①

Hamming Codes

Single error correcting binary codes

$$\left.\begin{array}{l} 01011 \\ 11010 \end{array}\right\} \text{Hamming Distance is } 2.$$

How to determine?

Check distance bitwise 1st bit 4th biT distance 2

Equivalent
$$\begin{array}{r} 01011 \\ 11010 \\ \hline 10001 \end{array}$$

Add & check # of 1's in result.

Hamming distance of a code:

$$d_H = \min_{i,j} (\text{Hamming} (i,j)).$$

Distance helps use determine detection & correction capabilities

Weight of a code word

distance from 0 codeword

Hamming Codes

$$\overset{H}{\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}} \qquad \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ m_4 \\ m_5 \\ m_6 \\ m_7 \end{bmatrix}$$

Let the data to be sent be: 1 0 1 0

∴ check bits are 0 0 1

∴ we send 0 0 1 1 0 1 0

Why 0 0 1 as check bits?

$$H \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

$$\therefore \quad \begin{aligned} c_1 \oplus m_4 \oplus m_6 \oplus m_7 &= 0 \\ c_2 \oplus m_4 \oplus m_5 \oplus m_6 &= 0 \\ c_3 \oplus m_5 \oplus m_6 \oplus m_7 &= 0 \end{aligned} \qquad \Rightarrow \quad \begin{aligned} c_1 &= 0 \\ c_2 &= 0 \\ c_3 &= 1 \end{aligned}$$

If no error we get $H \cdot v = 0$

Syndrome

Suppose 1 error.

0 0 1 1 0 1 0

$$H \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ \boxed{1} \\ 0 \end{bmatrix} \quad \overset{?}{\underline{\underline{\text{error}}}}$$

Know that $H \cdot r = 0$ if no error.

Instead of

$$\begin{matrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ \boxed{1} \\ 0 \end{matrix} \longrightarrow \text{error. get } 0.$$

Getting $r = v + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$

$H \cdot r$ we get what $H \cdot v + H \cdot e$

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

∴ compare what you get with the columns of H.
If you get a match there must have been 1 error in the $\underline{\underline{j^{th}}}$ column of r

(Youtube - Randell Heyman)

(Note terminology ie. $b_1 \dots b_7$ differ.)

$$\begin{array}{c}H\\ \begin{bmatrix}1&0&0&1&0&1&1\\0&1&0&1&1&1&0\\0&0&1&0&1&1&1\\ & & & & & & \\ & & & & & & \end{bmatrix}\end{array} \times \begin{bmatrix}c_1\\c_2\\c_3\\m_4\\m_5\\m_6\\m_7\end{bmatrix} = \begin{bmatrix}0\\0\\0\end{bmatrix}$$

↳ code word

If 3 check bits then 3 linear equations linearly independent.

$$c_1 + m_4 + m_6 + m_7 = 0$$
$$c_2 + m_4 + m_5 + m_6 = 0$$
$$c_3 + m_5 + m_6 + m_7 = 0$$

Equivalently $c_1 = m_4 + m_6 + m_7$

$$\left.\begin{array}{l}Ha = 0\\ Hb = 0\end{array}\right. \Rightarrow H(a+b) = 0$$

$\Rightarrow$ a+b is a code word.

③ How many code words

① Prove that the minimum weight of a block code is the Hamming distance of the code.

② Prove that the all 0 vector is always a codeword.

Def: block code. One in which ∃ matrix H with n-k rows such that
$H \cdot a = 0$

Generator Matrix

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

$$= \left[\begin{array}{c|cccc} I_{\underset{n-k\;\;n-k}{3\times 3}} & 1 & 0 & 1 & 1 \\ & 1 & 1 & 1 & 0 \\ & 0 & 1 & 1 & 1 \end{array}\right] = [I \mid A]$$

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

$$= \left[A^T \mid I_{\underset{k\;\;k}{4\times 4}} \right]$$

$$\therefore [1\ 0\ 1\ 0] \cdot G =$$

$$[0\ 0\ 1\ 1\ 0\ 1\ 0]$$

Generalizing the (7, 4) code with Hamming distance 3

H_r = $r \times 2^r - 1$ matrix where the columns are the binary representations of $1, \ldots 2^r - 1$.

This is a:

$$(2^r - 1,\ 2^r - r - 1)$$ with distance 3.

$r=4$ Eg. (15, 11) code.

11 data bites
4 check bits
code word of length 15.

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & & \\ 0 & 0 & 0 & 1 & 1 & & \\ 0 & 1 & 1 & 0 & 0 & & \\ 1 & 0 & 1 & 0 & 1 & \cdots & \end{pmatrix}$$

Golay code (23, 12)

$dH_{min} = 7$ ∴ correct upto 3 errors
detect 6 errors

Parity check Matrix is
$\underline{\underline{11 \times 23}}$

$$A_{11 \times 12} \mid I_{11 \times 11}$$

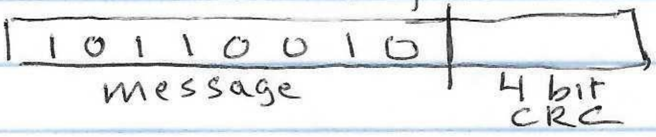
$\boxed{24, 12, 8}$

Voyager
1 & 2

Polynomial Codes

Example: Generator polynomial $x^4 + x^2 + 1$
Note this $G(x)$ has degree 4.

Let the message be 10110010
Note that the message has 8 bits
$M(x)$ is thus $x^7 + x^5 + x^4 + x$
When sending a message we can visualize this as follows:



Now
$$M(x) \cdot x^4 = x^{11} + x^9 + x^8 + x^5$$
We now divide $M(x) \cdot x^4$ by $G(x)$:

$$\begin{array}{r|l}
 & x^7 + x^4 + x^3 + x^2 = Q(x) \\
\hline
x^4 + x^2 + 1 & x^{11} + x^9 + x^8 + x^5 \\
 & \underline{x^{11} + x^9 + x^7} \\
 & x^8 + x^7 + x^5 \\
 & \underline{x^8 + x^6 + x^4} \\
 & x^7 + x^6 + x^5 + x^4 \\
 & \underline{x^7 + x^5 + x^3} \\
 & x^6 + x^4 + x^3 \\
 & \underline{x^6 + x^4 + x^2} \\
 & x^3 + x^2 = R(x)
\end{array}$$

The CRC is 1100
We transmit $M(x)x^4 + R(x)$ which is
$x^{11} + x^9 + x^8 + x^5 + x^3 + x^2$ or:

Actions at Receiver

Note that T(x) was:

T(x)	1 0 1 1 0 0 1 0	1 1 0 0

Assume received or arrived info is A(x):

A(x)	1 0 1 1 0 0 1 1	1 1 0 1
	↑	↑

Note that errors are indicated by the arrows.
There are 2 errors.

The receiver divides A(x) by G(x).

$$
\begin{array}{r l}
 & x^7 + x^4 + x^3 + x^2 + 1 \\ \cline{2-2}
x^4 + x^2 + 1 \big) & x^{11} + x^9 + x^8 + x^5 + x^4 + x^3 + x^2 + 1 \\
 & x^{11} + x^9 + x^7 \\ \cline{2-2}
 & x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1 \\
 & x^8 + x^6 + x^4 \\ \cline{2-2}
 & x^7 + x^6 + x^5 + x^3 + x^2 + 1 \\
 & x^7 + x^5 + x^3 \\ \cline{2-2}
 & x^6 + x^2 + 1 \\
 & x^6 + x^4 + x^2 \\ \cline{2-2}
 & x^4 + 1 \\
 & x^4 + x^2 + 1 \\ \cline{2-2}
 & x^2 \qquad \text{Non-zero remainder}
\end{array}
$$

There is a remainder hence there was an error in the transmission. We detected this fact.

Note that we can write

$A(x) = T(x) + E(x)$

Hence $E(x) = x^4 + 1$ which simply notes that the errors were in these 2 positions.
(Receiver of course does not know this)