(5) ハミング符号

$\Sigma = \{0,1\}^k$, $k \geq 3$, $n = 2^k - 1$ とし、

A を、k 個の $\{0,1\}$ の中に2個以上 1 が含まれるものの順列を全て並べた、$(n-k, k)$ 行列とする

例) $k=3$ なら $n=7$.　　$k=4$ なら、$n=15$

$$A = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$ である。

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ & \vdots & & \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ & \vdots & & \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$ である。

今、$x \in \Sigma$ に対し、$y \in \{0,1\}^{n-k}$ を、

$$y := \begin{bmatrix} y_1 \\ \vdots \\ y_{n-k} \end{bmatrix} = Ax = A \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix}$$ とし、

$\sigma(x) = xy$ を符号語にする。

<u>定理6.6</u>. ハミング符号は1-誤り訂正符号である。

(証) まず $\sigma(x) = EAx$ とできるので $\sigma(\Sigma)$ は $\{0,1\}$ を係数とするベクトル空間であることに注意

ここで、$w(z) := |\{i \mid z_i = 1, 1 \leq i \leq n\}|$ とおくと、
$z \in \{0,1\}^n$ に対し、

$\forall x \in \Sigma \setminus \{00\cdots0\}$ に対し、$w(\sigma(x)) \geq 3$ である

(ハ) $\sigma(x)=xy$ より　$w(x)\geq 3$ なら 明らか.

$w(x)=1$ なら. $w(y)\geq 2$ より成立.

$w(x)=2$ なら. $w(y)\geq 1$ より成立

ゆえに. $d(\sigma(x),\sigma(x'))=d(\sigma(x)-\sigma(x'),\sigma(x')-\sigma(x'))$

$=d(\sigma(x-x'),0)=w(x-x')\geq 3$　となる//