6.4 通信の限界

情報源から情報源記号：毎秒α個　$R=\alpha H(S)$ (bit/s)

通信路：毎秒β個　$\mathcal{C}=\beta C$ (bit/s)

$R<\mathcal{C}$：任意に小さい誤り率であて忠実に送ることができる。

$R>\mathcal{C}$：何らかのひずみを生じる。情報源からの通報をD^*に任意に近い

$\alpha R(D^*)=\mathcal{C}$ を満たす D^* を考える。$R(D^*+\varepsilon)<\alpha R(D^*)=\mathcal{C}$　平均ひずみで伝送できる

6.5 信頼性関数

記憶のない通信路に対し、復号誤り率が $P_e \le 2^{-nE(R)}$ となる符号長n，情報速度Rの符号が存在する。E(R)は信頼性関数

$$E(R)=\max_{\rho,P}\{-\rho R+E_0(\rho,P)\} \quad P=(p_1,\cdots p_r)$$

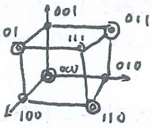
$$2^{-n[E_L(R)+o(n)]} \le P_{eo} \le 2^{-nE(R)}$$ 訂正能力

$$E_0(\rho,P)=-\log_2 \sum_{j=1}^{s}\left(\sum_{i=1}^{r} p_i P_{ij}^{1/(1+\rho)}\right)^{1+\rho} \quad (0<\rho\le 1)$$

2元対称通信路：

$$p_1^*=\frac{\sqrt{p}}{\sqrt{p}+\sqrt{1-p}}$$ pをビット誤り率とするとき $E(R)=p^*\log_2\frac{p^*}{p}+(1-p^*)\log_2\frac{1-p^*}{1-p}$

第7章 通信路符号化法



7.1 単一誤りの検出と訂正

7.1.1 単一パリティ検査符号

偶校验位：補1 bit 的 1，使全bit中1的个数为偶数，否则补0

$w=x_1x_2x_3\cdots x_kc$　情報記号/情報ビット：情報を伝達するために用いられる記号である。

誤り検出符号

c：(パリティ)検査記号 [(parity) check symbol]　単一パリティ検査符号

符号長 $n=k+1$　符号語数 $M=2^k$　$k=2$の場合：$C=\{000,011,101,110\}$

符号長n，情報記号数kの組織符号を(n,k)符号と書く。$\underbrace{a_1\cdots a_k}_{\text{情報記号}}\ \underbrace{a_{k+1}\cdots a_n}_{\text{検査記号}}$

効率 $\eta=\frac{k}{n}$

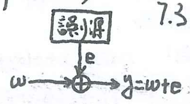
検査記号が情報記号の線形な式で与えられる符号 ―― 線形符号

性質：任意の二つの符号語について，その成分ごとの和をとると，それがまた符号語になるということである。逆にも成立することである。

単一パリティ検査符号Cの符号語は $w=(w_1,w_2,\cdots w_n)$ $(n=k+1)$

$w_1+w_2+\cdots w_{n-1}+w_n=0$　パリティ検査方程式

$y=w+e=(w_1+e_1,w_2+e_2,\cdots w_n+e_n)$



パリティ検査方程式(7.9)に受信語を代入した結果をシンドロームと呼ぶ。

7.1.2 水平垂直パリティ検査符号

x_{11}	x_{12}	c_1	行の検査
x_{21}	x_{22}	c_2	ビット
c_1'	c_2'	c''	検査ビットの
列の検査ビット			検査ビット

一般化：k_1k_2個の情報を$k_1\times k_2$の配列に並べ，

この符号の符号語は$(k_1+1)\times(k_2+1)$の配列である

1個の誤りが訂正できる　誤り訂正

2個の誤りの生じたことを知ることはできる。検出符号

7.1.3 (7,4)ハミング符号

$C_1=x_1+x_2+x_3$

$C_2=\quad x_2+x_3+x_4$

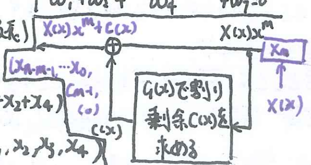
$C_3=x_1+x_2\quad +x_4$

$w=(x_1,x_2,x_3,x_4,c_1,c_2,c_3)$

パリティ検査方程式：

$$\begin{cases} w_1+w_2+w_3 \quad +w_5=0 \\ \quad w_2+w_3+w_4 \quad +w_6=0 \\ w_1+w_2+\quad w_4 \quad +w_7=0 \end{cases}$$

(符号長，情報長)



7.1.4 生成行列と検査行列

$w=(x_1,x_2,x_3,x_4,x_1+x_2+x_3,x_2+x_3+x_4,x_1+x_2+x_4)$

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

$w=xG$，$x=(x_1,x_2,x_3,x_4)$

生成行列 (generator matrix)

(n,k)線形符号の生成行列はk×n行列。

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

$wH^T=0$　検査行列　$(n-k)\times n$行列

$S=yH^T$　$S=(S_1,S_2,S_3)$　シンドロームパターン

7.1.5 一般のハミング符号

$S=(w+e)H^T=wH^T+eH^T=eH^T$

行列Hの行数はm 列数は2^m-1　検査符号長＝行数m，列数2^m-1＝検査ビット数

符号長 $n=2^m-1$　$=7$　$(m=3)$　(7,4)ハミング符号

情報ビット数 $k=2^m-1-m$　$=4$

検査ビット数 $n-k=m$　$=3$

$$\begin{cases} C_1=P_{11}x_1+P_{12}x_2+\cdots+P_{1k}x_k \\ C_2=P_{21}x_1+P_{22}x_2+\cdots+P_{2k}x_k \\ \vdots \\ C_m=P_{m1}x_1+P_{m2}x_2+\cdots+P_{mk}x_k \end{cases}$$

(n,k)ハミング符号の検査行列

$$H=\begin{bmatrix}P_{11}&P_{12}&\cdots&P_{1k}&1&0&\cdots&0\\P_{21}&P_{22}&\cdots&P_{2k}&0&1&\cdots&0\\\vdots&\vdots&&\vdots&&&\ddots&\vdots\\P_{m1}&P_{m2}&\cdots&P_{mk}&0&\cdots&0&1\end{bmatrix}$$

$w=(x_1,\cdots,x_k,c_1,\cdots,c_m)$

7.2 符号の誤り訂正能力

7.2.1 ハミング距離とハミング重み

二つのn次元ベクトル $u=(u_1,u_2\cdots u_n)$ と $v=(v_1,v_2,\cdots v_n)$ の間に $d_H(u,v)=\sum_{i=1}^{n}\delta(u_i v_i)$

$d_H(u,v)$ は互いに異なるものの数である。uとvのハミング距離　$\delta(u,v)=\begin{cases}0 & u=v\\1 & u\neq v\end{cases}$

距離の三公理：

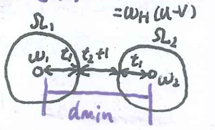
(i) $d_H(v_1,v_2)\ge 0$であり，等号が成立するのは $v_1=v_2$ のときに限る。

(ii) $d_H(v_1,v_2)=d_H(v_2,v_1)$　(iii) $d_H(v_1,v_2)+d_H(v_2,v_3)\ge d_H(v_1,v_3)$ (三角不等式)　$w_H(v)=d_H(v,0)$

一般に，n次元ベクトルvの0でない成分の数をvのハミング重みといい，$w_H(v)$で表す。　$d_H(u,v)=w_H(u-v)$

7.2.2 最小距離と誤り訂正能力

Cの最小ハミング距離 $d_{min}=\min_{u\neq v,\ u,v\in C}\{d_H(u,v)\}$　$d_{min}\ge 2t_1+1$ であれば t_1個以下の誤りを訂正できる。限界距離復号法



t_1の最大値は $t_1=\lfloor (d_{min}-1)/2\rfloor$ ($\lfloor x\rfloor$はx以下の最大整数を示す)　単一誤り訂正・2重誤り検出符号

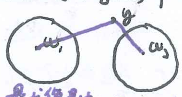
$t_2+1=d_{min}-2t_1$ のとき $(t_2\ge 1)$　(single-error-correcting/double-error-detecting code; SEC/DED符号)

t_1+1個以上，t_1+t_2個以下の誤りは訂正できないが検出可能となる

7.2.3 限界距離復号法と最尤復号法

2元対称通路(BSC)について：　ビット誤り率がp　wを送った，yが受信される $P(y|w)=p^t(1-p)^{n-t}$

tは誤りの個数　$t=d_H(w,y)$



最尤復号法：$P(y|w)$を最大とする符号語が送られたと推定する復号法。

正しく復号される確率	最尤≧限界距離	復号誤りの影響が非常に	最尤復号法：$y\to w_2$
実現の難しさ	最尤＞限界距離	深刻であるような場合には	限界距離復号法：誤りを検出。

限界距離∨

7.2.4 BSCにおける限界距離復号法の復号特性

正しく復号される確率 P_c

復号誤り率 P_e

訂正不可能な誤り検出率 P_d

① $P_c+P_e+P_d=1$

② $P_c=\sum_{i=0}^{t_1}{}_nC_i p^i(1-p)^{n-i}$

③ $P_e\le\sum_{i=t_1+t_2+1}^{n}{}_nC_i p^i(1-p)^{n-i}$

7.2.5 消失のある場合の復号

$d'_{min}\ge d_{min}-e$　① $d_{min}-1$個以下の任意の位置に生じた消失は訂正可能である

② 消失個失eが$d_{min}-1$より小さければ$d'_{min}>1$となるから，他の誤りの検出訂正もd'_{min}に応じて可能である。

7.2.6 バースト誤りの検出と訂正

バースト誤り訂正(検出)能力：訂正(検出)可能な最長のバースト誤り長さ。

条件：① Cの任意の符号語w_1に対して，w_1+eが別の符号語にならない (Cが線形符号であれば，eは符号語にならない)

② $w_1+e\neq w_2+e$

7.3 巡回符号

$v=(v_{n-1},v_{n-2},\cdots,v_1,v_0)$ の多項式表現 $V(x)=v_{n-1}x^{n-1}+v_{n-2}x^{n-2}+\cdots+v_1x+v_0$　符号多項式

$G(x)=x^m+g_{m-1}x^{m-1}+\cdots+g_1x+1$ ($g_1,\cdots g_{m-1}$は0または1である)

Cは $W(x)=A(x)G(x)$ という形の符号多項式からなる符号である。(A(x)はn-m-1次以下任意の多項式)

右のようにして，G(x)から作られる符号Cは巡回符号と呼ぶ

A(x)	W(x)=A(x)G(x)	w
0	0	0000000
1	$x^4+x^3+x^2+1$	0011101
x	$x^5+x^4+x^3+x$	0111010
⋮		

$$A(x)\cdot G(x)=W(x)$$

A(x)：情報の多項式表現　G(x)：生成多項式　W(x)：符号語Cの多項式

巡回符号は線形符号である。

$W_1(x)+W_2(x)=[A_1(x)+A_2(x)]G(x)$

m次G(x)で生成される巡回符号Cは(n,n-m)符号となることを示そう。

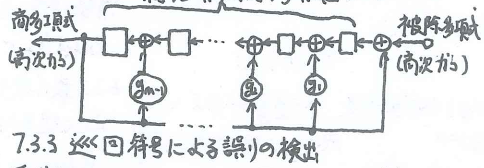
$G(x)\,|\,(x^n-1) \Rightarrow W(x)=w_{n-1}x^{n-1}+\cdots+w_1x+w_0$　　$w=(w_{n-1},\cdots\cdots w_1,w_0)$

G(x)の周期 (n＝符号長のとき，狭義巡回符号と呼ぶ)

$W'(x)=w_{n-2}x^{n-1}+\cdots+w_0x+w_{n-1}$　　$w'=(w_{n-2}\ \cdots\ w_0\ w_{n-1})$

$=xW(x)-w_{n-1}(x^n-1)$

7.3.2 符号器



7.3.3 巡回符号による誤りの検出

受信語 $y=(y_{n-1},\cdots,y_1,y_0)$　$Y(x)=y_{n-1}x^{n-1}+\cdots+y_1x+y_0$　巡回符号による誤り検出方法はCRC (cyclic redundancy check)

$G(x)=x^{16}+x^{12}+x^5+1$

$G(x)=(x+1)(x^{15}+x^{14}+x^{13}+x^{12}+x^4+x^3+x^2+x+1)$　周期32767

周期：1　$2^{15}-1=32767$　$d_{min}=4$。生成される符号長32767以下の符号により，3個以下の任意の誤りを検出できる

$E(x)=x^iB(x)$

$B(x)=x^{l-1}+b_{l-2}x^{l-2}+\cdots+b_1x+1$

B(x)がG(x)で割り切れなければ，このバースト誤りは検出可能

長さ16以下の任意バースト誤りは検出可能

巡回符号のバースト誤り検出能力は生成多項式の次数のみによって決まるのである。