbf{1} & 0 & 1 & 0 & 0 & 1 \\ 0 & \mathbf{1} & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & \mathbf{1} & 1 & 1 \end{pmatrix} \qquad (eq.2-2)$$

太字の１を leading entry（あるいはピボット）と呼ぶ。Hのランクは leading entry の数３である。

----eq. 2-2 の確認

$Hx = 0$ の両辺を「行列の行基本変形」で変形する。（GF(2)上で計算する）

第１行と第３行を入れ替え、第２行－第１行を第２行にし、第３行－第２行を第３行にする。このため、以下の操作を行う。

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} Hx = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} 0$$

左辺$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} Hx = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}\begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} x = \begin{pmatrix} \mathbf{1} & 0 & 1 & 0 & 0 & 1 \\ 0 & \mathbf{1} & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & \mathbf{1} & 1 & 1 \end{pmatrix} x$

右辺$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} 0 = 0$　（右辺は、どのような基本変形を行っても０ベクトルである）

以上より、$\begin{pmatrix} \mathbf{1} & 0 & 1 & 0 & 0 & 1 \\ 0 & \mathbf{1} & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & \mathbf{1} & 1 & 1 \end{pmatrix} x = 0$

（ステップ２）$Hx = 0$の連立方程式を考える。

$$Hx = \begin{pmatrix} \mathbf{1} & 0 & 1 & 0 & 0 & 1 \\ 0 & \mathbf{1} & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & \mathbf{1} & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} = 0 \qquad (eq.2-3)$$

leading entry に対応するx_1，x_2，x_4以外のxの要素、すなわち、x_3，x_5，x_6を自由変数（free variable）とし、以下のように変形する。（太文字の３行を追加）

$$\begin{pmatrix} \mathbf{1} & 0 & 1 & 0 & 0 & 1 \\ 0 & \mathbf{1} & 1 & 0 & 1 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ 0 & 0 & 0 & \mathbf{1} & 1 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ x_3 \\ 0 \\ x_5 \\ x_6 \end{pmatrix} \qquad (eq.2-4)$$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} = \begin{pmatrix} -1 & 0 & -1 \\ -1 & -1 & -1 \\ 1 & 0 & 0 \\ 0 & -1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_3 \\ x_5 \\ x_6 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_3 \\ x_5 \\ x_6 \end{pmatrix} \qquad (eq.2-5)$$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} x_3 + \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} x_5 + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} x_6 \qquad (eq.2-6)$$

これより、$Hx = 0$ となるxの集合（零空間）に属す任意のベクトル$(x_1, x_2, x_3, x_4, x_5, x_6)$は、(111000) (010110) (110101)の線形結合で表現されることがわかる。また、$(x_1, x_2, x_3, x_4, x_5, x_6) = 0$ となる必要十分条件は、x_3, x_5, x_6がすべて 0 であることである。従って、(111000) (010110) (110101)は一次独立である。以上より、(111000) (010110) (110101)は、基底ベクトルである。すなわち、これらがHの零空間の基底ベクトルである。なお、これらの基底ベクトルは直交していない。

Hの零空間$Null(H)$が基底ベクトルの線形結合で表現されることを以下のように表現する。

$$Null(H) = span\left(\begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \right) \qquad (eq.2-7)$$

この零空間の次元は 3 である。

符号長n、Hのランク、零空間の次元（nullity、free variable の数）kの間には、$n - \mathrm{rank}\, H = k$ の関係がある。（この場合は、6 - 3 = 3 である）

（ステップ３）生成行列Gを作成する。

零空間の基底を転置して求める。

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \qquad (eq.2-8)$$

B．方法２　標準形より求める方法

（１）今、検査行列H　（$m \times n$行列）が得られている場合に、生成行列G　（$k \times n$行列）を求めたいとする。（$k = n - m$ ）

検査行列が標準形、すなわち、$H = [\, A \mid I_m \,]$　であれば、$G = [\, I_k \mid A^T \,]$　として求められる。ここで、I_mは$m \times m$の単位行列、Aは$m \times k$行列である。

（２）例

eq. 2-1 と同じ検査行列を考える。

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \qquad (eq.2-1)$$

$H = (A|I_3)$　の形式となっているので、$G = (I_{6-3}|A^T)$　として求められる。

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \qquad (eq.2-9)$$

（３）証明

$H = [\,A \mid I_m\,]$、$G = [\,I_k \mid B\,]$　とする。Bは$k \times m$行列である。

$$GH^T = [\,I_k \mid B\,]\begin{bmatrix} A^T \\ - \\ [I_m]^T \end{bmatrix} = [\,I_k \mid B\,]\begin{bmatrix} A^T \\ - \\ I_m \end{bmatrix} = I_k\,A^T + BI_m = A^T + B \quad (eq.2-10)$$

よって、$B = -A^T$　（GF(2)上では、$B = A^T$）であれば、$GH^T = 0$となる。

Ｃ．方法３　列交換よる方法

（１）検査行列Hから生成行列Gを求める方法として、列交換による方法がある。

Hの列を入れ替えて標準形とできれば、方法２と同様に対応する生成行列を求められる。その後、再度列を入れ替えて（戻して）生成行列Gを求める。

（２）例

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \qquad (eq.2-11)$$

とする。Hの右から３列と４列目を入れ替えて標準形とする。

$$H_{34} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \qquad (eq.2-12)$$

H_{34}　に対する生成行列G_{34}を求める。

$$G_{34} = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right) \qquad (eq.2-13)$$

G_{34}　の右から３列目と４列目を入れ替えてG　を得る。

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \qquad (eq.2-14)$$

（３）証明

（ステップ１）Hのi列目とj列目を入れ替えて標準形H_1とする。そのために、i列目とj列目を入れ替える変換行列R_{ij}を右からかける。

$$H_1 = HR_{ij} = [\,A \mid I_m\,] \qquad (eq.2-15)$$

R_{ij}は、$n \times n$の正則行列であり、対称行列でもある。従って、以下が成立する。

$$R_{ij} = R_{ji} = \left(R_{ij}\right)^T = {R_{ij}}^{-1} \qquad (eq.2-16)$$

$$R_{ij}R_{ij} = I_n \qquad (eq.2-17)$$

また、eq. 2-15 より、以下を得る。

$$H = H_1\left(R_{ij}\right)^{-1} \qquad (eq.2-18)$$

（ステップ２）H_1に対する生成行列G_1を求める。

$$G_1 = [\, I_k \mid A^T \,] \quad (eq.2-19)$$

（ステップ３）G_1と${H_1}^T$の積を求める。

$$G_1{H_1}^T = [\, I_k \mid A^T \,] \begin{bmatrix} A^T \\ - \\ I_m \end{bmatrix} = 0 \quad (eq.2-20)$$

（ステップ４）G_1　のj列目とi列目を入れ替えた生成行列をG_xとする。

$$G_x = G_1 R_{ji} \qquad (eq.2-21)$$

（ステップ５）$G_x H^T$を計算すると、

$$G_x H^T = \left(G_1 R_{ji}\right) H^T \qquad (eq.2-21)\text{より}$$

$$= \left(G_1 R_{ij}\right) \left[H_1 \left(R_{ij}\right)^{-1}\right]^T \qquad (eq.2-18)\text{より}$$

$$= G_1 R_{ij} \left[\left(R_{ij}\right)^{-1}\right]^T {H_1}^T = G_1 R_{ij} \left(R_{ij}\right)^T {H_1}^T = G_1 R_{ij} R_{ij} {H_1}^T = G_1 {H_1}^T = 0 \qquad (eq.2-16)\text{より}$$

となり、G_xは、Hの生成行列であることが証明できる。

上記は、１回のR_{ij}で標準形に変形可能な場合である。複数回で行う場合も同様に示すことができる。また、（２）で示した例では、以下の変換行列を用いている。

$$R_{34} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad H_{34} = HR_{34} \quad G = G_{34} R_{43} \quad R_{34} * R_{34} = I_7$$

D．方法４　行基本変形による方法

（１）行基本変形によっても、検査行列Hから生成行列Gを求められる。

Hを行列の行基本変形で操作し標準形とできれば、方法２と同様に、対応する生成行列を求められる。

（２）例

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \qquad (eq.2-22)$$

Hを行基本変形して標準形とする。まず、2 行目に 1 行目の-1 倍を加算し、その後 3 行目に 1 行目の-1 倍を加算する。これをH_1とする。

$$H \sim \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} = H_1 = [\, A \mid I_3 \,] \quad (eq.2-23)$$

H_1に対する生成行列G_1を求める。

$$G_1 = [\, I_3 \mid A^T \,] = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} (eq.2-24)$$

このG_1がHに対応する生成行列となる。

（３）証明

（ステップ１）Hで、c_i倍のi行目をj行目に加算する行基本変形を$L(i,c_i,j)$とする。

$$L(i,c_i,j)=\begin{pmatrix}1&0&0&\cdots&0&\cdots&0&\cdots&0\\0&1&0&\cdots&0&\cdots&0&\cdots&0\\:&:&:&\cdots&:&\cdots&:&\cdots&:\\0&0&0&\cdots&1&\cdots&0&\cdots&0\\:&:&:&\cdots&:&\cdots&:&\cdots&:\\0&0&0&\cdots&c_i&\cdots&1&\cdots&0\\:&:&:&\cdots&:&\cdots&:&\cdots&:\\0&0&0&\cdots&0&\cdots&0&\cdots&1\end{pmatrix}\begin{matrix}\\\\\\i-th\ row\\\\j-th\ row\\\\\end{matrix}\quad(eq.2-25)$$

$$\begin{matrix}&&&&i-th\ col.&&j-th\ col.&&\end{matrix}$$

これをHに左からかけて、標準形H_1とする。

$$H_1=L(i,c_i,j)H=[\,A\mid I_m\,]\quad(eq.2-26)$$

$L(i,c_i,j)$は、正則であり、逆変換が存在する。

$$H=\left(L(i,c_i,j)\right)^{-1}H_1\quad(eq.2-27)$$

（ステップ２）H_1に対する生成行列G_1を求める。

$$G_1=[\,I_k\mid A^T\,]\quad(eq.2-28)$$

（ステップ３）G_1と${H_1}^T$の積を求める。

$$G_1{H_1}^T=[\,I_k\mid A^T\,]\begin{bmatrix}A^T\\-\\I_m\end{bmatrix}=0\quad(eq.2-29)$$

（ステップ４）G_1H^Tを計算する。

$$G_1H^T=G_1\left[\left(L(i,c_i,j)\right)^{-1}H_1\right]^T=G_1{H_1}^T\left[\left(L(i,c_i,j)\right)^{-1}\right]^T=0\quad(eq.2-30)$$

よって、G_1はHの生成行列となる。

上記は、１回のL_{ij}で標準形に変形可能な場合である。複数回で行う場合も同様に示すことができる。（２）の例の、2 行目に 1 行目の-1 倍を加算する変換行列L_{21}、3 行目に 1 行目の-1 倍を加算する変換行列L_{31}は以下である。

$$L_{21}=L(1,-1,2)=\begin{pmatrix}1&0&0\\-1&1&0\\0&0&1\end{pmatrix}\qquad L_{31}=L(1,-1,3)=\begin{pmatrix}1&0&0\\0&1&0\\-1&0&1\end{pmatrix}$$

３．　課題

（課題１）生成行列Gから検査行列Hを求めたい。方法３　列交換による方法、方法４　行基本変形による方法で求めることは可能か。

（課題２）方法３　列交換による方法のハミング符号への適用可能性を議論せよ。

（課題３）eq. 2-8 で求めたG、および eq. 2-9 で求めたG_2は同じ符号を生成することを確認せよ。

（課題４）検査行列Hが eq. 3-1 で与えられている。Hの RREF が eq. 3-2 となることを導け。また、零空間の基底ベクトルを求め、生成行列Gが eq. 3-3 となることを示せ。

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix} \qquad (eq. 3-1)$$

$$H\sim \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad (eq. 3-2)$$

$$G = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad (eq. 3-3)$$

（これは、第 7 章で登場する Goppa(9, 5, 3)符号である。）

以下は配布せず

３．（課題１の解答）

結果的には可能である。

生成行列から検査行列を求める方法

（１）生成行列Gから検査行列Hを求める。検査行列Hから生成行列Gを求める場合と同様に、１）零空間の基底より求める方法、２）標準形より求める方法、３）列交換による方法、４）行基本変形による方法がある。ここでは３）４）について述べる。

方法３　列交換による方法

生成行列G　（$k \times n$行列）が得られている場合に、検査行列H　（$m \times n$行列）を求めたい。($k = n - m$)このとき、生成行列Gの列を入れ替えて標準形とできれば、方法２と同様に対応する検査行列を求められる。その後、再度列を入れ替えて（戻して）検査行列Hを求める。

（２）例

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \qquad (eq.3-10)$$

とする。Gの右から３列目と４列目を入れ替えて標準形とする。

$$G_{34} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \qquad (eq.3-11)$$

G_{34}　に対する検査行列H_{34}を求める。

$$H_{34} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \qquad (eq.3-12)$$

H_{34}　の右から３列目と４列目を入れ替えてH　を得る。

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \qquad (eq.3-13)$$

（３）証明

（ステップ１）Gのi行目とj行目を入れ替えて標準形G_1とする。そのために、i列目とj列目を入れ替える変換行列R_{ij}を右からかける。

$$G_1 = GR_{ij} = [\, I_k \mid A \,] \qquad (eq.3-13)$$

R_{ij}は、$k \times k$の正則行列であり、対称行列でもある。従って、以下が成立する。

$$R_{ij} = R_{ji} = \left(R_{ij}\right)^T = {R_{ij}}^{-1} \qquad (eq.3-14)$$

$$R_{ij}R_{ij} = I_k \qquad (eq.3-15)$$

また、eq. 3-13 より、以下を得る。

$$G = G_1\left(R_{ij}\right)^{-1} \qquad (eq.3-16)$$

（ステップ２）G_1に対する検査行列H_1を求める。

$$H_1 = [\, A^T \mid I_m \,] \quad (eq.3-17)$$

（ステップ３）G_1と${H_1}^T$の積を求める。

$$G_1{H_1}^T = [\, I_k \mid A \,] \begin{bmatrix} A \\ - \\ I_m \end{bmatrix} = 0 \quad (eq.3-18)$$

（ステップ４）H_1　のj列目とi列目を入れ替えた生成行列をH_xとする。

$$H_x = H_1 R_{ji} \qquad (eq.3-19)$$

（ステップ５）$GH_x{}^T$を計算すると、

$$GH_x{}^T = G_1(R_{ij})^{-1} H_x{}^T = G_1(R_{ij})^{-1}[H_1 R_{ij}]^T = G_1(R_{ij})^{-1}[R_{ij}]^T H_1{}^T = G_1 R_{ij} R_{ij} H_1{}^T = G_1 H_1{}^T = 0$$

となり、H_xは、Gの検査行列である。

上記は、１回のR_{ij}で標準形に変形可能な場合である。複数回で行う場合も同様に示すことができる。

方法４　行基本変形による方法

検査行列G　（$k \times n$行列）が得られている場合に、生成行列H　（$m \times n$行列）を求めたい。($k = n - m$)このとき、生成行列Gの行を行基本変形して標準形とし、検査行列Hを求める。

（ステップ１）Gのi行目とj行目を行基本変形して標準形G_1にできたとする。そのための変換行列L_{ij}を左からかける。

$$G_1 = L_{ij} G = [\, I_k \mid A \,] \qquad (eq.3-20)$$

L_{ij}は、$k \times k$の正則行列であり、対称行列である。

（ステップ２）H_1を求める。

$$H_1 = [\, A^T \mid I_m \,] \qquad (eq.3-21)$$

（ステップ３）G_1と$H_1{}^T$の積を求める。

$$G_1 H_1{}^T = [\, I_k \mid A \,] \begin{bmatrix} A \\ - \\ I_m \end{bmatrix} = 0 \qquad (eq.3-22)$$

（ステップ４）この時、

$$G_1 H_1{}^T = (L_{ij} G) H_1{}^T = 0 \qquad (eq.3-23)$$

であり、この式に$(L_{ij})^{-1}$を左からかけると

$$(L_{ij})^{-1}(L_{ij} G) H_1{}^T = G H_1{}^T = 0 \qquad (eq.3-24)$$

すなわち、H_1は、Gの検査行列である。

３．（課題２の解答）

ハミング(n,k)符号は、必ず2^i $(i = 0,,,m-1,\ m = n-k)$ となる列が存在するため、列交換によって必ず標準形にすることが可能である。従って、常に列交換による方法が適用可能である。

３．（課題３の解答）

全符号語

111000　010110　110101　101110　001101　100011　011011　000000

最小距離は３，従ってこの(6,3)符号は１誤り訂正可能である。

ちなみに、この(6,3)符号の効率は、3/6=0.5 である。一方同じ１誤り訂正可能なハミング(7,4)符号の効率は、4/7=0.57 であり、ハミング(7,4)の方が効率がよい。

３．（課題４の解答）

ステップ１）ガウスージョルダン消去法を用いてHの Reduced Row Echelon Form を求める。

$$H=\begin{pmatrix}0&0&0&0&0&0&0&0&0\\1&0&1&1&0&1&0&0&1\\0&1&1&0&0&1&1&1&1\\1&0&0&0&1&1&1&1&1\\1&1&0&1&0&0&1&1&0\\0&0&1&1&1&0&1&1&0\\1&0&0&0&1&1&1&1&1\\1&1&0&1&1&1&1&0&0\end{pmatrix}\sim\begin{pmatrix}1&0&0&0&0&0&1&0&1\\0&1&0&1&0&0&0&1&1\\0&0&1&1&0&1&1&0&0\\0&0&0&0&1&1&0&1&0\\0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0\end{pmatrix}\qquad(eq.3-2)$$

この確認は、例えば以下を使う。

Matrix Row Reducer https://www.mathdetail.com/matrix.php

ステップ２）$Hx=0$の連立方程式に戻して考える。

$$Hx=\begin{pmatrix}1&0&0&0&0&0&1&0&1\\0&1&0&1&0&0&0&1&1\\0&0&1&1&0&1&1&0&0\\0&0&0&0&1&1&0&1&0\\0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\x_5\\x_6\\x_7\\x_8\\x_9\end{pmatrix}=0$$

leading entry に対応するx_1，x_2，x_3，x_5以外のxの要素、すなわち、x_4，x_6，x_7，x_8，x_9を自由変数（free variable）とし、以下のように変形する。（太文字の 5 行を追加）

$$\begin{pmatrix}1&0&0&0&0&0&1&0&1\\0&1&0&1&0&0&0&1&1\\0&0&1&1&0&1&1&0&0\\\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}\\0&0&0&0&1&1&0&1&0\\\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}\\\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}\\\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}\\\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\x_5\\x_6\\x_7\\x_8\\x_9\end{pmatrix}=\begin{pmatrix}0\\0\\0\\x_4\\0\\x_6\\x_7\\x_8\\x_9\end{pmatrix}$$

$$\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\x_5\\x_6\\x_7\\x_8\\x_9\end{pmatrix}=\begin{pmatrix}0&0&-1&0&-1\\-1&0&0&-1&-1\\-1&-1&-1&0&0\\1&0&0&0&0\\0&-1&0&-1&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}\begin{pmatrix}x_4\\x_6\\x_7\\x_8\\x_9\end{pmatrix}=\begin{pmatrix}0&0&1&0&1\\1&0&0&1&1\\1&1&1&0&0\\1&0&0&0&0\\0&1&0&1&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}\begin{pmatrix}x_4\\x_6\\x_7\\x_8\\x_9\end{pmatrix}$$

$$\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\x_5\\x_6\\x_7\\x_8\\x_9\end{pmatrix}=\begin{pmatrix}0\\1\\1\\1\\0\\0\\0\\0\\0\end{pmatrix}x_4+\begin{pmatrix}0\\0\\1\\0\\1\\1\\0\\0\\0\end{pmatrix}x_6+\begin{pmatrix}1\\0\\1\\0\\0\\0\\1\\0\\0\end{pmatrix}x_7+\begin{pmatrix}0\\1\\0\\0\\1\\0\\0\\1\\0\end{pmatrix}x_8+\begin{pmatrix}1\\1\\0\\0\\0\\0\\0\\0\\1\end{pmatrix}x_9$$

これにより、$Hx=0$ となるxの集合（零空間）に属す任意のベクトル$(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_9)$は、(011100000) (001011000) (101000100) (010010010) (110000001)の

線形結合で表現されることがわかる。

また、$(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9) = 0$となる必要十分条件は、$x_4, x_6, x_7, x_8, x_9$がすべて 0 であることである。従って、(011100000) (001011000) (101000100) (010010010) (110000001)は、一次独立である。

以上より、(011100000) (001011000) (101000100) (010010010) (110000001)は、基底ベクトルである。零空間の基底ベクトルであるのでこれらが零空間の基底である。（なお、これらの基底ベクトルは直交していない。）

$HG^T = 0$であるので、GはHの零空間基底ベクトルを並べた行列となる。

$$G = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad (eq.3-3)$$

$n - \mathrm{rank}\, H$ ＝ 零空間の次元（free variable の数）である。この例では、H のランクは 4，零空間の次元は 5 であり、9-4=5 である。

なお、この例は、第 7 章 Goppa 符号例 4 の Goppa(9, 5, 3)である。

原始多項式 $x^4 + x + 1$

ゴッパ集合L　$L \subseteq GF(2^4)$ $L = \{\alpha^i \; such \; that \; 1 \le i \le 9\} = \{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9\}$

ゴッパ多項式$g(z) = z^2 - 1$（non separable）　最小距離 $d \ge t + 1 = 2 + 1 = 3$ ）

$$H = \begin{pmatrix} \alpha^8 & \alpha^1 & \alpha^5 & \alpha^2 & \alpha^0 & \alpha^{10} & \alpha^4 & \alpha^4 & \alpha^{10} \\ \alpha^7 & \alpha^{14} & \alpha^2 & \alpha^{13} & \alpha^{10} & \alpha^4 & \alpha^{12} & \alpha^{11} & \alpha^1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

（参考；行列のカーネルの性質と求め方　美しい物語 https://mathtrain.jp/kernel）

https://study-guide.hatenablog.jp/entry/20150307/p1

Null space calculator https://www.mathdetail.com/null.php

Linear Algebra Tool Kit http://www.math.odu.edu/~bogacki/cgi-bin/lat.cgi?c=null

---GF(3)の例

$$H = \begin{pmatrix} 0 & 2 & 1 & 2 & 0 \\ 2 & 1 & 1 & 0 & 0 \\ 2 & 2 & 0 & 1 & 1 \end{pmatrix} \qquad (eq.gf3-1)$$

$$H = \begin{pmatrix} 0 & 2 & 1 & 2 & 0 \\ 2 & 1 & 1 & 0 & 0 \\ 2 & 2 & 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 2 & 2 & 0 & 1 & 1 \\ 2 & 1 & 1 & 0 & 0 \\ 0 & 2 & 1 & 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 2 & 0 & 1 & 1 \\ 0 & -1 & 1 & -1 & -1 \\ 0 & 2 & 1 & 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & -1 & -1 & 1 \\ 0 & 2 & 1 & 2 & 2 \\ 0 & 2 & 1 & 2 & 0 \end{pmatrix}$$

$$\sim \begin{pmatrix} 2 & 0 & 2 & 2 & 1 \\ 0 & 2 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & -2 \end{pmatrix} \sim \begin{pmatrix} 4 & 0 & 4 & 4 & 2 \\ 0 & 4 & 2 & 4 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 & 1 & 2 \\ 0 & 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} \mathbf{1} & 0 & 1 & 1 & 0 \\ 0 & \mathbf{1} & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} \end{pmatrix} \quad (eq.gf3-2)$$

1<->3、2-1->2、1-3->1、 3-2->3、1x2->1 2x2->2、1-3x2->1 2-3->2

$$Hx = \begin{pmatrix} \mathbf{1} & 0 & 1 & 1 & 0 \\ 0 & \mathbf{1} & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = 0 \qquad (eq.gf3-3)$$

$$\begin{pmatrix} \mathbf{1} & 0 & 1 & 1 & 0 \\ 0 & \mathbf{1} & 2 & 1 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ 0 & 0 & 0 & 0 & \mathbf{1} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ x_3 \\ x_4 \\ 0 \end{pmatrix} \qquad (eq.gf3-4)$$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ -2 & -1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 1 & 2 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x_3 \\ x_4 \end{pmatrix} \qquad (eq.gf3-5)$$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} x_3 + \begin{pmatrix} 2 \\ 2 \\ 0 \\ 1 \\ 0 \end{pmatrix} x_4 \qquad (eq.gf3-6)$$

$$Null(H) = span\left(\begin{pmatrix} 2 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 0 \\ 1 \\ 0 \end{pmatrix} \right) \qquad (eq.gf3-7)$$

$$G = \begin{pmatrix} 2 & 1 & 1 & 0 & 0 \\ 2 & 2 & 0 & 1 & 0 \end{pmatrix} \qquad (eq.gf3-8)$$

———別解

$$H \sim \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad (eq.gf3-9)$$

$$H_{35} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} = [\, I_3 \mid A \,] \quad (eq.gf3-10)$$

$$G_{35} = [\, -A^T \mid I_2 \,] = \begin{pmatrix} -1 & -1 & 0 & 1 & 0 \\ -1 & -2 & 0 & 0 & 1 \end{pmatrix} \quad (eq.gf3-11)$$

$$G = \begin{pmatrix} -1 & -1 & 0 & 1 & 0 \\ -1 & -2 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 0 & 1 & 0 \\ 2 & 1 & 1 & 0 & 0 \end{pmatrix} \quad (eq.gf3-12)$$

———

$$G_{35} = [\, -A^T : I_2 \,] = \begin{pmatrix} -1 & -1 & 0 & 1 & 0 \\ -1 & -2 & 0 & 0 & 1 \end{pmatrix} \quad (eq.gf3-11)$$

[]中の | が絶対値記号と認識されていて、行形式にした後、２次元形式に戻せない。

$$= [\, I_3 \mid A \,] \quad (eq.2-23)$$

情報通信基礎Ⅰ　第５章　島田 p113

情シス　渡辺

問 5.8 コセット

u_1	u_2	u_3	u_4	$\cdots$	u_x
g_1+u_1	g_1+u_2	g_1+u_3	g_1+u_4	$\cdots$	g_1+u_x
g_2+u_1	g_2+u_2	g_2+u_3	g_2+u_4	$\cdots$	g_2+u_x
		$\vdots$			
g_y+u_1	g_y+u_2	g_y+u_3	g_y+u_4	$\cdots$	g_y+u_x

一行がコセット

↑コセットリーダ

サイズxy の行列

(1) i 番目のコセットに関してシンドロームを計算する。

$s_i = v_i H^T = (g_i + u_i)H^T = g_i H^T + u_i H^T = g_i H^T$

これはコセット内のすべてのv_iに対して成立する。

(2)

0000000 0000111 0011001 0011110 0101010 0101101 0110011 0110100　1001011 1001100 1010010 1010101 1100001 1100110 1111000 1111111　$s_1 = 000$

0000001 0000110 0011000　$s_2 = 001$

:

1000000 1000111 1011001　$s_8 = 111$

8x16=128　$2^7 = 128$ よってこれで 7 次元ベクトル空間をすべて網羅している。

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

$$s_2 = (0000001)H^T = (0000001)\begin{pmatrix}1&1&1&1&0&0&0\\1&1&0&0&1&1&0\\1&0&1&0&1&0&1\end{pmatrix}^T = \begin{pmatrix}0\\0\\1\end{pmatrix} \qquad s_3 = (0000010)H^T = (0000010)\begin{pmatrix}1&1&1&1&0&0&0\\1&1&0&0&1&1&0\\1&0&1&0&1&0&1\end{pmatrix}^T = \begin{pmatrix}0\\1\\0\end{pmatrix}$$

$$s_4 = (0000100)H^T = (0000100)\begin{pmatrix}1&1&1&1&0&0&0\\1&1&0&0&1&1&0\\1&0&1&0&1&0&1\end{pmatrix}^T = \begin{pmatrix}0\\1\\1\end{pmatrix} \qquad s_5 = (0001000)H^T = (0001000)\begin{pmatrix}1&1&1&1&0&0&0\\1&1&0&0&1&1&0\\1&0&1&0&1&0&1\end{pmatrix}^T = \begin{pmatrix}1\\0\\0\end{pmatrix}$$

$$s_6 = (0010000)H^T = (0010000)\begin{pmatrix}1&1&1&1&0&0&0\\1&1&0&0&1&1&0\\1&0&1&0&1&0&1\end{pmatrix}^T = \begin{pmatrix}1\\0\\1\end{pmatrix} \qquad s_7 = (0100000)H^T = (0100000)\begin{pmatrix}1&1&1&1&0&0&0\\1&1&0&0&1&1&0\\1&0&1&0&1&0&1\end{pmatrix}^T = \begin{pmatrix}1\\1\\0\end{pmatrix}$$

$$s_8 = (1000000)H^T = (1000000)\begin{pmatrix}1&1&1&1&0&0&0\\1&1&0&0&1&1&0\\1&0&1&0&1&0&1\end{pmatrix}^T = \begin{pmatrix}1\\1\\1\end{pmatrix}$$

(3)

$$s = vH^T = (0111001)H^T = (0111001)\begin{pmatrix}1&1&1&1&0&0&0\\1&1&0&0&1&1&0\\1&0&1&0&1&0&1\end{pmatrix}^T = \begin{pmatrix}1\\1\\0\end{pmatrix} + \begin{pmatrix}1\\0\\1\end{pmatrix} + \begin{pmatrix}1\\0\\0\end{pmatrix} + \begin{pmatrix}0\\0\\1\end{pmatrix} = \begin{pmatrix}1\\1\\0\end{pmatrix} = s_7$$

$u = v - g_7 = (0111001) - (0100000) = (0011001)$

記号交差

情シス　渡辺

・バースト誤り訂正のための記号交差を考える。
・例えば、１誤り訂正可能な(n, k)符号を i 個組合わせた(ni, ki)符号はバースト長 i の誤り訂正が可能である。

例１　$g(x) = x^2 + x + 1$　で生成される(3, 1)符号　を　２つ交差させて(6, 2)符号を作る。(6, 2)符号の生成多項式を求めよ。

２つの(3, 1)符号を
$a_3x^2 + a_2x^1 + a_1$　　$b_3x^2 + b_2x^1 + b_1$　とすると、２交差の(6, 2)符号は、
$a_3x^5 + b_3x^4 + a_2x^3 + b_2x^2 + a_1x^1 + b_1$　と表現される。

$a_3x^2 + a_2x^1 + a_1 = g(x)A(x)$
$b_3x^2 + b_2x^1 + b_1 = g(x)B(x)$　であるから、

$$\begin{aligned} a_3x^5 \quad &+a_2x^3 \quad &+a_1x^1 \quad &= xg(x^2)A(x) \\ b_3x^4 \quad &+b_2x^2 \quad &+b_1 \quad &= g(x^2)B(x) \end{aligned}$$

両辺を加算する。
$a_3x^5 + b_3x^4 + a_2x^3 + b_2x^2 + a_1x^1 + b_1 = g(x^2)\{xA(x) + B(x)\}$

よって、(6,2)符号は、x^2で整除される。従って、生成多項式は、
$g2(x) = g(x^2) = x^4 + x^2 + 1$　である。

例２　$g(x) = x^3 + x + 1$　で生成される(7, 4)符号　を　２つ交差させて(14, 8)符号を作る。(14, 8)符号の生成多項式を求めよ。
２つの(7, 4)符号を
$a_7x^6 + a_6x^5 + a_5x^4 + a_4x^3 + a_3x^2 + a_2x^1 + a_1 = g(x)A(x)$
$b_7x^6 + b_6x^5 + b_5x^4 + b_4x^3 + b_3x^2 + b_2x^1 + b_1 = g(x)B(x)$
(14, 8)符号は、
$a_7x^{13} + b_7x^{12} + a_6x^{11} + b_6x^{10} + a_5x^9 + b_5x^8 + a_4x^7 + b_4x^6 + a_3x^5 + b_3x^4 + a_2x^3 + +b_2x^2 + a_1x^1 + b_1 = g(x^2)\{xA(x) + B(x)\}$
よって、(14, 8)符号は、x^2で整除される。従って、生成多項式は、
$g2(x) = g(x^2) = x^6 + x^2 + 1$　である。

例３　問 5.12 $g(x) = x^3 + x^2 + 1$ で生成される(7, 4)符号　を　３つ交差させて(21, 12)符号を作る。(21, 12)符号の生成多項式を求めよ。

問１，問２と同様に、(21, 12)符号は、x^3で整除される。従って、生成多項式は、

$g2(x) = g(x^3) = x^9 + x^6 + 1$　である。

情報通信基礎Ⅰ　第５章（一部６章）　レポート課題

問１）以下の行列H_1～H_5を検査行列とする符号C_1～C_5を考える。

$$H_1 = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

$$H_2 = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

$$H_3 = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

$$H_4 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

$$H_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

（１）C_1～C_5のそれぞれについて、①生成行列G_1～G_5、②全符号語、③最小距離d_{min1}～d_{min5}、④効率η_1～η_5を求めよ。生成行列は、検査行列Hの零空間を求める方法で計算せよ。零空間は、H_1に関しては手作業で求めよ。他は null space calculator 等のツールを用いてもよい。（GF(2)上の計算であることに注意せよ。）また、効率ηは、情報ビット数／符号長　と定義する。

（２）（１）の結果から、どのような状況でどの符号が適切かを議論せよ。

問２）検査行列を以下とする。

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

~~（１）Hの零空間を求め、生成行列Gを求めよ。~~

~~（２）生成行列Gで生成される符号語をすべて書き出せ。~~

~~（３）この符号の最小距離を求めよ。~~

~~（４）この符号の誤り訂正能力を求めよ。~~

（５）Hを行基本変形して、以下を得た。（2 行目に 1 行目の-1 倍を加算し、3 行目に 1 行目の-1 倍を加算する）

$$H_1 = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} = [\, A \mid I_3 \,]$$

I_3は3×3の単位行列である。この時、行列Zを$Z = [\, I_3 \mid A^T \,]$　とする。Zは、元のHの生成行列となるかを議論せよ。なぜそうなるかの理由も考えよ。ヒント：i行目にj行目の-1 倍を加算する変換行列をL_{ij}とすれば、$H_1 = L_{31}L_{21}H$　である。

問３）ハミング符号に関する以下の問に答えよ。

（１）検査ビット数を４とするハミング符号の検査行列H_4を求めよ。

（２）H_4を検査行列とする符号の生成行列G_4を求めよ。

（３）求めた符号が巡回符号であるかを調べるにはどうしたらよいか。（第６章の内容）

以下没問題

問３）生成行列H_1と生成行列H_2を考える。それぞれに対応する符号をそれぞれC_1，C_2とする。

$$H_1 = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \qquad H_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

１）H_2の生成行列を求めよ。

２）C_1とC_2の符号化率を比べて、どちらの符号がよいかを議論せよ。

問３）生成行列が以下で与えられた。

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

１）検査行列Hを求めよ。

２）この符号が巡回符号であるかを調べよ。（第６章の内容）

問２）検査行列を以下とする。

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

この生成行列を求めよ。

解答

問１）以下の行列H_1～H_5を検査行列とする符号C_1～C_5を考える。

$$H_1=\begin{pmatrix}0&0&1&1&0\\0&1&1&1&1\\1&0&0&1&1\end{pmatrix}$$
$$H_2=\begin{pmatrix}0&1&1&1&0\\0&1&1&1&0\\1&0&0&1&1\end{pmatrix}$$
$$H_3=\begin{pmatrix}0&0&1&1&0\\0&1&1&1&1\\0&0&0&1&1\end{pmatrix}$$
$$H_4=\begin{pmatrix}0&1&1&0\\1&1&1&1\\0&0&1&1\end{pmatrix}$$
$$H_5=(1\quad 1\quad 1\quad 1\quad 1)$$

（１）C_1～C_5のそれぞれについて、①生成行列G_1～G_5、②全符号語、③最小距離d_{min1}～d_{min5}、④効率η_1～η_5を求めよ。生成行列は、検査行列Hの零空間を求める方法で計算せよ。零空間は、H_1に関しては手作業で求めよ。他は null space calculator 等のツールを用いてもよい。（GF(2)上の計算であることに注意せよ。）また、効率ηは、情報ビット数／符号長　と定義する。

（２）（１）の結果から、どのような状況でどの符号が適切かを議論せよ。

問１）

（１）

==========H1

$$H_1=\begin{pmatrix}0&0&1&1&0\\0&1&1&1&1\\1&0&0&1&1\end{pmatrix}\sim\begin{pmatrix}1&0&0&1&1\\0&1&1&1&1\\0&0&1&1&0\end{pmatrix}\sim\begin{pmatrix}1&0&0&1&1\\0&1&0&0&1\\0&0&1&1&0\end{pmatrix}$$

1<->3　　2-3->2

$$Hx=\begin{pmatrix}1&0&0&1&1\\0&1&0&0&1\\0&0&1&1&0\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\x_5\end{pmatrix}=0$$

$$\begin{pmatrix}\mathbf{1}&0&0&1&1\\0&\mathbf{1}&0&0&1\\0&0&\mathbf{1}&1&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\x_5\end{pmatrix}=\begin{pmatrix}0\\0\\0\\x_4\\x_5\end{pmatrix}$$

①$G_1=\begin{pmatrix}1&0&1&1&0\\1&1&0&0&1\end{pmatrix}$

③$d_{min}=3$

②全符号語　４語　10110　11001　01111　00000

④効率$\eta=\frac{2}{5}=0.4$

==========H2

$$H_2=\begin{pmatrix}0&1&1&1&0\\0&1&1&1&0\\1&0&0&1&1\end{pmatrix}\sim\begin{pmatrix}0&1&1&1&0\\0&0&0&0&0\\1&0&0&1&1\end{pmatrix}\sim\begin{pmatrix}1&0&0&1&1\\0&1&1&1&0\\0&0&0&0&0\end{pmatrix}$$

1-2->2　　2<->3, 1<->2

$$Hx = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = 0$$

Hの最後の行は意味がないので削除する。

$$\begin{pmatrix} \mathbf{1} & 0 & 0 & 1 & 1 \\ 0 & \mathbf{1} & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix}$$

①$G_2 = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$

③$d_{min} = 2$

②全符号語　8語　01100　11010　10001　10110　11101　01011　00111　00000

④効率$\eta = \frac{3}{5} = 0.6$

==========H3

$$H_3 = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

1<->2　　1-2->1　　2-3->2

$$Hx = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = 0$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 1 \\ 0 & 0 & \mathbf{1} & 0 & 1 \\ 0 & 0 & 0 & \mathbf{1} & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} x_1 \\ 0 \\ 0 \\ 0 \\ x_5 \end{pmatrix}$$

①$G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix}$

③$d_{min} = 1$

②全符号語　4語　10000　01111　11111　00000

④効率$\eta = \frac{2}{5} = 0.4$

==========H4

$$H_4 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

1<->2　　1-2->1　　2-3->2

$$Hx = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = 0$$

$$\begin{pmatrix} \mathbf{1} & 0 & 0 & 1 \\ 0 & \mathbf{1} & 0 & 1 \\ 0 & 0 & \mathbf{1} & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ x_4 \end{pmatrix}$$

①$G_4 = (1 \quad 1 \quad 1 \quad 1)$

③$d_{min} = 4$

②全符号語　2 語　1111　0000

④効率$\eta = \frac{1}{4} = 0.25$

==========H5

$$H_5 = (1 \quad 1 \quad 1 \quad 1 \quad 1)$$

$$Hx = (1 \quad 1 \quad 1 \quad 1 \quad 1) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = 0$$

$$\begin{pmatrix} \mathbf{1} & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix}$$

①$G_5 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$

③$d_{min} = 2$

②全符号語　１６語

11000　10100　10010　10001　01100　01010　01001　00110

00101　00011　11101　11011　10111　11101　01111　00000

④効率$\eta = \frac{4}{5} = 0.8$

（２）効率だけを考えると、C5 すなわちパリティ符号がよい。

誤り訂正能力を考えると、C1 や C4 がよい。ただし、C4 は効率が低い。

C3 は誤り検出能力がない。（１ビット目を全くチェックしない。つまり、1 ビット目が誤ると他の符号となり訂正はできない）これらを踏まえて、妥当な考察の一つを以下に述べる。

　誤り率が高い伝送路で FEC を行うのであれば、C1 がよい。ARQ など検出だけを行うのであれば C5 がよい。誤り率が小さい場合は C5 がよい。C2, C3 を選択する理由はない。

（実際の判断は、実装等の別要因も勘案して行われるであろう）

発展：C3 で 11000 を受信したときを考える。

全符号語　10000　01111　11111　00000　との距離は、それぞれ 1，4，3，2 となり、10000 に復号で

きる。最小距離１であっても、受信語によっては復号できる。すなわち、最小距離はどんな受信語がきても復号できる能力を意味しているのに対し、個別の語については復号できる場合がある。

10000　-----4------　11111

　:1　　5/　¥5　　:1

00000　-----4------　01111

==========H6　BCH(5,1)

$$H_6 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

H_6

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

2-1<->2　　3-1->3　　4-1->4　　2+3->3

$$\sim \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

2+4<->4　　3+4->4　　3+4->3　　2+3->2　　1+2->1

$$Hx = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = 0$$

$$\begin{pmatrix} \mathbf{1} & 0 & 0 & 0 & 1 \\ 0 & \mathbf{1} & 0 & 0 & 1 \\ 0 & 0 & \mathbf{1} & 0 & 1 \\ 0 & 0 & 0 & \mathbf{1} & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ x_5 \end{pmatrix}$$

①$G_5 = (1 \quad 1 \quad 1 \quad 1 \quad 1)$

③$d_{min} = 5$

②全符号語　２語

　　11111　00000

④効率$\eta = \frac{1}{5} = 0.2$

n=5 の符号の中で、dmin が最大。一方効率は最小。

これは、BCH(5, 1)符号である。G_5、H_5と対比できる。

$x^5 + 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1)$、生成多項式　$g(x) = x^4 + x^3 + x^2 + x + 1$

だが、trivial な符号

==========H7

$$H_7=\begin{pmatrix}1&1&1&1&0\\1&1&1&0&1\\1&0&0&1&1\end{pmatrix}\sim\begin{pmatrix}1&1&1&1&0\\0&0&0&1&1\\1&0&0&1&1\end{pmatrix}\sim\begin{pmatrix}1&1&1&1&0\\0&0&0&1&1\\0&1&1&0&1\end{pmatrix}\sim\begin{pmatrix}1&1&1&1&0\\0&1&1&0&1\\0&0&0&1&1\end{pmatrix}$$
$$\sim\begin{pmatrix}1&1&1&1&0\\0&1&1&0&1\\0&0&0&1&1\end{pmatrix}\sim\begin{pmatrix}1&1&1&1&0\\0&1&1&0&1\\0&0&0&1&1\end{pmatrix}\sim\begin{pmatrix}1&1&1&0&1\\0&1&1&0&1\\0&0&0&1&1\end{pmatrix}\sim\begin{pmatrix}1&0&0&0&0\\0&1&1&0&1\\0&0&0&1&1\end{pmatrix}$$

$$Hx=\begin{pmatrix}1&0&0&0&0\\0&1&1&0&1\\0&0&0&1&1\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\x_5\end{pmatrix}=0$$

$$\begin{pmatrix}1&0&0&0&0\\0&1&1&0&1\\0&0&1&0&0\\0&0&0&1&1\\0&0&0&0&1\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\x_5\end{pmatrix}=\begin{pmatrix}0\\0\\x_3\\0\\x_5\end{pmatrix}$$

①$G_7=\begin{pmatrix}0&1&1&0&0\\0&1&0&1&1\end{pmatrix}$

③$d_{min}=2$

②全符号語　４語　01100　01011　00111　00000

１ビット目は常に０。

④効率$\eta=\frac{2}{5}=0.4$　１ビット目を落とせば$\eta=\frac{2}{4}=0.5$

問２）検査行列を以下とする。

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

~~（１）Hの零空間を求め、生成行列Gを求めよ。~~

~~（２）生成行列Gで生成される符号語をすべて書き出せ。~~

~~（３）この符号の最小距離を求めよ。~~

~~（４）この符号の誤り訂正能力を求めよ。~~

（５）Hを行基本変形して、以下を得た。（2 行目に 1 行目の-1 倍を加算し、3 行目に 1 行目の-1 倍を加算する）

$$H_1=\begin{pmatrix}0&1&1&1&0&0\\1&0&1&0&1&0\\1&1&0&0&0&1\end{pmatrix}=[\,A\mid I_3\,]$$

I_3は3×3の単位行列である。この時、行列Zを$Z=[\,I_3\mid A^T\,]$　とする。Zは、元のHの生成行列となるかを議論せよ。なぜそうなるかの理由も考えよ。ヒント：i行目にj行目の-1 倍を加算する変換行列をL_{ij}とすれば、$H_1=L_{31}L_{21}H$　である。

（１）

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

途中で２が出てくるので２回行う必要あり。

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

（2）略　8語

（3）$d_{min} = 3$

（4）1誤り訂正可能

（5）まず、$ZH^T = 0$を確認する。

$$ZH^T = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}^T = 0$$

従って、Z は生成行列である。

H の 2 行目に 1 行目の-1 倍を加算する変換行列L_{21}、3 行目に 1 行目の-1 倍を加算する変換行列L_{31}は以下である。

$$L_{21} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad L_{31} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}$$

$$H_1 = L_{31}L_{21}H = [\, A \mid I_m \,]$$

$$Z = [\, I_k \mid A^T \,]$$

$${Z{H_1}^T} = [\, I_k \mid A^T \,] \begin{bmatrix} A^T \\ - \\ I_m \end{bmatrix} = 0$$

$$H = (L_{21})^{-1}(L_{31})^{-1}H_1$$

以上より、

$$ZH^T = Z[(L_{21})^{-1}(L_{31})^{-1}H_1]^T = {Z{H_1}^T}[(L_{21})^{-1}(L_{31})^{-1}]^T = 0$$

よって、ZはHの生成行列となる。

より一般的に、c_i倍のi行目をj行目に加算する変換を$L(i, c_i, j)$とすると以下のように表現できる。

$$L(i, c_i, j) = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & c_i & \cdots & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ i-th\ row \\ \\ j-th\ row \\ \\ \\ \end{matrix}$$

$$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad i-th\ col. \qquad j-th\ col.$$

$L(i, c_i, j)$は、正則であり、逆変換が存在する。

問題文中のL_{21}、L_{31}は以下である。

$$L_{21} = L(1, -1, 2) = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad L_{31} = L(1, -1, 3) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}$$

問3）ハミング符号に関する以下の問に答えよ。

（1）検査ビット数を4とするハミング符号の検査行列H_4を求めよ。

（2）H_4を検査行列とする符号の生成行列G_4を求めよ。

（3）求めた符号が巡回符号であるかを調べるにはどうしたらよいか。（第6章の内容）

（1）一つの構成法を示す。以降の解答は、各自の構成法に依って異なる。

$$H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

（2）ここでは列入替で生成行列を求める。

$$H_{34} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$H_{34,48} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$G_{34,48} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$G_{34} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$G_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

（3）いくつかの方法が考えられる。

・すべての符号語を列挙して確認する。

・Gの各行を多項式で表現し、共通因子を求める。それが$x^n + 1$を整除すれば巡回符号である。

上の例では、最も低い次数の最終行の多項式表現は、

$$u_{11} = (0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,1) = x^4 + x^3 + 1$$

であり、これは GF(2)上の規約多項式である。従って、この符号が巡回符号ならば、すべての行はu_{11}で整除されねばならない。
下から２行目は、

$$(0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0) = x^5 + x^3 + x = x(x^4 + x^2 + 1)$$

であり、u_{11}では割り切れない。よって巡回符号ではない。

一応、巡回も含めてu_{11}で割ると、

```
          543210987654321
11001     101010000000000
          11001
           11000
           11001
                10000
                11001
                 10010
                 11001
                  10110
                  11001
                   11110
                   11001
                     11100
                     11001
                       10100 <------
                       11001
                        11010
                        11001
                            11000
                            11001
                                  100000
```

となり、u_{11}で整除できない。

null space calculator で計算すると

$$H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

$Hx = 0$は、

$$Hx = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \end{pmatrix} = 0$$

$$G_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

情報通信基礎Ⅰ　第６章　誤り訂正符号２（符号の多項式表現、巡回符号）

情シス　渡辺

ポイント

・第５章は符号語をベクトルで扱った。ここでは多項式で扱う方法を学ぶ。

・生成多項式$g(x)$をどのように作ったらよいかが重要。

・巡回符号、ＢＣＨ符号、ＲＳ（リードソロモン）符号　応用としてＱＲコードなど

・多くの符号語の中である基準を満たす符号語だけを利用する（シャノンの第２定理）

第５章：全ビットを加算すると０（パリティ）、検査行列を掛けると０（ハミング等）

第６章：符号語や生成多項式等を多項式で表現する。

生成多項式$g(x)$で割り切れる符号語だけを使う。これは、$g(x)$の根と関係が深い。

符号語を$u(x)$とする。

$g(x)$で割り切れるとは、$u(x) = A(x) \cdot g(x)$　となることである。

ここで、$g(x)$の根αを考えると、$g(\alpha) = 0$。よって、$u(\alpha) = A(\alpha) \cdot g(\alpha) = 0$

すなわち、αは$u(x)$の根でもある。

「生成多項式$g(x)$で割り切れる符号語だけを使う」＝「生成多項式$g(x)$の根を持つ符号語$u(x)$を使う」

６．１　基礎

符号の分類　別紙　補足資料１前半

誤りの種類　ランダム誤り、バースト誤り

６．２　多項式表現

６．２．１　符号の多項式表現

符号長nの符号語　$u = (a_{n-1}\, a_{n-2} \cdots a_0)$　$a_i \in GF(2)$　を　$GF(2)$　上の多項式で表現する。（係数が０と１、演算・＋）

$$u(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0$$

例　（１１０１）　－＞　$x^3 + x^2 + 1$

$GF(2)$上の多項式の演算

$0 + 0 = 0$　$0 + 1 = 1 + 0 = 1$　$1 + 1 = 0$　$0 - 1 = 1$　$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$　$1 \cdot 1 = 1$

$$ax^i + bx^i = (a + b)x^i \qquad eg.\ x^5 + x^5 = 0$$

$$\frac{ax^i}{bx^j} = \frac{a}{b}x^{i-j} \quad b \neq 0 \qquad eg.\ \frac{x^5}{x^3} = x^2$$

$$f(x) + g(x) = h(x) \ \ -> \ \ f(x) = g(x) + h(x), \qquad g(x) = f(x) + h(x),\ f(x) + g(x) + h(x) = 0$$

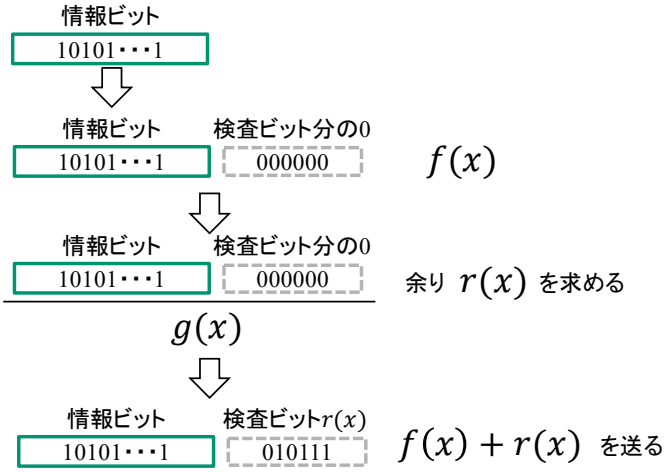
６．２．２　生成多項式

生成多項式$g(x)$：第５章の生成行列に相当するもの

６．２．３　送信・受信の手順

送信側では、検査ビットの初期値を０とし、

（情報ビット＋検査ビット）／生成多項式$g(x)$　の余り（剰余）を検査ビットとして加えて符号化する。



$g(x)$がm次とすると、$r(x)$は$m-1$次である。（つまり、検査ビット数はmビット）

$g(x)$で生成される符号は、(n,k)符号　$k=n-m$となる。

$n=7$、$k=4$の場合

情報ビット$(a_6\ a_5\ a_4\ a_3)$を　$a_6x^3+a_5x^2+a_4x+a_3$とする。次に、x^3をかけて、

$f(x)=a_6x^6+a_5x^5+a_4x^4+a_3x^3+0x^2+0x+0$　とし、

$f(x)$　を　$g(x)$で割った余り$r(x)$を求め、$f(x)+r(x)$　を符号語とする。つまり、

$f(x)=A(x)\cdot g(x)+r(x)$　　$f(x)+r(x)=A(x)\cdot g(x)$　となり、

$f(x)+r(x)$は、$g(x)$で割り切れる。（剰余が０、整除する、とも表現する）

受信側は、受信した符号語を生成多項式$g(x)$で割って余りが０になるかを調べる。

言い換えると、生成多項式$g(x)$で整除される符号語だけを用いていることになる。

例６．１　$g(x)=x^3+x^2+1=(1\,1\,0\,1)$は、$(7,4)$符号を生成する。（としよう）

１）送信側

今、情報ビット$x^3+x+1=(1\,0\,1\,1)$を送るとする。

$f(x)=(1\,0\,1\,1\,|\,0\,0\,0)=x^6+x^4+x^3$

$f(x)/g(x)$　を計算する。

【図６．１】　多項式の割り算

```
      1   1   0   0
    ---------------------
1101| 1   0   1   1   0   0   0
      1   1   0   1
    ---------------------
          1   1   0   0
          1   1   0   1
    ---------------------
              0   0   1   0
              0   0   0   0
    ---------------------
                  0   1   0   0
                  0   0   0   0
    ---------------------
                      1   0   0  <－ 重要
```

以上より、$r(x)=x^2=(1\,0\,0)$

よって、送信すべき符号語は、

$u(x)=f(x)+r(x)=x^6+x^4+x^3+x^2=(1\,0\,1\,1\,1\,0\,0)$

２）受信側

$v(x) = (1\,1\,1\,1\,1\,0\,0)$を受け取ったとする。

$v(x)/g(x)$ を計算する。

【図６．２】

```
                ---------------------------------
1101| 1   1   1   1   1   0   0
    | 1   1   0   1
    ---------------------------------
          0   1   0   1
              1   1   0   1
    ---------------------------------
                  1   1   1   0
                  1   1   0   1
    ---------------------------------
                      0   1   1
```

以上より、シンドロームは、

$s(x) = x + 1 \neq 0$

であり、少なくとも誤りがあることが分かる。

このシンドロームが全ての誤りパタンで異なれば、誤りを特定でき、訂正できる。

１誤りのパタンは７（符号長が７ビットだから）。３ビットでは８パタン表現可能。正しいものも含めて異なるパタンで特定できる可能性がある。（実際、$g(x) = x^3 + x^2 + 1$　は可能である。）

参考書等：

電子情報通信学会『知識の森』（http://www.ieice-hbkb.org/portal/doc_608.html/）１群（信号・システム）２編（符号理論）編主任　藤原融１章符号理論の基礎（鎌部、松嶋、鴻巣、高田）、２章代数的符号（藤原、常磐）

６．３　巡回符号

６．３．１　巡回符号

符号長nの符号Uのある符号語　$u = (a_{n-1}\, a_{n-2} \cdots a_0) \in U$　　（ただし$a_i \in GF(2)$）を考える。この符号語uを左に１ビットシフトした符号語u'は

$$u' = (a_{n-2}\, a_{n-3} \cdots a_0\, a_{n-1})$$

である。この語がやはり　U　に属すとき、すなわち $u' \in U$　の時、Uを巡回符号と呼ぶ。

巡回符号は、BCH, RS 等重要な符号の基礎となる。

６．３．２　巡回符号の生成多項式

$x^n + 1$を整除する多項式は、巡回符号の生成多項式となりうる。（全てではないことに注意）

$x^n + 1$を GF(2)上でそれ以上分解できないところまで、因数分解する。構成する各多項式を既約多項式と呼ぶ。

例６．２　$x^7 + 1 = (x + 1)(x^3 + x^2 + 1)(x^3 + x + 1)$

^^^^^^^^^ ^^^^^^^^

これらが、特に重要

```
        76543210
1101    1    ¥
        1101 ¥
         1010 ¥
         1101 ¥
          1110 ¥
          1101 ¥
            1100
            1101
               1
```

生成多項式$g(x) = x^3 + x^2 + 1$　は、$x^7 + 1$を整除する。確認－＞

$g(x) = x^3 + x^2 + 1$　は、$n = 7$、$m = 3$、$k = 4$の巡回(7, 4)符号を生成する。

情報ビットは、(0 0 0 0)~(1 1 1 1)であり、それぞれにx^3をかけた多項式を$g(x)$で割って余り$r(x)$を求める。（実際の計算は※参照）

	情報ビット	余り$r(x)$	符号語$u(x)$	巡回のパタン
0	0 0 0 0	0 0 0	0 0 0 0 0 0 0	p1
1	0 0 0 1	1 0 1	0 0 0 1 1 0 1	p2
2	0 0 1 0	1 1 1	0 0 1 0 1 1 1	p3
3	0 0 1 1	0 1 0	0 0 1 1 0 1 0	p2
4	0 1 0 0	0 1 1	0 1 0 0 0 1 1	p2
5	0 1 0 1	1 1 0	0 1 0 1 1 1 0	p3
6	0 1 1 0	1 0 0	0 1 1 0 1 0 0	p2
7	0 1 1 1	0 0 1	0 1 1 1 0 0 1	p3
8	1 0 0 0	1 1 0	1 0 0 0 1 1 0	p2
9	1 0 0 1	0 1 1	1 0 0 1 0 1 1	p3
10	1 0 1 0	0 0 1	1 0 1 0 0 0 1	p2
11	1 0 1 1	1 0 0	1 0 1 1 1 0 0	p3
12	1 1 0 0	1 0 1	1 1 0 0 1 0 1	p3
13	1 1 0 1	0 0 0	1 1 0 1 0 0 0	p2
14	1 1 1 0	0 1 0	1 1 1 0 0 1 0	p3
15	1 1 1 1	1 1 1	1 1 1 1 1 1 1	p4

※除算の例

```
1101 1000000     1101 1100000     1101 1010000     1101 1001000     1101 1110000     1101 1011000     1101 1101000
     1101             1101             1101             1101             1101             1101             1101
      101              001              111              100              011              110               000
     1101             0000             1101             1101             0000             1101
      111              010              011              101              110               100
     1101             0000             0000             1101             1101
      011              100              110              111              001
     0000             1101             1101             1101             0000
      110              101              001              011              010
```

全てを割り算で求めずに、いくつかを計算しそれらの線形結合で求めることもできる。例えば、6 の符号語は、2 と 4 の符号語の加算で求められる。

巡回符号Uが生成多項式$g(x)$で生成されるとする。ただし、$g(x)$は、x^n+1を整除する$GF(2)$上の多項式である。このとき、Uの任意の符号語uを左にkビットシフトした符号語$u^{(k)}$は、Uの符号語であることを示そう。

(1) $u(x)=a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots a_1x+a_0 \in U$ とする。

(2) $k=1$の時

$u^{(1)}=a_{n-2}x^{n-1}+\cdots+a_1x^2+a_0x+a_{n-1}$

$=(a_{n-1}x^{n-1}+\cdots+a_1x+a_0)x+a_{n-1}+a_{n-1}x^n=u(x)x+a_{n-1}(1+x^n)=g(x)\cdot A(x)$

$u(x)$は$g(x)$で整除可、$(1+x^n)$は$g(x)$で整除可

よって、$u^{(1)} \in U$

(3) $k=l(l \geq 1)$で成立すると仮定する。すなわち、 $u^{(l)}=g(x)A(x) \in U$ とすれば、

$u^{(l+1)}=xu^{(l)}+a_{n-l}(1+x^n)=g(x)B(x)$

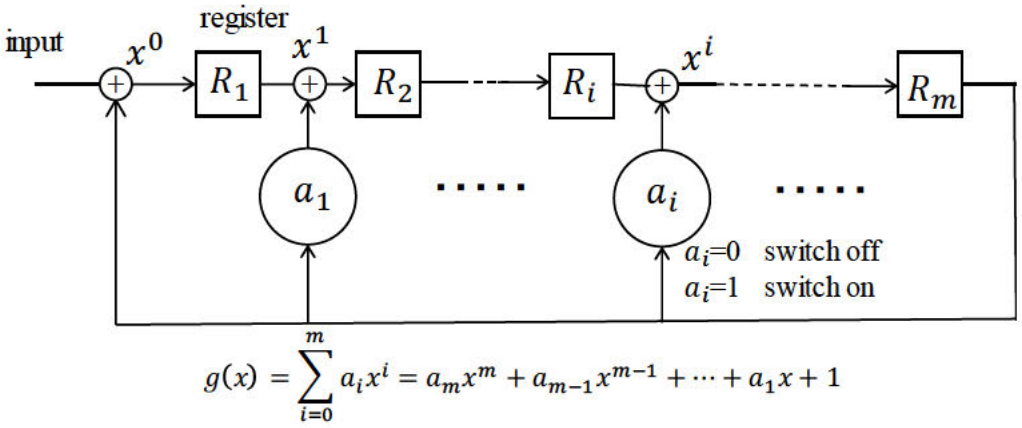
よって、$u^{(l+1)} \in U$

(4)(2)(3)より証明された。

６．３．３　割り算回路

送信側も受信側も生成多項式$g(x)$での割り算を行う。割り算回路はシフトレジスタを用いれば容易にハードウエアで実現できる。

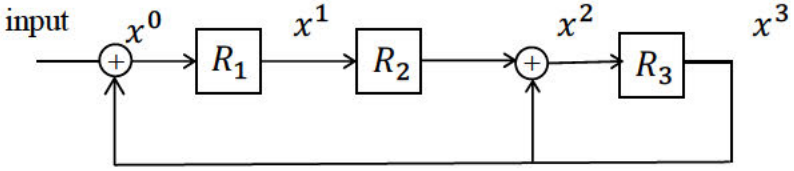
【図６．２】　割り算回路



$$g(x) = \sum_{i=0}^{m} a_i x^i = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + 1$$

例６．３　割り算回路の例

【図６．３】　割り算回路　$g(x) = x^3 + x^2 + 1$



レジスタの初期値を 000 とし、１００１０００が入力として与えられると、

入力	R1	R2	R3	
1	1	0	0	
0	0	1	0	
0	0	0	1	
1	0	0	1	＜－　下の［１］に相当
0	1	0	1	＜－　下の［２］に相当
0	1	1	1	＜－　下の［３」に相当
0	1	1	0	＜－　下の［４］に相当

従って、余りは(０１１)。よって(１００１０１１)を送信する。

確認のため、(１００１０００)を (１１０１)で割ると、

```
1101| 1   0   0   1   0   0   0
     1   1   0   1
    ---------------------------
        1   0   0   0           <－［1］
        1   1   0   1
    ---------------------------
            1   0   1   0       <－［2］
            1   1   0   1
    ---------------------------
                1   1   1   0           <－［3］
                1   1   0   1
    ---------------------------
                    0   1   1           <－［4］
```

となり、最終的なレジスタの内容と余りが一致している。

６．３．４　巡回符号の符号語の求め方、生成多項式と生成行列、検査行列

（１）巡回符号の符号語の求め方

方法としては

（A）情報符号語を生成多項式$g(x)$で割った余り$r(x)$を計算し求める方法

（B）$g(x)$から生成行列Gを求め、線形結合で求める方法

などがある。６．３．２で示したのは、Aの方法

（B）の方法を示す。

全ての符号語は、$u(x) = A(x) \cdot g(x)$　と表される。$g(x)$　の次数をm、生成される符号の符号長をnとする。

まず、$A(x) = 1$とした$u(x) = g(x)$は符号語であり、$g(x)$のベクトル表現（長さはn）をg_0とすると、g_0は生成行列の行となる。次に、$A(x) = x$とした$u(x) = xg(x)$も符号語であり、かつ$g(x)$とは一次独立である。また、$xg(x)$のベクトル表現g_1は、g_0を１ビット左シフトしたものである。g_1も生成行列の行となる。これを、$n-m-1$ビットシフトしたベクトルg_{n-m-1}まで繰り返すと以下のように生成行列が求められる。

$$G = \begin{pmatrix} g_{n-m-1} \\ g_{n-m-2} \\ \vdots \\ g_2 \\ g_1 \\ g_0 \end{pmatrix}$$

例として、生成多項式を$g(x) = x^3 + x^2 + 1$　とする。$n = 7$、$m = 3$、$g_0 = (0001101)$であるから生成行列は以下となる。

$$G = \begin{pmatrix} g_3 \\ g_2 \\ g_1 \\ g_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

g_0～g_3が一次独立であることは以下のように証明できる。

証明　$c_1x^3g(x) + c_2x^2g(x) + c_3xg(x) + c_41g(x) = 0$となるのは、$c_1 = c_2 = c_3 = c_4 = 0$のときであることを示せばよい。（見やすくするために転置して列ベクトルで考える）

$$c_1x^3g(x) + c_2x^2g(x) + c_3xg(x) + c_41g(x) = c_1(1\,1\,0\,1\,0\,0\,0)^T + c_2(0\,1\,1\,0\,1\,0\,0)^T + c_3(0\,0\,1\,1\,0\,1\,0)^T + c_4(0\,0\,0\,1\,1\,0\,1)^T$$

$$= \begin{pmatrix} c_1 & & & \\ c_1 & +c_2 & & \\ & c_2 & +c_3 & \\ c_1 & & +c_3 & +c_4 \\ & c_2 & & +c_4 \\ & & c_3 & \\ & & & c_4 \end{pmatrix} = 0$$

これより、$c_1 = c_2 = c_3 = c_4 = 0$。よって一次独立である。

扱いを簡単にするためにGを行列の基本変形で変形すると、

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

（わ；一行目＝①＋②＋③　　二行目＝②＋③＋④　　三行目＝③＋④　　四行目＝④）

これは既約梯陣形である。Ｇでも、Ｇ’でも同じ符号語ができる。

G'で生成されるすべての符号語を線形結合によって求める。

行の番号	線形結合	重み	パタン	
①	１０００１１０	3	1101	p1

②	0 1 0 0 0 1 1	3	1101	p1
③	0 0 1 0 1 1 1	4	10111	p2
④	0 0 0 1 1 0 1	3	1101	p1
①＋②	1 1 0 0 1 0 1	4	10111	p2
①＋③	1 0 1 0 0 0 1	3	1101	p1
①＋④	1 0 0 1 0 1 1	4	10111	p2
②＋③	0 1 1 0 1 0 0	3	1101	p1
②＋④	0 1 0 1 1 1 0	4	10111	p2
③＋④	0 0 1 1 0 1 0	3	1101	p1
①＋②＋③	1 1 1 0 0 1 0	4	10111	p2
①＋②＋④	1 1 0 1 0 0 0	3	1101	p1
①＋③＋④	1 0 1 1 1 0 0	4	10111	p2
②＋③＋④	0 1 1 1 0 0 1	4	10111	p2
①＋②＋③＋④	1 1 1 1 1 1 1	7	11111111	p3
①＋①	0 0 0 0 0 0 0	0	0000000	p4

以上１６個が符号語。p1 は７個、p2 は７個、p3 は１個、p4 は１個がそれぞれ巡回している。

別解　G'が巡回符号を生成することを前提とすれば、G'の一行目、二行目、四行目は同じ符号を巡回したものであり、従って、一行目と三行目の巡回を考えて求めてもよい。
また、Gでも同じ符号ができる。既約梯陣形G'の方が計算が容易である。

（２）生成多項式と生成行列、検査行列

例えば、符号語$(a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1)$を生成多項式$g(x) = x^3 + x^2 + 1 = (1101)$で割ることは、以下の計算をしていることとなる。（以下、7 とはa_7を、67 とは、$a_6 + a_7$を意味する。）

```
       7    67   567   456
     ----------------------------------------------
1101| 7    6    5     4     3     2     1
      7    7    0     7
           67   5     47
           67   67    0     67
                567   47    367
                567   567   0     567
                      456   367   2567
                      456   456   0     456
                            3457  2567  1456
```

よって余りは、$(a_3 + a_4 + a_5 + a_7)x^2 + (a_2 + a_5 + a_6 + a_7)x + (a_1 + a_4 + a_5 + a_6)$となる。
従って、シンドロームは

$$\begin{aligned} s_1 &= a_7 + a_5 + a_4 + a_3 \\ s_2 &= a_7 + a_6 + a_5 + a_2 \\ s_3 &= a_6 + a_5 + a_4 + a_1 \end{aligned}$$

で計算される。よって、検査行列は、以下となる。

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

これからGを求められる。

６．３．５　巡回ハミングと非巡回ハミング

別紙　補足資料１中盤

６．３．６　巡回ハミング符号から BCH 符号への拡張

（BCH 符号の後で読み返した方がより深く理解できる。）

参考文献　岩垂好裕　符号理論入門　昭晃堂 p.39-44　より

（１）巡回ハミング(7,4)符号

$x^7+1=(x+1)(x^3+x^2+1)(x^3+x+1)$を考える。

原始多項式を　$p(x)=x^3+x+1$とする。この根をαとすれば、$\alpha^3+\alpha+1=0$

$x^7+1=X(x)(x^3+x+1)$であるので、$\alpha^7+1=X(\alpha)p(\alpha)=0$

よって、$\alpha^7=1$　（$\alpha^7=1$　は、αは１の７乗根と言い換えられる。）

生成多項式を　$p(x)$と同じとする。

つまり、$g(x)=p(x)=x^3+x+1=(x+\alpha)(x+\alpha^2)(x+\alpha^4)$　わ；無理に因数分解する

生成多項式は、x^7+1を整除する。また３次であるので、符号長$n=7$、検査ビット数 3 の巡回ハミング(7, 4)符号を生成する。単一誤り訂正可能

（２）巡回ハミング(15,11)符号

$x^{15}+1=(x+1)(x^4+x^3+1)(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)$を考える。

原始多項式を　$p(x)=x^4+x+1$とする。

この根をαとすれば、$\alpha^4+\alpha+1=0$、$\alpha^{15}=1$　（αは１の１５乗根）

生成多項式　$g(x)=x^4+x+1=(x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8)$

生成多項式は、$x^{15}+1$を整除する。また４次であるので、符号長$n=15$、検査ビット数 4 の巡回ハミング(15, 11)符号を生成する。単一誤り訂正可能

（３）（２）巡回ハミング(15,11)符号を拡張して、2 誤り訂正可能になるようにしたい。

３－１）準備

(A) 符号語多項式$u(x)$は生成多項式$g(x)$で整除される。すなわち、$u(x)=X(x)g(x)$

従って、$g(x)$の根をαとすると、$u(\alpha)=X(\alpha)g(\alpha)$=0

すなわち、すべての符号語$u(x)$はαを根として持つ。

（別の表現：根αを持つ多項式で表現される符号語だけを使う。）

(B)GF(2)上の任意の多項式$p(x)$について、　$[p(x)]^2=p(x^2)$　（証明せよ）である。

$p(x)$の根をαとする（$p(\alpha)$=0）と、$[p(x)]^2|_{x=\alpha}=p(x^2)|_{x=\alpha}=0$より、

α^2も$p(x)$の根である。

３－２）巡回ハミング(15, 11)の生成多項式は、α^1、α^2、α^4、α^8を根に持つ。生成多項式$g(x)$がα^3も根として持つとどうなるか。持つと仮定しよう。

送信符号語$u(x)$ を送信し、i ビット目とj ビット目が誤って、$v(x)$ を受信したとする。

2 ビットの誤りは　$e(x)=x^i+x^j$　と表現できる。

送信符号語は、$u(x)=X(x)g(x)$

受信符号語は、$v(x)=u(x)+e(x)=X(x)g(x)+x^i+x^j$

受信符号語多項式に、αを代入する。準備(A)を考慮すると、以下のように変形できる。

$v(\alpha)=u(\alpha)+e(\alpha)=e(\alpha)=\alpha^i+\alpha^j=S_1$　　・・・（式１）

つぎに、$v(\alpha^3)$を計算すると、（＜－なぜ$v(\alpha^2)$を計算しないのか。$v(\alpha^2)$は役に立つか？）

$v(\alpha^3) = u(\alpha^3) + e(\alpha^3) = e(\alpha^3) = \alpha^{3i} + \alpha^{3j} = S_3$　（$v(\alpha^3)$をS_3とする。）

(式１)を変形して、${S_1}^2 = \alpha^{2i} + \alpha^{2j}$

一般に$a^3 + b^3 = (a+b)(a^2 + ab + b^2)$ であり、$a = \alpha^i$ 、$b = \alpha^j$　とおけば、

$$S_3 = \alpha^{3i} + \alpha^{3j} = (\alpha^i + \alpha^j)(\alpha^{2i} + \alpha^i\alpha^j + \alpha^{2j}) = (\alpha^i + \alpha^j)\{(\alpha^{2i} + \alpha^{2j}) + \alpha^i\alpha^j\}$$

$$= (\alpha^i + \alpha^j)\left\{(\alpha^i + \alpha^j)^2 + \alpha^i\alpha^j\right\} = S_1({S_1}^2 + \alpha^i\alpha^j)$$

よって、$\alpha^i\alpha^j = \frac{S_3}{S_1} + {S_1}^2$　・・・(式２)

（式１）と（式２）を連立方程式として解けば、α^iとα^jを求められる。つまり、iとjが求められ、2 誤り訂正が可能となる。

以上、<u>生成多項式$g(x)$がα^3も根に持てば 2 誤り訂正が可能である</u>ことがわかった。

３－３）生成多項式$g(x)$がα^3も根に持つようにする。

原始多項式　$p(x) = x^4 + x + 1$　　$\alpha^4 + \alpha + 1 = 0$

$q(x)$をα^3を根に持つ最小次元の多項式とし、生成多項式を　$g(x) = p(x)q(x)$　とする。

準備(B)より、$q(x)$がα^3を根に持つならば、α^6、α^{12}、$\alpha^{24} = \alpha^9$、（$\alpha^{48} = \alpha^3$）も根に持つ。

従って、$q(x) = (x+\alpha^3)(x+\alpha^6)(x+\alpha^9)(x+\alpha^{12}) = x^4 + x^3 + x^2 + x + 1$

以上より、生成多項式は、以下となる。

$$g(x) = p(x)q(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) = x^8 + x^7 + x^6 + x^4 + 1$$

$$= (x+\alpha^1)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)(x+\alpha^6)(x+\alpha^8)(x+\alpha^9)(x+\alpha^{12})$$

この生成多項式は、べきが連続した根　$\alpha^1, \alpha^2, \alpha^3, \alpha^4$　を持つため、$2t_0 = 4$より 2 誤り訂正可能である（後の BCH 符号の生成多項式を参照）。また、$x^{15} + 1$を整除し、8 次であるので、符号長$n = 15$、検査ビット数 8 の 2 誤り訂正可能な BCH(15, 7)符号を生成する。

（４）(15, 7)符号を元にして、３誤り訂正可能な符号を生成したい。

３－３）と同様に、生成多項式がα^5も根として持つように構成する。

結果は、(15, 5)符号となる。（確認せよ。）

（５）４，５，６誤り訂正可能な符号は？　７誤り訂正可能な符号は？

結果は 7 誤り訂正可能な(15, 1)符号。(00・・・0)(11・・・1)の 2 語しかない符号。

（６）まとめ

符号名	生成多項式の根	生成多項式の次数	符号語数
1 誤り訂正可能(15, 11)符号	$\alpha^1, \alpha^2, \alpha^4, \alpha^8$	4 次	$2^{11} = 2048$
2 誤り訂正可能(15, 7)符号	$\alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^8, \alpha^9, \alpha^{12}$	8 次	$2^7 = 128$
3 誤り訂正可能(15, 5)符号	$\alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{12}$	10 次	$2^5 = 32$
7 誤り訂正可能(15, 1)符号	$\alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}$	14 次	$2^1 = 2$

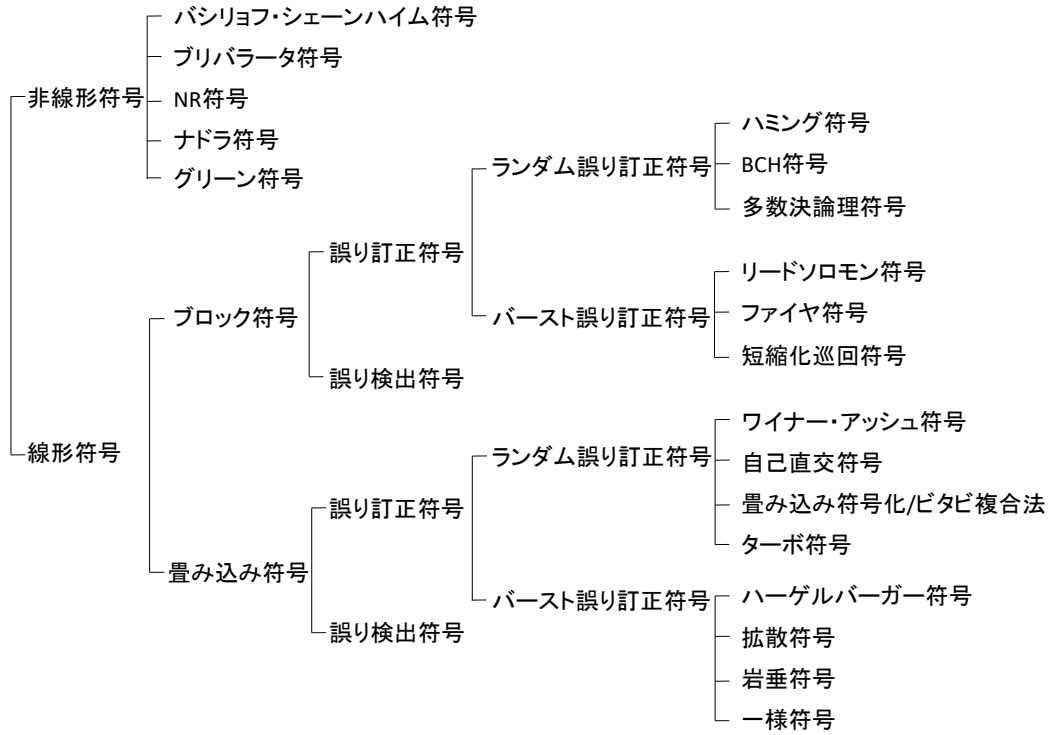
情報通信基礎Ⅰ　第６章　補足資料１

符号体系、巡回ハミングと非巡回ハミング

情シス　渡辺

１　符号体系

符号体系の例　（種々の体系化がある。ここに示すのはその一例）



２　巡回ハミングと非巡回ハミング

１）５．４　で示した検査行列H_1に対して求めた生成行列Gで生成される符号が巡回符号であるかを全符号語を求めて検討する。

$$H_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \qquad G = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

（$H = (A|I)$、$G = (I|B)$となる時、$B = A^T$）

Gの各行を①②③④とし、全符号語を線形結合で求める。

全符号語		重み	共通パタン	
①	１０００１１０	3	1101	p1
②	０１０００１１	3	1101	p1
③	００１０１０１	3	10101	なし
④	０００１１１１	4	1111	なし
①＋②	１１００１０１	4	10111	p2
①＋③	１０１００１１	4	11101	なし

①＋④	1 0 0 1 0 0 1	3	11001	なし
②＋③	0 1 1 0 1 1 0	4	11011	なし
②＋④	0 1 0 1 1 0 0	3	1011	なし
③＋④	0 0 1 1 0 1 0	3	1101	p1
①＋②＋③	1 1 1 0 0 0 0	3	111	なし
①＋②＋④	1 1 0 1 0 1 0	4	101101	なし
①＋③＋④	1 0 1 1 1 0 0	4	10111	p2
②＋③＋④	0 1 1 1 0 0 1	4	10111	p2
①＋②＋③＋④	1 1 1 1 1 1 1	7		なし
①＋①	0 0 0 0 0 0 0	0		なし

以上１６個が符号語。巡回している符号は、0000000 と 1111111 のみ。従って、巡回符号ではない。

２）６．３．４の例のGで生成される符号が巡回符号であるかを全符号語を求めて検討する。

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

Gの各行を①②③④とし、全符号語を線形結合で求める。

全符号語		重み	共通パタン	
①	1 1 0 1 0 0 0	3	1101	p1
②	0 1 1 0 1 0 0	3	1101	p1
③	0 0 1 1 0 1 0	3	1101	p1
④	0 0 0 1 1 0 1	3	1101	p1
①＋②	1 0 1 1 1 0 0	4	10111	p2
①＋③	1 1 1 0 0 1 0	4	10111	p2
①＋④	1 1 0 0 1 0 1	4	10111	p2
②＋③	0 1 0 1 1 1 0	4	10111	p2
②＋④	0 1 1 1 0 0 1	4	10111	p2
③＋④	0 0 1 0 1 1 1	4	10111	p2
①＋②＋③	1 0 0 0 1 1 0	3	1101	p1
①＋②＋④	1 0 1 0 0 0 1	3	1101	p1
①＋③＋④	1 1 1 1 1 1 1	7	1111111	p3
②＋③＋④	0 1 0 0 0 1 1	3	1101	p1
①＋②＋③＋④	1 0 0 1 0 1 1	4	10111	p2
①＋①	0 0 0 0 0 0 0	0	0000000	p4

以上１６個が符号語。p1 は７個、p2 は７個、p3 は１個、p4 は１個がそれぞれ巡回している。従って、巡回符号である。

３）６．３．４の検査行列の検討

① $G=\begin{pmatrix}1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\0&0&1&1&0&1&0\\0&0&0&1&1&0&1\end{pmatrix}$に対応する検査行列を求める。

$$G\cdot H^T=\begin{pmatrix}1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\0&0&1&1&0&1&0\\0&0&0&1&1&0&1\end{pmatrix}\cdot\begin{pmatrix}h_{11}&h_{12}&h_{13}\\h_{21}&h_{22}&h_{23}\\h_{31}&h_{32}&h_{33}\\h_{41}&h_{42}&h_{43}\\1&0&0\\0&1&0\\0&0&1\end{pmatrix}=0$$

より

$h_{11}+h_{21}+h_{41}=0$　　$h_{12}+h_{22}+h_{42}=0$　　$h_{13}+h_{23}+h_{43}=0$

$h_{21}+h_{31}+1=0$　　$h_{22}+h_{32}+0=0$　　$h_{23}+h_{33}+0=0$

$h_{31}+h_{41}+0=0$　　$h_{32}+h_{42}+1=0$　　$h_{33}+h_{43}+0=0$

$h_{41}+1=0$　　$h_{42}+0=0$　　$h_{43}+1=0$

これを解いて、

$h_{43}=1$　　$h_{42}=0$　　$h_{41}=1$

$h_{33}=1$　　$h_{32}=1$　　$h_{31}=1$

$h_{23}=1$　　$h_{22}=1$　　$h_{21}=0$

$h_{13}=0$　　$h_{12}=1$　　$h_{11}=1$

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

② $G'=\begin{pmatrix}1&0&0&0&1&1&0\\0&1&0&0&0&1&1\\0&0&1&0&1&1&1\\0&0&0&1&1&0&1\end{pmatrix}$ に対応する検査行列Hは、G'が既約梯陣形であることを利用して（$H=(A|I)$、$G=(I|B)$となる時、$B=A^T$）、$H=\begin{pmatrix}1&0&1&1&1&0&0\\1&1&1&0&0&1&0\\0&1&1&1&0&0&1\end{pmatrix}$ と求められる。

情報通信基礎Ⅰ　第７章　誤り訂正符号３（BCH, RS, Goppa）

情シス　渡辺

ポイント

・第６章では、２誤り以上の訂正が可能となるように巡回ハミングを拡張した。その際、生成多項式の根のべき乗の連続性がポイントとなった。ここではこの性質に基づいた BCH 符号、RS 符号、Goppa 符号を学ぶ。

・生成多項式$g(x)$をどのように作るかが重要。

７．１　BCH 符号

７．１．１　概要

・1959 年頃 Bose, Chaudhuri, Hocquenghem が考案

・巡回符号の一種

・生成多項式の$g(x)$の根、すなわち$g(\alpha)=0$となるαによって最小距離が決定される。

逆に言うと、必要な誤り訂正能力を実現するために最小距離から生成多項式を決定でき、符号を設計できる。

例）原始多項式$p(x)=x^4+x+1$、生成多項式$g(x)=p(x)=x^4+x+1$　とする BCH 符号

・$g(x)=0$の根は４つ。

・$g(x)$は、$x^{15}+1$を整除する。

従って、$n=15$。すなわち、$x^{15}+1=(x+1)(x^4+x+1)$…と書ける。結果的には、$g(x)$は、符号長１５、検査ビット４の巡回（15, 11）符号を生成する。

次に、$g(x)$の根の性質を調べてみる。一般には、$g(x)$は複数の根を持つが、そのうちの一つをαとする。このとき、以下の定理が成り立つ。（α^0～α^{14}は、α^0～α^3で表現可能。）

［定理７．１］

巡回符号を生成する生成多項式$g(x)$が

$$\alpha^1,\alpha^2,\alpha^3,\alpha^4,\cdots,\alpha^{2t_0}$$

のように連続したべき乗の根を持つとき、$g(x)$で生成される符号の最小距離は、$2t_0+1$となる。この生成多項式$g(x)$で生成される符号を BCH 符号と呼ぶ。（フーリエ変換などを使った証明がある。別紙　補足資料１後半）

（わ；より正確には、αは原始多項式（x^n+1を整除する周期nの規約多項式）の根。１のn乗根、$GF(2^m)$の原始根とも言う。$n=2^m-1$）

例７．１　生成多項式を$g(x)=x^4+x+1$　とする BCH 符号

生成多項式$g(x)$の一つの根をαとする。すなわち、$\alpha^4+\alpha+1=0$

$g(x)$が、α^2を根に持つかを調べる。

$g(\alpha^2)=\alpha^8+\alpha^2+1=(\alpha+1)^2+\alpha^2+1=0$　　従って、根に持つ。

$g(x)$が、α^3を根に持つかを調べる。

$g(\alpha^3)=\alpha^{12}+\alpha^3+1=(\alpha+1)^3+\alpha^3+1=\alpha^2+\alpha\neq 0$　よって、根に持たない。

以上より、生成多項式$g(x)$は、α^1, α^2をべき乗が連続する根として持つ。これより、
$2t_0 = 2$ であり、最小距離$2t_0 + 1$は３、１誤り訂正可能な符号を生成する。

$g(x)$の周期は１５（$x^{15} + 1$を整除する）　－＞符号長$n = 15$
$g(x)$の次数は４　－＞検査ビット数$m = 4$
これより、$g(x) = x^4 + x + 1$は、最小距離３の BCH(15, 11)符号を生成する。
（BCH(15, 11, 3)と書くこともある。）

例７．２　生成多項式を$g(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + 1) = x^8 + x^7 + x^6 + x^4 + 1$
とする。ただし、原始多項式を$p(x) = x^4 + x + 1$　とし、その根をα　とする。
・$g(x)$は、連続した根$\alpha^1, \alpha^2, \alpha^3, \alpha^4$　を持つ。$2t_0 = 4$ であり、最小距離$2t_0 + 1$は 5。従って、２誤り訂正可能
・$g(x)$は$x^{15} + 1$を整除する。　よって符号長は１５
・$g(x)$は８次。検査ビット数は８。
以上より、$g(x) = x^8 + x^7 + x^6 + x^4 + 1$は、BCH(15, 7, 5)を生成する。

これらの例は、生成多項式が与えられて最小距離を求めている。実際の符号を設計する時は、<u>最小距離から生成多項式を求めたい</u>。これは７．１．３で議論する。

７．１．２　拡大体
・体に何らかの元を追加することによって、体を拡大することを考える。基礎となった体を基礎体、拡大された後の体を拡大体と呼ぶ。（より正確には、基礎体上の多項式の根を追加して拡大体を構成する。）
・以下では符号理論に特に関係が深い$GF(2)$を基礎体とする。

（１）符号の多項式表現の復習
・多項式：$GF(2)$の元を係数とする多項式を考える。係数が 0, 1 の多項式。$x^3 + x + 1$など
　これを$GF(2)$上の多項式と表現する。
・既約多項式：$GF(2)$上の多項式でこれ以上因数分解できない多項式を既約多項式と呼ぶ。
　例 $x^7 + 1 = (x + 1)(x^3 + x^2 + 1)(x^3 + x + 1)$　$x^7 + 1$は非既約。$x + 1$、$x^3 + x^2 + 1$、$x^3 + x + 1$は既約。
・周期：ある多項式が$x^n + 1$を整除し、かつ$x^i + 1\ (i < n)$を整除しない時、その多項式の周期がnであると言う。
・原始多項式：既約多項式のうち、周期が最大となるものを原始多項式と言う。
　例 $x^7 + 1 = (x + 1)(x^3 + x^2 + 1)(x^3 + x + 1)$　原始多項式は、$x^3 + x^2 + 1$、$x^3 + x + 1$
　例 $x^{15} + 1 = (x + 1)(x^4 + x^3 + 1)(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)$
　　この原始多項式は、$(x^4 + x^3 + 1)$、$(x^4 + x + 1)$、$(x^4 + x^3 + x^2 + x + 1)$
　　$(x^2 + x + 1)$は、$(x^3 + 1)$を整除するので原始多項式ではない。

$GF(2)$上の原始多項式の例（主に３項からなる多項式）

1	$x+1$	9	x^9+x^4+1	17	$x^{17}+x^3+1$	25	$x^{25}+x^3+1$
2	x^2+x+1	10	$x^{10}+x^3+1$	18	$x^{18}+x^7+1$	26	$x^{26}+x^6+x^2+x+1$
3	x^3+x+1 x^3+x^2+1	11	$x^{11}+x^2+1$	19	$x^{19}+x^5+x^2+x+1$	27	$x^{27}+x^5+x^2+x+1$
4	x^4+x+1 x^4+x^3+1	12	$x^{12}+x^6+x^4+x+1$	20	$x^{20}+x^3+1$	28	$x^{28}+x^3+1$
5	x^5+x^2+1	13	$x^{13}+x^4+x^3+x+1$	21	$x^{21}+x^2+1$	29	$x^{29}+x^2+1$
6	x^6+x+1	14	$x^{14}+x^{10}+x^6+x+1$	22	$x^{22}+x+1$	30	$x^{30}+x^{23}+x^2+x+1$
7	x^7+x+1	15	$x^{15}+x+1$	23	$x^{23}+x^5+1$	31	$x^{31}+x^3+1$
8	$x^8+x^4+x^3+x^2+1$	16	$x^{16}+x^{12}+x^3+x+1$	24	$x^{24}+x^7+x^2+x+1$	32	$x^{32}+x^{22}+x^2+x+1$

・原始多項式の根を原始根という。原始多項式の周期をnとすると、原始根は１のn乗根である。
例 x^3+x^2+1の根α。x^3+x^2+1はx^7+1を整除するので、$\alpha^7+1=0$。よって、$\alpha^7=1$

・$GF(2)$上の任意の多項式$u(x)$を多項式$g(x)$で割り算した余りの多項式$r(x)$を考える。
例 $u(x)=x^6+x^5 \quad g(x)=x^3+x+1 \quad (x^6+x^5)\ mod\ (x^3+x+1)=x$
$g(x)$の次元をmとすると、余りの多項式$r(x)$の次元は$m-1$以下となる。
$GF(2)$上の任意の多項式$u(x)$をm次の多項式$g(x)$で除した余りの多項式（剰余多項式）の集合$\{r(x)\}$は、$m-1$次以下の多項式すべてが含まれる。$u(x)=f(x)g(x)+r(x)$であり、$u(x)$は任意であるので、$r(x)$はどのような$m-1$次以下の多項式にもなる。

（２）拡大体　$GF(2^m)$

・$GF(2)$上の多項式$u(x)$の根（つまり$u(\alpha)=0$となるα）は、一般には$GF(2)$上にはない。このαを$GF(2)$に追加して、拡大体を構成する。$GF(2)$は加法や乗法が定義されているので、αを加えることはαのべき乗などα以外の元も加えることになる。

・$GF(2)$上の任意の多項式$u(x)$をm次の原始多項式$g(x)$で除した余りの多項式の集合$\{r(x)\}$は、$m-1$次以下の多項式すべてが含まれ、０以外は$g(x)$の根（αとする）のべき乗で表現できる。集合$\{r(x)\}=\{0,\alpha^0,\alpha^1,\alpha^2,,,\}$は拡大体$GF(2^m)$をなす。

---例（2 次の原始多項式の例）

・$GF(2)$上の任意の多項式を二次の多項式で除した余りの集合（剰余多項式集合と呼ぶ）は、１次以下の多項式すべてが含まれる。剰余多項式集合の要素を列挙すると以下となる。

多項式	ベクトル表現
0	00
1	01
x	10
$x+1$	11

・$GF(2)$上の既約多項式（原始多項式）$g(x)=x^2+x+1$の根をα（つまり$g(\alpha)=\alpha^2+\alpha+1=0$）とする。剰余多項式集合の各多項式にαを代入した値は、以下となる。

多項式	ベクトル表現	αべき表現	
0	00	0	
1	01	1	$=\alpha^0$
x	10	α	$=\alpha^1$
$x+1$	11	$\alpha+1$	$=\alpha^2$

従って、<u>0 以外の要素をαのべき乗で表現できる</u>。
以上のことを、$GF(2)$上の任意の多項式を原始多項式$g(x)=x^2+x+1$で割った余りの多項式（剰余多項式）の集合は、拡大体$GF(2^2)=\{0,1,\alpha,\alpha^2\}$　を構成する、と言う。

・符号理論からすると、基礎体$GF(2)$の二要素から構成される符号の世界{0, 1}から、2 個の組合せ

でできる$GF(2^2)$の４要素で構成される世界{00, 01, 10, 11}に拡大した、と言える。

---例（３次の原始多項式の例）

・$GF(2)$上の任意の多項式を原始多項式x^3+x+1（ベクトル表現では 1011） で除した余りの集合は、以下となる。

多項式	ベクトル表現	αべき表現	
0	000	0	
1	001	1	$=\alpha^0$
x	010	α	$=\alpha^1$
$x+1$	011	$\alpha+1$	$=\alpha^3$
x^2	100	α^2	$=\alpha^2$
x^2+1	101	α^2+1	$=\alpha^6$
x^2+x	110	$\alpha^2+\alpha$	$=\alpha^4$
x^2+x+1	111	$\alpha^2+\alpha+1$	$=\alpha^5$

ここで、$\alpha^3+\alpha+1=0$　より

$\alpha^3=\alpha+1$

$\alpha^4=\alpha(\alpha+1)=\alpha^2+\alpha$

$\alpha^5=\alpha(\alpha^2+\alpha)=\alpha^3+\alpha^2=\alpha+1+\alpha^2$

$\alpha^6=\alpha(\alpha^2+\alpha+1)=\alpha^3+\alpha^2+\alpha=\alpha+1+\alpha^2+\alpha=\alpha^2+1$

を使っている。拡大体は、$GF(2^3)=\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6\}$である。

---例（４次の原始多項式の例）

・$GF(2)$上の任意の多項式を原始多項式x^4+x+1（ベクトル表現 10011)で除した余りの集合は、以下となる。

多項式表現	ベクトル表現	αべき乗表現	
0	0000	0	
1	0001	1	$=\alpha^0$
x	0010	α	$=\alpha^1$
$x+1$	0011	$\alpha+1$	$=\alpha^4$
x^2	0100	α^2	$=\alpha^2$
x^2+1	0101	α^2+1	$=\alpha^8$
x^2+x	0110	$\alpha^2+\alpha$	$=\alpha^5$
x^2+x+1	0111	$\alpha^2+\alpha+1$	$=\alpha^{10}$
x^3	1000	α^3	$=\alpha^3$
x^3+1	1001	α^3+1	$=\alpha^{14}$
x^3+x	1010	$\alpha^3+\alpha$	$=\alpha^9$
x^3+x+1	1011	$\alpha^3+\alpha+1$	$=\alpha^7$
x^3+x^2	1100	$\alpha^3+\alpha^2$	$=\alpha^6$
x^3+x^2+1	1101	$\alpha^3+\alpha^2+1$	$=\alpha^{13}$
x^3+x^2+x	1110	$\alpha^3+\alpha^2+\alpha$	$=\alpha^{11}$
x^3+x^2+x+1	1111	$\alpha^3+\alpha^2+\alpha+1$	$=\alpha^{12}$

拡大体は、$GF(2^4)=\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}\}$である。

７．１．３　BCH 詳細

（１）BCH の定義（以下は２元に限定して説明する）

・生成多項式の根に誤り訂正能力が依存する性質を利用。

・$GF(2^m)$上で演算を行う。

・m次の原始多項式を１つ選ぶ。その根を αとする。符号長は$n = 2^m - 1$である。（cf. primitive）

・達成したい最小距離d_{min}を$n = 2^m - 1$以下の整数で選ぶ。

・べき乗が連続した根（$\alpha^l, \alpha^{l+1}, \cdots, \alpha^{l+d_{min}-2}$）を持つ最小次数の多項式を生成多項式$g(x)$とする。

・この生成多項式$g(x)$により、最小距離がd_{min}である符号が構成される。

$$g(x) = \left[\prod_{i=l}^{l+d_{min}-2} \left(x - \alpha^i\right) \right] A(x) \quad （式 7.1.3.1）$$

ただし、$A(x)$は根α^l～$\alpha^{l+d_{min}-2}$の 2 乗、4 乗などを根として持つ多項式である。（$(x-\alpha^{2l})(x-\alpha^{4l})\cdots\left(x-\alpha^{2(l+1)}\right)\left(x-\alpha^{4(l+1)}\right)\cdots$）。また、$g(x)$の中に重複した項（重根）がないように構成する。

・lは任意の非負整数。普通は 0 または 1 が選ばれる（cf. narrow）

・最小距離がd_{min}の場合、t（$t = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$）個以下の誤りを訂正できる

（２）具体的な BCH 符号

１誤り訂正：$d_{min} = 3$　(3,1)(7,4)(15,11), , , (255,247)　巡回ハミング符号と同一

２誤り訂正：$d_{min} = 5$　(15,7)(31,21), , , (255,239)

３誤り訂正：$d_{min} = 7$　(15,5), , , (255,231)

４誤り訂正：$d_{min} = 9$　(63,39), , , (255,223)

（３）BCH 符号の構成方法

３－１　最小多項式による方法

・α^iを根とする多項式の内、最小の次数を持つものを $M_i(x)$とする。

・最小距離をd_{min}とする場合、生成多項式$g(x)$を以下の積の形とする。

$$g(x) = LCM\left(M_l(x), M_{l+1}(x), \cdots, M_{l+d_{min}-2}(x)\right) \quad （式 7.1.3.2）$$

ここで、LCM は、最小公倍多項式を意味する。すなわち $g(x)$は$M_l(x)$～$M_{l+d_{min}-2}(x)$で割り切れる最小の次数をもつ多項式である。

（わ；最終項のインデックス$l + d_{min} - 2$が偶数で、かつ、$(l + d_{min} - 2)/2$の項が含まれている場合は、最終項は省略可能。例：$M_2(x)$が含まれていれば最終項$M_4(x)$は省略可）

３－２　べきが連続した根の要素の積による方法

式 7.1.3.1 に従って、まず、生成多項式をべきが必要な数連続するように構成する。例えば、3 誤り訂正可能な符号としたい場合は、べきの初期値 l を 1 として、$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$ を根として持つ多項式を作る。

$$a(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)(x+\alpha^5)(x+\alpha^6)\cdot$$
$$(x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8)(x+\alpha^{16})(x+\alpha^{32})\cdots$$
$$(x+\alpha^3)(x+\alpha^6)(x+\alpha^{12})(x+\alpha^{24})(x+\alpha^{48})\cdots$$
$$(x+\alpha^5)(x+\alpha^{10})(x+\alpha^{20})(x+\alpha^{40})(x+\alpha^{80})\cdots$$

２段目以降は、それぞれ、$\alpha, \alpha^3, \alpha^5$ の２乗に対応する項であり、$\alpha^{n+1} = \alpha^1$，$\alpha^{3(n+1)} = \alpha^3$，$\alpha^{5(n+1)} = \alpha^5$ となるまで項をかけている。また、α^2, α^4などの偶数に対応する項がないのは、それ以前の奇数のべき乗の部分に含まれているからである。

最後に、$a(x)$ から重複する項（この例では、$(x+\alpha)$や$(x+\alpha^2)$ など）を削除する。これで最小次元の生成多項式$g(x)$が得られる。３－１で LCM を使っているのは、$g(x)$ に重複する項が含まれないようにするためである。

（４）構成例

原始多項式$x^4 + x + 1$（この根をα）を用いて、２誤り訂正能力を持つ２元(15, 7)BCH を構成する。

１）生成多項式$g(x)$の構成

式 7.1.3.2 で $l = 1$とする。最小距離 5 とすれば、$l + d_{min} - 2 = 1 + 5 - 2 = 4$より、$g(x) = LCM(M_1(x), M_2(x), M_3(x), M_4(x))$である。

$M_1(x)$, $M_2(x)$, $M_3(x)$, $M_4(x)$を議論する。

$M_1(x)$: αを根とする最小多項式－＞原始多項式そのもの　$x^4 + x + 1$

$M_2(x)$: α^2を根とする最小多項式－＞α^2も原始多項式の根。よって原始多項式そのもの（※１）

$M_3(x)$: α^3を根とする最小多項式－＞$x^4 + x^3 + x^2 + x + 1$　（※２）

$M_4(x)$: α^4を根とする最小多項式－＞$M_2(x)$と同様に原始多項式そのもの

従って、生成多項式は以下となる。

$g(x) = LCM\big(M_1(x), M_2(x), M_3(x), M_4(x)\big) = LCM\big(M_1(x), M_3(x)\big) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)$

２）各符号語は、$g(x)$を用いて構成する。

$g(x)$は、$\alpha, \alpha^2, \alpha^3, \alpha^4$を根に持つ。$g(x)$が$x^{15} + 1$を整除し、また、$g(x)$の次元が８次であることから、最小距離５、２誤り訂正可能な(15, 7)符号を構成する。

※１　$M_2(x) = M_1(x) = x^4 + x + 1$　の証明（$M_1(x)$がα^2を根に持つことの証明）

$M_1(\alpha^2) = \alpha^8 + \alpha^2 + 1 = (\alpha + 1)^2 + \alpha^2 + 1 = \alpha^2 + 1 + \alpha^2 + 1 = 0$　　$\because \alpha^4 + \alpha + 1 = 0$

一般に、$M_{2j}(x)$は、$M_j(x)$と同一である。

※２　$M_3(x)$の導出

$M_3(x)$　はα^3を根に持つ。従って、α^6、α^{12}、$\alpha^{24} = \alpha^9$、（$\alpha^{48} = \alpha^3$）も根に持つため、以下となる。

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

（別解）

$M_3(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x^1 + 1$とする。（できるだけ次数の少ない多項式とする）

この多項式がα^3を根に持つように、a_4～a_1を定めればよい。つまり、

$M_3(\alpha^3) = a_4\alpha^{12} + a_3\alpha^9 + a_2\alpha^6 + a_1\alpha^3 + 1 = 0$

となるa_4～a_1を求める。ここで、$\alpha^4 + \alpha + 1 = 0$を用いると、

$\alpha^{12} = (\alpha + 1)^3 = \alpha^3 + \alpha^2 + \alpha^1 + 1$

$\alpha^9 = (\alpha + 1)^2\alpha = (\alpha^2 + 1)\alpha = \alpha^3 + \alpha$

$\alpha^6 = (\alpha+1)\alpha^2 = \alpha^3 + \alpha^2$

従って、

$a_4(\alpha^3+\alpha^2+\alpha+1) + a_3(\alpha^3+\alpha) + a_2(\alpha^3+\alpha^2) + a_1\alpha^3 + 1 = 0$

$(a_4+a_3+a_2+a_1)\alpha^3 + (a_4+a_2)\alpha^2 + (a_4+a_3)\alpha + (a_4+1) = 0$

ここから、$a_4 = 1, a_3 = 1, a_2 = 1, a_1 = 1$　を得る。

（５）BCH 符号の検査行列（発展）

符号語多項式$u(x)$は生成多項式$g(x)$で整除される。すなわち、$u(x) = X(x)g(x)$である。　従って、$g(x)$の根をαとすると、$u(\alpha) = X(\alpha)g(\alpha)$=0　であり、これを利用して検査行列を作ることができる。受信語を$v = (a_{n-1} \quad a_{n-2} \quad \cdots \quad a_2 \quad a_1 \quad a_0)$、多項式表現を$v(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_2x^2 + a_1x + a_0$とすると、

$$v(\alpha) = a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_2\alpha^2 + a_1\alpha + a_0 = 0$$

を確認する。すなわち、

$$vH^T = (a_{n-1} \quad a_{n-2} \quad \cdots \quad a_2 \quad a_1 \quad a_0)\begin{pmatrix} \alpha^{n-1} \\ \alpha^{n-2} \\ \vdots \\ \alpha^2 \\ \alpha^1 \\ 1 \end{pmatrix} = 0$$

従って、$H = (\alpha^{n-1} \quad \alpha^{n-2} \quad \cdots \quad \alpha^2 \quad \alpha^1 \quad 1)$である。その他に根があれば、それも列挙することとなる。

例１　$GF(2^3)$上の原始多項式$p(x) = x^3 + x + 1$の場合。原始根をαとすれば、$\alpha^3 + \alpha + 1 = 0$。生成多項式が$\alpha$を根として持つ場合の符号化規則（検査規則）は、$u(\alpha) = a_6\alpha^6 + a_5\alpha^5 + a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0 = 0$である。$\alpha^6$などを２元で展開すれば、検査行列を以下のように書ける。（７．１．２　３次の例を参照）

$$H = (\alpha^6 \quad \alpha^5 \quad \alpha^4 \quad \alpha^3 \quad \alpha^2 \quad \alpha^1 \quad 1) = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

例２　$GF(2^3)$上の原始多項式$p(x) = x^3 + x^2 + 1$の場合。原始根をαとすれば、$\alpha^3 + \alpha^2 + 1 = 0$。

①生成多項式がαを根として持つ場合の符号化規則（検査規則）は、$u(\alpha) = a_6\alpha^6 + a_5\alpha^5 + a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0 = 0$である。$\alpha^6$などを２元で展開すれば、検査行列を以下のように書ける。

$$H = (\alpha^6 \quad \alpha^5 \quad \alpha^4 \quad \alpha^3 \quad \alpha^2 \quad \alpha^1 \quad 1) = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

②生成多項式がα, α^3を根として持つ場合は、

$$u(\alpha) = a_6\alpha^6 + a_5\alpha^5 + a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0 = 0$$

$$u(\alpha^3) = a_6\alpha^{18} + a_5\alpha^{15} + a_4\alpha^{12} + a_3\alpha^9 + a_2\alpha^6 + a_1\alpha^3 + a_0 = 0$$

である。α^6などを２元で展開すれば、検査行列を以下のように書ける。

$$H=\begin{pmatrix}\alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha^1 & 1\\ \alpha^{18} & \alpha^{15} & \alpha^{12} & \alpha^9 & \alpha^6 & \alpha^3 & 1\end{pmatrix}=\begin{pmatrix}\alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha^1 & 1\\ \alpha^4 & \alpha^1 & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 & 1\end{pmatrix}$$

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

例３　$GF(2^4)$上の原始多項式$p(x)=x^4+x+1$の場合。原始根をαとすれば、$\alpha^4+\alpha+1=0$。

①生成多項式がαを根として持つ場合（$\alpha,\alpha^2,\alpha^4,\alpha^8$を根に持つ）の符号化規則（検査規則）は、

$u(\alpha)=a_{14}\alpha^{14}+a_{13}\alpha^{13}+a_{12}\alpha^{12}+a_{11}\alpha^{11}+a_{10}\alpha^{10}+a_9\alpha^9+a_8\alpha^8+a_7\alpha^7+a_6\alpha^6+a_5\alpha^5+a_4\alpha^4+a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0$=0

であるので、検査行列は以下となる。

$$H=(\alpha^{14}\quad\alpha^{13}\quad\alpha^{12}\quad\alpha^{11}\quad\alpha^{10}\quad\alpha^9\quad\alpha^8\quad\alpha^7\quad\alpha^6\quad\alpha^5\quad\alpha^4\quad\alpha^3\quad\alpha^2\quad\alpha^1\quad 1)$$

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

②αとα^3を根として持つ場合（$\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^6,\alpha^8,\alpha^9,\alpha^{12}$も根に持つ）の検査行列は、

$u(\alpha)=a_{14}\alpha^{14}+a_{13}\alpha^{13}+a_{12}\alpha^{12}+a_{11}\alpha^{11}+a_{10}\alpha^{10}+a_9\alpha^9+a_8\alpha^8+a_7\alpha^7+a_6\alpha^6+a_5\alpha^5+a_4\alpha^4+a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0$=0

かつ

$u(\alpha^3)=a_{14}\alpha^{42}+a_{13}\alpha^{39}+a_{12}\alpha^{36}+a_{11}\alpha^{33}+a_{10}\alpha^{30}+a_9\alpha^{27}+a_8\alpha^{24}+a_7\alpha^{21}+a_6\alpha^{18}+a_5\alpha^{15}$
$+a_4\alpha^{12}+a_3\alpha^9+a_2\alpha^6+a_1\alpha^3+a_0$

$=a_{14}\alpha^{12}+a_{13}\alpha^9+a_{12}\alpha^6+a_{11}\alpha^3+a_{10}\alpha^0+a_9\alpha^{12}+a_8\alpha^9+a_7\alpha^6+a_6\alpha^3+a_5\alpha^0+a_4\alpha^{12}+a_3\alpha^9+a_2\alpha^6+a_1\alpha^3+a_0$=0

であるので、以下となる。

$$H=\begin{pmatrix}\alpha^{14}&\alpha^{13}&\alpha^{12}&\alpha^{11}&\alpha^{10}&\alpha^9&\alpha^8&\alpha^7&\alpha^6&\alpha^5&\alpha^4&\alpha^3&\alpha^2&\alpha^1&1\\ \alpha^{42}&\alpha^{39}&\alpha^{36}&\alpha^{33}&\alpha^{30}&\alpha^{27}&\alpha^{24}&\alpha^{21}&\alpha^{18}&\alpha^{15}&\alpha^{12}&\alpha^9&\alpha^6&\alpha^3&1\end{pmatrix}$$

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

（６）最小多項式（発展）

BCH を構成する際には最小多項式を用いる。

［最小多項式］

$GF(p^m)$上のm次の原始多項式を$p(x)$とする。この根（原始根）をαとする。すなわち、$p(\alpha)$=0 である。$q(\beta)=0\ (\beta\in GF(p^m))$　を満たす$GF(p)$上の多項式の中で次数が最小のもの$q(x)$を$GF(p)$上のβ

に対する最小多項式と呼ぶ。

例１　$GF(2^3)$上の原始多項式$p(x)=x^3+x+1$を考える。周期７。原始根をαとすれば、$\alpha^3+\alpha+1=0$、$\alpha^7=1$。ここで、$q(\beta)=0\ (\beta\in GF(2^3))$を満たす$GF(2)$上の最小多項式を求める。

$GF(2^3)=\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6\}$であるから、それぞれが$\beta$の候補となり得る。

$\beta=0$のとき、$q(x)|_{x=0}=0$　　最小多項式は$q(x)=x$
$\beta=1$のとき、$q(x)|_{x=1}=0$　　最小多項式は$q(x)=x+1$
$\beta=\alpha$のとき、$q(x)|_{x=\alpha}=0$　　最小多項式は$q(x)=x^3+x+1=p(x)$
$\beta=\alpha^2$のとき、$q(x)|_{x=\alpha^2}=0$　　最小多項式は$q(x)=x^3+x+1=p(x)$　　※２
$\beta=\alpha^3$のとき、$q(x)|_{x=\alpha^3}=0$　　最小多項式は$q(x)=x^3+x^2+1$　　※３
$\beta=\alpha^4$のとき、$q(x)|_{x=\alpha^4}=0$　　最小多項式は$q(x)=x^3+x+1=p(x)$　　※４
$\beta=\alpha^5$のとき、$q(x)|_{x=\alpha^5}=0$　　最小多項式は$q(x)=x^3+x^2+1$　　※５
$\beta=\alpha^6$のとき、$q(x)|_{x=\alpha^6}=0$　　最小多項式は$q(x)=x^3+x^2+1$　　※６

※２　$\alpha^6+\alpha^2+1=(\alpha+1)^2+\alpha^2+1=0$
※３　$\alpha^9+\alpha^6+1=\alpha^2+\alpha^2+1+1=0$
※４　$\alpha^{12}+\alpha^4+1=\alpha^5+\alpha^4+1=\alpha^2(\alpha+1)+\alpha^4+1=\alpha^3+\alpha^2+\alpha^2+\alpha+1=0$
※５　$\alpha^{15}+\alpha^{10}+1=\alpha^1+\alpha^3+1=0$
※６　$\alpha^{18}+\alpha^{12}+1=\alpha^4+\alpha^5+1=0$

例２　$GF(2^3)$上の原始多項式$p(x)=x^3+x^2+1$を考える。周期７。原始根をαとすれば、$\alpha^3+\alpha^2+1=0$。ここで、$q(\beta)=0\ (\beta\in GF(2^3))$を満たす$GF(2)$上の最小多項式を求める。

$GF(2^3)=\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6\}$であるから、それぞれが$\beta$の候補となり得る。

$\beta=0$のとき、$q(x)|_{x=0}=0$　　最小多項式は$q(x)=x$
$\beta=1$のとき、$q(x)|_{x=1}=0$　　最小多項式は$q(x)=x+1$
$\beta=\alpha$のとき、$q(x)|_{x=\alpha}=0$　　最小多項式は$q(x)=x^3+x^2+1=p(x)$
$\beta=\alpha^2$のとき、$q(x)|_{x=\alpha^2}=0$　　最小多項式は$q(x)=x^3+x^2+1=p(x)$　　※２
$\beta=\alpha^3$のとき、$q(x)|_{x=\alpha^3}=0$　　最小多項式は$q(x)=x^3+x+1$　　※３
$\beta=\alpha^4$のとき、$q(x)|_{x=\alpha^4}=0$　　最小多項式は$q(x)=x^3+x^2+1=p(x)$　　※４
$\beta=\alpha^5$のとき、$q(x)|_{x=\alpha^5}=0$　　最小多項式は$q(x)=x^3+x+1$　　※５
$\beta=\alpha^6$のとき、$q(x)|_{x=\alpha^6}=0$　　最小多項式は$q(x)=x^3+x+1$　　※６

※２　$\alpha^6+\alpha^4+1=(\alpha^2+1)^2+\alpha^4+1=\alpha^4+1+\alpha^4+1=0$
※３　$\alpha^9+\alpha^3+1=\alpha^2+\alpha^3+1=0$
※４　$\alpha^{12}+\alpha^8+1=\alpha^5+\alpha^1+1=\alpha^2(\alpha^2+1)+\alpha^1+1=\alpha^4+\alpha^2+\alpha^1+1=\alpha(\alpha^2+1)+\alpha^2+\alpha+1=0$
※５　$\alpha^{15}+\alpha^5+1=\alpha^1+\alpha^5+1=0$
※６　$\alpha^{18}+\alpha^6+1=\alpha^4+\alpha^6+1=0$

例３　４次の例

例　$GF(2^4)$上の原始多項式$p(x)=x^4+x+1$を考える。周期１５。原始根をαとすれば、$\alpha^4+\alpha+1=0$、$\alpha^{15}=1$。ここで、$q(\beta)=0\ (\beta\in GF(2^4))$を満たす$GF(2)$上の最小多項式を求める。

$GF(2^4)=\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}\}$であるから、それぞれが$\beta$の候補となり得る。（７．１．２　４次の例を参照）

$\beta=0$のとき、$q(x)|_{x=0}=0$　　最小多項式は$q(x)=x$
$\beta=1$のとき、$q(x)|_{x=1}=0$　　最小多項式は$q(x)=x+1$
$\beta=\alpha$のとき、$q(x)|_{x=\alpha}=0$　　最小多項式は$q(x)=x^4+x+1=p(x)$　　※1
$\beta=\alpha^2$のとき、$q(x)|_{x=\alpha^2}=0$　　最小多項式は$q(x)=x^4+x+1=p(x)$　　※2
$\beta=\alpha^3$のとき、$q(x)|_{x=\alpha^3}=0$　　最小多項式は$q(x)=x^4+x^3+x^2+x+1$　　※3
$\beta=\alpha^4$のとき、$q(x)|_{x=\alpha^4}=0$　　最小多項式は$q(x)=x^4+x+1=p(x)$　　※4
$\beta=\alpha^5$のとき、$q(x)|_{x=\alpha^5}=0$　　最小多項式は$q(x)=x^2+x+1$　　※5
$\beta=\alpha^6$のとき、$q(x)|_{x=\alpha^6}=0$　　最小多項式は$q(x)=x^4+x^3+x^2+x+1$　　※6
$\beta=\alpha^7$のとき、$q(x)|_{x=\alpha^7}=0$　　最小多項式は$q(x)=x^4+x^3+1$　　※7
$\beta=\alpha^8$のとき、$q(x)|_{x=\alpha^8}=0$　　最小多項式は$q(x)=x^4+x+1=p(x)$　　※8

$\beta=\alpha^9$のとき、$q(x)|_{x=\alpha^9}=0$　　最小多項式は$q(x)=x^4+x^3+x^2+x+1$　　※9
$\beta=\alpha^{10}$のとき、$q(x)|_{x=\alpha^{10}}=0$　　最小多項式は$q(x)=x^2+x+1$　　※10
$\beta=\alpha^{11}$のとき、$q(x)|_{x=\alpha^{11}}=0$　　最小多項式は$q(x)=x^4+x^3+1$　　※11
$\beta=\alpha^{12}$のとき、$q(x)|_{x=\alpha^{12}}=0$　　最小多項式は$q(x)=x^4+x^3+x^2+x+1$　　※12
$\beta=\alpha^{13}$のとき、$q(x)|_{x=\alpha^{13}}=0$　　最小多項式は$q(x)=x^4+x^3+1$　　※13
$\beta=\alpha^{14}$のとき、$q(x)|_{x=\alpha^{14}}=0$　　最小多項式は$q(x)=x^4+x^3+1$　　※14

※2　$\alpha^8+\alpha^2+1=(\alpha+1)^2+\alpha^2+1=\alpha^2+1+\alpha^2+1=0$　あるいは、$(0101)+(0100)+(0001)=0$
※3　$\alpha^{12}+\alpha^9+\alpha^6+\alpha^3+1=(1111)+(1010)+(1100)+(1000)+(0001)=0$
※4　$\alpha^{16}+\alpha^4+1=\alpha^1+\alpha^4+1=0$
※5　$\alpha^{10}+\alpha^5+1=(0111)+(0110)+(0001)=0$
※6　$\alpha^{24}+\alpha^{18}+\alpha^{12}+\alpha^6+1=\alpha^9+\alpha^3+\alpha^{12}+\alpha^6+1=(1010)+(1000)+(1111)+(1100)+(0001)=0$
※7　$\alpha^{28}+\alpha^{21}+1=\alpha^{13}+\alpha^6+1=(1101)+(1100)+(0001)=0$
※8　$\alpha^{32}+\alpha^8+1=\alpha^2+\alpha^8+1=(0100)+(0101)+(0001)=0$
※9　$\alpha^{36}+\alpha^{27}+\alpha^{18}+\alpha^9+1=\alpha^6+\alpha^{12}+\alpha^3+\alpha^9+1=0$
※10　$\alpha^{20}+\alpha^{10}+1=\alpha^5+\alpha^{10}+1=0$
※11　$\alpha^{44}+\alpha^{33}+1=\alpha^{14}+\alpha^3+1=(1001)+(1000)+(0001)=0$
※12　$\alpha^{48}+\alpha^{36}+\alpha^{24}+\alpha^{12}+1=\alpha^3+\alpha^6+\alpha^9+\alpha^{12}+1=0$
※13　$\alpha^{52}+\alpha^{39}+1=\alpha^7+\alpha^9+1=(1011)+(1010)+(0001)=0$
※14　$\alpha^{56}+\alpha^{42}+1=\alpha^{11}+\alpha^{12}+1=(1110)+(1111)+(0001)=0$

（7）復号（発展）

BCH 符号の復号には、ピーターソン、バーレカンプーマッシー、杉山の方法などがある。以下はピーターソンの方法に沿っている。

まず、第６章６．３．６に示した２誤り訂正可能 BCH(15, 7)符号を例に説明する。

原始多項式　$p(x)=x^4+x+1$　この根をαとすれば、$\alpha^4+\alpha+1=0$

生成多項式　$g(x)=(x^4+x+1)(x^4+x^3+x^2+x+1)$

送信符号語$u(x)$ を送信し、i ビット目とj ビット目が誤って、$v(x)$ を受信したとする。

2 ビットの誤りは　$e(x)=x^i+x^j$　と表現できる。

受信符号語を$v(x)$とし、シンドロームS_1、S_3を以下のように計算する。

$S_1=v(\alpha)=u(\alpha)+e(\alpha)=e(\alpha)=\alpha^i+\alpha^j$　　・・・（式１）

$S_3=v(\alpha^3)=u(\alpha^3)+\alpha^{3i}+\alpha^{3j}=\alpha^{3i}+\alpha^{3j}$

これらより、$\alpha^i\alpha^j=\alpha^{(i+j)}=\frac{S_3}{S_1}+{S_1}^2$　　・・・（式２）

式１，式２を連立して、i,jを求める。

今、$v(x)=(111000011110010)=x^{14}+x^{13}+x^{12}+x^7+x^6+x^5+x^4+x$を受信したとする。シンドロームを計算する。（７．１．２　４次の例を参照）

$S_1=v(\alpha)=\alpha^{14}+\alpha^{13}+\alpha^{12}+\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha=(1001)+(1101)+(1111)+(1011)+(1100)+(0110)+(0011)+(0010)=(1011)=\alpha^7$

$S_3=v(\alpha^3)=\alpha^{42}+\alpha^{39}+\alpha^{36}+\alpha^{21}+\alpha^{18}+\alpha^{15}+\alpha^{12}+\alpha^3=\alpha^{12}+\alpha^9+\alpha^6+\alpha^6+\alpha^3+1+\alpha^{12}+\alpha^3=\alpha^9+1=(1010)+(0001)=(1011)=\alpha^7$

$$\frac{S_3}{S_1}+{S_1}^2=\frac{\alpha^7}{\alpha^7}+\alpha^{7\cdot2}=1+\alpha^{14}=(0001)+(1001)=(1000)=\alpha^3$$

よって、式１は、$\alpha^i+\alpha^j=\alpha^7$。式２は、$\alpha^i\alpha^j=\alpha^{(i+j)}=\alpha^3$　となり、$i+j=3$ である。
これを解いて、$i=5$、$j=13$　と求められる。（総当たりしてもこの程度ならば容易）

一般的には、シンドロームと以下の誤り位置方程式を立てて求める。（京大　西田より）

$$\sigma(z) = (1 - \alpha^{j_1} z)(1 - \alpha^{j_2} z) \cdots (1 - \alpha^{j_l} z)$$

ただし、$0 \le j_1 < j_2 \cdots < j_l$、$l \le t$。ここから$l$本の方程式が立ち$l$個の$j_i$を特定する。

先ほどの２誤り訂正可能 BCH(15, 7)符号では、２誤り訂正可能であるので、$t = 2$。$j_1 = i,\ j_2 = j$ とすれば、誤り位置方程式は以下となる。

$$\sigma(z) = \left(1 - \alpha^i z\right)\left(1 - \alpha^j z\right) = 1 - \left(\alpha^i + \alpha^j\right)z + \alpha^{(i+j)} z^2$$

シンドロームS_1、S_3から、誤り位置方程式は、

$$\sigma(z) = 1 - S_1 z + (\frac{S_3}{S_1} + {S_1}^2) z^2$$

となる。$v(x) = (111000011110010) = x^{14} + x^{13} + x^{12} + x^7 + x^6 + x^5 + x^4 + x$を受信した場合は、以下となる。

$$\sigma(z) = 1 - \alpha^7 z + \alpha^3 z^2$$

この式のzにαのべき乗を代入すると、以下となる。

$\sigma(1) = 1 - \alpha^7 + \alpha^3 = \alpha$

$\sigma(\alpha) = 1 - \alpha^7\alpha + \alpha^3\alpha^2 = 1 + \alpha^8 + \alpha^5 = \alpha$

$\sigma(\alpha^2) = 1 - \alpha^7\alpha^2 + \alpha^3\alpha^4 = 1 + \alpha^9 + \alpha^7 = (0001) + (1010) + (1011) = 0$

$\sigma(\alpha^3) = 1 - \alpha^7\alpha^3 + \alpha^3\alpha^6 = 1 + \alpha^{10} + \alpha^9 = (0001) + (0111) + (1010) = (1100) = \alpha^6$

$\sigma(\alpha^4) = 1 - \alpha^7\alpha^4 + \alpha^3\alpha^8 = 1 + \alpha^{11} + \alpha^{11} = 1$

$\sigma(\alpha^5) = 1 - \alpha^7\alpha^5 + \alpha^3\alpha^{10} = 1 + \alpha^{12} + \alpha^{13} = (0001) + (1111) + (1101) = (0011) = \alpha^4$

$\sigma(\alpha^6) = 1 - \alpha^7\alpha^6 + \alpha^3\alpha^{12} = 1 + \alpha^{13} + 1 = \alpha^{13}$

$\sigma(\alpha^7) = 1 - \alpha^7\alpha^7 + \alpha^3\alpha^{14} = 1 + \alpha^{14} + \alpha^2 = (0001) + (1001) + (0100) = (1100) = \alpha^6$

$\sigma(\alpha^8) = 1 - \alpha^7\alpha^8 + \alpha^3\alpha^{16} = 1 + 1 + \alpha^4 = \alpha^4$

$\sigma(\alpha^9) = 1 - \alpha^7\alpha^9 + \alpha^3\alpha^{18} = 1 + \alpha^1 + \alpha^6 = (0001) + (0010) + (1100) = (1111) = \alpha^{12}$

$\sigma(\alpha^{10}) = 1 - \alpha^7\alpha^{10} + \alpha^3\alpha^{20} = 1 + \alpha^2 + \alpha^8 = (0001) + (0100) + (0101) = 0$

$\sigma(\alpha^{11}) = 1 - \alpha^7\alpha^{11} + \alpha^3\alpha^{22} = 1 + \alpha^3 + \alpha^{10} = (0001) + (1000) + (0111) = (1110) = \alpha^{11}$

$\sigma(\alpha^{12}) = 1 - \alpha^7\alpha^{12} + \alpha^3\alpha^{24} = 1 + \alpha^4 + \alpha^{12} = (0001) + (0011) + (1111) = (1101) = \alpha^{13}$

$\sigma(\alpha^{13}) = 1 - \alpha^7\alpha^{13} + \alpha^3\alpha^{26} = 1 + \alpha^5 + \alpha^{14} = (0001) + (0110) + (1001) = (1110) = \alpha^{11}$

$\sigma(\alpha^{14}) = 1 - \alpha^7\alpha^{14} + \alpha^3\alpha^{28} = 1 + \alpha^6 + \alpha^1 = (0001) + (1100) + (0010) = (1111) = \alpha^{12}$

ここから、$\sigma(z) = 1 - \alpha^7 z + \alpha^3 z^2 = (1 - \alpha^{-2} z)(1 - \alpha^{-10} z) = (1 - \alpha^{13} z)(1 - \alpha^5 z)$

と分解でき、誤り位置が特定できる。

（８）BCH の最小距離（発展）

設計時に設定した最小距離d_{min_d}と実際に作成される符号の最小距離d_{min_a}は、初期値 l に依存し、$d_{min_d} \le d_{min_a}$となる。これはlによって、最終的にできる生成多項式の連続するべき乗の根の数が変わるためである。

最小距離$d_{min} = 3$として設計する場合を考える。原始多項式を$x^4 + x + 1$とする。

生成多項式を以下に示す。

$$g(x) = \left[\prod_{i=l}^{l+d_{min}-2} \left(x - \alpha^i\right) \right] A(x) \quad \text{（式 1）}$$

$$g(x) = LCM\left(M_l(x), M_{l+1}(x), \cdots, M_{l+d_{min}-2}(x)\right) \quad \text{（式 2）}$$

$l + d_{min} - 2 = l + 3 - 2 = l + 1$　　である。いくつかのlに対して、式１に入る根と、式２の項、最終的に達成される最小距離を以下に示す。

l	$l + d_{min} - 2$	式１の根	式２の項	最終的な最小距離
0	1	$1, \alpha, (\alpha^2)$	M_0, M_1	$d_{min} = 4$となる
1	2	α, α^2	M_1, M_2	$d_{min} = 3$
2	3	$(\alpha), \alpha^2, \alpha^3, (\alpha^4)$	M_2, M_3	$d_{min} = 5$となる
3	4	$(\alpha), (\alpha^2), \alpha^3, \alpha^4$	M_3, M_4	$d_{min} = 5$となる

（）は、結果的に加わる根でべきが連続しているものである。

$l = 2$の場合を詳しく説明する。式１に従って、必要な根の項とそのべきの２乗の項の積を求める。

$$a(x) = (x + \alpha^2)(x + \alpha^3) \cdot$$
$$(x + \alpha^2)(x + \alpha^4)(x + \alpha^8)(x + \alpha^{16}) \cdot$$
$$(x + \alpha^3)(x + \alpha^6)(x + \alpha^{12})(x + \alpha^{24})(x + \alpha^{48})$$

よって、生成多項式は以下となる。

$g(x) = (x + \alpha)(x + \alpha^2)(x + \alpha^3)(x + \alpha^4)(x + \alpha^6)(x + \alpha^8)(x + \alpha^9)(x + \alpha^{12}) = x^8 + x^7 + x^6 + x^4 + 1$

$\alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4$ が連続しており、最小距離d_{min}は 5 となる。つまり、$d_{min} = 3$を目指して設計したが、$d_{min} = 5$の符号、すなわち、２誤り訂正可能 BCH(15,7)符号ができる。

式２の$g(x) = LCM\left(M_2(x), M_3(x)\right)$　でも同じ結果が得られる。

$M_2(x)$: α^2を根とする最小多項式－＞原始多項式$M_1(x)$

$M_3(x)$: α^3を根とする最小多項式－＞$x^4 + x^3 + x^2 + x + 1$

$g(x) = LCM\left(M_2(x), M_3(x)\right) = LCM\left(M_1(x), M_3(x)\right) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)$

$= x^8 + x^7 + x^6 + x^4 + 1$

$l = 3$の場合は、$g(x) = LCM\left(M_3(x), M_4(x)\right) = LCM\left(M_1(x), M_3(x)\right)$　であり、$l = 2$と同一の符号が得られる。

$l = 0$の場合は、$g(x) = (x + 1)(x + \alpha)(x + \alpha^2)(x + \alpha^4)(x + \alpha^8)$であり、$d_{min} = 4$の(15, 10)符号となる。この符号は、$l = 1$の$d_{min} = 3$の符号の生成多項式に$(x + 1)$の項が加わって、パリティビットが付いた符号となる。

まとめると以下となる。

l	$l + d_{min} - 2$	べきが連続する根	LCM の項	最終的な最小距離
0	1	$1, \alpha, \alpha^2$	M_0, M_1	$d_{min} = 4$
1	2	α, α^2	M_1, M_2	$d_{min} = 3$

2	3	$\alpha, \alpha^2, \alpha^3, \alpha^4$	M_2, M_3	$d_{min} = 5$
3	4	$\alpha, \alpha^2, \alpha^3, \alpha^4$	M_3, M_4	$d_{min} = 5$
4	5	$\alpha, \alpha^2 \mid \alpha^4, \alpha^5$	M_4, M_5	$d_{min} = 3$
5	6	$\alpha^5, \alpha^6 \mid \alpha^9, \alpha^{10}$	M_5, M_6	$d_{min} = 3$
6	7	$\alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}$	M_6, M_7	$d_{min} = 5$
7	8	$\alpha, \alpha^2 \mid \alpha^7, \alpha^8 \mid \alpha^{13}, \alpha^{14}$	M_7, M_8	$d_{min} = 3$
8	9	$\alpha, \alpha^2, \alpha^3, \alpha^4$	M_8, M_9	$d_{min} = 5$
9	10	$\alpha^5, \alpha^6 \mid \alpha^9, \alpha^{10}$	M_9, M_{10}	$d_{min} = 3$
10	11	$\alpha^{10}, \alpha^{11} \mid \alpha^{13}, \alpha^{14}$	M_{10}, M_{11}	$d_{min} = 3$
11	12	$\alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}$	M_{11}, M_{12}	$d_{min} = 5$
12	13	$\alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}$	M_{12}, M_{13}	$d_{min} = 5$
13	14	α^{13}, α^{14}	M_{13}, M_{14}	$d_{min} = 3$
14	15	$\alpha^{13}, \alpha^{14}, \alpha^{15} = 1$	M_{14}, M_0	$d_{min} = 4$

なお、$LCM\big(M_3(x), M_4(x)\big) = LCM\big(M_1(x), M_3(x)\big)$ から分かるように、最初からべきが連続している必要はない。例えば、$LCM\big(M_4(x), M_6(x)\big) = LCM\big(M_1(x), M_3(x)\big)$ であり、α^4, α^6を根として持つ生成多項式からも、$d_{min} = 5$の２誤り訂正可能 BCH(15,7)符号ができる。

また、生成多項式に原始多項式が含まれるのは、べきが連続する区間に、$\alpha, \alpha^2, \alpha^4, \alpha^8$のいずれかが含まれる場合である。例えば、$l = 6$の場合、$\alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}$が連続する根であり、$\alpha, \alpha^2, \alpha^4, \alpha^8$は含まれていない。従って、生成多項式には、原始多項式は含まれない。

$$g(x) = LCM\big(M_6(x), M_7(x)\big) = LCM\big(M_3(x), M_7(x)\big) = (x^4 + x^3 + x^2 + x + 1)(x^4 + x^3 + 1)$$

――――以下は配布しない　（８）最小距離の続き

最小距離$d_{min}=3$の場合で、

$l=4$の場合を考察する。式１に従って、必要な根の項とそのべきの２乗の項の積を求める。

$$a(x)=(x+\alpha^4)(x+\alpha^5)\cdot$$
$$(x+\alpha^8)(x+\alpha^{16})(x+\alpha^2)\cdot$$
$$(x+\alpha^5)(x+\alpha^{10})$$

よって、生成多項式は以下となる。

$$g(x)=(x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^5)(x+\alpha^8)(x+\alpha^{10})=x^6+x^5+x^4+x^3+1$$

α，α^2　と　α^4，α^5　が連続しており、最小距離d_{min}は　3　となる。結果的には、１誤り訂正可能BCH(15,9)符号ができる。

$g(x)=LCM\left(M_4(x),M_5(x)\right)$　　でも同じ結果が得られる。

$M_4(x)$: α^4を根とする最小多項式－＞原始多項式$M_1(x)$

$M_5(x)$: α^5を根とする最小多項式－＞x^2+x+1

$g(x)=LCM\left(M_4(x),M_5(x)\right)=LCM\left(M_1(x),M_5(x)\right)=(x^4+x+1)(x^2+x+1)$

$=x^6+x^5+x^4+x^3+1$

（２）最小距離$d_{min}=6$として設計する。生成多項式をx^4+x+1とする。

生成多項式を以下に示す。

$$g(x)=\left[\prod_{i=l}^{l+d_{min}-2}\left(x-\alpha^i\right)\right]A(x)\qquad（式１）$$

$$g(x)=LCM\left(M_l(x),M_{l+1}(x),\cdots,M_{l+d_{min}-2}(x)\right)\qquad（式２）$$

$l+d_{min}-2=l+6-2=l+4$ である。いくつかのlに対して、式１に入る根と、式２の項、最終的に達成される最小距離を以下に示す。

l	$l+d_{min}-2$	式１の根	式２の項	最終的な最小距離
0	4	$1,\alpha,\alpha^2,\alpha^3,\alpha^4$	M_0,M_1,M_2,M_3,M_4	$d_{min}=6$
1	5	$\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,(\alpha^6)$	M_1,M_2,M_3,M_4,M_5	$d_{min}=7$
2	6	$(\alpha),\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	M_2,M_3,M_4,M_5,M_6	$d_{min}=7$
3	7	$(\alpha),(\alpha^2),\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,(\alpha^8),(\alpha^9),(\alpha^{10}),(\alpha^{11}),(\alpha^{12}),(\alpha^{13}),(\alpha^{14})$		
			M_3,M_4,M_5,M_6,M_7	$d_{min}=15$
4	8	$(\alpha),(\alpha^2),(\alpha^3),\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,(\alpha^9),(\alpha^{10}),(\alpha^{11}),(\alpha^{12}),(\alpha^{13}),(\alpha^{14})$		
			M_4,M_5,M_6,M_7,M_8	$d_{min}=15$
:				
10	14	$(\alpha^9),\alpha^{10},\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}$	$M_{10},M_{11},M_{12},M_{13},M_{14}$	$d_{min}=7$

（）は、結果的に加わる根でべきが連続しているものである。

$l=1$の場合を考察する。式１に従って、必要な根の項とそのべきの２乗の項の積を求める。

$$a(x)=(x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)(x+\alpha^5)\cdot$$
$$(x+\alpha^2)(x+\alpha^4)(x+\alpha^8)(x+\alpha^{16})\cdot$$
$$(x+\alpha^3)(x+\alpha^6)(x+\alpha^{12})(x+\alpha^{24})(x+\alpha^{48})\cdot$$
$$(x+\alpha^5)(x+\alpha^{10})(x+\alpha^{20})$$

よって、生成多項式は以下となる。

$$g(x)=(x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)(x+\alpha^5)(x+\alpha^6)(x+\alpha^8)(x+\alpha^9)(x+\alpha^{10})(x+\alpha^{12})$$
$$=x^{10}+\cdots+1$$

$\alpha^1,\ \alpha^2,\ \alpha^3,\ \alpha^4,\alpha^5,\ \alpha^6$ が連続しており、最小距離d_{min}は７となる。つまり、$d_{min}=6$を目指して設計したが、$l=1$とすると$d_{min}=7$の符号、すなわち３誤り訂正可能 BCH(15, 5)符号ができることを意味している。

$g(x)=LCM\big(M_1(x),M_2(x),M_3(x),M_4(x),M_5(x)\big)$　でも同じ結果が得られる。

$M_1(x)$: αを根とする最小多項式－＞原始多項式そのもの x^4+x+1

$M_3(x)$: α^3を根とする最小多項式－＞$x^4+x^3+x^2+x+1$

$M_5(x)$: α^5を根とする最小多項式－＞x^2+x+1

$g(x)=LCM\big(M_1(x),M_3(x),M_5(x)\big)=(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)$
$=x^{10}+x^8+x^5+x^4+x^2+x+1$

元々あった BCH の説明

誤り訂正を前提として、l=1 で説明している。

７．１．３　BCH 詳細

（１）BCH の定義（以下は２元に限定して説明する）

・生成多項式の根の数に誤り訂正能力が依存する性質を利用。

・$GF(2^m)$上で演算を行う。

・m次の原始多項式を 1 つ選ぶ。その根を αとする。符号長は$n = 2^m - 1$である。（cf. primitive）

・達成したい最小距離d_{min}を$n = 2^m - 1$以下の任意の正整数で選ぶ。

・べき乗が連続した根（$\alpha^l, \alpha^{l+1}, \cdots, \alpha^{l+d_{min}-2}$）を持つ最小次数の多項式を生成多項式$g(x)$とする。

・この生成多項式$g(x)$により、最小距離がd_{min}である符号が構成される。

$$g(x) = \left[\prod_{i=l}^{l+d_{min}-2} \left(x - \alpha^i\right)\right] A(x) \quad （式 7.1.3.1）$$

ただし、$A(x)$は根α^l～$\alpha^{l+d_{min}-2}$の 2 乗、4 乗などを根として持つ多項式である。（$(x-\alpha^{2l})(x-\alpha^{4l})\cdots\left(x-\alpha^{2(l+1)}\right)\left(x-\alpha^{4(l+1)}\right)\cdots$）。また、$g(x)$の中に重複した項（重根）がないように構成する。

・lは任意の非負整数であり、普通は 0 または 1 が選ばれる（cf. narrow）

・以下では、特に断らない限り、$l = 1$とする。また、よく用いられる例として、$d_{min} = 2t + 1$　とする。この符号は、t以下の誤りを訂正可能である。この式を用いれば、（式 7.1.3.1）は以下のように変形できる。

$$g(x) = \left[\prod_{i=l}^{l+d_{min}-2} \left(x - \alpha^i\right)\right] A(x) = \left[\prod_{i=l}^{l+2t-1} \left(x - \alpha^i\right)\right] A(x) \quad （式 7.1.3.2）$$

（２）BCH 符号の構成方法

・α^iを根とする多項式の内、最小の次数を持つものを $M_i(x)$とする。

・t個以下の誤りを訂正する場合、生成多項式$g(x)$を以下の積の形とする。

$$g(x) = LCM\left(M_l(x), M_{l+1}(x), \cdots, M_{l+2t-2}(x)\right) \quad （式 7.1.3.3）$$

LCM は、最小公倍多項式を意味する。すなわち $g(x)$は$M_l(x)$～$M_{l+2t-2}(x)$で割り切れる最小の次数をもつ多項式である。

（最終項のインデックス$l + 2t - 2$が偶数で、かつ、$l + 2t - 4$の項が含まれている場合は、最終項は省略できる。例えば、$M_2(x)$が含まれていれば最終項$M_4(x)$は省略可）

（３）具体的な BCH 符号

１誤り訂正：$d_{min} = 3$　(3,1)(7,4)(15,11), , , (255,247)　巡回ハミング符号と同一

２誤り訂正：$d_{min} = 5$　(15,7)(31,21), , , (255,239)

３誤り訂正：$d_{min} = 7$　(15,5), , , (255,231)

４誤り訂正：$d_{min} = 9$　(63,39), , , (255,223)

（４）構成例

原始多項式x^4+x+1（この根をα）を用いて、２誤り訂正能力を持つ２元(15, 7)BCH を構成する。

１）生成多項式$g(x)$の構成

式 7.1.3.3 で $l=1$とする。２誤りを訂正可能とするためには、最小距離 5、すなわち$t=2$とすればよい。$l+2t-2=1+4-2=3$より、$g(x)=LCM(M_1(x),M_2(x),M_3(x))$である。

$M_1(x),\ M_2(x),\ M_3(x)$をまず求める。

$M_1(x)$: αを根とする最小多項式－＞原始多項式そのもの　x^4+x+1

$M_2(x)$: α^2を根とする最小多項式－＞α^2も原始多項式の根。よって原始多項式そのもの（※１）

$M_3(x)$: α^3を根とする最小多項式－＞$x^4+x^3+x^2+x+1$　（※２）

従って、

$g(x)=LCM\big(M_1(x),M_2(x),M_3(x)\big)=LCM\big(M_1(x),M_3(x)\big)=(x^4+x+1)(x^4+x^3+x^2+x+1)$

２）各符号語は、$g(x)$を用いて構成する。

$g(x)$は、$\alpha,\alpha^2,\alpha^3,\alpha^4$を根に持つ。$g(x)$が$x^{15}+1$を整除し、また、$g(x)$の次元が８次であることから、２誤り訂正可能な(15, 7)符号を構成する。

※１　$M_2(x)=M_1(x)=x^4+x+1$　の証明（$M_1(x)$がα^2を根に持つことの証明）

$M_1(\alpha^2)=\alpha^8+\alpha^2+1=(\alpha+1)^2+\alpha^2+1=\alpha^2+1+\alpha^2+1=0$　　$\because \alpha^4+\alpha+1=0$

一般に、$M_{2j}(x)$は、$M_j(x)$と同一である。

※２　$M_3(x)$の導出

$M_3(x)=a_4x^4+a_3x^3+a_2x^2+a_1x^1+1$とする。（できるだけ次数の少ない多項式とする）

この多項式がα^3を根に持つように、a_4～a_1を定めればよい。つまり、

$M_3(\alpha^3)=a_4\alpha^{12}+a_3\alpha^9+a_2\alpha^6+a_1\alpha^3+1=0$

となるa_4～a_1を求める。ここで、$\alpha^4+\alpha+1=0$を用いると、

$\alpha^{12}=(\alpha+1)^3=\alpha^3+\alpha^2+\alpha^1+1$

$\alpha^9=(\alpha+1)^2\alpha=(\alpha^2+1)\alpha=\alpha^3+\alpha$

$\alpha^6=(\alpha+1)\alpha^2=\alpha^3+\alpha^2$

従って、

$a_4(\alpha^3+\alpha^2+\alpha+1)+a_3(\alpha^3+\alpha)+a_2(\alpha^3+\alpha^2)+a_1\alpha^3+1=0$

$(a_4+a_3+a_2+a_1)\alpha^3+(a_4+a_2)\alpha^2+(a_4+a_3)\alpha+(a_4+1)=0$

ここから、$a_4=1,a_3=1,a_2=1,a_1=1$　を得る。

（別解）

$M_3(x)$　はα^3を根に持つ。従って、α^6、α^{12}、$\alpha^{24}=\alpha^9$、（$\alpha^{48}=\alpha^3$）も根に持つため、以下となる。

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

７．２　リードソロモン符号

７．２．１　ＲＳ基礎

・1960 年頃に Irving Reed と Gustave Solomon が考案

・巡回符号の一種

・笠原正雄：リード・ソロモン符号の半世紀

https://www.jstage.jst.go.jp/article/essfr/5/1/5_1_28/_pdf

・$GF(2^m)$上で演算を行う。

・多項式の係数にも拡大体を用いる。（情報記号も原始多項式の根αで表現する。）

・情報バイト数k、符号長nバイト、最小距離d_{min}、誤り訂正能力t　の関係

$$k = n - d_{min} + 1 \qquad d_{min} = 2t + 1 \qquad n = k + d_{min} - 1 = k + 2t$$

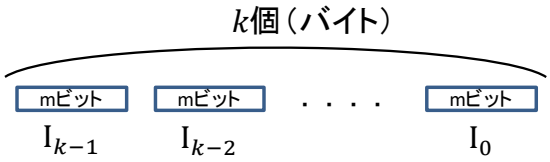
・生成多項式

$$G(y) = \prod_{i=l}^{l+d_{min}-2} (y - \alpha^i) = \prod_{i=l}^{l+2t-1} (y - \alpha^i) \qquad （式 7.2.1）$$

lは任意の非負整数。普通は 0 または 1 が選ばれる。（今井秀樹著「符号理論」電子情報通信学会 p.156 では、実装上$l = 0$が若干の優位性があるとされている。）

・非２元 BCH 符号　$n = q - 1$の場合とも言える。ただし、qは素数のべき乗である。ex. $2^3 = 8$

・k個の情報記号$I_{k-1}, \cdots, I_1, I_0$を符号化することを考える。ただし、これらの情報記号I_iは$GF(2^m)$の元とする。（各元は、原始多項式の根αのべき乗で表現可能であることに注意）。ここで、$I_i = (c_{m-1}, \cdots, c_1, c_0)$とし、この$m$ビットをバイトと表現する。$m$が 8 以外であっても RS 符号ではバイトと呼ぶ。バイト中に誤りが生じた場合は、1 バイト誤りと言う。（誤りが 1 ビットでもmビットでも）。RS 符号はバイト誤り訂正を効率的に検出訂正する符号であるとも言える。一方、I_kを多進数と捉えることもできる。



以下では、具体的な符号化を主として、生成多項式で除算する方法で説明する。

７．２．２　リード・ソロモン符号　具体的な例

以下では、$n = 2^m - 1$、$l = 0$を考える。

（１）$m = 3$の場合　　$n = 2^m - 1 = 7$　（7 バイトに注意）

１－１）

・$GF(2)$の上の原始多項式$p(x)$を$p(x) = x^3 + x + 1$とし、この根をαとする。すなわち$\alpha^3 + \alpha + 1 = 0$。

多項式	ベクトル表現	αべき表現	
0	000	0	
1	001	1	$=\alpha^0$
x	010	α	$=\alpha^1$
$x+1$	011	$\alpha+1$	$=\alpha^3$
x^2	100	α^2	$=\alpha^2$
x^2+1	101	α^2+1	$=\alpha^6$
x^2+x	110	$\alpha^2+\alpha$	$=\alpha^4$
x^2+x+1	111	$\alpha^2+\alpha+1$	$=\alpha^5$

拡大体は$GF(2^3)=\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6\}$

１－２）$n=2^m-1=7$　であるので、n,k,tの組み合わせは、以下がある。

n	k	$2t$	t	
7	5	2	1	(7, 5)符号
7	3	4	2	(7, 3)符号
7	1	6	3	(7, 1)符号

１－３）具体的な符号化の方法

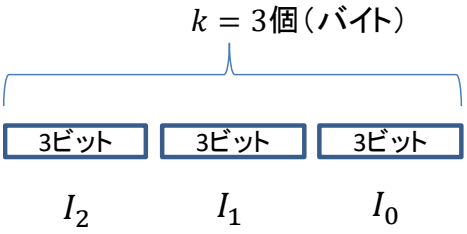
■例１　(7,3)符号　　$m=3,n=7,k=3,t=2,$ 原始多項式が$p(x)=x^3+x+1$の場合

①情報ビット系列を 3 ビット$(m=3)$ずつの 3 個$(k=3)$のブロック（バイト）に分割する。例えば

情報ビット　001 010 100

情報バイト　1　α^1　α^2

バイト番号　1　2　3



②情報バイトを多項式で表現する。

$$I(y)=I_{k-1}y^{k-1}+\cdots+I_1y+I_0=1y^2+\alpha^1y^1+\alpha^2y^0$$

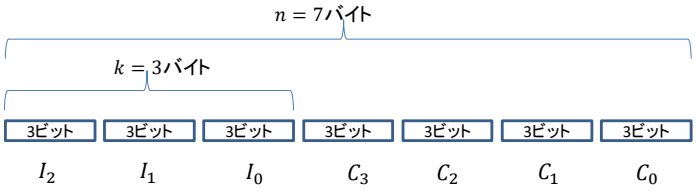
③生成多項式を求める。

$$G(y)=\prod_{i=l}^{l+2t-1}(y-\alpha^i)=\prod_{i=0}^{3}(y-\alpha^i)=(y-\alpha^0)(y-\alpha^1)(y-\alpha^2)(y-\alpha^3)$$
$$=y^4+\alpha^2y^3+\alpha^5y^2+\alpha^5y^1+\alpha^6$$

④情報多項式$I(y)*y^{n-k}$を生成多項式$G(y)$　で除算した余りを求める。

$$I(y)=I_{k-1}y^{k-1}+\cdots I_1y+I_0=1y^2+\alpha^1y^1+\alpha^2y^0$$
$$r(y)=I(y)*y^{n-k}\ mod\ G(y)=(1y^2+\alpha^1y^1+\alpha^2y^0)*y^4\ mod\ y^4+\alpha^2y^3+\alpha^5y^2+\alpha^5y^1+\alpha^6$$
$$=\alpha^4y^3+\alpha^6y^2+\alpha^5y+\alpha^3$$

⑤以上より



情報ビット	001	010	100				
情報バイト	1	α^1	α^2				
符号化後	1	α^1	α^2	α^4	α^6	α^5	α^3
RS 符号語	001	010	100	110	101	111	011
バイト番号	1	2	3	4	5	6	7

⑥③～⑤の別の方法　（生成多項式を陽に求めない方法）

符号語wを$w=(w_1,w_2,\cdots,w_n)=(I(\alpha^{n-1}),I(\alpha^{n-2}),\cdots,I(1))$で求める。

$I(y)=I_{k-1}y^{k-1}+\cdots I_1y+I_0=1y^2+\alpha^1y^1+\alpha^2y^0$

$w_7=I(y=\alpha^0)=I(y=1)=I_{k-1}+\cdots I_1+I_0=1+\alpha^1+\alpha^2=\alpha^5=(111)$

$w_6=I(y=\alpha^1)=1\alpha^2+\alpha^1\alpha^1+\alpha^2=\alpha^2+\alpha^2+\alpha^2=\alpha^2=(100)$

$w_5=I(y=\alpha^2)=1\alpha^4+\alpha^1\alpha^2+\alpha^2=\alpha^4+\alpha^3+\alpha^2=1=(001)$

$w_4=I(y=\alpha^3)=1\alpha^6+\alpha^1\alpha^3+\alpha^2=\alpha^6+\alpha^4+\alpha^2=\alpha^5=(111)$

$w_3=I(y=\alpha^4)=1\alpha^8+\alpha^1\alpha^4+\alpha^2=\alpha^1+\alpha^5+\alpha^2=1=(001)$

$w_2=I(y=\alpha^5)=1\alpha^{10}+\alpha^1\alpha^5+\alpha^2=\alpha^3+\alpha^6+\alpha^2=\alpha=(010)$

$w_1=I(y=\alpha^6)=1\alpha^{12}+\alpha^1\alpha^6+\alpha^2=\alpha^5+1+\alpha^2=\alpha=(010)$

以上より、

情報ビット	001	010	100				
情報バイト	1	α^1	α^2				
符号化後	α^1	α^1	α^0	α^5	α^0	α^2	α^5
RS 符号語	010	010	001	111	001	100	111
バイト番号	1	2	3	4	5	6	7

（2）$m=4$の場合　　$n=2^m-1=15$

2－1）

・情報記号は、$GF(2^4)$の上の元である。原始多項式を$p(x)=x^4+x+1$ とする。すなわち$\alpha^4+\alpha+1=0$。

多項式表現	ベクトル表現	αべき乗表現	
0	0000	0	
1	0001	1	$=\alpha^0$
x	0010	α	$=\alpha^1$
$x+1$	0011	$\alpha+1$	$=\alpha^4$
x^2	0100	α^2	$=\alpha^2$
x^2+1	0101	α^2+1	$=\alpha^8$
x^2+x	0110	$\alpha^2+\alpha$	$=\alpha^5$
x^2+x+1	0111	$\alpha^2+\alpha+1$	$=\alpha^{10}$
x^3	1000	α^3	$=\alpha^3$
x^3+1	1001	α^3+1	$=\alpha^{14}$
x^3+x	1010	$\alpha^3+\alpha$	$=\alpha^9$
x^3+x+1	1011	$\alpha^3+\alpha+1$	$=\alpha^7$
x^3+x^2	1100	$\alpha^3+\alpha^2$	$=\alpha^6$
x^3+x^2+1	1101	$\alpha^3+\alpha^2+1$	$=\alpha^{13}$
x^3+x^2+x	1110	$\alpha^3+\alpha^2+\alpha$	$=\alpha^{11}$
x^3+x^2+x+1	1111	$\alpha^3+\alpha^2+\alpha+1$	$=\alpha^{12}$

$GF(2^4)=\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}\}$

2－2）$n=2^m-1=15$

n	k	$2t$	t	
15	13	2	1	(15,13)符号
15	11	4	2	(15,11)符号
15	9	6	3	(15, 9)符号
15	7	8	4	(15, 7)符号
15	5	10	5	(15, 5)符号
15	3	12	6	(15, 3)符号

2－3）具体的な符号化の方法

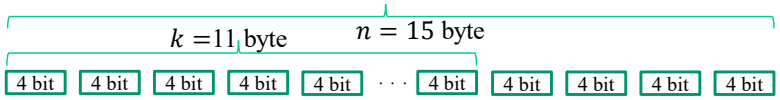
■例　(15, 11)符号　$m=4, n=15, k=11, t=2,$ 原始多項式が$p(x)=x^4+x+1$の場合

①情報ビット系列を 4 ビット$(m=4)$ずつの 11 個$(k=11)$のブロック（バイト）に分割する。例えば、

情報ビット	1010	0011	0011	1101	1110	0101	1101	1000	1010	0101	0000
情報バイト	α^9	α^4	α^4	α^{13}	α^{11}	α^8	α^{13}	α^3	α^9	α^8	0

バイト番号　1　2　3　4　5　6　7　8　9　10　11

②情報バイトを多項式で表現する。



$$I(y) = I_{k-1}y^{k-1} + \cdots I_1 y + I_0$$
$$= \alpha^9 y^{10} + \alpha^4 y^9 + \alpha^4 y^8 + \alpha^{13} y^7 + \alpha^{11} y^6 + \alpha^8 y^5 + \alpha^{13} y^4 + \alpha^3 y^3 + \alpha^9 y^2 + \alpha^8 y^1 + 0y^0$$

③生成多項式を求める。

$$G(y) = \prod_{i=l}^{l+2t-1}(y - \alpha^i) = \prod_{i=0}^{3}(y - \alpha^i) = (y - \alpha^0)(y - \alpha^1)(y - \alpha^2)(y - \alpha^3)$$
$$= y^4 + \alpha^{12} y^3 + \alpha^4 y^2 + y^1 + \alpha^6$$

④情報多項式$I(y) * y^{n-k}$を生成多項式$G(y)$　で除算した余りを求める。

$$I(y) = I_{k-1}y^{k-1} + \cdots I_1 y + I_0$$
$$= \alpha^9 y^{10} + \alpha^4 y^9 + \alpha^4 y^8 + \alpha^{13} y^7 + \alpha^{11} y^6 + \alpha^8 y^5 + \alpha^{13} y^4 + \alpha^3 y^3 + \alpha^9 y^2 + \alpha^8 y^1 + 0y^0$$
$$r(y) = I(y) * y^{n-k} \; mod \; G(y)$$
$$= (\alpha^9 y^{10} + \alpha^4 y^9 + \alpha^4 y^8 + \alpha^{13} y^7 + \alpha^{11} y^6 + \alpha^8 y^5 + \alpha^{13} y^4 + \alpha^3 y^3 + \alpha^9 y^2 + \alpha^8 y^1 + 0y^0) * y^4$$
$$mod \; y^4 + \alpha^{12} y^3 + \alpha^4 y^2 + y^1 + \alpha^6$$
$$= \alpha^{13} y^3 + \alpha^{13} y^2 + \alpha^0 y + \alpha^{10}$$

⑤以上より

情報ビット　1010 0011 0011 1101 1110 0101 1101 1000 1010 0101 0000

情報バイト　α^9　α^4　α^4　α^{13}　α^{11}　α^8　α^{13}　α^3　α^9　α^8　0

符号化後　α^9　α^4　α^4　α^{13}　α^{11}　α^8　α^{13}　α^3　α^9　α^8　0　α^{13}　α^{13}　α^0　α^{10}

RS 符号語　1010 0011 0011 1101 1110 0101 1101 1000 1010 0101 0000 1101 1101 0001 0111

バイト番号　1　2　3　4　5　6　7　8　9　10　11　12　13　14　15

⑥③～⑤の別の方法　（生成多項式を陽に求めない方法）

符号語wを$w = (w_1, w_2, \cdots, w_n) = (I(\alpha^{n-1}), I(\alpha^{n-2}), \cdots, I(1))$で求める。

$$I(y) = I_{k-1}y^{k-1} + \cdots I_1 y + I_0$$
$$= \alpha^9 y^{10} + \alpha^4 y^9 + \alpha^4 y^8 + \alpha^{13} y^7 + \alpha^{11} y^6 + \alpha^8 y^5 + \alpha^{13} y^4 + \alpha^3 y^3 + \alpha^9 y^2 + \alpha^8 y^1 + 0y^0$$
$$w_{15} = I(y = \alpha^0) = I(y = 1) = I_{k-1} + \cdots I_1 + I_0$$
$$= \alpha^9 + \alpha^4 + \alpha^4 + \alpha^{13} + \alpha^{11} + \alpha^8 + \alpha^{13} + \alpha^3 + \alpha^9 + \alpha^8 + 0$$
$$= \alpha^{11} + \alpha^3 = \alpha^3 + \alpha^2 + \alpha + \alpha^3 = \alpha^2 + \alpha = \alpha^5 = (0110)$$
$$w_{14} = I(y = \alpha^1) = I_{k-1}\alpha^{(n-i)(k-1)} + \cdots + I_1\alpha^{n-i} + I_0$$
$$= I_{10}\alpha^{(15-14)(11-1)} + I_9\alpha^{(15-14)(11-2)} + \cdots + I_1\alpha^{(15-14)(11-10)} + I_0$$
$$= I_{10}\alpha^{10} + I_9\alpha^9 + I_8\alpha^8 + I_7\alpha^7 + I_6\alpha^6 + I_5\alpha^5 + I_4\alpha^4 + I_3\alpha^3 + I_2\alpha^2 + I_1\alpha^1 + I_0$$
$$= \alpha^9\alpha^{10} + \alpha^4\alpha^9 + \alpha^4\alpha^8 + \alpha^{13}\alpha^7 + \alpha^{11}\alpha^6 + \alpha^8\alpha^5 + \alpha^{13}\alpha^4 + \alpha^3\alpha^3 + \alpha^9\alpha^2 + \alpha^8\alpha^1 + 0\alpha^0 = (0010)$$

$w_{13} = I(y = \alpha^2) = (0100)$　　$w_{12} = I(y = \alpha^3) = (1101)$　　$w_{11} = I(y = \alpha^4) = (1110)$

$w_{10} = I(y = \alpha^5) = (1011)$　　$w_9 = I(y = \alpha^6) = (1000)$　　$w_8 = I(y = \alpha^7) = (1011)$

$w_7 = I(y = \alpha^8) = (1110)$　　$w_6 = I(y = \alpha^9) = (0111)$　　$w_5 = I(y = \alpha^{10}) = (0011)$

$w_4 = I(y = \alpha^{11}) = (1111)$　　$w_3 = I(y = \alpha^{12}) = (1011)$　　$w_2 = I(y = \alpha^{13}) = (0111)$

$w_1 = I(y = \alpha^{14}) = (1001)$

情報ビット　1010 0011 0011 1101 1110 0101 1101 1000 1010 0101 0000

情報バイト　α^9　α^4　α^4　α^{13}　α^{11}　α^8　α^{13}　α^3　α^9　α^8　0

符号化後　α^{14}　α^{10}　α^7　α^{12}　α^4　α^{10}　α^{11}　α^7　α^3　α^7　α^{11}　α^{13}　α^2　α^1　α^5

RS 符号語　1001 0111 1011 1111 0011 0111 1110 1011 1000 1011 1110 1101 0100 0010 0110

バイト番号　1　2　3　4　5　6　7　8　9　10　11　12　13　14　15

２－４）復号方法の概要

種々の方法があるが、基本的には連立方程式を立てて解くこととなる。

まず、以前 BCH 符号で扱った方法を思いだそう。例えば、２誤り訂正可能な BCH 符号では、2 ビットの誤りを誤り多項式　$e(x)=x^i+x^j$　で表現し、受信符号語$v(x)$から、シンドロームS_1、S_3を以下のように計算した。

$S_1=v(\alpha)=u(\alpha)+e(\alpha)=e(\alpha)=\alpha^i+\alpha^j$　　・・・（式１）

$S_3=v(\alpha^3)=u(\alpha^3)+\alpha^{3i}+\alpha^{3j}=\alpha^{3i}+\alpha^{3j}$

$\alpha^i\alpha^j=\alpha^{(i+j)}=\frac{S_3}{S_1}+{S_1}^2$　　・・・（式２）

式１，式２を連立して、i、jを求めた。リードソロモンでは、誤り多項式は、拡大体の要素を係数に持つから、

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

と表現される。従って、４つの変数$e_i,\ e_i,\ i,\ j$　を求める必要がある。つまり、位置i、jだけでなく、その大きさ$e_i,\ e_j$を決定しなければならない。2 誤り訂正可能な RS 符号の生成多項式は、べきが連続した４つの根を持つので、

$S_0=v(1)=u(1)+e(1)=e(1)=e_i+e_j$

$S_1=v(\alpha)=u(\alpha)+e(\alpha)=e(\alpha)=e_i\alpha^i+e_j\alpha^j$

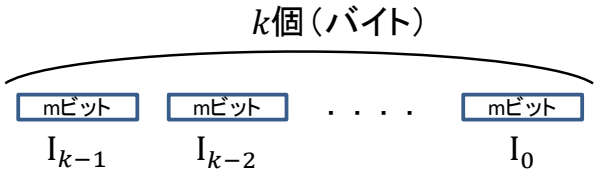
$S_2=v(\alpha^2)=e(\alpha^2)=e_i\alpha^{2i}+e_j\alpha^{2j}$

$S_3=v(\alpha^3)=e(\alpha^3)=e_i\alpha^{3i}+e_j\alpha^{3j}$

の４つの方程式が立てられ、これを解けば求めることが可能である。（注意：BCH の時は、$S_2=v(\alpha^2)$は意味がなかった。）より詳細については、７．２．４で述べる。

７．２．３　ＲＳ詳細（発展）

（１）定義



k個の情報記号$I_{k-1},\cdots,I_1,I_0$を符号化する。これらの情報記号I_iは$GF(2^m)$の元。すなわち、m個の$GF(2^m)$の元を用いて$I_i=(c_{m-1},\cdots,c_1,c_0)$と表現する。

k個の情報記号$I_{k-1},\cdots,I_1,I_0$を係数とする$GF(2^m)$上の多項式を考える。

$$I(y)=I_{k-1}y^{k-1}+\cdots+I_1y+I_0$$

nを$k<n\le 2^m$とする。n個の$GF(2^m)$の互いに異なる元を、$\alpha_1,\alpha_2,\cdots,\alpha_n$とし、下記のように構成する符号を、符号長$n$の$GF(2^m)$上の RS 符号と言う。

$$w=(\,I(\alpha_1),I(\alpha_2),\cdots,I(\alpha_n)\,)$$

（この手法とフーリエ変換の関係は、今井秀樹著「符号理論」電子情報通信学会 p.158。$I(y)$を$G(y)$で割った余りで求めてもよい。）

（２）$n=2^m-1$の RS 符号

αを$GF(2^m)$上の原始元とし、$n=2^m-1$とするとき、$GF(2^m)$上の$n-1$次以下の多項式$W(x)$が

$\alpha, \alpha^2, \cdots, \alpha^{n-k}$を根として持つならば、$W(x)$は符号長$n$、情報記号$k$、最小距離$d_{min} = n - k + 1$のRS符号の符号語となる。

符号語$w = (\, I(\alpha_1), I(\alpha_2), \cdots, I(\alpha_n)\,)$の $\alpha_1, \alpha_2, \cdots, \alpha_n$は、原始多項式$p(x)$の元（原始元）を$\alpha$とすると、$\alpha$のべき乗で表現できる。従って、

$$w = (w_1, w_2, \cdots, w_n) = (\, I(\alpha^{n-1}), I(\alpha^{n-2}), \cdots, I(1)\,)$$

$$w_n = I(y = \alpha^0) = I(y = 1) = I_{k-1} + \cdots I_1 + I_0$$
$$\vdots$$
$$w_i = I\left(\alpha^{n-i}\right) = I_{k-1}\alpha^{(n-i)(k-1)} + \cdots + I_1\alpha^{n-i} + I_0$$
$$\vdots$$
$$w_1 = I(\alpha^{n-1}) = I_{k-1}\alpha^{(n-1)(k-1)} + \cdots + I_1\alpha^{n-1} + I_0$$

と符号化する。これは、元の情報記号$I_{k-1}, \cdots, I_1, I_0$を$\alpha$のべき乗で重み付けした符号語に変換しているとも言える。あるいは、$I(y) = I_{k-1}y^{k-1} + \cdots + I_1 y + I_0$　は、元の情報記号$I_{k-1}, \cdots, I_1, I_0$を係数とする多項式曲線を表しているので、$w = (w_1, w_2, \cdots, w_n)$の各要素を情報記号$I_{k-1}, \cdots, I_1, I_0$で定義される曲線上に配置しているとも言える。

$w = (w_1, w_2, \cdots, w_n)$を多項式表現したもの（符号語多項式）は以下となる。

$$W(x) = w_1 x^n + w_2 x^{n-1} + \cdots + w_{n-1}x + w_n$$
$$= I(y = \alpha^{n-1})x^n + I(y = \alpha^{n-2})x^{n-1} + \cdots + I(y = \alpha^1)x + I(y = \alpha^0)$$

（３）最小距離

今、$w = (w_1, w_2, \cdots, w_n)$が０でなく、重みが$d$であったとする。（この場合の重みとは、非 0 の項を重み１とカウントする。）すなわち、n個の$w_1 \sim w_n$のうちd個が非０である。逆に言うと、$n - d$個のw_iが０となっている。これは、

$$\left.\begin{array}{l} w_n = I(y = \alpha^0) = I(1) = I_{k-1} + \cdots I_1 + I_0 \\ \vdots \\ w_i = I\left(\alpha^{n-i}\right) = I_{k-1}\alpha^{(n-i)(k-1)} + \cdots + I_1\alpha^{n-i} + I_0 \\ \vdots \\ w_1 = I(\alpha^{n-1}) = I_{k-1}\alpha^{(n-1)(k-1)} + \cdots + I_1\alpha^{n-1} + I_0 \end{array}\right\} \text{このうちの} n - d \text{個が } 0$$

を考えると、$I(y)$は、$n - d$個の根を持つ。$I(y) = I_{k-1}y^{k-1} + \cdots + I_1 y + I_0$の次元は、$k - 1$次以下であるので、根の数（$I(y) = 0$となる$y$の数）は$k - 1$個以下でなければならない。従って、$n - d \leq k - 1$が成立する。よって、$d \geq n - k + 1$である。すべての$d$に対して成立するので、最小距離$d_{min}$は$d_{min} \geq n - k + 1$となる。

一方、$I(y) = I_{k-1}y^{k-1} + \cdots + I_1 y + I_0 = (y - \alpha_1)(y - \alpha_2)\cdots(y - \alpha_{k-1})$とすると、$I(y)$は、$k - 1$次の多項式であり、$I\left(\alpha^j\right) \neq 0\ (j = k, k+1, \cdots, n)$（この個数が$n - k + 1$）となる。つまり、この$I(y)$で生成される符号語の０ではない成分は$n - k + 1$個あり、最小重みは$n - k + 1$であり、$d_{min} \leq n - k + 1$となる。

以上より、よって、最小距離は$d_{min} = n - k + 1$となる。RS 符号は最小距離の等号が成り立つ符

号（最大距離分離符号）である。

（4）誤り検出・訂正の基本

符号語$w=(w_1,w_2,\cdots,w_n)$の各要素は、

$w_n=I(\alpha^0)=I(1)=I_{k-1}+\cdots I_1+I_0$

：

$w_i=I\left(\alpha^{n-i}\right)=I_{k-1}\alpha^{(n-i)(k-1)}+\cdots+I_1\alpha^{n-i}+I_0$

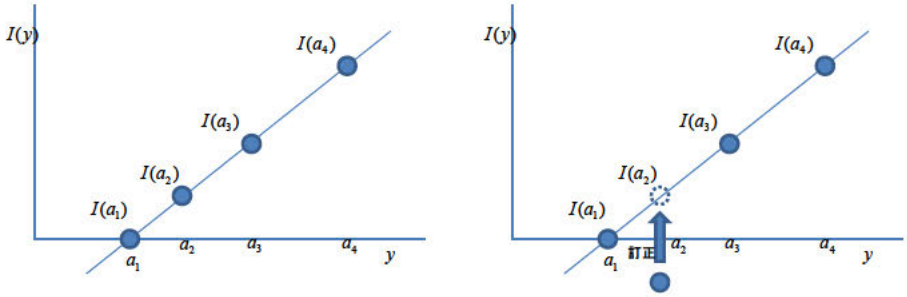
：

$w_1=I(\alpha^{n-1})=I_{k-1}\alpha^{(n-1)(k-1)}+\cdots+I_1\alpha^{n-1}+I_0$

で計算される。

つまり、$w=(w_1,w_2,\cdots,w_n)$の各要素は、$k-1$次元の曲線上に乗っていることになる。従って、復号時に曲線上にあるか否かで誤りを検出、訂正ができる。

例として、$n=4$、$k=2$でI_0、I_1を符号化することを考える。$I(y)$は$I(y)=I_1y+I_0$であり、$w=(w_1,w_2,w_3,w_4)$の各要素は、下左図のように直線上に並ぶ。０でない符号語で$I(y)=0$となるのは高々１であり、最小距離は３($d_{min}=n-k+1=4-2+1$)となる。つまり単一誤り訂正符号となる。下右図のように（バイトに）誤りが生じた場合に訂正できる。（今井秀樹著「情報・符号・暗号の理論」電子情報通信学会編　コロナ社 p.133）



（5）例題１

問 1）$GF(2^3)$において、情報バイト記号$(I_2,I_1,I_0)=(0,1,\alpha)$の時、符号長$n=2^3-1=7$、最小距離$d_{min}=5$（すなわち２誤り訂正可能）のリードソロモン符号語$w=(w_1,w_2,\cdots,w_n)$を求めよ。ただし、$\alpha$は、原始多項式$p(x)=x^3+x+1$の根であり、$GF(2^3)$の原始元であるとする。

解答)

情報バイト数kは$k=n-d_{min}+1=3$である。また、$I(y)=I_2y^2+I_1y+I_0=y+\alpha$である。

$w=(I(\alpha_1),I(\alpha_2),I(\alpha_3),I(\alpha_4),I(\alpha_5),I(\alpha_6),I(\alpha_7))=(w_1,w_2,w_3,w_4,w_5,w_6,w_7)$とする。$\alpha^3+\alpha+1=0$であるから、

$w_1=I(\alpha_1)=I(\alpha^6)=\alpha^6+\alpha=\alpha^2+1+\alpha=\alpha^3+\alpha^2=\alpha^5$　　同様に、

$w_2=I(\alpha_2)=I(\alpha^5)=\alpha^6$　$w_3=I(\alpha_3)=I(\alpha^4)=\alpha^2$　$w_4=I(\alpha_4)=I(\alpha^3)=1$

$w_5=I(\alpha_5)=I(\alpha^2)=\alpha^4$　$w_6=I(\alpha_6)=I(\alpha^1)=0$　$w_7=I(\alpha_7)=I(\alpha^0)=\alpha^3$

以上より、$w=(\alpha^5,\alpha^6,\alpha^2,1,\alpha^4,0,\alpha^3)$

問 2）問 1 の符号語$W(y)$は、$\alpha,\alpha^2,\cdots,\alpha^{n-k}=\alpha^4$を根として持つことを証明せよ。

$W(y)=\alpha^5y^6+\alpha^6y^5+\alpha^2y^4+y^3+\alpha^4y^2+\alpha^3$ であるので、

$W(\alpha)=\alpha^{11}+\alpha^{11}+\alpha^6+\alpha^3+\alpha^6+\alpha^3=0$

$W(\alpha^2) = \alpha^{17} + \alpha^{16} + \alpha^{10} + \alpha^6 + \alpha^8 + \alpha^3 = \alpha^3 + \alpha^2 + \alpha^3 + \alpha^6 + \alpha^1 + \alpha^3 = 0$

$W(\alpha^3) = \alpha^{23} + \alpha^{21} + \alpha^{14} + \alpha^9 + \alpha^{10} + \alpha^3 = 0$

$W(\alpha^4) = \alpha^{29} + \alpha^{26} + \alpha^{18} + \alpha^{12} + \alpha^{12} + \alpha^3 = 0$

問３）問１の符号語$W(y)$は生成多項式$G(y)$で整除されることを確認せよ。

生成多項式$G(y)$は、$\alpha, \alpha^2, \alpha^3, \alpha^{n-k} = \alpha^4$を根として持つから、

$$G(y) = (y-\alpha)(y-\alpha^2)(y-\alpha^3)(y-\alpha^4) = y^4 + \alpha^3 y^3 + 1y^2 + \alpha y + \alpha^3$$

$$W(y) = \alpha^5 y^6 + \alpha^6 y^5 + \alpha^2 y^4 + y^3 + \alpha^4 y^2 + \alpha^3 = (y^4 + \alpha^3 y^3 + 1y^2 + \alpha y + \alpha^3)(\alpha^5 y^2 + \alpha^5 y + 1)$$

$$= G(y)(\alpha^5 y^2 + \alpha^5 y + 1)$$

従って、$W(y)$は$G(y)$で整除される。

（６）例題２（岩垂好裕著「符号理論入門」昭晃堂 p.75 より）

問） ３誤り訂正可能な$GF(2^4)$上の RS 符号生成多項式を求めよ。ただし、αを$x^4 + x + 1$の原始元とする。

解） ３誤りを訂正するためには、生成多項式はべき数が連続する６つの根を持たねばならない。従って、生成多項式（の一つ）$G(x)$は、$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$を根として持つので以下となる。

$$G(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^5)(x-\alpha^6)$$

$$= x^6 + \alpha^{10} x^5 + \alpha^{14} x^4 + \alpha^4 x^3 + \alpha^6 x^2 + \alpha^9 x + \alpha^6$$

これによって生成される符号の符号長は$n = 2^4 - 1 = 15$、情報記号数は$k = 9$である。

７．２．４　リードソロモン符号の誤り訂正

１）概要

リードソロモンでは、誤りの位置だけでなく、誤りの大きさも決定する必要がある。

（cf. BCH では、誤りの大きさは１であったので位置を検出すればよかった。６．３．６および７．１．３（７）参照）

今、送信語$u(x)$ を送り、w個の誤りが生じて受信語$v(x)$ を受け取ったとする。

w個の誤りは、それぞれの誤りの位置をl_0、l_1、、、l_{w-1}とし、大きさをe_0、e_1、、、e_{w-1} とすれば、以下の式で表現できる。

$$e(x) = \sum_{c=0}^{w-1} e_c x^{l_c} \quad （式 7.2.2）$$

シンドロームは、

$$S_i = v(\alpha^i) = u(\alpha^i) + e(\alpha^i) = u(\alpha^i) + \sum_{c=0}^{w-1} e_c(\alpha^i)^{l_c} \quad （式 7.2.3）$$

で計算される。

t個の誤り訂正能力を持つ符号では、$2t$個のべきが連続した根を持つので、

$$u(\alpha^i) = 0 \; for \; i = 0,1,,,2t-1$$

である。従って、w（$\leq t$）個の誤りの訂正を行う場合は、

$$S_i = v(\alpha^i) = u(\alpha^i) + e(\alpha^i) = u(\alpha^i) + \sum_{c=0}^{w-1} e_c(\alpha^i)^{l_c}$$

$$= \sum_{c=0}^{w-1} e_c(\alpha^i)^{l_c} \; for \; i = 0,1,,,2t-1 （式 7.2.4）$$

となり、$2t$ 本の連立方程式が立てられる。

誤り多項式の未知変数は、位置l_0、l_1、、、l_{w-1}、大きさe_0、e_1、、、e_{w-1} の$2w$個あるので、連立方程式を解けば、誤り多項式を決定できる。この決定に関連する方法としては、ユークリッド互除法、Berlekamp-Massey, Chein Search, Forney 等がある。以下では、基本的な方法を述べる。

２）復号の手順　（2 誤り訂正の場合）

2 誤りの場合を例に挙げる。ただし、2 以上にも適応可能である。（参考　岩垂好裕著「符号理論入門」昭晃堂 p. 75-77 では３誤りを挙げている）

誤り多項式を以下のように表現する。

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

受信語は、

$$v(x) = u(x) + e(x)$$

である。２誤り訂正可能な場合は、生成多項式のべきの連続する根が４つ連続している。

シンドロームを以下で求める。

$h = 0$　$S_0 = v(\alpha^0) = u(1) + e(1) = e(1) = e_i + e_j$　式 2-1

$h = 1$　$S_1 = v(\alpha^1) = u(\alpha) + e(\alpha) = e(\alpha) = e_i\alpha^i + e_j\alpha^j$　式 2-2

$h = 2$　$S_2 = v(\alpha^2) = u(\alpha^2) + e(\alpha^2) = e(\alpha^2) = e_i\alpha^{2i} + e_j\alpha^{2j}$　式 2-3

$h = 3$　$S_3 = v(\alpha^3) = u(\alpha^3) + e(\alpha^3) = e(\alpha^3) = e_i\alpha^{3i} + e_j\alpha^{3j}$　式 2-4

（一般のhに対しては、 $S_h = e_i\alpha^{hi} + e_j\alpha^{hj} = e_i(\alpha^i)^h + e_j(\alpha^j)^h$である。）
σ_0, σ_1 を係数とする多項式（誤り位置多項式）$\sigma(x)$ を以下のように定義する。
$\sigma(x) = (x - \alpha^i)(x - \alpha^j) = x^2 + \sigma_1 x + \sigma_0$ 式 2-5
この式に、$x = \alpha^i$、$x = \alpha^j$ を代入する。
$0 = \alpha^{2i} + \sigma_1\alpha^i + \sigma_0$ 式 2-6
$0 = \alpha^{2j} + \sigma_1\alpha^j + \sigma_0$ 式 2-7

式 2-6 の左右辺を入れ替え、両辺に、$e_i(\alpha^i)^h$をかける。
$e_i(\alpha^i)^h\alpha^{2i} + e_i(\alpha^i)^h\sigma_1\alpha^i + e_i(\alpha^i)^h\sigma_0$=0
$e_i(\alpha^i)^{h+2} + e_i(\alpha^i)^{h+1}\sigma_1 + e_i(\alpha^i)^h\sigma_0$=0　　式 2-8
式 2-7 の左右辺を入れ替え、両辺に、$e_j(\alpha^j)^h$をかける。
$e_j(\alpha^j)^h\alpha^{2j} + e_j(\alpha^j)^h\sigma_1\alpha^j + e_j(\alpha^j)^h\sigma_0$=0
$e_j(\alpha^j)^{h+2} + e_j(\alpha^j)^{h+1}\sigma_1 + e_j(\alpha^j)^h\sigma_0$=0　　式 2-9

式 2-8、2-9 の両辺を縦に加算して、整理する。

$$\left[e_i(\alpha^i)^{h+2} + e_j(\alpha^j)^{h+2}\right] + \sigma_1\left[e_i(\alpha^i)^{h+1} + e_j(\alpha^j)^{h+1}\right] + \sigma_0\left[e_i(\alpha^i)^h + e_j(\alpha^j)^h\right] = 0$$

この式は、
$S_{h+2} + \sigma_1 S_{h+1} + \sigma_0 S_h = 0$ を意味している。

$h = 0, 1$に対して計算すると、以下となる。
$h = 0$　$S_2 + \sigma_1 S_1 + \sigma_0 S_0 = 0$　式 2-10
$h = 1$　$S_3 + \sigma_1 S_2 + \sigma_0 S_1 = 0$　式 2-11

復号の手順
ステップ１）式 2-1～2-4（の前半部；$S_h = v(\alpha^h)$）により、S_0～S_3 を求める。
ステップ２）式 2-10～2-11 により、σ_0、σ_1 を求める。
ステップ３）式 2-5 を用いて、α^i、α^j を求める。
　つまり、$\sigma(x) = x^2 + \sigma_1 x + \sigma_0 = (x - \alpha^i)(x - \alpha^j)$ となるように因数分解して、α^i、α^j を定め、i、jを求める。（式 2-6～2-7 から求めていることと同じ）
ステップ４）式 2-1～2-2 により、e_i、e_j を求める。
　$h = 0$　$S_0 = v(\alpha^0) = v(1) = u(1) + e(1) = e(1) = e_i + e_j$　式 2-1
　$h = 1$　$S_1 = v(\alpha^1) = v(\alpha) = u(\alpha) + e(\alpha) = e(\alpha) = e_i\alpha^i + e_j\alpha^j$　式 2-2
　なお、式 2-3, 2-4 は使わないが満たされる。
ステップ５）i、j、e_i、e_j から、誤り多項式 $e(x) = e_i x^i + e_j x^j$ を決定し、$u(x) = v(x) - e(x)$ で誤り訂正を行う。

３）具体的な例
３－１）準備
以下では、$n = 2^m - 1$、$l = 0$、$m = 3$ を考える。

$n = 2^m - 1 = 7$　（7 バイトに注意）

$GF(2)$の上の原始多項式$p(x)$を$p(x) = x^3 + x + 1$とし、この根をαとする。すなわち$\alpha^3 + \alpha + 1 = 0$。

多項式	ベクトル表現	αべき表現	
0	000	0	
1	001	1	$=\alpha^0$
x	010	α	$=\alpha^1$
$x+1$	011	$\alpha+1$	$=\alpha^3$
x^2	100	α^2	$=\alpha^2$
x^2+1	101	α^2+1	$=\alpha^6$
x^2+x	110	$\alpha^2+\alpha$	$=\alpha^4$
x^2+x+1	111	$\alpha^2+\alpha+1$	$=\alpha^5$

拡大体は$GF(2^3) = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$

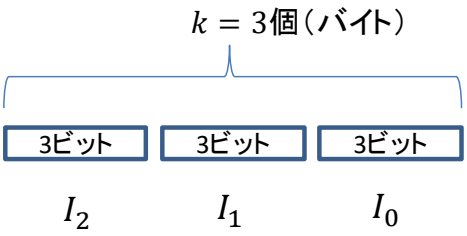
３－２）(7,3)符号　　$m = 3, n = 7, k = 3, t = 2$

①情報ビット系列を 3 ビット$(m = 3)$ずつの 3 個$(k = 3)$のブロック（バイト）に分割する。例えば

情報ビット　001 010 100

情報バイト　1　α^1　α^2

バイト番号　1　2　3



②情報バイトを多項式で表現する。

$I(y) = I_{k-1}y^{k-1} + \cdots + I_1 y + I_0 = 1y^2 + \alpha^1 y^1 + \alpha^2 y^0$

③生成多項式を求める。

$G(y) = \prod_{i=l}^{l+2t-1}(y - \alpha^i) = \prod_{i=0}^{3}(y - \alpha^i) = (y - \alpha^0)(y - \alpha^1)(y - \alpha^2)(y - \alpha^3)$

$= y^4 + \alpha^2 y^3 + \alpha^5 y^2 + \alpha^5 y^1 + \alpha^6$

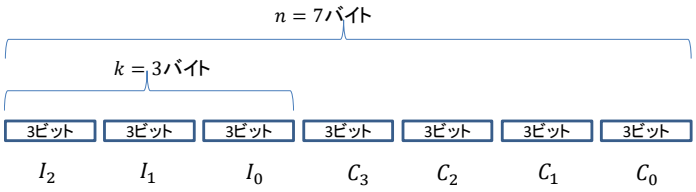
④情報多項式$I(y) * y^{n-k}$を生成多項式$G(y)$　で除算した余りを求める。

$I(y) = I_{k-1}y^{k-1} + \cdots I_1 y + I_0 = 1y^2 + \alpha^1 y^1 + \alpha^2 y^0$

$r(y) = I(y) * y^{n-k} \; mod \; G(y) = (1y^2 + \alpha^1 y^1 + \alpha^2 y^0) * y^4 \; mod \; y^4 + \alpha^2 y^3 + \alpha^5 y^2 + \alpha^5 y^1 + \alpha^6$

$= \alpha^4 y^3 + \alpha^6 y^2 + \alpha^5 y + \alpha^3$

⑤以上より



情報ビット	001	010	100				
情報バイト	1	α^1	α^2				
符号化後	1	α^1	α^2	α^4	α^6	α^5	α^3
RS 符号語	001	010	100	110	101	111	011
バイト番号	1	2	3	4	5	6	7

３－３）誤りがある受信語の誤り訂正

$u(x)$　を送信し、2 バイト誤り　$e(x)$　が生じた　$v(x)$　を受信したとする。

送信語　$u(x) = 1x^6 + \alpha^1 x^5 + \alpha^2 x^4 + \alpha^4 x^3 + \alpha^6 x^2 + \alpha^5 x + \alpha^3$

受信語　$v(x) = 1x^6 + 0x^5 + \alpha^2 x^4 + \alpha^5 x^3 + \alpha^6 x^2 + \alpha^5 x + \alpha^3$

誤り多項式　$e(x) = e_i x^i + e_j x^j$　　iバイト目の誤りe_i、jバイト目の誤りe_j

ステップ１）式 2-1～2-4（の前半部；$S_h = v(\alpha^h)$）により、S_0～S_3　を求める。

$S_0 = v(1) = 1 + 0 + \alpha^2 + \alpha^5 + \alpha^6 + \alpha^5 + \alpha^3 = (001) + (100) + (101) + (011) = (011) = \alpha^3$

$S_1 = v(\alpha) = 1\alpha^6 + 0 + \alpha^2\alpha^4 + \alpha^5\alpha^3 + \alpha^6\alpha^2 + \alpha^5\alpha + \alpha^3 = \alpha^6 + \alpha^6 + \alpha^8 + \alpha^8 + \alpha^6 + \alpha^3 = \alpha^6 + \alpha^3 =$
$(101) + (011) = (110) = \alpha^4$
$S_2 = v(\alpha^2) = 1\alpha^{12} + 0 + \alpha^2\alpha^8 + \alpha^5\alpha^6 + \alpha^6\alpha^4 + \alpha^5\alpha^2 + \alpha^3 = \alpha^{12} + \alpha^{10} + \alpha^{11} + \alpha^{10} + \alpha^7 + \alpha^3 =$
$\alpha^5 + \alpha^4 + 1 + \alpha^3 = (111) + (110) + (001) + (011) = (011) = \alpha^3$
$S_3 = v(\alpha^3) = 1\alpha^{18} + 0 + \alpha^2\alpha^{12} + \alpha^5\alpha^9 + \alpha^6\alpha^6 + \alpha^5\alpha^3 + \alpha^3 = \alpha^{18} + \alpha^{14} + \alpha^{14} + \alpha^{12} + \alpha^8 + \alpha^3 =$
$\alpha^4 + \alpha^5 + \alpha^1 + \alpha^3 = (110) + (111) + (010) + (011) = (000) = 0$

ステップ２）式 2-10～2-11 により、σ_0、σ_1　を求める。
$S_2 + \sigma_1 S_1 + \sigma_0 S_0 = 0$　　式 2-10
　$\alpha^3 + \sigma_1\alpha^4 + \sigma_0\alpha^3 = 0$　　式 2-2-1
$S_3 + \sigma_1 S_2 + \sigma_0 S_1 = 0$　　式 2-11
　$0 + \sigma_1\alpha^3 + \sigma_0\alpha^4 = 0$　　式 2-2-2
式 2-2-2 より、　$\sigma_1 + \sigma_0\alpha^1 = 0$ よって、$\sigma_1 = \sigma_0\alpha^1$
これを式 2-2-1 に入れて、
$\alpha^3 + \sigma_0\alpha^1\alpha^4 + \sigma_0\alpha^3 = 0$
$\alpha^3 + \sigma_0(\alpha^5 + \alpha^3) = 0$
　$\alpha^5 + \alpha^3 = (111) + (011) = (100) = \alpha^2$　より
$\alpha^3 + \sigma_0\alpha^2 = 0$　　よって、　$\sigma_0 = \alpha^1$
$\sigma_1 = \sigma_0\alpha^1 = \alpha^2$
以上より、$\sigma_0 = \alpha^1$　　$\sigma_1 = \alpha^2$

ステップ３）式 2-5 を用いて、α^i、α^j　を求める。
　つまり、$\sigma(x) = x^2 + \sigma_1 x + \sigma_0 = (x - \alpha^i)(x - \alpha^j)$ となるように因数分解して、α^i、α^j　を定め、i、jを求める。
　$\sigma(x) = x^2 + \sigma_1 x + \sigma_0 = x^2 + \alpha^2 x + \alpha^1 = (x + \alpha^3)(x + \alpha^5)$
　（xにα　のべき乗を入れて確認する。α^3を入れると 0 となることが分かれば、$\alpha^3 * y = \alpha^1$　から、$y = \alpha^5$ と求められる。その後、$\alpha^3 + \alpha^5 = (011) + (111) = (100) = \alpha^2$　を確認する。）
　これより、$\alpha^i = \alpha^3$、$\alpha^j = \alpha^5$　となり、$i = 3$、$j = 5$ が決定される。

ステップ４）式 2-1～2-2 により、e_i、e_j　を求める。
　　$S_0 = v(\alpha^0) = v(1) = u(1) + e(1) = e(1) = e_i + e_j = e_3 + e_5 = \alpha^3$　　式 2-4-1
　　$S_1 = v(\alpha^1) = v(\alpha) = u(\alpha) + e(\alpha) = e(\alpha) = e_i\alpha^i + e_j\alpha^j = e_3\alpha^3 + e_5\alpha^5 = \alpha^4$　式 2-4-2
式 2-4-1 より、$e_5 = \alpha^3 + e_3$　これを式 2-4-2 に入れる。
$e_3\alpha^3 + (\alpha^3 + e_3)\alpha^5 = \alpha^4$
$(\alpha^3 + \alpha^5)e_3 + \alpha^8 = \alpha^4$
$\alpha^3 + \alpha^5 = (011) + (111) = (100) = \alpha^2$
$\alpha^8 + \alpha^4 = \alpha^1 + \alpha^4 = (010) + (110) = (100) = \alpha^2$
よって
$\alpha^2 e_3 = \alpha^2$　　$e_3 = 1$
$e_5 = \alpha^3 + e_3 = \alpha^3 + 1 = (011) + (001) = (010) = \alpha^1$

以上より、$e_3 = 1$　　$e_5 = \alpha$

ステップ５）i、j、e_i、e_j　から、誤り多項式　$e(x) = e_i x^i + e_j x^j$　を決定し、$u(x) = v(x) - e(x)$ で誤り訂正を行う。

誤り多項式　$e(x) = e_i x^i + e_j x^j = e_3 x^3 + e_5 x^5 = 1x^3 + \alpha x^5$

$v(x) = 1x^6 + 0x^5 + \alpha^2 x^4 + \alpha^5 x^3 + \alpha^6 x^2 + \alpha^5 x + \alpha^3$

$u(x) = v(x) - e(x) = (1x^6 + 0x^5 + \alpha^2 x^4 + \alpha^5 x^3 + \alpha^6 x^2 + \alpha^5 x + \alpha^3) - (1x^3 + \alpha x^5)$

$= 1x^6 + (0 + \alpha^1)x^5 + \alpha^2 x^4 + (\alpha^5 + 1)x^3 + \alpha^6 x^2 + \alpha^5 x + \alpha^3$

$= 1x^6 + \alpha^1 x^5 + \alpha^2 x^4 + \alpha^4 x^3 + \alpha^6 x^2 + \alpha^5 x + \alpha^3$

$\because 1 + \alpha^5 = (001) + (111) = (110) = \alpha^4$

以上より、正しく復号された。

（以下、式 2-3, 2-4 が満たされるか確認する。

$h = 2$　$S_2 = v(\alpha^2) = u(\alpha^2) + e(\alpha^2) = e(\alpha^2) = e_i \alpha^{2i} + e_j \alpha^{2j}$　式 2-3

$h = 3$　$S_3 = v(\alpha^3) = u(\alpha^3) + e(\alpha^3) = e(\alpha^3) = e_i \alpha^{3i} + e_j \alpha^{3j}$　式 2-4

$S_2 = v(\alpha^2) = e(\alpha^2) = e_i \alpha^{2i} + e_j \alpha^{2j} = e_3 \alpha^6 + e_5 \alpha^{10} = 1\alpha^6 + \alpha^1 \alpha^{10} = \alpha^6 + \alpha^{11} = \alpha^6 + \alpha^4 = (101) + (110) = (011) = \alpha^3$

$S_2 = v(\alpha^2) = 1\alpha^{12} + 0\alpha^{10} + \alpha^2 \alpha^8 + \alpha^5 \alpha^6 + \alpha^6 \alpha^4 + \alpha^5 \alpha^2 + \alpha^3 = \alpha^{12} + \alpha^{10} + \alpha^{11} + \alpha^{10} + \alpha^7 + \alpha^3 = \alpha^5 + \alpha^4 + 1 + \alpha^3 = (111) + (110) + (001) + (011) = (011) = \alpha^3$

$S_3 = v(\alpha^3) = e(\alpha^3) = e_i \alpha^{3i} + e_j \alpha^{3j} = e_3 \alpha^9 + e_5 \alpha^{15} = 1\alpha^9 + \alpha^1 \alpha^{15} = \alpha^9 + \alpha^{16} = \alpha^2 + \alpha^2 = 0$

$S_3 = v(\alpha^3) = 1\alpha^{18} + 0\alpha^{15} + \alpha^2 \alpha^{12} + \alpha^5 \alpha^9 + \alpha^6 \alpha^6 + \alpha^5 \alpha^3 + \alpha^3 = \alpha^{18} + \alpha^{14} + \alpha^{14} + \alpha^{12} + \alpha^8 + \alpha^3 = \alpha^4 + \alpha^5 + \alpha^1 + \alpha^3 = (110) + (111) + (010) + (011) = (000) = 0$

以上より、式 2-3, 2-4 が満たされていることが確認できる。）

―――Microjamjar　で確認する。

http://www.ujamjar.com/demo/ocaml/2014/06/18/reed-solomon-demo.html

確認）３次の例　(7, 3)符号

m=3, t=2

Primitive polynomial 11 = (1011) = $x^3 + x + 1$　　Primitive element=2

Initial root b =0　（生成多項式の１のこと）

情報ビット　001 010 100　　[1 2 4]

Message 4 2 1　　<- 逆順に入れる

誤りビット　000 010 000 001 000 000 000 [0 2 0 1 0 0 0]

$\because 0 - \alpha^1 = (000) + (010) = (010) = \alpha^1$　　$\alpha^5 - \alpha^4 = (111) + (110) = (001) = \alpha^0$

Errors 0 0 0 1 0 2 0　<- 逆順に入れる

とし、calculate を押すと、

Code word $1x^6 + 2x^5 + 4x^4 + 6x^3 + 5x^2 + 7x + 3$

Received code word $1x^6 + 0x^5 + 4x^4 + 7x^3 + 5x^2 + 7x + 3$

Syndromes　$S_0 = \alpha^3 = 3$　　$S_1 = \alpha^4 = 6$　　$S_2 = \alpha^3 = 3$　　$S_3 = 0 = 0$

となり、シンドロームを確認できる。そして、Euclid, Berlekamp-massey, Error-locator, Chein search, Forney 等が表示されたあと、

Corrected polynomial $1x^6 + 2x^5 + 4x^4 + 6x^3 + 5x^2 + 7x + 3$

が得られ、

訂正後　001 010 100 110 101 111 011

1　α^1　α^2　α^4　α^6　α^5　α^3

$u(x) = 1x^6 + \alpha^1 x^5 + \alpha^2 x^4 + \alpha^4 x^3 + \alpha^6 x^2 + \alpha^5 x + \alpha^3$　と一致することが確認できる。

７．２．５　BCH と RS のまとめ

・生成多項式$g(x)$がポイント

・巡回符号：$g(x)$はx^n-1を整除する。

・情報記号多項式$I(x)$／生成多項式$g(x)$＝$A(x)$ 余り $r(x)$

$u(x)=I(x)\cdot x^m+r(x)$　$u(x)$は生成多項式$g(x)$で整除される。$u(x)$を送信する。

受信側は受信語$v(x)$が$g(x)$で整除されるかを検査

・$u(x)$が$g(x)$で整除される　＜－＞　$u(\alpha)=0$　　α：$g(x)$の根

$u(x)$が$g(x)$で整除されるから、$u(x)=X(x)g(x)$

αは$g(x)$の根なので、$u(\alpha)=X(\alpha)g(\alpha)$=0

・すべての符号語$u(x)$はαを根として持つ。根αを持つ符号語だけを使う。

・生成多項式$g(x)$

BCH の生成多項式（式 7.1.3.1）と RS の生成多項式（式 7.2.1）の違い。BCH は$GF(2)$上、RS は$GF(2^m)$上（mは検査バイト数）

・BCH と RS 練習問題　補足資料２

7．2．6　リード・ソロモン符号の追加例と計算方法

以下は暫定

1）RS 符号の例２

(15, 9)符号　$m=4, n=15, k=9, t=3$, 原始多項式が$p(x)=x^4+x+1$の場合

多項式表現	ベクトル表現	αべき乗表現	
0	0000	0	
1	0001	1	$=\alpha^0$
x	0010	α	$=\alpha^1$
$x+1$	0011	$\alpha+1$	$=\alpha^4$
x^2	0100	α^2	$=\alpha^2$
x^2+1	0101	α^2+1	$=\alpha^8$
x^2+x	0110	$\alpha^2+\alpha$	$=\alpha^5$
x^2+x+1	0111	$\alpha^2+\alpha+1$	$=\alpha^{10}$
x^3	1000	α^3	$=\alpha^3$
x^3+1	1001	α^3+1	$=\alpha^{14}$
x^3+x	1010	$\alpha^3+\alpha$	$=\alpha^9$
x^3+x+1	1011	$\alpha^3+\alpha+1$	$=\alpha^7$
x^3+x^2	1100	$\alpha^3+\alpha^2$	$=\alpha^6$
x^3+x^2+1	1101	$\alpha^3+\alpha^2+1$	$=\alpha^{13}$
x^3+x^2+x	1110	$\alpha^3+\alpha^2+\alpha$	$=\alpha^{11}$
x^3+x^2+x+1	1111	$\alpha^3+\alpha^2+\alpha+1$	$=\alpha^{12}$

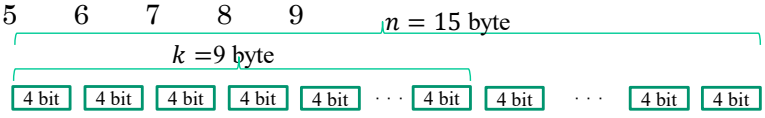
$GF(2^4)=\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}\}$

■例２　(15, 9)符号　$m=4, n=15, k=9, t=3$, 原始多項式が$p(x)=x^4+x+1$の場合

①情報ビット系列を 4 ビット$(m=4)$ずつの 9 個$(k=9)$のブロック（バイト）に分割する。例えば、

情報ビット　1010 0011 0011 1101 1110 0101 1101 1000 1010

情報バイト	α^9	α^4	α^4	α^{13}	α^{11}	α^8	α^{13}	α^3	α^9
バイト番号	1	2	3	4	5	6	7	8	9



②情報バイトを多項式で表現する。

$$I(y)=I_{k-1}y^{k-1}+\cdots I_1y+I_0$$
$$=\alpha^9y^8+\alpha^4y^7+\alpha^4y^6+\alpha^{13}y^5+\alpha^{11}y^4+\alpha^8y^3+\alpha^{13}y^2+\alpha^3y^1+\alpha^9$$

③生成多項式を求める。

$$G(y)=\prod_{i=l}^{l+2t-1}(y-\alpha^i)=\prod_{i=0}^{5}(y-\alpha^i)=(y-\alpha^0)(y-\alpha^1)(y-\alpha^2)(y-\alpha^3)(y-\alpha^4)(y-\alpha^5)$$
$$=y^6+\alpha^9y^5+\alpha^{12}y^4+\alpha^1y^3+\alpha^2y^2+\alpha^4y^1+\alpha^0$$

④情報多項式$I(y)*y^{n-k}$を生成多項式$G(y)$　で除算した余りを求める。

$$I(y)=I_{k-1}y^{k-1}+\cdots I_1y+I_0$$
$$=\alpha^9y^8+\alpha^4y^7+\alpha^4y^6+\alpha^{13}y^5+\alpha^{11}y^4+\alpha^8y^3+\alpha^{13}y^2+\alpha^3y^1+\alpha^9$$
$$r(y)=I(y)*y^{n-k}\ mod\ G(y)$$
$$=(\alpha^9y^8+\alpha^4y^7+\alpha^4y^6+\alpha^{13}y^5+\alpha^{11}y^4+\alpha^8y^3+\alpha^{13}y^2+\alpha^3y^1+\alpha^9)*y^6$$
$$mod\ y^6+\alpha^9y^5+\alpha^{12}y^4+\alpha^1y^3+\alpha^2y^2+\alpha^4y^1+\alpha^0$$
$$=\alpha^0y^5+\alpha^8y^4+\alpha^{14}y^3+\alpha^{11}y^2+\alpha^3y+\alpha^3$$

⑤以上より

情報ビット　1010 0011 0011 1101 1110 0101 1101 1000 1010

情報バイト	α^9	α^4	α^4	α^{13}	α^{11}	α^8	α^{13}	α^3	α^9

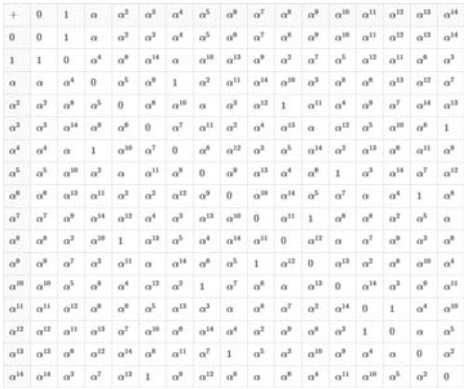
符号化後	α^9	α^4	α^4	α^{13}	α^{11}	α^8	α^{13}	α^3	α^9	α^0	α^8	α^{14}	α^{11}	α^3	α^3
RS 符号語	1010	0011	0011	1101	1110	0101	1101	1000	1010	0001	0101	1001	1110	1000	1000
バイト番号	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

となる。

剰余計算の方法１：ストレートな方法

```
                  9    7   13
                  ---------------------
0 9 12 1 2 4 0|9    4    4    13    11    8    13    3    9    x    x    x    x    x    x
              9   18   21   10    11   13     9
                  =3   =6
   ---------------------------------------------------------------
                  4+3  4+6   13+10  x   8+13  13+9
                  =7   =12   =9     x   =3    =10    3
                  7    16    19     8    9     11     7
                       =1    =4
   ---------------------------------------------------------------
                       12+1  9+4     8   3+9   10+11  3+7
                       =13   =14     8   =1    =14    =4   9

                                                  :（以下省略）
```



この計算には、GF(2^4)の加算表があると便利である。
例えば、https://hg.hatenablog.jp/entry/2018/03/11/011748　には上の表が掲載されている。
（表中の１はα^0であることに注意）

剰余計算の方法２：ユークリッド互除法を用いる

剰余計算の方法３：計算機を利用する。

１）カナダの Department of Electrical and Computer Engineering - University of New Brunswick のサイト

http://www.ee.unb.ca/cgi-bin/tervo/calc2.pl?num=10+3+3+13+14+5+13+8+10+0+0+0+0+0+0&den=1+10+15+2+4+3+1&f=d&p=4&d=1&y=1&m=1

このサイトでは、$GF(2^m)$上の計算を行える。

根のべき乗はベクトル表現を１０進で読んで入力する。

例：α^9 -> (1010) -> [10]

例２の計算

・情報多項式$I(y) * y^{n-k}$を生成多項式$G(y)$　で除算した余りを求める。

$r(y) = I(y) * y^{n-k} \ mod \ G(y)$

$= (\alpha^9 y^8 + \alpha^4 y^7 + \alpha^4 y^6 + \alpha^{13} y^5 + \alpha^{11} y^4 + \alpha^8 y^3 + \alpha^{13} y^2 + \alpha^3 y^1 + \alpha^9) * y^6$

$mod \ y^6 + \alpha^9 y^5 + \alpha^{12} y^4 + \alpha^1 y^3 + \alpha^2 y^2 + \alpha^4 y^1 + \alpha^0$

$= \alpha^1 y^5 + \alpha^1 y^4 + \alpha^7 y^3 + \alpha^3 y^2 + \alpha^{10} y + \alpha^{10}$

・　A 欄　$(\alpha^9 y^8 + \alpha^4 y^7 + \alpha^4 y^6 + \alpha^{13} y^5 + \alpha^{11} y^4 + \alpha^8 y^3 + \alpha^{13} y^2 + \alpha^3 y^1 + \alpha^9) y^6$

=> $(\alpha^9 \ \alpha^4 \ \alpha^4 \ \alpha^{13} \ \alpha^{11} \ \alpha^8 \ \alpha^{13} \ \alpha^3 \ \alpha^9 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0)$　=> [10 3 3 13 14 5 13 8 10 0 0 0 0 0 0]

・　B 欄　$y^6 + \alpha^9 y^5 + \alpha^{12} y^4 + \alpha^1 y^3 + \alpha^2 y^2 + \alpha^4 y^1 + \alpha^0$　=>　$(\alpha^0 \ \alpha^9 \ \alpha^{12} \ \alpha^1 \ \alpha^2 \ \alpha^4 \ \alpha^0)$

=> [1 10 15 2 4 3 1]

・　結果　[1 5 9 14 8 8] -> $\alpha^0\ \alpha^8\ \alpha^{14}\ \alpha^{11}\ \alpha^3\ \alpha^3$　-> $\alpha^0 y^5 + \alpha^8 y^4 + \alpha^{14} y^3 + \alpha^{11} y^2 + \alpha^3 y + \alpha^3$

・生成多項式も unb のサイトを使って計算できる。

$G(y) = \prod_{i=l}^{l+2t-1}(y - \alpha^i) = \prod_{i=0}^{5}(y - \alpha^i) = (y - \alpha^0)(y - \alpha^1)(y - \alpha^2)(y - \alpha^3)(y - \alpha^4)(y - \alpha^5)$

$= y^6 + \alpha^9 y^5 + \alpha^{12} y^4 + \alpha^1 y^3 + \alpha^2 y^2 + \alpha^4 y^1 + \alpha^0$

unb のサイトで

$(y - \alpha^0)$ => [1 1]、$(y - \alpha^1)$ => [1 2] 、$(y - \alpha^2)$ => [1 4] 、$(y - \alpha^3)$ => [1 8]

$(y - \alpha^4)$ => [1 3] 、$(y - \alpha^5)$ => [1 6] として順次かけ算を行う。

結果　[1 10 15 2 4 3 1] => $\alpha^0\ \alpha^9\ \alpha^{12}\ \alpha^1\ \alpha^2\ \alpha^4\ \alpha^0$

２）microjamjar

RS 符号の符号化、復号をデモンストレーションしている。

http://www.ujamjar.com/demo/ocaml/2014/06/18/reed-solomon-demo.html

確認１）３次の例　(7, 3)符号

$I(y) = I_{k-1} y^{k-1} + \cdots + I_1 y + I_0 = 1y^2 + \alpha^1 y^1 + \alpha^2 y^0$

情報ビット 001 010 100

[1 2 4]

m=3, t=2

Primitive polynomial 11 = (1011) = x^3+x+1　　Primitive element=2

Initial root b =0　(l のこと)

Message 4 2 1　　<- 逆順に入れる

Errors　全て 0

とし、calculate を押すと、

$1x^6 + 2x^5 + 4x^4 + 6x^3 + 5x^2 + 7x + 3$

が得られる。すなわち

RS 符号語 001　010　100　110　101　111　011

と一致する。

確認２）４次の例１　(15, 11)符号

$I(y) = I_{k-1} y^{k-1} + \cdots I_1 y + I_0$

$= \alpha^9 y^{10} + \alpha^4 y^9 + \alpha^4 y^8 + \alpha^{13} y^7 + \alpha^{11} y^6 + \alpha^8 y^5 + \alpha^{13} y^4 + \alpha^3 y^3 + \alpha^9 y^2 + \alpha^8 y^1 + 0y^0$

情報ビット 1010 0011 0011 1101 1110 0101 1101 1000 1010 0101 0000

[10 3 3 13 14 5 13 8 10 5 0]

m=4, t=2

Primitive polynomial 19 = (10011) =x^4+x+1　　Primitive element=2

Initial root b =0　(l のこと)

Message　0 5 10 8 13 5 14 13 3 3 10　　<- 逆順に入れる

Errors　全て 0
とし、calculate を押すと、
10x14+3x13+3x12+13x11+14x10+5x9+13x8+8x7+10x6+5x5+13x3+13x2+x+7
が得られる。すなわち
　RS 符号語　1010 0011 0011 1101 1110 0101 1101 1000 1010 0101 0000 1101 1101 0001 0111
と一致する。

確認３）4 次の例２　(15, 9)符号

$$I(y) = I_{k-1}y^{k-1} + \cdots I_1 y + I_0$$
$$= \alpha^9 y^8 + \alpha^4 y^7 + \alpha^4 y^6 + \alpha^{13} y^5 + \alpha^{11} y^4 + \alpha^8 y^3 + \alpha^{13} y^2 + \alpha^3 y^1 + \alpha^9$$

　情報ビット 1010 0011 0011 1101 1110 0101 1101 1000 1010
[10 3 3 13 14 5 13 8 10]

m=4, t=3
Primitive polynomial 19 = (10011) =x^4+x+1　　Primitive element=2
Initial root b =0　(1 のこと)
Message 10 8 13 5 14 13 3 3 10　　<- 逆順に入れる
Errors　全て 0
とし、calculate を押すと、
10x14+3x13+3x12+13x11+14x10+5x9+13x8+8x7+10x6+x5+5x4+9x3+14x2+8x+8
が得られる。すなわち
　RS 符号語　1010 0011 0011 1101 1110 0101 1101 1000 1010 0001 0101 1001 1110 1000 1000
と一致する。

７．２．７　３誤り訂正の例

「７．２．６　リード・ソロモン符号の追加例と計算方法」で取り上げた RS(15, 9)符号を元にする

３誤りの例１

１）RS 符号の例２

(15, 9)符号　$m=4, n=15, k=9, t=3$, 原始多項式が$p(x)=x^4+x+1$の場合

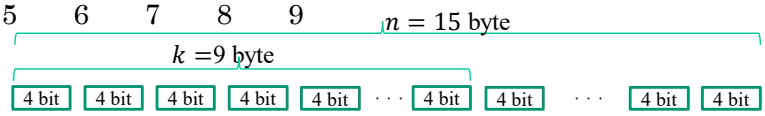
多項式表現	ベクトル表現	αべき乗表現	
0	0000	0	
1	0001	1	$=\alpha^0$
x	0010	α	$=\alpha^1$
$x+1$	0011	$\alpha+1$	$=\alpha^4$
x^2	0100	α^2	$=\alpha^2$
x^2+1	0101	α^2+1	$=\alpha^8$
x^2+x	0110	$\alpha^2+\alpha$	$=\alpha^5$
x^2+x+1	0111	$\alpha^2+\alpha+1$	$=\alpha^{10}$
x^3	1000	α^3	$=\alpha^3$
x^3+1	1001	α^3+1	$=\alpha^{14}$
x^3+x	1010	$\alpha^3+\alpha$	$=\alpha^9$
x^3+x+1	1011	$\alpha^3+\alpha+1$	$=\alpha^7$
x^3+x^2	1100	$\alpha^3+\alpha^2$	$=\alpha^6$
x^3+x^2+1	1101	$\alpha^3+\alpha^2+1$	$=\alpha^{13}$
x^3+x^2+x	1110	$\alpha^3+\alpha^2+\alpha$	$=\alpha^{11}$
x^3+x^2+x+1	1111	$\alpha^3+\alpha^2+\alpha+1$	$=\alpha^{12}$

$GF(2^4)=\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}\}$

■例２　(15, 9)符号　$m=4, n=15, k=9, t=3$, 原始多項式が$p(x)=x^4+x+1$の場合

①情報ビット系列を 4 ビット$(m=4)$ずつの 9 個$(k=9)$のブロック（バイト）に分割する。例えば、

情報ビット	1010	0011	0011	1101	1110	0101	1101	1000	1010
情報バイト	α^9	α^4	α^4	α^{13}	α^{11}	α^8	α^{13}	α^3	α^9
バイト番号	1	2	3	4	5	6	7	8	9



②情報バイトを多項式で表現する。

$$I(y)=I_{k-1}y^{k-1}+\cdots I_1y+I_0$$
$$=\alpha^9y^8+\alpha^4y^7+\alpha^4y^6+\alpha^{13}y^5+\alpha^{11}y^4+\alpha^8y^3+\alpha^{13}y^2+\alpha^3y^1+\alpha^9$$

③生成多項式を求める。

$$G(y)=\prod_{i=l}^{l+2t-1}(y-\alpha^i)=\prod_{i=0}^{5}(y-\alpha^i)=(y-\alpha^0)(y-\alpha^1)(y-\alpha^2)(y-\alpha^3)(y-\alpha^4)(y-\alpha^5)$$
$$=y^6+\alpha^9y^5+\alpha^{12}y^4+\alpha^1y^3+\alpha^2y^2+\alpha^4y^1+\alpha^0$$

④情報多項式$I(y)*y^{n-k}$を生成多項式$G(y)$　で除算した余りを求める。

$$I(y)=I_{k-1}y^{k-1}+\cdots I_1y+I_0$$
$$=\alpha^9y^8+\alpha^4y^7+\alpha^4y^6+\alpha^{13}y^5+\alpha^{11}y^4+\alpha^8y^3+\alpha^{13}y^2+\alpha^3y^1+\alpha^9$$
$$r(y)=I(y)*y^{n-k}\ mod\ G(y)$$
$$=(\alpha^9y^8+\alpha^4y^7+\alpha^4y^6+\alpha^{13}y^5+\alpha^{11}y^4+\alpha^8y^3+\alpha^{13}y^2+\alpha^3y^1+\alpha^9)*y^6$$
$$mod\ y^6+\alpha^9y^5+\alpha^{12}y^4+\alpha^1y^3+\alpha^2y^2+\alpha^4y^1+\alpha^0$$
$$=\alpha^0y^5+\alpha^8y^4+\alpha^{14}y^3+\alpha^{11}y^2+\alpha^3y+\alpha^3$$

⑤以上より

情報ビット　1010 0011 0011 1101 1110 0101 1101 1000 1010

情報バイト　α^9　α^4　α^4　α^{13}　α^{11}　α^8　α^{13}　α^3　α^9

符号化後　α^9　α^4　α^4　α^{13}　α^{11}　α^8　α^{13}　α^3　α^9　α^0　α^8　α^{14}　α^{11}　α^3　α^3

RS 符号語　1010 0011 0011 1101 1110 0101 1101 1000 1010 0001 0101 1001 1110 1000 1000

バイト番号　1　2　3　4　5　6　7　8　9　10　11　12　13　14　15

となる。

⑥３誤り訂正

$u(x)$ を送信し、3バイト誤り $e(x)$ が生じた $v(x)$ を受信したとする。

送信語

$$u(x) = \alpha^9x^{14} + \alpha^4x^{13} + \alpha^4x^{12} + \alpha^{13}x^{11} + \alpha^{11}x^{10} + \alpha^8x^9 + \alpha^{13}x^8 + \alpha^3x^7 + \alpha^9x^6 + \alpha^0x^5 + \alpha^8x^4 + \alpha^{14}x^3 + \alpha^{11}x^2 + \alpha^3x + \alpha^3$$

受信語

$$v(x) = \alpha^9x^{14} + 0x^{13} + 0x^{12} + \alpha^{13}x^{11} + 0x^{10} + \alpha^8x^9 + \alpha^{13}x^8 + \alpha^3x^7 + \alpha^9x^6 + \alpha^0x^5 + \alpha^8x^4 + \alpha^{14}x^3 + \alpha^{11}x^2 + \alpha^3x + \alpha^3$$

誤り多項式　$e(x) = e_ix^i + e_jx^j + e_kx^k$

iバイト目の誤りe_i、jバイト目の誤りe_j、kバイト目の誤りe_k

ステップ１）式 2-1～2-4（の前半部；$S_h = v(\alpha^h)$）を拡張して、S_0～S_5　を求める。

$$S_0 = v(1) = \alpha^9 + 0 + 0 + \alpha^{13} + 0 + \alpha^8 + \alpha^{13} + \alpha^3 + \alpha^9 + \alpha^0 + \alpha^8 + \alpha^{14} + \alpha^{11} + \alpha^3 + \alpha^3$$
$$= \alpha^3 + \alpha^0 + \alpha^{14} + \alpha^{11} = (1000) + (0001) + (1001) + (1110) = (1110) = \alpha^{11}$$

$$S_1 = v(\alpha) = \alpha^9\alpha^{14} + 0\alpha^{13} + 0\alpha^{12} + \alpha^{13}\alpha^{11} + 0\alpha^{10} + \alpha^8\alpha^9 + \alpha^{13}\alpha^8 + \alpha^3\alpha^7 + \alpha^9\alpha^6 + \alpha^0\alpha^5 + \alpha^8\alpha^4 + \alpha^{14}\alpha^3 + \alpha^{11}\alpha^2 + \alpha^3\alpha^1 + \alpha^3$$
$$= \alpha^{23} + \alpha^{24} + \alpha^{17} + \alpha^{21} + \alpha^{10} + \alpha^{15} + \alpha^5 + \alpha^{12} + \alpha^{17} + \alpha^{13} + \alpha^4 + \alpha^3$$
$$= \alpha^8 + \alpha^9 + \alpha^6 + \alpha^{10} + \alpha^0 + \alpha^5 + \alpha^{12} + \alpha^{13} + \alpha^4 + \alpha^3$$
$$= (0101) + (1010) + (1100) + (0111) + (0001) + (0110) + (1111) + (1101) + (0011) + (1000) = (1010) = \alpha^9$$

$$S_2 = v(\alpha^2) = \alpha^9\alpha^{28} + 0\alpha^{26} + 0\alpha^{24} + \alpha^{13}\alpha^{22} + 0\alpha^{20} + \alpha^8\alpha^{18} + \alpha^{13}\alpha^{16} + \alpha^3\alpha^{14} + \alpha^9\alpha^{12} + \alpha^0\alpha^{10} + \alpha^8\alpha^8 + \alpha^{14}\alpha^6 + \alpha^{11}\alpha^4 + \alpha^3\alpha^2 + \alpha^3$$
$$= \alpha^{37} + \alpha^{35} + \alpha^{26} + \alpha^{29} + \alpha^{17} + \alpha^{21} + \alpha^{10} + \alpha^{16} + \alpha^{20} + \alpha^{15} + \alpha^5 + \alpha^3$$
$$= \alpha^7 + \alpha^5 + \alpha^{11} + \alpha^{14} + \alpha^2 + \alpha^6 + \alpha^{10} + \alpha^1 + \alpha^5 + \alpha^0 + \alpha^5 + \alpha^3$$
$$= (1011) + (1110) + (1001) + (0100) + (1100) + (0111) + (0010) + (0001) + (0110) + (1000) = (1110) = \alpha^{11}$$

$$S_3 = v(\alpha^3) = \alpha^9\alpha^{42} + 0\alpha^{39} + 0\alpha^{36} + \alpha^{13}\alpha^{33} + 0\alpha^{30} + \alpha^8\alpha^{27} + \alpha^{13}\alpha^{24} + \alpha^3\alpha^{21} + \alpha^9\alpha^{18} + \alpha^0\alpha^{15} + \alpha^8\alpha^{12} + \alpha^{14}\alpha^9 + \alpha^{11}\alpha^6 + \alpha^3\alpha^3 + \alpha^3$$
$$= \alpha^{51} + \alpha^{46} + \alpha^{35} + \alpha^{37} + \alpha^{24} + \alpha^{27} + \alpha^{15} + \alpha^{20} + \alpha^{23} + \alpha^{17} + \alpha^6 + \alpha^3$$
$$= \alpha^6 + \alpha^1 + \alpha^5 + \alpha^7 + \alpha^9 + \alpha^{12} + \alpha^0 + \alpha^5 + \alpha^8 + \alpha^2 + \alpha^6 + \alpha^3$$
$$= (0010) + (1011) + (1010) + (1111) + (0001) + (0101) + (0100) + (1000)$$
$$= (0100) = \alpha^2$$

$$S_4 = v(\alpha^4) = \alpha^9\alpha^{56} + 0\alpha^{52} + 0\alpha^{48} + \alpha^{13}\alpha^{44} + 0\alpha^{40} + \alpha^8\alpha^{36} + \alpha^{13}\alpha^{32} + \alpha^3\alpha^{28} + \alpha^9\alpha^{24} + \alpha^0\alpha^{20}$$
$$+ \alpha^8\alpha^{16} + \alpha^{14}\alpha^{12} + \alpha^{11}\alpha^8 + \alpha^3\alpha^4 + \alpha^3$$
$$= \alpha^{65} + \alpha^{57} + \alpha^{44} + \alpha^{45} + \alpha^{31} + \alpha^{33} + \alpha^{20} + \alpha^{24} + \alpha^{26} + \alpha^{19} + \alpha^7 + \alpha^3$$
$$= \alpha^5 + \alpha^{12} + \alpha^{14} + \alpha^0 + \alpha^1 + \alpha^3 + \alpha^5 + \alpha^9 + \alpha^{11} + \alpha^4 + \alpha^7 + \alpha^3$$
$$= (1111) + (1001) + (0001) + (0010) + (1010) + (1110) + (0011) + (1011)$$
$$= (1001) = \alpha^{14}$$
$$S_5 = v(\alpha^5) = \alpha^9\alpha^{70} + 0\alpha^{65} + 0\alpha^{60} + \alpha^{13}\alpha^{55} + 0\alpha^{50} + \alpha^8\alpha^{45} + \alpha^{13}\alpha^{40} + \alpha^3\alpha^{35} + \alpha^9\alpha^{30} + \alpha^0\alpha^{25}$$
$$+ \alpha^8\alpha^{20} + \alpha^{14}\alpha^{15} + \alpha^{11}\alpha^{10} + \alpha^3\alpha^5 + \alpha^3$$
$$= \alpha^{79} + \alpha^{68} + \alpha^{53} + \alpha^{53} + \alpha^{38} + \alpha^{39} + \alpha^{25} + \alpha^{28} + \alpha^{29} + \alpha^{21} + \alpha^8 + \alpha^3$$
$$= \alpha^4 + \alpha^8 + \alpha^8 + \alpha^9 + \alpha^{10} + \alpha^{13} + \alpha^{14} + \alpha^6 + \alpha^8 + \alpha^3$$
$$= (0011) + (1010) + (0111) + (1101) + (1001) + (1100) + (0101) + (1000)$$
$$= (1011) = \alpha^7$$

以上より、$S_0 = \alpha^{11}$、$S_1 = \alpha^9$、$S_2 = \alpha^{11}$、$S_3 = \alpha^2$、$S_4 = \alpha^{14}$、$S_5 = \alpha^7$
（microjamjar で確認済み）

ステップ２）式 2-10～2-11 を拡張した以下の式により、σ_0、σ_1、σ_2　を求める。
$S_{h+3} + \sigma_2 S_{h+2} + \sigma_1 S_{h+1} + \sigma_0 S_h = 0$

$h = 0, 1, 2$に対して計算すると、以下となる。
$h = 0$　$S_3 + \sigma_2 S_2 + \sigma_1 S_1 + \sigma_0 S_0 = 0$
$h = 1$　$S_4 + \sigma_2 S_3 + \sigma_1 S_2 + \sigma_0 S_1 = 0$
$h = 2$　$S_5 + \sigma_2 S_4 + \sigma_1 S_3 + \sigma_0 S_2 = 0$

$S_3 + \sigma_2 S_2 + \sigma_1 S_1 + \sigma_0 S_0 = 0$　　式 2-10 相当
　$\alpha^2 + \sigma_2\alpha^{11} + \sigma_1\alpha^9 + \sigma_0\alpha^{11} = 0$　　式 x-2-1
$S_4 + \sigma_2 S_3 + \sigma_1 S_2 + \sigma_0 S_1 = 0$　　式 2-10 相当
　$\alpha^{14} + \sigma_2\alpha^2 + \sigma_1\alpha^{11} + \sigma_0\alpha^9 = 0$　　式 x-2-2
$S_5 + \sigma_2 S_4 + \sigma_1 S_3 + \sigma_0 S_2 = 0$　　式 2-10 相当
　$\alpha^7 + \sigma_2\alpha^{14} + \sigma_1\alpha^2 + \sigma_0\alpha^{11} = 0$　　式 x-2-3

式 x-2-1 より
$\sigma_2\alpha^{11} = \alpha^2 + \sigma_1\alpha^9 + \sigma_0\alpha^{11} = \alpha^{17} + \sigma_1\alpha^{24} + \sigma_0\alpha^{11}$　よって、$\sigma_2 = \alpha^6 + \sigma_1\alpha^{13} + \sigma_0\alpha^0$　式 x-2-4

式 x-2-4 を式 x-2-2 に代入して、
　$\alpha^{14} + \sigma_2\alpha^2 + \sigma_1\alpha^{11} + \sigma_0\alpha^9 = \alpha^{14} + (\alpha^6 + \sigma_1\alpha^{13} + \sigma_0\alpha^0)\alpha^2 + \sigma_1\alpha^{11} + \sigma_0\alpha^9 = \alpha^{14} + \alpha^8 + \sigma_1\alpha^{15} +$
$\sigma_0\alpha^2 + \sigma_1\alpha^{11} + \sigma_0\alpha^9 = \alpha^6 + \sigma_1\alpha^{12} + \sigma_0\alpha^{11} = 0$　　式 x-2-5
　　$\because \alpha^{14} + \alpha^8 = (1001) + (0101) = (1100) = \alpha^6$
　　$\because \alpha^{15} + \alpha^{11} = \alpha^0 + \alpha^{11} = (0001) + (1110) = (1111) = \alpha^{12}$
　　$\because \alpha^2 + \alpha^9 = (0100) + (1010) = (1110) = \alpha^{11}$

式 x-2-4 を式 x-2-3 に代入して、

$\alpha^7+\sigma_2\alpha^{14}+\sigma_1\alpha^2+\sigma_0\alpha^{11}=\alpha^7+(\alpha^6+\sigma_1\alpha^{13}+\sigma_0\alpha^0)\alpha^{14}+\sigma_1\alpha^2+\sigma_0\alpha^{11}=\alpha^7+\alpha^{20}+\sigma_1\alpha^{27}+\sigma_0\alpha^{14}+\sigma_1\alpha^2+\sigma_0\alpha^{11}=\alpha^{13}+\sigma_1\alpha^7+\sigma_0\alpha^{10}=0$　式 x-2-6

$\because \alpha^7+\alpha^{20}=\alpha^7+\alpha^5=(1011)+(0110)=(1101)=\alpha^{13}$

$\because \alpha^{27}+\alpha^2=\alpha^{12}+\alpha^2=(1111)+(0100)=(1011)=\alpha^7$

$\because \alpha^{14}+\alpha^{11}=(1001)+(1110)=(0111)=\alpha^{10}$

式 x-2-5 より

$\alpha^6+\sigma_1\alpha^{12}+\sigma_0\alpha^{11}=0$ よって、$\sigma_1\alpha^{12}=\alpha^6+\sigma_0\alpha^{11}=\alpha^{21}+\sigma_0\alpha^{26}=0 \quad \sigma_1=\alpha^9+\sigma_0\alpha^{14}$

式 x-2-6 に代入して

$\alpha^{13}+\sigma_1\alpha^7+\sigma_0\alpha^{10}=\alpha^{13}+(\alpha^9+\sigma_0\alpha^{14})\alpha^7+\sigma_0\alpha^{10}=\alpha^{13}+\alpha^{16}+\sigma_0\alpha^{21}+\sigma_0\alpha^{10}=\alpha^{12}+\sigma_0\,\alpha^7=0$

$\because \alpha^{13}+\alpha^{16}=\alpha^{13}+\alpha^1=(1101)+(0010)=(1111)=\alpha^{12}$

$\because \alpha^{21}+\alpha^{10}=\alpha^6+\alpha^{10}=(1100)+(0111)=(1011)=\alpha^7$

よって、$\sigma_0=\alpha^5$

$\sigma_1=\alpha^9+\sigma_0\alpha^{14}=\alpha^9+\alpha^5\alpha^{14}=\alpha^9+\alpha^{19}=\alpha^9+\alpha^4=(1010)+(0011)=(1001)=\alpha^{14}$

$\sigma_2=\alpha^6+\sigma_1\alpha^{13}+\sigma_0\alpha^0=\alpha^6+\alpha^{14}\alpha^{13}+\alpha^5\alpha^0=\alpha^6+\alpha^{27}+\alpha^5=\alpha^6+\alpha^{12}+\alpha^5=(1100)+(1111)+(0110)=(0101)=\alpha^8$

以上より、$\sigma_0=\alpha^5$、$\sigma_1=\alpha^{14}$、$\sigma_2=\alpha^8$

ステップ３）式 2-5 を拡張して、α^i、α^j、α^k　を求める。

つまり、$\sigma(x)=x^3-\sigma_2x^2+\sigma_1x-\sigma_0=(x-\alpha^i)(x-\alpha^j)(x-\alpha^k)$ となるように因数分解して、α^i、α^j、α^k　を定め、i、j、kを求める。

$$\sigma(x)=x^3-\sigma_2x^2+\sigma_1x-\sigma_0=x^3+\alpha^8x^2+\alpha^{14}x+\alpha^5=(x+\alpha^{10})(x+\alpha^{12})(x+\alpha^{13})$$

これより、誤りの位置は、$i=10,j=12,k=13$　と決定される。

（xにα　のべき乗を入れて確認する。

1 ： $x^3+\alpha^8x^2+\alpha^{14}x+\alpha^5=1+\alpha^8+\alpha^{14}+\alpha^5=(0001)+(0101)+(1001)+(0110)=(1011)\neq 0$

α^1　：　$x^3+\alpha^8x^2+\alpha^{14}x+\alpha^5=\alpha^3+\alpha^8\alpha^2+\alpha^{14}\alpha^1+\alpha^5=\alpha^3+\alpha^{10}+\alpha^{15}+\alpha^5=(1000)+(0111)+(0001)+(0110)=(1000)\neq 0$

α^2 ： $x^3+\alpha^8x^2+\alpha^{14}x+\alpha^5=\alpha^6+\alpha^8\alpha^4+\alpha^{14}\alpha^2+\alpha^5=\alpha^6+\alpha^{12}+\alpha^{16}+\alpha^5=\alpha^6+\alpha^{12}+\alpha^1+\alpha^5=(1100)+(1111)+(0010)+(0110)=(0101)\neq 0$

α^3 ： $x^3+\alpha^8x^2+\alpha^{14}x+\alpha^5=\alpha^9+\alpha^8\alpha^6+\alpha^{14}\alpha^3+\alpha^5=\alpha^9+\alpha^{14}+\alpha^{17}+\alpha^5=\alpha^9+\alpha^{14}+\alpha^2+\alpha^5=(1010)+(1001)+(0100)+(0110)=(0001)\neq 0$

α^4　：　$x^3+\alpha^8x^2+\alpha^{14}x+\alpha^5=\alpha^{12}+\alpha^8\alpha^8+\alpha^{14}\alpha^4+\alpha^5=\alpha^{12}+\alpha^{16}+\alpha^{18}+\alpha^5=\alpha^{12}+\alpha^1+\alpha^3+\alpha^5=(1111)+(0010)+(1000)+(0110)=(0011)\neq 0$

α^5　：　$x^3+\alpha^8x^2+\alpha^{14}x+\alpha^5=\alpha^{15}+\alpha^8\alpha^{10}+\alpha^{14}\alpha^5+\alpha^5=\alpha^{15}+\alpha^{18}+\alpha^{19}+\alpha^5=\alpha^0+\alpha^3+\alpha^4+\alpha^5=(0001)+(1000)+(0011)+(0110)=(1100)\neq 0$

α^6　：　$x^3+\alpha^8x^2+\alpha^{14}x+\alpha^5=\alpha^{18}+\alpha^8\alpha^{12}+\alpha^{14}\alpha^6+\alpha^5=\alpha^{18}+\alpha^{20}+\alpha^{20}+\alpha^5=\alpha^3+\alpha^5=$

$(1000)+(0110)=(1110)\neq 0$

α^7 ： $x^3+\alpha^8x^2+\alpha^{14}x+\alpha^5=\alpha^{21}+\alpha^8\alpha^{14}+\alpha^{14}\alpha^7+\alpha^5=\alpha^{21}+\alpha^{22}+\alpha^{21}+\alpha^5=\alpha^6+\alpha^7+\alpha^6+\alpha^5=\alpha^7+\alpha^5=(1011)+(0110)=(1101)\neq 0$

α^8 ： $x^3+\alpha^8x^2+\alpha^{14}x+\alpha^5=\alpha^{24}+\alpha^8\alpha^{16}+\alpha^{14}\alpha^8+\alpha^5=\alpha^{24}+\alpha^{24}+\alpha^{22}+\alpha^5=\alpha^7+\alpha^5=(1011)+(0110)=(1101)\neq 0$

α^9 ： $x^3+\alpha^8x^2+\alpha^{14}x+\alpha^5=\alpha^{27}+\alpha^8\alpha^{18}+\alpha^{14}\alpha^9+\alpha^5=\alpha^{27}+\alpha^{26}+\alpha^{23}+\alpha^5=\alpha^{12}+\alpha^{11}+\alpha^8+\alpha^5=(1111)+(1110)+(0101)+(0110)=(0010)\neq 0$

α^{10} ： $x^3+\alpha^8x^2+\alpha^{14}x+\alpha^5=\alpha^{30}+\alpha^8\alpha^{20}+\alpha^{14}\alpha^{10}+\alpha^5=\alpha^{30}+\alpha^{28}+\alpha^{24}+\alpha^5=\alpha^0+\alpha^{13}+\alpha^9+\alpha^5=(0001)+(1101)+(1010)+(0110)=(0000)=0$

α^{10}を入れると 0 となる。これを元に因数分解する。

$x^3+\alpha^8x^2+\alpha^{14}x+\alpha^5=(x+\alpha^{10})(x^2+\alpha^1x+\alpha^{10})$

（確認 $\alpha^{10}+\alpha^1=(0111)+(0010)=(0101)=\alpha^8$

$\alpha^{10}+\alpha^{11}=(0111)+(1110)=(1001)=\alpha^{14}$ ）

次に、$(x^2+\alpha^1x+\alpha^{10})$ を検討する。

$0-\alpha^{10}$までは、根ではないので、$x^2+\alpha^1x+\alpha^{10}$ の根は、α^{11}以上である。

α^{11} ： $x^2+\alpha^1x+\alpha^{10}=\alpha^{22}+\alpha^1\alpha^{11}+\alpha^{10}=\alpha^{22}+\alpha^{12}+\alpha^{10}=\alpha^7+\alpha^{12}+\alpha^{10}=(1011)+(1111)+(0111)=(0011)\neq 0$

α^{12} ： $x^2+\alpha^1x+\alpha^{10}=\alpha^{24}+\alpha^1\alpha^{12}+\alpha^{10}=\alpha^{24}+\alpha^{13}+\alpha^{10}=\alpha^9+\alpha^{13}+\alpha^{10}=(1010)+(1101)+(0111)=(0000)=0$

従って、α^{12}は根である。よって、以下となる。

$x^2+\alpha^1x+\alpha^{10}=(x+\alpha^{12})(x+\alpha^{13})$

（確認 $\alpha^{12}+\alpha^{13}=(1111)+(1101)=(0010)=\alpha^1$ ）

ステップ４）式 2-1～2-2 により、e_i、e_j、e_k を求める。

ステップ 1 より、$S_0=\alpha^{11}$、$S_1=\alpha^9$、$S_2=\alpha^{11}$、$S_3=\alpha^2$、$S_4=\alpha^{14}$、$S_5=\alpha^7$

$S_0=v(\alpha^0)=v(1)=u(1)+e(1)=e(1)=e_i+e_j+e_k=e_{10}+e_{12}+e_{13}=\alpha^{11}$

式 2-4-1

$S_1=v(\alpha^1)=v(\alpha)=u(\alpha)+e(\alpha)=e(\alpha)=e_i\alpha^i+e_j\alpha^j+e_k\alpha^k=e_{10}\alpha^{10}+e_{12}\alpha^{12}+e_{13}\alpha^{13}=\alpha^9$

式 2-4-2

$S_2=v(\alpha^2)=u(\alpha^2)+e(\alpha^2)=e(\alpha^2)=e_i\alpha^{2i}+e_j\alpha^{2j}+e_k\alpha^{2k}=e_{10}(\alpha^{10})^2+e_{12}(\alpha^{12})^2+e_{13}(\alpha^{13})^2=e_{10}\alpha^{20}+e_{12}\alpha^{24}+e_{13}\alpha^{26}=e_{10}\alpha^5+e_{12}\alpha^9+e_{13}\alpha^{11}=\alpha^{11}$ 式 2-4-3

式 2-4-1 より、$e_{10}+e_{12}+e_{13}=\alpha^{11}$ $e_{13}=\alpha^{11}+e_{10}+e_{12}$ 式 2-4-5

これを式 2-4-2 に入れて、

$$e_{10}\alpha^{10}+e_{12}\alpha^{12}+e_{13}\alpha^{13}=e_{10}\alpha^{10}+e_{12}\alpha^{12}+(\alpha^{11}+e_{10}+e_{12})\alpha^{13}$$
$$=e_{10}\alpha^{10}+e_{12}\alpha^{12}+\alpha^{24}+e_{10}\alpha^{13}+e_{12}\alpha^{13}=\alpha^{24}+(\alpha^{10}+\alpha^{13})e_{10}+(\alpha^{12}+\alpha^{13})e_{12}$$
$$=\alpha^9+e_{10}\alpha^9+e_{12}\alpha^1=\alpha^9$$

$\because \alpha^{10}+\alpha^{13}=(0111)+(1101)=(1010)=\alpha^9$

$\because \alpha^{12} + \alpha^{13} = (1111) + (1101) = (0010) = \alpha^1$

よって、$e_{10}\alpha^9 + e_{12}\alpha^1 = 0$

$e_{12}\alpha^1 = e_{10}\alpha^9$ よって、$e_{12} = e_{10}\alpha^8$　　式 2-4-6

式 2-4-5 に式 2-4-6 を代入する。

$e_{13} = \alpha^{11} + e_{10} + e_{12} = \alpha^{11} + e_{10} + e_{10}\alpha^8 = \alpha^{11} + e_{10}(1 + \alpha^8) = \alpha^{11} + e_{10}\alpha^2$　式 2-4-7

$\because 1 + \alpha^8 = (0001) + (0101) = (0100) = \alpha^2$

式 2-4-3 に式 2-4-6, 式 2-4-7 を代入する。

$e_{10}\alpha^5 + e_{12}\alpha^9 + e_{13}\alpha^{11} = e_{10}\alpha^5 + e_{10}\alpha^8\alpha^9 + (\alpha^{11} + e_{10}\alpha^2)\alpha^{11} = e_{10}\alpha^5 + e_{10}\alpha^{17} + \alpha^{22} + e_{10}\alpha^{13} = (\alpha^5 + \alpha^{17} + \alpha^{13})e_{10} + \alpha^{22} = e_{10}\alpha^{12} + \alpha^{22} = \alpha^{11}$

$\because \alpha^5 + \alpha^{17} + \alpha^{13} = \alpha^5 + \alpha^2 + \alpha^{13} = (0110) + (0100) + (1101) = (1111) = \alpha^{12}$

以上より、$e_{10}\alpha^{12} = \alpha^{11} + \alpha^{22} = \alpha^{11} + \alpha^7 == (1110) + (1011) = (0101) = \alpha^8 = \alpha^{23}$　　$e_{10} = \alpha^{11}$

式 2-4-6 より、

$e_{12} = e_{10}\alpha^8 = \alpha^{11}\alpha^8 = \alpha^{19} = \alpha^4$

式 2-4-7 より、

$e_{13} = \alpha^{11} + e_{10}\alpha^2 = \alpha^{11} + \alpha^{11}\alpha^2 = \alpha^{11} + \alpha^{13} = (1110) + (1101) = (0011) = \alpha^4$

以上より、$e_{10} = \alpha^{11}$　　$e_{12} = \alpha^4$　　$e_{13} = \alpha^4$

確認

$$S_3 = v(\alpha^3) = u(\alpha^3) + e(\alpha^3) = e(\alpha^3) = e_i\alpha^{3i} + e_j\alpha^{3j} + e_k\alpha^{3k} = e_{10}(\alpha^{10})^3 + e_{12}(\alpha^{12})^3 + e_{13}(\alpha^{13})^3$$
$$= e_{10}\alpha^{30} + e_{12}\alpha^{36} + e_{13}\alpha^{39} = e_{10}\alpha^0 + e_{12}\alpha^6 + e_{13}\alpha^9 = \alpha^{11}\alpha^0 + \alpha^4\alpha^6 + \alpha^4\alpha^9$$
$$= \alpha^{11} + \alpha^{10} + \alpha^{13} = (1110) + (0111) + (1101) = (0100) = \alpha^2$$
$$S_4 = v(\alpha^4) = u(\alpha^4) + e(\alpha^4) = e(\alpha^4) = e_i\alpha^{4i} + e_j\alpha^{4j} + e_k\alpha^{4k} = e_{10}(\alpha^{10})^4 + e_{12}(\alpha^{12})^4 + e_{13}(\alpha^{13})^4$$
$$= e_{10}\alpha^{40} + e_{12}\alpha^{48} + e_{13}\alpha^{52} = e_{10}\alpha^{10} + e_{12}\alpha^3 + e_{13}\alpha^7 = \alpha^{11}\alpha^{10} + \alpha^4\alpha^3 + \alpha^4\alpha^7$$
$$= \alpha^{21} + \alpha^7 + \alpha^{11} = \alpha^6 + \alpha^7 + \alpha^{11} = (1100) + (1011) + (1110) = (1001) = \alpha^{14}$$
$$S_5 = v(\alpha^5) = u(\alpha^5) + e(\alpha^5) = e(\alpha^5) = e_i\alpha^{5i} + e_j\alpha^{5j} + e_k\alpha^{5k} = e_{10}(\alpha^{10})^5 + e_{12}(\alpha^{12})^5 + e_{13}(\alpha^{13})^5$$
$$= e_{10}\alpha^{50} + e_{12}\alpha^{60} + e_{13}\alpha^{65} = e_{10}\alpha^5 + e_{12}\alpha^0 + e_{13}\alpha^5 = \alpha^{11}\alpha^5 + \alpha^4\alpha^0 + \alpha^4\alpha^5$$
$$= \alpha^{16} + \alpha^4 + \alpha^9 = \alpha^1 + \alpha^4 + \alpha^9 = (0010) + (0011) + (1010) = (1011) = \alpha^7$$

以上より、確認できた。

ステップ５）i、j、k、e_i、e_j、e_k　から、誤り多項式　$e(x) = e_ix^i + e_jx^j + e_kx^k$　を決定し、$u(x) = v(x) - e(x)$　で誤り訂正を行う。

誤り多項式　$e(x) = e_ix^i + e_jx^j + e_kx^k = e_{10}x^{10} + e_{12}x^{12} + e_{13}x^{13} = \alpha^{11}x^{10} + \alpha^4x^{12} + \alpha^4x^{13}$

$$v(x) = \alpha^9x^{14} + 0x^{13} + 0x^{12} + \alpha^{13}x^{11} + 0x^{10} + \alpha^8x^9 + \alpha^{13}x^8 + \alpha^3x^7 + \alpha^9x^6 + \alpha^0x^5 + \alpha^8x^4 + \alpha^{14}x^3 + \alpha^{11}x^2 + \alpha^3x + \alpha^3$$
$$u(x) = \alpha^9x^{14} + \alpha^4x^{13} + \alpha^4x^{12} + \alpha^{13}x^{11} + \alpha^{11}x^{10} + \alpha^8x^9 + \alpha^{13}x^8 + \alpha^3x^7 + \alpha^9x^6 + \alpha^0x^5 + \alpha^8x^4 + \alpha^{14}x^3 + \alpha^{11}x^2 + \alpha^3x + \alpha^3$$

以上より、正しく復号された。

———

Microjamjar　で確認する。

http://www.ujamjar.com/demo/ocaml/2014/06/18/reed-solomon-demo.html

確認） 4 次の例　(15, 9)符号

m=4, t=3

Primitive polynomial 19 = (10011) = $x^4 + x + 1$　　Primitive element=2

Initial root b =0　（生成多項式の l のこと）

情報ビット 1010 0011 0011 1101 1110 0101 1101 1000 1010

情報バイト α^9 α^4 α^4 α^{13} α^{11} α^8 α^{13} α^3 α^9

符号化後 α^9 α^4 α^4 α^{13} α^{11} α^8 α^{13} α^3 α^9 α^0 α^8 α^{14} α^{11} α^3 α^3

RS 符号語 1010 0011 0011 1101 1110 0101 1101 1000 1010 0001 0101 1001 1110 1000 1000

バイト番号 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

情報ビット 1010 0011 0011 1101 1110 0101 1101 1000 1010　[10 3 3 13 14 5 13 8 10]

Message 10 8 13 5 14 13 3 3 10　<- 逆順に入れる

送信語

$$u(x) = \alpha^9x^{14} + \alpha^4x^{13} + \alpha^4x^{12} + \alpha^{13}x^{11} + \alpha^{11}x^{10} + \alpha^8x^9 + \alpha^{13}x^8 + \alpha^3x^7 + \alpha^9x^6 + \alpha^0x^5 + \alpha^8x^4 + \alpha^{14}x^3 + \alpha^{11}x^2 + \alpha^3x + \alpha^3$$

受信語

$$v(x) = \alpha^9x^{14} + 0x^{13} + 0x^{12} + \alpha^{13}x^{11} + 0x^{10} + \alpha^8x^9 + \alpha^{13}x^8 + \alpha^3x^7 + \alpha^9x^6 + \alpha^0x^5 + \alpha^8x^4 + \alpha^{14}x^3 + \alpha^{11}x^2 + \alpha^3x + \alpha^3$$

情報ビット 0000 0011 0011 0000 1110 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

[0 3 3 0 14 0 0 0 0 0 0 0 0 0 0]

∵ $0 - \alpha^4 = (0000) + (0011) = (0011) = \alpha^4$　　$0 - \alpha^{11} = (0000) + (1110) = (1110) = \alpha^{11}$

Errors 0 0 0 0 0 0 0 0 0 0 14 0 3 3 0　<- 逆順に入れる

とし、calculate を押すと、

Code word

$$10x^{14} + 3x^{13} + 3x^{12} + 13x^{11} + 14x^{10} + 5x^9 + 13x^8 + 8x^7 + 10x^6 + 1x^5 + 5x^4 + 9x^3 + 14x^2 + 8x + 8$$

Received code word

$$10x^{14} + 0x^{13} + 0x^{12} + 13x^{11} + 0x^{10} + 5x^9 + 13x^8 + 8x^7 + 10x^6 + 1x^5 + 5x^4 + 9x^3 + 14x^2 + 8x + 8$$

Syndromes

$S_0 = \alpha^{11} = 14$　$S_1 = \alpha^9 = 10$　$S_2 = \alpha^{11} = 14$　$S_3 = \alpha^2 = 4$　$S_4 = \alpha^{14} = 9$　$S_5 = \alpha^7 = 11$

となり、シンドロームを確認できる。そして、Euclid, Berlekamp-massey, Error-locator, Chein search, Forney 等が表示されたあと、

Corrected polynomial

$10x^{14} + 3x^{13} + 3x^{12} + 13x^{11} + 14x^{10} + 5x^9 + 13x^8 + 8x^7 + 10x^6 + 1x^5 + 5x^4 + 9x^3 + 14x^2 + 8x + 8$

が得られ、

訂正後　1010 0011 0011 1101 1110 0101 1101 1000 1010 0001 0101 1001 1110 1000 1000

と u(x)一致することが確認できる。

----------シグマを確認したときの計算（不要）

結果からすれば、

$\sigma(x) = x^3 - \sigma_2 x^2 + \sigma_1 x - \sigma_0 = (x + \alpha^{10})(x + \alpha^{12})(x + \alpha^{13}) = (x^2 + [\alpha^{10} + \alpha^{12}]x + \alpha^{22})(x + \alpha^{13})$

$= (x^2 + \alpha^3 x + \alpha^7)(x + \alpha^{13}) = x^3 + (\alpha^{13} + \alpha^3)x^2 + (\alpha^7 + \alpha^{16})x + \alpha^{20}$

$= x^3 + \alpha^8 x^2 + \alpha^{14} x + \alpha^5$

$\alpha^{10} + \alpha^{12} = (0111) + (1111) = (1000) = \alpha^3$

$\alpha^{13} + \alpha^3 = (1101) + (1000) = (0101) = \alpha^8$

$\alpha^7 + \alpha^{16} = \alpha^7 + \alpha^1 = (1011) + (0010) = (1001) = \alpha^{14}$

以上より、$\sigma_0 = \alpha^5$、$\sigma_1 = \alpha^{14}$、$\sigma_2 = \alpha^8$　でないといけない。

Unb で確認する。

$\alpha^{10} = (0111)$ =[7],　$\alpha^{12} = (1111)$ [15] $\alpha^{13} = (1101)$ [13]

[1 7] x [1 15] = [1 8 11]

[1 8 11]x [1 13] = [1 5 9 6]　x^3 + a^8 * x^2 + a^14 * x + a^5

７．２．９　岩垂教科書より

岩垂教科書　リードソロモン　誤り訂正

岩垂好裕著「符号理論入門」昭晃堂 p. 75-

渡辺用　岩垂教科書

■岩垂A）3 誤り訂正の例

原始多項式を$p(x) = x^4 + x + 1$ とする。

uバイト目の場所の誤りを、Y_u（大きさ），V_u（位置）とする。

3 誤りなら、

$E(x) = Y_1V_1 + Y_2V_2 + Y_3V_3$

（わ；i,j,kバイトに誤りがあれば $V_1 = \alpha^i,\ V_2 = \alpha^j,\ V_3 = \alpha^k$　である。）

3 誤り訂正可能な場合は、生成多項式のべきの連続する根が$i = 0,1,2,3,4,5$である。

各iに対して、シンドロームを以下で求める。

$S_i = \sum_{u=1}^{3} Y_u(V_u)^{i+1}$　$i = 0,1,2,3,4,5$

$i = 0$　$S_0 = Y_1(V_1)^1 + Y_2(V_2)^1 + Y_3(V_3)^1$　式 I-1

$i = 1$　$S_1 = Y_1(V_1)^2 + Y_2(V_2)^2 + Y_3(V_3)^2$　式 I-2

$i = 2$　$S_2 = Y_1(V_1)^3 + Y_2(V_2)^3 + Y_3(V_3)^3$　式 I-3

$i = 3$　$S_3 = Y_1(V_1)^4 + Y_2(V_2)^4 + Y_3(V_3)^4$　式 I-4

$i = 4$　$S_4 = Y_1(V_1)^5 + Y_2(V_2)^5 + Y_3(V_3)^5$　式 I-5

$i = 5$　$S_5 = Y_1(V_1)^6 + Y_2(V_2)^6 + Y_3(V_3)^6$　式 I-6

一般に、 $S_i = Y_1(V_1)^{i+1} + Y_2(V_2)^{i+1} + Y_3(V_3)^{i+1}$

（わ；2 個の場合は、Y3=0、V3=0 とする。これについては、後で議論する）

$\sigma_1, \sigma_2, \sigma_3$　を係数とする多項式$\sigma(x)$　を以下のように定義する。

$\sigma(x) = (V_1 - x)(V_2 - x)(V_3 - x) = \sigma_3 - \sigma_2 x + \sigma_1 x^2 - x^3$　式 I-7

この式に、V_1、V_2、V_3を代入する。

$0 = \sigma_3 - \sigma_2 V_1 + \sigma_1 (V_1)^2 - (V_1)^3$　式 I-8

$0 = \sigma_3 - \sigma_2 V_2 + \sigma_1 (V_2)^2 - (V_2)^3$　式 I-9

$0 = \sigma_3 - \sigma_2 V_3 + \sigma_1 (V_3)^2 - (V_3)^3$　式 I-10

式 I-8 の両辺に、$Y_1(V_1)^{1+i}$をかける。0 を移動する。

$Y_1(V_1)^{1+i}\sigma_3 - Y_1(V_1)^{1+i}\sigma_2 V_1 + Y_1(V_1)^{1+i}\sigma_1 (V_1)^2 - Y_1(V_1)^{1+i}(V_1)^3 = 0$

$Y_1(V_1)^{1+i}\sigma_3 - Y_1(V_1)^{2+i}\sigma_2 + Y_1(V_1)^{3+i}\sigma_1 - Y_1(V_1)^{4+i} = 0$　式 I-11

同様に、式 I-9 の両辺に$Y_2(V_2)^{1+i}$を、式 I-10 の両辺に$Y_3(V_3)^{1+i}$をかける。

$Y_2(V_2)^{1+i}\sigma_3 - Y_2(V_2)^{1+i}\sigma_2 V_2 + Y_2(V_2)^{1+i}\sigma_1 (V_2)^2 - Y_2(V_2)^{1+i}(V_2)^3 = 0$

$Y_2(V_2)^{1+i}\sigma_3 - Y_2(V_2)^{2+i}\sigma_2 + Y_2(V_2)^{3+i}\sigma_1 - Y_2(V_2)^{4+i} = 0$　式 I-12

$Y_3(V_3)^{1+i}\sigma_3 - Y_3(V_3)^{1+i}\sigma_2 V_3 + Y_3(V_3)^{1+i}\sigma_1 (V_3)^2 - Y_3(V_3)^{1+i}(V_3)^3 = 0$

$Y_3(V_3)^{1+i}\sigma_3 - Y_3(V_3)^{2+i}\sigma_2 + Y_3(V_3)^{3+i}\sigma_1 - Y_3(V_3)^{4+i} = 0$　式 I-13

式 I-11、I-12、I-13 を加算する。（そして、縦に整理する。）

$$\sigma_3\left[Y_1(V_1)^{1+i}+Y_2(V_2)^{1+i}+Y_3(V_3)^{1+i}\right]-\sigma_2\left[Y_1(V_1)^{2+i}+Y_2(V_2)^{2+i}+Y_3(V_3)^{2+i}\right]$$
$$+\sigma_1\left[Y_1(V_1)^{3+i}+Y_2(V_2)^{3+i}+Y_3(V_3)^{3+i}\right]-\left[Y_1(V_1)^{4+i}+Y_2(V_2)^{4+i}+Y_3(V_3)^{4+i}\right]=0$$

式 I-1 等を考慮すると、

$\sigma_3 S_i-\sigma_2 S_{i+1}+\sigma_1 S_{i+2}-S_{i+3}=0$ を意味している。

$i=0,1,2$に対して計算すると、以下となる。

$i=0$　$\sigma_3 S_0-\sigma_2 S_1+\sigma_1 S_2-S_3=0$　　式 I-14

$i=1$　$\sigma_3 S_1-\sigma_2 S_2+\sigma_1 S_3-S_4=0$　　式 I-15

$i=2$　$\sigma_3 S_2-\sigma_2 S_3+\sigma_1 S_4-S_5=0$　　式 I-16

■岩垂Ｂ）復号の手順

ステップ１）式 I-1～I6（これは受信多項式にαのべき乗を入れていることと等しい）により、S_0～S_5　を求める。

ステップ２）式 I-14～I16 により、σ_1～σ_3　を求める。

ステップ３）式 I-7 を用いて、V_1～V_3　を求める。

　つまり、$\sigma(x)=\sigma_3-\sigma_2 x+\sigma_1 x^2-x^3=(V_1-x)(V_2-x)(V_3-x)$ となるように因数分解して、V_1～V_3　を求める。

　別の言い方をすると$\sigma(x)$の３つの根であるV_1～V_3　を求める。これは、式 I-8～I-10 により、V_1～V_3　を求めていることでもある。

　例えば、　$0=\sigma_3-\sigma_2 V_1+\sigma_1(V_1)^2-(V_1)^3$　式 I-8　－＞V_1

ステップ４）式 I-1～I-3 により、　Y_1～Y_3　を求める。

　$i=0$　$S_0=Y_1(V_1)^1+Y_2(V_2)^1+Y_3(V_3)^1$　式 I-1

　$i=1$　$S_1=Y_1(V_1)^2+Y_2(V_2)^2+Y_3(V_3)^2$　式 I-2

　$i=2$　$S_2=Y_1(V_1)^3+Y_2(V_2)^3+Y_3(V_3)^3$　式 I-3

　なお、式 I-4～I-6 は使わない。。。。

　$i=3$　$S_3=Y_1(V_1)^4+Y_2(V_2)^4+Y_3(V_3)^4$　式 I-4

　$i=4$　$S_4=Y_1(V_1)^5+Y_2(V_2)^5+Y_3(V_3)^5$　式 I-5

　$i=5$　$S_5=Y_1(V_1)^6+Y_2(V_2)^6+Y_3(V_3)^6$　式 I-6

ステップ５）Y_1～Y_3、V_1～V_3　から　$E(x)=Y_1V_1+Y_2V_2+Y_3V_3$　を求め、

　$R(x)-E(x)$　により訂正を行う。

■岩垂Ｃ）具体的な復号例

原始多項式を　$p(x)=x^4+x+1$ とする。

送信語　$(0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0)$

受信語　$(0\,\alpha^4\,0\,0\,\alpha^7\,0\,0\,0\,0\,0\,0\,0\,\alpha^5\,0)$

受信語の多項式　$R(x)=\alpha^4 x+\alpha^7 x^4+\alpha^5 x^{13}$

ステップ１）式 I-1～I6（これは受信多項式にαのべき乗を入れていることと等しい）により、S_0～S_5　を求める。

$i=0$　　$S_0=R(\alpha^1)=\alpha^4\alpha^1+\alpha^7\alpha^4+\alpha^5\alpha^{13}=\alpha^5+\alpha^{11}+\alpha^{18}=\alpha^5+\alpha^{11}+\alpha^3=(0110)+(1110)+(1000)=0$　　式 I-1

$i=1$　　$S_1=R(\alpha^2)=\alpha^4\alpha^2+\alpha^7\alpha^8+\alpha^5\alpha^{26}=\alpha^6+\alpha^{15}+\alpha^{31}=\alpha^6+\alpha^0+\alpha^1=(1100)+(0001)+(0010)=(1111)=\alpha^{12}$　　式 I-2

$i=2$　　$S_2=R(\alpha^3)=\alpha^4\alpha^3+\alpha^7\alpha^{12}+\alpha^5\alpha^{39}=\alpha^7+\alpha^{19}+\alpha^{44}=\alpha^7+\alpha^4+\alpha^{14}=(1011)+(0011)+(1001)=(0001)=1$　　式 I-3

$i=3$　　$S_3=R(\alpha^4)=\alpha^4\alpha^4+\alpha^7\alpha^{16}+\alpha^5\alpha^{52}=\alpha^8+\alpha^{23}+\alpha^{57}=\alpha^8+\alpha^8+\alpha^{12}=\alpha^{12}$　　式 I-4

$i=4$　　$S_4=R(\alpha^5)=\alpha^4\alpha^5+\alpha^7\alpha^{20}+\alpha^5\alpha^{65}=\alpha^9+\alpha^{27}+\alpha^{70}=\alpha^9+\alpha^{12}+\alpha^{10}=(1010)+(1111)+(0111)=(0010)=\alpha^1$　　式 I-5

$i=5$　　$S_5=R(\alpha^6)=\alpha^4\alpha^6+\alpha^7\alpha^{24}+\alpha^5\alpha^{78}=\alpha^{10}+\alpha^{31}+\alpha^{83}=\alpha^7+\alpha^1+\alpha^8=(0111)+(0010)+(0101)=(0000)=0$　　式 I-6

ステップ２）式 I-14～I16 により、σ_1～σ_3　を求める。

$\sigma_3S_0-\sigma_2S_1+\sigma_1S_2-S_3=0$　　式 I-14

$\sigma_3 0-\sigma_2\alpha^{12}+\sigma_1 1-\alpha^{12}=0$　　よって　$-\sigma_2\alpha^{12}+\sigma_1-\alpha^{12}=0$　式 I2-1

$\sigma_3S_1-\sigma_2S_2+\sigma_1S_3-S_4=0$　　式 I-15

$\sigma_3\alpha^{12}-\sigma_2 1+\sigma_1\alpha^{12}-\alpha^1=0$　　よって　$\sigma_3\alpha^{12}-\sigma_2+\sigma_1\alpha^{12}-\alpha^1=0$　式 I2-2

$\sigma_3S_2-\sigma_2S_3+\sigma_1S_4-S_5=0$　　式 I-16

$\sigma_3 1-\sigma_2\alpha^{12}+\sigma_1\alpha^1-0=0$　　よって　$\sigma_3-\sigma_2\alpha^{12}+\sigma_1\alpha^1=0$　式 I2-3

式 I2-1 より

$\sigma_1=\sigma_2\alpha^{12}+\alpha^{12}$　式 I2-4

式 I2-2 に式 I2-4 を入れて

$\sigma_3\alpha^{12}-\sigma_2+\sigma_1\alpha^{12}-\alpha^1=\sigma_3\alpha^{12}-\sigma_2+(\sigma_2\alpha^{12}+\alpha^{12})\alpha^{12}-\alpha^1=\sigma_3\alpha^{12}+\sigma_2(\alpha^{24}-1)+\alpha^{24}-\alpha^1=0$

式 I2-5

式 I2-3 に式 I2-4 を入れて

$\sigma_3-\sigma_2\alpha^{12}+\sigma_1\alpha^1=\sigma_3-\sigma_2\alpha^{12}+(\sigma_2\alpha^{12}+\alpha^{12})\alpha^1=\sigma_3+\sigma_2(\alpha^{13}-\alpha^{12})+\alpha^{13}=0$　　式 I2-6

式 I2-5 から　式 I2-6×α^{12}を引いて、

$\sigma_3\alpha^{12}+\sigma_2(\alpha^{24}-1)+\alpha^{24}-\alpha^1=0$

$\sigma_3\alpha^{12}+\sigma_2\alpha^{12}(\alpha^{13}-\alpha^{12})+\alpha^{12}\alpha^{13}=0$

$\sigma_2(\alpha^{24}-1-\alpha^{25}+\alpha^{24})+\alpha^{24}-\alpha^1+\alpha^{25}=0$

$\sigma_2(-1-\alpha^{10})+\alpha^9-\alpha^1+\alpha^{10}=0$

$-1-\alpha^{10}=(0001)+(0111)=(0110)=\alpha^5$

$\alpha^9-\alpha^1+\alpha^{10}=(1010)+(0010)+(0111)=(1111)=\alpha^{12}$

$\sigma_2\alpha^5=\alpha^{12}$　　$\therefore\ \sigma_2=\alpha^7$

式 I2-6 より

$\sigma_3=\sigma_2(\alpha^{13}-\alpha^{12})+\alpha^{13}=\alpha^7(\alpha^{13}-\alpha^{12})+\alpha^{13}=\alpha^{20}+\alpha^{19}+\alpha^{13}=\alpha^5+\alpha^4+\alpha^{13}=(0110)+$

$(0011)+(1101)=(1000)=\alpha^3$

式 I2-4 より

$\sigma_1=\sigma_2\alpha^{12}+\alpha^{12}=\alpha^7\alpha^{12}+\alpha^{12}=\alpha^{19}+\alpha^{12}=\alpha^4+\alpha^{12}=(0011)+(1111)=(1100)=\alpha^6$

以上より、$\sigma_1=\alpha^6$　　$\sigma_2=\alpha^7$　　$\sigma_3=\alpha^3$

従って、

$\sigma(x)=\sigma_3-\sigma_2x+\sigma_1x^2-x^3=\alpha^3-\alpha^7x+\alpha^6x^2-x^3$

ステップ３）式 I-7 を用いて、V_1～V_3　を求める。

$\sigma(x)=\sigma_3-\sigma_2x+\sigma_1x^2-x^3=(V_1-x)(V_2-x)(V_3-x)$ となるように因数分解する。

$GF(2^4)$の全要素を総当たりして、α^1、α^4、α^{13}を代入すると０となることがわかるので、

$\sigma(x)=(\alpha^1-x)(\alpha^4-x)(\alpha^{13}-x)=(V_1-x)(V_2-x)(V_3-x)=\sigma_3-\sigma_2x+\sigma_1x^2-x^3$

となり、

$V_1=\alpha^1$　　$V_2=\alpha^4$　　$V_3=\alpha^{13}$

となる。

確認

$\sigma(\alpha^1)=\sigma_3-\sigma_2\alpha^1+\sigma_1\alpha^2-\alpha^3=\alpha^3-\alpha^7\alpha^1+\alpha^6\alpha^2-\alpha^3=\alpha^3-\alpha^8+\alpha^8-\alpha^3=0$

$\sigma(\alpha^4)=\sigma_3-\sigma_2\alpha^4+\sigma_1\alpha^8-\alpha^{12}=\alpha^3-\alpha^7\alpha^4+\alpha^6\alpha^8-\alpha^{12}=\alpha^3-\alpha^{11}+\alpha^{14}-\alpha^{12}=(1000)+(1110)+(1001)+(1111)=0$

$\sigma(\alpha^{13})=\sigma_3-\sigma_2\alpha^{13}+\sigma_1\alpha^{26}-\alpha^{39}=\alpha^3-\alpha^7\alpha^{13}+\alpha^6\alpha^{26}-\alpha^{39}=\alpha^3-\alpha^{20}+\alpha^{32}-\alpha^{39}=\alpha^3-\alpha^5+\alpha^2-\alpha^9=(1000)+(0110)+(0100)+(1010)=0$

ステップ４）式 I-1～I-3 により、　Y_1～Y_3　を求める。

$i=0$　$S_0=Y_1(V_1)^1+Y_2(V_2)^1+Y_3(V_3)^1=0$　式 I-1

$i=1$　$S_1=Y_1(V_1)^2+Y_2(V_2)^2+Y_3(V_3)^2=\alpha^{12}$　式 I-2

$i=2$　$S_2=Y_1(V_1)^3+Y_2(V_2)^3+Y_3(V_3)^3=1$　式 I-3

$Y_1(V_1)^1+Y_2(V_2)^1+Y_3(V_3)^1=Y_1(\alpha^1)^1+Y_2(\alpha^4)^1+Y_3(\alpha^{13})^1=Y_1\alpha^1+Y_2\alpha^4+Y_3\alpha^{13}=0$ 式 I4-1

$Y_1(V_1)^2+Y_2(V_2)^2+Y_3(V_3)^2=Y_1(\alpha^1)^2+Y_2(\alpha^4)^2+Y_3(\alpha^{13})^2=Y_1\alpha^2+Y_2\alpha^8+Y_3\alpha^{26}=Y_1\alpha^2+Y_2\alpha^8+Y_3\alpha^{11}=\alpha^{12}$ 式 I4-2

$Y_1(V_1)^3+Y_2(V_2)^3+Y_3(V_3)^3=Y_1(\alpha^1)^3+Y_2(\alpha^4)^3+Y_3(\alpha^{13})^3=Y_1\alpha^3+Y_2\alpha^{12}+Y_3\alpha^{39}=Y_1\alpha^3+Y_2\alpha^{12}+Y_3\alpha^9=1$ 式 I4-3

これらを解く。式 I4-1 は、

$Y_1\alpha^1+Y_2\alpha^4+Y_3\alpha^{13}=0$　　$Y_1=Y_2\alpha^3+Y_3\alpha^{12}$　式 I4-4

式 I4-2 に式 I4-4 を入れて

$Y_1\alpha^2+Y_2\alpha^8+Y_3\alpha^{11}=\alpha^{12}$　　$Y_1\alpha^2+Y_2\alpha^8+Y_3\alpha^{11}=(Y_2\alpha^3+Y_3\alpha^{12})\alpha^2+Y_2\alpha^8+Y_3\alpha^{11}=Y_2\alpha^5+Y_3\alpha^{14}+Y_2\alpha^8+Y_3\alpha^{11}=Y_2(\alpha^5+\alpha^8)+Y_3(\alpha^{14}+\alpha^{11})=\alpha^{12}$

$\alpha^5 + \alpha^8 = (0110) + (0101) = (0011) = \alpha^4$

$\alpha^{14} + \alpha^{11} = (1001) + (1110) = (0111) = \alpha^{10}$

よって、

$Y_2(\alpha^5 + \alpha^8) + Y_3(\alpha^{14} + \alpha^{11}) = Y_2\alpha^4 + Y_3\alpha^{10} = \alpha^{12}$　　式 I4-5

式 I4-3 に式 I4-4 を入れる。

$Y_1\alpha^3 + Y_2\alpha^{12} + Y_3\alpha^9 = (Y_2\alpha^3 + Y_3\alpha^{12})\alpha^3 + Y_2\alpha^{12} + Y_3\alpha^9 = Y_2(\alpha^6 + \alpha^{12}) + Y_3(\alpha^{15} + \alpha^9) = 1$

$\alpha^6 + \alpha^{12} = (1100) + (1111) = (0011) = \alpha^4$

$\alpha^{15} + \alpha^9 = (0001) + (1010) = (1011) = \alpha^7$

よって

$Y_2(\alpha^6 + \alpha^{12}) + Y_3(\alpha^{15} + \alpha^9) = Y_2\alpha^4 + Y_3\alpha^7 = 1$　　式 I4-6

式 I4-5 から式 I4-6 を引く

$Y_2\alpha^4 + Y_3\alpha^{10} = \alpha^{12}$

$Y_2\alpha^4 + Y_3\alpha^7 = 1$

$Y_3(\alpha^{10} + \alpha^7) = \alpha^{12} + 1$

$\alpha^{10} + \alpha^7 = (0111) + (1011) = (1100) = \alpha^6$

$\alpha^{12} + 1 = (1111) + (0001) = (1110) = \alpha^{11}$

$Y_3\alpha^6 = \alpha^{11}$　　$\therefore\ Y_3 = \alpha^5$

式 I4-6 より

$Y_2\alpha^4 + Y_3\alpha^7 = Y_2\alpha^4 + \alpha^5\alpha^7 = Y_2\alpha^4 + \alpha^{12} = 1$

$1 + \alpha^{12} = (0001) + (1111) = (1110) = \alpha^{11}$

$Y_2\alpha^4 = \alpha^{11}$　　$\therefore\ Y_2 = \alpha^7$

式 I4-4 より、

$Y_1 = Y_2\alpha^3 + Y_3\alpha^{12} = \alpha^7\alpha^3 + \alpha^5\alpha^{12} = \alpha^{10} + \alpha^{17} = \alpha^{10} + \alpha^2 = (0111) + (0100) = (0011) = \alpha^4$

$Y_1 = \alpha^4$　　$Y_2 = \alpha^7$　　$Y_3 = \alpha^5$

ステップ５）Y_1～Y_3、V_1～V_3　から　誤り多項式　$E(x) = Y_1x^l + Y_2x^m + Y_3x^n$　を求め、

$R(x) - E(x)$　により訂正を行う。(l、m、nは、V_1＝α^l、V_2＝α^m、V_3＝α^n　から求める)

$E(x) = Y_1x^l + Y_2x^m + Y_3x^n = \alpha^4x^1 + \alpha^7x^4 + \alpha^5x^{13}$

$R(x) - E(x) = (\alpha^4x + \alpha^7x^4 + \alpha^5x^{13}) - (\alpha^4x + \alpha^7x^4 + \alpha^5x^{13}) = 0$

この場合、送信符号語は all 0 であったので、正しく復号できたこととなる。

■岩垂Ｄ）誤り訂正能力３に対して、2 誤りの場合の処理

例２（前の例と同じで、2 個の場合）：$p(x) = x^4 + x + 1$

送信語 all0　受信語(0 0 0 0 α^7 0 0 0 0 0 0 0 0 0 α^5 0)

受信語の多項式　$R(x) = \alpha^7x^4 + \alpha^5x^{13}$

ステップ１）式 I-1～I6（これは受信多項式にαのべき乗を入れていることと等しい）により、S_0～S_5　を求める。

$i=0$　　$S_0 = R(\alpha^1) = \alpha^7\alpha^4 + \alpha^5\alpha^{13} = \alpha^{11} + \alpha^{18} = \alpha^{11} + \alpha^3 = (1110) + (1000) = (0110) = \alpha^5$
式 I-1

$i=1$　　$S_1 = R(\alpha^2) = \alpha^7\alpha^8 + \alpha^5\alpha^{26} = \alpha^{15} + \alpha^{31} = 1 + \alpha^1 = (0001) + (0010) = (0011) = \alpha^4$
式 I-2

$i=2$　　$S_2 = R(\alpha^3) = \alpha^7\alpha^{12} + \alpha^5\alpha^{39} = \alpha^{19} + \alpha^{44} = \alpha^4 + \alpha^{14} = (0011) + (1001) = (1010) = \alpha^9$
式 I-3

$i=3$　　$S_3 = R(\alpha^4) = \alpha^7\alpha^{16} + \alpha^5\alpha^{52} = \alpha^{23} + \alpha^{57} = \alpha^8 + \alpha^{12} = (0101) + (1111) = (1010) = \alpha^9$
式 I-4

$i=4$　　$S_4 = R(\alpha^5) = \alpha^7\alpha^{20} + \alpha^5\alpha^{65} = \alpha^{27} + \alpha^{70} = \alpha^{12} + \alpha^{10} = (1111) + (0111) = (1000) = \alpha^3$
式 I-5

$i=5$　　$S_5 = R(\alpha^6) = \alpha^7\alpha^{24} + \alpha^5\alpha^{78} = \alpha^{31} + \alpha^{83} = \alpha^1 + \alpha^8 = (0010) + (0101) = (0111) = \alpha^{10}$
式 I-6

ステップ２）式 I-14～I16 により、σ_1～σ_3　を求める。

$\sigma_3 S_0 - \sigma_2 S_1 + \sigma_1 S_2 - S_3 = 0$　式 I-14
$\sigma_3\alpha^5 - \sigma_2\alpha^4 + \sigma_1\alpha^9 - \alpha^9 = 0$　　式 I2-1

$\sigma_3 S_1 - \sigma_2 S_2 + \sigma_1 S_3 - S_4 = 0$　式 I-15
$\sigma_3\alpha^4 - \sigma_2\alpha^9 + \sigma_1\alpha^9 - \alpha^3 = 0$　　式 I2-2

$\sigma_3 S_2 - \sigma_2 S_3 + \sigma_1 S_4 - S_5 = 0$　式 I-16
$\sigma_3\alpha^9 - \sigma_2\alpha^9 + \sigma_1\alpha^3 - \alpha^{10} = 0$　　式 I2-3

式 I2-1 * α^4 から 式 I2-2 *α^5 を引く
$\sigma_3\alpha^9 - \sigma_2\alpha^8 + \sigma_1\alpha^{13} - \alpha^{13} = 0$
$\sigma_3\alpha^9 - \sigma_2\alpha^{14} + \sigma_1\alpha^{14} - \alpha^8 = 0$
$\sigma_2(\alpha^8 + \alpha^{14}) + \sigma_1(\alpha^{13} + \alpha^{14}) + \alpha^{13} + \alpha^8 = \sigma_2\alpha^6 + \sigma_1\alpha^2 + \alpha^3 = 0$ 式 I2-4
$\alpha^8 + \alpha^{14} = (0101) + (1001) = (1100) = \alpha^6$
$\alpha^{13} + \alpha^{14} = (1101) + (1001) = (0100) = \alpha^2$
$\alpha^{13} + \alpha^8 = (1101) + (0101) = (1000) = \alpha^3$

同様に、式 I2-2 * α^9 から 式 I2-3 *α^4 を引く
$\sigma_3\alpha^{13} - \sigma_2\alpha^{18} + \sigma_1\alpha^{18} - \alpha^{12} = 0$
$\sigma_3\alpha^{13} - \sigma_2\alpha^{13} + \sigma_1\alpha^7 - \alpha^{14} = 0$
$\sigma_2(\alpha^3 + \alpha^{13}) + \sigma_1(\alpha^3 + \alpha^7) + \alpha^{12} + \alpha^{14} = \sigma_2\alpha^8 + \sigma_1\alpha^4 + \alpha^5 = 0$ 式 I2-5
$\alpha^3 + \alpha^{13} = (1000) + (1101) = (0101) = \alpha^8$
$\alpha^3 + \alpha^7 = (1000) + (1011) = (0011) = \alpha^4$
$\alpha^{12} + \alpha^{14} = (1111) + (1001) = (0110) = \alpha^5$

式 I2-4 * α^2 は 式 I2-5　と同一。

では、式 I2-1 * α^9 から 式 I2-3 *α^5 を引いてみる

$\sigma_3\alpha^{14} - \sigma_2\alpha^{13} + \sigma_1\alpha^{18} - \alpha^{18} = 0$

$\sigma_3\alpha^{14} - \sigma_2\alpha^{14} + \sigma_1\alpha^{8} - \alpha^{15} = 0$

$\sigma_2(\alpha^{13} + \alpha^{14}) + \sigma_1(\alpha^3 + \alpha^8) + \alpha^3 + \alpha^0 = \sigma_2\alpha^2 + \sigma_1\alpha^{13} + \alpha^{14} = 0$ 式 I2-6

$\alpha^{13} + \alpha^{14} = (1101) + (1001) = (0100) = \alpha^2$

$\alpha^3 + \alpha^8 = (1000) + (0101) = (1101) = \alpha^{13}$

$\alpha^3 + \alpha^0 = (1000) + (0001) = (1001) = \alpha^{14}$

やはり同一であり、解けない。

式 I2-4、式 I2-5、式 I2-6　のいずれも　$\sigma_2 + \sigma_1\alpha^{11} + \alpha^{12} = 0$　の定数倍

つまり、式 I2-4、式 I2-5、式 I2-6 は独立ではなく、従属。

そこで、$\sigma_3 = 0$　と仮定する。

$\sigma_3\alpha^5 - \sigma_2\alpha^4 + \sigma_1\alpha^9 - \alpha^9 = 0$　　式 I2-1

$\sigma_3\alpha^4 - \sigma_2\alpha^9 + \sigma_1\alpha^9 - \alpha^3 = 0$　　式 I2-2

$\sigma_2\alpha^4 + \sigma_1\alpha^9 - \alpha^9 = 0$

$\sigma_2\alpha^9 + \sigma_1\alpha^9 - \alpha^3 = 0$

$\sigma_2\alpha^9 + \sigma_1\alpha^{14} - \alpha^{14} = 0$

$\sigma_2\alpha^9 + \sigma_1\alpha^9 - \alpha^3 = 0$

$\sigma_1(\alpha^{14} + \alpha^9) = \alpha^{14} + \alpha^3$

$\alpha^{14} + \alpha^9 = (1001) + (1010) = (0011) = \alpha^4$

$\alpha^{14} + \alpha^3 = (1001) + (1000) = (0001) = \alpha^0$

$\sigma_1\alpha^4 = \alpha^0$　　$\sigma_1 = \alpha^{11}$

$\sigma_2\alpha^4 = \sigma_1\alpha^9 + \alpha^9 = \alpha^{11}\alpha^9 + \alpha^9 = \alpha^{20} + \alpha^9 = \alpha^5 + \alpha^9 = (0110) + (1010) = (1100) = \alpha^6$

よって、$\sigma_2 = \alpha^2$

以上より、$\sigma_1 = \alpha^{11}$　　$\sigma_2 = \alpha^2$　　$\sigma_3 = 0$

従って、

$\sigma(x) = \sigma_3 - \sigma_2 x + \sigma_1 x^2 - x^3 = -\alpha^2 x + \alpha^{11}x^2 - x^3 = x(-\alpha^2 + \alpha^{11}x - x^2)$

ステップ３）式 I-7 を用いて、V_1～V_3　を求める。

$\sigma(x) = \sigma_3 - \sigma_2 x + \sigma_1 x^2 - x^3 = (V_1 - x)(V_2 - x)(V_3 - x)$ となるように因数分解する。

V_3は 0 である。$GF(2^4)$の全要素を総当たりする。

$x = 1$　　$-\alpha^2 + \alpha^{11}x - x^2 = -\alpha^2 + \alpha^{11}1 - 1 = (0100) + (1110) + (0001) = (1011) \neq 0$

$x = \alpha^1$　$-\alpha^2 + \alpha^{11}x - x^2 = -\alpha^2 + \alpha^{11}\alpha^1 - \alpha^2 = -\alpha^2 + \alpha^{12} - \alpha^2 \neq 0$

$x = \alpha^2$　$-\alpha^2 + \alpha^{11}x - x^2 = -\alpha^2 + \alpha^{11}\alpha^2 - \alpha^4 = -\alpha^2 + \alpha^{13} - \alpha^4 = (0100) + (1101) + (0011) =$

$(1010) \neq 0$

$x = \alpha^3 \quad -\alpha^2 + \alpha^{11}x - x^2 = -\alpha^2 + \alpha^{11}\alpha^3 - \alpha^6 = -\alpha^2 + \alpha^{14} - \alpha^6 = (0100) + (1001) + (1100) = (0001) \neq 0$

$x = \alpha^4 \quad -\alpha^2 + \alpha^{11}x - x^2 = -\alpha^2 + \alpha^{11}\alpha^4 - \alpha^8 = -\alpha^2 + \alpha^{15} - \alpha^8 = (0100) + (0001) + (0101) = (0000)$　よって、$V_1 = \alpha^4$

$V_2 = \frac{\alpha^2}{\alpha^4} = \alpha^{13}$

（確認、$V_1 + V_2 = \alpha^4 + \alpha^{13} = (0011) + (1101) = (1110) = \alpha^{11}$　確かに満たしている）

以上より、

$V_1 = \alpha^4 \qquad V_2 = \alpha^{13} \qquad V_3 = 0$

となる。

ステップ４）式 I-1～I-3 により、　Y_1～Y_3　を求める。

$i = 0 \quad S_0 = Y_1(V_1)^1 + Y_2(V_2)^1 + Y_3(V_3)^1 = \alpha^5$　式 I-1

$i = 1 \quad S_1 = Y_1(V_1)^2 + Y_2(V_2)^2 + Y_3(V_3)^2 = \alpha^4$　式 I-2

$i = 2 \quad S_2 = Y_1(V_1)^3 + Y_2(V_2)^3 + Y_3(V_3)^3 = \alpha^9$　式 I-3

$Y_1(V_1)^1 + Y_2(V_2)^1 + Y_3(V_3)^1 = Y_1(\alpha^4)^1 + Y_2(\alpha^{13})^1 + Y_3(0)^1 = Y_1\alpha^4 + Y_2\alpha^{13} = \alpha^5$ 式 I4-1

$Y_1(V_1)^2 + Y_2(V_2)^2 + Y_3(V_3)^2 = Y_1(\alpha^4)^2 + Y_2(\alpha^{13})^2 + Y_3(0)^2 = Y_1\alpha^8 + Y_2\alpha^{26} = Y_1\alpha^8 + Y_2\alpha^{11} = \alpha^4$　式 I4-2

$Y_1(V_1)^3 + Y_2(V_2)^3 + Y_3(V_3)^3 = Y_1(\alpha^4)^3 + Y_2(\alpha^{13})^3 + Y_3(0)^3 = Y_1\alpha^{12} + Y_2\alpha^{39} = Y_1\alpha^{12} + Y_2\alpha^9 = \alpha^9$　式 I4-3

これらを解く。式 I4-1 は、

$Y_1\alpha^4 + Y_2\alpha^{13} = \alpha^5 \qquad Y_1\alpha^4 = Y_2\alpha^{13} + \alpha^5$　よって、$Y_1 = Y_2\alpha^9 + \alpha^1$　式 I4-4

式 I4-2 に、式 I4-4 を入れて

$Y_1\alpha^8 + Y_2\alpha^{11} = \alpha^4 \qquad Y_1\alpha^8 + Y_2\alpha^{11} = (Y_2\alpha^9 + \alpha^1)\alpha^8 + Y_2\alpha^{11} = Y_2\alpha^{17} + \alpha^9 + Y_2\alpha^{11} = Y_2(\alpha^{17} + \alpha^{11}) + \alpha^9 = Y_2\alpha^9 + \alpha^9 = \alpha^4$

$\alpha^{17} + \alpha^{11} = \alpha^2 + \alpha^{11} = (0100) + (1110) = (1010) = \alpha^9$

$Y_2\alpha^9 = \alpha^9 + \alpha^4 = \alpha^{14}$

$\alpha^9 + \alpha^4 = (1010) + (0011) = (1001) = \alpha^{14}$

よって、$Y_2 = \alpha^5$

式 I4-4 より

$Y_1 = Y_2\alpha^9 + \alpha^1 = \alpha^5\alpha^9 + \alpha^1 = \alpha^{14} + \alpha^1 = (1001) + (0010) = (1011) = \alpha^7$

（式 I4-3 を確認する。

$Y_1\alpha^{12} + Y_2\alpha^9 = \alpha^7\alpha^{12} + \alpha^5\alpha^9 = \alpha^{19} + \alpha^{14} = \alpha^4 + \alpha^{14} = (0011) + (1001) = (1010) = \alpha^9$

一致することが確認できた）

以上より、

$Y_1 = \alpha^7$　　$Y_2 = \alpha^5$　　Y_3不定。　Y_3は0とする。

ステップ５）Y_1～Y_3、V_1～V_3　から　誤り多項式　$E(x) = Y_1x^l + Y_2x^m + Y_3x^n$　を求め、

$R(x) - E(x)$　により訂正を行う。(l、m、nは、V_1＝α^l、V_2＝α^m、V_3＝α^n　から求める)

V_1＝α^4、V_2＝α^{13}、V_3＝0　より、$l = 4$、$m = 13$　とする。nは不定だが、Y_3＝0　とするので問題ない。

$E(x) = Y_1x^l + Y_2x^m + Y_3x^n = \alpha^7x^4 + \alpha^5x^{13} + 0$

$R(x) - E(x) = (\alpha^7x^4 + \alpha^5x^{13}) - (\alpha^7x^4 + \alpha^5x^{13}) = 0$

となり、正しく復号できる。

■岩垂Ｅ）誤り訂正能力tに対して、誤りの数が$t-1$以下の場合の処理

岩垂Ｄより、例えば、3誤り訂正能力がある場合、

① シンドローム　$S_i = v(\alpha^i) = 0\ for\ i = 0,1,,,2t-1$　を確認する。確認できれば、受信語は正しい符号語として終了（他の正しい符号語である可能性もある）。確認できない場合は②へ

② 3誤りと仮定して解く。解ければ誤り訂正終了。解けなければ③へ

③ 2誤りと仮定して$Y_3 = 0$、$V_3 = 0$として解く。解ければ誤り訂正終了。解けなければ④へ

④ 1誤りと仮定して$Y_2 = 0$、$Y_3 = 0$、$V_2 = 0$、$V_3 = 0$として解く。解ければ誤り訂正終了。解けなければ、誤り検出。

７．２．１０　３次の例１，４次の例１の unb サイトでの確認

１）３次■例１　(7,3)符号　　$m=3, n=7, k=3, t=2$, 原始多項式が$p(x)=x^3+x+1$の場合

・情報多項式$I(y)*y^{n-k}$を生成多項式$G(y)$　で除算した余りを求める。

$I(y)=I_{k-1}y^{k-1}+\cdots I_1 y+I_0=1y^2+\alpha^1 y^1+\alpha^2 y^0$

$r(y)=I(y)*y^{n-k}\ mod\ G(y)=(1y^2+\alpha^1 y^1+\alpha^2 y^0)*y^4\ mod\ y^4+\alpha^2 y^3+\alpha^5 y^2+\alpha^5 y^1+\alpha^6$

$=\alpha^4 y^3+\alpha^6 y^2+\alpha^5 y+\alpha^3$

・　A 欄　$(1y^2+\alpha^1 y^1+\alpha^2 y^0)y^4$　=> ($\alpha^0\ \alpha^1\ \alpha^2$ 0 0 0 0) => [1 2 4 0 0 0 0]

・　B 欄　$y^4+\alpha^2 y^3+\alpha^5 y^2+\alpha^5 y^1+\alpha^6$　=>　($\alpha^0\ \alpha^2\ \alpha^5\ \alpha^5\ \alpha^6$)　=> [1 4 7 7 5]

・　結果　[6 5 7 3] -> $\alpha^4\ \alpha^6\ \alpha^5\ \alpha^3$　-> $\alpha^4 y^3+\alpha^6 y^2+\alpha^5 y+\alpha^3$　確認 OK

２）４次■例　(15, 11)符号　$m=4, n=15, k=11, t=2$, 原始多項式が$p(x)=x^4+x+1$の場合

・情報多項式$I(y)*y^{n-k}$を生成多項式$G(y)$　で除算した余りを求める。

$I(y)=I_{k-1}y^{k-1}+\cdots I_1 y+I_0$

$=\alpha^9 y^{10}+\alpha^4 y^9+\alpha^4 y^8+\alpha^{13} y^7+\alpha^{11} y^6+\alpha^8 y^5+\alpha^{13} y^4+\alpha^3 y^3+\alpha^9 y^2+\alpha^8 y^1+0y^0$

$r(y)=I(y)*y^{n-k}\ mod\ G(y)$

$=(\alpha^9 y^{10}+\alpha^4 y^9+\alpha^4 y^8+\alpha^{13} y^7+\alpha^{11} y^6+\alpha^8 y^5+\alpha^{13} y^4+\alpha^3 y^3+\alpha^9 y^2+\alpha^8 y^1+0y^0)*y^4$

$mod\ y^4+\alpha^{12} y^3+\alpha^4 y^2+y^1+\alpha^6$

$=\alpha^{13} y^3+\alpha^{13} y^2+\alpha^0 y+\alpha^{10}$

・　A 欄　$(\alpha^9 y^{10}+\alpha^4 y^9+\alpha^4 y^8+\alpha^{13} y^7+\alpha^{11} y^6+\alpha^8 y^5+\alpha^{13} y^4+\alpha^3 y^3+\alpha^9 y^2+\alpha^8 y^1+0y^0)y^4$

=> ($\alpha^9\ \alpha^4\ \alpha^4\ \alpha^{13}\ \alpha^{11}\ \alpha^8\ \alpha^{13}\ \alpha^3\ \alpha^9\ \alpha^8$ 0 0 0 0 0)

=> [10 3 3 13 14 5 13 8 10 5 0 0 0 0 0]

・　B 欄　$y^4+\alpha^{12} y^3+\alpha^4 y^2+y^1+\alpha^6$　=>　($\alpha^0\ \alpha^{12}\ \alpha^4\ \alpha^0\ \alpha^6$)　=> [1 15 3 1 12]

・　結果　[13 13 1 7] -> $\alpha^{13}\ \alpha^{13}\ \alpha^0\ \alpha^{10}$　-> $\alpha^{13} y^3+\alpha^{13} y^2+\alpha^0 y+\alpha^{10}$　確認 OK

上式の計算をするには、GF(2^4)の加算表、乗算表　も役立つ

http://www.ee.unb.ca/cgi-bin/tervo/galois3.pl?p=4&D=1&A=1

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
4	4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
5	5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
6	6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
7	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
11	11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
12	12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
13	13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
14	14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
15	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

×	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	2	4	6	8	10	12	14	3	1	7	5	11	9	15	13
3	3	6	5	12	15	10	9	11	8	13	14	7	4	1	2
4	4	8	12	3	7	11	15	6	2	14	10	5	1	13	9
5	5	10	15	7	2	13	8	14	11	4	1	9	12	3	6
6	6	12	10	11	13	7	1	5	3	9	15	14	8	2	4
7	7	14	9	15	8	1	6	13	10	3	4	2	5	12	11
8	8	3	11	6	14	5	13	12	4	15	7	10	2	9	1
9	9	1	8	2	11	3	10	4	13	5	12	6	15	7	14
10	10	7	13	14	4	9	3	15	5	8	2	1	11	6	12
11	11	5	14	10	1	15	4	7	12	2	9	13	6	8	3
12	12	11	7	5	9	14	2	10	6	1	13	15	3	4	8
13	13	9	4	1	12	8	5	2	15	11	6	3	14	10	7
14	14	15	1	13	3	2	12	9	7	6	8	4	10	11	5
15	15	13	2	9	6	4	11	1	14	12	3	8	7	5	10

途中で断念した割り算の手計算

```
                  9   7  13
                ---------------------
0 9 12 1 2 4 0 |9   4   4   13   11   8   13   3   9   x   x   x   x   x   x
```

```
            9  18    21   10    11   13     9
               =3    =6
-------------------------------------------------------
               4+3  4+6   13+10  x   8+13  13+9
               7    12     9     x   3     10    3
               7    16     19    8   9     11    7
                    =1     =4
-------------------------------------------------------
                   12+1  9+4     8   3+9   10+11  3+7
                   13    14      8   1     14     4     9
                   13    22      25  14    15     17    13
                         =7      =10         =0     =2
-------------------------------------------------------
                         14+7    8+10  1+14  14+0   4+2   9+13
                         1         1   7     3      10    10
```

７．３　Goppa 符号

７．３．１　概要

・1970 年頃 V. D. Goppa が考案（古典 Goppa 符号）。その後 1980 年頃に拡張（代数幾何符号）

・一般的には非巡回符号。巡回符号 BCH, RS を包含する。

・BCH, RS の符号長に関する制約を緩和。

・有理式を用いる。留数型符号

・VG 限界を超える高効率な Goppa 符号があることが報告されている。

Tsfasman, Vladut, Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, Mathematische Nachrichten, vol 109, 1982

・MacEliece 暗号の基礎

以下では、古典 Goppa 符号について述べる。

参考：

・Ellen Jochemsz: Goppa Codes and the McEliece Cryptosystem, Vrije Universiteit Amasterdam
https://klevas.mif.vu.lt/~skersys/vsd/crypto_on_codes/goppamceliece.pdf

・Elwyn Berlekamp, Goppa Codes, IEEE Transactions on Information Theory, Vol. IT-19, No. 5, Sep. 1973
https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1055088

・上原剛：代数幾何符号に関する研究
http://www.jssac.org/Editor/Suushiki/V09/No2/V9N2_104.pdf

・E. Berlekamp, "Goppa codes," in IEEE Transactions on Information Theory, vol. 19, no. 5, pp. 590-592, September 1973, doi: 10.1109/TIT.1973.1055088.
https://ieeexplore.ieee.org/abstract/document/1055088

７．３．２　定義

ある原始多項式で生成される拡大体$GF(q^m)$を考える。ただし、qは素数である。

$GF(q^m)$は、原始元αのべき乗と０を要素として持つ。すなわち、

$$GF(q^m) = \{0, 1, \alpha^1, \alpha^2 ,,, \alpha^{q^m-2}\}$$

$GF(q^m)$上のt次の多項式（ゴッパ多項式）を

$$g(z) = \sum_{i=0}^{t} g_i z^i = g_t z^t + g_{t-1} z^{t-1} + g_{t-2} z^{t-2} + \cdots + g_1 z^1 + g_0 \quad (1)$$

とする。（生成多項式ではないことに注意せよ）

$GF(q^m)$のn個の要素からなる部分集合Lを以下とする。

$$L = \{\alpha_1, \alpha_2, \alpha_3 ,,, \alpha_n\} \subseteq GF(q^m)$$

ただし、$g(\alpha_i) \neq 0$である。（すなわち、ゴッパ多項式の根ではない）

$GF(q)$上のベクトル$c = \{c_1, c_2, c_3,,, c_n\}$と多項式

$$R_C(z) = \sum_{i=1}^{n} \frac{c_i}{z - \alpha_i}$$

を考え、

$$R_C(z) = \sum_{i=1}^{n} \frac{c_i}{z-\alpha_i} = 0 \; mod \; g(z) \quad (2)$$

となるベクトル$c = \{c_1, c_2, c_3, , , c_n\}$をゴッパ符号という。

７．３．３　ゴッパ符号のパラメータ(n, k, d)

$g(z)$はt次であるから、$\frac{1}{z-\alpha_i} \; mod \; g(z)$は、$t-1$次以下の多項式で表現できる。すなわち、

$$\frac{1}{z-\alpha_i} = p_i(z) = p_{it}z^{t-1} + p_{i(t-1)}z^{t-2} + p_{i(t-2)}z^{t-2} + \cdots + p_{i2}z + p_{i1} \;\; mod \; g(z)$$

と置くことができる。従って、(2)式は、

$$R_C(z) = \sum_{i=1}^{n} \frac{c_i}{z-\alpha_i} = \sum_{i=1}^{n} c_i p_i(z) = \sum_{i=1}^{n} c_i(p_{it}z^{t-1} + p_{i(t-1)}z^{t-2} + p_{i(t-2)}z^{t-2} + \cdots + p_{i2}z + p_{i1})$$
$$= 0 \; mod \; g(z) \quad (3)$$

と書き換えられる。z^jの項の係数はすべて０である。すなわち、

$$\sum_{i=1}^{n} c_i p_{ij} = 0 \;\; for \; 1 \le j \le t \;\; (4)$$

である。

$g(z)$で定義されるゴッパ符号は、$GF(q^m)$上のt個の線形式で定義される。これは、$GF(q)$上でのmt以下の方程式に縮退可能である。従って、kは$n-mt$以上でなければならない。従って、$k \ge n-mt$ である。また、

$$\sum_{i=1}^{n} \frac{c_i}{z-\alpha_i} = \frac{\sum_{j=1}^{\omega} c_{i_j} \prod_{1 \le k \le \omega, k \ne j}(z-\alpha_{i_k})}{\prod_{j=1}^{\omega}(z-\alpha_{i_j})}$$

であるため、分母は$g(z)$と共通の因子を持たないので、$g(z)$分子を割り切らねばならない。

分子の次元は、$\omega - 1$以下であるので、$\omega - 1 \ge t$となり、これにより最小距離は

$d \ge t+1$　　となる。

符号長n, 情報ビットk, 最小距離dのゴッパ符号を(n, k, d)ゴッパ符号と表現する。

７．３．４　検査行列と生成行列

式(4)を再掲する。

$$\sum_{i=1}^{n} c_i p_{ij} = 0 \;\; for \; 1 \le j \le t$$

すべてのjに関してまとめて以下のように表現できる。

$$c = (c_1, c_2, c_3, , , c_n)$$

$$(c_1, c_2, c_3, , , c_n) \begin{pmatrix} p_{11} & p_{12} & p_{13} & & p_{1t} \\ p_{21} & p_{22} & p_{23} & \cdots & \\ p_{31} & & & & \\ \vdots & & & \ddots & \\ p_{n1} & & & & p_{nt} \end{pmatrix} = 0$$

係数　z^0　z^1　z^2　z^{t-1}

これは、検査ルールを表現している。したがって、検査行列Hを以下のように定義すれば、

$$H = \begin{pmatrix} p_{11} & p_{21} & p_{31} & & p_{n1} \\ p_{12} & p_{22} & p_{32} & \cdots & \\ p_{13} & & & & \\ \vdots & & & \ddots & \\ p_{1t} & & & & p_{nt} \end{pmatrix}$$

検査ルールを

$$cH^T = 0$$

と表現できる。なお、Hは、$t \times n$行列である。

さらに、

$$p_i(z) = \frac{1}{z-\alpha_i} = \frac{g(z)-g(\alpha_i)}{z-\alpha_i}\frac{-1}{g(\alpha_i)} \quad mod\ g(z)$$

であるので、（証明は※１）

※１ ----------

$$(z-\alpha_i)\frac{g(z)-g(\alpha_i)}{z-\alpha_i}\frac{-1}{g(\alpha_i)} = \frac{-1}{g(\alpha_i)}\big(g(z)-g(\alpha_i)\big) = \frac{-1}{g(\alpha_i)}g(z) + \frac{g(\alpha_i)}{g(\alpha_i)} = \frac{-1}{g(\alpha_i)}g(z) + 1$$

$$= 1\ mod\ g(z)$$

よって、

$$\frac{g(z)-g(\alpha_i)}{z-\alpha_i}\frac{-1}{g(\alpha_i)} = \frac{1}{z-\alpha_i}$$

$$p_i(z) = \frac{1}{z-\alpha_i} = -\frac{g_t z^t + g_{t-1}z^{t-1} + g_{t-2}z^{t-2} + \cdots + g_1 z^1 + g_0 - g(\alpha_i)}{z-\alpha_i}\frac{1}{g(\alpha_i)}$$

$$= -\frac{g_t(z^t - {\alpha_i}^t) + g_{t-1}(z^{t-1} - {\alpha_i}^{t-1}) + g_{t-2}(z^{t-2} - {\alpha_i}^{t-2}) + \cdots + g_1(z^1 - {\alpha_i}^1) + g_0(z^0 - {\alpha_i}^0)}{z-\alpha_i}\frac{1}{g(\alpha_i)}$$

$$= -\{(g_t(z^{t-1} + z^{t-2}{\alpha_i}^1 + z^{t-3}{\alpha_i}^2 + \cdots + {\alpha_i}^{t-1}) + g_{t-1}(z^{t-2} + z^{t-3}{\alpha_i}^1 + z^{t-4}{\alpha_i}^2 + \cdots + {\alpha_i}^{t-2}) + \cdots$$

$$+ g_2(z^1 + {\alpha_i}^1) + g_1\}\frac{1}{g(\alpha_i)}$$

と変形でき、この式と

$$p_i(z) = p_{it}z^{t-1} + p_{i(t-1)}z^{t-2} + p_{i(t-2)}z^{t-2} + \cdots + p_{i2}z + p_{i1}$$

のz^jの係数を比較して以下を得る。

z^0: $p_{i1} = -(g_t{\alpha_i}^{t-1} + g_{t-1}{\alpha_i}^{t-2} + g_{t-2}{\alpha_i}^{t-3} + \cdots + g_2{\alpha_i}^1 + g_1)\frac{1}{g(\alpha_i)}$

z^1: $p_{i2} = -(g_t{\alpha_i}^{t-2} + g_{t-1}{\alpha_i}^{t-3} + g_{t-2}{\alpha_i}^{t-4} + \cdots + g_2)\frac{1}{g(\alpha_i)}$

z^2: $p_{i3} = -(g_t{\alpha_i}^{t-3} + g_{t-1}{\alpha_i}^{t-4} + g_{t-2}{\alpha_i}^{t-5} + \cdots + g_3)\frac{1}{g(\alpha_i)}$

z^{t-2}: $p_{i(t-1)} = -\frac{(g_t{\alpha_i}^1 + g_{t-1})1}{g(\alpha_i)}$

z^{t-1}: $p_{it} = -g_t\frac{1}{g(\alpha_i)}$

したがって、以下のように検査行列Hを３つの行列の積で表現できる。

$$H = \begin{pmatrix} p_{11} & p_{21} & p_{31} & & p_{n1} \\ p_{12} & p_{22} & p_{32} & \cdots & \\ p_{13} & & & & \\ \vdots & & & \ddots & \\ p_{1t} & & & & p_{nt} \end{pmatrix} = XYZ$$

$$X = \begin{pmatrix} -g_t & -g_{t-1} & -g_{t-2} & & -g_1 \\ 0 & -g_t & -g_{t-1} & \cdots & -g_2 \\ 0 & 0 & -g_t & & -g_3 \\ & \vdots & & \ddots & \\ 0 & 0 & 0 & & -g_t \end{pmatrix}$$

Xは$t \times t$行列

$$Y = \begin{pmatrix} {\alpha_1}^{t-1} & {\alpha_2}^{t-1} & {\alpha_3}^{t-1} & & {\alpha_n}^{t-1} \\ {\alpha_1}^{t-2} & {\alpha_2}^{t-2} & {\alpha_3}^{t-2} & \cdots & {\alpha_n}^{t-2} \\ {\alpha_1}^{t-3} & {\alpha_2}^{t-3} & {\alpha_3}^{t-3} & & {\alpha_n}^{t-3} \\ & \vdots & & \ddots & \\ {\alpha_1}^{1} & {\alpha_2}^{1} & {\alpha_3}^{1} & & {\alpha_n}^{1} \\ 1 & 1 & 1 & & 1 \end{pmatrix}$$

Yは$t \times n$行列

$$Z = \begin{pmatrix} \frac{1}{g(\alpha_1)} & 0 & 0 & & 0 \\ 0 & \frac{1}{g(\alpha_2)} & 0 & \cdots & 0 \\ 0 & 0 & \frac{1}{g(\alpha_3)} & & 0 \\ & \vdots & & \ddots & \\ 0 & 0 & 0 & & \frac{1}{g(\alpha_n)} \end{pmatrix}$$

Zは$n \times n$行列

生成行列Gは、$GH^T = 0$より得られる。

（より正確には、Hの零空間(null space)の基底を求め、その基底から G を決定する。）

７．３．５　Goppa 符号の例

■例１（Amsterdam 大の資料 Jochemsz, Ellen. “Goppa Codes & the McEliece Cryptosystem.” Amsterdam: Vrije Universiteit Amsterdam, 2002. Print. https://pdfcoffee.com/goppa-codes-and-the-mceliece-cryptosystem-pdf-free.html p.8,　2.6.1 を元にした。）

$GF(2^4)$上の Goppa 符号を考察する。$q = 2,\quad m = 4$

１）まず、

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

である。

２）原始多項式を$ap(x) = x^4 + x + 1$　とする。

・$GF(2)$上の任意の多項式を原始多項式$ap(x) = x^4 + x + 1$（ベクトル表現　10011)で除した余りの集合は、以下となる。

多項式	ベクトル表現	αべき表現
0	0000	0
1	0001	α^0
x	0010	α^1
$x+1$	0011	α^4
x^2	0100	α^2
x^2+1	0101	α^8
x^2+x	0110	α^5
x^2+x+1	0111	α^{10}
x^3	1000	α^3
x^3+1	1001	α^{14}
x^3+x	1010	α^9
x^3+x+1	1011	α^7
x^3+x^2	1100	α^6
x^3+x^2+1	1101	α^{13}
x^3+x^2+x	1110	α^{11}
x^3+x^2+x+1	1111	α^{12}

拡大体は、$GF(2^4)=\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}\}$である。

3）ゴッパ集合Lを以下とする。$L \subseteq GF(2^4)$　（Lは$GF(2^4)$の部分集合）

$$L=\{\alpha^i \; such\; that\; 2\le i\le 13\}=\{\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},\alpha^{11},\alpha^{12},\alpha^{13}\}$$

ゴッパ集合Lの要素数により、符号長nが決定される。この場合は、$n=12$である。

4）ゴッパ多項式 $g(z)$を決める。$g(z)$の根は、ゴッパ集合Lに含まれないようにする。

ここでは、以下とする。（separable；重根を持たない場合）

$$g(z)=(z+\alpha^1)(z+\alpha^{14})=z^2+\alpha^7 z+1=g_2z^2+g_1z+g_0$$

（　$\because$　$\alpha^1+\alpha^{14}=(0\,0\,1\,0)+(1\,0\,0\,1)=(1\,0\,1\,1)=\alpha^7$　　）

5）以上より、このゴッパ符号のパラメータは以下となる。

$$q=2,\quad m=4,\quad n=12,\quad t=2,\quad d\ge 2t+1=4+1=5$$

$\alpha_1=\alpha^2\;\; \alpha_2=\alpha^3\;\; \alpha_3=\alpha^4\;\; \alpha_4=\alpha^5\;\; \alpha_5=\alpha^6\;\; \alpha_6=\alpha^7\;\; \alpha_7=\alpha^8\;\; \alpha_8=\alpha^9\;\; \alpha_9=\alpha^{10}\;\; \alpha_{10}=\alpha^{11}\;\; \alpha_{11}=\alpha^{12}\;\; \alpha_{12}=\alpha^{13}$

$g_0=1\quad g_1=\alpha^7\quad g_2=1$

これにより、$(12,\ge 4,\ge 5)$Goppa 符号が構成される。

6）検査行列 H を求める。

$H=XYZ$

$X: t\times t=2\times 2$行列、$Y: t\times n=2\times 12$行列、$Z: n\times n=12\times 12$行列、$H: t\times n=2\times 12$行列

まず、X行列を求める。

$$X=\begin{pmatrix} -g_t & -g_{t-1} & -g_{t-2} & \cdots & -g_1 \\ 0 & -g_t & -g_{t-1} & \cdots & -g_2 \\ 0 & 0 & -g_t & \cdots & -g_3 \\ \vdots & \vdots & \vdots & \ddots & \\ 0 & 0 & 0 & & -g_t \end{pmatrix}=\begin{pmatrix} -g_2 & -g_1 \\ 0 & -g_2 \end{pmatrix}=\begin{pmatrix} 1 & \alpha^7 \\ 0 & 1 \end{pmatrix}$$

次に、Y行列を求める。

$$Y = \begin{pmatrix} {\alpha_1}^{t-1} & {\alpha_2}^{t-1} & {\alpha_3}^{t-1} & \cdots & {\alpha_n}^{t-1} \\ {\alpha_1}^{t-2} & {\alpha_2}^{t-2} & {\alpha_3}^{t-2} & & {\alpha_n}^{t-2} \\ {\alpha_1}^{t-3} & {\alpha_2}^{t-3} & {\alpha_3}^{t-3} & & {\alpha_n}^{t-3} \\ & \vdots & & & \\ {\alpha_1}^{1} & {\alpha_2}^{1} & {\alpha_3}^{1} & \ddots & {\alpha_n}^{1} \\ 1 & 1 & 1 & & 1 \end{pmatrix}$$

$$= \begin{pmatrix} \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Z行列を求める。

$$\frac{1}{g(\alpha_1)} = \frac{1}{(\alpha^2)^2+\alpha^7\alpha^2+1} = \frac{1}{\alpha^4+\alpha^9+1} = \{(0011)+(1010)+(0001)\}^{-1} = \{(1000)\}^{-1} = \{\alpha^3\}^{-1} = \alpha^{-3} = \alpha^{12}$$

$$\frac{1}{g(\alpha_2)} = \frac{1}{(\alpha^3)^2+\alpha^7\alpha^3+1} = \frac{1}{\alpha^6+\alpha^{10}+1} = \{(1100)+(0111)+(0001)\}^{-1} = \{(1010)\}^{-1} = \{\alpha^9\}^{-1} = \alpha^{-9} = \alpha^6$$

$$\frac{1}{g(\alpha_3)} = \frac{1}{(\alpha^4)^2+\alpha^7\alpha^4+1} = \frac{1}{\alpha^8+\alpha^{11}+1} = \{(0101)+(1110)+(0001)\}^{-1} = \{(1010)\}^{-1} = \{\alpha^9\}^{-1} = \alpha^{-9} = \alpha^6$$

$$\frac{1}{g(\alpha_4)} = \frac{1}{(\alpha^5)^2+\alpha^7\alpha^5+1} = \frac{1}{\alpha^{10}+\alpha^{12}+1} = \{(0111)+(1111)+(0001)\}^{-1} = \{(1001)\}^{-1} = \{\alpha^{14}\}^{-1} = \alpha^{-14} = \alpha^1$$

$$\frac{1}{g(\alpha_5)} = \frac{1}{(\alpha^6)^2+\alpha^7\alpha^6+1} = \frac{1}{\alpha^{12}+\alpha^{13}+1} = \{(1111)+(1101)+(0001)\}^{-1} = \{(0011)\}^{-1} = \{\alpha^4\}^{-1} = \alpha^{-4} = \alpha^{11}$$

$$\frac{1}{g(\alpha_6)} = \frac{1}{(\alpha^7)^2+\alpha^7\alpha^7+1} = \frac{1}{\alpha^{14}+\alpha^{14}+1} = \{1\}^{-1} = 1$$

$$\frac{1}{g(\alpha_7)} = \frac{1}{(\alpha^8)^2+\alpha^7\alpha^8+1} = \frac{1}{\alpha^{16}+\alpha^{15}+1} = \frac{1}{\alpha^1+1+1} = \alpha^{-1} = \alpha^{14}$$

$$\frac{1}{g(\alpha_8)} = \frac{1}{(\alpha^9)^2+\alpha^7\alpha^9+1} = \frac{1}{\alpha^{18}+\alpha^{16}+1} = \frac{1}{\alpha^3+\alpha^1+1} = \{(1000)+(0010)+(0001)\}^{-1} = \{(1011)\}^{-1} = \{\alpha^7\}^{-1} =$$

$$\alpha^{-7} = \alpha^8$$

$$\frac{1}{g(\alpha_9)} = \frac{1}{(\alpha^{10})^2+\alpha^7\alpha^{10}+1} = \frac{1}{\alpha^{20}+\alpha^{17}+1} = \frac{1}{\alpha^5+\alpha^2+1} = \{(0110)+(0100)+(0001)\}^{-1} = \{(0011)\}^{-1} = \{\alpha^4\}^{-1} =$$

$$\alpha^{-4} = \alpha^{11}$$

$$\frac{1}{g(\alpha_{10})} = \frac{1}{(\alpha^{11})^2+\alpha^7\alpha^{11}+1} = \frac{1}{\alpha^{22}+\alpha^{18}+1} = \frac{1}{\alpha^7+\alpha^3+1} = \{(1011)+(1000)+(0001)\}^{-1} = \{(0010)\}^{-1} =$$

$$\{\alpha^1\}^{-1} = \alpha^{-1} = \alpha^{14}$$

$$\frac{1}{g(\alpha_{11})} = \frac{1}{(\alpha^{12})^2+\alpha^7\alpha^{12}+1} = \frac{1}{\alpha^{24}+\alpha^{19}+1} = \frac{1}{\alpha^9+\alpha^4+1} = \{(1010)+(0011)+(0001)\}^{-1} = \{(1000)\}^{-1} =$$

$$\{\alpha^3\}^{-1} = \alpha^{-3} = \alpha^{12}$$

$$\frac{1}{g(\alpha_{12})} = \frac{1}{(\alpha^{13})^2+\alpha^7\alpha^{13}+1} = \frac{1}{\alpha^{26}+\alpha^{20}+1} = \frac{1}{\alpha^{11}+\alpha^5+1} = \{(1110)+(0110)+(0001)\}^{-1} = \{(1001)\}^{-1} =$$

$$\{\alpha^{14}\}^{-1} = \alpha^{-14} = \alpha^1$$

以上より、Zは、

$$Z = \begin{pmatrix} \frac{1}{g(\alpha_1)} & 0 & 0 & & 0 \\ 0 & \frac{1}{g(\alpha_2)} & 0 & \cdots & 0 \\ 0 & 0 & \frac{1}{g(\alpha_3)} & & 0 \\ & \vdots & & \ddots & \\ 0 & 0 & 0 & & \frac{1}{g(\alpha_n)} \end{pmatrix}$$

$$= \begin{pmatrix} \alpha^{12} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha^{6} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha^{6} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha^{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha^{11} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{14} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{8} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{11} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{14} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{12} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{1} \end{pmatrix}$$

となる。従って、H は以下のように求められる。

$$H = XYZ = \begin{pmatrix} 1 & \alpha^7 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} \alpha^{12} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha^{6} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha^{6} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha^{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha^{11} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{14} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{8} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{11} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{14} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{12} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{1} \end{pmatrix}$$

$$= \begin{pmatrix} (\alpha^2+\alpha^7) & (\alpha^3+\alpha^7) & (\alpha^4+\alpha^7) & (\alpha^5+\alpha^7) & (\alpha^6+\alpha^7) & (\alpha^7+\alpha^7) & (\alpha^8+\alpha^7) & (\alpha^9+\alpha^7) & (\alpha^{10}+\alpha^7) & (\alpha^{11}+\alpha^7) & (\alpha^{12}+\alpha^7) & (\alpha^{13}+\alpha^7) \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} \alpha^{12} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha^{6} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha^{6} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha^{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha^{11} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{14} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{8} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{11} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{14} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{12} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{1} \end{pmatrix} = \begin{pmatrix} \alpha^9 & \alpha^{10} & \alpha^9 & \alpha^{14} & \alpha^6 & 0 & \alpha^{10} & \alpha^8 & \alpha^2 & \alpha^7 & \alpha^{14} & \alpha^6 \\ \alpha^{12} & \alpha^6 & \alpha^6 & \alpha^1 & \alpha^{11} & 1 & \alpha^{14} & \alpha^8 & \alpha^{11} & \alpha^{14} & \alpha^{12} & \alpha^1 \end{pmatrix}$$

Hの最初の列に注目する。第1行目と第2行目にzをかけたものを加算した$\alpha^9 + \alpha^{12}z$は、$\alpha^9 + \alpha^{12}z = \frac{1}{z-\alpha^2}$ である。なぜならば、

$(\alpha^9 + \alpha^{12}z)(z - \alpha^2) = \alpha^{12}z^2 + \alpha^9 z - \alpha^{14}z - \alpha^{11} = \alpha^{12}z^2 + \alpha^4 z - \alpha^{11} = -\alpha^{11} - \alpha^{12} = 1 \; mod \; g(z)$

であるから。以下の割り算を参考のこと。

$$\begin{array}{lll} 1\,\alpha^7\,1 \quad | & \alpha^{12} & \alpha^4 \quad \alpha^{11} \\ & \alpha^{12} & \alpha^{19} \quad \alpha^{12} \\ & & \alpha^{11} + \alpha^{12} = 1 \end{array}$$

さて、$cH^T = 0$であるから以下を得る。

$$cH^T = (c_1, c_2, c_3, , , c_{12}) \begin{pmatrix} \alpha^9 & \alpha^{10} & \alpha^9 & \alpha^{14} & \alpha^6 & 0 & \alpha^{10} & \alpha^8 & \alpha^2 & \alpha^7 & \alpha^{14} & \alpha^6 \\ \alpha^{12} & \alpha^6 & \alpha^6 & \alpha^1 & \alpha^{11} & 1 & \alpha^{14} & \alpha^8 & \alpha^{11} & \alpha^{14} & \alpha^{12} & \alpha^1 \end{pmatrix}^T = 0$$

展開すると、

$$c_1\alpha^9 + c_2\alpha^{10} + c_3\alpha^9 + c_4\alpha^{14} + c_5\alpha^6 + c_6 0 + c_7\alpha^{10} + c_8\alpha^8 + c_9\alpha^2 + c_{10}\alpha^7 + c_{11}\alpha^{14} + c_{12}\alpha^6 = 0$$

$$c_1\alpha^{12} + c_2\alpha^6 + c_3\alpha^6 + c_4\alpha^1 + c_5\alpha^{11} + c_6 1 + c_7\alpha^{14} + c_8\alpha^8 + c_9\alpha^{11} + c_{10}\alpha^{14} + c_{11}\alpha^{12} + c_{12}\alpha^1 = 0$$

であり、第二式にzをかけて両辺を加算すると、

$$\begin{aligned}
&(c_1\alpha^9 + c_2\alpha^{10} + c_3\alpha^9 + c_4\alpha^{14} + c_5\alpha^6 + c_6 0 + c_7\alpha^{10} + c_8\alpha^8 + c_9\alpha^2 + c_{10}\alpha^7 + c_{11}\alpha^{14} + c_{12}\alpha^6) \\
&\quad + z(c_1\alpha^{12} + c_2\alpha^6 + c_3\alpha^6 + c_4\alpha^1 + c_5\alpha^{11} + c_6 1 + c_7\alpha^{14} + c_8\alpha^8 + c_9\alpha^{11} + c_{10}\alpha^{14} + c_{11}\alpha^{12} + c_{12}\alpha^1) \\
&\quad = c_1(\alpha^9 + \alpha^{12}z) + c_2(\alpha^{10} + \alpha^6 z) + c_3(\alpha^9 + \alpha^6 z) + c_4(\alpha^{14} + \alpha^1 z) + c_5(\alpha^6 + \alpha^{11}z) + c_6(0 + z) + c_7(\alpha^{10} + \alpha^{14}z) \\
&\quad + c_8(\alpha^8 + \alpha^8 z) + c_9(\alpha^2 + \alpha^{11}z) + c_{10}(\alpha^7 + \alpha^{14}z) + c_{11}(\alpha^{14} + \alpha^{12}z) + c_{12}(\alpha^6 + \alpha^1 z) \\
&\quad = \frac{c_1}{z-\alpha^2} + \frac{c_2}{z-\alpha^3} + \frac{c_3}{z-\alpha^4} + \frac{c_4}{z-\alpha^5} + \frac{c_5}{z-\alpha^6} + \frac{c_6}{z-\alpha^7} + \frac{c_7}{z-\alpha^8} + \frac{c_8}{z-\alpha^9} + \frac{c_9}{z-\alpha^{10}} + \frac{c_{10}}{z-\alpha^{11}} + \frac{c_{11}}{z-\alpha^{12}} + \frac{c_{12}}{z-\alpha^{13}} \\
&\quad = 0
\end{aligned}$$

となる。この式は、Goppa 符号の一般的な定義式と一致している。

Hをベクトルで表現すれば、以下となる。

$$H = \begin{pmatrix} \alpha^9 & \alpha^{10} & \alpha^9 & \alpha^{14} & \alpha^6 & 0 & \alpha^{10} & \alpha^8 & \alpha^2 & \alpha^7 & \alpha^{14} & \alpha^6 \\ \alpha^{12} & \alpha^6 & \alpha^6 & \alpha^1 & \alpha^{11} & 1 & \alpha^{14} & \alpha^8 & \alpha^{11} & \alpha^{14} & \alpha^{12} & \alpha^1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

生成行列Gは、$GH^T = 0$より得られる。まず、Hの零空間(null space)の基底を求める。Hを以下のように基本変形して RREF(Reduced Row Echelon Form)を求める。なお、Hのランクは８である。

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

ここから、null space の基底は、(0 0 1 0 1 0 1 1 1 0 0 0) (1 1 1 1 0 1 0 1 0 1 0 0) (0 1 0 0 1 1 1 1 0 0 1 0) (0 1 0 1 0 0 1 1 0 0 0 1) となる。（https://www.mathdetail.com/null.php にて確認）

これにより、生成行列Gが求められる。

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

全符号語は、Gの線形結合によって求められる。

Goppa(12, 4, 5)符号

行の番号	線形結合	重み
①	**0010 1011 1000**	5
②	**1111 0101 0100**	7
③	**0100 1111 0010**	5

④	**0101 0011 0001**	5
①＋②	**1101 1110 1100**	8
①＋③	**0110 0100 1010**	5
①＋④	**0111 1000 1001**	6
②＋③	**1011 1010 0110**	7
②＋④	**1010 0110 0101**	6
③＋④	**0001 1100 0011**	5
①＋②＋③	**1001 0001 1110**	6
②＋③＋④	**1110 1001 0111**	8
①＋②＋④	**1000 1101 1101**	7
①＋③＋④	**0011 0111 1011**	8
①＋②＋③＋④	**1100 0010 1111**	7
①＋①	**0000 0000 0000**	0

・最初の４ビットに 0000 – 1111 の１６語が現れている。

・この符号は、符号語間の距離がすべて５以上であり（確認せよ）、２誤り訂正が可能である。

・符号効率：k/n=4/12=0.33

Cf. ２誤り生成可能な BCH(15, 7)符号 k/n=7/15=0.467

■例２（Goppa で非巡回ハミング（7,4）となる例）

$GF(2^3)$上の Goppa 符号を考える。$q=2,\quad m=3$

原始多項式を$ap(x)=x^3+x+1$　とする。

１）x^7+1の因数分解。省略

２）原始多項式からの拡大体の構成。

多項式	ベクトル表現	αべき表現	
0	000	0	
1	001	1	$=\alpha^0$
x	010	α	$=\alpha^1$
$x+1$	011	$\alpha+1$	$=\alpha^3$
x^2	100	α^2	$=\alpha^2$
x^2+1	101	α^2+1	$=\alpha^6$
x^2+x	110	$\alpha^2+\alpha$	$=\alpha^4$
x^2+x+1	111	$\alpha^2+\alpha+1$	$=\alpha^5$

拡大体は$GF(2^3)=\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6\}$

３）ゴッパ集合Lを以下とする。$L\subseteq GF(2^3)$　（Lは$GF(2^3)$の部分集合）

$$L=\{0,\alpha^1,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6\}$$

ゴッパ集合Lの要素数により、符号長nが決定される。この場合は、$n=7$である。

４）ゴッパ多項式 $g(z)$を決める。$g(z)$の根は、ゴッパ集合Lに含まれないようにする。

ここでは、以下とする。

$$g(z)=z+1=g_1z+g_0$$

５）以上より、このゴッパ符号のパラメータは以下となる。

$$q=2,\qquad m=3,\qquad n=7,\qquad t=1,\qquad d\geq 2t+1=2+1=3$$

$\alpha_1=0\ \ \alpha_2=\alpha^1\ \ \alpha_3=\alpha^2\ \ \alpha_4=\alpha^3\ \ \alpha_5=\alpha^4\ \ \alpha_6=\alpha^5\ \ \alpha_7=\alpha^6\quad g_0=1\quad g_1=1$

これにより、$(7,4,3)$Goppa 符号が構成される。

６）検査行列 H を求める。

$H=XYZ$

$X:t\times t=1\times 1$行列、$Y:t\times n=1\times 7$行列、$Z:n\times n=7\times 7$行列、$H:t\times n=1\times 7$行列

まず、X行列を求める。

$$X=\begin{pmatrix} -g_t & -g_{t-1} & -g_{t-2} & & -g_1 \\ 0 & -g_t & -g_{t-1} & \cdots & -g_2 \\ 0 & 0 & -g_t & & -g_3 \\ & \vdots & & \ddots & \\ 0 & 0 & 0 & & -g_t \end{pmatrix}=(-g_1)=(1)$$

次に、Y行列を求める。

$$Y=\begin{pmatrix} {\alpha_1}^{t-1} & {\alpha_2}^{t-1} & {\alpha_3}^{t-1} & & {\alpha_n}^{t-1} \\ {\alpha_1}^{t-2} & {\alpha_2}^{t-2} & {\alpha_3}^{t-2} & \cdots & {\alpha_n}^{t-2} \\ {\alpha_1}^{t-3} & {\alpha_2}^{t-3} & {\alpha_3}^{t-3} & & {\alpha_n}^{t-3} \\ & \vdots & & & \\ {\alpha_1}^{1} & {\alpha_2}^{1} & {\alpha_3}^{1} & \ddots & {\alpha_n}^{1} \\ 1 & 1 & 1 & & 1 \end{pmatrix}=(1\quad 1\quad 1\quad 1\quad 1\quad 1\quad 1)$$

Z行列を求める。

$\frac{1}{g(\alpha_1)}=\frac{1}{g(0)}=\frac{1}{1}=1$　　$\frac{1}{g(\alpha_2)}=\frac{1}{g(\alpha^1)}=\frac{1}{\alpha^1+1}=\frac{1}{\alpha^3}=\alpha^{-3}$

$$\frac{1}{g(\alpha_3)} = \frac{1}{g(\alpha^2)} = \frac{1}{\alpha^2+1} = \{(100)+(001)\}^{-1} = \{(101)\}^{-1} = \alpha^{-6}$$

$$\frac{1}{g(\alpha_4)} = \frac{1}{g(\alpha^3)} = \frac{1}{\alpha^3+1} = \{(011)+(001)\}^{-1} = \{(010)\}^{-1} = \alpha^{-1}$$

$$\frac{1}{g(\alpha_5)} = \frac{1}{g(\alpha^4)} = \frac{1}{\alpha^4+1} = \{(110)+(001)\}^{-1} = \{(111)\}^{-1} = \alpha^{-5}$$

$$\frac{1}{g(\alpha_6)} = \frac{1}{g(\alpha^5)} = \frac{1}{\alpha^5+1} = \{(111)+(001)\}^{-1} = \{(110)\}^{-1} = \alpha^{-4}$$

$$\frac{1}{g(\alpha_7)} = \frac{1}{g(\alpha^6)} = \frac{1}{\alpha^6+1} = \{(101)+(001)\}^{-1} = \{(100)\}^{-1} = \alpha^{-2}$$

以上より、Zは、

$$Z = \begin{pmatrix} \frac{1}{g(\alpha_1)} & 0 & 0 & & 0 \\ 0 & \frac{1}{g(\alpha_2)} & 0 & \cdots & 0 \\ 0 & 0 & \frac{1}{g(\alpha_3)} & & 0 \\ & \vdots & & \ddots & \\ 0 & 0 & 0 & & \frac{1}{g(\alpha_n)} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha^{-3} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha^{-6} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha^{-1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha^{-5} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \alpha^{-4} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{-2} \end{pmatrix}$$

となる。従って、H は以下のように求められる。

$$H = XYZ = (1)\cdot(1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1)\cdot\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha^{-3} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha^{-6} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha^{-1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha^{-5} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \alpha^{-4} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{-2} \end{pmatrix}$$

$$= (1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1)\cdot\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha^{-3} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha^{-6} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha^{-1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha^{-5} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \alpha^{-4} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{-2} \end{pmatrix}$$

$$= (1 \quad \alpha^{-3} \quad \alpha^{-6} \quad \alpha^{-1} \quad \alpha^{-5} \quad \alpha^{-4} \quad \alpha^{-2}) = (1 \quad \alpha^4 \quad \alpha^1 \quad \alpha^6 \quad \alpha^2 \quad \alpha^3 \quad \alpha^5) = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

生成行列Gは、$GH^T = 0$より得られる。

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

$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$ の 1 列目と 7 列目を入れ替えて、$H_{17} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$。次に、3 列目と 6

列目を入れ替えて、$H_{17/36} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$

よって、$G_{17/36} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$　これを 3 列目と 6 列目、1 列目と 7 列目を入れ替えて、$G =$

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

（カシオのサイト https://keisan.casio.jp/exec/system/1308269580 で確認した）

全符号語は、Gの線形結合によって求められる。

行の番号	線形結合	巡回のパタン	重み
①	**1010 101**	-	4
②	**0110 100**	-	3
③	**1010 010**	-	3
④	**1001 100**	-	3
①＋②	**1100 001**	-	3
①＋③	**0000 111**	-	3
①＋④	**0011 001**	-	3
②＋③	**1100 110**	-	4
②＋④	**1111 000**	-	4
③＋④	**0011 110**	-	4
①＋②＋③	**0110 011**	-	4
①＋②＋④	**0101 101**	-	4
①＋③＋④	**1001 011**	-	4
②＋③＋④	**0101 010**	-	3
①＋②＋③＋④	**1111 111**	-	7
①＋①	**0000 000**	-	0

・この Goppa(7, 4)符号は、非巡回ハミング(7, 4)符号である。

７．３．６　McEliece 暗号

公開鍵暗号の一種である。

$GF(q^m)$上のt次の separable 多項式$g(z)$とLによって定義される$(n, k \geq n - mt, d \geq 2t + 1)$Goppa 符号を考える。$k \times n$の生成行列$G$、random dense $k \times k$ nonsingular 行列S、$n \times n$ permutation 行列Pを求める。$G^* = SGP$とする。G^*とtを公開し、それ以外を秘密鍵とする。

送信者：

長さkの二進文字列を送信するとする。m個の二進文字列ごとに、長さnのランダムなエラーパタンeを計算する。ただし、eの最大重みはtとする。mを$y = mG^* + e$ と暗号化して送信する。

受信者：

$$y' = yP^{-1} = mG^*P^{-1} + eP^{-1} = mSGPP^{-1} + e' = (mS)G + e'$$

ここでe'の最大重みはtである。通常の（暗号化していない時の）Goppa 復号によりe'を求め、$m' = mS$よりm'を求める。その後、$m = m'S^{-1}$よりmを求める。

McEliece は、具体的な方法として、$m = 10,\ t = 50$次元の既約多項式$g(z), n = 2^{10} = 1024,\ k \geq 1024 - 10 * 50 = 525$の暗号化を議論している。

７．３．７　発展

・復号アルゴリズム　ベールカンプ＝マッシー法

・McEliece 暗号　の具体例

７．３．８　有理数

Goppa 符号では有理数で符号が定義されるが、これは項の加算に変形できる。

例を以下に示す。原始多項式を$p(z) = z^4 + z + 1$とする。

$$\frac{b}{z + a} = z^2 + cz + d \mod p(z)$$

$$b = (z + a)(z^2 + cz + d) = z^3 + (a + c)z^2 + (ac + d)z + ad \mod p(z)$$

$$z^3 + (a + c)z^2 + (ac + d)z + ad - b = 0 \mod p(z)$$

$$\alpha^3 + (a + c)\alpha^2 + (ac + d)\alpha + ad - b = 0$$

これが満たされるように、a, b, c, dを求めることができる。

以下は配布せず

７．３．８　Goppa 例の追加

■例３（Goppa で巡回ハミング（7,4）となる例）

$GF(2^3)$上の Goppa 符号を考える。$q=2,\quad m=3$

原始多項式を$ap(x)=x^3+x+1$　とする。

１）x^7+1の因数分解。省略

２）原始多項式からの拡大体の構成。

多項式	ベクトル表現	αべき表現	
0	000	0	
1	001	1	$=\alpha^0$
x	010	α	$=\alpha^1$
$x+1$	011	$\alpha+1$	$=\alpha^3$
x^2	100	α^2	$=\alpha^2$
x^2+1	101	α^2+1	$=\alpha^6$
x^2+x	110	$\alpha^2+\alpha$	$=\alpha^4$
x^2+x+1	111	$\alpha^2+\alpha+1$	$=\alpha^5$

拡大体は$GF(2^3)=\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6\}$

３）ゴッパ集合Lを以下とする。$L\subseteq GF(2^3)$　（Lは$GF(2^3)$の部分集合）

$$L=\{1,\alpha^1,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6\}$$

ゴッパ集合Lの要素数により、符号長nが決定される。この場合は、$n=7$である。

４）ゴッパ多項式 $g(z)$を決める。$g(z)$の根は、ゴッパ集合Lに含まれないようにする。

ここでは、以下とする。

$$g(z)=z=g_1z+g_0$$

５）以上より、このゴッパ符号のパラメータは以下となる。

$$q=2,\quad m=3,\quad n=7,\quad t=1,\quad d\geq 2t+1=2+1=3$$

$\alpha_1=1\ \alpha_2=\alpha^1\ \alpha_3=\alpha^2\ \alpha_4=\alpha^3\ \alpha_5=\alpha^4\ \alpha_6=\alpha^5\ \alpha_7=\alpha^6\quad g_0=0\quad g_1=1$

これにより、$(7,4,3)$Goppa 符号が構成される。

６）検査行列 H を求める。

$H=XYZ$

$X:t\times t=1\times 1$行列、$Y:t\times n=1\times 7$行列、$Z:n\times n=7\times 7$行列、$H:t\times n=1\times 7$行列

まず、X行列を求める。

$$X=\begin{pmatrix} -g_t & -g_{t-1} & -g_{t-2} & \cdots & -g_1 \\ 0 & -g_t & -g_{t-1} & \cdots & -g_2 \\ 0 & 0 & -g_t & & -g_3 \\ & \vdots & & \ddots & \\ 0 & 0 & 0 & & -g_t \end{pmatrix}=(-g_1)=(1)$$

次に、Y行列を求める。

$$Y=\begin{pmatrix} {\alpha_1}^{t-1} & {\alpha_2}^{t-1} & {\alpha_3}^{t-1} & \cdots & {\alpha_n}^{t-1} \\ {\alpha_1}^{t-2} & {\alpha_2}^{t-2} & {\alpha_3}^{t-2} & & {\alpha_n}^{t-2} \\ {\alpha_1}^{t-3} & {\alpha_2}^{t-3} & {\alpha_3}^{t-3} & & {\alpha_n}^{t-3} \\ & \vdots & & & \\ {\alpha_1}^{1} & {\alpha_2}^{1} & {\alpha_3}^{1} & \ddots & {\alpha_n}^{1} \\ 1 & 1 & 1 & & 1 \end{pmatrix}=(1\quad 1\quad 1\quad 1\quad 1\quad 1\quad 1)$$

Z行列を求める。

$$\frac{1}{g(\alpha_1)}=\frac{1}{g(1)}=\frac{1}{1}=1 \qquad \frac{1}{g(\alpha_2)}=\frac{1}{g(\alpha^1)}=\frac{1}{\alpha^1}=\alpha^{-1} \qquad \frac{1}{g(\alpha_3)}=\frac{1}{g(\alpha^2)}=\frac{1}{\alpha^2}=\alpha^{-2}$$

$\frac{1}{g(\alpha_4)} = \frac{1}{g(\alpha^3)} = \frac{1}{\alpha^3} = \alpha^{-3}$　$\frac{1}{g(\alpha_5)} = \frac{1}{g(\alpha^4)} = \frac{1}{\alpha^4} = \alpha^{-4}$　$\frac{1}{g(\alpha_6)} = \frac{1}{g(\alpha^5)} = \frac{1}{\alpha^5} = \alpha^{-5}$　$\frac{1}{g(\alpha_7)} = \frac{1}{g(\alpha^6)} = \frac{1}{\alpha^6} = \alpha^{-6}$

以上より、Zは、

$$Z = \begin{pmatrix} \frac{1}{g(\alpha_1)} & 0 & 0 & & 0 \\ 0 & \frac{1}{g(\alpha_2)} & 0 & \cdots & 0 \\ 0 & 0 & \frac{1}{g(\alpha_3)} & & 0 \\ & \vdots & & \ddots & \\ 0 & 0 & 0 & & \frac{1}{g(\alpha_n)} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha^{-1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha^{-2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha^{-3} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha^{-4} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \alpha^{-5} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{-6} \end{pmatrix}$$

となる。従って、H は以下のように求められる。

$$H = XYZ = (1) \cdot (1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1) \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha^{-1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha^{-2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha^{-3} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha^{-4} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \alpha^{-5} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{-6} \end{pmatrix}$$

$$= (1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1) \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha^{-1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha^{-2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha^{-3} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha^{-4} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \alpha^{-5} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{-6} \end{pmatrix} = (1 \quad \alpha^{-1} \quad \alpha^{-2} \quad \alpha^{-3} \quad \alpha^{-4} \quad \alpha^{-5} \quad \alpha^{-6}) =$$

$$= (1 \quad \alpha^6 \quad \alpha^5 \quad \alpha^4 \quad \alpha^3 \quad \alpha^2 \quad \alpha^1) = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

生成行列Gは、$GH^T = 0$より得られる。

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

$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$ の１列目と５列目を入れ替えて、$H_{15} = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$。次に、行を入れ替えて$H_{15} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$

よって、$G_{15} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$　これを１列目と５列目を入れ替えて$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$

（カシオのサイト https://keisan.casio.jp/exec/system/1308269580 で確認した）

全符号語は、Gの線形結合によって求められる。

行の番号	線形結合	巡回のパタン	重み
①	**1000 101**	1011	3
②	**1100 010**	1011	3
③	**1010 011**	11101	4

④	***0001 011***	1011	3
①＋②	***0100 111***	11101	4
①＋③	***0010 110***	1011	3
①＋④	***1001 110***	11101	4
②＋③	***0110 001***	1011	3
②＋④	***1101 001***	11101	4
③＋④	***1011 000***	1011	3
①＋②＋③	***1110 100***	11101	4
①＋②＋④	***0101 100***	1011	3
①＋③＋④	***0011 101***	11101	4
②＋③＋④	***0111 010***	11101	4
①＋②＋③＋④	***1111 111***		7
①＋①	***0000 000***		0

・この Goppa(7, 4)符号は、巡回ハミング(7, 4)符号である。

■例４

（ゴッパ多項式が non separable（重根を持つ）の例。（剰余計算が容易になる？反面、最小距離が$t+1$となる。）（Amsterdam 大の資料 Jochemsz, Ellen. “Goppa Codes & the McEliece Cryptosystem. ” Amsterdam: Vrije Universiteit Amsterdam, 2002. Print. https://pdfcoffee.com/goppa-codes-and-the-mceliece-cryptosystem-pdf-free.html p.10, 2.6.2 を元にした。ただし途中から異なる）

例１と同様に、$GF(2^4)$上の Goppa 符号を考える。$q=2,\quad m=4$

原始多項式を$ap(x)=x^4+x+1$　とする。

１）ゴッパ集合Lを以下とする。$L \subseteq GF(2^4)$　（Lは$GF(2^4)$の部分集合）

$$L=\{\alpha^i\ such\ that\ \ 1\le i\le 9\}=\{\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9\}$$

ゴッパ集合Lの要素数により、符号長nが決定される。この場合は、$n=9$である。

２）ゴッパ多項式 $g(z)$を決める。$g(z)$の根は、ゴッパ集合Lに含まれないようにする。

ここでは、以下とする。（non separable）

$$g(z)=z^2-1=g_2z^2+g_1z+g_0$$

３）以上より、このゴッパ符号のパラメータは以下となる。

$$q=2,\quad m=4,\quad n=9,\quad t=2,\quad k\ge 9-4*2=1,\quad d\ge t+1=2+1=3$$

$\alpha_1=\alpha^1\ \ \alpha_2=\alpha^2\ \ \alpha_3=\alpha^3\ \ \alpha_4=\alpha^4\ \ \alpha_5=\alpha^5\ \ \alpha_6=\alpha^6\ \ \alpha_7=\alpha^7\ \ \alpha_8=\alpha^8\ \ \alpha_9=\alpha^9$

$g_0=1\quad g_1=0\quad g_2=1$

これにより、$(9,\ge 1,\ge 3)$Goppa 符号が構成されることが確定する。実際には、以下の議論のように、(9, 5, 3)Goppa 符号となる。

４）$h_i=\{g(\alpha_i)\}^{-1}$ を計算してHを得る。例えば、

$h_1=\{g(\alpha)\}^{-1}=\{\alpha^2-1\}^{-1}=\{(0100)+(0001)\}^{-1}=\{(0101)\}^{-1}=\{\alpha^8\}^{-1}=\alpha^{-8}=\alpha^7$

よって、

$$H=\begin{pmatrix}\alpha^1h_1 & \alpha^2h_2 & \cdots & \alpha^9h_9\\ h_1 & h_2 & \cdots & h_9\end{pmatrix}=\begin{pmatrix}\alpha^8 & \alpha^1 & \alpha^5 & \alpha^2 & \alpha^0 & \alpha^{10} & \alpha^4 & \alpha^4 & \alpha^{10}\\ \alpha^7 & \alpha^{14} & \alpha^2 & \alpha^{13} & \alpha^{10} & \alpha^4 & \alpha^{12} & \alpha^{11} & \alpha^1\end{pmatrix}$$

$\frac{1}{z-\alpha^9}=\alpha^{10}+\alpha^1z\ \ (mod\ z^2-1)$　である。なぜならば、

$$(z-\alpha^9)(\alpha^{10}+\alpha^1z)=\alpha^1z^2+\alpha^4=\alpha^1z^2+\alpha^4+\alpha\ \ (z^2-1)=\alpha^4-\alpha\quad =1\ mod\ g(z)$$

Hをベクトル表現すれば、以下となる。

$$H=\begin{pmatrix}\alpha^8 & \alpha^1 & \alpha^5 & \alpha^2 & \alpha^0 & \alpha^{10} & \alpha^4 & \alpha^4 & \alpha^{10}\\ \alpha^7 & \alpha^{14} & \alpha^2 & \alpha^{13} & \alpha^{10} & \alpha^4 & \alpha^{12} & \alpha^{11} & \alpha^1\end{pmatrix}=\begin{pmatrix}0&0&0&0&0&0&0&0&0\\1&0&1&1&0&1&0&0&1\\0&1&1&0&0&1&1&1&1\\1&0&0&0&1&1&1&1&1\\1&1&0&1&0&0&1&1&0\\0&0&1&1&1&0&1&1&0\\1&0&0&0&1&1&1&1&1\\1&1&0&1&1&1&1&0&0\end{pmatrix}$$

生成行列Gは、$GH^T=0$より得られる。まず、Hの零空間(null space)の基底を求める。Hを以下のように基本変形して RREF(Reduced Row Echelon Form)を求める。なお、Hのランクは４である。

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

ここから、null space の基底は、(0 1 1 1 0 0 0 0 0) (0 0 1 0 1 1 0 0 0) (1 0 1 0 0 0 1 0 0) (0 1 0 0 1 0 0 1 0) (1 1 0 0 0 0 0 0 1) となる。（https://www.mathdetail.com/null.php にて確認）

これにより、生成行列Gが求められる。n – rankH = k (9-4=5)

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

（カシオのサイトで GHt=0 を確認した。https://keisan.casio.jp/exec/system/1308269580 ）

ここから、全符号語が以下のように求められる。各行を①、②、③、④、⑤とする。

1）自己の加算　5C0　個

00000000

2）①～⑤そのもの　5C1=5 個

01110 0000　00101 1000　10100 0100　01001 0010　11000 0001

3） 2 個の組み合わせ　5C2 = 10

①＋②01011 1000　①＋③11010 0100　①＋④00111 0010　①＋⑤10110 0001

②＋③10001 1100　②＋④01100 1010　②＋⑤11101 1001　③＋④11101 0110

③＋⑤01100 0101　④＋⑤10001 0011

4） 3 個の組み合わせ　5C3 = 10

①＋②＋③11111 1100　①＋②＋④00010 1010　①＋②＋⑤10011 1001　①＋③＋④10011 0110

①＋③＋⑤00010 0101　①＋④＋⑤11111 0011　②＋③＋④11000 1110　②＋③＋⑤01001 1101

②＋④＋⑤10100 1011　③＋④＋⑤00101 0111

5） 4 個の組み合わせ　5C4 = 5 個

①＋②＋③＋④10110 1110　①＋②＋③＋⑤00111 1101　①＋②＋④＋⑤11010 1011

①＋③＋④＋⑤01011 0111　②＋③＋④＋⑤11010 1011

6） 5 個の組み合わせ　5C5 = 1

①＋②＋③＋④＋⑤01110 1111

以上、32 個が符号語であり、最小重みは、3 である。また非巡回符号でもある。この符号は、(9, 5, 3)Goppa 符号である。

H から null space basis を求める方法：

RREF が求められた後、Ax=0 の連立方程式に戻して考える。

例４の場合。詳細な計算は、https://www.mathdetail.com/null.php

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

$$\begin{pmatrix}1&0&0&0&0&0&1&0&1\\0&1&0&1&0&0&0&1&1\\0&0&1&1&0&1&1&0&0\\0&0&0&0&1&1&0&1&0\\0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\x_5\\x_6\\x_7\\x_8\\x_9\end{pmatrix}=0$$

$$\begin{pmatrix}1&0&0&0&0&0&1&0&1\\0&1&0&1&0&0&0&1&1\\0&0&1&1&0&1&1&0&0\\0&0&0&1&0&0&0&0&0\\0&0&0&0&1&1&0&1&0\\0&0&0&0&0&1&0&0&0\\0&0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0&1\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\x_5\\x_6\\x_7\\x_8\\x_9\end{pmatrix}=\begin{pmatrix}0\\0\\0\\x_4\\0\\x_6\\x_7\\x_8\\x_9\end{pmatrix}$$

$$\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\x_5\\x_6\\x_7\\x_8\\x_9\end{pmatrix}=\begin{pmatrix}0&0&1&0&1\\1&0&0&1&1\\1&1&1&0&0\\1&0&0&0&0\\0&1&0&1&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}\begin{pmatrix}x_4\\x_6\\x_7\\x_8\\x_9\end{pmatrix}$$

$$\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\x_5\\x_6\\x_7\\x_8\\x_9\end{pmatrix}=x_4\begin{pmatrix}0\\1\\1\\1\\0\\0\\0\\0\\0\end{pmatrix}+x_6\begin{pmatrix}0\\0\\1\\0\\1\\1\\0\\0\\0\end{pmatrix}+x_7\begin{pmatrix}1\\0\\1\\0\\0\\0\\1\\0\\0\end{pmatrix}+x_8\begin{pmatrix}0\\1\\0\\0\\1\\0\\0\\1\\0\end{pmatrix}+x_9\begin{pmatrix}1\\1\\0\\0\\0\\0\\0\\0\\1\end{pmatrix}$$

これより、null space の基底は、(011100000) (001011000) (101000100) (010010010) (110000001) となる。（∵任意のベクトル$(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_9)$は、これらの線形結合となっている。また、$(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_9)=0$となる必要十分条件は、$x_4,x_6,x_7,x_8,x_9$がすべて 0 であることである。従って、一次独立である。以上より、(011100000) (001011000) (101000100) (010010010) (110000001)は、基底ベクトルである。なお、これらの基底ベクトルは直交していない。）

■例５

（Syracuse 大の資料 Ashley Valentijn: "Goppa Codes and Their Use in the McEliece Cryptosystems",
https://surface.syr.edu/cgi/viewcontent.cgi?article=1846&context=honors_capstone を元にした。
ただし、Syracuse 大は H の計算で誤りがあるため、H から異なる）

例１と同様に、$GF(2^4)$上の Goppa 符号を考える。$q=2,\quad m=4$

原始多項式を$ap(x)=x^4+x+1$　とする。

１）$x^{15}-1$の因数分解。省略

２）原始多項式からの拡大体の構成。省略

３）ゴッパ集合Lを以下とする。$L \subseteq GF(2^4)$　（Lは$GF(2^4)$の部分集合）

$$L=\{\alpha^i \; such\; that\; 2\le i\le 13\}=\{\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},\alpha^{11},\alpha^{12},\alpha^{13}\}$$

ゴッパ集合Lの要素数により、符号長nが決定される。この場合は、$n=12$である。

４）ゴッパ多項式 $g(z)$を決める。$g(z)$の根は、ゴッパ集合Lに含まれないようにする。

ここでは、以下とする。

$$g(z)=z^2+z+\alpha^3=g_2z^2+g_1z+g_0$$

５）以上より、このゴッパ符号のパラメータは以下となる。

$$q=2,\quad m=4,\quad n=12,\quad t=2,\quad d\ge 2t+1=4+1=5$$

$\alpha_1=\alpha^2\;\; \alpha_2=\alpha^3\;\; \alpha_3=\alpha^4\;\; \alpha_4=\alpha^5\;\; \alpha_5=\alpha^6\;\; \alpha_6=\alpha^7\;\; \alpha_7=\alpha^8\;\; \alpha_8=\alpha^9\;\; \alpha_9=\alpha^{10}\;\; \alpha_{10}=\alpha^{11}\;\; \alpha_{11}=\alpha^{12}\;\; \alpha_{12}=\alpha^{13}$

$g_0=\alpha^3\quad g_1=1\quad g_2=1$

これにより、$(12,\ge 4,\ge 5)$Goppa 符号が構成される。

６）検査行列 H を求める。

$H=XYZ$

$X: t\times t=2\times 2$行列、$Y: t\times n=2\times 12$行列、$Z: n\times n=12\times 12$行列、$H: t\times n=2\times 12$行列

まず、X行列を求める。

$$X=\begin{pmatrix} -g_t & -g_{t-1} & -g_{t-2} & \cdots & -g_1 \\ 0 & -g_t & -g_{t-1} & \cdots & -g_2 \\ 0 & 0 & -g_t & & -g_3 \\ & \vdots & & \ddots & \\ 0 & 0 & 0 & & -g_t \end{pmatrix}=\begin{pmatrix} -g_2 & -g_1 \\ 0 & -g_2 \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

次に、Y行列を求める。

$$Y=\begin{pmatrix} {\alpha_1}^{t-1} & {\alpha_2}^{t-1} & {\alpha_3}^{t-1} & \cdots & {\alpha_n}^{t-1} \\ {\alpha_1}^{t-2} & {\alpha_2}^{t-2} & {\alpha_3}^{t-2} & & {\alpha_n}^{t-2} \\ {\alpha_1}^{t-3} & {\alpha_2}^{t-3} & {\alpha_3}^{t-3} & & {\alpha_n}^{t-3} \\ & \vdots & & & \\ {\alpha_1}^{1} & {\alpha_2}^{1} & {\alpha_3}^{1} & \ddots & {\alpha_n}^{1} \\ 1 & 1 & 1 & & 1 \end{pmatrix}$$

$$=\begin{pmatrix} \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Z行列を求める。

$$\frac{1}{g(\alpha_1)}=\frac{1}{(\alpha^2)^2+\alpha^2+\alpha^3}=\frac{1}{\alpha^4+\alpha^2+\alpha^3}=\{(0011)+(0100)+(1000)\}^{-1}=\{(1111)\}^{-1}=\{\alpha^{12}\}^{-1}=\alpha^{-12}=\alpha^3$$

$\frac{1}{g(\alpha_2)} = \frac{1}{(\alpha^3)^2+\alpha^3+\alpha^3} = \frac{1}{\alpha^6} = \alpha^{-6} = \alpha^9$

$\frac{1}{g(\alpha_3)} = \frac{1}{(\alpha^4)^2+\alpha^4+\alpha^3} = \frac{1}{\alpha^8+\alpha^4+\alpha^3} = \{(0101) + (0011) + (1000)\}^{-1} = \{(1110)\}^{-1} = \{\alpha^{11}\}^{-1} = \alpha^{-11} = \alpha^4$

$\frac{1}{g(\alpha_4)} = \frac{1}{(\alpha^5)^2+\alpha^5+\alpha^3} = \frac{1}{\alpha^{10}+\alpha^5+\alpha^3} = \{(0111) + (0110) + (1000)\}^{-1} = \{(1001)\}^{-1} = \{\alpha^{14}\}^{-1} = \alpha^{-14} = \alpha^1$

$\frac{1}{g(\alpha_5)} = \frac{1}{(\alpha^6)^2+\alpha^6+\alpha^3} = \frac{1}{\alpha^{12}+\alpha^6+\alpha^3} = \{(1111) + (1100) + (1000)\}^{-1} = \{(1011)\}^{-1} = \{\alpha^7\}^{-1} = \alpha^{-7} = \alpha^8$

$\frac{1}{g(\alpha_6)} = \frac{1}{(\alpha^7)^2+\alpha^7+\alpha^3} = \frac{1}{\alpha^{14}+\alpha^7+\alpha^3} = \{(1001) + (1011) + (1000)\}^{-1} = \{(1010)\}^{-1} = \{\alpha^9\}^{-1} = \alpha^{-9} = \alpha^6$

$\frac{1}{g(\alpha_7)} = \frac{1}{(\alpha^8)^2+\alpha^8+\alpha^3} = \frac{1}{\alpha^{16}+\alpha^8+\alpha^3} = \frac{1}{\alpha^1+\alpha^8+\alpha^3} = \{(0010) + (0101) + (1000)\}^{-1} = \{(1111)\}^{-1} = \alpha^{-12} = \alpha^3$

$\frac{1}{g(\alpha_8)} = \frac{1}{(\alpha^9)^2+\alpha^9+\alpha^3} = \frac{1}{\alpha^{18}+\alpha^9+\alpha^3} = \frac{1}{\alpha^3+\alpha^9+\alpha^3} = \alpha^{-9} = \alpha^6$

$\frac{1}{g(\alpha_9)} = \frac{1}{(\alpha^{10})^2+\alpha^{10}+\alpha^3} = \frac{1}{\alpha^{20}+\alpha^{10}+\alpha^3} = \frac{1}{\alpha^5+\alpha^{10}+\alpha^3} = \{(0110) + (0111) + (1000)\}^{-1} = \{(1001)\}^{-1} =$

$\{\alpha^{14}\}^{-1} = \alpha^{-14} = \alpha^1$

$\frac{1}{g(\alpha_{10})} = \frac{1}{(\alpha^{11})^2+\alpha^{11}+\alpha^3} = \frac{1}{\alpha^{22}+\alpha^{11}+\alpha^3} = \frac{1}{\alpha^7+\alpha^{11}+\alpha^3} = \{(1011) + (1110) + (1000)\}^{-1} = \{(1101)\}^{-1} =$

$\{\alpha^{13}\}^{-1} = \alpha^{-13} = \alpha^2$

$\frac{1}{g(\alpha_{11})} = \frac{1}{(\alpha^{12})^2+\alpha^{12}+\alpha^3} = \frac{1}{\alpha^{24}+\alpha^{12}+\alpha^3} = \frac{1}{\alpha^9+\alpha^{12}+\alpha^3} = \{(1010) + (1111) + (1000)\}^{-1} = \{(1101)\}^{-1} =$

$\{\alpha^{13}\}^{-1} = \alpha^{-13} = \alpha^2$

$\frac{1}{g(\alpha_{12})} = \frac{1}{(\alpha^{13})^2+\alpha^{13}+\alpha^3} = \frac{1}{\alpha^{26}+\alpha^{13}+\alpha^3} = \frac{1}{\alpha^{11}+\alpha^{13}+\alpha^3} = \{(1110) + (1101) + (1000)\}^{-1} = \{(1011)\}^{-1} =$

$\{\alpha^7\}^{-1} = \alpha^{-7} = \alpha^8$

以上より、Zは、

$$Z = \begin{pmatrix} \frac{1}{g(\alpha_1)} & 0 & 0 & & 0 \\ 0 & \frac{1}{g(\alpha_2)} & 0 & \cdots & 0 \\ 0 & 0 & \frac{1}{g(\alpha_3)} & & 0 \\ & \vdots & & \ddots & \\ 0 & 0 & 0 & & \frac{1}{g(\alpha_n)} \end{pmatrix}$$

$$= \begin{pmatrix} \alpha^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha^9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha^4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha^1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha^8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \alpha^6 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha^3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^8 \end{pmatrix}$$

となる。従って、H は以下のように求められる。

$$H = XYZ = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}\alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13}\\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\end{pmatrix}\begin{pmatrix}\alpha^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & \alpha^9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & \alpha^4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & \alpha^1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & \alpha^8 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & \alpha^6 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha^3 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^6 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^2 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^2 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^8\end{pmatrix}$$

$$= \begin{pmatrix}(\alpha^2+1) & (\alpha^3+1) & (\alpha^4+1) & (\alpha^5+1) & (\alpha^6+1) & (\alpha^7+1) & (\alpha^8+1) & (\alpha^9+1) & (\alpha^{10}+1) & (\alpha^{11}+1) & (\alpha^{12}+1) & (\alpha^{13}+1)\\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\end{pmatrix}$$

$$\begin{pmatrix}\alpha^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & \alpha^9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & \alpha^4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & \alpha^1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & \alpha^8 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & \alpha^6 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha^3 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^6 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^2 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^2 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^8\end{pmatrix}$$

$$= \begin{pmatrix}\alpha^8 & \alpha^{14} & \alpha^1 & \alpha^{10} & \alpha^{13} & \alpha^9 & \alpha^2 & \alpha^7 & \alpha^5 & \alpha^{12} & \alpha^{11} & \alpha^6\\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\end{pmatrix}\begin{pmatrix}\alpha^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & \alpha^9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & \alpha^4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & \alpha^1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & \alpha^8 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & \alpha^6 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha^3 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^6 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^2 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^2 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^8\end{pmatrix}$$

$$= \begin{pmatrix}\alpha^{11} & \alpha^{23} & \alpha^5 & \alpha^{11} & \alpha^{21} & \alpha^{15} & \alpha^5 & \alpha^{13} & \alpha^6 & \alpha^{14} & \alpha^{13} & \alpha^{14}\\ \alpha^3 & \alpha^9 & \alpha^4 & \alpha^1 & \alpha^8 & \alpha^6 & \alpha^3 & \alpha^6 & \alpha^1 & \alpha^2 & \alpha^2 & \alpha^8\end{pmatrix} = \begin{pmatrix}\alpha^{11} & \alpha^8 & \alpha^5 & \alpha^{11} & \alpha^6 & \alpha^0 & \alpha^5 & \alpha^{13} & \alpha^6 & \alpha^{14} & \alpha^{13} & \alpha^{14}\\ \alpha^3 & \alpha^9 & \alpha^4 & \alpha^1 & \alpha^8 & \alpha^6 & \alpha^3 & \alpha^6 & \alpha^1 & \alpha^2 & \alpha^2 & \alpha^8\end{pmatrix}$$

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

$\alpha^2+1 = (0100)+(0001) = (0101) = \alpha^8$　　$\alpha^3+1 = (1000)+(0001) = (1001) = \alpha^1$　　$\alpha^{\ }+1 = (0011)+(0001) = (0010) = \alpha^1$
$\alpha^5+1 = (0110)+(0001) = (0111) = \alpha^{10}$　　$\alpha^6+1 = (1100)+(0001) = (1101) = \alpha^{13}$　　$\alpha^7+1 = (1011)+(0001) = (1010) = \alpha^9$
$\alpha^8+1 = (0101)+(0001) = (0100) = \alpha^2$　　$\alpha^9+1 = \alpha^7$　　$\alpha^{10}+1 = \alpha^5$　　$\alpha^{11}+1 = (1110)+(0001) = (1111) = \alpha^{12}$
$\alpha^{12}+1 = \alpha^{11}$　　$\alpha^{13}+1 = \alpha^6$

生成行列Gは、$GH^T = 0$より得られる。まず、Hの零空間(null space)の基底を求める。Hを以下のように基本変形して RREF(Reduced Row Echelon Form)を求める。なお、Hのランクは８である。

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

ここから、null space の基底は、(１０１１１１１１０００)　(１１０００１１０１０００)　(０１１０１０１００１００)　(１１０１１０００００１)　となる。（https://www.mathdetail.com/null.php にて確認）

これにより、生成行列Gが求められる。n – rankH = k (12-8=4)

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

全符号語は、Gの線形結合によって求められる。

Goppa(12, 4, 5)符号

行の番号	線形結合	重み
①	1011 1111 0000	7
②	1100 0110 1000	5
③	0110 1010 0100	5
④	1101 1000 0001	5
①＋②	0111 1001 1000	6
①＋③	1101 0101 0100	6
①＋④	0110 0111 0001	6
②＋③	1010 1100 1100	6
②＋④	0001 1110 1001	6
③＋④	1011 0010 0101	6
①＋②＋③	0001 0011 1100	5
①＋②＋④	1010 0001 1001	5
①＋③＋④	0000 1101 0101	5
②＋③＋④	0111 0100 1101	7
①＋②＋③＋④	1100 1011 1101	8
①＋①	0000 0000 0000	0

Syracuse 大の資料では以下となっている。

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

（GHt=0 であるので、この G も生成行列になりうる。

（ Ashley Valentijn: "Goppa Codes and Their Use in the McEliece Cryptosystems", https://surface.syr.edu/cgi/viewcontent.cgi?article=1846&context=honors_capstone）

https://wims.unice.fr/~wims/wims.cgi?session=QSE853E244.3&+lang=en&+module=tool%2Flinear%2Fmatrix.en で確認した。

https://wims.unice.fr/~wims/wims.cgi?session=QSE853E244.5&lang=en&cmd=reply&module=tool%2Flinear%2Fmatmult.en&matA=1%2C0%2C0%2C1%2C1%2C0%2C0%2C1%2C1%2C1%2C1%2C1%0D%0A1%2C1%2C1%2C1%2C1%2C0%2C1%2C1%2C1%2C0%2C1%2C0%0D%0A1%2C0%2C1%2C1%2C0%2C0%2C1%2C0%2C0%2C0%2C0%2C0%0D%0A0%2C1%2C0%2C0%2C0%2C1%2C0%2C1%2C0%2C1%2C1%2C1%0D%0A1%2C1%2C0%2C0%2C0%2C1%2C1%2C1%2C0%2C0%2C0%2C0%0D%0A0%2C0%2C0%2C0%2C1%2C0%2C0%2C1%2C0%2C1%2C1%2C1%0D%0A0%2C1%2C1%2C1%2C0%2C0%2C0%2C0%2C1%2C0%2C0%2C0%0D%0A0%2C0%2C1%2C0%2C1%2C0%2C0%2C0%2C0%2C0%2C0%2C1&matB=0%2C0%2C1%2C1%0D%0A1%2C1%2C1%2C1%0D%0A1%2C1%2C0%2C1%0D%0A0%2C1%2C1%2C0%0D%0A1%2C1%2C1%2C1%0D%0A0%2C0%2C0%2C1%0D%0A1%2C0%2C0%2C0%0D%0A0%2C1%2C0%2C1%0D%0A0%2C1%2C0%2C0%0D%0A1%2C0%2C0%2C0%0D%0A0%2C0%2C0%2C1%0D%0A0%2C0%2C1%2C0&sh

ow=A*B

全符号語は、Gの線形結合によって求められる。

Goppa(12, 4, 5)符号

行の番号	線形結合	重み
①	0110 1010 0100	5
②	0111 1001 1000	6
③	1101 1000 0001	5
④	1110 1101 0010	7
①＋②	0001 0011 1100	5
①＋③	1011 0010 0101	6
①＋④	1000 0111 0110	6
②＋③	1010 0001 1001	5
②＋④	1001 0100 1010	5
③＋④	0011 0101 0011	6
①＋②＋③	1100 1011 1101	8
①＋②＋④	1111 1110 1110	10
①＋③＋④	0101 1111 0111	9
②＋③＋④	0100 1100 1011	6
①＋②＋③＋④	0010 0110 1111	7
①＋①	0000 0000 0000	0

・この符号は、符号語間の距離がすべて５以上であり、２誤り訂正が可能である。

７．３．９　McEliece 暗号と復号例

（１）概要

公開鍵暗号の一種である。

$GF(q^m)$上のt次の separable 多項式$g(z)$とLによって定義される$(n, k \geq n - mt, d \geq 2t + 1)$Goppa 符号を考える。$k \times n$の生成行列$G$、random dense $k \times k$ nonsingular 行列S、$n \times n$ permutation 行列Pを求める。$G^* = SGP$とする。G^*とtを公開し、それ以外を秘密鍵とする。

送信者：

長さkの二進文字列を送信するとする。m個の二進文字列ごとに、長さnのランダムなエラーパタンeを計算する。ただし、eの最大重みはtとする。mを$y = mG^* + e$ と暗号化して送信する。

受信者：

$$y' = yP^{-1} = mG^*P^{-1} + eP^{-1} = mSGPP^{-1} + e' = (mS)G + e'$$

ここでe'の最大重みはtである。通常の（暗号化していない時の）Goppa 復号によりe'を求め、$m' = mS$よりm'を求める。その後、$m = m'S^{-1}$よりmを求める。

McEliece は、具体的な方法として、$m = 10,\ t = 50$次元の既約多項式$g(z), n = 2^{10} = 1024,\ k \geq 1024 - 10 * 50 = 525$の暗号化を議論している。

（２）例

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

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

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

とする。

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

送信側：$m = (m_1\ m_2\ m_3\ m_4) = (0\ 1\ 0\ 1)$を暗号化して送信する。

$$mG^* = (0\ 1\ 0\ 1)\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} = (1\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1)$$

$$y = mG^* + e = (1\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1) + (0\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0) = (1\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1)$$

受信側：

$$yP^{-1} = (1\,0\,0\,1\,0\,1\,0\,0\,0\,1\,1\,1)\begin{pmatrix}0&0&0&1&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0&0&1&0\\0&0&0&0&1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0&0&0&0&0\\1&0&0&0&0&0&0&0&0&0&0&0\\0&0&0&0&0&1&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0&0&0&0&0\\0&0&0&0&0&0&0&0&0&1&0&0\\0&0&1&0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&1&0&0&0\\0&0&0&0&0&0&0&1&0&0&0&0\end{pmatrix}^{-1} = mSG + e' = (1\,1\,0\,0\,1\,1\,1\,0\,1\,0\,0\,0)$$

$$mSG = (1\,1\,0\,1\,1\,1\,1\,0\,1\,1\,0\,0)$$

$$[G^T|(mS)^T] = \left(\begin{array}{cccc|c}1&0&0&0&1\\1&1&0&1&1\\1&0&1&0&0\\1&0&0&1&1\\0&1&1&0&1\\1&1&0&0&1\\0&1&1&1&1\\1&1&1&1&0\\0&0&1&0&1\\1&0&0&0&1\\0&1&0&0&0\\0&0&0&1&0\end{array}\right)$$

行列の基本変形を行って以下を得る。

$$[G^T|(mS)^T] \sim \left(\begin{array}{cccc|c}1&0&0&0&1\\0&1&0&0&0\\0&0&1&0&1\\0&0&0&1&0\\1&1&0&1&1\\1&0&1&0&0\\1&0&0&1&1\\0&1&1&0&1\\1&1&0&0&1\\0&1&1&1&1\\1&1&1&1&0\\1&0&0&0&1\end{array}\right) = \begin{pmatrix} I_k & \vdots \; m_1 S \\ \hline A_{(n-k)(k+1)} & \vdots \; m_k S \end{pmatrix}$$

ここで、~は行列の基本変形、I_kは$k \times k$の単位行列、$A_{(n-k)(k+1)}$は$(n-k) \times (k+1)$の行列である。行列の右上より、$mS = (1\,0\,1\,0)$となる。これから、

$$m = mS \cdot S^{-1} = (1\,0\,1\,0) \cdot \begin{pmatrix}1&0&1&1\\0&1&0&1\\1&1&0&1\\1&1&1&1\end{pmatrix}^{-1} = (0\,1\,0\,1)$$

となり、復号できる。

７．４　その他の話題

７．４．１　実際に使われている符号

１）QR (Quick Response)コード

符号語：８ビット　リードソロモン符号

各ブロックはリードソロモン符号語　　フォーマット情報:BCH 符号

エラー訂正レベル

L (Low)　　約 7%エラー訂正可

M (Medium)　約 15%エラー訂正可

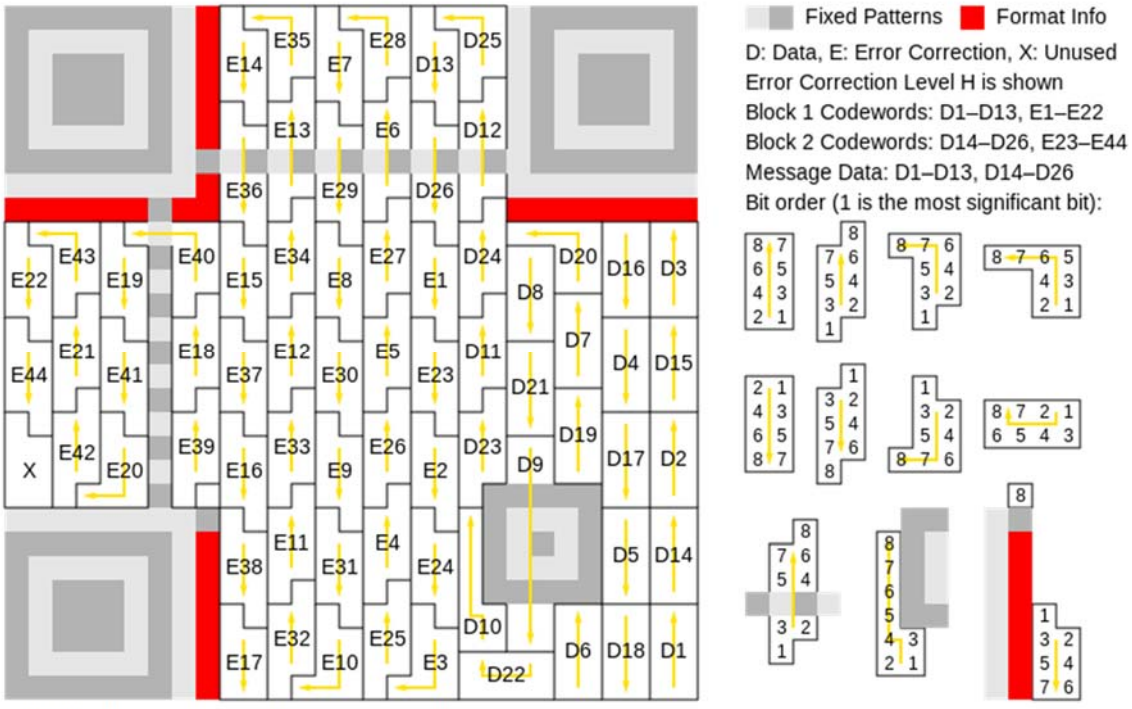
Q (Quartile)　約 25%エラー訂正可

H (High)　　約 30%エラー訂正可

短縮(n, k, t)RS 符号の生成多項式　$G(x) = (x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{n-k-1})$

型番	総コード数	誤り訂正レベル	(n, k, t)	RS ブロック数	生成多項式次数
1	２６	L	26, 19, 2	1	7
1	３６	M	26, 16, 4	1	１０
1	２６	Q	26, 13, 6	1	１３
1	２６	H	26, 9, 8	1	１７
2	４４	L	44, 34, 4	1	１０
2	４４	M	44, 28, 8	1	１６
2	４４	Q	44, 22, 11	1	２２
2	４４	H	44, 16, 14	1	２８
3	７０	L	70, 55, 7	1	１５
3	７０	M	70, 44, 13	1	２６
3	７０	Q	35, 17, 9	2	１８
3	７０	H	35, 13, 11	2	２２

例：3-H の場合、(n, k, t)=(35, 13, 11)



(3H 型 QR コード　Wikipedia 英語版より)

２）　CRC (Cyclic Redundancy Check)　巡回冗長検査

・誤り検出を目的とした符号化。多くの分野で用いられている。

・よく利用される符号

CRC-16-CCITT

$p(x) = x^{16} + x^{12} + x^5 + 1 = (x+1)(x^{15} + x^{14} + x^{13} + x^{12} + x^4 + x^3 + x^2 + x + 1)$　(0x1021)

この数字は 4bit ずつ区切った 0001 0000 0010 0001 を表現しており、

x^{12}, x^5, x^0が要素として存在することを意味している。（x^{16}は当然なので省略）

X.25, V.41, HDLC, Bluetooth, SD, etc.

CRC-16-ANSI(IBM)　$p(x) = x^{16} + x^{15} + x^2 + 1 = (x+1)(x^{15} + x + 1)$　(0x8005)

USB データ他

CRC-32　$p(x) = x^{32} + x^{26} + \cdots\cdots + x^{15} + 1$　(0x04C11DB7)

V.42, Ethernet, IEEE802.3, Serial ATA, MPEG2, Zip, PNG 他

32 ビット以下のバースト誤りを検出可能

バースト長 33 の誤りを検出できない確率=$\left(1/2\right)^{33}$ =20 億分の 1

その他、CRC-32C(Castagnoli), CRC-32K(Koopman)など

・Koopman , Castagnoli at CMU らの議論(Koopman, 2002 など)

CRC-32 の（最小）ハミング距離=4

3bit 誤り検出可能、4bit 誤りでは 223059 の正しい符号語が存在。

フレーム長 1514bytes+CRC32bit=12144bit　で、4bit 誤る組み合わせは、

$$\binom{12144}{4} = 9.06 \times 10^{14}$$

よって、4bit 誤りを誤訂正する確率は、$223059 / \binom{12144}{4} = 2.46 \times 10^{-10}$

3）　BCH, RS のその他の応用

・RS 符号　　ボイジャー Deep space communication

・QR コード　　RS+BCH

・地上デジタル放送

RS(255, 239)

符号化生成多項式　$g(x) = (x+1)(x+\alpha^1)\cdots\cdots(x+\alpha^{15})$

体生成多項式　$p(x) = x^8 + x^4 + x^3 + x^2 + 1$

を元にした短縮化 RS(204, 188)がトランスポートストリーム(TS)パケットの符号化に用いられている。

未完 2020/7/11
赤文字、青文字、背景黄色などの部分は配布しない。

7．4．2　RS とフーリエ変換（RS 符号の別の表現）

今井秀樹著「符号理論」電子情報通信学会　第 7 章　p.158 より抜粋

本書では、GF(q)（q は素数のべき乗）で議論を行っているが、ここでは$GF(2^4)$に限定する。

定理 7．2　$GF(2^4)$に限定した定理

I_{k-1}, I_{k-2}, …, I_1, I_0 を$GF(2^4)$ の任意の元とし、これらを係数とする多項式

$I(y) = I_{k-1}y^{k-1} + I_{k-2}y^{k-2} + \cdots + I_1y^1 + I_0$ を考える。

このとき、α を$GF(2^4)$ の原始根とすれば、

$$w = (I(\alpha^{14}), I(\alpha^{13}), \cdots, I(\alpha^1), I(\alpha^0))$$

という$GF(2^4)$ 上のすべてのベクトルを符号語とする符号長$2^4 - 1 = 15$ の符号は、

$\alpha^1, \alpha^2, \cdots, \alpha^{16-1-k}$ を根とする$(2^4 - 1, k)$RS 符号となる。

【証明】

この定理を証明するには、$\alpha^1, \alpha^2, \cdots, \alpha^{16-1-k}$ （k 個）が

$$W(y) = I(\alpha^{14})y^{14} + I(\alpha^{13})y^{13} + \cdots + I(\alpha^1)y^1 + I(1)$$

の根となっていればよい。

w は、$(0, 0, \cdots, 0, I_{k-1}, I_{k-2}, \cdots, I_1, I_0)$ という$2^4 - 1 = 15$ 次元ベクトルのフーリエ変換となっている。（補足資料１：マトソンソロモン多項式の部分を参照する）

一方、$(W(\alpha^{-14}), W(\alpha^{-13}), \cdots, W(\alpha^{-1}), W(1))$ は、wのフーリエ逆変換である。従って、

$$W(\alpha^{-14}) = W(\alpha^{-13}) = \cdots = W(\alpha^{-k}) = 0$$

が得られる。このことは、$W(y)$が、$\alpha^{-14} = \alpha^1, \alpha^{-13} = \alpha^2, \cdots, \alpha^{-k} = \alpha^{16-1-k}$を根として持つこと、従って 16 元$(2^4 - 1, k)$RS 符号の符号多項式であることを意味している。

より一般の RS 符号については次の系が成立する。

系 7.2.1

定理７．２と同様の仮定のもとに、

$$\left(\alpha^{(l-1)*14}I(\alpha^{14}),\ \alpha^{(l-1)*13}I(\alpha^{13}),\ \cdots,\ \alpha^{(l-1)}I(\alpha^1),\ \alpha^{(l-1)}M(1)\right)$$

という$GF(2^4)$上のすべてのベクトルを符号語とする符号長$2^4 - 1 = 15$ の符号は、

$$\alpha^l, \alpha^{(l+1)}, \cdots, \alpha^{(l+16-1-k)}$$

を根とする$(2^4 - 1, k)$ RS 符号である。

（以下は、今井秀樹著「符号理論」電子情報通信学会　第７章　p.158 からの記述で q=16 とした場合）

定理７．２は、RS 符号が k-1 次以下の多項式 I(x)の$2^4 - 1 = 15$ 個の点における値を符号語とするものであることを意味している。これを直感的に示したのが図７．１である。

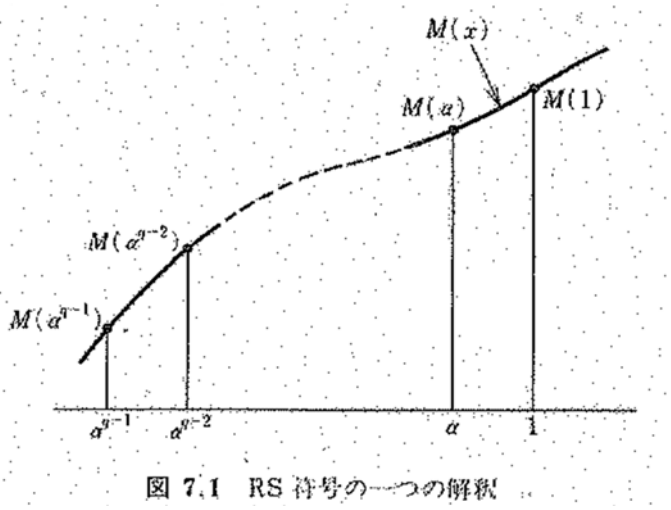


図 7.1　RS 符号の一つの解釈

$W(y) = I(\alpha^{14})y^{14} + I(\alpha^{13})y^{13} + \cdots + I(\alpha^1)y^1 + I(1)$ が 、 $\alpha^{-14} = \alpha^1, \alpha^{-13} = \alpha^2, \cdots, \alpha^{-k} = \alpha^{16-1-k}$を根として持つことを図に示すと、k 個の点で、曲線が一意に決定できることを利用している。

このような解釈によると$(2^4 - 1, k)$RS 符号の最小距離が$2^4 - k$ であることが、直感的にはすぐにわかる。実際、k 個の点をきめると、k-1 次以下の曲線（k-1 次以下の多項式で表現される曲線）は一通りに決まるから、k 個の点で 0 となる k-1 次以下の曲線はあらゆる点で 0 となる直線しかない。従って、式７．１６の形の非零の符号語は高々k-1 個の点でしか 0 となれず、ハミング重みは$2^4 - k$ 以上となるのである。

７．４．３　BCH 符号、RS 符号の初期値 l

第 7 章の資料では、BCH 符号では l=1、RS 符号では l=0 を挙げて説明した。ここでは、１）BCH 符号で l=0 の場合、２）RS 符号で、l=1 の場合を考える。

１）BCH 符号で、l=0 の場合

BCH の生成多項式は以下で構成される。

$$g(x)=\left[\prod_{i=l}^{l+d_{min}-2}\left(x-\alpha^{i}\right)\right]A(x)=\left[\prod_{i=l}^{l+2t-1}\left(x-\alpha^{i}\right)\right]A(x)\quad\text{（式 6.4.3.1）}$$

（$d_{min}=2t+1$）ただし、$A(x)$は根α^{l}～α^{l+2t-1}の 2 乗、4 乗などを根として持つ多項式。

例えば、原始多項式をx^3+x+1とする。l=0、t=1 では l+2t-1=1 であるので、生成多項式は、

$$g(x)=\left[\prod_{i=0}^{1}\left(x-\alpha^{i}\right)\right]A(x)=(x-\alpha^{0})(x-\alpha^{1})A(x)$$

となる。0 乗, 1 乗の根が連続して入るため最小距離は 3 となりそうである。しかし、1 乗を根として持つと、２，４乗も根として持つ。よって実際には、

$$g(x)=(x-\alpha^{0})(x-\alpha^{1})A(x)=(x-\alpha^{0})(x-\alpha^{1})(x-\alpha^{2})(x-\alpha^{4})$$

であり、０乗、１乗、２乗が連続した根となっており、dmin=4 になる。これは、１誤り訂正可能、２誤り検出可能である。別の言い方をすると、l=1 の場合に対して、パリティが追加されている符号とも考えられる。従って、l=0 は導入の例としてはあまり適切ではなく、７．１では l=1 を選択している。

２）RS 符号で、l=1 の場合

RS 符号の場合、l=0 でも l=1 でも特に問題なく同様な議論ができる。

例えば、資料で扱った RS(7,3)符号の方法を以下に示す。

■例１　(7,3)符号　　$m=3,n=7,k=3,t=2,$ 原始多項式が$p(x)=x^3+x+1$の場合

で、l=1 の場合を検討する。

①情報ビット系列を 3 ビット$(m=3)$ずつの 3 個$(k=3)$のブロック（バイト）に分割する。例えば

情報ビット　001 010 100

情報バイト　1　α^1　α^2

バイト番号　1　2　3

②情報バイトを多項式で表現する。

$$I(y)=I_{k-1}y^{k-1}+\cdots+I_1y+I_0=1y^2+\alpha^1y^1+\alpha^2y^0$$

③生成多項式を求める。

$$G(y)=\prod_{i=l}^{l+2t-1}(y-\alpha^{i})=\prod_{i=1}^{4}(y-\alpha^{i})=(y-\alpha^{1})(y-\alpha^{2})(y-\alpha^{3})(y-\alpha^{4})$$
$$=y^4+\alpha^3y^3+y^2+\alpha^1y^1+\alpha^3$$

④情報多項式$I(y)*y^{n-k}$を生成多項式$G(y)$　で除算した余りを求める。

$$I(y)=I_{k-1}y^{k-1}+\cdots I_1y+I_0=1y^2+\alpha^1y^1+\alpha^2y^0$$
$$r(y)=I(y)*y^{n-k}\ mod\ G(y)=(1y^2+\alpha^1y^1+\alpha^2y^0)*y^4\ mod\ y^4+\alpha^3y^3+y^2+\alpha^1y^1+\alpha^3$$
$$=\alpha^1y^3+\alpha^5y^2+\alpha^2y+\alpha^0$$

⑤以上より

情報ビット	001	010	100				
情報バイト	1	α^1	α^2				
符号化後	1	α^1	α^2	α^1	α^5	α^2	α^0
RS 符号語	001	010	100	010	111	100	001
バイト番号	1	2	3	4	5	6	7

情報通信基礎Ⅰ　第７章　補足資料１

符号語のフーリエ変換と BCH 限界

情シス　渡辺

１．符号語のフーリエ変換

（１）フーリエ変換

符号語を　　$w=(w_{n-1},w_{n-2},,,w_2,w_1,w_0)$　とする。

これに対する符号語多項式は、以下である。

$$W(x)=w_{n-1}x^{n-1}+w_{n-2}x^{n-2}+\cdots+w_2x^2+w_1x+w_0=\sum_{i=0}^{n-1}w_ix^i \quad \text{・・・式 1.1}$$

符号語多項式を以下により変換する。

$$\tilde{w}_j=W(\alpha^j) \quad \text{・・・式 1.2}$$

これを符号語のフーリエ変換と呼ぶ。書き直すと、

$$\tilde{w}_j=W(\alpha^j)=w_{n-1}[\alpha^j]^{n-1}+w_{n-2}[\alpha^j]^{n-2}+\cdots+w_2[\alpha^j]^2+w_1[\alpha^j]^1+w_0[\alpha^j]^0$$

$$=\sum_{k=0}^{n-1}w_k[\alpha^j]^k \quad \text{・・・式 1.3}$$

である。（通常のフーリエ変換との関係は４で述べる）

（２）マトソン・ソロモン多項式

次に、$\tilde{w}_j$を要素とするベクトル$\tilde{w}$を考える。

$$\tilde{w}=(\tilde{w}_{n-1},\tilde{w}_{n-2},,,,\tilde{w}_2,\tilde{w}_1,\tilde{w}_0) \quad \text{・・・式 1.4}$$

この多項式表現

$$\tilde{W}(x)=\tilde{w}_{n-1}x^{n-1}+\tilde{w}_{n-2}x^{n-2}+\cdots+\tilde{w}_2x^2+\tilde{w}_1x+\tilde{w}_0=\sum_{i=0}^{n-1}\tilde{w}_ix^i$$

$$=\sum_{i=0}^{n-1}W(\alpha^i)x^i \quad \text{・・・式 1.5}$$

をマトソン・ソロモン多項式と呼ぶ。

（３）フーリエ逆変換

また、以下をフーリエ逆変換と呼ぶ。

$$w_j=n^{-1}\tilde{W}(\alpha^{-j}) \quad \text{・・・式 1.6}$$

逆変換は以下のように導出できる。

まず、式 1.5 に、$x=\alpha^{-j}$を代入する。

$$\tilde{W}(\alpha^{-j})=\sum_{k=0}^{n-1}\tilde{w}_k[\alpha^{-j}]^k=\sum_{k=0}^{n-1}W(\alpha^k)[\alpha^{-j}]^k$$

Σの中は、

$$W(\alpha^k)[\alpha^{-j}]^k = [\alpha^{-j}]^k \sum_{i=0}^{n-1} w_i[\alpha^k]^i$$
$$= [\alpha^{-j}]^k\{w_0[\alpha^k]^0 + w_1[\alpha^k]^1 + \cdots + w_{n-2}[\alpha^k]^{n-2} + w_{n-1}[\alpha^k]^{n-1}\}$$
$$= w_0[\alpha^k]^{-j+0} + w_1[\alpha^k]^{-j+1} + \cdots + w_{n-2}[\alpha^k]^{-j+n-2} + w_{n-1}[\alpha^k]^{-j+n-1}$$

となる。従って、

$\widetilde{W}(\alpha^{-j}) = \sum_{k=0}^{n-1} W(\alpha^k)[\alpha^{-j}]^k =$

$w_0[\alpha^0]^{-j+0} + w_1[\alpha^0]^{-j+1} + \cdots + w_j[\alpha^0]^{-j+j} + \cdots + w_{n-2}[\alpha^0]^{-j+n-2} + w_{n-1}[\alpha^0]^{-j+n-1} + +$

$w_0[\alpha^1]^{-j+0} + w_1[\alpha^1]^{-j+1} + \cdots + w_j[\alpha^1]^{-j+j} + \cdots + w_{n-2}[\alpha^1]^{-j+n-2} + w_{n-1}[\alpha^1]^{-j+n-1} +$

・・・

$w_0[\alpha^{n-2}]^{-j+0} + w_1[\alpha^{n-2}]^{-j+1} + \cdots + w_j[\alpha^{n-2}]^{-j+j} + \cdots + w_{n-2}[\alpha^{n-2}]^{-j+n-2} + w_{n-1}[\alpha^{n-2}]^{-j+n-1} +$

$w_0[\alpha^{n-1}]^{-j+0} + w_1[\alpha^{n-1}]^{-j+1} + \cdots + w_j[\alpha^{n-1}]^{-j+j} + \cdots + w_{n-2}[\alpha^{n-1}]^{-j+n-2} + w_{n-1}[\alpha^{n-1}]^{-j+n-1}$

$= w_0\left\{[\alpha^0]^{-j+0} + [\alpha^1]^{-j+0} + \cdots + [\alpha^{n-1}]^{-j+0}\right\} +$

$w_1\left\{[\alpha^0]^{-j+1} + [\alpha^1]^{-j+1} + \cdots + [\alpha^{n-1}]^{-j+1}\right\} +$

…

$w_j\left\{[\alpha^0]^0 + [\alpha^1]^0 + \cdots + (\alpha^{n-1})^0\right\} +$

…

$w_{n-1}\left\{[\alpha^0]^{-j+n-1} + [\alpha^1]^{-j+n-1} + \cdots + [\alpha^{n-1}]^{-j+n-1}\right\}$

$= w_0 \sum_{i=0}^{n-1} \alpha^{i(-j)} + w_1 \sum_{i=0}^{n-1} \alpha^{i(-j+1)} + \cdots + w_j \sum_{i=0}^{n-1} \alpha^{i\cdot 0} + \cdots + w_{n-1} \sum_{i=0}^{n-1} \alpha^{i(-j+n-1)}$

$= nw_j(\alpha)^0 = nw_j$（※　jのところだけが残る。）

-----※の補足説明

$$\sum_{i=0}^{n-1} \alpha^{ij} = \begin{cases} n, & j = 0 \\ 0, & otherwise \end{cases}$$

を以下のように証明する。

(1) $j = 0$の時は、自明。

(2) $j \neq 0$の時を考える。

α^jは、$x^n - 1$の根である。$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$であるから、$\alpha^j(\neq 1)$は、$(x^{n-1} + x^{n-2} + \cdots + x + 1)$の根となる。つまり、

$$[\alpha^j]^{n-1} + [\alpha^j]^{n-2} + \cdots + [\alpha^j] \quad + 1 = 0$$

よって、

$$[\alpha^j]^{n-1} + [\alpha^j]^{n-2} + \cdots + [\alpha^j] \quad + 1 = \sum_{i=0}^{n-1} [\alpha^j]^i = \sum_{i=0}^{n-1} \alpha^{ij} = 0$$

以上より、

$$\widetilde{W}(\alpha^{-j}) = \sum_{k=0}^{n-1} W(\alpha^k)[\alpha^{-j}]^k = nw_j$$
$$w_j = n^{-1}\widetilde{W}(\alpha^{-j})$$

上の導出からも分かるとおり、$GF(2)$上の場合、n^{-1}はnが奇数では１となる。
（n^{-1}の説明；nの逆元をxとすると、$n*x=1$となるxがn^{-1}である。例えば、$GF(3)$上で8^{-1}とは、８にかけたら１になる元。すなわち、2。8*2=16=1 mod 3）

（４）フーリエ変換の意味

$$\tilde{w}_j = W(\alpha^j) \qquad \cdots \text{式 1.7}$$

から、符号語$w=(w_{n-1},w_{n-2},,,w_2,w_1,w_0)$が、$\alpha^i$を根として持つとき、$\tilde{w}_i=0$となる。従って、符号語のフーリエ変換は、根の位置を示していると言える。（$\tilde{w}_0$はパリティ計算）

（５）例

今井秀樹著「符号理論」電子情報通信学会　p.125 例 5.10

問）原始多項式を　$p(x)=x^3+x+1$、生成多項式を$g(x)=p(x)$として生成された符号語$w=(w_6,w_5,w_4,w_3,w_2,w_1,w_0)=(0\,0\,1\,1\,1\,0\,1)$　のフーリエ変換を求め、マトソン・ソロモン多項式で示せ。

答）フーリエ変換の定義

$$\tilde{w}_j = W(\alpha^j) = w_{n-1}[\alpha^j]^{n-1} + w_{n-2}[\alpha^j]^{n-2} + \cdots + w_2[\alpha^j]^2 + w_1[\alpha^j]^1 + w_0[\alpha^j]^0$$
$$= \sum_{k=0}^{n-1} w_k[\alpha^j]^k \qquad \cdots \text{式 1.8}$$

より、

$\tilde{w}_0 = W(\alpha^0) = w_6[\alpha^0]^6 + w_5[\alpha^0]^5 + w_4[\alpha^0]^4 + w_3[\alpha^0]^3 + w_2[\alpha^0]^2 + w_1[\alpha^0]^1 + w_0[\alpha^0]^0 = 0+0+1+1+1+0+1=0$

$\tilde{w}_1 = W(\alpha^1) = w_6[\alpha^1]^6 + w_5[\alpha^1]^5 + w_4[\alpha^1]^4 + w_3[\alpha^1]^3 + w_2[\alpha^1]^2 + w_1[\alpha^1]^1 + w_0[\alpha^1]^0 = w_4[\alpha^1]^4 + w_3[\alpha^1]^3 + w_2[\alpha^1]^2 + w_0[\alpha^1]^0 = \alpha^4+\alpha^3+\alpha^2+1 = (110)+(011)+(100)+(001) = (000) = 0$

$\tilde{w}_2 = W(\alpha^2) = w_6[\alpha^2]^6 + w_5[\alpha^2]^5 + w_4[\alpha^2]^4 + w_3[\alpha^2]^3 + w_2[\alpha^2]^2 + w_1[\alpha^2]^1 + w_0[\alpha^2]^0 = w_4[\alpha^2]^4 + w_3[\alpha^2]^3 + w_2[\alpha^2]^2 + w_0[\alpha^2]^0 = \alpha^8+\alpha^6+\alpha^4+1 = \alpha+\alpha^6+\alpha^4+1 = (010)+(101)+(110)+(001) = (000) = 0$

$\tilde{w}_3 = W(\alpha^3) = w_6[\alpha^3]^6 + w_5[\alpha^3]^5 + w_4[\alpha^3]^4 + w_3[\alpha^3]^3 + w_2[\alpha^3]^2 + w_1[\alpha^3]^1 + w_0[\alpha^3]^0 = w_4[\alpha^3]^4 + w_3[\alpha^3]^3 + w_2[\alpha^3]^2 + w_0[\alpha^3]^0 = \alpha^{12}+\alpha^9+\alpha^6+1 = \alpha^5+\alpha^2+\alpha^6+1 = (111)+(100)+(101)+(001) = (111) = \alpha^5$

$\tilde{w}_4 = W(\alpha^4) = w_6[\alpha^4]^6 + w_5[\alpha^4]^5 + w_4[\alpha^4]^4 + w_3[\alpha^4]^3 + w_2[\alpha^4]^2 + w_1[\alpha^4]^1 + w_0[\alpha^4]^0 = w_4[\alpha^4]^4 + w_3[\alpha^4]^3 + w_2[\alpha^4]^2 + w_0[\alpha^4]^0 = \alpha^{16}+\alpha^{12}+\alpha^8+1 = \alpha^2+\alpha^5+\alpha^1+1 = (100)+(111)+(010)+(001) = (000) = 0$

$\tilde{w}_5 = W(\alpha^5) = w_6[\alpha^5]^6 + w_5[\alpha^5]^5 + w_4[\alpha^5]^4 + w_3[\alpha^5]^3 + w_2[\alpha^5]^2 + w_1[\alpha^5]^1 + w_0[\alpha^5]^0 = w_4[\alpha^5]^4 + w_3[\alpha^5]^3 + w_2[\alpha^5]^2 + w_0[\alpha^5]^0 = \alpha^{20}+\alpha^{15}+\alpha^{10}+1 = \alpha^6+\alpha^1+\alpha^3+1 =$

$(101)+(010)+(011)+(001)=(101)=\alpha^6$

$\tilde{w}_6=W(\alpha^6)=w_6[\alpha^6]^6+w_5[\alpha^6]^5+w_4[\alpha^6]^4+w_3[\alpha^6]^3+w_2[\alpha^6]^2+w_1[\alpha^6]^1+w_0[\alpha^6]^0=$
$w_4[\alpha^6]^4+w_3[\alpha^6]^3+w_2[\alpha^6]^2+w_0[\alpha^6]^0=\alpha^{24}+\alpha^{18}+\alpha^{12}+1=\alpha^3+\alpha^4+\alpha^5+1=$
$(011)+(110)+(111)+(001)=(011)=\alpha^3$

以上より、

$$\tilde{w}=(\tilde{w}_6,\tilde{w}_5,\tilde{w}_4,\tilde{w}_3,\tilde{w}_2,\tilde{w}_1,\tilde{w}_0)=(\alpha^3\ \alpha^6\ 0\ \alpha^5\ 0\ 0\ 0)$$
$$\tilde{W}(x)=\alpha^3x^6+\alpha^6x^5+\alpha^5x^3$$

確かに、$g(x)=x^3+x+1=(x+\alpha^1)(x+\alpha^2)(x+\alpha^4)$であり、$\tilde{w}_4=\tilde{w}_2=\tilde{w}_1=0$となっている。ただし、$\tilde{w}_0=0$であることにも注意する。

２．BCH 限界の証明

（１）BCH 限界の証明

巡回符号の生成多項式$g(x)$が、べき乗が連続した$2t$個の根、$\alpha^l,\alpha^{l+1},\cdots,\alpha^{l+2t-1}$を持つとき、最小距離は$2t+1$以上になることを証明する。

（２）符号語多項式を

$$W(x)=w_{n-1}x^{n-1}+w_{n-2}x^{n-2}+\cdots+w_2x^2+w_1x+w_0=\sum_{i=0}^{n-1}w_ix^i$$

とする。$W(x)=A(x)g(x)$　であり、$g(x)$が$\alpha^l,\alpha^{l+1},\cdots,\alpha^{l+2t-1}$を根に持つ、つまり$g(\alpha^l)=g(\alpha^{l+1})=\cdots=g(\alpha^{l+2t-1})=0$から、

$$\left.\begin{array}{c}W(\alpha^l)=0\\W(\alpha^{l+1})=0\\\vdots\\W(\alpha^{l+2t-1})=0\end{array}\right\}$$

2t 個　・・・式 2.1

$W(x)$をフーリエ変換して、マトソン・ソロモン多項式$\tilde{W}(x)$を以下のように求める。

$$\tilde{W}(x)=\tilde{w}_{n-1}x^{n-1}+\tilde{w}_{n-2}x^{n-2}+\cdots+\tilde{w}_2x^2+\tilde{w}_1x+\tilde{w}_0=\sum_{i=0}^{n-1}\tilde{w}_ix^i=\sum_{i=0}^{n-1}W(\alpha^i)x^i$$
$$=W(\alpha^{n-1})x^{n-1}+W(\alpha^{n-2})x^{n-2}+\cdots+W(\alpha^2)x^2+W(\alpha^1)x^1+W(\alpha^0)$$

式 2.1 を考えると、$\tilde{W}(x)$のn個の要素のうち、$2t$個の係数が連続して０となっている。

（３）次に、$\tilde{W}(x)$の逆フーリエを考える。

$$w_j=n^{-1}\tilde{W}(\alpha^{-j})\ \cdots\text{式 2.2}$$

より、$w_j=0$となるためには、$\tilde{W}(\alpha^{-j})=0$でなければならない。

従って、$\tilde{W}(x)$がα^{-j}を根に持たねばならない。

n個の $\alpha^{-j}=\alpha^n\alpha^{-j}=\alpha^{n-j}$　$(j=0,1,,,n)$ は、x^n-1の根であり、x^n-1はそれ以外の根を持たない。

従って、w_iのうち０となるものの数をzとすると、zは、$\tilde{W}(x)$とx^n-1の共通の根の数とな

る。つまり、zは、

$$D(x) = LCM(\widetilde{W}(x), x^n - 1)$$

の次数に等しい。

（4）$\widetilde{W}'^{(x)} = \left[x^{n-l-2t}\widetilde{W}(x)\right] mod\ x^n - 1$

とする。（連続する根が最上位ビットになるように桁上げする。）

xと$x^n - 1$は、互いに素であるので、

$$D(x) = LCM(\widetilde{W}(x), x^n - 1) = LCM(\widetilde{W}'(x), x^n - 1)$$

である。

$\widetilde{W}'(x)$は、x^{n-l-2t}がかかっているから、 $x^{n-1}, x^{n-2}, , , x^{n-2t}$ の係数は0となっている。

従って、$\widetilde{W}'(x)$の次数は、$n - 2t - 1$以下である。

よって、$D(x) = LCM(\widetilde{W}'(x), x^n - 1)$ の次元も$n - 2t - 1$以下である。

（5）以上より、$\widetilde{W}(x)$と$x^n - 1$の共通の根の数zも、$n - 2t - 1$以下である。

よって、w_iのうち、0となるものの数は、$n - 2t - 1$以下である。

逆に、1となるものの数、すなわち重みωは、$n - (n - 2t - 1) = 2t + 1$以上である。

従って、$\omega \geq 2t + 1$。最小重みω_{min}は、$\omega_{min} \geq 2t + 1$となる。また、$\omega_{min} = d_{min}$である。

以上より、

$$d_{min} \geq 2t + 1$$

となる。

BCH 限界の証明には、この他に、検査行列から一次独立な列を選び、そこからファンデヤモンデ行列式を利用して最小距離を求める方法がある。

３．具体的な符号を用いた BCH 限界の証明

（1）原始多項式を　$p(x) = x^3 + x + 1$、生成多項式を$g(x) = p(x) = (x + \alpha^1)(x + \alpha^2)(x + \alpha^4)$として生成された符号語の、最小距離は$2t + 1$以上になることを証明する。

（2）符号語多項式を

$$W(x) = w_6x^6 + w_5x^5 + \cdots + w_2x^2 + w_1x + w_0 = \sum_{i=0}^{6} w_i x^i$$

とする。$W(x) = A(x)g(x)$　であり、$g(x)$がα^1, α^2を根に持つ、つまり$g(\alpha^1) = g(\alpha^2) = 0$から、

$$\left.\begin{matrix} W(\alpha^1) = 0 \\ W(\alpha^2) = 0 \end{matrix}\right\} \boxed{\text{2 個　・・・式 3.1}}$$

（ただし、$l = 1$としている。）

$W(x)$をフーリエ変換したマトソン・ソロモン多項式$\widetilde{W}(x)$を以下のように求める。

$$\begin{aligned}\widetilde{W}(x) &= \widetilde{w}_6x^6 + \widetilde{w}_5x^5 + \widetilde{w}_4x^4 + \widetilde{w}_3x^3 + \widetilde{w}_2x^2 + \widetilde{w}_1x + \widetilde{w}_0 \\ &= W(\alpha^6)x^6 + W(\alpha^5)x^5 + W(\alpha^4)x^4 + W(\alpha^3)x^3 + W(\alpha^2)x^2 + W(\alpha^1)x^1 \\ &\quad + W(\alpha^0)\end{aligned}$$

式 3.1 を考えると、$\widetilde{W}(x)$の 7 個の係数のうち、$2t = 2$個が連続して0となっている。

（３）次に、$\widetilde{W}(x)$の逆フーリエを考える。

$$w_j = 7^{-1}\widetilde{W}(\alpha^{-j}) = \widetilde{W}(\alpha^{-j}) \quad \cdots \text{式 3.3}$$

より、$w_j = 0$となるためには、$\widetilde{W}(\alpha^{-j}) = 0$でなければならない。

従って、$\widetilde{W}(x)$がα^{-j}を根に持たねばならない。

７個の $\alpha^{-j}=\alpha^{n}\alpha^{-j} = \alpha^{n-j} \quad (j = 0,1,,,6)$ は、$x^7 - 1$の根であり、$x^7 - 1$はそれ以外の根を持たない。

従って、w_iのうち０となるものの数をzとすると、zは、$\widetilde{W}(x)$と$x^7 - 1$の共通の根の数となる。つまり、zは、

$$D(x) = LCM(\widetilde{W}(x), x^7 - 1)$$

の次数に等しい。

（４）$\widetilde{W}'^{(x)} = \left[x^{n-l-2t}\widetilde{W}(x)\right] mod\ x^n - 1 = \left[x^{7-1-2}\widetilde{W}(x)\right] mod\ x^7 - 1 = \left[x^4\widetilde{W}(x)\right] mod\ x^7 - 1$

とする。（連続する根が最上位ビットになるように桁上げする。）

xと$x^7 - 1$は、互いに素であるので、

$$D(x) = LCM(\widetilde{W}(x), x^7 - 1) = LCM(\widetilde{W}'(x), x^7 - 1)$$

である。

$\widetilde{W}'(x)$は、$x^{n-l-2t} = x^4$がかかっているから、 x^6, x^5 の係数は０となっている。

従って、$\widetilde{W}'(x)$の次数は、$n - 2t - 1 = 4$以下である。

よって、$D(x) = LCM(\widetilde{W}'(x), x^7 - 1)$ の次元も$n - 2t - 1 = 4$以下である。

（５）以上より、$\widetilde{W}(x)$と$x^7 - 1$の共通の根の数zも、$n - 2t - 1 = 4$以下である。

よって、w_iのうち、０となるものの数は、$n - 2t - 1 = 4$以下である。

逆に、１となるものの数、すなわち重みωは、$n - (n - 2t - 1) = 2t + 1 = 3$以上である。

従って、$\omega \geq 2t + 1 = 3$。最小重みω_{min}は、$\omega_{min} \geq 2t + 1 = 3$となる。また、$\omega_{min} = d_{min}$である。

以上より、

$$d_{min} \geq 2t + 1 = 3$$

となる。

４　フーリエ変換との関連

符号語

$$W(x) = w_{n-1}x^{n-1} + w_{n-2}x^{n-2} + \cdots + w_2x^2 + w_1x + w_0 = \sum_{i=0}^{n-1} w_i x^i \quad \cdots \text{式 4.1}$$

に対するフーリエ変換は次式である。

$$\begin{aligned}\widetilde{w}_j = W(\alpha^j) &= w_{n-1}[\alpha^j]^{n-1} + w_{n-2}[\alpha^j]^{n-2} + \cdots + w_2[\alpha^j]^2 + w_1[\alpha^j]^1 + w_0[\alpha^j]^0 \\ &= \sum_{k=0}^{n-1} w_k[\alpha^j]^k \quad \cdots \text{式 4.2}\end{aligned}$$

今、αが$x^n + 1$の根であるとすると、αは、１のn乗根である。すなわち、

$$\alpha = e^{-\frac{2\pi}{n}i} \quad \cdots \text{式 4.3}$$

と書ける。従って、

$$\tilde{w}_j = \sum_{k=0}^{n-1} w_k[\alpha^j]^k = \sum_{k=0}^{n-1} w_k[e^{-\frac{2\pi}{n}i}]^k = \sum_{k=0}^{n-1} w_k e^{-\frac{2\pi k}{n}i} \quad \cdots \text{式 4.4}$$

となり、これは通常のフーリエ変換と一致する。

情報通信基礎Ⅰ　第７章　補足資料２　追加問題　BCH とＲＳ（完全版）

渡辺

問１）原始多項式を$p(x) = x^3 + x + 1$とし、その根αを$GF(2^3)$の原始元とする。以下の小問に答えよ。

１－１）原始多項式$p(x)$で構成される拡大体$GF(2^3)$の全要素を 0 およびαのべき乗の形で示せ。

１－２）１－１）の$GF(2^3)$において、情報バイト記号$(I_2, I_1, I_0) = (0, 1, \alpha)$の時、符号長$n = 2^3 - 1 = 7$、最小距離$d_{min} = 5$（２誤り訂正可能）のリードソロモン符号語$w = (w_1, w_2, \cdots, w_n)$を求めよ。

１－３）１－２）で求めたwの符号多項式$W(y)$は、$\alpha, \alpha^2, \cdots, \alpha^{n-k} = \alpha^4$を根として持つことを示せ。

１－４）１－３）の符号語多項式$W(y)$は、生成多項式$G(y)$で整除されることを示せ。

問２）αを$x^4 + x + 1$の原始元とする。３誤り訂正可能な$GF(2^4)$上の RS 符号生成多項式を求めよ。

問３）$GF(2)$上の２つの多項式$p_1(x)$、$p_2(x)$を

$p_1(x) = x^3 + x + 1$　　$p_2(x) = x^3 + x^2 + 1$　　とし、以下の小問に答えよ。

３－１）$p_1(x)$、$p_2(x)$の周期を求めよ。

３－２）原始多項式を$p_1(x)$、$p_1(x)$の根をαとする。$p_1(x)$によって構成される拡大体$GF(2^3)$の全要素を 0 およびαのべき乗の形で示せ。

３－３）原始多項式を$p_1(x)$、生成多項式$g_1(x)$を$g_1(x) = p_1(x)$とする。この生成多項式$g_1(x)$によって生成される符号C_1は、何と呼ばれるか。

３－４）C_1の全符号語を求め、巡回していることを示せ。

３－５）C_1の検査行列H_1を求めよ。

３－６）C_1の誤り訂正能力を論じよ。

３－７）原始多項式を$p_1(x)$とし、生成多項式$g_2(x)$を$g_2(x) = (x + 1)p_1(x)$とする。この生成多項式$g_2(x)$によって生成される符号C_2の全符号語を求めよ。

３－８）C_2の誤り訂正検出能力をC_1と比較して論じよ。

３－９）原始多項式を$p_1(x)$とし、生成多項式$g_3(x)$を$g_3(x) = p_2(x)$とする。この生成多項式$g_3(x)$によって生成される符号C_3の全符号語を求めよ。

３－１０）C_3の誤り訂正能力を論じよ。

３－１１）原始多項式を$p_1(x)$とした拡大体$GF(2^3)$の情報記号を RS 符号化する。２バイト誤りを訂正可能となるように生成多項式$g_4(x)$を求めよ。

３－１２）$g_4(x)$で生成される RS 符号C_4の全符号語はいくつあるかを求めよ。

３－１３）情報記号$I_A = (1, \alpha, \alpha^2)$、$I_B = (1, 0, \alpha^6)$、$I_C = (\alpha^4, \alpha^5, \alpha^3)$に対する RS 符号$C_4$の符号語をそれぞれ求めよ。

３－１４）情報源から発生した文字列が、

00101010000100010111011011・・・

であった。C_1、C_2、C_3、C_4でそれぞれ符号化せよ。

解答

問１）原始多項式を$p(x)=x^3+x+1$とし、その根αを$GF(2^3)$の原始元とする。以下の小問に答えよ。

１－１）原始多項式$p(x)$で構成される拡大体$GF(2^3)$の全要素を 0 およびαのべき乗の形で示せ。

$p(x)=x^3+x+1$を原始多項式として構築される$GF(2^3)$を求める。

多項式表現	ベクトル表現	αべき乗表現	
0 000	0		
1 001	1		$=\alpha^0$
x 010	α		$=\alpha^1$
$x+1$	011	$\alpha+1$	$=\alpha^3$
x^2	100	α^2	$=\alpha^2$
x^2+1	101	α^2+1	$=\alpha^6$
x^2+x	110	$\alpha^2+\alpha$	$=\alpha^4$
x^2+x+1	111	$\alpha^2+\alpha+1$	$=\alpha^5$

拡大体は、$GF(2^3)=\{0,1,\alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4,\ \alpha^5,\ \alpha^6\}$

１－２）１－１）の$GF(2^3)$において、情報バイト記号$(I_2,I_1,I_0)=(0,1,\alpha)$の時、符号長$n=2^3-1=7$、最小距離$d_{min}=5$（２誤り訂正可能）のリードソロモン符号語$w=(w_1,w_2,\cdots,w_n)$を求めよ。

情報バイト数kは$k=n-d_{min}+1=3$である。また、$I(y)=I_2y^2+I_1y+I_0=y+\alpha$である。

$w=(\ I(\alpha_1),I(\alpha_2),I(\alpha_3),I(\alpha_4),I(\alpha_5),I(\alpha_6),I(\alpha_7)\ )=(w_1,w_2,w_3,w_4,w_5,w_6,w_7)$とする。$\alpha_3+\alpha+1=0$であるから、

$w_1=I(\alpha_1)=I(\alpha^6)=\alpha^6+\alpha=\alpha^2+1+\alpha=\alpha^3+\alpha^2=\alpha^5$　　同様に、

$w_2=I(\alpha_2)=I(\alpha^5)=\alpha^6$　$w_3=I(\alpha_3)=I(\alpha^4)=\alpha^2$　$w_4=I(\alpha_4)=I(\alpha^3)=1$

$w_5=I(\alpha_5)=I(\alpha^2)=\alpha^4$　$w_6=I(\alpha_6)=I(\alpha^1)=0$　$w_7=I(\alpha_7)=I(\alpha^0)=\alpha^3$

以上より、$w=(\alpha^5,\alpha^6,\alpha^2,1,\alpha^4,0,\alpha^3)$

１－３）１－２）で求めたwの符号多項式$W(y)$は、$\alpha,\alpha^2,\cdots,\alpha^{n-k}=\alpha^4$を根として持つことを示せ。

$W(y)=\alpha^5y^6+\alpha^6y^5+\alpha^2y^4+y^3+\alpha^4y^2+\alpha^3$　であるので、

$W(\alpha)=\alpha^{11}+\alpha^{11}+\alpha^6+\alpha^3+\alpha^6+\alpha^3=0$

$W(\alpha^2)=\alpha^{17}+\alpha^{16}+\alpha^{10}+\alpha^6+\alpha^8+\alpha^3=\alpha^3+\alpha^2+\alpha^3+\alpha^6+\alpha^1+\alpha^3=0$

$W(\alpha^3)=\alpha^{23}+\alpha^{21}+\alpha^{14}+\alpha^9+\alpha^{10}+\alpha^3=0$

$W(\alpha^4)=\alpha^{29}+\alpha^{26}+\alpha^{18}+\alpha^{12}+\alpha^{12}+\alpha^3=0$

１－４）１－３）の符号語多項式$W(y)$は、生成多項式$G(y)$で整除されることを示せ。

１－３より、生成多項式$G(y)$は、$\alpha,\alpha^2,\alpha^3,\alpha^{n-k}=\alpha^4$を根として持つから、

$$G(y)=(y-\alpha)(y-\alpha^2)(y-\alpha^3)(y-\alpha^4)=y^4+\alpha^3y^3+1y^2+\alpha y+\alpha^3$$

unb [1 2][1 4][1 3][1 6]=[1 6 3][1 4][1 3][1 6]=[1 5 2 5][1 6]=[1 3 1 2 3]

$$W(y) = \alpha^5 y^6 + \alpha^6 y^5 + \alpha^2 y^4 + y^3 + \alpha^4 y^2 + \alpha^3 = (y^4 + \alpha^3 y^3 + 1y^2 + \alpha y + \alpha^3)(\alpha^5 y^2 + \alpha^5 y + 1)$$
$$= G(y)(\alpha^5 y^2 + \alpha^5 y + 1)$$

unb [7 5 4 1 6 0 3]/[1 3 1 2 3]=[7 7 1]

従って、$W(y)$は$G(y)$で整除される。

問２）αを$x^4 + x + 1$の原始元とする。３誤り訂正可能な$GF(2^4)$上の RS 符号生成多項式を求めよ。

３誤りを訂正するためには、生成多項式はべき数が連続する６つの根を持たねばならない。従って、生成多項式（の一つ）$G(x)$は、$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$を根として持つので以下となる。

$$G(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^5)(x-\alpha^6)$$
$$= x^6 + \alpha^{10}x^5 + \alpha^{14}x^4 + \alpha^4 x^3 + \alpha^6 x^2 + \alpha^9 x + \alpha^6$$

これによって生成される符号の符号長は$n = 2^4 - 1 = 15$、情報記号数は$k = 9$である。

（この問題は、岩垂 p.74　より）

unb [1 2][1 4][1 8][1 3][1 6][1 12]=[1 6 8][1 8][1 3][1 6][1 12]=[1 14 13 12][1 3][1 6][1 12]=[1 13 12 8 7][1 6][1 12]=[1 11 4 6 2 1][1 12]=[1 7 9 3 12 10 12]

問３）

３－１）$p_1(x)$、$p_2(x)$の周期を求めよ。

$p_1(x)$、$p_2(x)$ともに、$x^7 + 1$を整除し、それ以下の次元を整除しないので、周期は７。

３－２）原始多項式を$p_1(x)$、$p_1(x)$の根をαとする。$p_1(x)$によって構成される拡大体$GF(2^3)$の全要素を 0 およびαのべき乗の形で示せ。

$p_1(x) = x^3 + x + 1$を原始多項式として構築される$GF(2^3)$を求める。

多項式表現	ベクトル表現	αべき乗表現	
0 000	0		
1 001	1		$=\alpha^0$
x　010	α		$=\alpha^1$
$x+1$	011	$\alpha+1$	$=\alpha^3$
x^2	100	α^2	$=\alpha^2$
x^2　$+1$	101	α^2+1	$=\alpha^6$
x^2+x	110	$\alpha^2+\alpha$	$=\alpha^4$
x^2+x+1	111	$\alpha^2+\alpha+1$	$=\alpha^5$

拡大体は、$GF(2^3) = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$

３－３）原始多項式を$p_1(x)$、生成多項式$g_1(x)$を$g_1(x) = p_1(x)$とする。この生成多項式$g_1(x)$によって生成される符号C_1は、何と呼ばれるか。

符号長７、検査ビット数３、情報ビット数４

よって、巡回ハミング(7, 4)符号、または BCH(7,4)符号

３－４）C_1の全符号語を求め、巡回していることを示せ。

情報ビットにx^3をかけた多項式を$g_1(x)$で割って余り$r(x)$を計算して求める。

	情報ビット	余り$r(x)$	符号語$u(x)$	巡回のパターン
0	0 0 0 0	0 0 0	0 0 0 0 0 0 0	1
1	0 0 0 1	0 1 1	0 0 0 1 0 1 1	2
2	0 0 1 0	1 1 0	0 0 1 0 1 1 0	2
3	0 0 1 1	1 0 1	0 0 1 1 1 0 1	3
4	0 1 0 0	1 1 1	0 1 0 0 1 1 1	3
5	0 1 0 1	1 0 0	0 1 0 1 1 0 0	2
6	0 1 1 0	0 0 1	0 1 1 0 0 0 1	2
7	0 1 1 1	0 1 0	0 1 1 1 0 1 0	3
8	1 0 0 0	1 0 1	1 0 0 0 1 0 1	2
9	1 0 0 1	1 1 0	1 0 0 1 1 1 0	3
10	1 0 1 0	0 1 1	1 0 1 0 0 1 1	3
11	1 0 1 1	0 0 0	1 0 1 1 0 0 0	2
12	1 1 0 0	0 1 0	1 1 0 0 0 1 0	2
13	1 1 0 1	0 0 1	1 1 0 1 0 0 1	3
14	1 1 1 0	1 0 0	1 1 1 0 1 0 0	3
15	1 1 1 1	1 1 1	1 1 1 1 1 1 1	4

３－５）C_1の検査行列H_1を求めよ。

$1 * g_1(x) = (0001011)$　　$x * g_1(x) =(0010110)$

$x^2 * g_1(x) = (0101100)$　　$x^3 * g_1(x) = (1011000)$

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

行列の基本変形により、

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

これより、

$$H_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

３－６）C_1の誤り訂正能力を論じよ。

H_1　のどの２つの列ベクトルを加算しても０とはならない。一方、加算すると０となる３つの列ベ

クトルが存在する。従って、独立な列ベクトルの数は２。これより、最小距離は３であり、単一誤り訂正が可能である。

３－７）原始多項式を$p_1(x)$とし、生成多項式$g_2(x)$を$g_2(x)=(x+1)p_1(x)$とする。この生成多項式$g_2(x)$によって生成される符号C_2の全符号語を求めよ。

$g_2(x)=(x+1)p_1(x)=(x+1)(x^3+x+1)=x^4+x^3+x^2+1$

$g_2(x)$は、x^7+1を整除する。符号長７。検査ビット数４の(7,3)符号を生成する。

情報ビットにx^4をかけた多項式を$g_2(x)$で割って余り$r(x)$を計算して求める。

	情報ビット	余り$r(x)$	符号語$u(x)$	巡回のパターン
0	0 0 0	0 0 0 0	0 0 0 0 0 0 0	1
1	0 0 1	1 1 0 1	0 0 1 1 1 0 1	2
2	0 1 0	0 1 1 1	0 1 0 0 1 1 1	2
3	0 1 1	1 0 1 0	0 1 1 1 0 1 0	2
4	1 0 0	1 1 1 0	1 0 0 1 1 1 0	2
5	1 0 1	0 0 1 1	1 0 1 0 0 1 1	2
6	1 1 0	1 0 1 0	1 1 0 1 0 1 0	2
7	1 1 1	0 1 0 0	1 1 1 0 1 0 0	2

３－８）C_2の誤り訂正検出能力をC_1と比較して論じよ。

$g_1(x)=x^3+x+1=(x+\alpha)(x+\alpha^2)(x+\alpha^4)$

$g_2(x)=x^4+x^3+x^2+1=(x+\alpha^0)(x+\alpha^1)(x+\alpha^2)(x+\alpha^4)$

$g_1(x)$は、べき乗が連続する根α^1、α^2を持つ。一方$g_2(x)$は、べき乗が連続する根α^0、α^1、α^2　を持つ。従って、C_1は、最小距離３であり、一誤り訂正が可能。C_2は、最小距離４であり、一誤り訂正、２誤り検出が可能。

別解　$g_2(x)$は、BCH の定義の$l=0$の場合に相当する。$l+d_{min}-2=2$　$d_{min}=4$　BCH(7, 3, 4)符号となる。（資料６．４．３の BCH 符号定義：$\alpha^l,\alpha^{l+1},\cdots,\alpha^{l+d_{min}-2}$の根を持つ符号）

３－９）原始多項式を$p_1(x)$とし、生成多項式$g_3(x)$を$g_3(x)=p_2(x)$とする。この生成多項式$g_3(x)$によって生成される符号C_3の全符号語を求めよ。

$g_3(x)=x^3+x^2+1=(x+\alpha^3)(x+\alpha^5)(x+\alpha^6)$

$g_3(x)$で生成される符号は、符号長７、検査ビット数３、情報ビット数４

情報ビットにx^3をかけた多項式を$g_1(x)$で割って余り$r(x)$を計算して求める。

	情報ビット	余り$r(x)$	符号語$u(x)$	巡回のパターン
0	0 0 0 0	0 0 0	0 0 0 0 0 0 0	1
1	0 0 0 1	1 0 1	0 0 0 1 1 0 1	2
2	0 0 1 0	1 1 1	0 0 1 0 1 1 1	3
3	0 0 1 1	0 1 0	0 0 1 1 0 1 0	2

4	0 1 0 0	0 1 1	0 1 0 0 0 1 1	2
5	0 1 0 1	1 1 0	0 1 0 1 1 1 0	3
6	0 1 1 0	1 0 0	0 1 1 0 1 0 0	2
7	0 1 1 1	0 0 1	0 1 1 1 0 0 1	3
8	1 0 0 0	1 1 0	1 0 0 0 1 1 0	2
9	1 0 0 1	0 1 1	1 0 0 1 0 1 1	3
10	1 0 1 0	0 0 1	1 0 1 0 0 0 1	2
11	1 0 1 1	1 0 0	1 0 1 1 1 0 0	3
12	1 1 0 0	1 0 1	1 1 0 0 1 0 1	3
13	1 1 0 1	0 0 0	1 1 0 1 0 0 0	2
14	1 1 1 0	0 1 0	1 1 1 0 0 1 0	3
15	1 1 1 1	1 1 1	1 1 1 1 1 1 1	4

３－１０）C_3の誤り訂正能力を論じよ。

$g_3(x) = x^3 + x^2 + 1 = (x + \alpha^3)(x + \alpha^5)(x + \alpha^6)$

$g_3(x)$は、べき乗が連続する根α^5、α^6を持つ。従って、C_3の最小距離３であり、一誤り訂正が可能。

３－１１）原始多項式を$p_1(x)$とした拡大体$GF(2^3)$の情報記号を RS 符号化する。２バイト誤りを訂正可能となるように生成多項式$g_4(x)$を求めよ。

$m = 3$より、$n = 2^m - 1 = 7$、$k = n - 2t = 7 - 4 = 3$。これより、RS(7, 3)符号を構成する。

RS 符号の生成多項式の定義より、$G(y) = \prod_{i=l}^{l+2t-1}(y - \alpha^i)$

ここで、$t = 2$ 、$l = 0$として、

$g_4(x) = \prod_{i=0}^{3}(x - \alpha^i) = (x - \alpha^0)(x - \alpha^1)(x - \alpha^2)(x - \alpha^3) = x^4 + \alpha^2 x^3 + \alpha^5 x^2 + \alpha^5 x + \alpha^6$

３－１２）$g_4(x)$で生成される RS 符号C_4の全符号語はいくつあるかを求めよ。

$g_4(x)$は、$x^7 + 1$を整除する。符号長７。検査記号数４の RS(7,3)符号を生成する。

RS 符号では、情報記号にも３－２）で求めた拡大体$GF(2^3) = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$の要素を用いる。すなわち、(0 0 0)～(α^6 α^6 α^6) の $8^3 = 512$ 個存在する。

３－１３）情報記号$I_A = (1, \alpha, \alpha^2)$、$I_B = (1, 0, \alpha^6)$、$I_C = (\alpha^4, \alpha^5, \alpha^3)$に対する RS 符号$C_4$の符号語をそれぞれ求めよ。

001 010 100　　001 000 101　　110 111 011

$I_A(x) = 1x^2 + \alpha x + \alpha^2 = x^2 + \alpha x + \alpha^2$

$I_B(x) = 1x^2 + 0x + \alpha^6 = x^2 + \alpha^6$

$I_C(x) = \alpha^4 x^2 + \alpha^5 x + \alpha^3$

これらにx^4をかけそれぞれ$g_4(x)$で割って余りを計算して求める。

$I_A(x) * x^4 \ mod \ g_4(x) = \alpha^4 x^4 + \alpha^6 x^4 + \alpha^5 x + \alpha^3$ $\quad I_A => (1, \alpha, \alpha^2, \alpha^4, \alpha^6, \alpha^5, \alpha^3)$

$I_B(x) * x^4 \ mod \ g_4(x) = 0x^4 + \alpha^6 x^4 + \alpha^3 x + \alpha^1$ $\quad I_B => (1, 0, \alpha^6, 0, \alpha^6, \alpha^3, \alpha^1)$

$I_C(x) * x^4 \ mod \ g_4(x) = \alpha^5 x^4 + \alpha^5 x^4 + 0x + \alpha$ $\quad I_C => (\alpha^4, \alpha^5, \alpha^3, \alpha^5, \alpha^5, 0, \alpha)$

別解

$I_A(x) = 1x^2 + \alpha x + \alpha^2 = x^2 + \alpha x + \alpha^2$

$I_A(\alpha^0) = 1 + \alpha + \alpha^2 = \alpha^5$

$I_A(\alpha^1) = \alpha^2 + \alpha^2 + \alpha^2 = \alpha^2$

$I_A(\alpha^2) = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^2 + \alpha + \alpha + 1 + \alpha^2 = 1$

$I_A(\alpha^3) = \alpha^6 + \alpha^4 + \alpha^2 = \alpha^2 + 1 + \alpha^2 + \alpha + \alpha^2 = \alpha^2 + \alpha + 1 = \alpha^5$

$I_A(\alpha^4) = \alpha^8 + \alpha^5 + \alpha^2 = \alpha + \alpha^2 + \alpha + 1 + \alpha^2 = 1$

$I_A(\alpha^5) = \alpha^{10} + \alpha^6 + \alpha^2 = \alpha + 1 + \alpha^2 + 1 + \alpha^2 = \alpha$

$I_A(\alpha^6) = \alpha^{12} + \alpha^7 + \alpha^2 = \alpha^2 + \alpha + 1 + 1 + \alpha^2 = \alpha$

より、I_Aに対する RS 符号語は、$(\alpha, \alpha, 1, \alpha^5, 1, \alpha^2, \alpha^5)$

$I_B(x) = 1x^2 + 0x + \alpha^6 = x^2 + \alpha^6$

$I_B(\alpha^0) = 1 + \alpha^6 = 1 + \alpha^2 + 1 = \alpha^2$

$I_B(\alpha^1) = \alpha^2 + \alpha^6 = \alpha^2 + \alpha^2 + 1 = 1$

$I_B(\alpha^2) = \alpha^4 + \alpha^6 = \alpha^2 + \alpha + \alpha^2 + 1 = \alpha^3$

$I_B(\alpha^3) = \alpha^6 + \alpha^6 = 0$

$I_B(\alpha^4) = \alpha^8 + \alpha^6 = \alpha + \alpha^2 + 1 = \alpha^5$

$I_B(\alpha^5) = \alpha^{10} + \alpha^6 = \alpha + 1 + \alpha^2 + 1 = \alpha^2 + \alpha = \alpha^4$

$I_B(\alpha^6) = \alpha^{12} + \alpha^6 = \alpha^2 + \alpha + 1 + \alpha^2 + 1 = \alpha$

より、I_Bに対する RS 符号語は、$(\alpha, \alpha^4, \alpha^5, 0, \alpha^3, 1, \alpha^2)$

$I_C(x) = \alpha^4 x^2 + \alpha^5 x + \alpha^3$

$I_C(\alpha^0) = \alpha^4 + \alpha^5 + \alpha^3 = \alpha^2 + \alpha + \alpha^2 + \alpha + 1 + \alpha + 1 = \alpha$

$I_C(\alpha^1) = \alpha^6 + \alpha^6 + \alpha^3 = \alpha^3$

$I_C(\alpha^2) = \alpha^8 + \alpha^7 + \alpha^3 = \alpha + 1 + \alpha + 1 = 0$

$I_C(\alpha^3) = \alpha^{10} + \alpha^8 + \alpha^3 = \alpha + 1 + \alpha + \alpha + 1 = \alpha$

$I_C(\alpha^4) = \alpha^{12} + \alpha^9 + \alpha^3 = \alpha^2 + \alpha + 1 + \alpha^2 + \alpha + 1 = 0$

$I_C(\alpha^5) = \alpha^{14} + \alpha^{10} + \alpha^3 = 1 + \alpha + 1 + \alpha + 1 = 1$

$I_C(\alpha^6) = \alpha^{16} + \alpha^{11} + \alpha^3 = \alpha^2 + \alpha^2 + \alpha + \alpha + 1 = 1$

より、I_Cに対する RS 符号語は、$(1, 1, 0, \alpha, 0, \alpha^3, \alpha)$

３－１４）情報源から発生した文字列が、

00101010000100010111011011・・・
であった。C_1、C_2、C_3、C_4でそれぞれ符号化せよ。

C_1:
３－４）より
0010　1010　0001　0001　0111　0111　011・・・
0010110　1010011　0001011　0001011　0111010　00111010

C_2:
３－７）より
001　010　100　001　000　101　110　111　011
0011101　0100111　1001110　0011101　0000000　1010011　1101001　1110100　0111010

C_3:
３－９）より
0010　1010　0001　0001　0111　0111　011・・・
0010111　1010011　0001101　0001101　0111001　0111001

C_4:
３－１３）より
001 010 100　001 000 101　110 111 011
001 010 100 110 101 111 011　001 000 101 000 101 011 010　110 111 011 111 111 000 010
（上段は情報記号列、下段は RS 符号語列）

別解
３－１３）別解より
I_1に対する RS 符号語は、$(\alpha, \alpha, 1, \alpha^5, 1, \alpha^2, \alpha^5)$　010 010 001 111 001 100 111
I_2に対する RS 符号語は、$(\alpha, \alpha^4, \alpha^5, 0, \alpha^3, 1, \alpha^2)$　010 110 111 000 011 001 100
I_3に対する RS 符号語は、$(1, 1, 0, \alpha, 0, \alpha^3, \alpha)$　001 001 000 010 000 011 010

001 010 100　001 000 101　110 111 011
010 010 001 111 001 100 111　011 110 111 000 011 001 100　001 001 000 010 000 011 010
（上段は情報記号列、下段は RS 符号語列）

情報通信基礎Ⅰ　第７章　補足資料３

ガロア体 GF(3)

情シス　渡辺

ガロア体 GF(3)と原始多項式

・GF(2)は基礎としては容易であるが、より GF について理解するために、$GF(3)$と$GF(3^2)$を例に取り上げる。

・$GF(3)$、$GF(3^2)$を求める。

・$GF(3^2)$上の原始多項式(Primitive Polynomial)を求める。

１）　ガロア体 GF(3)

・p を素数とするとき、法 p に関する整数の剰余の集合（$F=\{0,1,2,,,,p-1\}$）は、法 p に関する加法と乗法の元に体$GF(p)$をなす。

・法 3 に関する整数の剰余の集合 F={0 1 2}は、下の加法+　と乗法・の元で体となる。これをガロア体$GF(3)$と呼ぶ。

＋	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

２）　拡大体$GF(3^2)$

・$GF(3)$上の任意の多項式を二次の多項式で除した余りの集合（剰余多項式集合）は、１次以下の多項式すべてが含まれる。剰余多項式集合の要素を列挙すると以下となる。

多項式	ベクトル表現
0	00
1	01
2	02
x	10
$x+1$	11
$x+2$	12
$2x$	20
$2x+1$	21
$2x+2$	22

・$GF(3)$上の既約多項式（原始多項式）$p(x)=x^2+x+2$の根をα（つまり$p(\alpha)=\alpha^2+\alpha+2=0$）とする。剰余多項式集合の各多項式に α を代入した値は、以下となる。

多項式	ベクトル表現	αべき表現	
0	00	0	
1	01	1	$=\alpha^0$
2	02	2	$=\alpha^4$
x	10	α	$=\alpha^1$
$x+1$	11	$\alpha+1$	$=\alpha^7$
$x+2$	12	$\alpha+2$	$=\alpha^6$
$2x$	20	2α	$=\alpha^5$
$2x+1$	21	$2\alpha+1$	$=\alpha^2$
$2x+2$	22	$2\alpha+2$	$=\alpha^3$

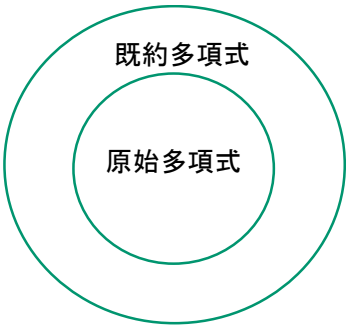
以下を用いている。

$\alpha^2 = -\alpha - 2 = 2\alpha + 1$
$\alpha^3 = \alpha^2\alpha = (2\alpha + 1)\alpha = 2\alpha^2 + \alpha = 2(2\alpha + 1) + \alpha = 4\alpha + 2 + \alpha = 2\alpha + 2$
$\alpha^4 = \alpha^3\alpha = (2\alpha + 2)\alpha = 2\alpha^2 + 2\alpha = 2(2\alpha + 1) + 2\alpha = 4\alpha + 2 + 2\alpha = 2$
$\alpha^5 = \alpha^4\alpha = 2\alpha$
$\alpha^6 = \alpha^4\alpha^2 = 2(2\alpha + 1) = 4\alpha + 2 = \alpha + 2$
$\alpha^7 = \alpha^4\alpha^3 = 2(2\alpha + 2) = 4\alpha + 4 = \alpha + 1$
$\alpha^8 = \alpha^4\alpha^4 = 2 * 2 = 4 = 1$

0 以外の要素をαのべき乗で表現できている。

拡大体$GF(3^2) = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}$　を構成する。

3）　拡大体$GF(3^2)$上での原始多項式の求め方



・原始多項式：既約多項式のうち、周期が最大となるものを原始多項式と言う。（注意：体論と環論で異なる定義がなされている。ここでは体論の原始多項式。環論の定義は、多項式の係数の最大公約数が 1 の時）

・$GF(p^m)$で議論する。ここでは、p=3, m=2 である。

・m 次以下の多項式で整除されない原始多項式を求めたい。

・多項式で、最上位桁の係数が 1 の多項式をモニック多項式と呼ぶ。（$GF(2)$では常に 1 だったのでこの話は出てこなかった。）

（あ）原始多項式を議論するときには、モニック多項式となる原始多項式を議論すればよい。（非モニックの原始多項式は、モニックの原始多項式の議論に帰着されるため。９）を参照）

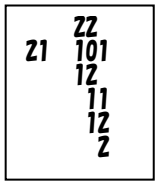
（い）さらに、原始多項式の最下位桁は非 0 でなければならない。なぜならば、0 であれば、xで整除されるので既約多項式とならないからである。

（あ）（い）より、GF(3)上の２次の原始多項式は、$p(x) = x^2 + ax + b \quad b \neq 0$　となる。

・従って、原始多項式の候補としては、

①　$p(x) = x^2 + 1$
②　$p(x) = x^2 + 2$
③　$p(x) = x^2 + x + 1$
④　$p(x) = x^2 + x + 2$
⑤　$p(x) = x^2 + 2x + 1$
⑥　$p(x) = x^2 + 2x + 2$

があり得る。上記の候補に対して、それぞれ以下の 2 ステップを行って原始多項式かどうかを確認する。



ステップ１）まず、候補が既約多項式であるかを確認する。

すなわち、m 次より小さい次数の多項式で整除されるかを調べる。

$GF(3^2)$であるので、m=2。従って、一次の多項式は、

A：$q(x) = x + 1$　　B：$q(x) = x + 2$　　C：$q(x) = 2x + 1$　　D：$q(x) = 2x + 2$

がある。このうち、モニック多項式のＡとＢで整除されるかを確認すれば十分である。（９）を参照）A，B で整除されれば既約多項式ではなく、原始多項式でもない。ステップ 1 で終了する。

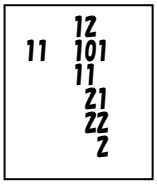
ステップ２）周期が最大であることを確認する。

x^q-1（この場合、$q=p^m-1=3^2-1=8$　なのでx^8-1）を整除し、かつ周期が最大のqであることを確認する。これは言い換えると$p(x)$で生成される$GF(3^2)=\{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}$の（０を除く）全要素が$\alpha$のべき乗で表現されることを確認することでもある。

① $p(x)=x^2+1$

ステップ１－１）x^2+1が、(A) $x+1$　で整除されるかを確認する。

右図より、剰余が２となり、整除されない。

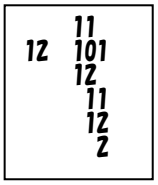


ステップ１－２）x^2+1が、(B) $x+2$　で整除されるかを確認する。

右図より、剰余が２となり、整除されない。

ステップ１－３）以上より、x^2+1は既約多項式であることがわかる。

ステップ２）$p(x)$で生成される$GF(3^2)=\{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}$の（０を除く）全要素が$\alpha$のべき乗で表現されることを確認する。



k	α^k	ベクトル表現	多項式表現
0	α^0	01	1
1	α^1	10	α
2	α^2	02	2
3	α^3	20	2α
4	α^4	01	1
5	α^5	10	α
6	α^6	02	2
7	α^7	20	2α
8	α^8	01	1

$\alpha^2+1=0$　だから

$\alpha^2=-1=2$

$\alpha^3=\alpha^2\alpha=2\alpha$

$\alpha^4=\alpha^3\alpha=2\alpha^2=4=1$

$\alpha^5=\alpha^4\alpha=\alpha$

$\alpha^6=\alpha^4\alpha^2=2$

$\alpha^7=\alpha^4\alpha^3=2\alpha$

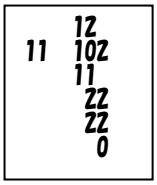
$\alpha^8=\alpha^4\alpha^4=1$

これより、例えば、$2\alpha+2$　をαのベキ乗で表現できないことが分かる。また、周期は４である。すなわち、x^2+1はx^8-1を整除するものの、x^4-1も整除し周期が最大ではない。従って、x^2+1は原始多項式ではない。

② $p(x)=x^2+2$

ステップ１－１）x^2+2が、(A) $x+1$　で整除されるかを確認する。

右図より、剰余が０となり、整除される。



ステップ１－２）略

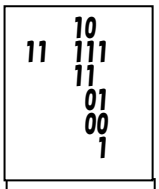
ステップ１－３）以上より、x^2+2は既約多項式ではない。

よって、x^2+2は原始多項式ではない。

③ $p(x)=x^2+x+1$

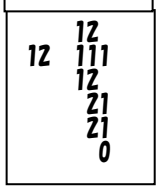
ステップ１－１）x^2+x+1が、(A) $x+1$　で整除されるかを確認する。

右図より、剰余が１となり、整除されない。



ステップ１－２）x^2+x+1が、(B) $x+2$　で整除されるかを確認する。

右図より、剰余が０となり、整除される。



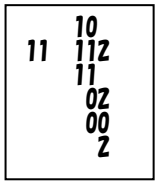
ステップ１－３）以上より、x^2+x+1は既約多項式ではない。

よって、x^2+x+1は原始多項式ではない。

④　$p(x)=x^2+x+2$

ステップ１－１）x^2+x+2が、(A) $x+1$　で整除されるかを確認する。

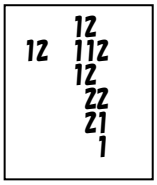
右図より、剰余が２となり、整除されない。



ステップ１－２）x^2+x+2が、(B) $x+2$　で整除されるかを確認する。

右図より、剰余が１となり、整除されない。

ステップ１－３）以上より、x^2+x+2は既約多項式であることがわかる。



ステップ２）$p(x)$で生成される$GF(3^2)=\{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}$の（０を除く）全要素が$\alpha$のべき乗で表現されることを確認する。

k	α^k	ベクトル表現	多項式表現
0	α^0	01	1
1	α^1	10	α
2	α^2	21	$2\alpha+1$
3	α^3	22	$2\alpha+2$
4	α^4	02	2
5	α^5	20	2α
6	α^6	12	$\alpha+2$
7	α^7	11	$\alpha+1$
8	α^8	01	1

$\alpha^2+\alpha+2=0$　だから

$\alpha^2=-\alpha-2=2\alpha+1$

$\alpha^3=\alpha^2\alpha=(2\alpha+1)\alpha=2\alpha^2+\alpha=2(2\alpha+1)+\alpha=4\alpha+2+\alpha=2\alpha+2$

$\alpha^4=\alpha^3\alpha=(2\alpha+2)\alpha=2\alpha^2+2\alpha=2(2\alpha+1)+2\alpha=4\alpha+2+2\alpha=2$

$\alpha^5=\alpha^4\alpha=2\alpha$

$\alpha^6=\alpha^4\alpha^2=2(2\alpha+1)=4\alpha+2=\alpha+2$

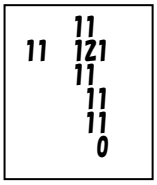
$\alpha^7=\alpha^4\alpha^3=2(2\alpha+2)=4\alpha+4=\alpha+1$

$\alpha^8=\alpha^4\alpha^4=4=1$

これより、$GF(3^2)=\{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}$の（０を除く）全要素が$\alpha$のべき乗で表現できることが分かる。また、周期は、８である。すなわち、x^2+x+2は、x^8-1を整除し、その周期は最大の８となっている。従って、x^2+x+2は原始多項式である。

⑤　$p(x)=x^2+2x+1$

ステップ１－１）x^2+2x+1が、(A) $x+1$　で整除されるかを確認す



る。

右図より、剰余が０となり、整除される。

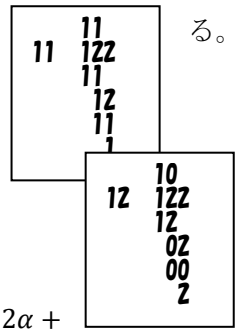
ステップ１－２）略

ステップ１－３）以上より、x^2+2x+1は既約多項式ではない。

よって、x^2+2x+1は原始多項式ではない。

⑥　$p(x)=x^2+2x+2$

ステップ１－１）x^2+2x+2が、(A) $x+1$　で整除されるかを確認する。



右図より、剰余が１となり、整除されない。

ステップ１－２）x^2+2x+2が、(B) $x+2$　で整除されるかを確認する。

右図より、剰余が２となり、整除されない。

ステップ１－３）以上より、x^2+2x+2は既約多項式であることがわかる。

ステップ２）$p(x)$で生成される$GF(3^2)=\{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}$の（０を除く）全要素が$\alpha$のべき乗で表現されることを確認する。

k	α^k	ベクトル表現	多項式表現
0	α^0	01	1
1	α^1	10	α
2	α^2	11	$\alpha+1$
3	α^3	21	$2\alpha+1$
4	α^4	02	2
5	α^5	20	2α
6	α^6	22	$2\alpha+2$
7	α^7	12	$\alpha+2$
8	α^8	01	1

$\alpha^2+2\alpha+2=0$　だから

$\alpha^2=-2\alpha-2=\alpha+1$

$\alpha^3=\alpha^2\alpha=(\alpha+1)\alpha=\alpha^2+\alpha=\alpha+1+\alpha=2\alpha+1$

$\alpha^4=\alpha^3\alpha=(2\alpha+1)\alpha=2\alpha^2+\alpha=2(\alpha+1)+\alpha=2\alpha+2+\alpha=2$

$\alpha^5=\alpha^4\alpha=2\alpha$

$\alpha^6=\alpha^4\alpha^2=2(\alpha+1)=2\alpha+2$

$\alpha^7=\alpha^4\alpha^3=2(2\alpha+1)=4\alpha+2=\alpha+2$

$\alpha^8=\alpha^4\alpha^4=4=1$

これより、$GF(3^2)=\{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}$の（０を除く）全要素が$\alpha$のべき乗で表現できることが分かる。また、周期は、８である。すなわち、x^2+2x+2は、x^8-1を整除し、その周期は最大の８となっている。従って、x^2+2x+2は原始多項式である。

以上より、

④　$p(x)=x^2+x+2$　　⑥　$p(x)=x^2+2x+2$

が原始多項式であることがわかった。（正確には、モニックな原始多項式）

９）モニック多項式と非モニック多項式

９－１）非モニック原始多項式とモニック原始多項式

３）では、モニック多項式だけを原始多項式候補として検討した。$GF(3)$に属す二次の多項式には、以下の非モニック多項式がある。ここでは、これらの非モニックな多項式が原始多項式となるかの議論は、モニック多項式の多項式が原始多項式となるかの議論に帰着されることを示す。

①’$p(x)=2x^2+1$

②’$p(x)=2x^2+2$

③’$p(x)=2x^2+x+1$

④’$p(x)=2x^2+x+2$

⑤’$p(x)=2x^2+2x+1$

⑥’$p(x)=2x^2+2x+2$

原始多項式であることを示すには、ステップ１）で既約多項式であるかを確認した後、ステップ２）で周期が最大となっているかを確認する。ステップ２では、候補となる多項式の根αで議論した。以下では、非モニック多項式でのステップ２の議論がモニック多項式での議論に帰着されることを示す。

①’ $p(x) = 2x^2 + 1$

$2\alpha^2 + 1 = 0$　だから　　$2\alpha^2 = -1 = 2$　　$\alpha^2 = 1$

（$GF(3)$上での割り算；a を b で割る、つまり a/b=c とすると、a=b*c。b に何かをかけたら a になるそういう c を探すことになる。この場合、2/2=c, 2=c*2。c=1）

このことから、ステップ２で周期の議論をするときには、$\alpha^2 - 1 = \alpha^2 + 2 = 0$で議論することとなる。従って、これは３）②に帰着される。

②’ $p(x) = 2x^2 + 2$

$2\alpha^2 + 2 = 0$　だから　　$2\alpha^2 = -2 = 1$　　$\alpha^2 = 2$　（1/2=c, 1=c*2。c=2）

このことから、ステップ２で周期の議論をするときには、$\alpha^2 - 2 = \alpha^2 + 1 = 0$で議論することとなる。従って、これは３）①に帰着される。

③’ $p(x) = 2x^2 + x + 1$

$2\alpha^2 + \alpha + 1 = 0$　だから　　$2\alpha^2 = -\alpha - 1 = 2\alpha + 2$　　$\alpha^2 = \alpha + 1$　（2/2=c, 2=c*2。c=1）

このことから、ステップ２で周期の議論をするときには、$\alpha^2 - \alpha - 1 = \alpha^2 + 2\alpha + 2 = 0$で議論することとなる。従って、これは３）⑥に帰着される。

④’ $p(x) = 2x^2 + x + 2$

$2\alpha^2 + \alpha + 2 = 0$　だから　　$2\alpha^2 = -\alpha - 2 = 2\alpha + 1$　　$\alpha^2 = \alpha + 2$　（1/2=c, 1=c*2。c=2）

このことから、ステップ２で周期の議論をするときには、$\alpha^2 - \alpha - 2 = \alpha^2 + 2\alpha + 1 = 0$で議論することとなる。従って、これは３）⑤に帰着される。

⑤’ $p(x) = 2x^2 + 2x + 1$

$2\alpha^2 + 2\alpha + 1 = 0$　だから　　$2\alpha^2 = -2\alpha - 1 = \alpha + 2$　　$\alpha^2 = 2\alpha + 1$　（1/2=c, 1=c*2。c=2）

このことから、ステップ２で周期の議論をするときには、$\alpha^2 - 2\alpha - 1 = \alpha^2 + \alpha + 2 = 0$で議論することとなる。従って、これは３）④に帰着される。

⑥’ $p(x) = 2x^2 + 2x + 2$

$2\alpha^2 + 2\alpha + 2 = 0$　だから　　$2\alpha^2 = -2\alpha - 2 = \alpha + 1$　　$\alpha^2 = 2\alpha + 2$　（1/2=c, 1=c*2。c=2）

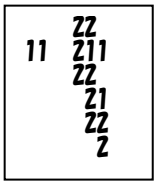
このことから、ステップ２で周期の議論をするときには、$\alpha^2 - 2\alpha - 2 = \alpha^2 + \alpha + 1 = 0$で議論することとなる。従って、これは３）③に帰着される。

以上を多項式をベクトルとして表現すると、

(2 0 1) -> (1 0 2)　　(2 0 2) -> (1 0 1)　　(2 1 1) -> (1 2 2)

(2 1 2) -> (1 2 1)　　(2 2 1) -> (1 1 2)　　(2 2 2) -> (1 1 1)

例として、③’ $p(x) = 2x^2 + x + 1$が原始多項式かを確認する。



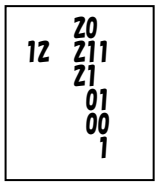
③’ $p(x) = 2x^2 + x + 1$

ステップ１－１）$2x^2 + x + 1$が、(A) $x + 1$　で整除されるかを確認する。

右図より、剰余が２となり、整除されない。

ステップ１－２）$2x^2 + x + 1$が、(B) $x + 2$　で整除されるかを確認する。

右図より、剰余が１となり、整除されない。



ステップ１－３）以上より、$2x^2+x+1$は既約多項式であることがわかる。

ステップ２）$p(x)$で生成される$GF(3^2)=\{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}$の（０を除く）全要素が$\alpha$のべき乗で表現されることを確認する。

k	α^k	ベクトル表現	多項式表現
0	α^0	01	1
1	α^1	10	α
2	α^2	11	$\alpha+1$
3	α^3	21	$2\alpha+1$
4	α^4	02	2
5	α^5	20	2α
6	α^6	22	$2\alpha+2$
7	α^7	12	$\alpha+2$
8	α^8	01	1

$2\alpha^2+\alpha+1=0$　だから

$\alpha^2=\alpha+1$

$\alpha^3=\alpha^2\alpha=(\alpha+1)\alpha=\alpha^2+\alpha=\alpha+1+\alpha=2\alpha+1$

$\alpha^4=\alpha^3\alpha=(2\alpha+1)\alpha=2\alpha^2+\alpha=2(\alpha+1)+\alpha=2\alpha+2+\alpha=2$

$\alpha^5=\alpha^4\alpha=2\alpha$

$\alpha^6=\alpha^4\alpha^2=2(\alpha+1)=2\alpha+2$

$\alpha^7=\alpha^4\alpha^3=2(2\alpha+1)=4\alpha+2=\alpha+2$

$\alpha^8=\alpha^4\alpha^4=4=1$

これより、$GF(3^2)=\{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}$の（０を除く）全要素が$\alpha$のべき乗で表現できることが分かる。また、周期は、８である。すなわち、$2x^2+x+1$は、x^8-1を整除し、その周期は最大の８となっている。従って、$2x^2+x+1$は原始多項式である。

以上より、非モニック原始多項式の議論はモニック原始多項式の議論に帰着される。ただし、非モニックであっても原始多項式あることには変わりない。？？？

情報通信基礎Ⅰ　第８章　たたみ込み符号

情シス　渡辺

ポイント

・今まで議論してきた符号はブロック符号と呼ばれ、ランダム誤りに対応している。

・バースト誤りに強い符号として、たたみ込み符号がある。

・効率のよい復号法としてビタビ復号がある。

８．１　基礎

８．１．１　誤り

ランダム誤り：各ビットが乱数で決定されるように誤る

バースト誤り：複数のビットがまとまって誤る

８．１．２　ブロック符号とたたみ込み符号

（１）ブロック符号

代表的な例としては、巡回符号、ＣＲＣ（Cyclic Redundancy Check）符号、ハミング符号、ＢＣＨ符号、リードソロモン符号などがある。ランダム誤り訂正に適している。

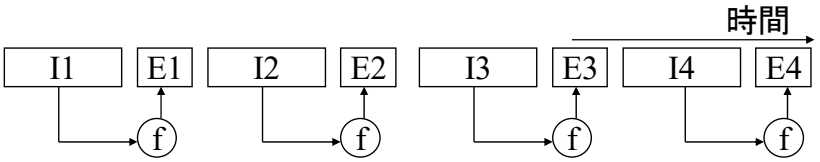


図８．１　ブロック符号

（２）畳み込み符号

バースト誤りに適している符号化である。ただし、バースト誤り訂正を行えるブロック符号もある。例えば、リードソロモン符号、ファイア符号などがある。

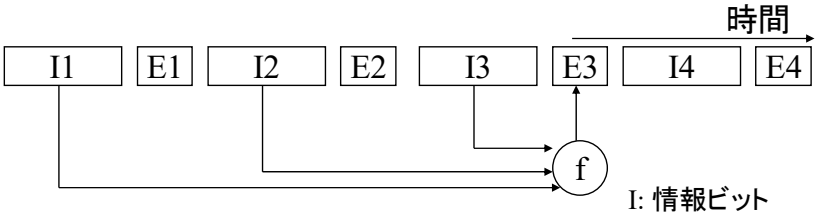


図８．２　たたみ込み符号

（３）たたみ込み符号の重要なパラメータ

重要なパラメータとしては、以下の２つがある。

拘束長Ｋ：　　情報１ビットが何ビット後まで影響するか。

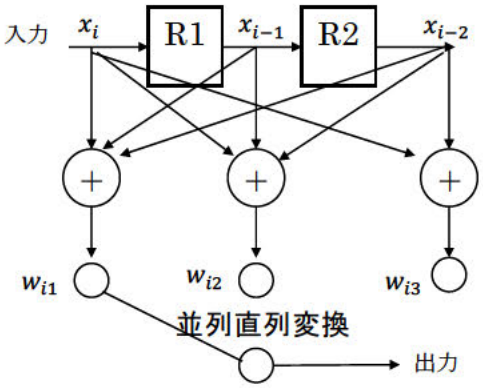
符号化率Ｒ：　情報１ビットが何ビットになるか。

拘束長Ｋは、レジスタ数に反映される

符号化率Ｒは、入力数と出力数に反映される

８．１．３　拘束長３　符号化率１／３の例

K=3, R=1/3 の例を示す。



$$w_{i1} = x_i + x_{i-1} + x_{i-2}$$
$$w_{i2} = x_i + x_{i-1} + x_{i-2}$$
$$w_{i3} = x_i + x_{i-2}$$

図8．3　拘束長3　符号化率1/3の例

レジスタの初期値を 0 として、入力が（101100）のときの出力 U は、以下となる。

U = (111, 110, 000, 001, 001, 111)

入力が(101100)の場合の状態遷移と出力

入力	出力
x_i	$x_i x_{i-1} x_{i-2}$ $w_{i1} w_{i2} w_{i3}$
1	1 0 0　1 1 1
0	0 1 0　1 1 0
1	1 0 1　0 0 0
1	1 1 0　0 0 1
0	0 1 1　0 0 1
0	0 0 1　1 1 1

図8．4　(101100)に対する出力

８．２　ビタビ復号

たたみ込み符号の効率のよい復号方式としてビタビ復号法がある。

８．２．１　ビタビ復号

・受信側では、トレリスダイヤグラムを用意する。

・トレリスダイヤグラムは、０が送信された時と１が送信された時のレジスタ状態の遷移を表現している。

・初期状態は００、最終状態は００とする。最終状態が００となるように、送るべき情報ビットの最後にビット列（テールビット）を挿入する。

・受信したビット列と正しいと想定されるビット列との差をメトリックとして記録する。
（メトリック：正しい符号語列との距離；何ビット誤ったらこの状態にたどり着くか）

・同じ状態になる複数のパスがある場合は、メトリックの小さいパスを残存させる。

・同じ状態になる同一のメトリックの複数のパスがある場合は、いずれかを選択する。

８．２．２　拘束長３　符号化率１／３の例

図８．３の例に対して、次のようなトレリスダイヤグラムを作成できる。１ブロック（こ

の例の場合 3 ビット）を受信する毎に 1 クロック時刻が進むとする。状態は、２つのレジスタの値で定義する。

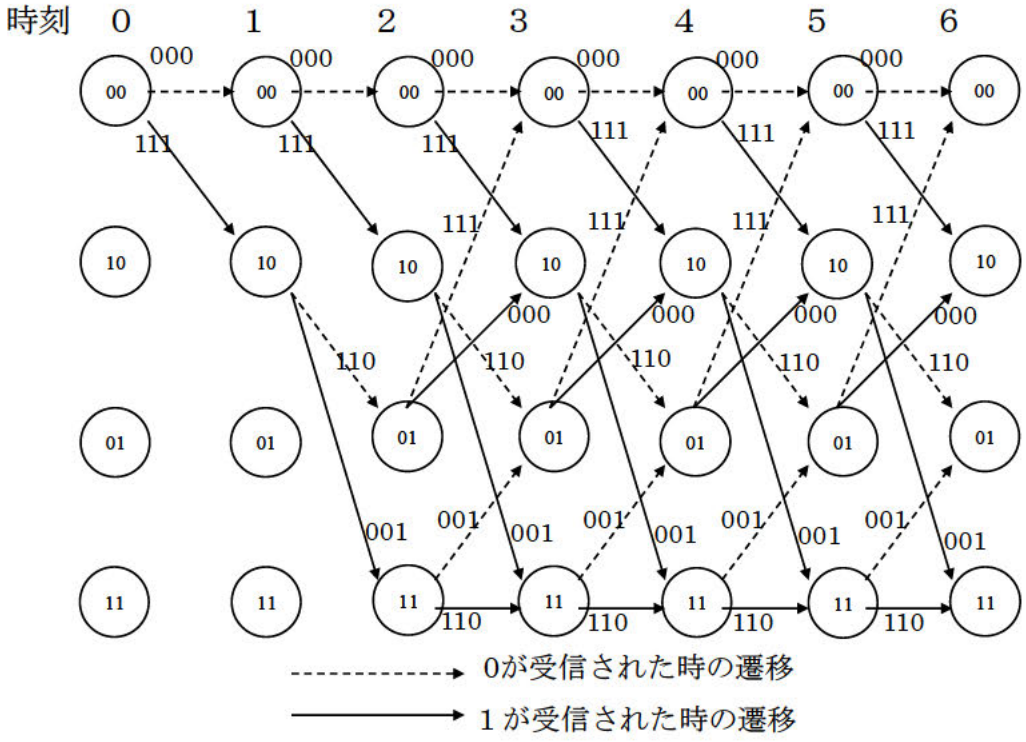


図8．５ トレリスダイヤグラム

今、情報　(1,0,1,1)に対してテールビットを加えた(1,0,1,1,0,0)を送ることを考える。符号化器で符号化し、Uを送ったところ、誤りが生じた符号語Vを受信したとする。

送信符号語列

U = (111, 110, 000, 001, 001, 111)

受信符号語列

V = (110, 010, 011, 101, 001, 111)

符号語を受信する度に、トレリスダイヤグラムを辿り遷移可能な状態への正しいパスとの差を計算してメトリックを求める。

時刻３の時のトレリスダイヤグラムを図８．６に示す。

★では、状態 00 からのパスのメトリックが５であるのに対し、状態 01 からのメトリックが３である。つまり、状態 01 を経由する方が誤る個数が少ないことを意味している。ここでは、00 からのパスを削除し、01 からのパスを残す。

※では、00 からのパスのメトリックと、01 からのパスのメトリックが同一である。この場合、いずれかを選択する。

時刻６の最終状態を図８．７に示す。この残存パスを逆に辿って復号する。この場合、(111, 110, 000, 001, 001, 111)に正しく復号できる。

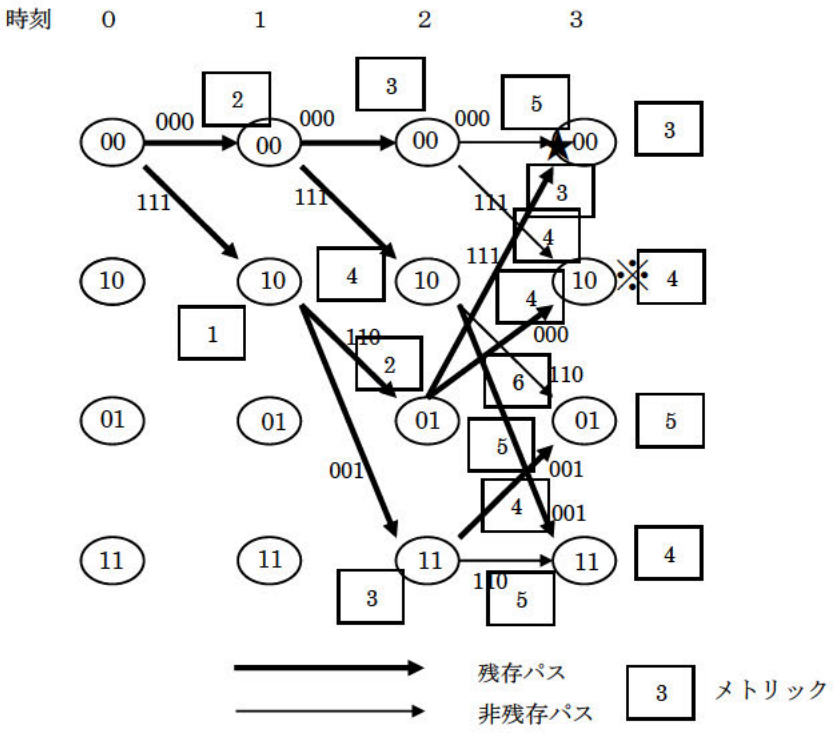


図8．6　時刻3での状態

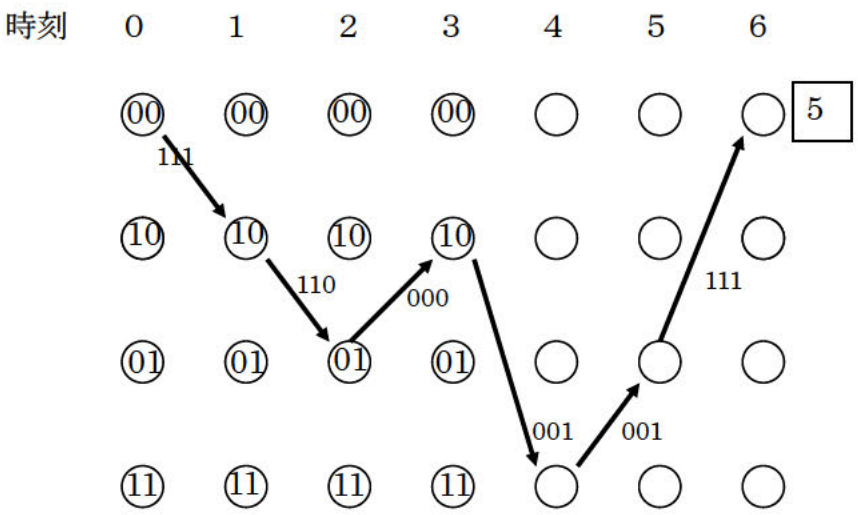
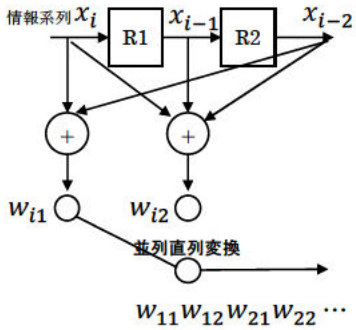


図8．7　時刻6での状態

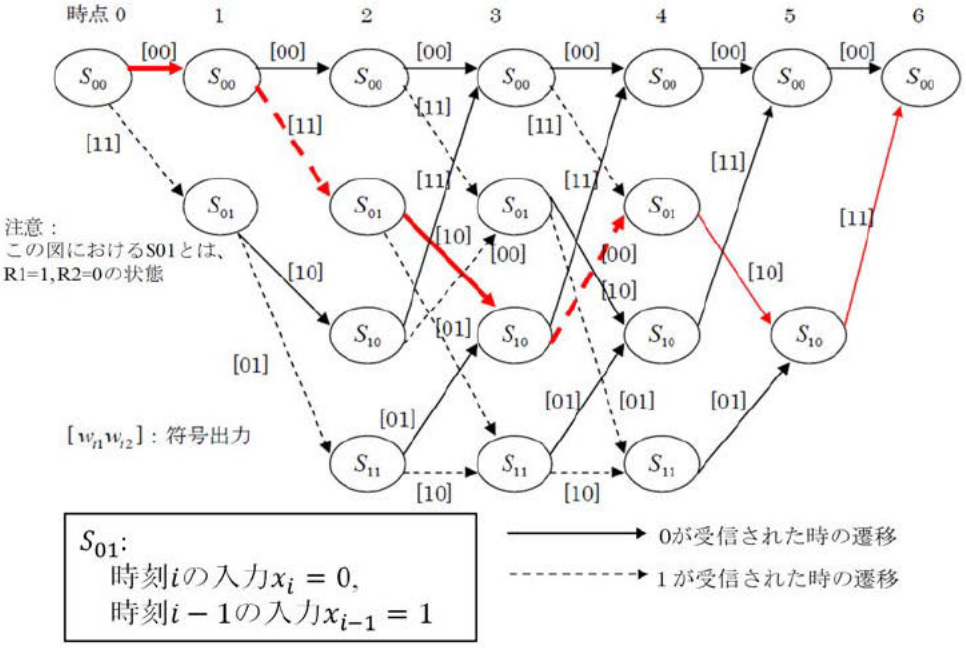
８．２．３　拘束長３　符号化率１／２の例

K=3, R=1/2 の例の符号化器とトレリスダイヤグラムを図８．８、図８．９に示す。



$$w_{i1} = x_i + x_{i-2}$$
$$w_{i2} = x_i + x_{i-1} + x_{i-2}$$

図8．8　K=3, R=1/2の例



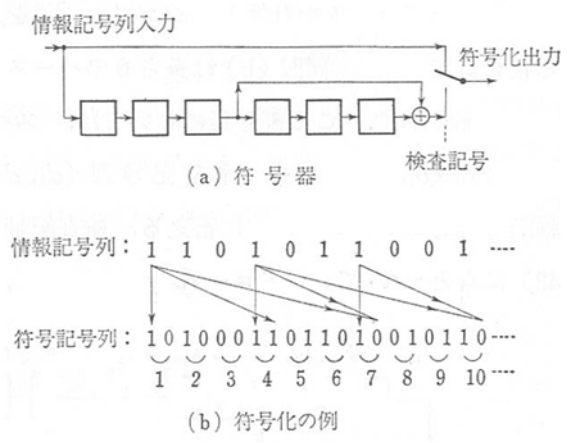
入力(010100)－＞出力(00 11 10 00 10 11)

図8．９　K=3, R=1/2のトレリスダイヤグラム

８．３　その他のたたみ込み符号

８．３．１　ハーゲルバーガー(14, 7)符号

島田良作、木内陽介、大松繁著「わかる情報理論」　日新出版　より抜粋



(mn_0, mk_0)の畳み込み符号で最も簡単な符号であり、長さ６までのバースト誤りを訂正可能である。　$k_0 = 1, m_0 = 1, m = 7,\ n_0 = k_0 + m_0$

この符号の生成行列は以下となる。

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

符号化方法

情報ビットを$(a_1\ a_2\ a_3\ a_4\ a_5\ ,,,,)$とすると、検査記号　c_iを以下のように求める。

c_i: 検査記号　$c_i = a_{i-3} + c_{i-6}$

送信する符号語は、$(a_1 c_1\ a_2 c_2\ a_3 c_3\ a_4 c_4\ a_5 c_5\ ,,,,)$ とする。

情シス　渡辺

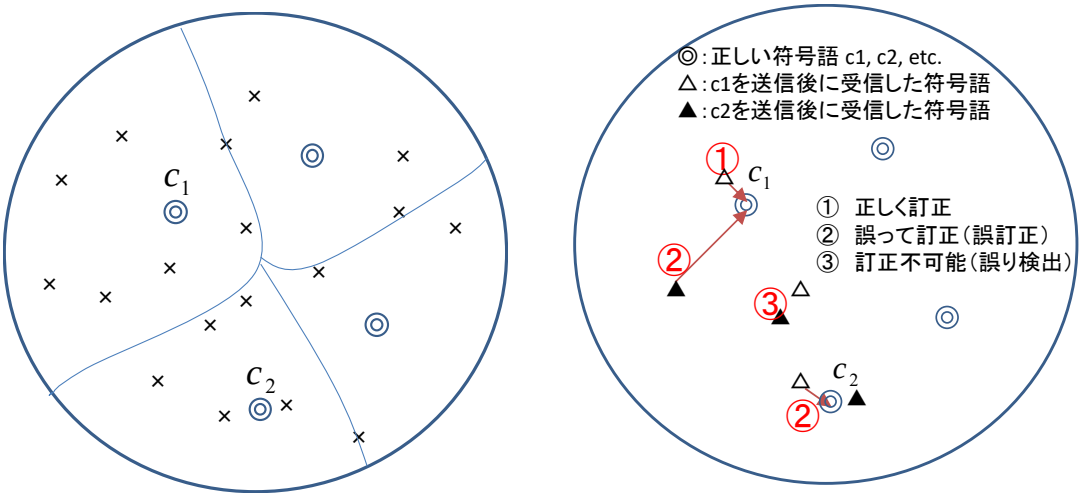
ポイント

・この章では、受信側で復号する立場で考察する。

・復号方式としては、MAP 復号、MLD 復号、MDD 復号、BDD 復号がある。

・符号長、情報ビット長、誤り訂正能力の議論

９．１　復号方式



９．１．１　復号の基礎

１）確率的復号

符号語の生起確率や通信路行列を利用する

MAP 復号、MLD 復号

２）代数的復号

符号語と受信語の距離を利用する

シンドローム復号、MDD, BDD

・MAP 復号　最大事後確率復号法（maximum a posterior probability decoding）

・MLD 復号　最尤復号法（maximum likelihood decoding）

・MDD 復号　最小距離復号法（minimum distance decoding）

・BDD 復号　限界距離復号法（bounded distance decoding）

・その他（繰り返し復号、ビタビ復号等）

９．１．２）MAP 復号　最大事後確率復号（maximum a posterior probability decoding）

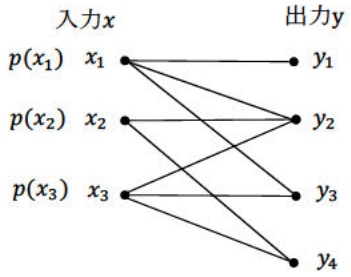
受信語r に対して、すべての符号語c_i $(i = 1,2,\ M)$（M は符号語数）についての事後確率$P(c_i|r)$を求め、それを最大とする符号語を選ぶ。すなわち、

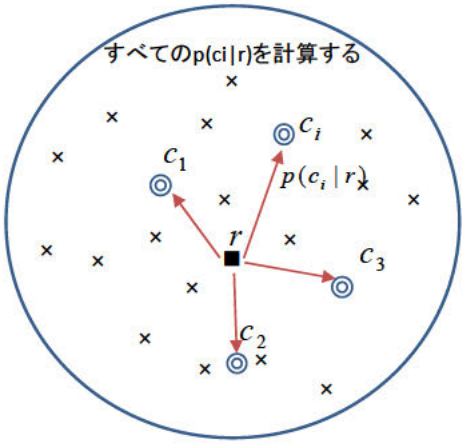
$\hat{m} = \arg\max_i P(c_i|r)$　　となる符号語$c_{\hat{m}}$を送信符号語と推定する復号法を MAP 復号という。最大事後確率復号法は、復号誤り確率を最小とする。

MAP 例：通信路行列および生起確率を以下とする。

$$\mathrm{P}=\begin{pmatrix} p(y_1|x_1) & p(y_2|x_1) & p(y_3|x_1) & p(y_4|x_1) \\ p(y_1|x_2) & p(y_2|x_2) & p(y_3|x_2) & p(y_4|x_2) \\ p(y_1|x_3) & p(y_2|x_3) & p(y_3|x_3) & p(y_4|x_3) \end{pmatrix}=\begin{pmatrix} 0.3 & 0.5 & 0.2 & 0 \\ 0 & 0.5 & 0 & 0.5 \\ 0 & 0.3 & 0.4 & 0.3 \end{pmatrix}$$

$p(x_1)=0.4 \qquad p(x_2)=0.3 \qquad p(x_3)=0.3$





ベイズ則

$$p(x_i|y_j)=\frac{p(x_i,y_j)}{p(y_j)}=\frac{p(x_i)p(y_j|x_i)}{\sum_{k=1}^{3}p(x_k)p(y_j|x_k)}$$

を利用して、$p(x_i|y_j)$を求める。

y_jに対して、$p(x_i|y_j)$が最大となるx_iに復号する。

$$p(x_1|y_1)=\frac{p(x_1)p(y_1|x_1)}{p(x_1)p(y_1|x_1)+p(x_2)p(y_1|x_2)+p(x_3)p(y_1|x_3)}=\frac{0.4*0.3}{0.4*0.3+0.3*0+0.3*0}=1$$ ←y_1に対して最大

$p(x_2|y_1)=0 \qquad p(x_3|y_1)=0$

$$\mathrm{p}(x_1|y_2)=\frac{p(x_1)p(y_2|x_1)}{p(x_1)p(y_1|x_1)+p(x_2)p(y_1|x_2)+p(x_3)p(y_1|x_3)}=\frac{0.4*0.5}{0.4*0.5+0.3*0.5+0.3*0.3}=\frac{0.2}{0.44}=\frac{20}{44}$$ ←y_2に対して最大

$$\mathrm{p}(x_2|y_2)=\frac{p(x_2)p(y_2|x_2)}{p(x_1)p(y_2|x_1)+p(x_2)p(y_2|x_2)+p(x_3)p(y_2|x_3)}=\frac{0.3*0.5}{0.4*0.5+0.3*0.5+0.3*0.3}=\frac{0.15}{0.44}=\frac{15}{44}$$

$$\mathrm{p}(x_3|y_2)=\frac{p(x_3)p(y_2|x_3)}{p(x_1)p(y_2|x_1)+p(x_2)p(y_2|x_2)+p(x_3)p(y_2|x_3)}=\frac{0.3*0.3}{0.4*0.5+0.3*0.5+0.3*0.3}=\frac{0.09}{0.44}=\frac{9}{22}$$

$$\mathrm{p}(x_1|y_3)=\frac{p(x_1)p(y_3|x_1)}{p(x_1)p(y_3|x_1)+p(x_2)p(y_3|x_2)+p(x_3)p(y_3|x_3)}=\frac{0.4*0.2}{0.4*0.2+0.3*0+0.3*0.4}=\frac{0.08}{0.2}=\frac{2}{5}$$

$$p(x_2|y_3)=\frac{p(x_2)p(y_3|x_2)}{p(x_1)p(y_3|x_1)+p(x_2)p(y_3|x_2)+p(x_3)p(y_3|x_3)}=\frac{0.3*0}{0.4*0.2+0.3*0+0.3*0.4}=0$$

$$\mathrm{p}(x_3|y_3)=\frac{p(x_3)p(y_3|x_3)}{p(x_1)p(y_3|x_1)+p(x_2)p(y_3|x_2)+p(x_3)p(y_3|x_3)}=\frac{0.3*0.4}{0.4*0.2+0.3*0+0.3*0.4}=\frac{0.12}{0.2}=\frac{3}{5}$$ ←y_3に対して最大

$$\mathrm{p}(x_1|y_4)=\frac{p(x_1)p(y_4|x_1)}{p(x_1)p(y_4|x_1)+p(x_2)p(y_4|x_2)+p(x_3)p(y_4|x_3)}=\frac{0.4*0}{0.4*0+0.3*0.5+0.3*0.3}=\frac{0}{0.24}=0$$

$$p(x_2|y_4)=\frac{p(x_2)p(y_4|x_2)}{p(x_1)p(y_4|x_1)+p(x_2)p(y_4|x_2)+p(x_3)p(y_4|x_3)}=\frac{0.3*0.5}{0.4*0+0.3*0.5+0.3*0.3}=\frac{0.15}{0.24}=\frac{5}{8}$$ ←y_4に対して最大

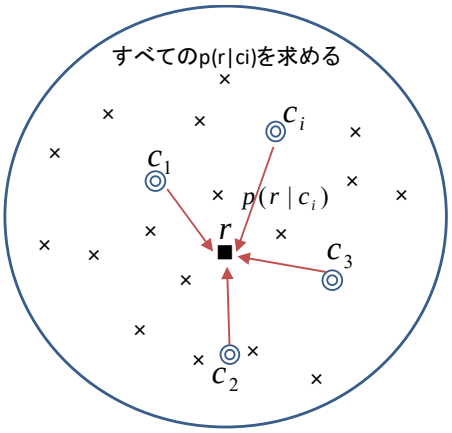
$$\mathrm{p}(x_3|y_4)=\frac{p(x_3)p(y_4|x_3)}{p(x_1)p(y_4|x_1)+p(x_2)p(y_4|x_2)+p(x_3)p(y_4|x_3)}=\frac{0.3*0.3}{0.4*0+0.3*0.5+0.3*0.3}=\frac{0.09}{0.24}=\frac{3}{8}$$

以上より、y_jを受信したときには以下のように復号する。

$y_1 \to x_1$　　$y_2 \to x_1$　　$y_3 \to x_3$　　$y_4 \to x_2$

９．１．３　MLD 復号　最尤復号（maximum likelihood decoding）

通常、符号語c_i は等確率で生起すると仮定できる。（第一定理を考えよ。）このとき、事後確率$P(c_i|r)$を最大にする符号語を求めることは、ベイズ規則より尤度$P(r|c_i)$ を最大にする符号語を求めることと等しい。すなわち、$\hat{m} = arg \max_i P(r|c_i)$となる符号語$c_{\hat{m}}$を送信符号語とできる。この復号法を MLD 復号という。通信路行列から比較的容易に判断できる。最尤復号法は、符号語の生起確率が等確率のとき復号誤り確率を最小とする復号法である。



MLD 例：通信路行列を以下とする。（MAP 例と同じ）

$$P = \begin{pmatrix} 0.3 & 0.5 & 0.2 & 0 \\ 0 & 0.5 & 0 & 0.5 \\ 0 & 0.3 & 0.4 & 0.3 \end{pmatrix}$$

列ベクトルの最大要素を選ぶ

$$P = \begin{pmatrix} 0.3 & 0.5 & 0.2 & 0 \\ 0 & 0.5 & 0 & 0.5 \\ 0 & 0.3 & 0.4 & 0.3 \end{pmatrix}$$

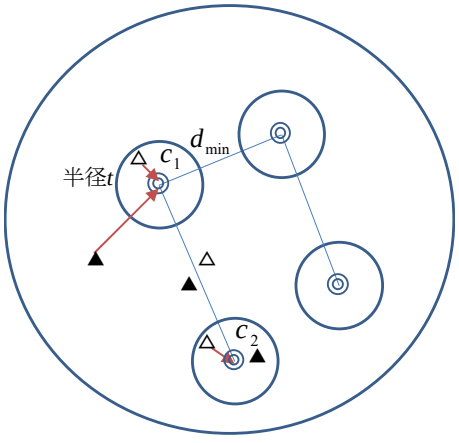
以上より、y_jを受信したときには以下のように復号する。

$y_1 \to x_1$　　$y_2 \to x_1 \ or \ x_2$　　$y_3 \to x_3$　　$y_4 \to x_2$

９．１．４　MDD 復号　最小距離復号（minimum distance decoding）

受信語rが受信されたとき、rから最小の距離に位置する符号語を送信符号語$c_{\hat{m}}$と推定する。二元対称通信路では、最小距離復号は最尤復号と等価である。

９．１．５　BDD 復号　限界距離復号（bounded distance decoding）



最小ハミング距離d_{min}に対して、

$d_{min} \geq 2t_1 + 1$

を満足するt_1を定め、受信語r が受信されたとき、

$d_H(c_i, r) \leq t_1$

なる符号語を送信符号語$c_{\hat{m}}$と推定する。

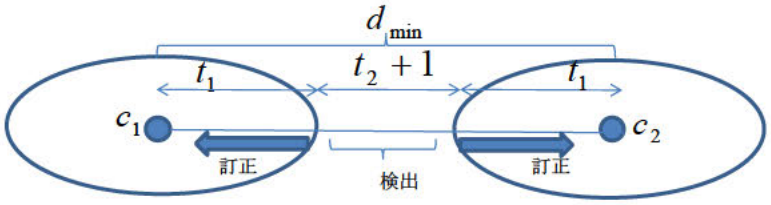
ただし、$d_H(c_i, c_j)$は、符号語c_iとc_jのハミング距離である。

この復号法では、t_1個以下の誤りを訂正する。

$t_0 = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$個までの誤りに対しては復号領域の重なりがないため，

正しく訂正することが可能である。すなわち、t_1の最大値は$t_0 = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$である。

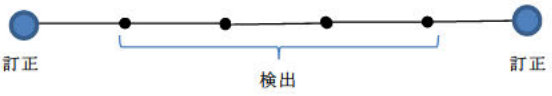
５－１）$d_{min} \geq 2t_1 + 1$となるようなt_1個以下の誤り訂正を行う



$t_2 + 1 = d_{min} - 2t_1$とおくと、上図では、t_1個以下の誤り訂正と、$t_1 + 1$個以上、$t_1 + t_2$個以下の誤り検出可能

t_1を大きくすると訂正能力は高くなるが誤って復号される確率も増大する。

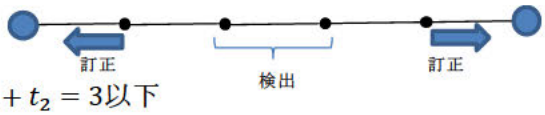
(例)　$d_{min} = 5$の符号を考える。



訂正能力　$t_1 = 0$　の時　　$t_2 + 1 = 5$

従って検出能力は、$t_1 + 1 = 1$以上　$t_1 + t_2 = 4$以下

訂正能力　$t_1 = 1$　の時　　$t_2 + 1 = 3$



従って検出能力は、$t_1 + 1 = 2$以上　$t_1 + t_2 = 3$以下

訂正能力　$t_1 = 2$　の時　　$t_2 + 1 = 1$

従って検出能力は、$t_1 + 1 = 3$以上　$t_1 + t_2 = 2$以下（不可）

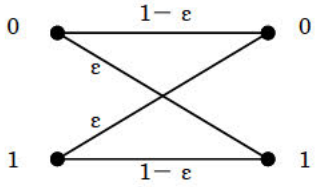
訂正能力は増大するが、検出能力は０で、復号誤り確率が増大する。

訂正ができなくても検出ができれば、ARQ で再送する方法があり得る。従って、訂正能力をあまり大きくしない方が総合的にはよい場合がある。

５－２）BSC(binary symmetric channel)における距離限界復号法の復号特性

符号長をn、ビット誤り率をεとすると、正しく復号される確率p_cは、

$$p_c = \sum_{i=0}^{t_1} \binom{n}{i} \varepsilon^i (1-\varepsilon)^{n-i}$$



となる。一方$t_1 + t_2 + 1$個以上のビット誤りが生じると、復号誤りが発生するので、復号誤り率p_eは、以下が成立する。

$$p_e \leq \sum_{i=t_1+t_2+1}^{n} \binom{n}{i} \varepsilon^i (1-\varepsilon)^{n-i}$$

訂正不可能な誤りが検出される確率(誤り検出率):　$p_d = 1 - p_c - p_e$

一般に、p_e、p_dは求めることが難しい。例えば、p_eには符号語の重み分布が必要であり、p_eは上界を示すことが多い。

９．１．６　いくつかの議論

１）最尤復号 MLD、限界距離復号法 BDD の比較

・BDD も MLD と同様に受信語に最も近い符号語を推定するが、すべての受信語に対して行うのではなく、各符号語を中心とする半径 t の球内に入る受信語に対してのみこの推定を行う。それ以外については推定を放棄する。

・正しく復号される確率p_cは、最尤復号の方が大きい　　pc（最尤復号）＞pc（限界距離復号）

・BDD の方が比較的容易に実現できる。
・最小距離は「確実に」誤り訂正できる距離を示している。逆に言うと、誤り訂正の限界を示しているわけではない。

例）符号語　A (0000000)　B(1100010)　C(0001011)　D(1110100)

最小距離＝３　従って、２ビット以上の誤りの訂正は保証されない。

・送信語 A(0000000)　受信語 V=(1100000)　の時

最小距離から求めると、A, B, C, D との距離は、それぞれ 2, 1, 3, 2

B(1100010)に復号される－＞誤訂正

・送信語 A(0000000)　受信語 V=(0001100)　の時

最小距離から求めると、A, B, C, D との距離は、それぞれ 2, 5, 3, 4

A(0000000)に復号できる。

つまり同じ２ビット誤りでも正しく訂正される場合とそうでない場合がある。

例えば、BSC（誤り率ε）で BCH(15, 7)符号を考える。BCH(15, 7)符号は最小距離$d_{min} = 5$。よって２ビット誤りまで訂正可能。

限界距離復号法で２ビット誤りまで訂正する（$t_1 = 2, t_2 = 0$）とすると、訂正できない誤りは３ビット以上であるので、

$$p_e = \sum_{i=t_1+t_2+1}^{n} \binom{n}{i} \varepsilon^i (1-\varepsilon)^{n-i} = \sum_{i=3}^{15} \binom{15}{i} \varepsilon^i (1-\varepsilon)^{15-i} = 1 - \sum_{i=0}^{15} \binom{15}{i} \varepsilon^i (1-\varepsilon)^{15-i}$$

$\varepsilon = 0.05$の場合、$p_e = 0.036$となる。一方、最尤復号法では（シミュレーションによって求めると）、$p_e = 0.0038$となる。この差は、最尤復号法では２ビット以上の誤りも訂正しているためである。

２）計算複雑度

最尤復号法や最小距離復号法は、受信語とすべての符号語に対して、尤度やハミング距離の比較を行わなければならない。よって、符号長nの指数オーダの演算回数、例えば二元符号については$O(2^{nR})$を必要とする。R は符号化比率である。しかし、代数的復号法は、nの多項式オーダの演算回数（例えば二元 BCH 符号においては$O(n(\log n)^2)$）で実行する復号アルゴリズムが存在する。バーレカンプ-マッシーアルゴリズム、ユークリッド復号アルゴリズムなどはその例であり、広く実用に供されている。また、畳込み符号のように最尤復号を少ない計算量で実行する復号アルゴリズムも存在する。

参考書等
１．電子情報通信学会『知識の森』（http://www.ieice-hbkb.org/）1 群（信号・システム）2 編（符号理論）1 章符号理論の基礎（鎌部浩、鴻巣敏之）
２．今井秀樹　情報理論　昭晃堂
３．村上孝三　情報通信基礎１講義資料
４．平澤茂一　符号理論

９．２　符号の限界式（発展）

９．２．１　概要と準備

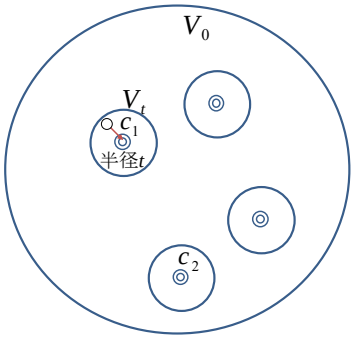
・線形符号の訂正能力と符号化率の間のトレードオフ

・符号長n、符号語数M、最小距離d_{min}の間の関係
・ハミング限界式、プロトキン限界式、シングルトン限界式
　　n、d_{min}に対して、符号語数Mの上界を与える
　　あるパラメータにおける符号の非存在性を与えている
・バルシャモフ-ギルバート限界式
　　n、M、d_{min}がある関係式を満たすならばその符号の存在を保証
・準備
　　q元(n, k, d_{min})線形符号Cを考える。
　　符号長n、符号語数M、最小距離d_{min}
　　nとMが与えられた時、d_{min}をできる限り大きくする
　　nとd_{min} が与えられた時、M をできる限り大きくする
　　情報シンボル数$k = log_q M$、検査シンボル数$m = n - k$、最大誤り訂正能力$t = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$

９．２．２　ハミング限界(Hamming bound)

$$M \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i} \quad \cdots (1)$$

・符号長nと誤り訂正能力tが与えられたとき符号語数Mの上界
・等号が成立する符号は完全符号と呼ばれる
　　2 元完全符号：ハミング符号、ゴーレイ符号
・証明概略：符号のq 次元ベクトル空間球体とその中の符号語c_iを中心とする球から、球体に存在しうる符号語数を求める。



　　c_iから距離 $0 (i = 0)$にある符号語の数 1
　　c_iから距離 $1 (i = 1)$ にある符号語の数 $\binom{n}{1}(q-1)^1$
　　c_iから距離 $2 (i = 2)$にある符号語の数 $\binom{n}{2}(q-1)^2$
　　従って、c_iから距離t以下の符号の総数（体積）V_tは、

$$V_t = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \quad \cdots (2)$$

となる。全符号語数（空間体積）V_0は$V_0 = q^n$。球体の中に入る球の数から$M \leq \frac{V_0}{V_t}$となる。

・（１）式は、$n - k = m \geq log_2 \sum_{i=0}^{t} \binom{n}{i}$ とも表現される。$(q = 2)$

９．２．３　プロトキン限界(Plotkin bound)

$$d_{min} \leq \frac{nM(q-1)}{(M-1)q} \quad \cdots (3)$$

・n、Mに対する最小距離d_{min}の上界
・任意の２つの符号語間の距離の平均値は、最小距離より大きくなることから導出可能
・等号が成立する符号は等距離符号と呼ばれる。
　　等距離符号：シンプレックス符号

９．２．４　シングルトン限界(Singleton bound)

$d_{min} \leq n - k + 1$　・・・（４）

・検査行列のランクが、高々$n-k$であることから導出可能。

・等号を満たす符号は最大距離分離符号（maximum distance separable code; MDS 符号）と呼ばれる。

・二元の MDS 符号：$(n, 1, n)$反復符号、$(n, n-1, 2)$パリティ検査符号（３項組は(n, k, d_{min})）。

q元の MDS 符号：リードソロモン符号

・（４）式は、$M = q^k \leq q^{n-d_{min}+1}$　とも表現できる。

９．２．５　バルシャモフ-ギルバート限界（Varshamov-Gilbert bound）、VG 限界（線形符号）

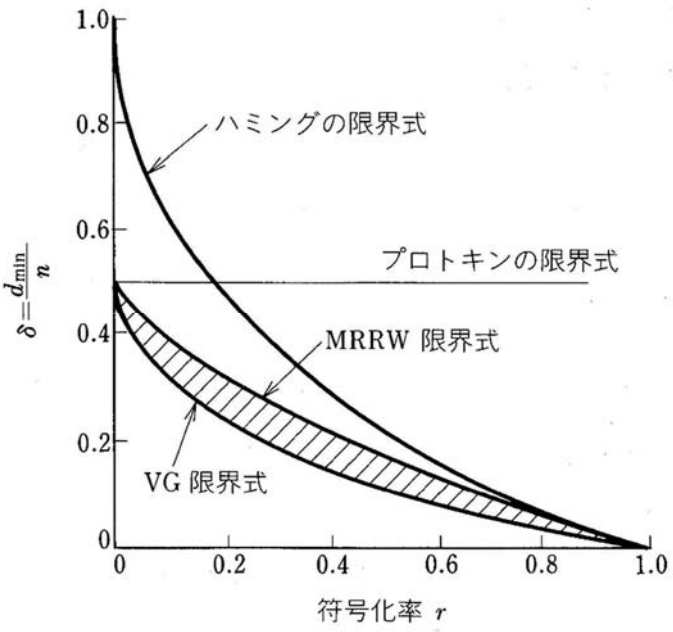
$$q^{n-k} > \sum_{i=0}^{d_{min}-2} \binom{n-1}{i} (q-1)^i \quad \cdots (5)$$

を満たすならば、q元(n, k, d_{min})符号が存在する。（今井　p.143）

・ハミング限界、プロトキン限界、シングルトン限界は符号が存在するための必要条件であるのに対し、VG 限界は十分条件

・VG 限界は符号長が短い場合は厳密な限界式にはならない。実際に符号長 1000 以下の BCH 符号は多くの場合この限界を超えている。一方、符号長が長い範囲ではこの限界式に達する符号を構成することは容易ではないが、代数幾何符号においていくつかの構成法が与えられている。

・その他の上界の限界式として、マクエリース-ロディミッチ-ルンセィ-ウェルチ限界（McEliece-Rodemich-Rumsey-Welch bound; MRRW 限界）がある。



参考書等

１.今井秀樹　符号理論　電子情報通信学会

２．電子情報通信学会『知識の森』（http://www.ieice-hbkb.org/）１群（信号・システム）２編（符号理論）１章符号理論の基礎（鴻巣敏之）、３ 章符号の性能（和田山正、森井昌克）

プロトキン限界の証明

０）全体像

・以下では、$q = 3$、$n = 4$、$\{0, 1, 2\}$を例として挙げるが、容易にq元へ一般化可能

・符号語の全ペアの総距離を導出（１～８）、全ペア数で割って平均を導出（９～１１）

１）全符号語

0000
0001
0002
　$3^4 = q^n$個

0010

:

2222

２）この中で、１番目の記号が 0 のものの数M_1は、

0000
0001
0002　$M_1 = 3^3 = q^{n-1}$個
0010
:
0222

３）逆に１番目の記号が 0 ではないものの数は、$M - M_1$個

４）第 1 記号=0 の符号語と第 1 記号≠0 の符号語のペアの「第 1 記号だけに限った距離」（以下第 1 記号距離と表現）は、１。（例：0001 と 2012 の第 1 記号距離は１）

従って、第 1 記号=0 の符号語と第 1 記号≠0 の符号語の全ペアの第 1 記号距離の総和は、組み合わせの数と同数。つまり、２）と３）の組み合わせの数、$M_1(M - M_1)$。

５）次に第 1 記号=1 の符号語を考える。４）と同様に、第 1 記号=1 の符号語と第 1 記号≠1 の符号語のペアの第 1 記号距離は、１。従って、第 1 記号=1 の符号語と第 1 記号≠1 の符号語の全ペアの第 1 記号距離の総和は、組み合わせの数と同数。第 1 記号=1 の符号語の数をM_2とすれば、２）と３）と同様に考えて組み合わせの数、$M_2(M - M_2)$。

同様に、第 1 記号=$q-1$の符号語と第 1 記号≠ $q-1$の符号語の全ペアの第 1 記号距離の総和は、$M_q(M - M_q)$。

６）よって、第 1 記号距離の総和S_1は、

$S_1 = M_1(M - M_1) + M_2(M - M_2) + \cdots + M_q(M - M_q) = M^2 - ({M_1}^2 + {M_1}^2 + \cdots + {M_q}^2)$

７）$S_1 = M^2 - ({M_1}^2 + {M_1}^2 + \cdots + {M_q}^2)$　が最大となるのは、

$M_1 = M_2 = \cdots = M_q = \frac{M}{q}$　の時（証明は※）

よって、$S_1 \le M^2 - q\left(\frac{M}{q}\right)^2 = \frac{q-1}{q}M^2$

８）１）～７）と同様に第２記号距離の総和S_2を求めると、$S_2 \le \frac{q-1}{q}M^2$

よって、全符号語ペアの距離の総和Sは、$S = S_1 + S_2 + \cdots + S_n \le n\frac{q-1}{q}M^2$

９）全符号ペア数は、５）で逆順（例えば、1-2 と 2-1）も重複してカウントしていることに注意すると、${}_MP_2 = M(M-1)$

１０）よって、１ペアの符号間の距離の平均、すなわち平均距離d_{ave}は、

$$d_{ave} = \frac{S}{{}_MP_2} = \frac{n\frac{M^2(q-1)}{q}}{M(M-1)} = \frac{nM(q-1)}{q(M-1)}$$

１１）d_{min}は、d_{ave}より小さいので、$d_{min} \le d_{ave} = \frac{nM(q-1)}{q(M-1)}$

※ $M = M_1 + M_2 + \cdots + M_q$ の条件下で、$f(\mathbb{M}) = \sum_{i=1}^{q} {M_i}^2$を最小化する。

Lagrange の未定定数法を用いる。

$F(\mathbb{M}, \lambda) = \sum_{i=1}^{q} {M_i}^2 + \lambda g(\mathbb{M})$　　ただし、$\mathrm{g}(\mathbb{M}) = \sum_{i=1}^{q} M_i - M = 0$

とする。

$\frac{\partial}{\partial M_i} F(\mathbb{M}, \lambda) = 2M_i + \lambda = 0$　　$\therefore M_i = -\frac{\lambda}{2}$ for all i

$\mathrm{g}(\mathbb{M}) = \sum_{i=1}^{q} M_i - M = 0$

より、$M_i = \frac{M}{q}$

シャノン第一定理と MAP, MLD の説明

シャノンの第１定理に従って情報源符号化がなされていれば、符号語c_i は等確率で生起する。

$p(x_i|y_j) = \frac{p(x_i,y_j)}{p(y_j)} = \frac{p(x_i)p(y_j|x_i)}{\sum_k p(x_k)p(y_j|x_k)}$

$p(x_i)$ =一定　とすると、

$p(x_i|y_j) = \frac{p(x_i)p(y_j|x_i)}{p(x_i)\sum_k p(y_j|x_k)} = \frac{p(y_j|x_i)}{\sum_k p(y_j|x_k)}$　が成立する。

ここで、分母の$\sum_k p(y_j|x_k)$は j に関しては一定であるので、$\max_i p(x_i|y_j)$は、$\max_i p(x_i|y_j)$と等価である。以上より、事後確率を最大にする符号語を選ぶこと（$\hat{m} = \arg\max_i P(c_i|r)$）と、尤度を最大にする符号語を選ぶこと（$\hat{m} = arg\ \max_i P(r|c_i)$）は等価となる。

情報通信基礎Ⅰ　第１０章　近年の話題

情シス　渡辺

ポイント

・情報理論の近年の話題

・符号理論の近年の話題

１０．１　符号理論の近年の話題

１０．１．１　概要

ターボ符号、低密度パリティ検査符号（LDPC)、レートレス符号

・1993 年に提案されたターボ符号、1960 年代の発明から 30 年以上を経て再発見された低密度パリティ検査（LDPC）符号は、大きな変革をもたらし現在では実用化・標準化されている。

・共通事項

－簡単な符号化を組み合わせた連接符号化＋繰り返し復号

－符号長が大きい場合でも実装可能な程度の計算量で復号が可能

－適切に長い符号を設計することで通信路容量（シャノン限界）に迫る特性を達成する

・ターボ符号は、帰還結線を有する畳み込み符号化器を２個組み合わせたもの

・LDPC 符号は、非零成分の密度が低い疎な検査行列をもつ線形符号

単一パリティ検査符号と繰り返し符号の組み合わせ

・要素符号に対しては低複雑度の復号法が存在する。

サム・プロダクトアルゴリズムにより効率的に復号可能。受信語が与えられたもとで符号語の各シンボルに対して事後確率の周辺分布を計算する。

・各要素符号に対してシンボル単位の復号を行い、そこで得られる値をほかの要素符号の復号器で各シンボルの事前確率として用いることが繰り返される。

・復号誤り確率に関しては符号長が大きければ理論的限界に近い性能

１０．１．２　ターボ符号（turbo code）

１）基礎

・1993 年ベロー（Berrou）らにより提案

・従来の符号では、実用上十分低い誤り率を実現するには、理論限界に比べ、少なくとも 2[dB] 良好な信号対雑音電力比（SNR）が必要だったが、ターボ符号は、現実的な復号処理量で、これを 0.5[dB] まで近づけた。

・第 3 世代携帯電話でデータ通信時に使われている。

２）符号化器

・２個の畳み込み符号器（それぞれを要素符号器と呼ぶ）が含まれている。

・パリティビット系列１の生成：要素符号器１によりパリティビット系列１を生成

・パリティビット系列２の生成：ある単位（インタリーバサイズ）に区切り、インタリー

バ（interleaver）で系列の順番を入れ替える。

典型的なインタリーバサイズは 64k 程度

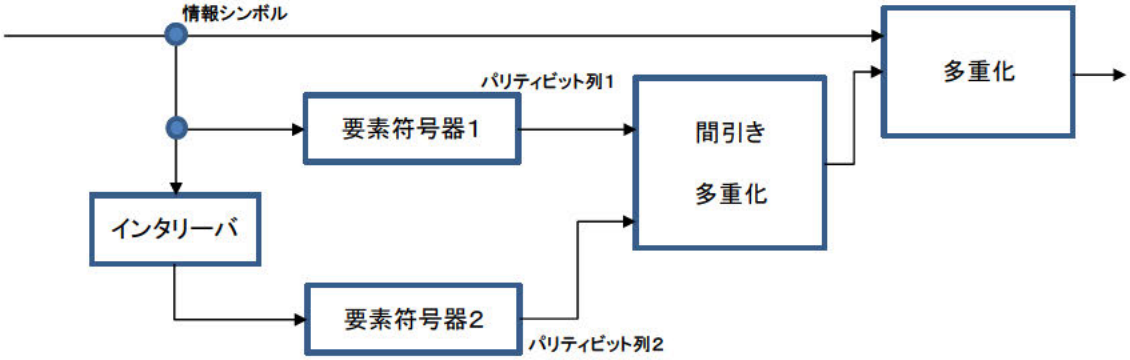
要素符号器 2 によりパリティビット系列 2 を生成

・間引き多重化：パリティビット系列 1 およびパリティビット系列 2 を間引いて多重化

・多重化：間引き多重化出力と情報系列とを多重化

・並列連接畳み込み符号（parallel concatenated convolutional code）

・各要素符号器は、フィードバック型畳み込み符号器



ターボ符号の符号器

3）復号器

・受信系列から要素復号器 1 に入力される

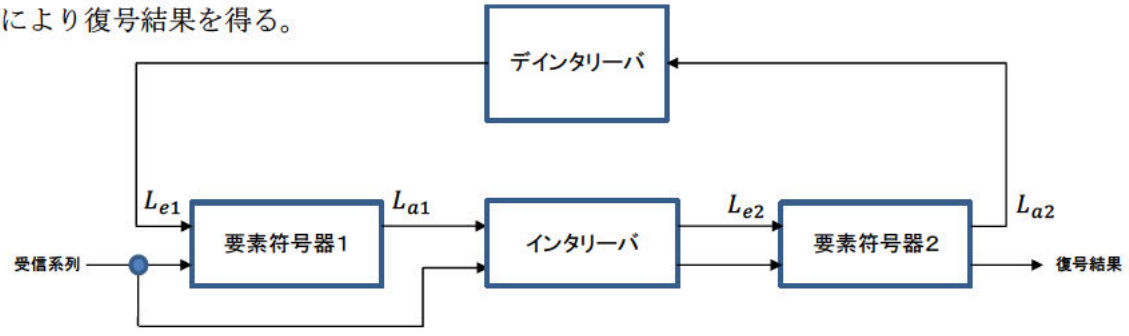
・通信路値（channel value）と要素復号器 2 から伝えられる事前値（a priori value）L_{a1} を用い、BCJR アルゴリズム（Bahl-Cocke-Jelinek-Raviv algorithm; 1974）あるいは max log MAP アルゴリズムにより、外部値（extrinsic value）L_{e1} を得る。（初期値は 0）

・L_{e1} は、インタリーバで並べ替えられ、要素復号器 2 の事前値 L_{a2} として入力される。

・要素復号器 2 は、要素復号器 1 と同様の動作により外部値 L_{e2} を求める。

・L_{e1} は、デインタリーバを介して、要素復号器 2 の事前値となる。

・これを 10 回程度繰り返した後、事後値（a posteriori value）を求め、硬判定することにより復号結果を得る。



ターボ符号の復号器

・繰り返し回数を増加させると特性が改善される

・符号化率 1/2、通信路は白色ガウス雑音通信路の例では、理論限界（シャノン限界）0.2dB に対して、0.5dB まで近づく。

１０．１．３　LDPC（Low-Density Parity Check、低密度パリティ検査）符号

１）基礎

・疎な検査行列により定義される線形符号

・サム・プロダクト（sum-product）アルゴリズムに基づく反復復号法（iterative decoding）（サム・プロダクト復号法）と組み合わせることより、シャノン限界に迫る高い復号性能を達成する。

・LDPC 符号の元は 1960 年代初頭のギャラガー（Gallager）の博士論文

・1950～1960 年代は、重要な BCH 符号や RS 符号が開発され、代数的符号理論の基礎が築かれつつあった。LDPC 符号が再注目されたのは、1990 年代初頭のターボ符号の成功と確率推論に基づく誤り訂正符号の見直しから。マッカイ（MacKay）による LDPC 符号の再発見、確率推論や機械学習、統計力学などの応用数理分野と LDPC 符号の研究との結合

・イーサネットや衛星通信などにおける誤り訂正方式として標準化

・以下では GF(2) 上の 2 元 LDPC 符号のみを考える。

２）LDPC 符号

・IEEE 802.16e、10Gbps Ether、衛星デジタルテレビ放送 DVB-S2、G975 等で利用

・GF(2)上の$m \times n$ 行列$H = [h_{ij}]$を検査行列とする線形符号C

・Hが疎行列（sparse matrix）のときC を LDPC 符号と呼ぶ。

LDPC(12, 6)の検査行列（右図）

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

・正則 LDPC 符号（regular LDPC code）：Hの各行及び各列の重みが一定値

・検査行列Hから一意に定まる二部グラフ（bipartite graph）を考える

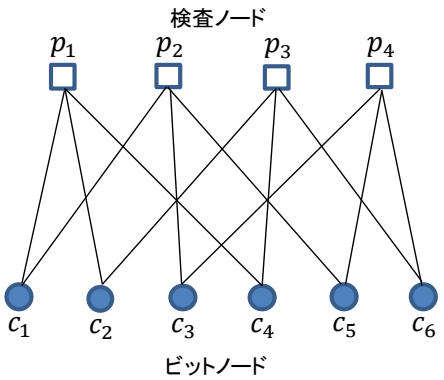
・Hの各行に対応する節点を$p_i\ (i = 1, 2, , , m)$とする。p_iを検査ノード（check node）と呼ぶ。p_iの点集合を$V_c = \{p_1, p_{2,,,} p_m\}$ とする。

・Hの各列に対応する節点を$c_j\ (j = 1, 2, , , n)$ とする。c_jをビットノード（bit node）と呼ぶ。c_jの点集合を$V_b = \{c_1, c_{2,,,} c_n\}$ とする。

・ $V = V_c \cup V_b$ を節点集合、 $E = \{(p_i, c_j) \in V_c \times V_b \mid h_{ij} = 1\}$を枝集合とする二部グラフ$\Gamma = (V, E)$を考える。

・Γを線形符号CのHに関するタナー（Tanner）グラフと呼ぶ。

・LDPC 符号では、検査行列Hにおける非零要素の個数が符号長の定数倍程度であるとき、H を疎行列とみなすことが多い。



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

３）復号

メッセージ・パッシング復号法等が用いられる。省略

文献

[1] 電子情報通信学会『知識の森』（http://www.ieice-hbkb.org/）◆1 群－2 編－6 章■1 群（信号・システム）-- 2 編（符号理論）6 章ターボ符号・LDPC 符号（井坂元彦、荻原春生）

[2]低密度パリティ検査(LDPC)符号技術　三菱電機　松本渉

[3] "A 32 Gbps 2048-bit 10GBASE-T Ethernet Energy Efficient LDPC Decoder with Split-Row Threshold Decoding Method", Tinoosh Mohsenin and Bevan M. Baas, University of California, Davis

１０．２　情報理論の近年の話題

情報通信基礎Ⅰ　第１１章　付録

2021/12/ 8

情シス　渡辺

目次

１１．１　（符号理論のための）線形代数の復習（5 章の付録）

１）ベクトル空間（あるいは線形空間）

定義

２項演算として、ベクトル加法、スカラー乗法を定義する。

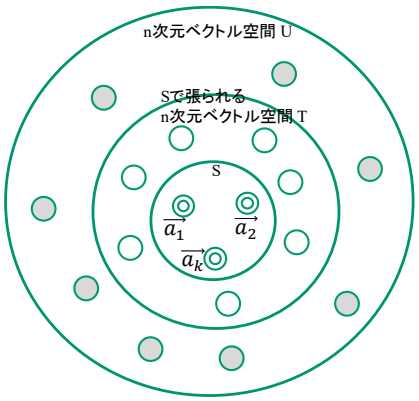
体Fを定義する。ベクトル集合Vが以下を満たすとき、Vを体F上のベクトル空間という。

ベクトル加法：閉塞性、結合則、可換則、恒等元、逆元　（以上まとめて可換群）

スカラー乗法：閉塞性、結合則、恒等元

ベクトル加法・スカラー乗法：2 種類の分配則

ベクトル加法、スカラー乗法とは別に、体の加法、体の乗法があることに注意する。このことは、一般化して関数など数値以外をベクトルとする場合には重要である。詳細は、９）ベクトル空間詳細を参照のこと



体の例：（課題：体の定義を再確認すること）

$\mathbb{R}$: 実数体 real number field

$\mathbb{Q}$: 有理数体 rational number field

$\mathbb{C}$: 複素数体 complex number field

F_q: ガロア体（有限体）q 素数、GF(q)とも書く　Galois Field, finite field

n個の要素からなるベクトルをn次元ベクトルと呼ぶ。例えば、各要素が実数のn次元ベクトルは、$r = (r_1,\ r_2, \cdots, r_n) \quad r_i \in \mathbb{R} \quad r \in \mathbb{R}^n$ と表現される。また、$r_1,\ r_2, \cdots, r_n$の全ての組み合わせで表現されるベクトル空間をn次元ベクトル空間と呼ぶ。

n次元ベクトルUの部分集合であるTが、あるベクトルの集合Sの要素の線形結合によって表現されうるとき、SがTを張る(span)と言う。例えば、ベクトル$\overrightarrow{a_1},\ \overrightarrow{a_2}, \cdots\ \overrightarrow{a_k}$（$\overrightarrow{a_i}$は$n$次元ベクトル）からなる集合$S$によって、ベクトル空間$T$が構成されることを、

$$T = span(\overrightarrow{a_1}, \overrightarrow{a_2}, \cdots, \overrightarrow{a_k})$$

と表現する。

例：実数からなる 3 次元ベクトル空間$U = \mathbb{R}^3$を考える。Uに属する列ベクトルを要素とする集合$S = \left\{\begin{bmatrix}1\\2\\3\end{bmatrix}, \begin{bmatrix}1\\1\\4\end{bmatrix}, \begin{bmatrix}1\\4\\1\end{bmatrix}, \begin{bmatrix}1\\3\\2\end{bmatrix}\right\}$ から構成されるベクトル空間Tは$T = span\left(\begin{bmatrix}1\\2\\3\end{bmatrix}, \begin{bmatrix}1\\1\\4\end{bmatrix}, \begin{bmatrix}1\\4\\1\end{bmatrix}, \begin{bmatrix}1\\3\\2\end{bmatrix}\right) \subset \mathbb{R}^3$ である。

（注意：$\begin{bmatrix}1\\2\\3\end{bmatrix}, \begin{bmatrix}1\\1\\4\end{bmatrix}, \begin{bmatrix}1\\4\\1\end{bmatrix}, \begin{bmatrix}1\\3\\2\end{bmatrix}$は基底ではない。一次独立ではない。直交していない。）

2）連立一次方程式

2－1）連立一次方程式

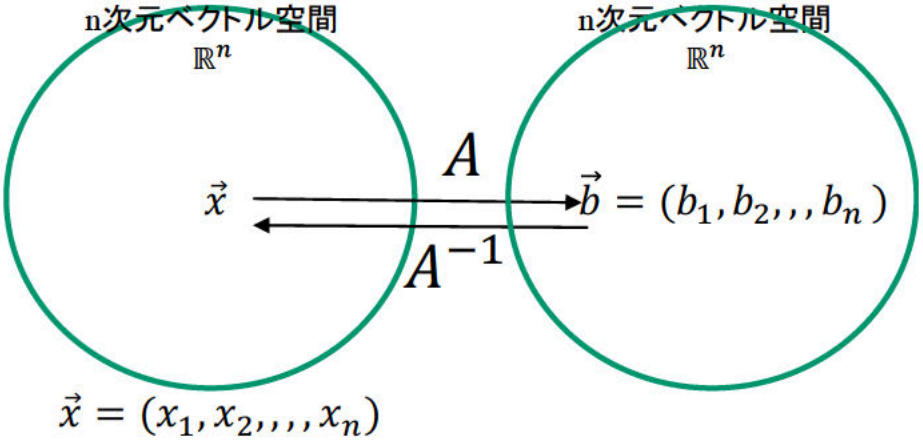
連立一次方程式を以下の行列で表現する。

$$Ax = b \quad （式2－1）$$

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & & \\ a_{31} & & & & \\ \vdots & & \ddots & & \\ a_{m1} & & & & a_{mn} \end{bmatrix} \quad x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \quad b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

Aは$m \times n$行列、xはn次元列ベクトル、bはm次元列ベクトルである。実数で議論する場合は、$x \in \mathbb{R}^n$、$b \in \mathbb{R}^m$であり、Aを写像と捉えて$A: \mathbb{R}^n \to \mathbb{R}^m$と表現する。

最も簡単な例は、$m = n$かつAがランクnの正方行列の場合である$(x \in \mathbb{R}^n, b \in \mathbb{R}^n, A: \mathbb{R}^n \to \mathbb{R}^n)$。これは、図のように$n \times n$行列$A$と$n$次元ベクトル$b$が与えられた時に、元となる$n$次元ベクトル$x$をuniqueに決定することである。



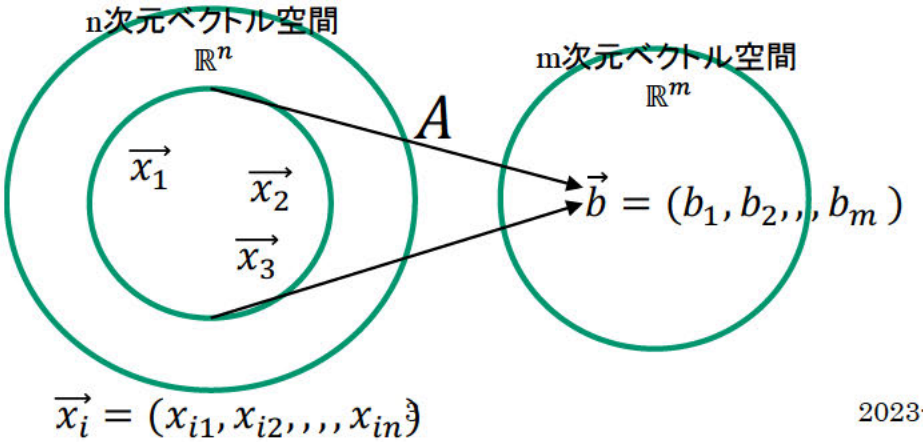
例：「普通」の連立一次方程式

$$x + y = 5$$
$$2x + 4y = 16 \quad （式2－2）$$

は、以下のように行列で表現できる。

$$\begin{bmatrix} 1 & 1 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 5 \\ 16 \end{bmatrix} \quad （式2－3）$$

拡張して、$m \neq n$（ここでは、$n > m$とする）の場合を議論する。式2－1は、下図のように、$m \times n$行列Aとm次元ベクトルbが与えられた時に、解xが含まれる集合を求めることを意味している。



例として、以下の連立一次方程式を考える。

$$x + y - 3z = 0$$
$$2x + y - 4z = -1$$
$$\begin{bmatrix}1 & 1 & -3\\ 2 & 1 & -4\end{bmatrix}\begin{bmatrix}x\\ y\\ z\end{bmatrix} = \begin{bmatrix}0\\ -1\end{bmatrix} \quad \text{（式２－４）}$$

未知数の数が方程式より多いため一般には解けない。しかし、例えば、x, yをzで表現することは可能である。すなわち、zをパラメータとしてx, yを表現できる。あるいは、xyz空間で、x,y,zの間にある関係（平面上にあるなど）を求められる。この求め方の概略を以下に示す。

$$\begin{bmatrix}1 & 1 & -3\\ 2 & 1 & -4\end{bmatrix}\begin{bmatrix}x\\ y\\ z\end{bmatrix} = \begin{bmatrix}0\\ -1\end{bmatrix} \quad \text{（式２－５）}$$

行列と結果を拡大行列で表現し、行基本変形によって、

$$\left[\begin{array}{ccc|c}1 & 1 & -3 & 0\\ 2 & 1 & -4 & -1\end{array}\right] \sim \left[\begin{array}{ccc|c}1 & 1 & -3 & 0\\ 0 & -1 & 2 & -1\end{array}\right] \sim \left[\begin{array}{ccc|c}1 & 0 & -1 & -1\\ 0 & -1 & 2 & -1\end{array}\right] \sim \left[\begin{array}{ccc|c}1 & 0 & -1 & -1\\ 0 & 1 & -2 & 1\end{array}\right] \quad \text{（式２－６）}$$

と変形する。元の方程式は、

$$\begin{bmatrix}1 & 0 & \mathbf{-1}\\ 0 & 1 & \mathbf{-2}\end{bmatrix}\begin{bmatrix}x\\ y\\ z\end{bmatrix} = \begin{bmatrix}-1\\ 1\end{bmatrix} \quad \text{（式２－７）}$$

に変形されたことになる。これより、

$$x = z - 1$$
$$y = 2z + 1 \quad \text{（式２－８）}$$

を得る。これは

$$\begin{bmatrix}x\\ y\\ z\end{bmatrix} = \begin{bmatrix}\mathbf{1}\\ \mathbf{2}\\ 1\end{bmatrix} z + \begin{bmatrix}-1\\ 1\\ 0\end{bmatrix} \quad \text{（式２－９）}$$

と表現できる。

以下の点に注意せよ。式２－７と式２－９の太字が対応している。式２－９の z の係数の(1 2 1)は後に述べる零空間の基底である。解が$\begin{bmatrix}1 & 0 & -1\\ 0 & 1 & -2\end{bmatrix}\begin{bmatrix}x\\ y\\ z\end{bmatrix} = \begin{bmatrix}0\\ 0\end{bmatrix}$ の解（一般解）と z=0 の特殊解$\begin{bmatrix}-1\\ 1\\ 0\end{bmatrix}$の和で表現されている。つまり、零空間の基底*z + 特殊解の形をしている。

２－２）連立一次方程式の解法

連立一次方程式の解法は多数ある。大きくは、直接法、反復法、共役勾配法等に分類され、計算効率（速度、メモリ量、並列計算等）で優劣がある。（http://ri2t.kyushu-u.ac.jp/~watanabe/RESERCH_/MANUSCRIPT/KOHO/GEPP/GEPP.pdf 「連立一次方程式の基礎知識（渡部善隆）」には多くの手法が整理されている。）

この資料で述べるガウス消去法(Gaussian Elimination)および、ガウスージョルダン消去法(Gauss-Jordan Elimination)は直接法である。

２－３）連立一次方程式と部分空間

$m \times n$の行列Aに対して、行空間（row space）、列空間（column space）、零空間（null space）、左零空間（left null space）の４つの部分空間（ベクトル加法、スカラー乗法の元に閉じている）が定義される。

３）行列の基本変形

３－１）基本変形

ある性質を保存したまま行列を変形することを基本変形と呼ぶ。ある性質とは、列ベクトルの独立性や階級の普遍性などである。変形することにより連立一次方程式を容易に解くことができる。基本変形には、行基本変形と列基本変形がある。ここでは、行基本変形を取り上げる。

以下の操作を行基本変形（Elementary row operations）と呼ぶ。

・行を入れ替える　Row switching

・行を定数倍する。Row multiplication

・定数倍した行を他の行に加算する。Row addition

この資料では、以下の記法を用いる。

$R1 \to r2\ R2 \to r1$　　旧１行目を新２行目とし、旧２行目を新１行目とする。

$R1 + R2 \times 2 \to r1$　　旧１行目と２倍した旧２行目を加えて新１行目とする

行基本変形は、左から変換行列（これを基本行列とも呼ぶ）をかけていることになる。

$$Ax = b \ \rightarrow \ LAx = Lb \quad （式３－１）$$

（一方、列基本変形は、xを行ベクトルとした方程式$(x_1, x_2, , , x_n)A = (b_1, b_2, , , , b_n)$に、右から変換行列をかける。行基本変形を左基本変形、列基本変形を右基本変形と呼ぶこともある。）

3x3 の行列を用いて例示する。今、目的の連立一次方程式が以下のように与えられたとする。

$$Ax = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} x \ = \ b = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} \quad （式３－２）$$

例１：２行目と３行目を入れ替える　　$R1 \to r1 \quad R2 \to r3 \quad R3 \to r2$

この変換に対応する変換行列Lは、$L = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$　である。

左辺　$$LAx = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} Ax = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} x = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{31} & a_{32} & a_{33} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} x$$

右辺　$$Lb = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} b = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_3 \\ b_2 \end{bmatrix}$$

これにより、$Ax = b$は、

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{31} & a_{32} & a_{33} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} x = \begin{bmatrix} b_1 \\ b_3 \\ b_2 \end{bmatrix} \quad （式３－３）$$

に変換される。式３－３は式３－２と内容が同一であることに注意する。

例２：１行目から２行目を引いて２行目とする。１行目から３行目を引いて３行目とする。

$R1 \to r1 \quad R1 - R2 \to r2 \quad R1 - R3 \to r3$

左辺　$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{bmatrix} Ax = \begin{bmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} x = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{11} - a_{21} & a_{12} - a_{22} & a_{13} - a_{23} \\ a_{11} - a_{31} & a_{12} - a_{32} & a_{13} - a_{33} \end{bmatrix} x$$

右辺 $\begin{bmatrix}1 & 0 & 0\\ 1 & -1 & 0\\ 1 & 0 & -1\end{bmatrix} b = \begin{bmatrix}1 & 0 & 0\\ 1 & -1 & 0\\ 1 & 0 & -1\end{bmatrix}\begin{bmatrix}b_1\\ b_2\\ b_3\end{bmatrix} = \begin{bmatrix}b_1\\ b_1-b_2\\ b_1-b_3\end{bmatrix}$

これにより、$Ax = b$は、

$$\begin{bmatrix}a_{11} & a_{12} & a_{13}\\ a_{11}-a_{21} & a_{12}-a_{22} & a_{13}-a_{23}\\ a_{11}-a_{31} & a_{12}-a_{32} & a_{13}-a_{33}\end{bmatrix} x = \begin{bmatrix}b_1\\ b_1-b_2\\ b_1-b_3\end{bmatrix} \quad (式３－４)$$

に変換される。式３－４も式３－２と内容が同一であることに注意する。

３－２）拡大行列（Augmented Matrix）

行列の行基本変形では、Aとbを同時に変形する。これを表現しやくするために、$[A|b]$の形式をした Augmented Matrix を使うことが多い。例えば、例１では、

$\begin{bmatrix}1 & 0 & 0\\ 0 & 0 & 1\\ 0 & 1 & 0\end{bmatrix}\left[\begin{array}{ccc|c}a_{11} & a_{12} & a_{13} & b_1\\ a_{21} & a_{22} & a_{23} & b_3\\ a_{31} & a_{32} & a_{33} & b_2\end{array}\right] = \left[\begin{array}{ccc|c}a_{11} & a_{12} & a_{13} & b_1\\ a_{31} & a_{32} & a_{33} & b_3\\ a_{21} & a_{22} & a_{23} & b_2\end{array}\right]$ である。

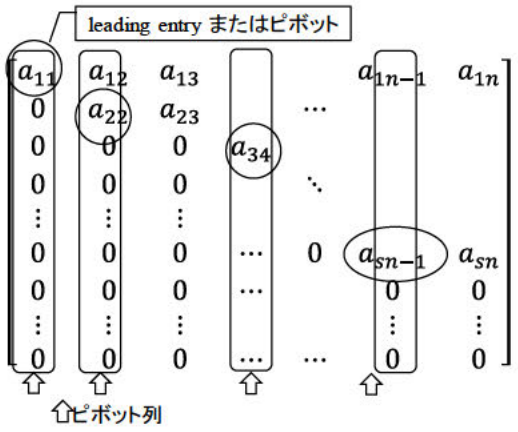
３－３）REF と RREF

基本変形を施し、下三角が 0 となるように変形した形式を Row Echelon Form (REF)とよぶ。REF は以下の特徴を持つ。

・すべて０の行は行列の下部に存在する

・非０の行の一番左の非０の項（leading entry、主成分、あるいはピボット）は、その上にある行の leading entry の必ず右側に存在する。

・ピボット列は一次独立である。



REF をさらに変形し、以下の形式になるように変形したものを Reduced Row Echelon Form (RREF)と呼ぶ。

$$\begin{bmatrix}1 & 0 & & 0 & & & a_{1n-1} & a_{1n}\\ 0 & 1 & & 0 & & \cdots & & \\ 0 & 0 & 0 & 1 & & & & \\ & & & & \ddots & & & \\ \vdots & \vdots & \vdots & \vdots & & & & \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & a_{sn}\\ 0 & 0 & 0 & 0 & \cdots & & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & & & \vdots & \vdots\\ 0 & 0 & 0 & 0 & \cdots & \cdots & 0 & 0\end{bmatrix}$$

RREF は、REF に加えて以下の特徴を持つ。

・leading entry は 1 である。

・leading entry を持つ列（ピボット列）は、leading entry 以外は０である。

・RREF は行列に対して一意に決定される。これ以上基本変形できない。

３－４）行基本変形の性質

・行基本変形は可逆である。すなわち、変換行列（基本行列）Lは正則行列である（逆行列が存在する）

$$A_0x=b_0 \underset{\substack{A_0=A\\ b_0=b}}{} \overset{L_1}{\underset{(L_1)^{-1}}{\rightleftarrows}} A_1x=b_1 \overset{L_2}{\underset{(L_2)^{-1}}{\rightleftarrows}} A_2x=b_2 \overset{L_3}{\underset{(L_3)^{-1}}{\rightleftarrows}} \cdots \rightarrow A_{ref}x=b_{ref} \overset{L_{\mathrm{rref}}}{\underset{(L_{rref})^{-1}}{\rightleftarrows}} A_{rref}x=b_{rref}$$

$$L_1A_0x=A_1x \;=\; L_1b_0=b_1$$
$$(L_1)^{-1}A_1x=(L_1)^{-1}L_1A_0x=A_0x \;=\; (L_1)^{-1}b_1=(L_1)^{-1}L_1b_0=b_0$$

・**行**基本変形により、**列**ベクトルの一次独立性は保存される。「行基本変形は列ベクトルの線形関係を保つ」とも表現する。８）列空間の「８－６）方法２の補足説明」を参照。

・leading entry（ピボット）の数が行列のランクとなる。

・列の入れ替えを行う方法もあるが後で列を再度入れ替える必要がある。この資料では列の入れ替えは行わないものとする。

３－５）例

（１）

$$A=\begin{bmatrix}1&2&3&-4\\2&-3&4&1\\1&1&3&5\\3&-1&7&-3\end{bmatrix}\sim\underset{\text{REF（の一つ）}}{\begin{bmatrix}3&6&9&-12\\0&6&2&0\\0&0&1&27\\0&0&0&0\end{bmatrix}}\sim\underset{\text{RREF}}{\begin{bmatrix}1&0&0&-67\\0&1&0&-9\\0&0&1&27\\0&0&0&0\end{bmatrix}}$$ （式３－５）

（２）

$$A=\begin{bmatrix}2&4&2&4\\4&8&1&5\\1&2&1&2\end{bmatrix}\sim\underset{\text{REF（の一つ）}}{\begin{bmatrix}2&4&2&4\\0&0&-3&-3\\0&0&0&0\end{bmatrix}}\sim\underset{\text{RREF}}{\begin{bmatrix}1&2&0&1\\0&0&1&1\\0&0&0&0\end{bmatrix}}$$ （式３－６）

4）ガウス消去法、ガウスージョルダン消去法

連立一次方程式の解法の直接法に属するガウス消去法、ガウスージョルダン消去法を述べる。これらは原理的には、中学高校で行ってきたものと同じと考えよい。

4－1）ガウス消去法

ガウス消去法は、前進消去フェーズと後退代入フェーズがある。

1）前進消去（Forward Elimination）フェーズ

行列の行基本変形を繰り返し適用し、REF 形式に変形する。

途中でピボットが 0 となった場合には、行を入れ替えて操作を続ける。

2）後退代入（Backward Substitution）フェーズ

前進消去フェーズで求められた REF が

$$Ax\sim\begin{bmatrix} a_{11} & a_{12} & a_{13} & & & a_{1n-1} & a_{1n} \\ 0 & a_{22} & a_{23} & \cdots & & & \\ 0 & 0 & a_{33} & & & & \\ 0 & 0 & 0 & \ddots & & & \\ \vdots & \vdots & \vdots & & & & \\ 0 & 0 & 0 & \cdots & 0 & a_{sn-1} & a_{sn} \\ 0 & 0 & 0 & \cdots & & 0 & 0 \\ \vdots & \vdots & \vdots & & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \cdots & 0 & 0 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = b' = \begin{bmatrix} b'_1 \\ b'_2 \\ \vdots \\ b'_s \end{bmatrix} \quad \text{（式４－１－１）}$$

であるとき、最下部の非 0 の行よりx_iを解く。この結果を使って、さらにその次の非 0 の行を利用して、全x_iを求める。

4－2）ガウスージョルダン消去法

REF からさらに行基本変形を繰り返し適用し、RREF に変形する。RREF では、ピボット列はピボットの係数が 1 でありそれ以外は 0 であるので、全てのx_iが容易に求められる。

4－3）例

4－3－1）ガウス消去法の例

以下では、行列が正方行列である簡単な例を扱う。

$A=\begin{bmatrix} 1 & 4 & 3 \\ 1 & 1 & 5 \\ 1 & 1 & 1 \end{bmatrix}$、$b=\begin{bmatrix} b_1 \\ b_2 \\ b_2 \end{bmatrix}$　を例とする。

ステップ 0）準備

Augmented Matrix は以下である。

$$[A|b]=\left[\begin{array}{ccc|c} 1 & 4 & 3 & b_1 \\ 1 & 1 & 5 & b_2 \\ 1 & 1 & 1 & b_3 \end{array}\right] \quad \text{（式４－３－１）}$$

ステップ G1）$R1\to r1 \quad R1-R2\to r2 \quad R1-R3\to r3$　　（前進消去）

（ガウス消去法の行基本変形）

$$\begin{bmatrix}1&0&0\\1&-1&0\\1&0&-1\end{bmatrix}\left[\begin{array}{ccc|c}1&4&3&b_1\\1&1&5&b_2\\1&1&1&b_3\end{array}\right]=\left[\begin{array}{ccc|c}1&4&3&b_1\\0&3&-2&b_1-b_2\\0&3&2&b_1-b_3\end{array}\right]$$ （式４－３－２）

（対応する連立一次方程式の操作）

$$\begin{bmatrix}1&0&0\\1&-1&0\\1&0&-1\end{bmatrix}Ax=\begin{bmatrix}1&0&0\\1&-1&0\\1&0&-1\end{bmatrix}b$$

左辺$=\begin{bmatrix}1&0&0\\1&-1&0\\1&0&-1\end{bmatrix}Ax=\begin{bmatrix}1&0&0\\1&-1&0\\1&0&-1\end{bmatrix}\begin{bmatrix}1&4&3\\1&1&5\\1&1&1\end{bmatrix}x=\begin{bmatrix}1&4&3\\0&3&-2\\0&3&2\end{bmatrix}x$

右辺$=\begin{bmatrix}1&0&0\\1&-1&0\\1&0&-1\end{bmatrix}b=\begin{bmatrix}b_1\\b_1-b_2\\b_1-b_3\end{bmatrix}$

$$\therefore\begin{bmatrix}1&4&3\\0&3&-2\\0&3&2\end{bmatrix}x=\begin{bmatrix}b_1\\b_1-b_2\\b_1-b_3\end{bmatrix}$$ （式４－３－３）

ステップ G2）$R1\to r1\quad R2\to r2\quad R3-R2\to r3$ （前進消去）

（ガウス消去法の行基本変形）

$$\begin{bmatrix}1&0&0\\0&1&0\\0&-1&1\end{bmatrix}\left[\begin{array}{ccc|c}1&4&3&b_1\\0&3&-2&b_1-b_2\\0&3&2&b_1-b_3\end{array}\right]=\left[\begin{array}{ccc|c}1&4&3&b_1\\0&3&-2&b_1-b_2\\0&0&4&b_2-b_3\end{array}\right]$$ （式４－３－４）

（対応する連立一次方程式の操作）

$$\begin{bmatrix}1&0&0\\0&1&0\\0&-1&1\end{bmatrix}\begin{bmatrix}1&4&3\\0&3&-2\\0&3&2\end{bmatrix}x=\begin{bmatrix}1&0&0\\0&1&0\\0&-1&1\end{bmatrix}\begin{bmatrix}b_1\\b_1-b_2\\b_1-b_3\end{bmatrix}$$

左辺$=\begin{bmatrix}1&0&0\\0&1&0\\0&-1&1\end{bmatrix}\begin{bmatrix}1&4&3\\0&3&-2\\0&3&2\end{bmatrix}x=\begin{bmatrix}1&4&3\\0&3&-2\\0&0&4\end{bmatrix}x$

右辺$=\begin{bmatrix}1&0&0\\0&1&0\\0&-1&1\end{bmatrix}\begin{bmatrix}b_1\\b_1-b_2\\b_1-b_3\end{bmatrix}=\begin{bmatrix}b_1\\b_1-b_2\\b_2-b_3\end{bmatrix}$

$$\therefore\begin{bmatrix}1&4&3\\0&3&-2\\0&0&4\end{bmatrix}x=\begin{bmatrix}b_1\\b_1-b_2\\b_2-b_3\end{bmatrix}$$ （式４－３－５）

ステップ G3）最下位行から解を求める。（後退代入）

$$\begin{bmatrix}1&4&3\\0&3&-2\\0&0&4\end{bmatrix}\begin{bmatrix}x_1\\x_2\\x_3\end{bmatrix}=\begin{bmatrix}b_1\\b_1-b_2\\b_2-b_3\end{bmatrix}$$ （式４－３－６）

最終行より、$4x_3=b_2-b_3$ であり、x_3が求められる。次に、第２行に入れて、$3x_2-2x_3=3x_2-\frac{b_2-b_3}{2}=b_1-b_2$ を解いてx_2を求める。最後に、x_3，x_2を第１行に入れてx_1を求める。

４－３－２）ガウスージョルダン消去法の例

ガウスージョルダン消去法は、最終的には、

$$\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\begin{bmatrix}x_1\\x_2\\x_3\end{bmatrix}=b' \quad (式4-3-7)$$

のような RREF にして、x_1, x_2, x_3を求める。ガウス消去法では下三角を消去するのに対して、ガウスージョルダンは、上三角も消去する。消去する順序は任意である。以下では、ガウス消去法の例の式４－３－６から続けて行う。すなわち、

$$\begin{bmatrix}1&4&3\\0&3&-2\\0&0&4\end{bmatrix}\begin{bmatrix}x_1\\x_2\\x_3\end{bmatrix}=\begin{bmatrix}b_1\\b_1-b_2\\b_2-b_3\end{bmatrix} \quad (式4-3-8)$$

からスタートする。

ステップ GJ1）$R1\to r1 \quad R2\times\frac{1}{3}\to r2 \quad R3\times\frac{1}{4}\to r3$

（ガウスージョルダン消去法の行基本変形）

$$\begin{bmatrix}1&0&0\\0&\frac{1}{3}&0\\0&0&\frac{1}{4}\end{bmatrix}\left[\begin{array}{ccc|c}1&4&3&b_1\\0&3&-2&b_1-b_2\\0&0&4&b_2-b_3\end{array}\right]=\left[\begin{array}{ccc|c}1&4&3&b_1\\0&1&-\frac{2}{3}&\frac{b_1-b_2}{3}\\0&0&1&\frac{b_2-b_3}{4}\end{array}\right]$$

（対応する連立一次方程式の操作）

$$\begin{bmatrix}1&0&0\\0&\frac{1}{3}&0\\0&0&\frac{1}{4}\end{bmatrix}\begin{bmatrix}1&4&3\\0&3&-2\\0&0&4\end{bmatrix}x=\begin{bmatrix}1&0&0\\0&\frac{1}{3}&0\\0&0&\frac{1}{4}\end{bmatrix}\begin{bmatrix}b_1\\b_1-b_2\\b_2-b_3\end{bmatrix}$$

$$\text{左辺}=\begin{bmatrix}1&0&0\\0&\frac{1}{3}&0\\0&0&\frac{1}{4}\end{bmatrix}\begin{bmatrix}1&4&3\\0&3&-2\\0&0&4\end{bmatrix}x=\begin{bmatrix}1&4&3\\0&1&-\frac{2}{3}\\0&0&1\end{bmatrix}x$$

$$\text{右辺}=\begin{bmatrix}1&0&0\\0&\frac{1}{3}&0\\0&0&\frac{1}{4}\end{bmatrix}\begin{bmatrix}b_1\\b_1-b_2\\b_2-b_3\end{bmatrix}=\begin{bmatrix}b_1\\\frac{b_1-b_2}{3}\\\frac{b_2-b_3}{4}\end{bmatrix}$$

$$\therefore\begin{bmatrix}1&4&3\\0&1&-\frac{2}{3}\\0&0&1\end{bmatrix}x=\begin{bmatrix}b_1\\\frac{b_1-b_2}{3}\\\frac{b_2-b_3}{4}\end{bmatrix}$$

ステップ GJ2）$R1-R2\times4\to r1 \quad R2+\frac{2}{3}R3\to r2 \quad R3\to r3$

（ガウスージョルダン消去法の行基本変形）

$$\begin{bmatrix}1&-4&0\\0&1&\frac{2}{3}\\0&0&1\end{bmatrix}\left[\begin{array}{ccc|c}1&4&3&b_1\\0&1&-\frac{2}{3}&\frac{b_1-b_2}{3}\\0&0&1&\frac{b_2-b_3}{4}\end{array}\right]=\left[\begin{array}{ccc|c}1&0&\frac{17}{3}&\frac{-b_1+4b_2}{3}\\0&1&0&\frac{2b_1-b_2-b_3}{6}\\0&0&1&\frac{b_2-b_3}{4}\end{array}\right]$$

$$b_1-\frac{b_1-b_2}{3}\times4=\frac{3b_1-4b_1+4b_2}{3}=\frac{-b_1+4b_2}{3}$$

$$\frac{b_1-b_2}{3}+\frac{b_2-b_3}{4}\times\frac{2}{3}=\frac{2b_1-2b_2+b_2-b_3}{6}=\frac{2b_1-b_2-b_3}{6}$$

（対応する連立一次方程式の操作）

$$\begin{bmatrix}1 & -4 & 0\\ 0 & 1 & \frac{2}{3}\\ 0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 4 & 3\\ 0 & 1 & -\frac{2}{3}\\ 0 & 0 & 1\end{bmatrix}x=\begin{bmatrix}1 & -4 & 0\\ 0 & 1 & \frac{2}{3}\\ 0 & 0 & 1\end{bmatrix}\begin{bmatrix}b_1\\ \frac{b_1-b_2}{3}\\ \frac{b_2-b_3}{4}\end{bmatrix}$$

左辺$=\begin{bmatrix}1 & -4 & 0\\ 0 & 1 & \frac{2}{3}\\ 0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 4 & 3\\ 0 & 1 & -\frac{2}{3}\\ 0 & 0 & 1\end{bmatrix}x=\begin{bmatrix}1 & 0 & \frac{17}{3}\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}x$

右辺$=\begin{bmatrix}1 & -4 & 0\\ 0 & 1 & \frac{2}{3}\\ 0 & 0 & 1\end{bmatrix}\begin{bmatrix}b_1\\ \frac{b_1-b_2}{3}\\ \frac{b_2-b_3}{4}\end{bmatrix}=\begin{bmatrix}\frac{-b_1+4b_2}{3}\\ \frac{2b_1-b_2-b_3}{6}\\ \frac{b_2-b_3}{4}\end{bmatrix}$

$$\therefore\begin{bmatrix}1 & 0 & \frac{17}{3}\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}x=\begin{bmatrix}\frac{-b_1+4b_2}{3}\\ \frac{2b_1-b_2-b_3}{6}\\ \frac{b_2-b_3}{4}\end{bmatrix}$$

ステップ GJ3）$R1-R3\times\frac{17}{3}\to r1\quad R2\to r2\quad R3\to r3$

（ガウスージョルダン消去法の行基本変形）

$$\begin{bmatrix}1 & 0 & -\frac{17}{3}\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}\left[\begin{array}{ccc|c}1 & 0 & \frac{17}{3} & \frac{-b_1+4b_2}{3}\\ 0 & 1 & 0 & \frac{2b_1-b_2-b_3}{6}\\ 0 & 0 & 1 & \frac{b_2-b_3}{4}\end{array}\right]=\left[\begin{array}{ccc|c}1 & 0 & 0 & \frac{-4b_1-b_2+17b_3}{12}\\ 0 & 1 & 0 & \frac{2b_1-b_2-b_3}{6}\\ 0 & 0 & 1 & \frac{b_2-b_3}{4}\end{array}\right]$$

$$\frac{-b_1+4b_2}{3}-\frac{b_2-b_3}{4}\times\frac{17}{3}=\frac{-4b_1+16b_2-17b_2+17b_3}{12}=\frac{-4b_1-b_2+17b_3}{12}$$

（対応する連立一次方程式の操作）

$$\begin{bmatrix}1 & 0 & -\frac{17}{3}\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & \frac{17}{3}\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}x=\begin{bmatrix}1 & 0 & -\frac{17}{3}\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}\begin{bmatrix}\frac{-b_1+4b_2}{3}\\ \frac{2b_1-b_2-b_3}{6}\\ \frac{b_2-b_3}{4}\end{bmatrix}$$

左辺$=\begin{bmatrix}1 & 0 & -\frac{17}{3}\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & \frac{17}{3}\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}x=\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}x$

右辺$=\begin{bmatrix}1 & 0 & -\frac{17}{3}\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}\begin{bmatrix}\frac{-b_1+4b_2}{3}\\ \frac{2b_1-b_2-b_3}{6}\\ \frac{b_2-b_3}{4}\end{bmatrix}=\begin{bmatrix}\frac{-4b_1-b_2+17b_3}{12}\\ \frac{2b_1-b_2-b_3}{6}\\ \frac{b_2-b_3}{4}\end{bmatrix}$

$$\therefore\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}x=\begin{bmatrix}\frac{-4b_1-b_2+17b_3}{12}\\ \frac{2b_1-b_2-b_3}{6}\\ \frac{b_2-b_3}{4}\end{bmatrix}\qquad（式4-3-9）$$

以上より、$x_1 = \frac{-4b_1-b_2+17b_3}{12}$　　$x_2 = \frac{2b_1-b_2-b_3}{6}$　$x_3 = \frac{b_2-b_3}{4}$　となる。

４－３－３）ピボット操作に関する処理が必要な例

ピボットが０となると変形ができなくなる。その場合は、行を入れ替える。

$A = \begin{bmatrix}1 & 4 & 3\\1 & 4 & 2\\1 & 1 & 1\end{bmatrix}$、$b = \begin{bmatrix}b_1\\b_2\\b_2\end{bmatrix}$　を例として挙げる。

ステップ Gp1）$R1 \to r1$　$R1 - R2 \to r2$　$R1 - R3 \to r3$　　（前進変形）

（ガウス消去法の行基本変形）

$$\begin{bmatrix}1 & 0 & 0\\1 & -1 & 0\\1 & 0 & -1\end{bmatrix}\left[\begin{array}{ccc|c}1 & 4 & 3 & b_1\\1 & 4 & 2 & b_2\\1 & 1 & 1 & b_3\end{array}\right] = \left[\begin{array}{ccc|c}1 & 4 & 3 & b_1\\0 & 0 & 1 & b_1 - b_2\\0 & 3 & 2 & b_1 - b_3\end{array}\right]$$　（式４－３－１０）

（対応する連立一次方程式の操作）

$$\begin{bmatrix}1 & 0 & 0\\1 & -1 & 0\\1 & 0 & -1\end{bmatrix}Ax = \begin{bmatrix}1 & 0 & 0\\1 & -1 & 0\\1 & 0 & -1\end{bmatrix}b$$

$$\text{左辺}= \begin{bmatrix}1 & 0 & 0\\1 & -1 & 0\\1 & 0 & -1\end{bmatrix}Ax = \begin{bmatrix}1 & 0 & 0\\1 & -1 & 0\\1 & 0 & -1\end{bmatrix}\begin{bmatrix}1 & 4 & 3\\1 & 4 & 2\\1 & 1 & 1\end{bmatrix}x = \begin{bmatrix}1 & 4 & 3\\0 & 0 & 1\\0 & 3 & 2\end{bmatrix}x$$

$$\text{右辺}= \begin{bmatrix}1 & 0 & 0\\1 & -1 & 0\\1 & 0 & -1\end{bmatrix}b = \begin{bmatrix}b_1\\b_1 - b_2\\b_1 - b_3\end{bmatrix}$$

$$\therefore \begin{bmatrix}1 & 4 & 3\\0 & \mathbf{0} & 1\\0 & 3 & 2\end{bmatrix}x = \begin{bmatrix}b_1\\b_1 - b_2\\b_1 - b_3\end{bmatrix}$$　（式４－３－１１）

ピボットとする第２行第２列が０となっているので、２行目と３行目を入れ替える。

ステップ Gp2）$R1 \to r1$　$R2 \to r3$　$R3 \to r2$　（前進変形）

（ガウス消去法の行基本変形）

$$\begin{bmatrix}1 & 0 & 0\\0 & 0 & 1\\0 & 1 & 0\end{bmatrix}\left[\begin{array}{ccc|c}1 & 4 & 3 & b_1\\0 & 0 & 1 & b_1 - b_2\\0 & 3 & 2 & b_1 - b_3\end{array}\right] = \left[\begin{array}{ccc|c}1 & 4 & 3 & b_1\\0 & 3 & 2 & b_1 - b_3\\0 & 0 & 1 & b_1 - b_2\end{array}\right]$$　（式４－３－１２）

（対応する連立一次方程式の操作）

$$\begin{bmatrix}1 & 0 & 0\\0 & 0 & 1\\0 & 1 & 0\end{bmatrix}\begin{bmatrix}1 & 4 & 3\\0 & 0 & 1\\0 & 3 & 2\end{bmatrix}x = \begin{bmatrix}1 & 0 & 0\\0 & 0 & 1\\0 & 1 & 0\end{bmatrix}\begin{bmatrix}b_1\\b_1 - b_2\\b_1 - b_3\end{bmatrix}$$

$$\text{左辺}= \begin{bmatrix}1 & 0 & 0\\0 & 0 & 1\\0 & 1 & 0\end{bmatrix}\begin{bmatrix}1 & 4 & 3\\0 & 0 & 1\\0 & 3 & 2\end{bmatrix}x = \begin{bmatrix}1 & 4 & 3\\0 & 3 & 2\\0 & 0 & 1\end{bmatrix}x$$

右辺= $\begin{bmatrix}1 & 0 & 0\\0 & 0 & 1\\0 & 1 & 0\end{bmatrix}\begin{bmatrix}b_1\\b_1-b_2\\b_1-b_3\end{bmatrix}=\begin{bmatrix}b_1\\b_1-b_3\\b_1-b_2\end{bmatrix}$

$\therefore \begin{bmatrix}1 & 4 & 3\\0 & 3 & 2\\0 & 0 & 1\end{bmatrix}x=\begin{bmatrix}b_1\\b_1-b_3\\b_1-b_2\end{bmatrix}$　　（式４－３－１３）

ステップ Gp3）式４－３－１３より、

$x_3=b_1-b_2$　　$3x_2+2x_3=b_1-b_3$　　$x_1+4x_2+3x_3=b_1$を解いて、x_1，x_2，x_3を求める。

（$x_1=\frac{-2b_1+b_2+4b_3}{3}$　　$x_2=\frac{-b_1+2b_2-b_3}{3}$　$x_3=b_1-b_2$）

さらに、ガウスージョルダン消去法を用いると以下となる。

ステップ GJp1）$R1-R3\times 3\rightarrow r1$　$R2-R3\times 2\rightarrow r2$　$R3\rightarrow r3$

（ガウスージョルダン消去法の行基本変形）

$\left[\begin{array}{ccc|c}1 & 0 & -3 & \\0 & 1 & -2 & \\0 & 0 & 1 & \end{array}\right]\left[\begin{array}{ccc|c}1 & 4 & 3 & b_1\\0 & 3 & 2 & b_1-b_3\\0 & 0 & 1 & b_1-b_2\end{array}\right]=\left[\begin{array}{ccc|c}1 & 4 & 0 & b_1-3b_1+3b_2\\0 & 3 & 0 & b_1-b_3-2b_1+2b_2\\0 & 0 & 1 & b_1-b_2\end{array}\right]=\left[\begin{array}{ccc|c}1 & 4 & 0 & -2b_1+3b_2\\0 & 3 & 0 & -b_1+2b_2-b_3\\0 & 0 & 1 & b_1-b_2\end{array}\right]$

（対応する連立一次方程式の操作）

$\begin{bmatrix}1 & 0 & -3\\0 & 1 & -2\\0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 4 & 3\\0 & 3 & 2\\0 & 0 & 1\end{bmatrix}x=\begin{bmatrix}1 & 0 & -3\\0 & 1 & -2\\0 & 0 & 1\end{bmatrix}\begin{bmatrix}b_1\\b_1-b_3\\b_1-b_2\end{bmatrix}$

左辺= $\begin{bmatrix}1 & 0 & -3\\0 & 1 & -2\\0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 4 & 3\\0 & 3 & 2\\0 & 0 & 1\end{bmatrix}x=\begin{bmatrix}1 & 4 & 0\\0 & 3 & 0\\0 & 0 & 1\end{bmatrix}x$

右辺= $\begin{bmatrix}1 & 0 & -3\\0 & 1 & -2\\0 & 0 & 1\end{bmatrix}\begin{bmatrix}b_1\\b_1-b_3\\b_1-b_2\end{bmatrix}=\begin{bmatrix}-2b_1+3b_2\\-b_1+2b_2-b_3\\b_1-b_2\end{bmatrix}$

$\therefore \begin{bmatrix}1 & 4 & 0\\0 & 3 & 0\\0 & 0 & 1\end{bmatrix}x=\begin{bmatrix}-2b_1+3b_2\\-b_1+2b_2-b_3\\b_1-b_2\end{bmatrix}$

ステップ GJp2）$R1\rightarrow r1$　$R2\times\frac{1}{3}\rightarrow r2$　$R3\rightarrow r3$

（ガウスージョルダン消去法の行基本変形）

$\left[\begin{array}{ccc|c}1 & 0 & 0 & \\0 & \frac{1}{3} & 0 & \\0 & 0 & 1 & \end{array}\right]\left[\begin{array}{ccc|c}1 & 4 & 0 & -2b_1+3b_2\\0 & 3 & 0 & -b_1+2b_2-b_3\\0 & 0 & 1 & b_1-b_2\end{array}\right]=\left[\begin{array}{ccc|c}1 & 1 & 0 & -2b_1+3b_2\\0 & 1 & 0 & \frac{-b_1+2b_2-b_3}{3}\\0 & 0 & 1 & b_1-b_2\end{array}\right]$

（対応する連立一次方程式の操作）

$$\begin{bmatrix}1&0&0\\0&\frac{1}{3}&0\\0&0&1\end{bmatrix}\begin{bmatrix}1&4&0\\0&3&0\\0&0&1\end{bmatrix}x=\begin{bmatrix}1&0&0\\0&\frac{1}{3}&0\\0&0&1\end{bmatrix}\begin{bmatrix}-2b_1+3b_2\\-b_1+2b_2-b_3\\b_1-b_2\end{bmatrix}$$

左辺$=\begin{bmatrix}1&0&0\\0&\frac{1}{3}&0\\0&0&1\end{bmatrix}\begin{bmatrix}1&4&0\\0&3&0\\0&0&1\end{bmatrix}x=\begin{bmatrix}1&4&0\\0&1&0\\0&0&1\end{bmatrix}x$

右辺$=\begin{bmatrix}1&0&0\\0&\frac{1}{3}&0\\0&0&1\end{bmatrix}\begin{bmatrix}-2b_1+3b_2\\-b_1+2b_2-b_3\\b_1-b_2\end{bmatrix}=\begin{bmatrix}-2b_1+3b_2\\\frac{-b_1+2b_2-b_3}{3}\\b_1-b_2\end{bmatrix}$

$$\therefore\begin{bmatrix}1&4&0\\0&1&0\\0&0&1\end{bmatrix}x=\begin{bmatrix}-2b_1+3b_2\\\frac{-b_1+2b_2-b_3}{3}\\b_1-b_2\end{bmatrix}$$

ステップ GJp3）$R1-4\times R2\to r1\quad R2\to r2\quad R3\to r3$

（ガウスージョルダン消去法の行基本変形）

$$\begin{bmatrix}1&-4&0\\0&1&0\\0&0&1\end{bmatrix}\left[\begin{array}{ccc|c}1&4&0&-2b_1+3b_2\\0&1&0&\frac{-b_1+2b_2-b_3}{3}\\0&0&1&b_1-b_2\end{array}\right]=\left[\begin{array}{ccc|c}1&0&0&\frac{-2b_1+b_2+4b_3}{3}\\0&1&0&\frac{-b_1+2b_2-b_3}{3}\\0&0&1&b_1-b_2\end{array}\right]$$

$$-2b_1+3b_2-\frac{-4b_1+8b_2-4b_3}{3}=\frac{-6b_1+9b_2+4b_1-8b_2+4b_3}{3}=\frac{-2b_1+b_2+4b_3}{3}$$

（対応する連立一次方程式の操作）

$$\begin{bmatrix}1&-4&0\\0&1&0\\0&0&1\end{bmatrix}\begin{bmatrix}1&4&0\\0&1&0\\0&0&1\end{bmatrix}x=\begin{bmatrix}1&-4&0\\0&1&0\\0&0&1\end{bmatrix}\begin{bmatrix}-2b_1+2b_2\\\frac{-b_1+2b_2-b_3}{3}\\b_1-b_2\end{bmatrix}$$

左辺$=\begin{bmatrix}1&-4&0\\0&1&0\\0&0&1\end{bmatrix}\begin{bmatrix}1&4&0\\0&1&0\\0&0&1\end{bmatrix}x=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}x$

右辺$=\begin{bmatrix}1&-4&0\\0&1&0\\0&0&1\end{bmatrix}\begin{bmatrix}-2b_1+2b_2\\\frac{-b_1+2b_2-b_3}{3}\\b_1-b_2\end{bmatrix}=\begin{bmatrix}\frac{-2b_1+b_2+4b_3}{3}\\\frac{-b_1+2b_2-b_3}{3}\\b_1-b_2\end{bmatrix}$

$$\therefore\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}x=\begin{bmatrix}\frac{-2b_1+b_2+4b_3}{3}\\\frac{-b_1+2b_2-b_3}{3}\\b_1-b_2\end{bmatrix}$$

以上より、$x_1=\frac{-2b_1+b_2+4b_3}{3}\qquad x_2=\frac{-b_1+2b_2-b_3}{3}\quad x_3=b_1-b_2$　と求められる。

４－３－４）正方行列ではないなどの例

ここでは、行列Aが$m\times n$行列の場合$(m<n)$　の場合について述べる。Aが$n\times n$の正方行列であってもAのランクがnより小さいとき、すなわち$rand\ A<n$でも同様な状況が生じる。

例として、以下を考える。

$$B=\begin{bmatrix}2&4&2&2\\4&10&3&3\\2&6&1&1\\3&7&1&4\end{bmatrix}\qquad x=\begin{bmatrix}x_1\\x_2\\x_3\\x_4\end{bmatrix}\qquad b=\begin{bmatrix}8\\17\\9\\11\end{bmatrix}\qquad (式４－３－１４)$$

ガウス消去法前進消去により以下を得る。

$$[B|b]=\left[\begin{array}{cccc|c}2&4&2&2&8\\4&10&3&3&17\\2&6&1&1&9\\3&7&1&4&11\end{array}\right]\sim\left[\begin{array}{cccc|c}1&2&1&1&4\\0&2&-1&-1&1\\0&0&1&-1&1\\0&0&0&0&0\end{array}\right]\qquad (式４－３－１５)$$

$Bx=b$ に戻す。

$$\begin{bmatrix}1&2&1&1\\0&2&-1&-1\\0&0&1&-1\\0&0&0&0\end{bmatrix}\begin{bmatrix}x_1\\x_2\\x_3\\x_4\end{bmatrix}=\begin{bmatrix}4\\1\\1\\0\end{bmatrix}\qquad (式４－３－１６)$$

これより、Bのランクは３である。

後方代入する。leading entry に対応するx_1，x_2，x_3以外のxの要素、すなわち、x_4を自由変数（free variable）とし、以下のように変形する。

$$\begin{bmatrix}1&2&1&1\\0&2&-1&-1\\0&0&1&-1\\0&0&0&1\end{bmatrix}\begin{bmatrix}x_1\\x_2\\x_3\\x_4\end{bmatrix}=\begin{bmatrix}4\\1\\1\\x_4\end{bmatrix}\qquad (式４－３－１７)$$

これより、

$$x_1+2x_2+x_3+x_4=4$$
$$2x_2-x_3-x_4=1$$
$$x_3-x_4=1$$
$$x_4=x_4$$

である。後退代入をx_3から行う。

$x_3-x_4=1$　　$\therefore x_3=x_4+1$

$2x_2-x_3-x_4=1$　　$\therefore x_2=\frac{1}{2}x_3+\frac{1}{2}x_4+\frac{1}{2}=\frac{1}{2}x_4+\frac{1}{2}+\frac{1}{2}x_4+\frac{1}{2}=x_4+1$

$x_1+2x_2+x_3+x_4=4$　　$\therefore x_1=-2x_2-x_3-x_4+4=-2x_4-2-x_4-1-x_4+4=-4x_4+1$

すなわち、

$$\begin{bmatrix}x_1\\x_2\\x_3\\x_4\end{bmatrix}=\begin{bmatrix}-4\\1\\1\\1\end{bmatrix}x_4+\begin{bmatrix}1\\1\\1\\0\end{bmatrix}\qquad (式４－３－１８)$$

と求められる。

また、ガウスージョルダン消去法で RREF に変形すれば、以下のように求められる。

$$\left[\begin{array}{cccc|c}2&4&2&2&8\\4&10&3&3&17\\2&6&1&1&9\\3&7&1&4&11\end{array}\right]\sim\left[\begin{array}{cccc|c}1&2&1&1&4\\0&2&-1&-1&1\\0&0&1&-1&1\\0&0&0&0&0\end{array}\right]\sim\left[\begin{array}{cccc|c}1&0&0&4&1\\0&1&0&-1&1\\0&0&1&-1&1\\0&0&0&0&0\end{array}\right]\qquad (式４－３－１９)$$

$$\begin{bmatrix}1&0&0&\mathbf{4}\\0&1&0&\mathbf{-1}\\0&0&1&\mathbf{-1}\\0&0&0&\mathbf{1}\end{bmatrix}\begin{bmatrix}x_1\\x_2\\x_3\\x_4\end{bmatrix}=\begin{bmatrix}0\\0\\0\\x_4\end{bmatrix}+\begin{bmatrix}1\\1\\1\\0\end{bmatrix}\qquad (式４－３－２０)$$

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} -4 \\ 1 \\ 1 \\ 1 \end{bmatrix} x_4 + \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} \quad \text{（式４－３－２１）}$$

４－３－５）その他

（１）ピボットと解の存在

$m \times n$の行列Aの REF の全ての行でピボットを持つとき、すなわち、

$$A \sim \begin{bmatrix} p & a_{12} & a_{13} & & & a_{1n-1} & a_{1n} \\ 0 & p & a_{23} & & \cdots & & \\ 0 & 0 & p & & & & \\ 0 & 0 & 0 & & \ddots & & \\ \vdots & \vdots & \vdots & & & & \\ 0 & 0 & 0 & \cdots & 0 & p & a_{sn} \end{bmatrix} \quad \text{（式４－３－２２）}$$

の時、$Ax = b$は「少なくとも」１つの解を持つ。

$m \times n$の行列Aの REF の全ての列でピボットを持つとき、すなわち、

$$A \sim \begin{bmatrix} p & a_{12} & a_{13} & & & a_{1n-1} & a_{1n} \\ 0 & p & a_{23} & & \cdots & & \\ 0 & 0 & p & & & & \\ 0 & 0 & 0 & & \ddots & & \\ \vdots & \vdots & \vdots & & & & p \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix} \quad \text{（式４－３－２３）}$$

の時、$Ax = b$は「たかだか」１つの解を持つ。つまり、解を持たないか、１つの解を持つ。

（１－１）

以下では、非０の項をzとする。

$$A = \begin{bmatrix} p & z & z & z \\ 0 & p & z & z \\ 0 & 0 & p & z \end{bmatrix} \qquad x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \qquad b = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} \quad \text{（式４－３－２４）}$$

ランク３、変数４、方程式３本である。$Ax = b$は、

$$Ax = \begin{bmatrix} p & z & z & z \\ 0 & p & z & z \\ 0 & 0 & p & z \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} px_1 + zx_2 + zx_3 + zx_4 \\ px_2 + zx_3 + zx_4 \\ px_3 + zx_4 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} \quad \text{（式４－３－２５）}$$

である。最終行より、x_3は、x_4とb_3で表現され、同様にx_1、x_2も求められる。従って、解が存在する。

（１－２）

$$B = \begin{bmatrix} p & z & z \\ 0 & p & z \\ 0 & 0 & p \\ 0 & 0 & 0 \end{bmatrix} \qquad x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \qquad b = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix} \quad \text{（式４－３－２６）}$$

ランク３、変数３、方程式４本である。$Bx = b$は、

$$B = \begin{bmatrix} p & z & z \\ 0 & p & z \\ 0 & 0 & p \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} px_1 + zx_2 + zx_3 \\ px_2 + zx_3 \\ px_3 \\ 0 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix} \quad \text{（式４－３－２７）}$$

である。最終行より、$b_4 = 0$でなければ、解が存在しない。$b_4 = 0$であれば、第３行目よりx_3が一意に求まり、続いてx_2、x_1が一意に決定される。従って、たかだか１つの解を持つ。

（１－３）

$$C = \begin{bmatrix} p & z & z & z \\ 0 & p & z & z \\ 0 & 0 & p & z \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \qquad b = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix} \qquad \text{（式４－３－２８）}$$

ランク３、変数４、方程式４本である。$Cx = b$は、

$$C = \begin{bmatrix} p & z & z & z \\ 0 & p & z & z \\ 0 & 0 & p & z \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} px_1 + zx_2 + zx_3 + zx_4 \\ px_2 + zx_3 + zx_4 \\ px_3 + zx_4 \\ 0 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix} \qquad \text{（式４－３－２９）}$$

である。最終行より、$b_4 = 0$でなければ、解が存在しない。$b_4 = 0$であれば、最終行より、x_3は、x_4とb_3で表現され、同様にx_1、x_2も求められる。従って、解が存在する。

（１－４）例

$$A = \begin{bmatrix} 2 & 4 & 2 & 2 \\ 4 & 10 & 5 & 5 \\ 2 & 4 & 3 & 1 \end{bmatrix} \qquad x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \qquad b = \begin{bmatrix} 8 \\ 9 \\ 9 \end{bmatrix}$$

$$[A|b] = \left[\begin{array}{cccc|c} 2 & 4 & 2 & 2 & 8 \\ 4 & 10 & 5 & 5 & 9 \\ 2 & 4 & 3 & 1 & 9 \end{array}\right] \sim \left[\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 4 \\ 0 & 2 & 1 & 1 & -7 \\ 0 & 0 & 1 & -1 & 1 \end{array}\right] \sim \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 11 \\ 0 & 1 & 0 & 1 & -4 \\ 0 & 0 & 1 & -1 & 1 \end{array}\right] \qquad x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \\ 1 \\ 1 \end{bmatrix} x_4 + \begin{bmatrix} 11 \\ -4 \\ 1 \\ 0 \end{bmatrix}$$

解は無限に存在する。

$$B1 = \begin{bmatrix} 2 & 4 & 2 \\ 4 & 10 & 3 \\ 2 & 6 & 1 \\ 3 & 7 & 1 \end{bmatrix} \qquad x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \qquad b = \begin{bmatrix} 0 \\ -7 \\ -7 \\ -8 \end{bmatrix}$$

$$[B1|b] = \left[\begin{array}{ccc|c} 2 & 4 & 2 & 0 \\ 4 & 10 & 3 & -7 \\ 2 & 6 & 1 & -7 \\ 3 & 7 & 1 & -8 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 2 & 1 & 0 \\ 0 & 2 & -1 & -7 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{array}\right] \qquad x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 \\ -2 \\ 3 \end{bmatrix} \quad \text{唯一の解}$$

$$B2 = \begin{bmatrix} 2 & 4 & 2 \\ 4 & 10 & 3 \\ 2 & 6 & 1 \\ 3 & 7 & 1 \end{bmatrix} \qquad x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \qquad b = \begin{bmatrix} 8 \\ 9 \\ 9 \\ 1 \end{bmatrix}$$

$$[B2|b] = \left[\begin{array}{ccc|c} 2 & 4 & 2 & 8 \\ 4 & 10 & 3 & 9 \\ 2 & 6 & 1 & 9 \\ 3 & 7 & 1 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 2 & 1 & 0 \\ 0 & 2 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right] \qquad \text{解なし}$$

$$C1 = \begin{bmatrix} 2 & 4 & 2 & 2 \\ 4 & 10 & 3 & 3 \\ 2 & 6 & 1 & 1 \\ 3 & 7 & 1 & 4 \end{bmatrix} \qquad x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \qquad b = \begin{bmatrix} 8 \\ 17 \\ 9 \\ 11 \end{bmatrix}$$

$$[C1|b]=\left[\begin{array}{cccc|c}2&4&2&2&8\\4&10&3&3&17\\2&6&1&1&9\\3&7&1&4&11\end{array}\right]\sim\left[\begin{array}{cccc|c}1&2&1&1&4\\0&2&-1&-1&1\\0&0&1&-1&1\\0&0&0&0&0\end{array}\right]\qquad x=\begin{bmatrix}x_1\\x_2\\x_3\\x_4\end{bmatrix}=\begin{bmatrix}-4\\1\\1\\1\end{bmatrix}x_4+\begin{bmatrix}1\\1\\1\\0\end{bmatrix}$$ 解は無限に存在する

$$C2=\begin{bmatrix}2&4&2&2\\4&10&3&3\\2&6&1&1\\3&7&1&4\end{bmatrix}\qquad x=\begin{bmatrix}x_1\\x_2\\x_3\\x_4\end{bmatrix}\qquad b=\begin{bmatrix}8\\17\\-9\\11\end{bmatrix}$$

$$[C2|b]=\left[\begin{array}{cccc|c}2&4&2&2&8\\4&10&3&3&17\\2&6&1&1&-9\\3&7&1&4&11\end{array}\right]\sim\left[\begin{array}{cccc|c}1&2&1&1&4\\0&2&-1&-1&1\\0&0&1&-1&1\\0&0&0&0&1\end{array}\right]$$ 解なし

（２）一次独立の証明方法

ベクトル、$\overrightarrow{a_1}$、$\overrightarrow{a_2}$、、、$\overrightarrow{a_n}$　が一次独立であることを証明する方法

（方法１）

$c_1\overrightarrow{a_1}+c_2\overrightarrow{a_2}+\cdots+c_n\overrightarrow{a_n}=0 \quad\Leftrightarrow\quad c_1=c_2=\cdots=c_n=0$　を示す。

（方法２）

$A=[\overrightarrow{a_1},\overrightarrow{a_2},,,\overrightarrow{a_n}]$ とし、 $Null(A)=\{\vec{0}\}$　を示す。

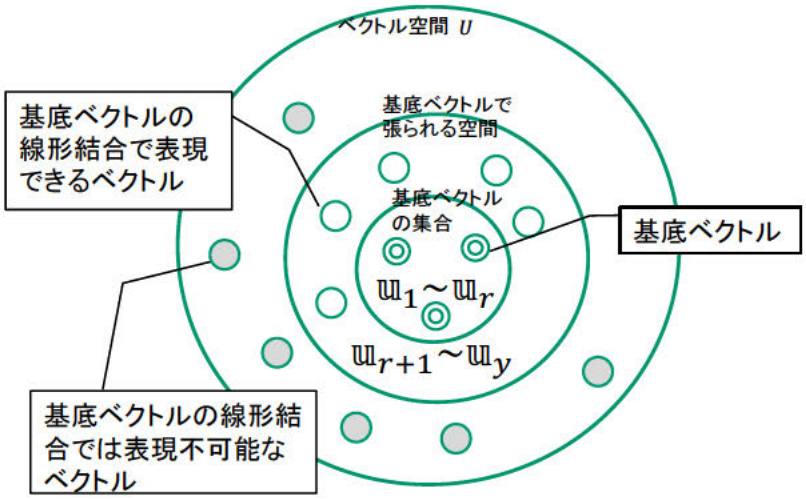
（方法３）

$A=[\overrightarrow{a_1},\overrightarrow{a_2},,,\overrightarrow{a_n}]$ とし、 Aが１対１写像であること、すなわち$Av=Aw \quad\Leftrightarrow\quad v=w$　を示す。

5）基底(Basis)

あるベクトル空間を必要十分に表現するベクトルの集合

その空間に属す全てのベクトルが基底ベクトルの線形結合で表現される。



基底の条件

・基底を構成するベクトルは一次独立である。

・対象となるベクトル空間中のベクトルは、基底ベクトルの線形結合で表現できる。

例として、実数を要素とする 3 次元ベクトル全体の集合をUとする。すなわち、$U = \mathbb{R}^3$　である。

Uの部分集合であるSに属す 4 つのベクトル(1 2 3)(1 1 4)(1 4 1)(1 3 2)が、部分空間Tを張ることを以下のように表現する。

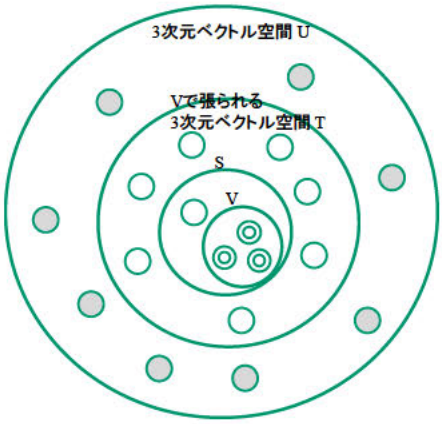
$$T = span\left(\begin{bmatrix}1\\2\\3\end{bmatrix}, \begin{bmatrix}1\\1\\4\end{bmatrix}, \begin{bmatrix}1\\4\\1\end{bmatrix}, \begin{bmatrix}1\\3\\2\end{bmatrix}\right) \quad （式５－１）$$

4 つのベクトルのうち、(1 2 3)(1 1 4)(1 4 1)は、一次独立である。

（証明　$c_1\begin{bmatrix}1\\2\\3\end{bmatrix} + c_2\begin{bmatrix}1\\1\\4\end{bmatrix} + c_3\begin{bmatrix}1\\4\\1\end{bmatrix} = 0$とし$c_1 = c_2 = c_3 = 0$となること、すなわち$\begin{bmatrix}1 & 1 & 1\\2 & 1 & 4\\3 & 4 & 1\end{bmatrix}\begin{bmatrix}c1\\c2\\c3\end{bmatrix} = 0$の解が 0 ベクトルであることを証明する。）

従って、$V = \{(1\ 2\ 3)(1\ 1\ 4)(1\ 4\ 1)\}$は、$T$の基底となる。

$$T = span\left(\begin{bmatrix}1\\2\\3\end{bmatrix}, \begin{bmatrix}1\\1\\4\end{bmatrix}, \begin{bmatrix}1\\4\\1\end{bmatrix}\right) \quad （式５－２）$$



6）零空間（null space）

6－1）

連立一次方程式を考える。

$$Ax = b \quad （式6－1）$$

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & & \\ a_{31} & & & & \\ \vdots & & & \ddots & \\ a_{m1} & & & & a_{mn} \end{bmatrix} \quad x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \quad b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

零空間（null space）とは、$b = 0$すなわち、

$$Ax = 0 \quad （式6－2）$$

となるベクトルxの集合をさす。式 6-2 は homogeneous equation とも呼ばれる。零空間を$Null(A)$と表現する。ベクトルxが実数のn次元ベクトルの場合は、$Null(A) = \{x \in \mathbb{R}^n | Ax = 0\}$ となる。

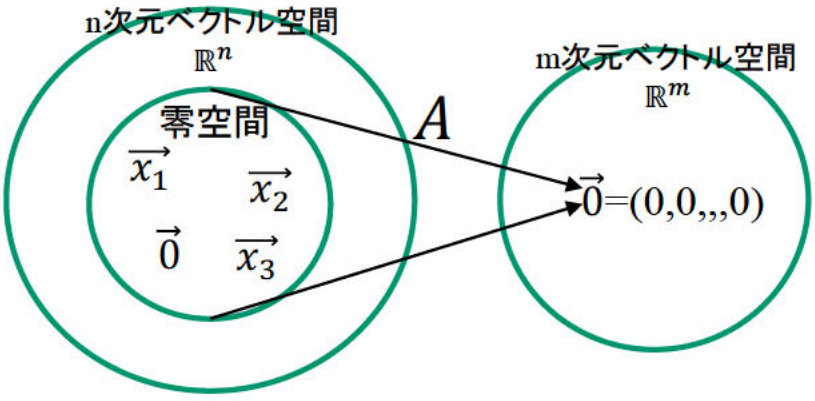
式 6-2 を書き直すと、

$$Ax = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & & \\ a_{31} & & & & \\ \vdots & & & \ddots & \\ a_{m1} & & & & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \quad （式6－3）$$

であるので、式 6-2 を満たすベクトルxは、Aのすべての行との内積が 0 である、すなわち、直交している。したがって、零空間とは、Aのすべての行ベクトルと直交する列ベクトルの集合とも言える。（これは、後に出てくる行空間と零空間が直交していることを意味している。）

また、$Ax = 0$とは、図のように、零空間に属するどの列ベクトルもAで写像すると 0 ベクトルとなることを意味している。従って、零空間を核（kernel）とも呼ぶ。なお、要素がすべて 0 の列ベクトルも零空間に属していることを注意しておく。

零空間には複数の列ベクトルが存在するが、それらはいくつかの基本ベクトル（基底ベクトル）の線形結合によって作り出せる。すなわち基底ベクトル（の集合）を求められれば零空間を曖昧性なく表現することができる。これを零空間の基底と呼ぶ。



$(\vec{x_i} = (x_{i1}, x_{i2}, , , , x_{in})\ x_{ij} \in$ 実数体$\mathbb{R}$　の場合）

具体例

例 1

$A = \begin{bmatrix} 1 & 2 & 3 & -4 \\ 2 & -3 & 4 & 1 \\ 1 & 1 & 3 & 5 \\ 3 & -1 & 7 & -3 \end{bmatrix}$の零空間の基底を求める。

行基本変形して RREF を求める。

$$\begin{bmatrix} 1 & 2 & 3 & -4 \\ 2 & -3 & 4 & 1 \\ 1 & 1 & 3 & 5 \\ 3 & -1 & 7 & -3 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 3 & -4 \\ 0 & -7 & -2 & 9 \\ 0 & -1 & 0 & 9 \\ 0 & -7 & -2 & 9 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 3 & -4 \\ 0 & 7 & 2 & -9 \\ 0 & -1 & 0 & 9 \\ 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 3 & -4 \\ 0 & 3 & 1 & 0 \\ 0 & -1 & 0 & 9 \\ 0 & 0 & 0 & 0 \end{bmatrix} \sim$$

$$\begin{bmatrix} 1 & 2 & 3 & -4 \\ 0 & 3 & 1 & 0 \\ 0 & 0 & 1 & 27 \\ 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 3 & 6 & 9 & -12 \\ 0 & 6 & 2 & 0 \\ 0 & 0 & 1 & 27 \\ 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 3 & 0 & 7 & -12 \\ 0 & 6 & 2 & 0 \\ 0 & 0 & 1 & 27 \\ 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 3 & 0 & 7 & -12 \\ 0 & 6 & 2 & 0 \\ 0 & 0 & 2 & 54 \\ 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 3 & 0 & 7 & -12 \\ 0 & 6 & 0 & -54 \\ 0 & 0 & 2 & 54 \\ 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 6 & 0 & 14 & -24 \\ 0 & 6 & 0 & -54 \\ 0 & 0 & 14 & 378 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\sim \begin{bmatrix} 6 & 0 & 0 & -402 \\ 0 & 1 & 0 & -9 \\ 0 & 0 & 2 & 54 \\ 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & -67 \\ 0 & 1 & 0 & -9 \\ 0 & 0 & 1 & 27 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{（式６－４）}$$

$Ax = 0$の連立一次方程式に戻す。

$$\begin{bmatrix} \mathbf{1} & 0 & 0 & -67 \\ 0 & \mathbf{1} & 0 & -9 \\ 0 & 0 & \mathbf{1} & 27 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = 0 \quad \text{（式６－５）}$$

leading entry に対応するx_1, x_2, x_3以外のxの要素、すなわち、x_4を自由変数（free variable、free variable (non-pivot variable)とし、以下のように変形する。（太文字の行を追加）

$$\begin{bmatrix} 1 & 0 & 0 & -67 \\ 0 & 1 & 0 & -9 \\ 0 & 0 & 1 & 27 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} x_1 - 67x_4 \\ x_2 - 9x_4 \\ x_3 + 27x_4 \\ x_4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ x_4 \end{bmatrix} \quad \text{（式６－６）}$$

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 67 \\ 9 \\ -27 \\ 1 \end{bmatrix} x_4 \quad \text{（式６－７）}$$

以上より、零空間の基底は、(67 9 -27 1)となる。また、leading entry の数が３であるため、Aのランクは３である。零空間は、以下で表現される。また、零空間の次元は１である。

$$Null(A) = span\left(\begin{bmatrix} 67 \\ 9 \\ -27 \\ 1 \end{bmatrix} \right) \quad \text{（式６－８）}$$

例２

$E = \begin{bmatrix} 1 & 0 & -2 & 1 \\ 1 & 1 & -5 & -1 \\ 2 & 1 & -7 & 0 \end{bmatrix}$の零空間の基底を求める。

行基本変形して RREF を求める。

$$\begin{bmatrix} 1 & 0 & -2 & 1 \\ 1 & 1 & -5 & -1 \\ 2 & 1 & -7 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & -2 & 1 \\ 0 & 1 & -3 & -2 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{（式６－９）}$$

$Ex = 0$の連立一次方程式に戻す。

$$\begin{bmatrix}1 & 0 & -2 & 1\\ 0 & 1 & -3 & -2\\ 0 & 0 & 0 & 0\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\\ x_4\end{bmatrix}=0 \quad \text{（式６－１０）}$$

leading entry に対応するx_1, x_2以外のxの要素、すなわち、x_3, x_4を自由変数（free variable、free variable (non-pivot variable)とし、以下のように変形する。（太文字の行を追加）

$$\begin{bmatrix}1 & 0 & -2 & 1\\ 0 & 1 & -3 & -2\\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0}\\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1}\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\\ x_4\end{bmatrix}=\begin{bmatrix}x_1-2x_3+x_4\\ x_2-3x_3-2x_4\\ x_3\\ x_4\end{bmatrix}=\begin{bmatrix}0\\ 0\\ x_3\\ x_4\end{bmatrix} \quad \text{（式６－１１）}$$

$$\begin{bmatrix}x_1\\ x_2\\ x_3\\ x_4\end{bmatrix}=\begin{bmatrix}2 & -1\\ 3 & 2\\ 1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}x_3\\ x_4\end{bmatrix} \quad \text{（式６－１２）}$$

$$\begin{bmatrix}x_1\\ x_2\\ x_3\\ x_4\end{bmatrix}=\begin{bmatrix}2\\ 3\\ 1\\ 0\end{bmatrix}x_3+\begin{bmatrix}-1\\ 2\\ 0\\ 1\end{bmatrix}x_4 \quad \text{（式６－１３）}$$

これより、$Ex=0$となるxの集合（零空間）に属す任意のベクトル$(x_1,\ x_2,\ x_3,\ x_4)$は、(2 3 1 0)(-1 2 0 1)の線形結合で表現されることがわかる。また、$(x_1,\ x_2,\ x_3,\ x_4)=0$となる必要十分条件は、$x_3=x_4=0$であることである。従って、(2 3 1 0) (-1 2 0 1)は一次独立である。以上より、(2 3 1 0) (-1 2 0 1)は、基底ベクトルである。すなわち、これらがEの零空間の基底ベクトルである。Eのランクは２である。零空間は、以下で表現される。また、零空間の次元は 2 である。

$$Null(E)=span\left(\begin{bmatrix}2\\ 3\\ 1\\ 0\end{bmatrix},\begin{bmatrix}-1\\ 2\\ 0\\ 1\end{bmatrix}\right) \quad \text{（式６－１４）}$$

６－２）零空間に関するいくつかの指摘

以下を行列の行基本変形で示した。

$$\underset{\substack{A_0=A\\ b_0=b}}{A_0x=b_0} \underset{(L_1)^{-1}}{\overset{L_1}{\underset{\leftarrow}{\rightarrow}}} A_1x=b_1 \underset{(L_2)^{-1}}{\overset{L_2}{\underset{\leftarrow}{\rightarrow}}} A_2x=b_2 \underset{(L_3)^{-1}}{\overset{L_3}{\underset{\leftarrow}{\rightarrow}}} \cdots \rightarrow A_{ref}x=b_{ref} \underset{(L_{rref})^{-1}}{\overset{L_{\mathrm{rref}}}{\underset{\leftarrow}{\rightarrow}}} A_{rref}x=b_{rref}$$

変形の途中の行列の零空間は一致する。すなわち、以下が成立する。

$Null(A_0)=Null(A_1)=\cdots=Null(A_{ref})=Null(A_{rref})$

（また、行空間$Row(A)$は一致する。つまり、$Row(A_0)=Row(A_{rref})$である。例 1 で、1x(1 0 0 -67)+2x(0 1 0 -9)+3x(0 0 1 27)=(1 2 3 -4)であり、元のベクトルの 1 行目は、REF の基底ベクトルの線形結合で表現されている。つまり、$Row(A)$と$Row(A_{rref})$は同一の空間をとる。

一方、列空間$Col(A)$は一致しない。つまり、$Col(A_0)\neq Col(A_{rref})$である。$Col(A)$=span[(1 2 1 3)(2 -3 1 -1)(...)(...)]、$Col(A_{rref})$=span[(1000)(0100)(0010)(-67 -9 27 0)]である。第 4 項目を見る。$Col(A)$には第 4 項が 0 ではないベクトルが存在する一方、$Col(A_{rref})$は第 4 項は必ず 0 である。従って、$Col(A)$は$Col(A_{rref})$と一致しない）

（課題６－１）

$F = \begin{bmatrix} 1 & 2 & 3 & -4 \\ 2 & -3 & 4 & 1 \\ 1 & 1 & 3 & 5 \end{bmatrix}$とする。

問 1）Fの零空間$Null(F)$を求めよ。

問２）$u = \begin{bmatrix} 2 \\ 3 \\ 1 \\ 0 \end{bmatrix}$ が$Null(F)$に含まれるかを考察せよ。

（ヒント：２つの方法があり得る。①$Null(F)$の基底を求めuが線形結合で表現されるかを検討する。②$Null(F)$に含まれているならば$Fx = 0$。よって、$Fu = 0$かどうかを調べる。）

解答

問１）$Null(F) = span\left(\begin{bmatrix} 67 \\ 9 \\ -27 \\ 1 \end{bmatrix}\right)$

問２）　$Row(F) = span\left(\begin{bmatrix} 1 \\ 2 \\ 3 \\ -4 \end{bmatrix}, \begin{bmatrix} 2 \\ -3 \\ 4 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 3 \\ 5 \end{bmatrix}\right)$

①$\begin{bmatrix} 2 \\ 3 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 1 \\ 2 & -3 & 1 \\ 3 & 4 & 3 \\ -4 & 1 & 5 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix}$　　$\left[\begin{array}{ccc|c} 1 & 2 & 1 & 2 \\ 2 & -3 & 1 & 3 \\ 3 & 4 & 3 & 1 \\ -4 & 1 & 5 & 0 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right]$　よって、解なし、含まれない

②$\begin{bmatrix} 1 & 2 & 3 & -4 \\ 2 & -3 & 4 & 1 \\ 1 & 1 & 3 & 5 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2+6+3 \\ 4-9+4 \\ 2+3+3 \end{bmatrix} \neq 0$　よって、含まれない

階数・退化次数の定理（Rank–nullity theorem）

$m \times n$行列Aの RREF がr個の leading entry を持っていたとする。このとき、Aのランクはrである。また、Aの零空間の次元（nullity、free variable の数）kは$n - r$である。従って、$n - r = k$が成立する。

7）行空間

7－1）行空間

行列Aの行ベクトルで張られる空間（すなわち、行ベクトルの線形結合で表現されるベクトルの集合）を行空間と呼び、$Row(A)$と書く。$m \times n$の行列Aの行ベクトルはn次元ベクトルである。従って、行空間$Row(A)$もn次元ベクトルの集合であり、n次元ベクトルの部分空間である。

$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & \\ a_{31} & & & & \\ & \vdots & & \ddots & \\ a_{m1} & & & & a_{mn} \end{bmatrix}$に対する行空間は、

$$Row(A) = span\left(\begin{bmatrix} a_{11} \\ a_{12} \\ \cdots \\ a_{1n} \end{bmatrix}, \begin{bmatrix} a_{21} \\ a_{22} \\ \cdots \\ a_{2n} \end{bmatrix}, \cdots, \begin{bmatrix} a_{m1} \\ a_{m2} \\ \cdots \\ a_{mn} \end{bmatrix}\right) = \begin{Bmatrix} \{a_{11} & a_{12} & \cdots & a_{1n}\} \\ \{a_{21} & a_{22} & \cdots & a_{2n}\} \\ & \vdots & & \\ \{a_{m1} & a_{m2} & \cdots & a_{mn}\} \\ & \vdots & & \end{Bmatrix} \quad （式７－１）$$

である。$\begin{bmatrix} a_{11} \\ a_{12} \\ \cdots \\ a_{1n} \end{bmatrix}$　などは基底ではないことに注意する。

7－2）行空間の性質

・行空間のランク、列空間のランク、元の行列Aのランクは一致する。

7－3）行空間の基底ベクトルの求め方

$m \times n$の行列A を考える。

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & \\ a_{31} & & & & \\ & \vdots & & \ddots & \\ a_{m1} & & & & a_{mn} \end{bmatrix} \quad （式７－２）$$

・各行を表現できる必要十分なベクトル（の集合）を基底ベクトルという。基底ベクトルは唯一ではない。

・基底ベクトルを求めるためには、一次独立な行ベクトルを求めればよい。

・０ベクトルはどのようなベクトルに対しても従属である。なぜなら、$0 = 0 \times c_1 + 0 \times c_2 + \cdots$　であり非０のc_iが存在するから。よって０ベクトルは基底ベクトルにはなり得ない。

従って、Aを行列の行基本変形で変形し０ベクトルを次々と求め、それ以上変形できなくなったら、０ベクトル以外が基底となるはずである。

・０ベクトルを求める方法のひとつがガウス消去法である。ガウス消去法では、REF が求まる。行空間の基底を求めるだけなら RREF まで求める必要はない。

7－4）具体例

次の行列Aの行空間の基底ベクトルを求める。

$$A=\begin{bmatrix}1 & 2 & 3 & -4\\ 2 & -3 & 4 & 1\\ 1 & 1 & 3 & 5\\ 3 & -1 & 7 & -3\end{bmatrix}$$

Aの行空間は、$Row(A)=span\left(\begin{bmatrix}1\\2\\3\\-4\end{bmatrix},\begin{bmatrix}2\\-3\\4\\1\end{bmatrix},\begin{bmatrix}1\\1\\3\\5\end{bmatrix},\begin{bmatrix}3\\-1\\7\\-3\end{bmatrix}\right)$　である。

まず、以下のステップで行基本変形を行う。

ステップ１）$R1\to r1\quad R2-2*R1\to r2\quad R3-R1\to r3\quad R4-3*R1\to r4$

ステップ２）$R1\to r1\quad -R2\to r2\quad R3\to r3\quad R4-R2\to r4$

$$A=\begin{bmatrix}1 & 2 & 3 & -4\\ 2 & -3 & 4 & 1\\ 1 & 1 & 3 & 5\\ 3 & -1 & 7 & -3\end{bmatrix}\sim\begin{bmatrix}1 & 2 & 3 & -4\\ 0 & -7 & -2 & 9\\ 0 & -1 & 0 & 9\\ 0 & -7 & -2 & 9\end{bmatrix}\sim\begin{bmatrix}1 & 2 & 3 & -4\\ 0 & 7 & 2 & -9\\ 0 & -1 & 0 & 9\\ 0 & 0 & 0 & 0\end{bmatrix}$$　（式７－３）

この段階で、(1 2 3 -4) (0 7 2 -9) (0 -1 0 9)はこれ以上０ベクトルにはできない。すなわち独立である。よって、基底（の１セット）はこの３つのベクトルである。Aのランクは３である。

さらに変形して、$\begin{bmatrix}1 & 2 & 3 & -4\\ 0 & 3 & 1 & 0\\ 0 & -1 & 0 & 9\\ 0 & 0 & 0 & 0\end{bmatrix}$とし、(1 2 3 -4) (0 3 1 0) (0 -1 0 9)を基底としてもよい。

（課題７－１）基底(1 2 3 -4) (0 7 2 -9) (0 -1 0 9) で張られるベクトル空間をu_1とする。(1 2 3 -4) (0 3 1 0) (0 -1 0 9)はこの空間の基底となることを確認せよ。（ヒント：(1 2 3 -4) (0 3 1 0) (0 -1 0 9)が一次独立であること、u_1に属す全てのベクトルが(1 2 3 -4) (0 3 1 0) (0 -1 0 9)の線形結合で表現されることを示す。）

例２

$$B=\begin{bmatrix}2 & 4 & 2 & 2\\ 4 & 10 & 3 & 3\\ 2 & 6 & 1 & 1\\ 3 & 7 & 1 & 4\end{bmatrix}$$

以下の２ステップで行基本変形を行う。

ステップ１）$\frac{1}{2}*R1\to r1\quad R2-2*R1\to r2\quad R3-R1\to r3\quad R4-\frac{3}{2}*R1\to r4$

ステップ２）$R1\to r1\quad R2\to r2\quad R3-R2\to r3\quad R4-\frac{1}{2}*R2\to r4$

ステップ３）$R1\to r1\quad R2\to r2\quad R3\to r4\quad R4\to r3$

ステップ４）$R1\to r1\quad R2\to r2\quad \frac{2}{3}*R3\to r3\quad R4\to r4$

$$B=\begin{bmatrix}2 & 4 & 2 & 2\\ 4 & 10 & 3 & 3\\ 2 & 6 & 1 & 1\\ 3 & 7 & 1 & 4\end{bmatrix}\sim\begin{bmatrix}1 & 2 & 1 & 1\\ 0 & 2 & -1 & -1\\ 0 & 2 & -1 & -1\\ 0 & 1 & -2 & 1\end{bmatrix}\sim\begin{bmatrix}1 & 2 & 1 & 1\\ 0 & 2 & -1 & -1\\ 0 & 0 & 0 & 0\\ 0 & 0 & -\frac{3}{2} & \frac{3}{2}\end{bmatrix}\sim\begin{bmatrix}1 & 2 & 1 & 1\\ 0 & 2 & -1 & -1\\ 0 & 0 & -\frac{3}{2} & \frac{3}{2}\\ 0 & 0 & 0 & 0\end{bmatrix}$$

$$\sim\begin{bmatrix}1 & 2 & 1 & 1\\ 0 & 2 & -1 & -1\\ 0 & 0 & -1 & 1\\ 0 & 0 & 0 & 0\end{bmatrix}$$　（式７－４）

基底（の１セット）は、(1 2 1 1) (0 2 -1 -1) (0 0 -1 1)である。B のランクは３である。

８）列空間

８－１）列空間

行列Aの列ベクトルで張られる空間（すなわち、列ベクトルの線形結合で表現されるベクトルの集合）を列空間と呼び、$Col(A)$と書く。$m \times n$の行列A の列ベクトルはm次元ベクトルである。従って、列空間$Col(A)$もm次元ベクトルの集合であり、m次元ベクトルの部分空間である。

$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & \\ a_{31} & & & & \\ & \vdots & & \ddots & \\ a_{m1} & & & & a_{mn} \end{bmatrix}$に対する列空間は、

$$Col(A) = span\left(\begin{bmatrix} a_{11} \\ a_{21} \\ \cdots \\ a_{m1} \end{bmatrix}, \begin{bmatrix} a_{12} \\ a_{22} \\ \cdots \\ a_{m2} \end{bmatrix}, \cdots, \begin{bmatrix} a_{11} \\ a_{2n} \\ \cdots \\ a_{mn} \end{bmatrix}\right) = \left\{\begin{Bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{Bmatrix} \begin{Bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{Bmatrix} \cdots \begin{Bmatrix} a_{11} \\ a_{2n} \\ \vdots \\ a_{mn} \end{Bmatrix} \cdots\right\} \quad （式８－１）$$

である。$\begin{bmatrix} a_{11} \\ a_{21} \\ \cdots \\ a_{m1} \end{bmatrix}$ などは基底ではないことに注意する。

８－２）列空間の性質

・行空間のランク、列空間のランク、A のランクは一致する

８－３）列空間の基底ベクトルの求め方

列空間の基底ベクトルを求めるには、２つの方法がある。

（方法１）行空間の場合と同様に列基本変形を行う方法

（方法２）行基本行列を行って REF を求め、列空間を求める方法

８－４）具体例

（方法１）行空間の場合と同様に列基本変形を行う方法

列基本変形を行ってもよいが、ここでは転置して行基本変形を行って基底ベクトルを求める。

例１：

$$A = \begin{bmatrix} 1 & 2 & 3 & -4 \\ 2 & -3 & 4 & 1 \\ 1 & 1 & 3 & 5 \\ 3 & -1 & 7 & -3 \end{bmatrix}$$

転置する。

$$A^T = \begin{bmatrix} 1 & 2 & 1 & 3 \\ 2 & -3 & 1 & -1 \\ 3 & 4 & 3 & 7 \\ -4 & 1 & 5 & -3 \end{bmatrix} \quad （式８－２）$$

行変形する

ステップ１）$R1 \to r1 \quad R2 - 2 * R1 \to r2 \quad R3 - 3 * R1 \to r3 \quad R4 + 4 * R1 \to r4$

ステップ２）$R1 \to r1 \quad R2 \to r2 \quad R3 - \frac{2}{7}R2 \to r3 \quad R4 + \frac{9}{7}R2 \to r4$

ステップ３）$R1 \to r1 \quad R2 \to r2 \quad \frac{7}{2}R3 \to r3 \quad R4 - \frac{54}{2}R3 \to r4$

$$A^T = \begin{bmatrix} 1 & 2 & 1 & 3 \\ 2 & -3 & 1 & -1 \\ 3 & 4 & 3 & 7 \\ -4 & 1 & 5 & -3 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & -7 & -1 & -7 \\ 0 & -2 & 0 & -2 \\ 0 & 9 & 9 & 9 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & -7 & -1 & -7 \\ 0 & 0 & \frac{2}{7} & 0 \\ 0 & 0 & \frac{54}{7} & 0 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & -7 & -1 & -7 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad (式８－３)$$

よって、基底（の一つ）は、(1 2 1 3)(0 -7 -1 -7)(0 0 1 0)となる。A^Tのランクは３である。
行空間で求めたランクと一致していることに注意せよ。

例２：

$$B = \begin{bmatrix} 2 & 4 & 2 & 2 \\ 4 & 10 & 3 & 3 \\ 2 & 6 & 1 & 1 \\ 3 & 7 & 1 & 4 \end{bmatrix}$$

転置する。

$$B^T = \begin{bmatrix} 2 & 4 & 2 & 3 \\ 4 & 10 & 6 & 7 \\ 2 & 3 & 1 & 1 \\ 2 & 3 & 1 & 4 \end{bmatrix}$$

行変形する。

ステップ１）$R1 \to r1 \quad R2 - 2 * R1 \to r2 \quad R3 - R1 \to r3 \quad R4 - R1 \to r4$

ステップ２）$R1 \to r1 \quad R2 \to r2 \quad R3 + \frac{1}{2}R2 \to r3 \quad R4 + \frac{1}{2} * R2 \to r4$

ステップ３）$R1 \to r1 \quad R2 \to r2 \quad R3 \to r3 \quad R4 + \frac{3}{2} * R3 \to r4$

$$B^T = \begin{bmatrix} 2 & 4 & 2 & 3 \\ 4 & 10 & 6 & 7 \\ 2 & 3 & 1 & 1 \\ 2 & 3 & 1 & 4 \end{bmatrix} \sim \begin{bmatrix} 2 & 4 & 2 & 3 \\ 0 & 2 & 2 & 1 \\ 0 & -1 & -1 & -2 \\ 0 & -1 & -1 & 1 \end{bmatrix} \sim \begin{bmatrix} 2 & 4 & 2 & 3 \\ 0 & 2 & 2 & 1 \\ 0 & 0 & 0 & -\frac{3}{2} \\ 0 & 0 & 0 & -\frac{1}{2} \end{bmatrix} \sim \begin{bmatrix} 2 & 4 & 2 & 3 \\ 0 & 2 & 2 & 1 \\ 0 & 0 & 0 & -\frac{3}{2} \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

以上より、列空間の基底ベクトルは、(2 4 2 3) (0 2 2 1) (0 0 0 1)となる。B^Tのランクは３である。

（方法２）行基本変形を行って REF を求め、列空間を求める方法

ガウス消去法は、一次独立な列を求める手段と考えてもよい。従って、REF を求め、leading entry を持つ列（ピボット列）の元々の行列Aの列を基底ベクトルとしてもよい。また、その数がランクである。

例１：

$$A = \begin{bmatrix} 1 & 2 & 3 & -4 \\ 2 & -3 & 4 & 1 \\ 1 & 1 & 3 & 5 \\ 3 & -1 & 7 & -3 \end{bmatrix} \quad (式８－４)$$

$$A=\begin{bmatrix}1&2&3&-4\\2&-3&4&1\\1&1&3&5\\3&-1&7&-3\end{bmatrix}\sim\begin{bmatrix}1&2&4&-4\\0&-7&-2&9\\0&0&1&27\\0&0&0&0\end{bmatrix}\quad\text{（式８－５）}$$

↑ ↑ ↑

ピボット列

これより、(1 2 1 3) (2 -3 1 -1) (3 4 3 7)が列空間の基底（の１セット）である。

$$Col(A)=span\left(\begin{bmatrix}1\\2\\1\\3\end{bmatrix},\begin{bmatrix}2\\-3\\1\\-1\end{bmatrix},\begin{bmatrix}3\\4\\3\\7\end{bmatrix}\right)\quad\text{（式８－６）}$$

Aのランクは３である。

（課題８－１）(1 2 1 3) (2 -3 1 -1) (3 4 3 7) が一次独立であることを確認せよ。

（課題８－２）(1 2 1 3) (0 7 1 7) (0 0 1 0) も上記のAの列空間$Col(A)$の基底であることを確認せよ。

（ヒント：一次独立であること、(1 2 1 3) (0 7 1 7) (0 0 1 0)が(1 2 1 3) (2 -3 1 -1) (3 4 3 7)の線形結合で表現されることを示す。） ((1 2 1 3) (0 7 1 7) (0 0 1 0)は方法１例１で求めた基底である)

例２：

$$B=\begin{bmatrix}2&4&2&2\\4&10&3&3\\2&6&1&1\\3&7&1&4\end{bmatrix}$$

$$B=\begin{bmatrix}2&4&2&2\\4&10&3&3\\2&6&1&1\\3&7&1&4\end{bmatrix}\sim\begin{bmatrix}1&2&1&1\\0&2&-1&-1\\0&0&1&-1\\0&0&0&0\end{bmatrix}$$

↑ ↑ ↑

ピボット列

これより、(2 4 2 3)(4 10 6 7) (2 3 1 1)が列空間の基底（の１セット）である。

$$Col(B)=span\left(\begin{bmatrix}2\\4\\2\\3\end{bmatrix},\begin{bmatrix}4\\10\\6\\7\end{bmatrix},\begin{bmatrix}2\\3\\1\\1\end{bmatrix}\right)$$

念のため、(2 4 2 3) (4 10 6 7) (2 3 1 1)が独立であることを調べる。

$c_1\begin{bmatrix}2\\4\\2\\3\end{bmatrix}+c_2\begin{bmatrix}4\\10\\6\\7\end{bmatrix}+c_3\begin{bmatrix}2\\3\\1\\1\end{bmatrix}=0$　とし、$c_1=c_2=c_3=0$となることを証明することと等価である。すなわち、$\begin{bmatrix}2&4&2\\4&10&3\\2&6&1\\3&7&1\end{bmatrix}\begin{bmatrix}c_1\\c_2\\c_3\end{bmatrix}=0$　の解が 0 ベクトルであることを証明すればよい。（零空間の議論と同じことをやっていることに注意する。）

行列を RREF に変形すると、

$$\begin{bmatrix}2&4&2\\4&10&3\\2&6&1\\3&7&1\end{bmatrix}\sim\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\\0&0&0\end{bmatrix}$$

となる。すなわち、

$$\begin{bmatrix}2 & 4 & 2\\ 4 & 10 & 3\\ 2 & 6 & 1\\ 3 & 7 & 1\end{bmatrix}\begin{bmatrix}c_1\\ c_2\\ c_3\end{bmatrix}=0 \sim \begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\\ 0 & 0 & 0\end{bmatrix}\begin{bmatrix}c_1\\ c_2\\ c_3\end{bmatrix}=0$$

これより、$c_1=c_2=c_3=0$であり、(2 4 2 3) (4 10 6 7) (2 3 1 1)は独立である。

８－５）列空間と連立一次方程式

（８－５－１）零空間、列空間、行空間などの関係

Aを行基本変形してA_{ref}を得たとする。このとき、以下が成立する。

１）Aの零空間とA_{ref}の零空間は同一である　　$Null(A)=Null(A_{ref})$

２）Aの行空間とA_{ref}の行空間は同一である　　$Row(A)=Row(A_{ref})$

３）Aの列空間とA_{ref}の列空間は同一ではない　　$Col(A)\neq Col(A_{ref})$

４）Aの列空間の次元、A_{ref}の列空間の次元は一致し、Aのランクである

$$\dim\big(Col(A)\big)=\dim\Big(Col\big(A_{ref}\big)\Big)=rank(A)$$

５）Aの行空間の次元、A_{ref}の行空間の次元は一致し、Aのランクである

$$\dim\big(Row(A)\big)=\dim\Big(Row\big(A_{ref}\big)\Big)=rank(A)$$

６）$m\times n$行列のAのランクとAの零空間の次元の和は、Aの列の数nである

$$rank(A)+\dim\big(Null(A)\big)=n$$

（８－５－２）連立一次方程式の解の存在

n次元ベクトル$\in \mathbb{R}^n$において、

$Ax=b$が解を持つ　⇔　bが$Col(A)$に含まれている　$b\in Col(A)$

である。従って、$Col(A)=\{b\in\mathbb{R}^m | Ax=b, x\in\mathbb{R}^n\}$とも書ける。

また、以下の関係がある。

１　$Col(A)=\mathbb{R}^n$　⇔　どのようなbでも解が存在する

２　$Col(A)\neq\mathbb{R}^n$　⇔　$b\in Col(A)$　なら解がある。解の個数は無限大

証明

今、実数の要素からなる行列Aを$A=[\overrightarrow{V_1},\overrightarrow{V_2},,,\overrightarrow{V_n}]$　　$\overrightarrow{V_i}\in\mathbb{R}^n$

とする。列空間は、$Col(A)=span(\overrightarrow{V_1},\overrightarrow{V_2},,,\overrightarrow{V_n})$である。よって、

$$c_1\overrightarrow{V_1}+c_2\overrightarrow{V_2}+\cdots+c_n\overrightarrow{V_n}\in Col(A)\qquad(式８－７)$$

である。ここで、$Ax=b$ を考えると、

$$Ax=[\overrightarrow{V_1},\overrightarrow{V_2},,,\overrightarrow{V_n}]\begin{bmatrix}x_1\\ x_2\\ \vdots\\ x_n\end{bmatrix}=x_1\overrightarrow{V_1}+x_2\overrightarrow{V_2}+\cdots+x_n\overrightarrow{V_n}\quad(式８－８)$$

であり、式８－７と比べれば、

$\therefore Ax\in Col(A)$　　となる。

従って、$b\in Col(A)$　であれば、$Ax=b$は解が存在する。

$b \notin Col(A)$　であれば、$Ax = b$は解はない

次に、$m \times n$の行列A とするとき、n元連立一次方程式$Ax = b$が解を持つかを検討する。

$rank(A) \neq rank(A|b)$ の時、解なし

$rank(A) = rank(A|b)$ の時、解あり

$n = rank(A)$ならば、解は唯一

$n > rank(A)$ならば、零空間の基底と特殊解で表現可

より詳細には、$n - rank(A)$の個数の(基底*free variable)+特殊解の形式で表現可能

$b = 0$であれば、$rank(A) = rank(A|b)$ であり、必ず解がある（零空間）。

８－６）方法２の補足説明

（以下は、シドニー大の資料　Column Space Basis https://www.maths.usyd.edu.au/u/geoffp/lm-ss/lectp11.pdf の例を元にしている）

「行基本変形は、列間の依存関係（一次独立性）を保存する」ことの説明

$$G = \begin{bmatrix} 1 & 4 & -1 & 6 & 4 & 5 \\ 0 & -1 & 1 & 5 & 6 & 6 \\ 4 & 2 & 10 & -4 & 2 & 6 \\ 1 & 0 & 3 & 0 & 2 & 3 \end{bmatrix}$$ を考える。

Gの RREF を求める。

$$G \sim G_{RREF} = \begin{bmatrix} 1 & 0 & 3 & 0 & 2 & 3 \\ 0 & 1 & -1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$　（式８－９）

G_{RREF}の列をC_{R1}，C_{R2},,，C_{R6}とすると、

$$C_{R3} = 3C_{R1} - C_{R2}$$
$$C_{R5} = 2C_{R1} - C_{R2} + C_{R4}$$　（式８－１０）
$$C_{R6} = 3C_{R1} - C_{R2} + C_{R4}$$

が成立する。すなわち、C_{R3}，C_{R5}，C_{R6}はC_{R1}，C_{R2}，C_{R4}の線形結合で表現される。（leading entry を持つピボット列は一次独立である。ガウス消去法は一次独立な列を見つけていることに相当する）

式８－９より、G_{RREF}の列空間は、

$$Col(G_{RREF}) = span\left(\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}\right)$$　（式８－１１）

となる。C_{R1}，C_{R2}，C_{R4}は基底ベクトルである。

一方、元の行列Gの列をC_{O1}，C_{O2},,，C_{O6}とすると、列間に全く同じ関係、すなわち

$$C_{O3} = 3C_{O1} - C_{O2}$$
$$C_{O5} = 2C_{O1} - C_{O2} + C_{O4}$$　（式８－１２）
$$C_{O6} = 3C_{O1} - C_{O2} + C_{O4}$$

が成立している。つまり、行基本変形は、列間の依存関係（一次独立性）を保存している。C_{O1}，C_{O2}，C_{O4}は一次独立であり、また、Gの列空間は、C_{O1}，C_{O2}，C_{O4}で表現できる。つまり、

$$Col(G) = span(C_{O1}, C_{O2}, C_{O4}) = span\left(\begin{bmatrix}1\\0\\4\\1\end{bmatrix}, \begin{bmatrix}4\\-1\\2\\0\end{bmatrix}, \begin{bmatrix}6\\5\\-4\\1\end{bmatrix}\right) \quad （式８－１３）$$

である。すなわち、G_{RREF}の列空間の基底ベクトル（C_{R1}，C_{R2}，C_{R4}）に対応する、元の行列Gの列（C_{O1}，C_{O2}，C_{O4}）が、列空間の基底ベクトルとなる。

上記は RREF で議論したが、REF でも同じ議論が可能である。また、$Col(G_{RREF}) \neq Col(G)$である。（第 4 項目を考えれば容易に分かる）

「行基本変形は列ベクトルの線形関係を保存する」ことの証明は、以下などにもある。

理数アラカルト　http://risalc.info/src/elementary-row-operations.html

９）ベクトル空間詳細

線形空間とも呼ばれる。（アリゾナ大の資料 Fields and vector spaces/ definitions and examples https://www.math.arizona.edu/~cais/223Page/hout/236w06fields.pdf が良い参考になる）

９－１）定義

・体Fを定義する。

（このとき、集合とともに、加法（体加法$+_F$）、乗法（体乗法$*_F$）が定義される。）

・ベクトルに関する２つの２項演算を定義する。

$+_V$：ベクトル加法(vector addition)、$*_V$：スカラー乗法(scalar multiplication)

・$+_F: F \times F \longrightarrow F$　　$*_F : F \times F \longrightarrow F$　　$+_V: V \times V \longrightarrow V$　　$*_V : F \times V \longrightarrow V$　であることに注意せよ。ここで、例えば$*_V : F \times V \longrightarrow V$とは、演算$*_V$の２引数がそれぞれ$F$と$V$に属しており、演算結果が$V$に属すことを意味している。このことを明確にするために、$*_V$は$*_{FVV}$と表現した方がよい。$+_F$と$+_V$を区別なしに+で表現している文献が多い。演算の引数と結果の形式を意識して区別することが重要である。

・以下見やすさのため、$+_F$を+、$*_F$を*、$+_V$を$\oplus$　、$*_V$を×　と表現することとする。

・集合Vが以下の（１）～（１０）を満たすとき、Vを体F上のベクトル空間と言う。

（１）ベクトル加法：閉塞性が成立　　$\forall u \in V,\ \forall v \in V,\ u \oplus v \in V$

（２）ベクトル加法：結合則が成立　　$\forall u \in V,\ \forall v \in V,\ \forall \mathrm{w} \in V\ \ (u \oplus v) \oplus w = u \oplus (v \oplus w)$

（３）ベクトル加法：可換則が成立　　$\forall u \in V,\ \forall v \in V,\ u \oplus v = v \oplus u$

（４）ベクトル加法：恒等元が存在　　$\forall u \in V,\ \exists e \in V,\ u \oplus e = u$　e:0 元と呼ぶ

（５）ベクトル加法：逆元が存在　　$\forall u \in V,\ \exists v \in V,\ u \oplus v = e$

（６）スカラー乗法：閉塞性が成立　$\forall u \in V,\ \forall a \in F,\ a \times u \in V$

（７）スカラー乗法：結合則が成立　$\forall u \in V,\ \forall a \in F,\ \forall b \in F,\ a \times (b \times u) = (a * b) \times u$

（８）スカラー乗法：恒等元が存在　$\forall u \in V,\ \exists e \in F,\ e \times u = u$

（９）ベクトル加法、スカラー乗法：分配則１が成立

$\forall u \in V,\ \forall v \in V,\ \forall a \in F,\ a \times (u \oplus v) = a \times u \oplus a \times v$

（１０）ベクトル加法、スカラー乗法：分配則２が成立

$\forall u \in V,\ \forall a, b \in F,\ (a + b) \times u = a \times u \oplus b \times u$

（１）－（５）をまとめると、ベクトル加法は可換群（アーベル群）をなすと言える。

（６）－（８）は、スカラー乗法は可換群から可換則と逆元を除いた性質を持つと言える。

参考

閉塞性：closure	結合則：associative law	可換則：commutative law
恒等元：identity	逆元：inverse	分配則：distributive law

ベクトル空間の定義は、数値ベクトル以外にも適用できる。例えば、行列、多項式などである。従って、一般的に記述する場合、矢印ではなく太文字が使用される。

９－２）例

集合とともに、体、ベクトル加法の定義、スカラー乗法の定義がなされる必要がある。ときに自

明のときはこれらが省略されていることがあるので注意する。

1）$\mathbb{R}^n=\{(x_1,x_2,,,,x_n)|x_i\in\mathbb{R}\}$　　n 次元実数ベクトル

実数体$\mathbb{R}$　（$+_F$ $*_F$が定義されている）

ベクトル加法$+_V$の定義　$(x_1,x_2,,,,x_n)+_V(y_1,y_2,,,,y_n)\triangleq(x_1+_Fy_1,\ x_2+_Fy_2,,,,x_n+_Fy_n)$

スカラー乗法$*_V$の定義　$k*_V(x_1,x_2,,,,x_n)\triangleq(k*_Fx_1,\ k*_Fx_2,,,,k*_Fx_n)$

これらの定義の元、$\mathbb{R}^n$はベクトル空間となる

2）$M_n(\mathbb{R})=\left\{\begin{bmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\a_{21}&a_{22}&\cdots&a_{2n}\\\vdots&\vdots&\vdots&\vdots\\a_{n1}&a_{n2}&\cdots&a_{nn}\end{bmatrix}\middle|\middle|\ n\in\mathbb{N}\setminus0,\ a_{ij}\in\mathbb{R},\ 1\le i,j\le n,\ i,j\in\mathbb{N}\setminus0\right\}$　実n次元正方行列

ここで、$\mathbb{N}\setminus0$とは、集合$\mathbb{N}$から０を除いた集合を意味している。

実数体$\mathbb{R}$　（$+_F$ $*_F$が定義されている）

ベクトル加法$+_V$の定義

$$\begin{bmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\a_{21}&a_{22}&\cdots&a_{2n}\\\vdots&\vdots&\vdots&\vdots\\a_{n1}&a_{n2}&\cdots&a_{nn}\end{bmatrix}+_V\begin{bmatrix}b_{11}&b_{12}&\cdots&b_{1n}\\b_{21}&b_{22}&\cdots&b_{2n}\\\vdots&\vdots&\vdots&\vdots\\b_{n1}&b_{n2}&\cdots&b_{nn}\end{bmatrix}\triangleq\begin{bmatrix}a_{11}+_Fb_{11}&a_{12}+_Fb_{12}&\cdots&a_{1n}+_Fb_{1n}\\a_{21}+_Fb_{21}&a_{22}+_Fb_{22}&\cdots&a_{21}+_Fb_{21}\\\vdots&\vdots&\vdots&\vdots\\a_{n1}+_Fb_{n1}&a_{n2}+_Fb_{n2}&\cdots&a_{nn}+_Fb_{nn}\end{bmatrix}\quad（式\ 9-1）$$

スカラー乗法$*_V$の定義

$$k*_V\begin{bmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\a_{21}&a_{22}&\cdots&a_{2n}\\\vdots&\vdots&\vdots&\vdots\\a_{n1}&a_{n2}&\cdots&a_{nn}\end{bmatrix}\triangleq\begin{bmatrix}k*_Fa_{11}&k*_Fa_{12}&\cdots&k*_Fa_{1n}\\k*_Fa_{21}&k*_Fa_{22}&\cdots&k*_Fa_{2n}\\\vdots&\vdots&\vdots&\vdots\\k*_Fa_{n1}&k*_Fa_{n2}&\cdots&k*_Fa_{nn}\end{bmatrix}\quad（式\ 9-2）$$

これらの定義の元、$M_n(\mathbb{R})$はベクトル空間となる

3）$\mathbb{R}^\infty=\{(x_1,x_2,,,,)|x_i\in\mathbb{R}\}$　無限次元の実数ベクトル

実数体$\mathbb{R}$　（$+_F$ $*_F$が定義されている）

~~4）$F=\{(x_1,x_2,,,,)\in\mathbb{Z}^\infty|x_1=0,x_2=1,x_{i+2}=x_i+x_{i+1},\ i\ge1,\ x_i\in\mathbb{Z},\ i\in\mathbb{N}\setminus0\}$フィボナッチ数列~~

~~整数$\mathbb{Z}$　（$+_F$が定義されている）~~

5）$C^0=\{f|f(x):\mathbb{R}\to\mathbb{R}\ の写像,\ x\in\mathbb{R}\}$　C^0級の関数

6）$C^1=\{f\in C^0\mid\exists f'(x)\in C^0\}$　一回微分可能なC^1級の関数

7）$Poly_d=\{f(x)\in C^1\mid f(x)=\sum_{i=0}^d c_ix^i,c_i\in\mathbb{R}\}$　d次元以下のC^1級の多項式関数

5）の説明

・以下、()は関数の引数を示し、[]はくくりを意味する。

・体として実数体$\mathbb{R}$（$+_F$ $*_F$が定義されている）を考える。以下見やすさのため、$+_F$を+、$*_F$を*と表現する。

・ベクトル（関数）の同値関係を定義する。

ベクトルfとgが同値（≡で表現）であるとは、それらが引数として取るxの定義域全体において値が同一であることと定義する。

#0 $f\equiv g\ \triangleq\ f(x)=g(x)$　（式９－３）

・ベクトル加法$+_V$を定義する。以下見やすさのため、$+_V$を$\oplus$と表現する。

$f\in C^0$、$g\in C^0$　とするとき、以下をベクトル加法と定義する。

#1 $[f\oplus g](x)\ \triangleq\ f(x)+g(x)\in\mathbb{R}$　（式９－４）

２つのベクトルの和のxの写像は、各ベクトルのxの写像の和となっている。

つまり、ベクトル加法$\oplus$を、実数体へ写像した値の体加法+で定義している。

・スカラー乗法$*_V$を定義する。以下見やすさのため、$*_V$を×と表現する。

$f \in C^0$、$k \in F$　とするとき、以下をスカラー乗法と定義する。

#2 $[k \times f](x) \triangleq k * f(x) \in \mathbb{R}$　（式９－５）

kを乗算したベクトルのxの写像は、ベクトルのxの写像のk倍となっている。

つまり、スカラー乗法×を、スカラーと実数体へ写像した値との体乗法*で定義している。

（５－１）ベクトル加法：閉塞性の確認

$f, g \in C^0$のとき、　$f \oplus g \in C^0$　を示したい。左辺の関数のxの定義域における値を考える（形式的には、左辺に(x)を追加する。）

$[f \oplus g](x) = f(x) + g(x)$　（#1 ベクトル加法の定義より）

$\in \mathbb{R}$

すなわち、$f \oplus g$は$x \in \mathbb{R}$を$f(x) + g(x) \in \mathbb{R}$へ写像する。つまり、$\mathbb{R} \to \mathbb{R}$の写像であり、$C^0$の定義に当てはまる。よって、$f \oplus g \in C^0$である。

（５－２）ベクトル加法：結合則

$f, g, h \in C^0$のとき、$[f \oplus g] \oplus h \equiv f \oplus [g \oplus h]$を示したい。左辺の関数の$x$の定義域における値を考える（形式的には、左辺に$(x)$を追加する。）

$[[f \oplus g] \oplus h](x) = [f \oplus g](x) + h(x)$　（#1 ベクトル加法の定義より）

$= f(x) + g(x) + h(x)$　（#1 ベクトル加法の定義より。

体加法（実数の和）だけになっていることに注意

$= f(x) + [g(x) + f(x)]$　（体加法は結合則を満たすため）

$= f(x) + [g \oplus h](x)$　（#1 ベクトル加法の定義より（逆））

$= [f \oplus [g \oplus h]](x)$　（#1 ベクトル加法の定義より（逆））

すなわち、xの定義域において値が同一である。ベクトルの同値関係#0 より、

$[f \oplus g] \oplus h \equiv f \oplus [g \oplus h]$　（形式的には、両辺から(x)を取り除いている）

よって成立

（５－３）ベクトル加法：可換則

$f, g \in C^0$のとき、$f \oplus g \equiv g \oplus f$を示したい。左辺の関数の$x$の定義域における値を考える（形式的には、左辺に$(x)$を追加する。）

$[f \oplus g](x) = f(x) + g(x)$　（#1 ベクトル加法の定義より）

$= g(x) + f(x)$　（体加法は可換則を満たすため）

$= [g \oplus f](x)$　（#1 ベクトル加法の定義より（逆））

すなわち、xの定義域において値が同一である。ベクトルの同値関係#0 より、

$f \oplus g \equiv g \oplus f$　（形式的には、両辺から(x)を取り除いている）

よって成立

（５－４）ベクトル加法：恒等元

どのようなxに対しても常に 0 を返す関数を$O \in C^0$とする。$\forall x\ O(x) = 0$

（Oは、関数の一つであり 0 というスカラーではないことに注意）

$[f \oplus O](x) = f(x) + O(x)$　（#1 ベクトル加法の定義より）

$= f(x) + 0$　（$O(x)$の定義より）

$= f(x)$　（体加法には恒等元が存在しその値は 0 である）

すなわち、xの定義域において値が同一である。ベクトルの同値関係#0 より、

$f \oplus O = f$　（形式的には、両辺から(x)を取り除いている）

よって成立

（５－５）ベクトル加法：逆元

まず、$g \in C^0$を考える。

$[f \oplus g](x) = f(x) + g(x)$　（#1 ベクトル加法の定義より）

$= 0$　（体加法は逆元を持つ。従って、結果が 0 となる$g(x)$が存在する）

$= O(x)$

すなわち、xの定義域において値が同一である。ベクトルの同値関係#0 より、

$f \oplus g = O$　となるgが存在する。

（形式的には、両辺から(x)を取り除いている）

よって成立

（５－６）スカラー乗法：閉塞性

$f \in C^0$、$k \in F$　のとき、　$k \times f \in C^0$　を示したい。左辺の関数のxの定義域における値を考える（形式的には、左辺に(x)を追加する。）

$[k \times f](x) = k * f(x)$　（#2 スカラー乗法の定義より）$\in \mathbb{R}$

すなわち、$k \times f$は$x \in \mathbb{R}$を$k * f(x) \in \mathbb{R}$へ写像する。つまり、$\mathbb{R} \to \mathbb{R}$の写像であり、$C^0$の定義に当てはまる。よって、$k \times f \in C^0$である。

（５－７）スカラー乗法：結合則

$\forall f \in V,\ \forall k, l \in F$

$k \times [l \times f] \equiv [k * l] \times f$ を示したい。左辺の関数のxの定義域における値を考える（形式的には、左辺に(x)を追加する。）

$\big[k \times [l \times f]\big](x) = k * [l \times f](x)$　（#2 スカラー乗法の定義より）

$= k * [l * f(x)]$　（#2 スカラー乗法の定義より）

$= k * l * f(x)$　（体乗法は結合則を満たすため）

$= [k * l] * f(x)$　（体乗法は結合則を満たすため）

$= \big[[k * l] \times f\big](x)$（#2 スカラー乗法の定義より（逆））

すなわち、xの定義域において値が同一である。ベクトルの同値関係#0 より、

$k \times [l \times f] \equiv [k * l] \times f$　（形式的には、両辺から(x)を取り除いている）

よって成立

（５－８）スカラー乗法：恒等元が存在

$\forall f \in V,\ \exists e \in F$

$e \times f \equiv f$ となるeが存在することを示したい。左辺の関数のxの定義域における値を考える（形式的には、左辺に(x)を追加する。）

$[e \times f](x) = e * f(x)$　（#2 スカラー乗法の定義より）

$= f(x)$　（体乗法には恒等元が存在しその値は 1 である。従って$e = 1$が存在する）

すなわち、xの定義域において値が同一である。ベクトルの同値関係#0 より、

$e \times f \equiv f$　（形式的には、両辺から(x)を取り除いている）

よって成立

（５－９）ベクトル加法、スカラー乗法：分配則１

$\forall f,g \in V,\ \forall k \in F$

$k \times [f \oplus g] \equiv k \times f \oplus k \times g$　を示したい。左辺の関数のxの定義域における値を考える（形式的には、左辺に(x)を追加する。）

$[k \times [f \oplus g]](x) = k * [f \oplus g](x)$　（#2 スカラー乗法の定義より）

$= k * [f(x) + g(x)]$　#1 ベクトル加法の定義より）

$= k * f(x) + k * g(x)$　（体加法・体乗法は分配則を満たすため）

$= [k \times f](x) + [k \times g](x)$（#2 スカラー乗法の定義より（逆））

$= [k \times f \oplus k \times g](x)$　（#1 ベクトル加法の定義より（逆））

すなわち、xの定義域において値が同一である。ベクトルの同値関係#0 より、

$k \times [f \oplus g] \equiv k \times f \oplus k \times g$（形式的には、両辺から$(x)$を取り除いている）

よって成立

（５－１０）ベクトル加法、スカラー乗法：分配則２

$\forall f \in V,\ \forall k,l \in F$

$[k + l] \times f \equiv k \times f \oplus l \times f$　を示したい。左辺の関数のxの定義域における値を考える（形式的には、左辺に(x)を追加する。）

$[[k + l] \times f](x) = [k + l] * f(x)$　（#2 スカラー乗法の定義より）

$= k * f(x) + l * f(x)$　（体加法・体乗法は分配則が成立）

$= [k \times f](x) + [l \times f](x)$　（#2 スカラー乗法の定義より（逆））

$= [k \times f \oplus l \times f](x)$　（#1 ベクトル加法の定義より（逆）

すなわち、xの定義域において値が同一である。ベクトルの同値関係#0 より、

$[k + l] \times f \equiv k \times f \oplus l \times f$（形式的には、両辺から$(x)$を取り除いている）

以上、（５－１）～（５－１０）によって成立

９－３）ベクトル空間と体

上記は、体F上でのベクトル空間を論じた。ベクトル空間の定義と体の定義が似ているため、この両者を議論する場合がある。

体

演算として、加法、乗算が定義される。

加法：閉塞性、結合則、恒等元、逆元、可換則　（可換群）

乗法：閉塞性、結合則、可換則、恒等元、（加法の恒等元 0 以外は逆元）（0 以外は可換群）

加法・乗法：分配則

ベクトル空間と体の違い

ベクトル空間は、スカラー乗法の係数がベクトル空間外の体の要素を用いる。一方、体は内部で閉じている。

１０）その他（部分空間、固有値など）

１０－１）部分空間

（１０－１－１）定義

まず、ベクトル空間Vを考える。（集合Vがベクトル空間である　⇔　ベクトル加法$\oplus$、スカラー乗法$*$、体Fが定義され、閉塞性、結合則、可換則、分配則等の１－１０の性質が成立する）

「ある集合Wがベクトル空間Vの部分空間である」　とは、Wが以下の性質を満たすことである。

・Wがベクトル空間Vの部分集合であること　　$W \subseteq V$

・Wがベクトル空間であること

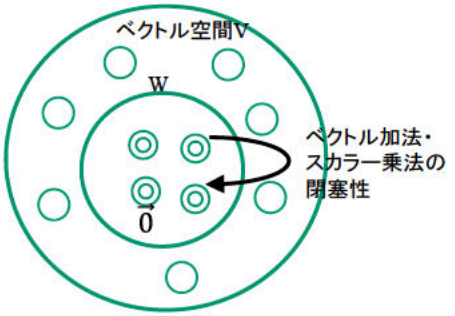
従って、厳密には、Wが体FのVの部分空間であることを確認するためには、すべての条件を調べることとなるが、多くの場合は、

・Wがベクトル加法$\oplus$の元に閉じている　　$a, b \in W$のとき、$a \oplus b \in W$

・Wがスカラー乗法$\times$の元に閉じている　　$a \in W, k \in F$のとき、$k \times a \in W$

・Wに０元が存在する

を調べれば十分である。念のため、ベクトル加法$\oplus: V \times V \to V$、スカラー乗法$\times: F \times V \to V$　であることを再度指摘する。



（１０－１－２）例

以下の例では、実数体$\mathbb{R}$を考える。ベクトル加法$+_V$、スカラー乗法$*_V$を以下のように定義する。

実数体$\mathbb{R}$　（$+_F$ $*_F$が定義されている）

ベクトル加法$+_V$の定義　$(a,b,c) +_V (d,e,f) \triangleq (a+_F d,\ b+_F e,\ c+_F f)$

スカラー乗法$*_V$の定義　$k *_V (a,b,c) \triangleq (k *_F a,\ k *_F b,\ k *_F c)$

（以下見やすさのため、$+_F$= +、$*_F$=*、$+_V$= $\oplus$、$*_V$=×　と表現することとする）

A) $S = \{(x,y) | y = 2x, x \in \mathbb{R}, y \in \mathbb{R}\}$　Sは$\mathbb{R}^2$の部分空間である。

証明：

１）ベクトル加法の閉塞性

$u_1 = (x_1, y_1) \in S, u_2 = (x_2, y_2) \in S$ のとき、$u_1 \oplus u_2 = (x_1 + x_2, y_1 + y_2) \in S$

$\because y_1 + y_2 = 2(x_1 + x_2)$

２）スカラー乗法の閉塞性

$u = (x,y) \in S, k \in \mathbb{R}$ のとき、$k \times u = (k * x, k * y) \in S$ $\because k * y = 2 * k * x$

３）０元の存在

$x = y = 0$のとき、０元$(0, 0)$となる。

B) $S = \{(x,y) | y = x^2, x \in \mathbb{R}, y \in \mathbb{R}\}$　　Sは$\mathbb{R}^2$の部分空間ではない。

証明：

１）ベクトル加法の閉塞性

$u_1 = (x_1, y_1) \in S, u_2 = (x_2, y_2) \in S$ のとき、$u_1 \oplus u_2 = (x_1 + x_2, y_1 + y_2) \notin S$

$\because y_1 + y_2 \neq (x_1 + x_2)^2$

２）スカラー乗法の閉塞性

$u = (x,y) \in S, k \in \mathbb{R}$ のとき、$k \times u = (k * x, k * y) \notin S$ $\because k * y \neq (k * x)^2$

３） ０元の存在

$x = y = 0$のとき、０元$(0, 0)$となる。

例からわかるように、n次元実数ベクトル$\mathbb{R}^n$に対し、原点を含む 直線、平面は、部分空間である。ベクトル空間V自身や零元だけから成る集合はVの部分空間である。これを自明な部分空間という。従って、どのベクトル空間も必ず２つの部分空間を持つ。

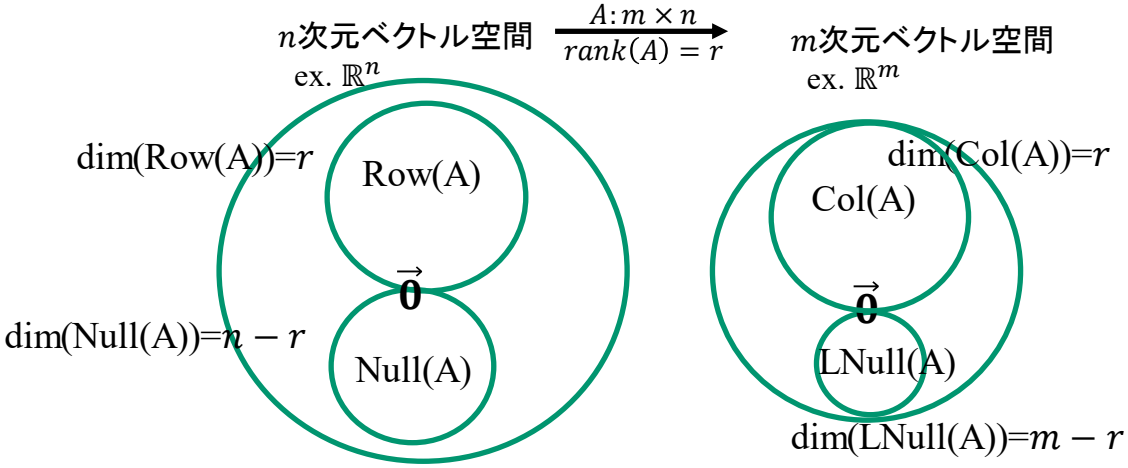
（１０－１－３）行列で定義される部分空間

（１）　$m \times n$の行列Aに対して、行空間（row space）、列空間（column space）、零空間（null space）、左零空間（left null space）の４つの部分空間が定義される。

零空間$Null(A)$と行空間$Row(A)$は直交する。$Null(A) \perp Row(A)$

左零空間$LNull(A)$と列空間$Col(A)$は直交する。$LNull(A) \perp Col(A)$

$LNull(A) = Null(A^T)$、$Col(A) = Row(A^T)$　である。



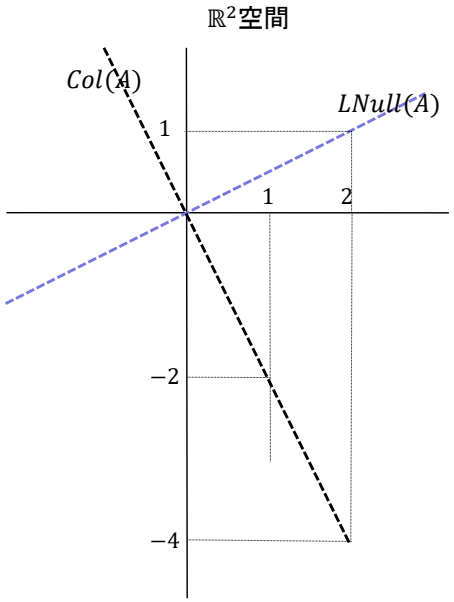
$r = n = m$のとき、$dm\big(Null(A)\big) = 0$ つまり、$Null(A) = \{\vec{0}\}$ である。

つまり、$Ax = 0$　となるxは、０ベクトルだけである。

$Ax = b$は一意に求まる。

（２）行空間、列空間、零空間、左零空間の関係

（この例は Khan academy の youtube, Row sapce and left null space, https://www.youtube.com/watch?v=qBfc57x_RSg から）



$$A = \begin{bmatrix} 2 & -1 & -3 \\ -4 & 2 & 6 \end{bmatrix} \sim \begin{bmatrix} 1 & -\frac{1}{2} & -\frac{3}{2} \\ 0 & 0 & 0 \end{bmatrix}$$

$$Row(A) = span\left(\begin{bmatrix} 1 \\ -\frac{1}{2} \\ -\frac{3}{2} \end{bmatrix}\right) = span\left(\begin{bmatrix} 2 \\ -1 \\ -3 \end{bmatrix}\right) \subset \mathbb{R}^3$$

$$Null(A) = span\left(\begin{bmatrix} \frac{1}{2} \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} \frac{3}{2} \\ 0 \\ 1 \end{bmatrix}\right) \subset \mathbb{R}^3$$

$$Col(A) = span\left(\begin{bmatrix} 2 \\ -4 \end{bmatrix}\right) \subset \mathbb{R}^2$$

$$LNull(A) = span\left(\begin{bmatrix} 2 \\ 1 \end{bmatrix}\right) \subset \mathbb{R}^2$$

$Col(A) \perp LNull(A)$　$\begin{bmatrix} 2 \\ -4 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 1 \end{bmatrix} = 0$　　直交する２直線（図）

$Row(A) \perp Null(A)$ $\begin{bmatrix}2\\-1\\-3\end{bmatrix}\cdot\begin{bmatrix}\frac{1}{2}\\1\\0\end{bmatrix}=0$ $\begin{bmatrix}2\\-1\\-3\end{bmatrix}\cdot\begin{bmatrix}\frac{3}{2}\\0\\1\end{bmatrix}=0$ 直交する直線と平面

・体 F の拡大体は、F 上のベクトル空間である。

$GF(2)$の拡大体$GF(2^3)$を考える。$GF(2)=\{0,1\}$ $GF(2^3)=\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6\}$

ベクトル加法$+_V$ 閉塞性、結合則、可換則、恒等元、逆元　成立

スカラー乗法$*_V$ 閉塞性、結合則、恒等元　成立

$+_V$,$*_V$ 分配則１、分配則２　成立

１０－２）固有値、固有ベクトル

（１０－２－１）定義

$Ax = \lambda x$ となるλ を固有値、x を固有ベクトルと言う。

（１０－２－２）固有値、固有ベクトルの求め方

まず、固有値を求める。

$Ax - \lambda x = 0$　が成立するためには、$|A| = 0$。

$A = \begin{bmatrix} 5 & 3 \\ 4 & 9 \end{bmatrix}$　とする。

$|A| = (5-\lambda)(9-\lambda) - 12 = (\lambda - 3)(\lambda - 11) = 0$

よって、$\lambda = 3, 11$

$\lambda = 3$ に対応する固有ベクトルは、

$$Ax - \lambda x = \begin{bmatrix} 2 & 3 \\ 4 & 6 \end{bmatrix} x = \begin{bmatrix} 2x_1 & 3x_2 \\ 4x_1 & 6x_2 \end{bmatrix} = \begin{bmatrix} 2x_1 + 3x_2 \\ 4x_1 + 6x_2 \end{bmatrix} = 0$$

$x_1 = t$　とすれば、$x_1 = t$、$x_2 = -\frac{2}{3}t$。よって、固有ベクトル（の一つ）は、$\begin{bmatrix} 3 \\ -2 \end{bmatrix}$。

$\lambda = 11$ に対応する固有ベクトルは、

$$Ax - \lambda x = \begin{bmatrix} -6 & 3 \\ 4 & -2 \end{bmatrix} x = \begin{bmatrix} -6x_1 & 3x_2 \\ 4x_1 & -2x_2 \end{bmatrix} = \begin{bmatrix} -6x_1 + 3x_2 \\ 4x_1 - 2x_2 \end{bmatrix} = 0$$

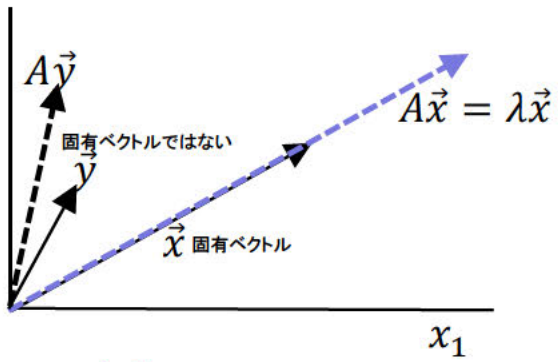
$x_1 = t$　とすれば、$x_1 = t$、$x_2 = 2t$。よって、固有ベクトル（の一つ）は、$\begin{bmatrix} 1 \\ 2 \end{bmatrix}$。

（２－３）固有値、固有ベクトルの意味

$Ax = \lambda x$ とは、x をA で写像したベクトルAxは、xのλ倍であることである。つまり、方向は変わらず長さがλ倍となることを意味している。

上の例で固有値$\lambda = 3$、固有ベクトル$\begin{bmatrix} 3 \\ -2 \end{bmatrix}$

$$A\begin{bmatrix} 3 \\ -2 \end{bmatrix} = \begin{bmatrix} 5 & 3 \\ 4 & 9 \end{bmatrix}\begin{bmatrix} 3 \\ -2 \end{bmatrix} = \begin{bmatrix} 9 \\ -6 \end{bmatrix} = 3\begin{bmatrix} 3 \\ -2 \end{bmatrix} = 3x$$



１０－３）テンソル

０次テンソル　＝　スカラー、数値　　0　100 3.14 など

１次テンソル　＝　ベクトル　(0, 3) (-3, 5)など

２次テンソル　＝　行列　$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix}$　など

３次テンソル　＝　３次元の行列

ｎ次テンソル　＝　多次元配列

(p, q)型テンソル T　　(p+q)次元配列

T: $V^* \times V^* \times \cdots \times V^* \times V \times V \times \cdots \times V$　V^*がp個、Vがq個。

力 F と加速度 a の関係は(1, 1)型テンソルで説明が可能

テンソル　延びる物、応力を発生する物

１０－４）ベクトル空間とフーリエ展開

１０－５）アフィン空間
線形空間（ベクトル空間）Ax=b　は、０を中心としていた。0 以外の点を中心となるように平行移動させた空間をアフィン空間と呼ぶ。

１１）練習問題

問１）Col(A), Row(A), Null(A)　の問題

次の行列Aを考える。$A=\begin{bmatrix}1&1&1&1\\2&1&4&3\\3&4&1&2\end{bmatrix}$

問１－１）A の RREF を求めよ。

$$A=\begin{bmatrix}1&1&1&1\\2&1&4&3\\3&4&1&2\end{bmatrix}\sim\begin{bmatrix}1&1&1&1\\2&1&0&0\\3&0&1&0\end{bmatrix}\sim\begin{bmatrix}\mathbf{1}&0&3&2\\0&\mathbf{1}&-2&-1\\0&0&0&0\end{bmatrix}$$

問１－２）Aの零空間を求めよ。

$$Null(A)=Null(rref(A))=span\left(\begin{bmatrix}-3\\2\\1\\0\end{bmatrix},\begin{bmatrix}-2\\1\\0\\1\end{bmatrix}\right)\quad 式９－１$$

なぜならば、

$$\begin{bmatrix}\mathbf{1}&0&3&2\\0&\mathbf{1}&-2&-1\\0&0&0&0\end{bmatrix}\begin{bmatrix}x_1\\x_2\\x_3\\x_4\end{bmatrix}=\begin{bmatrix}x_1+3x_3+2x_4\\x_2-2x_3-x_4\\0\end{bmatrix}=\begin{bmatrix}0\\0\\0\end{bmatrix}$$

$$x_1+3x_3+2x_4=0$$

$$x_2-2x_3-x_4=0$$

であるので、free variable (non-pivot variable)を x_3, x_4とすれば、

$$x_1=-3x_3-2x_4$$

$$x_2=2x_3+x_4$$

$$\begin{bmatrix}x_1\\x_2\\x_3\\x_4\end{bmatrix}=\begin{bmatrix}-3&-2\\2&1\\1&0\\0&1\end{bmatrix}\begin{bmatrix}x_3\\x_4\end{bmatrix}=\begin{bmatrix}-3\\2\\1\\0\end{bmatrix}x_3+\begin{bmatrix}-2\\1\\0\\1\end{bmatrix}x_4$$

であるからである。

問１－３）Aの行空間を求めよ。

Aによって構成される行空間$Row(A)$（の一つ）は、行ベクトルを列挙すればよい。（他の解もある）

$$Row(A)=span\left(\begin{bmatrix}1\\1\\1\\1\end{bmatrix},\begin{bmatrix}2\\1\\4\\3\end{bmatrix},\begin{bmatrix}3\\4\\1\\2\end{bmatrix}\right)$$

問１－４）Aの行空間の基底を求めよ。

行空間の基底は、RREF のピボット行ベクトルである。すなわち、(1 0 3 2)(0 1 -2 -1)。従って、行空間を以下のようにも記述できる。

$$Row(A)=span\left(\begin{bmatrix}1\\0\\3\\2\end{bmatrix},\begin{bmatrix}0\\1\\-2\\-1\end{bmatrix}\right)$$

問１－５）Aの列空間を求めよ。

Aによって構成される列空間$Col(A)$（の一つ）は、列ベクトルを列挙すればよい。（他の解もある）

$$Col(A)=span\left(\begin{bmatrix}1\\2\\3\end{bmatrix},\begin{bmatrix}1\\1\\4\end{bmatrix},\begin{bmatrix}1\\4\\1\end{bmatrix},\begin{bmatrix}1\\3\\2\end{bmatrix}\right)\quad \text{である。}$$

問１－６）Aの列空間の基底を求めよ。

問１－１で求めた RREF$\begin{bmatrix}\mathbf{1} & 0 & 3 & 2\\ 0 & \mathbf{1} & -2 & -1\\ 0 & 0 & 0 & 0\end{bmatrix}$の pivot 列に相当するオリジナルの列、$\begin{bmatrix}1\\2\\3\end{bmatrix},\begin{bmatrix}1\\1\\4\end{bmatrix}$が$Col(A)$の基底ベクトルとなる。

$$Col(A) = \text{span}\left(\begin{bmatrix}1\\2\\3\end{bmatrix},\begin{bmatrix}1\\1\\4\end{bmatrix}\right)$$

（補足）問１－５で求めた$col(A)$の各列ベクトルが一次独立であるかを調べる。これは、

$$c_1\begin{bmatrix}1\\2\\3\end{bmatrix}+c_2\begin{bmatrix}1\\1\\4\end{bmatrix}+c_3\begin{bmatrix}1\\4\\1\end{bmatrix}+c_4\begin{bmatrix}1\\3\\2\end{bmatrix}=0 \iff c_1=c_2=c_3=c_4=0$$

を調べることであり、$\begin{bmatrix}1 & 1 & 1 & 1\\ 2 & 1 & 4 & 3\\ 3 & 4 & 1 & 2\end{bmatrix}\begin{bmatrix}c_1\\c_2\\c_3\\c_4\end{bmatrix}=\begin{bmatrix}0\\0\\0\end{bmatrix}$の解$\begin{bmatrix}c_1\\c_2\\c_3\\c_4\end{bmatrix}$が$\begin{bmatrix}0\\0\\0\\0\end{bmatrix}$であることを示すことと等価である。

つまり、Aの零空間が$\{\vec{0}\}$であること、すなわち零ベクトルしか存在しないことを証明することである。実は、これについては既に問１－２で求められている。つまり、Aの零空間の基底は、２つの基底ベクトルで張られており、零空間は$\{\vec{0}\}$ではない。従って、$Col(A)$の各列ベクトルは独立ではない。以上より、$\begin{bmatrix}1\\2\\3\end{bmatrix},\begin{bmatrix}1\\1\\4\end{bmatrix},\begin{bmatrix}1\\4\\1\end{bmatrix},\begin{bmatrix}1\\3\\2\end{bmatrix}$は基底ではない。

次に、$Col(A)$の基底を検討する。つまり、$\begin{bmatrix}1\\2\\3\end{bmatrix},\begin{bmatrix}1\\1\\4\end{bmatrix},\begin{bmatrix}1\\4\\1\end{bmatrix},\begin{bmatrix}1\\3\\2\end{bmatrix}$を必要十分に表現可能な列ベクトルを決定する。例えば、$\begin{bmatrix}1\\3\\2\end{bmatrix}$が$\begin{bmatrix}1\\2\\3\end{bmatrix},\begin{bmatrix}1\\1\\4\end{bmatrix},\begin{bmatrix}1\\4\\1\end{bmatrix}$の線形結合で表現できれば、$\begin{bmatrix}1\\3\\2\end{bmatrix}$は不要となる。これは、$\begin{bmatrix}1\\3\\2\end{bmatrix}=c_1\begin{bmatrix}1\\2\\3\end{bmatrix}+c_2\begin{bmatrix}1\\1\\4\end{bmatrix}+c_3\begin{bmatrix}1\\4\\1\end{bmatrix}$ となる$c_1,\ c_2,\ c_3$を見いだすことに他ならない。より一般的に言えば、

$$x_1\begin{bmatrix}1\\2\\3\end{bmatrix}+x_2\begin{bmatrix}1\\1\\4\end{bmatrix}+x_3\begin{bmatrix}1\\4\\1\end{bmatrix}+x_4\begin{bmatrix}1\\3\\2\end{bmatrix}=0$$

となる$x_1,\ x_2,\ x_3,\ x_4$（ただし$x_1,\ x_2,\ x_3,\ x_4$はすべて 0 となってはいけない）を見つけることである。（このことは、零空間の議論と同じことをやっていることに注意する。）

今、free variable である$x_3\ x_4$を$x_3=0,\ x_4=-1$ とすると、（適当に決めた）

$x_1\begin{bmatrix}1\\2\\3\end{bmatrix}+x_2\begin{bmatrix}1\\1\\4\end{bmatrix}=\begin{bmatrix}1\\3\\2\end{bmatrix}$　　$x_1=2,\ x_2=-1$　が解となる。従って、$\begin{bmatrix}1\\3\\2\end{bmatrix}$は$\begin{bmatrix}1\\2\\3\end{bmatrix},\begin{bmatrix}1\\1\\4\end{bmatrix}$に対して従属である。

また、$x_3=-1,\ x_4=0$　とすると、

$x_1\begin{bmatrix}1\\2\\3\end{bmatrix}+x_2\begin{bmatrix}1\\1\\4\end{bmatrix}=\begin{bmatrix}1\\4\\1\end{bmatrix}$　　$x_1=3,\ x_2=-2$　が解となる。従って、$\begin{bmatrix}1\\4\\1\end{bmatrix}$は$\begin{bmatrix}1\\2\\3\end{bmatrix},\begin{bmatrix}1\\1\\4\end{bmatrix}$に対して従属である。

以上より、$Col(A)$の基底ベクトルは、$\begin{bmatrix}1\\2\\3\end{bmatrix},\begin{bmatrix}1\\1\\4\end{bmatrix}$　である。

問２）span の練習問題

$V=\mathbb{R}^3$とする。$W=span\left(\begin{bmatrix}1\\2\\1\end{bmatrix},\begin{bmatrix}3\\-1\\-4\end{bmatrix},\begin{bmatrix}0\\7\\7\end{bmatrix}\right)$ とするとき、$W=\{(x,y,z)\in V|ax+by+cz=0\}$と表現したい。$a,b,c$を求めよ。また、$W$の基底を求めよ。

（解答）

$W=span\left(\begin{bmatrix}1\\2\\1\end{bmatrix},\begin{bmatrix}3\\-1\\-4\end{bmatrix},\begin{bmatrix}0\\7\\7\end{bmatrix}\right)$

$u=\begin{bmatrix}x\\y\\z\end{bmatrix}\in W$ とすると、$u=c_1\begin{bmatrix}1\\2\\1\end{bmatrix}+c_2\begin{bmatrix}3\\-1\\-4\end{bmatrix}+c_3\begin{bmatrix}0\\7\\7\end{bmatrix}=\begin{bmatrix}x\\y\\z\end{bmatrix}$ である。従って、

$x=c_1+3c_2 \quad y=2c_1-c_2+7c_3 \quad z=c_1-4c_2+7c_3$

$$ax+by+cz=ac_1+3ac_2+2bc_1-bc_2+7bc_3+cc_1-4cc_2+7cc_3$$
$$=(a+2b+c)c_1+(3a-b-4c)c_2+(7b+7c)c_3=0$$

任意のu、つまりc_iに対してこの式が成立する必要がある。従って、この式をc_iの恒等式と見て、

$$a+2b+c=0$$
$$3a-b-4c=0$$
$$7b+7c=0$$

とする。$a=1,b=-1,c=1$ で満たされる。以上より、

$$W=\{(x,y,z)\in V|x-y+z=0\}$$

次にWの基底を求める。

$$A=\begin{bmatrix}1&3&0\\2&-1&7\\1&-4&7\end{bmatrix}\sim\begin{bmatrix}1&3&0\\0&1&-1\\0&0&0\end{bmatrix}$$

よって、

$$W=Col(A)=span\left(\begin{bmatrix}1\\2\\1\end{bmatrix},\begin{bmatrix}3\\-1\\-4\end{bmatrix}\right)$$

（(0 7 7) は(1 2 1)(3 -1 -4)の線形結合で表現可能である）

問３）部分空間の問題

問３－１）

以下で表現される集合が、$\mathbb{R}^3$の部分空間となるかをそれぞれ調べよ。

ただし、実数体$\mathbb{R}$（$+,*$が定義されている）上で議論し、以下が定義されているとする。

ベクトル加法$\oplus$の定義　$(a,b,c)\oplus(d,e,f)\triangleq(a+d,\ b+e,\ c+f)$

スカラー乗法$\times$の定義　$k\times(a,b,c)\triangleq(k*a,\ k*b,\ k*c)$

A) $S_1=\{v=(a,b,1)|a\in\mathbb{R},b\in\mathbb{R}\}$

B) $S_2=\{v=(a,0,c)|a\in\mathbb{R},c\in\mathbb{R}\}$

C) $S_3=\{v=(a,b,c)|a=b+c,a\in\mathbb{R},b\in\mathbb{R},c\in\mathbb{R}\}$

D) $S_4=\{v=(a,b,c)|a*b=0,a\in\mathbb{R},b\in\mathbb{R},\ c\in\mathbb{R}\}$

E) $S_5=\{v=(a,b,c)|a=b,a\in\mathbb{R},b\in\mathbb{R},\ c\in\mathbb{R}\}$

F) $S_6=\{v=(a,b,c)|a=b+3,a\in\mathbb{R},b\in\mathbb{R},\ c\in\mathbb{R}\}$

（解答）

S_iが部分空間であることを示すには以下が満たされることを示す。

$p1$:　Sに 0 元が含まれている

$p2$:　Sがベクトル加法の元に閉じている

$p3$:　Sがスカラー乗算の元に閉じている

A) $S_1 = \{v = (a, b, 1) | a \in \mathbb{R}, b \in \mathbb{R}\}$

・$p1$: $v = (a, b, 1) \in S_1$は、0 元となり得ない。$p1$を満たさない。

・$p2$: $v_1 = (a_1, b_1, 1) \in S_1$と$v_2 = (a_2, b_2, 1) \in S_1$を考える。$u = v_1 \oplus v_2 = (a_1, b_1, 1) \oplus (a_2, b_2, 1) = (a_1 + a_2, b_1 + b_2, 1 + 1) = (a_1 + a_2, b_1 + b_1, 2)$。　よって$u$は$(a, b, 1)$と表現できず$u \notin S_1$であり閉じていない。$p2$を満たさない。

・$p3$:　$v = k \times (a_1, b_1, 1) = (k * a_1, k * b_1, k * 1)\ k \in F$　よってvは$(a, b, 1)$と常には表現できず$v \notin S_1$であり閉じていない。$p3$を満たさない。

以上より、$p1$不成立、$p2$不成立、$p3$不成立となり、部分空間ではない。　$x = 1$の平面。

B) $S_2 = \{v = (a, 0, c) | a \in \mathbb{R}, c \in \mathbb{R}\}$

・$p1$:　$v = (a, 0, c) \in S_2$は、$a = c = 0$のとき 0 元(0,0,0)となる。従って、S_2は 0 元を持つ。$p1$を満たす。

・$p2$:　$v_1 = (a_1, 0, c_1) \in S_2$と$v_2 = (a_2, 0, c_2) \in S_2$を考える。$u = v_1 \oplus v_2 = (a_1, 0, c_1) \oplus (a_2, 0, c_2) = (a_1 + a_2, 0 + 0,\ c_1 + c_2) = (a_1 + a_2,\ 0,\ c_1 + c_2)$。　よって$u$は$(a, 0, c)$と表現できる。（体$\mathbb{R}$は体加法に関して閉じている、また 0 元がある。）$u \in S_2$であり閉じている。$p2$を満たす。

・$p3$:　$v = k \times (a_1, 0, c_1) = (k * a_1, k * 0, k * c_1) = (k * a_1, 0, k * c_1)\ k \in F$　よってvは$(a, 0, c)$と表現でき（体$\mathbb{R}$は体乗法に関して閉じている）$v \in S_2$であり閉じている。$p3$を満たす。

以上より、$p1$成立、$p2$成立、$p3$成立となり、部分空間である。$y = 0$の平面。

C) $S_3 = \{v = (a, b, c) | a = b + c, a \in \mathbb{R}, b \in \mathbb{R}, c \in \mathbb{R}\}$

・$p1$:　$v = (a, b, c) \in S_3$（ただし$a = b + c$)は、$a = 0, b = 0, c = 0$のとき$a = b + c$を満たしかつ、0 元$(0, 0, 0)$となる。従ってS_3は 0 元を持つ。$p1$を満たす。

・$p2$:　$v_1 = (a_1, b_1, c_1) \in S_3$と$v_2 = (a_2, b_2, c_2) \in S_3$を考える。$a_1 = b_1 + c_1$、$a_2 = b_2 + c_2$である。$u = v_1 \oplus v_2 = (a_1, b_1, c_1) \oplus (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2,\ c_1 + c_2)$。このとき、$(b_1 + b_2) + (c_1 + c_2) = (b_1 + c_1) + (b_2 + c_2) = a_1 + a_2$。よって$u$は$(a, b, c)\ a = b + c$を満たし$u \in S_3$であり閉じている。（体$\mathbb{R}$は体加法で閉じている。また可換則が成り立つ。）$p2$を満たす。

・$p3$:　$v = k \times (a_1, b_1, c_1) = (k * a_1, k * b_1, k * c_1)\ k \in F,\ \ a_1 = b_1 + c_1$。このとき、$k * b_1 + k * c_1 = k * (b_1 + c_1) = k * a_1$。従って、$v$は$(a, b, c)\ a = b + c$を満たし$v \in S_3$であり閉じている。（体$\mathbb{R}$は体加法と体乗法に関して分配則が成り立つ）$p3$を満たす。

以上より、$p1$成立、$p2$成立、$p3$成立となり、部分空間である。

D) $S_4 = \{v = (a, b, c) | a * b = 0, a \in \mathbb{R}, b \in \mathbb{R},\ c \in \mathbb{R}\}$

・$p1$:　$v = (a, b, c) \in S_4$（ただし$a * b = 0$)は、$a = 0, b = 0, c = 0$のとき$a * b = 0$であり、0 元$(0, 0, 0)$となる。従ってS_4は 0 元を持つ。$p1$を満たす。

・$p2$:　$v_1 = (a_1, b_1, c_1) \in S_4$と$v_2 = (a_2, b_2, c_2) \in S_4$を考える。$a_1 * b_1 = 0$、$a_2 * b_2 = 0$である。$u = v_1 \oplus v_2 = (a_1, b_1, c_1) \oplus (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2)$。このとき、$(a_1 + a_2) * (b_1 + b_2) = a_1 * b_1 + a_1 * b_2 + a_2 * b_1 + a_2 * b_2$　である。（体$\mathbb{R}$は体加法と体乗法に関して分配則が成り立つ）例えば、$a_1 = 0,\ b_1 = 1,\ a_2 = 0,\ b_2 = 1$の時、$(a_1 + a_2) * (b_1 + b_1) = 0$を満たさない。従って$u \notin S_4$であり閉じていない。$p2$を満たさない。

・$p3$:　$v = k \times (a_1, b_1, c_1) = (k * a_1, k * b_1, k * c_1)$ $k \in F,\ a_1 * b_1 = 0$。このとき、$k * a_1 * k * b_1 = k * k * a_1 * b_1 = 0$。従って、$v$は$(a, b, c)$ $(a * b = 0)$を満たし$v \in S_4$であり閉じている。（体$\mathbb{R}$は体乗法に関して可換則が成り立つ。）$p3$を満たす。

以上より、$p1$成立、$p2$不成立、$p3$成立となり、部分空間ではない。

E) $S_5 = \{(a, b, c) | a = b, a \in \mathbb{R}, b \in \mathbb{R},\ c \in \mathbb{R}\}$

・$p1$:　$v = (a, b, c) \in S_5$（ただし$a = b$)は、$a = 0, b = 0, c = 0$のとき$a = b$であり、0 元$(0, 0, 0)$となる。従ってS_5は 0 元を持つ。$p1$を満たす。

・$p2$:　$v_1 = (a_1, b_1, c_1) \in S_5$と$v_2 = (a_2, b_2, c_2) \in S_5$を考える。$a_1 = b_1$、$a_2 = b_2$である。$u = v_1 \oplus v_2 = (a_1, b_1, c_1) \oplus (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2)$。このとき、$a_1 + a_2 = b_1 + b_2$である。（体$\mathbb{R}$は加法で閉じている。）従って$u \in S_5$であり閉じている。$p2$を満たす。

・$p3$:　$v = k \times (a_1, b_1, c_1) = (k * a_1, k * b_1, k * c_1)$　$k \in F,\ a_1 = b_1$。このとき、$k * a_1 = k * b_1$。従って、vは(a, b, c) $(a = b)$を満たし$v \in S_5$であり閉じている。（体$\mathbb{R}$は体乗法に関して閉じている）$p3$を満たす。

以上より、$p1$成立、$p2$成立、$p3$成立となり、部分空間である。(x, x, z)の平面。

F) $S_6 = \{(a, b, c) | a = b + 3, a \in \mathbb{R}, b \in \mathbb{R},\ c \in \mathbb{R}\}$

・$p1$:　$v = (a, b, c) \in S_6$（ただし$a = b + 3$)は、0 元$(0, 0, 0)$とならずS_5は 0 元を持たない。$p1$を満たさない。

・$p2$:　$v_1 = (a_1, b_1, c_1) \in S_6$と$v_2 = (a_2, b_2, c_2) \in S_6$を考える。$a_1 = b_1 + 3$、$a_2 = b_2 + 3$である。$u = v_1 \oplus v_2 = (a_1, b_1, c_1) \oplus (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2)$。このとき、$(a_1 + a_2) = (b_1 + 3) + (b_2 + 3) = (b_1 + b_2) + (3 + 3) = b_1 + b_2 + 6$である。（体$\mathbb{R}$は体加法に関して結合則が成り立つ。）従って$u \notin S_6$であり閉じていない。$p2$を満たさない。

・$p3$:　$v = k \times (a_1, b_1, c_1) = (k * a_1, k * b_1, k * c_1)$ $k \in F,\ a_1 = b_1 + 3$。このとき、$k * a_1 = k * (b_1 + 3) = k * b_1 + k * 3$。従って、$v \notin S_6$であり閉じていない。$p3$を満たさない。

以上より、$p1$不成立、$p2$不成立、$p3$不成立となり、部分空間ではない。

問３－２）

以下で表現される集合S_7は、$\mathbb{R}^3$の部分空間となるかを調べよ。

ただし、実数体$\mathbb{R}$（$+_F$,$*_F$が定義されている）上で考え、以下が定義されているとする。見やすさのため、$+_F$は$+$、$*_F$は$*$と表記する。

ベクトル加法$+_V$の定義　$(a, b, c) +_V (d, e, f) \triangleq (a + d,\ b + e,\ c + f)$

スカラー乗法$*_{FV}$の定義　$k *_{FV} (a, b, c) \triangleq (k * a,\ k * b,\ k * c)$

ベクトル乗法$*_V$の定義　$(a, b, c) *_V (d, e, f)^T \triangleq a * d + b * e + c * f$

$S_7 = \{v = (a, b, c) | (a, b, c) *_V (1, 1, 1)^T = 0, a \in \mathbb{R}, b \in \mathbb{R},\ c \in \mathbb{R}\}$

解答

$S_7 = \{(a, b, c) | (a, b, c) *_V (1, 1, 1)^T = 0, a \in \mathbb{R}, b \in \mathbb{R},\ c \in \mathbb{R}\}$

$(a, b, c) *_V (1, 1, 1)^T = a * 1 + b * 1 + c * 1 = a + b + c$ よって、$a + b + c = 0$

・$p1$:　$v = (a, b, c) \in S_7$（ただし$a + b + c = 0$)は、$a = 0, b = 0, c = 0$のとき$a + b + c = 0$であり、0 元$(0, 0, 0)$となる。従ってS_7は 0 元を持つ。$p1$を満たす。

・$p2$:　$v_1 = (a_1, b_1, c_1) \in S_7$と$v_2 = (a_2, b_2, c_2) \in S_7$を考える。$a_1 + b_1 + c_1 = 0$、$a_2 + b_2 + c_2 = 0$である。$u = v_1 +_V v_2 = (a_1, b_1, c_1) +_V (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2)$。このとき、$(a_1 + a_2) + (b_1 + b_2) + (c_1 + c_2) = (a_1 + b_1 + c_1) + (a_2 + b_2 + c_2) = 0$である。従って$u \in S_7$であり閉じている。（体$\mathbb{R}$は体加法に関して結合則、可換則が成り立つ）$p2$を満たす。

・$p3$:　$v = k *_{FV} (a_1, b_1, c_1) = (k * a_1, k * b_1, k * c_1)$　$k \in F$, $a_1 + b_1 + c_1 = 0$。このとき、$k * a_1 + k * b_1 + k * c_1 = k * (a_1 + b_1 + c_1) = 0$。従って、$v$は$(a, b, c)$　$(a + b + c = 0)$を満たし$v \in S_7$であり閉じている。（体$\mathbb{R}$は体加法と体乗法に関して分配則が成り立つ。）$p3$を満たす。

以上より、$p1$成立、$p2$成立、$p3$成立となり、部分空間である。$x + y + z = 0$の平面。

問３－３）

以下で表現される集合S_8は、実数を要素とする2×2正方行列全部の集合$M_2(\mathbb{R})$の部分空間となるかを調べたい。まず、通常の行列の和と積を用いてベクトル加法とスカラー乗法を定義せよ。その後、S_8が$M_2(\mathbb{R})$の部分空間となるかを調べよ。

$$S_8 = \left\{ v = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \middle| \, a \in \mathbb{R}, b \in \mathbb{R}, \ d \in \mathbb{R} \right\}$$

解答

$S_8 = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \middle| \, a \in \mathbb{R}, b \in \mathbb{R}, \ d \in \mathbb{R} \right\}$ は、2x2 行列の部分空間となるかを議論する。

実数体$\mathbb{R}$　（$+_F$　$*_F$が定義されている）

まず、ベクトル加法$+_V$とスカラー乗法$*_V$を以下のように定義する。

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} +_V \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \triangleq \begin{bmatrix} a_{11} +_F b_{11} & a_{12} +_F b_{12} \\ a_{21} +_F b_{21} & a_{21} +_F b_{22} \end{bmatrix}$$

$$k *_V \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \triangleq \begin{bmatrix} k *_F a_{11} & k *_F a_{12} \\ k *_F a_{21} & k *_F a_{22} \end{bmatrix}$$

・$p1$:　$A = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in S_8$は、$a = 0, b = 0, d = 0$のとき、0 元となる。従って 0 元を持つ。$p1$を満たす。

・$p2$:　$A_1 = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in S_8$、$A_2 = \begin{bmatrix} e & f \\ 0 & h \end{bmatrix} \in S_8$を考える。$u = A_1 + A_2 = \begin{bmatrix} a +_F e & b +_F f \\ 0 & d +_F h \end{bmatrix} = \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix}$となる$a', b', c'$は、$a', b', c' \in \mathbb{R}$である。（体$\mathbb{R}$は体加法に関して閉じている）従って$u \in S_8$であり閉じている。$p2$を満たす。

・$p3$:　$k \in F$とする。$v = k *_V A = \begin{bmatrix} k *_F a & k *_F b \\ 0 & k *_F d \end{bmatrix} = \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix}$となる$a', b', c'$は、$a', b', c' \in \mathbb{R}$である。（体$\mathbb{R}$は体乗法に関して閉じている）従って、$v \in S_8$であり閉じている。$p3$を満たす。

以上より、$p1$成立、$p2$成立、$p3$成立となり、部分空間である。

問４）実数体$\mathbb{R}^3$を考える。ベクトル加法、スカラー乗法を以下のように定義するとき、S = $\{v = (a, b, c) | \, a \in \mathbb{R}, b \in \mathbb{R}, \ c \in \mathbb{R}\}$は、体$\mathbb{R}$上のベクトル空間となるか調べよ。

ベクトル加法$+_V$の定義　$(a, b, c) +_V (d, e, f) \triangleq (a + f, \ b + e, \ c + d)$

スカラー乗法$*_V$の定義　$k *_V (a,b,c) \triangleq (\frac{a}{k},\frac{b}{k},\frac{c}{k})$

解答：ベクトル空間とはならない。以下その理由。

ベクトル加法$+_V$について。閉塞性成立。可換則不成立。

$(a,b,c)+_V(d,e,f) = (a+f,b+e,c+d)$

$(d,e,f)+_V(a,b,c) = (d+c,b+e,f+c)$　よって、可換則が成立しない。

スカラー乗法$*_V$について、閉塞性、結合則や分配則１は成立するが、分配則２不成立。

結合則

$k *_V [l *_V (a,b,c)] = k *_V [(\frac{a}{l},\frac{b}{l},\frac{c}{l})] = (\frac{a}{kl},\frac{b}{kl},\frac{c}{kl})$

$[k *_F l] *_V (a,b,c) = [k * l] *_V (a,b,c) = (\frac{a}{kl},\frac{b}{kl},\frac{c}{kl})$　よって結合則成立。

分配則１

$k *_V [(a,b,c)+_V(d,e,f)] = k *_V [(a+f,b+e,c+d)] = (\frac{a+f}{k},\frac{b+e}{k},\frac{c+d}{k})$

$k *_V (a,b,c)+_V k *_V (d,e,f) = (\frac{a}{k},\frac{b}{k},\frac{c}{k}) +_V (\frac{d}{k},\frac{e}{k},\frac{f}{k}) = (\frac{a+f}{k},\frac{b+e}{k},\frac{c+d}{k})$ よって、分配則１成立。

分配則２

$(k+_F l) *_V (a,b,c) = (\frac{a}{k+l},\frac{b}{k+l},\frac{c}{k+l})$

$k *_V (a,b,c)+_V l *_V (a,b,c) = (\frac{a}{k},\frac{b}{k},\frac{c}{k}) +_V (\frac{a}{l},\frac{b}{l},\frac{c}{l}) = (\frac{a}{k}+\frac{a}{l},\frac{b}{k}+\frac{b}{l},\frac{c}{k}+\frac{c}{k})$　よって、分配則２不成立。