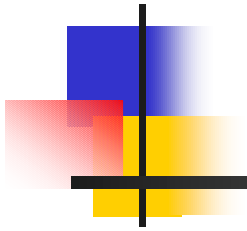


情報理論　#10

第10回講義　6月27日

情報科学研究科　　井上純一

http://chaosweb.complex.eng.hokudai.ac.jp/~j_inoue/

既約多項式

$f(x)=x^3+x+1$　　f(X)=0はx=0,1の解を持たない　⇒ f(x)はGF(2)上での既約多項式

$f(a)=a^3+a+1=0$を用いて、$a^0, a^1, a^2, \ldots$を書き直すと

$a^0=1$

$a^1=a$

$a^2=a^2$

$a^3=-(a+1)=a+1$

$a^4=a^3\cdot a=(a+1)\cdot a=a^2+a$

$a^5=a^4\cdot a=(a^2+a)\cdot a=a^3+a^2=a^2+a+1$

$a^6=\cdots=a^2+1$

$a^7=\cdots=a^0=1$

$f(x)=0$の解をaとしたとき、$a^0, a, \ldots, a^6$の中にaのa^2以下の全ての多項式が含まれる
⇒ $f(x)$は**原始既約多項式**である

巡回ハミング符号

$f(x)=x^3+x+1=0$の解aの冪を書き下す

$$a^0 = 1+0\cdot a+0\cdot a^2$$
$$a^1 = 0+1\cdot a+0\cdot a^2$$
$$a^2 = 0+0\cdot a+1\cdot a^2$$
$$a^3 = 1+1\cdot a+0\cdot a^2$$
$$a^4 = 0+1\cdot a+1\cdot a^2$$
$$a^5 = 1+1\cdot a+1\cdot a^2$$
$$a^6 = 1+0\cdot a+1\cdot a^2$$

係数ベクトル各列にとり、7 x 3 の
行列を作り、それをパリティ検査行列とする

$$H(a^0\cdots a^6)=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\\1&1&0\\0&1&1\\1&1&1\\1&0&1\end{pmatrix}$$

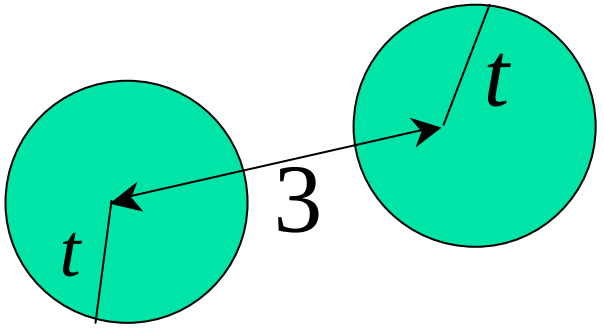
(7、4、3)-線形符号

ハミング不等式とハミング符号

(7, 4, 3)線形符号の最小距離は3であることから、
t ビットまでの誤りを訂正できるためには

$$3 \geq 2t+1 \quad \Rightarrow \quad \boxed{t \leq 1}$$

1ビットまでの訂正が可能



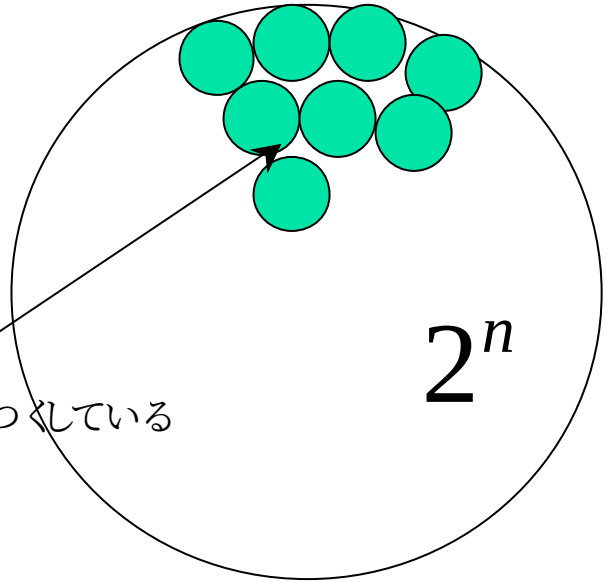
このとき、ハミング不等式は

$$M \leq \frac{2^n}{n+1}$$

$M = 2^4, n = 7$ を代入すると

$$\boxed{2^4 \leq \frac{2^7}{7+1} = 2^4}$$

ハミング不等式をぎりぎり満たす⇒ハミング符号



半径が1ビットの
ハミング球が
空間全体を覆いつくしている
（イメージ図）

パリティ検査方程式

符号語ベクトル $\mathbf{x} = (x_0, x_1, \ldots, x_6)$ に対し、パリティ検査方程式　：

$H\mathbf{x}' = \mathbf{0}$ を書き出してみると

パリティ検査ビット

$$\begin{aligned} x_0 &= x_3 + x_5 + x_6 \\ x_1 &= x_3 + x_4 + x_5 \\ x_2 &= x_4 + x_5 + x_6 \end{aligned}$$

情報ビット

具体的に$M = 2^4 = 16$個の符号語を求めると

$$C = \left\{ \begin{array}{l} (000000), (1010001), (1110010), (0100011), \\ (0110100), (1100101), (1000110), (0010111), \\ (1101000), (0111001), (0011010), (1001011), \\ (1011100), (0001101), (0101110), (1111111) \end{array} \right\}$$

なぜ 巡回」符号か？

$H=(a^0,a,...,a^6)$ とすると、パリティ検査方程式は

$$(a^0,a,...,a^6)\begin{pmatrix}x_0\\x_1\\\cdot\\\cdot\\x_6\end{pmatrix}=0,\ \text{つまり},\ 0=x_0a^0+\cdots+x_6a^6$$

この両辺からaをかけると

$$0=x_0a+x_1a^2+\cdots+x_6a^7=x_6a^0+x_0a+\cdots+x_5a^6$$

$\mathbf{x}=(x_6,x_0,...,x_5)$もパリティ検査方程式の解である

この手続きを進めることにより

$$(x_5,x_6,x_0,...,x_4),(x_4,x_5,x_6,x_0,...,x_3),....$$

xの巡回ベクトル

もパリティ検査方程式の解であることがわかる

巡回符号の多項式表現

符号語 $\mathbf{a}=(a_0,\ldots,a_{n-1})\in C$ に多項式: $f(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}$ を対応させ、$f(x)$を符号語と呼ぶことにする

すると

$$\begin{aligned} xf(x) &= a_0x+a_1x^2+\cdots+a_{n-1}x^n \\ &= a_0x+a_1x^2+\cdots+a_{n-2}x^{n-1}+a_{n-1}(x_n-1)+a_{n-1} \\ &= a_{n-1}+a_0x+\cdots+a_{n-2}x^{n-1} \pmod{(x^n-1)} \end{aligned}$$

つまり

$$f(x)\in C \quad\Rightarrow\quad xf(x)\in C \pmod{(x^n-1)}$$

さらに

$$f(x)\in C \quad\Rightarrow\quad xf(x), x^2f(x), x^3f(x), \ldots\in C$$

$$f_1(x), f_2(x)\in C \quad\Rightarrow\quad f_1(x)+f_2(x)\in C$$

線形符号の性質より

従って、一般に

$$C=\{b(x)g(x) \mid b(x)\text{は}\{0,1\}\text{上の}k-1\text{次以下の多項式}\}$$

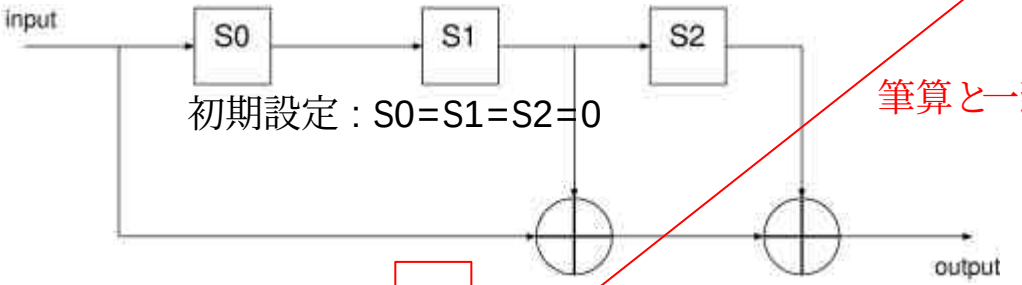
生成多項式

シフトレジスタでの復号器

生成多項式$g(x)=x^3+x+$として、$b(x)=a_0x^2+a_1x+a_2$

$(a_0=a_1=1,a_2=0)$の符号器を作る

予め、手計算で出力の確認をしておくと　$b(x)g(x)=1\cdot x^5+1\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+0$



筆算と一致する

具体的な復号器の出力

$x_0=a_0+S_1+S_2=1$ $(S_0=a_0=1,S_1=S_2=0)$

$x_1=a_1+S_1+S_2=1$ $(S_0=a_1=1,S_1=a_0=1,S_2=0)$

$x_2=a_2+S_1+S_2=1$ $(S_0=a_2=0,S_1=a_1=1,S_2=a_0=1)$

$x_3=0+S_1+S_2=0$ $(S_0=0,S_1=a_2=0,S_2=a_1=1)$

$x_4=0+S_1+S_2=1$ $(S_0=0,S_1=S_0=0,S_2=a_2=0)$

$x_5=0+S_1+S_2=0$ $(S_0=0,S_1=S_0=0,S_2=S_0=0)$

シンドローム多項式

$\{0,1\}$ 上で $x^{15}-1$ は次の積に因数分解される

$$m_1(x)=x+1$$
$$m_2(x)=x^2+x+1$$
$$m_3(x)=x^4+x^3+x^2+x+1$$
$$m_4(x)=x^4+x+1$$
$$m_5(x)=x^4+x^3+1$$

生成多項式

3，8ビット目に誤りを起こすノイズ多項式

符号語 $c(x)=b(x)m_3(x)m_4(x)$ を送信したとき、$e(x)=x^3+x^8$ が加わった

受信語は

$$\overline{c}(x)=c(x)+e(x)=1+x^3+x^4+x^6+x^7 \pmod{g(x)}$$

シンドローム多項式

受信ベクトルから送信ベクトルを復号するためには、受信多項式を
生成多項式で割ればよい

具体的には **例題 10** を見てみよう