

### 3.13 Hamming Code

- The first class of binary linear block code discovered by R. W. Hamming (1915 – 1998)

R. W. Hamming, “Error detecting and error correcting codes”,  
*Bell System Technical Journal*, vol. 29, pp. 147 – 160, 1950.

- For any positive integer  $m \geq 3$ , there exists a Hamming code with the following parameters:

block code length  $n = 2^m - 1$

message length  $k = 2^m - 1 - m$

minimum Hamming distance  $d_{min} = 3$

error-correction capability  $t = 1$

**Example:** (7, 4) Hamming code (Example 3.1 & 3.5)

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

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

- For a Hamming code of length  $2^m - 1$ , its parity-check matrix is a matrix whose columns consist of the entire set of the non-zero binary  $m$ -tuples.

### 3.14 Golay Code

- The  $(23,12)$  Golay code is the only known multiple-error-correcting binary perfect code, which is capable of correcting 3 or fewer random errors in a block of 23 digits,  $d_{min} = 7$ . (Discovered by Golay in 1949).

- The  $(23, 12)$  Golay code is either generated by

$$g_1(x) = 1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11}$$

or by  $g_2(x) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}$

- Both  $g_1(x)$  and  $g_2(x)$  are factors of  $x^{23} + 1$   
and  $x^{23} + 1 = (1 + x)g_1(x)g_2(x)$

- **Golay's paper was published in 1949.**

**M. J. E. Golay, "Notes on digital coding", *proc. IRE*, 37, pp. 567, June 1949.**

- **Golay codes have been frequent application in the US space program, most notably with the Voyager I and II spacecraft, providing (1979 – 81) clear color pictures of Jupiter and Saturn.**

### **3.15 Reed-Muller Code (RM Code)**

- **Reed-Muller codes were discovered by Muller in 1954, and shortly thereafter a better algebraic representation was provided by Reed along with an elegant decoding algorithm.**
- **The first-order RM code of length 32 was used in 1969 for the error-control system of the Mariner and Viking deep-space probes of Mars.**

- The original  $r$ -th order RM codes were binary and noncyclic, and formed a special subclass of Euclidean geometry (EG) codes.

(Details can also be found in Lin / Costello Book, chap. 8)

The  $r$ -th order binary RM code has the following parameters:

$$n = 2^m$$

$$k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$$

$$n - k = 2^m - k = \sum_{i=0}^{m-r-1} \binom{m}{i}$$

$$d_{min} = 2^{m-r}$$

Where  $r < m$  for any integer  $m$ .

- Since a RM code is a linear code, it is defined by a procedure for constructing a nonsystematic generator matrix.

Let  $\bar{u} = (u_0, u_1, \dots, u_{n-1})$

$\bar{v} = (v_0, v_1, \dots, v_{n-1})$  be two vectors.

Define vector sum as

$$\bar{u} + \bar{v} = (u_0 + v_0, u_1 + v_1, \dots, u_{n-1} + v_{n-1})$$

and vector product as

$$\bar{u} \cdot \bar{v} = (u_0 v_0, u_1 v_1, \dots, u_{n-1} v_{n-1})$$

- Let  $\bar{v}_0$  be a vector whose  $2^m$  components are all 1s. Then  $\bar{v}_0$  is called an identity vector.

Let  $\bar{v}_1, \bar{v}_2, \dots, \bar{v}_m$  be the rows of a matrix with all possible  $m$ -tuples as columns. We call them the basis vectors.

The  $r$ -th order RM code is formed by using the basis vectors  $\bar{v}_1, \bar{v}_2, \dots, \bar{v}_m$  and all of their vector products  $r$  or fewer at a time.

- The generator matrix of the  $r$ -th order RM code is defined as

$$G = \begin{bmatrix} \bar{v}_0 \\ \bar{v}_1 \\ \vdots \\ \bar{v}_m \\ \bar{v}_1 \bar{v}_2 \\ \bar{v}_1 \bar{v}_3 \\ \vdots \\ \bar{v}_{m-1} \bar{v}_m \\ \bar{v}_1 \bar{v}_2 \bar{v}_3 \\ \vdots \\ \bar{v}_{m-2} \bar{v}_{m-1} \bar{v}_m \\ \vdots \\ \bar{v}_1 \bar{v}_2 \cdots \bar{v}_r \\ \vdots \\ \bar{v}_{m-r+1} \cdots \bar{v}_{m-1} \bar{v}_m \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} \bar{v}_0 \\ \bar{v}_m \\ \bar{v}_{m-1} \\ \vdots \\ \bar{v}_1 \\ \bar{v}_m \bar{v}_{m-1} \\ \bar{v}_m \bar{v}_{m-2} \\ \vdots \\ \bar{v}_2 \bar{v}_1 \\ \bar{v}_m \bar{v}_{m-1} \bar{v}_{m-2} \\ \vdots \\ \vdots \\ \bar{v}_m \bar{v}_{m-1} \cdots \bar{v}_{m-r+1} \end{bmatrix}$$

where  $\bar{v}_i = (v_{i,0}, v_{i,1}, \dots, v_{i,n-1})$

**Example:** Consider the 2<sup>nd</sup>-order RM code for  $m = 4$ ,

$$n = 2^4 = 16$$

$$k = 1 + \binom{4}{1} + \binom{4}{2} = 11$$

$$n - k = 16 - 11 = 5$$

$$d_{\min} = 2^2 = 4$$

This is a (16, 11) linear code.

The generator matrix is given by

$$\mathbf{G}_{R(2,4)} = \begin{bmatrix} \bar{v}_0 \\ \bar{v}_4 \\ \bar{v}_3 \\ \bar{v}_2 \\ \bar{v}_1 \\ \bar{v}_4\bar{v}_3 \\ \bar{v}_4\bar{v}_2 \\ \bar{v}_4\bar{v}_1 \\ \bar{v}_3\bar{v}_2 \\ \bar{v}_3\bar{v}_1 \\ \bar{v}_2\bar{v}_1 \end{bmatrix}$$

where

$$\bar{v}_0 = (1111 \ 1111 \ 1111 \ 1111)$$

$$\bar{v}_4 = (0000 \ 0000 \ 1111 \ 1111)$$

$$\bar{v}_3 = (0000 \ 1111 \ 0000 \ 1111)$$

$$\bar{v}_2 = (0011 \ 0011 \ 0011 \ 0011)$$

$$\bar{v}_1 = (0101 \ 0101 \ 0101 \ 0101)$$

$$\bar{v}_4\bar{v}_3 = (0000 \ 0000 \ 0000 \ 1111)$$

$$\bar{v}_4\bar{v}_2 = (0000 \ 0000 \ 0011 \ 0011)$$

$$\bar{v}_4\bar{v}_1 = (0000 \ 0000 \ 0101 \ 0101)$$

$$\bar{v}_3\bar{v}_2 = (0000 \ 0011 \ 0000 \ 0011)$$

$$\bar{v}_3\bar{v}_1 = (0000 \ 0101 \ 0000 \ 0101)$$

$$\bar{v}_2\bar{v}_1 = (0001 \ 0001 \ 0001 \ 0001)$$

- Since  $k = \binom{m}{0} + \binom{m}{1} + \binom{m}{2} + \dots + \binom{m}{r}$

gives the number of information bits of the  $r$ -th order RM code of

length  $2^m$ , the information vector is generally expressed as

$$\bar{d} = (d_0 \ d_m \ d_{m-1} \ \dots \ d_1 \ d_{m,m-1} \ d_{m,m-2} \ \dots \ d_{m,m-1,\dots,m-r+1})$$

For example,  $r = 2, m = 4, k = 11$

We have  $\bar{d} = (d_0 \ d_4 \ d_3 \ d_2 \ d_1 \ d_{43} \ d_{42} \ d_{41} \ d_{32} \ d_{31} \ d_{21})$

- The codewords are given by

$$\bar{c} = \bar{d} \cdot G$$

**Example:**  $r = 1, m = 3$

$$\bar{c} = (c_0 \ c_1 \ \cdots \ c_7) = (d_0 \ d_3 \ d_2 \ d_1) \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$