For a message word $a = a_1a_2a_3a_4$, we have

$$\mathbf{aG} = (a_1 + a_2 + a_4 \quad a_1 + a_3 + a_4 \quad a_1 \quad a_2 + a_3 + a_4 \quad a_2 \quad a_3 \quad a_4)$$

Observe that the message symbols occupy the 3rd, 5th, 6th and 7th positions while the 1st, 2nd and 4th positions are occupied by check symbols as they do in the case of Hamming codes defined originally.

Going back to the case of arbitrary m, we may define

$$\boldsymbol{\sigma} = \begin{pmatrix} 1 & 2 & 2^2 & \cdots & 2^{m-1} & 3 & 5 & 6 & 7 & 9\cdots \\ n & n-1 & n-2 & \cdots & n-m+1 & 1 & 2 & 3 & 4 & 5\cdots \end{pmatrix}$$

Applying $\boldsymbol{\sigma}$ to the columns of $\mathbf{H}^t$ gives

$$\mathbf{H}_1 = (\mathbf{A} \quad \mathbf{I}_m)$$

so that the corresponding generating matrix is

$$\mathbf{G}_1 = (\mathbf{I}_{n-m} \quad \mathbf{A}^t)$$

Now applying $\boldsymbol{\sigma}^{-1}$ to the columns of $\mathbf{G}_1$ gives the generator matrix $\mathbf{G}$ of the code corresponding to the parity check matrix $\mathbf{H}^t$. With this generating matrix $\mathbf{G}$, we find that the code word in the Hamming code corresponding to the message word a is the same as the code word corresponding to a for the Hamming code originally defined. Thus, the two definitions of the Hamming code give the *same* code.

Let $\mathscr{C}$ be a Hamming code of length $n = 2^r - 1$ so that $\mathscr{C}$ is a code with a parity check matrix $\mathbf{H}$ of order $r \times n$ in which the columns are the binary representations of the numbers $1, 2, \ldots, n$. Then no two columns of $\mathbf{H}$ are identical and so the code is single error correcting (Theorem 1.5). But then the minimum distance of the code is at least 3 (Theorem 1.2). Thus we have an alternative proof of Theorem 3.1.

Examples 6.1

Case (i)

As a first illustration of the use of the above discussion we obtain all the code words of binary Hamming code of length $7 = 2^3 - 1$. A parity check matrix of this code is

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Applying the permutation

$$\boldsymbol{\sigma} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 1 & 5 & 2 & 3 & 4 \end{pmatrix}$$

to the columns of **H** gives a parity check matrix

$$\mathbf{H}_1 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

The corresponding generator matrix is

$$\mathbf{G}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Now apply the permutation $\boldsymbol{\sigma}^{-1}$ to the columns of $\mathbf{G}_1$ to obtain the generator **G** matrix corresponding to the parity check matrix **H**:

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

The code words of this Hamming code are:

0	0	0	0	0	0	0	1	0	0	0	0	1	1	0	1	0	1	1	1	1
1	1	0	1	0	0	1	0	1	0	0	1	0	1	0	1	1	0	0	1	1
0	1	0	1	0	1	0	0	0	1	1	0	0	1	1	0	1	0	1	0	1
1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	0	1	0	1	1	0
1	1	1	0	0	0	0	1	0	1	1	0	1	0	1	1	1	1	1	1	1
							0	1	1	1	1	0	0							

Case (ii)

Our second illustration results in a generator matrix of binary Hamming code of length $15 = 2^4 - 1$. A parity check matrix of this code is

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

To obtain a canonical form of parity check matrix, we consider a permutation

$$\boldsymbol{\sigma} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 15 & 14 & 1 & 13 & 2 & 3 & 4 & 12 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \end{pmatrix}$$

Then

$$\mathbf{H}_1 = \boldsymbol{\sigma}(\mathbf{H}) = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Corresponding to $\mathbf{H}_1$ the generator matrix is $\mathbf{G}_1 = (\mathbf{I}_{11} \quad \mathbf{A}^t)$, where

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Applying the permutation $\boldsymbol{\sigma}^{-1}$ to the columns of $\mathbf{G}_1$, we obtain the generator matrix of the Hamming code as

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Theorem 6.3
The binary cyclic code of length $n = 2^m - 1$ for which the generator is the minimal polynomial of a primitive element of GF(2^m) is equivalent to the $(n - m, n)$ Hamming code.

Proof
Let α be a primitive element of GF(2^m). Let $m(X)$ be the minimal polynomial of α over $\mathbb{B}$. Since for $\beta \in \text{GF}(2^m)$, β and β^2 have the same minimal polynomial, $\alpha, \alpha^2, \ldots, \alpha^{2^{m-1}}$ are distinct roots of $m(X)$. Since the degree $[\text{GF}(2^m):\mathbb{B}] = m$, the degree of the minimal polynomial of any element of GF(2^m) over $\mathbb{B}$ is at most m. Hence

$$m(X) = (X - \alpha)(X - \alpha^2)\cdots(X - \alpha^{2^{m-1}})$$

The elements $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$ form a basis of GF(2^m) over $\mathbb{B}$ and, therefore,

every element of GF(2^m) can be uniquely written as

$$\sum_{i=0}^{m-1} e_i \alpha^i \quad e_i \in \mathbb{B}$$

For $0 \leq j \leq 2^m - 2$, let

$$\alpha^j = \sum_{i=0}^{m-1} e_{ij} \alpha^i$$

and let **H** be the $m \times n$ matrix, the $(j+1)$th column of which is

$$(e_{0j} \quad e_{1j} \quad \cdots \quad e_{m-1,j})^t$$

Every row vector

$$(e_{0j} \quad e_{1j} \quad \cdots \quad e_{m-1,j})$$

gives the binary representation of one and only one positive integer at most n.

Now $a(X) + \langle X^n - 1 \rangle$ belongs to the cyclic code generated by $m(X)$ iff $a(\alpha) = 0$. But this is so iff $\mathbf{H}a^t = 0$, where $a = (a_0 a_1 \cdots a_{n-1})$ with

$$a(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$$

Therefore, the cyclic code generated by $m(X)$ is the same as the code given by the parity check matrix **H**. But **H** is obtained by permutating the binary representations of the numbers $1, 2, \ldots, n$. This completes the proof.

Remark 6.1

Observe that, in the above proof, we have also shown that a binary Hamming code is a BCH code (up to equivalence).

We have seen earlier that every non-zero element of GF(2^m) is a root of the polynomial $X^n - 1$ with $n = 2^m - 1$. Therefore, the minimal polynomial of every element β of GF(2^m) divides $X^n - 1$. Also the minimal polynomials of two elements are either identical or relatively coprime. Hence, if α is a primitive element of GF(2^m) and $d \geq 2$ is a positive integer then

$$g(X) = \text{LCM}\{m_1(X), \ldots, m_{d-1}(X)\}$$

where $m_i(X)$ denotes the minimal polynomial of α^i, divides $X^n - 1$. It then follows that the polynomial code of length n generated by $g(X)$ is the same as the cyclic code with generator $g(X)$. Thus, every binary BCH code is a cyclic code.

6.4 NON-BINARY HAMMING CODES

We have so far restricted ourselves only to binary Hamming codes. However, Hamming codes may be defined over any finite field GF(q).