BINARY HAMMING CODES

$(n, 2^k, 3)$

$n = 2^r - 1 \qquad k = n - r$

$HAM(r,2): (2^r - 1,\ 2^{2^r - 1 - r},\ 3)$

$$H = \underbrace{\begin{bmatrix} \quad & \quad & \quad \\ & & \\ & & \end{bmatrix}}_{2^r - 1} \Big\} r$$

Columns of H are <u>all</u> nonzero r-bit vectors

All columns of H are different $\Rightarrow$ sum of any two columns is not equal to 0.

<u>$d = 3$</u>

EXAMPLE

$q=2 \quad n=7 \quad k=4$

$$G=\begin{bmatrix} 1000 & 101 \\ 0100 & 011 \\ 0010 & 110 \\ 0001 & 111 \end{bmatrix} \Longrightarrow$$

$$H=\begin{bmatrix} 1011 & 100 \\ 0111 & 010 \\ 1101 & 001 \end{bmatrix}$$

$$\hat{x} = x + e \qquad \|e\| = 1$$

$$e = [0010000]$$

$$S = H\hat{x} = Hx + He = He =$$

$$= \begin{bmatrix} 1011 & 100 \\ 0111 & 010 \\ 1101 & 001 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

THIRD COLUMN of H

IN GENERAL FOR HAM(r,2)

$H = [h_1, h_2, \dots, h_n]$ $\quad n = 2^r - 1$

$h_i \in \mathbb{Z}_2^r$

FOR SINGLE ERRORS:

$$S_i = H \cdot e_i = [h_1, h_2, \dots, h_i, \dots, h_n] \begin{array}{c} \\ \\ \\ i \\ \\ \\ \end{array} \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} =$$

$$= h_i$$

Since $h_i \neq h_j \Rightarrow S_i \neq S_j$

Different errors have different syndromes $\Rightarrow$ Error can be computed if we know the syndrome

EXAMPLE 1) $n=7$, $k=4$, $q=2$

$$H=\begin{bmatrix}1&0&1&1&1&0&0\\1&1&0&1&0&1&0\\1&1&1&0&0&0&1\end{bmatrix}=\begin{bmatrix}h_1 & h_2 & h_3 & h_4 & h_5 & h_6 & h_7\end{bmatrix}$$

If $s=\begin{bmatrix}1\\1\\0\end{bmatrix}$ then $e=\begin{bmatrix}0\\0\\0\\1\\0\\0\\0\end{bmatrix}$.

Bit number four is distorted in the message since

$$s=h_4.$$

2) $G=\begin{bmatrix}1&1&1\end{bmatrix}$ – Repetition code $n=3$

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

Repetition code for $n=3$ is $(3,2,3)$ HAMMING CODE

HAM$(2,2)$

HAMMING CODES $(n, 2^k, 3) =$

$(2^r-1, 2^{2^r-1-r}, 3)$ are <u>perfect</u>

FOR $q=2$

<u>Proof</u> $\ell = 1$

$2^k = 2^{2^r-1-r}$

volume of a ball with radius $\ell = 1$ is $1+n = 1+2^r-1 = 2^r$

$$2^k = 2^{2^r-1-r} = \frac{2^n}{n+1} = \frac{2^{2^r-1}}{2^r}$$

<u>EXAMPLE</u>. $n=7, k=4, r=3$

$$|Ham(3,2)| = 16$$

$$16 = \frac{2^7}{1+7} = 2^{7-3}$$

$HAM(r,2)$ is $(2^r-1, 2^{2^r-r-1}, 3)$

perfect single error correcting code

If

$$H = [h_1, h_2, \ldots, h_n]$$

$$n = 2^r - 1$$

Then $h_i \neq 0$, $h_i \neq h_j$

$$h_i \in \mathbb{Z}_2^r$$

EXAMPLE

$HAM(3,2)$ $(7,16,3)$ code

$$G = \left[\begin{array}{cccc|ccc} 1&0&0&0&0&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&1&1&1 \end{array}\right]; \quad H = \left[\begin{array}{cccc|ccc} 0&1&1&1&1&0&0 \\ 1&0&1&1&0&1&0 \\ 1&1&0&1&0&0&1 \end{array}\right]$$

If $H = [h_1, h_2, \dots, h_n]$

$S = H\hat{x} = He$ Then $e = (0..0\overset{i}{1}0..0)$
$= e_i$

Iff $S = h_i$

Extended Binary HAMMING CODE

$(2^r, 2^{2^r - r - 1}, 4)$

detecting 3 errors

$$H_{ext} = \left.\begin{bmatrix} H & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ \hline 1\,1 \cdots 1 & 1 \end{bmatrix}\right\} r+1$$

correct single errors
and detect double errors

Any 3 columns in H_{ext} are linearly independent (sum of any three columns is not equal to the column of all zeros, since in the last rows in the sum we have one)

<u>EXAMPLE</u> $r=3$ $(8,16,4)$ extended HAMMING CODE with

$$H=\left[\begin{array}{ccccccc|c} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right]$$

DECODING

LET $S = H\hat{x} = \begin{bmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \end{bmatrix}$ $(r=3)$

1. If $S_4 = 0$ and $(S_1, S_2, S_3) = 0 \Rightarrow$ no errors

2. If $S_4 = 0$ and $(S_1, S_2, S_3) \neq 0 \Rightarrow$ double errors

3. If $S_4 = 1$ and $(S_1, S_2, S_3) = 0 \Rightarrow$ error in the last bit

4. If $S_4 = 1$ and $(S_1, S_2, S_3) \neq 0$ $\Rightarrow$ single error in the bit j where (S_1, S_2, S_3) is the binary representation of j