7.3.4 巡回ハミング符号

原始多項式：周期がちょうど 2^m-1 となる m次の多項式

m次の原始多項式を生成多項式とする符号長 $n=2^m-1$ の符号のとき，

d_{min} は3以上．符号長 $n=2^m-1$，情報ビット数 $k=2^m-1-m$

検査ビット数 m の単一誤り訂正符号．

x^i を $G(x)=x^3+x+1$ で割った剰余多項式 $R_i(x)$

i	$R_i(x)$
0	1
1	x
2	x^2
3	$x+1$
4	x^2+x
5	x^2+x+1
6	x^2+1

↑ ↑ ↑

$$\sum_{i=0}^{6} w_i R_i(x)=0 \Rightarrow \left.\begin{aligned} w_6+w_5+w_4\quad +w_2\quad &=0\\ w_5+w_4+w_3\quad +w_1\quad &=0\\ w_6+w_5\quad +w_3\quad +w_0 &=0\end{aligned}\right|$$

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

誤りトラップ復号法(error-trap decoding)

7.4 ガロア体

7.4.1 素体

ガロア体は位数 q が素数 p のべき(指数) p^m のときまたそのときに限って存在する．(p 素数 m 正整数)

位数 $=p$　$GF(p)$ は素体、 $-a=\begin{cases}0 & a=0\\ p-a & その他\end{cases}$　$a^{-1}a\equiv 1 \bmod p$

7.4.2 拡大体

$m\geq 2$ のとき $GF(p^m)$ は拡大体　$GF(p)$ に $GF(p)$ 上の m次既約多項式の根一つ付加して体を作ることにより，拡大体 $GF(p^m)$ が得られる．

$GF(2)$ 上の多項式：x^2+x+1．根は α とし　$\alpha^0=1$　$\alpha^1=\alpha$　$\alpha^2=\alpha+1$　$\alpha^3=\alpha^2+\alpha=1=\alpha^0$　⋮

$GF(2^m)$：0 と m次原始多項式の根 α のべき $\alpha^0,\alpha^1,\alpha^2,\ldots\alpha^{2m-2}$ とで構成できる．

$\alpha^{2m-1}=1 \Rightarrow \alpha^{-i}=\alpha^{[2m-1-i] \bmod 2^m-1}$

べき表現	$\alpha^3\alpha^2\alpha 1$ による展開	ベクトル表現
0	0	0000
1	1	0001
α	α	0010
α^2	α^2	0100
α^3	α^3	1000
α^4	$\alpha+1$	0011
α^5	$\alpha^2+\alpha$	0110
α^6	$\alpha^3+\alpha^2$	1100
α^7	$\alpha^3+\alpha+1$	1011
α^8	α^2+1	0101
α^9	$\alpha^3+\alpha$	1010
α^{10}	$\alpha^2+\alpha+1$	0111
α^{11}	$\alpha^3+\alpha^2+\alpha$	1110
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1111
α^{13}	$\alpha^3+\alpha^2+1$	1101
α^{14}	α^3+1	1001

加算：ベクトル⊕ベクトル　減算 $-x=x$

乗算：①乗 ② Mod

除算：$\alpha^{-i}=\alpha^{[2m-1-i] \bmod 2^m-1}$

例)：$\alpha^3(\alpha^7+\alpha^5)^3+\dfrac{\alpha^9+\alpha^3}{1+\alpha^{10}}$

$=\alpha^3(\alpha^{13})^3+\dfrac{\alpha}{\alpha^5}$

$=\alpha^3\alpha^4+\alpha\alpha^{10}=\alpha^{12}+\alpha^{11}=1$

7.5 BCH符号

7.5.1 BCH符号の定義

α を $GF(2^m)$ の原始元とし，d を $n=2^m-1$ 以下の任意の正整数とする．

$\alpha^l,\alpha^{l+1},\ldots\alpha^{l+d-2}$ をすべて根として持つ，最小次数の GF(2) 上の多項式を生成多項式とする符号長 $n=2^m-1$ の2元巡回符号が BCH符号である．(l: ふつう $l=1$ or 0)

BCH限界：$d_{min}\geq d$　$F(x)=f_s x^s+f_{s-1}x^{s-1}+\cdots+f_1x+f_0$ が α^i を根とするなら

例)：$l=1$　$d=2t+1$　$F(\alpha^{2i})=[F(\alpha^i)]^2=0$

符号長 $n=2^m-1$

情報ビット数 $k\geq 2^m-1-mt$

誤り訂正能力 $t_0\geq t$

$t=1$ の BCH符号は巡回ハミング符号に他ならない．

例：α を原始多項式 x^4+x+1 の根とし，符号長 $n=2^4-1=15$，$t=2$ の BCH符号．

生成多項式 $G(x)$ の次数は $mt=8$ 以下．$G(x)=g_8x^8+\cdots+g_1x^1+1$ とおく(定数項は常に非零)

$G(x)$ は α と α^3 を根として持つから

$$\left.\begin{aligned}G(\alpha)&=g_8\alpha^8+g_7\alpha^7+\cdots g_1\alpha+1=0\\ G(\alpha^3)&=g_8\alpha^{24}+g_7\alpha^{21}+\cdots g_1\alpha^3+1=0\end{aligned}\right\}$$

$$\begin{bmatrix}0&1&1&0&0&1&0&0\\1&0&1&1&0&0&1&0\\0&1&0&1&1&0&0&1\\1&1&0&0&1&0&0&0\\1&1&1&0&1&1&1&1\\0&1&0&0&1&0&1&0\\1&0&0&0&1&1&0&0\\0&0&0&1&1&0&0&0\end{bmatrix}\begin{bmatrix}g_8\\g_7\\g_6\\g_5\\g_4\\g_3\\g_2\\g_1\end{bmatrix}=\begin{bmatrix}0\\0\\0\\1\\0\\0\\0\\1\end{bmatrix}$$

$g_8=1$　$g_7=1$　$g_6=1$　$g_5=0$　$g_4=1$　$g_3=0$　$g_2=0$　$g_1=0$

$G(x)=x^8+x^7+x^6+x^4+1$

検査ビット $n-k=8$　$d_{min}\geq 5$　誤り訂正能力は $t_0=2$

7.5.2 BCH符号の復号

(1) 受信語からシンドローム $S_1,S_2,\ldots S_{2t}$ を求める

(2) シンドロームがすべて 0 なら誤りなしと判定する

(3) シンドロームに0ならないものがあれば，シンドロームから誤り位置多項式 $\sigma(z)$ を求める

(4) $\sigma(z)$ の根 $\alpha^{-j_1},\alpha^{-j_2},\ldots\alpha^{-j_2}$ を求める

(5) $\alpha^{-j_1},\alpha^{-j_2},\ldots\alpha^{-j_L}$ から $j_1,j_2,\ldots j_L$ を求め，これらの位置の記号を訂正する

$\sigma(z)=(1-\alpha^{j_1}z)(1-\alpha^{j_2}z)\cdots(1-\alpha^{j_L}z)$

$\sigma(z)=1+S_1z+(S_1^3+S_3)S_1^{-1}z^2$

$S_1=Y(\alpha)$

$S_3=Y(\alpha^3)$

例：$y=(000100010000000)$

$Y(x)=x^{11}+x^7$

$S_1=Y(\alpha)=\alpha^{11}+\alpha^7=\alpha^8$

$S_3=Y(\alpha^3)=\alpha^{33}+\alpha^{21}=\alpha^3+\alpha^6=\alpha^2$

$\sigma(z)=1+\alpha^8z+(\alpha^{24}+\alpha^2)\alpha^{-8}z^2$

$=1+\alpha^8z+\alpha^3z^2$

根：$\alpha^4=\alpha^{-11}$　$\alpha^8=\alpha^{-7}$

位置11と7に誤りが生じた

あらすじ

情報源

1.1 記憶のない定常情報源

定常情報源≒エルゴード情報源 ($\overline{f(x)}=\langle f(x)\rangle$)（無数の同じ情報源について平均：集合　時間）

1.2 m重マルコフ情報源

只与之前 m 个出力有关．2^m 個の状態を持ち(状態図)　既約マルコフ情報源(一つの閉じた状態集合だけ)

状態の分類 $\begin{cases}過渡状態\\ 閉じた状態集合(周期的/非周期的)\end{cases}$

遷移確率行列 $\Pi=\begin{bmatrix}P_{00}&\cdots&P_{0,N-1}\\ \vdots&&\vdots\\ P_{N-1,0}&\cdots&P_{N-1,N-1}\end{bmatrix}$　時点 t 状態 S_j の確率：$w_j^{(t)}$

ベクトル $w_t=(w_0^{(t)},w_1^{(t)},\ldots w_{N-1}^{(t)})$

極限分布：$\lim_{t\to\infty}w_t=w_0\lim_{t\to\infty}\Pi^t=w_0U=u$　状態確率分布ベクトル

定常分布：$w=(w_0,w_1,\cdots w_{N-1})$　$w\Pi=w$　唯一つ存在する

情報源符号化

2.1 情報源符号化の基础概念

(1) 情報源符号化に必要な条件(一意復号可能．瞬時符号 best；1記号当たりの平均符号長短い)

(2) 符号の木　(3) クラフトの不等式 $q^{-l_1}+q^{-l_2}+\cdots+q^{-l_M}\leq 1$

2.2 平均符号長の限界

$P(a_i)=p_i\ (i=1,2,\cdots M)$　1情報源記号当たりの平均符号長 $L=l_1p_1+\cdots+l_Mp_M$

S の1次エントロピー：$H_1(S)=-\sum_x P(x)\log_2 P(x)=-\sum_i p_i\log_2 p_i$

2.3 基本的な情報源のエントロピー

(1) 記憶のない情報源のエントロピー(平均符号長の限界)

$H(S)=H_1(S)=-\sum_{i=1}^{m}p_i\log_2 p_i$　$\mathcal{H}(x)=-x\log_2x-(1-x)\log_2(1-x)$

(2) マルコフ情報源のエントロピー

$H(S)=\sum_{i=0}^{N-1}w_i\left[-\sum_{j=1}^{M}P(a_j|S_i)\log_2 P(a_j|S_i)\right]$

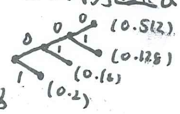
2.4 基本的情報源符号化法

(1) ハフマンブロック符号化法　(符号化の符号化)

一定個数の情報源記号ごとにまとめて符号化する方法

(2) 非等長情報源系列の符号化　1,0 を確率0.2,0.8で四つの系列を選び

符号化すべき情報源系列を非等長にしてみる



(3) ランレングス符号化法

同じ記号が連続する長さ(run length)を符号化する

(4) 算術符号

情報源系列全体を一つの符号語に符号化してしまう．累積確率を符号化

情報量とひずみ

3.1 情報量

エントロピー＝1情報量記号当たりの平均符号長の下限　曖昧さを表す尺度

情報量＝情報を受け取ることによるエントロピーの変化 $I(p)$ と書く

相対エントロピー：$h(S)=\dfrac{H(S)}{\log_2 M}$　冗長度：$\rho(S)=1-h(S)$

3.2 相対情報量

Y で条件をつけた X の条件付エントロピーと呼ばれ，Y を知ったとき X についてなお残っている平均の曖昧さの尺度を与える．　$I(X;Y)=\sum_x\sum_y P(x,y)\log_2\dfrac{P(x,y)}{P(x)P(y)}=H(X)-H(X|Y)=H(Y)-H(Y|X)$

3.3 ひずみ

$d(x,y)=\begin{cases}0 & x=y\\ 1 & x\neq y\end{cases}$　$\bar{d}=\sum_x\sum_y d(x,y)P(x,y)$　$I(X;Y)=\mathcal{H}(p)-\mathcal{H}(D)=R(D)$

送らねばならない情報量の最小値