In the matrix form, these may be rewritten as

$$(c_0 \quad c_1 \quad \cdots \quad c_6)\begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = 0$$

or $\mathbf{cH} = 0$, where $\mathbf{H}$ is the 7×7 matrix

$$\begin{pmatrix} 0 & 0 & h_4 & h_3 & h_2 & h_1 & h_0 \\ 0 & h_4 & h_3 & h_2 & h_1 & h_0 & 0 \\ h_4 & h_3 & h_2 & h_1 & h_0 & 0 & 0 \\ h_3 & h_2 & h_1 & h_0 & 0 & 0 & h_4 \\ h_2 & h_1 & h_0 & 0 & 0 & h_4 & h_3 \\ h_1 & h_0 & 0 & 0 & h_4 & h_3 & h_2 \\ h_0 & 0 & 0 & h_4 & h_3 & h_2 & h_1 \end{pmatrix}$$

Definition 6.1

Now let $\mathscr{C}$ be a cyclic code of length n over F with generator polynomial $g(X)$ of degree r. Let

$$h(X) = h_0 + h_1 X + \cdots + h_{n-r} X^{n-r}$$

be its check polynomial. Then a word

$$c(X) + I = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1} + I$$

is in $\mathscr{C}$, iff $c(X)h(X) = 0$ in $F[X]/I$, where as before $I = \langle X^n - 1 \rangle$. This is equivalent to saying that

$$\sum_{i=0}^{n-1} c_i h_{j-i} = 0 \quad j = 0, 1, 2, \ldots, n-1$$

where the subscripts are taken modulo n and where it is also understood that $h_j = 0$ if $j > n - r$. These are the n check equations and, in the matrix form, may be rewritten as

$$\mathbf{cH} = (c_0 \quad c_1 \quad \cdots \quad c_{n-1})\mathbf{H} = 0$$

where $\mathbf{H}$ is the $n \times n$ matrix

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & h_{n-r} & \cdots & h_1 & h_0 \\ 0 & & & h_{n-r} & h_{n-r-1} & \cdots & h_0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & & \vdots \\ h_0 & 0 & \cdots & \cdots & \cdots & \cdots & h_2 & h_1 \end{pmatrix}$$

the rows of which are defined inductively as follows:

The first row is taken as

$$0 \quad \cdots \quad 0 \quad h_{n-r} \quad \cdots \quad h_1 \quad h_0$$

and once the ith row is defined, the $(i+1)$th row is obtained by giving a cyclic shift to the ith. The matrix $\mathbf{H}$ thus obtained is called the **parity check matrix** of the cyclic code $\mathscr{C}$ (mark the difference from the usual definition of a parity check matrix!)

Thus $c(X)+I$ is in $\mathscr{C}$ iff $\mathbf{cH}=0$ or equivalently $\mathbf{H}^t\mathbf{c}^t=0$. From this, it follows that the dual code $\mathscr{C}^\perp$ contains the linear code generated by the rows of $\mathbf{H}^t=\mathbf{H}$, as $\mathbf{H}$ is clearly a symmetric matrix. The dual code $\mathscr{C}^\perp$ is of dimension $n-(n-r)=r$ and clearly the first r rows of $\mathbf{H}$ are linearly independent. Therefore, the linear code generated by $\mathbf{H}$ must be of dimension r, and hence, it must equal $\mathscr{C}^\perp$. Also, we could as well have taken the $r \times n$ matrix

$$\mathbf{H}_1 = \begin{pmatrix} 0 & 0 & 0 & h_{n-r} & \cdots & h_1 & h_0 \\ 0 & & h_{n-r} & h_{n-r-1} & \cdots & h_0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ h_{n-r} & \cdots & \cdots & \cdots & h_0 & 0 & 0 \end{pmatrix}$$

as the parity check matrix of $\mathscr{C}$. (Now we have the usual form of the parity check matrix!)

Since the rows of the matrix $\mathbf{H}$ are all the possible cyclic shifts of the vector

$$0 \quad \cdots \quad 0 \quad h_{n-r} \quad \cdots \quad h_1 \quad h_0$$

of length n, any linear combination over F of the rows of $\mathbf{H}$ will again be a linear combination of the rows of $\mathbf{H}$. Hence $\mathscr{C}^\perp$, the code generated by $\mathbf{H}$ (or $\mathbf{H}_1$) is again cyclic.

Reversing the order of the rows of $\mathbf{H}_1$, we may take the parity check matrix of $\mathscr{C}$ (and, so, also the generator matrix of $\mathscr{C}^\perp$) as

$$\mathbf{H}_2 = \begin{pmatrix} h_{n-r} & \cdots & h_1 & h_0 & 0 & \cdots & \cdots & 0 \\ 0 & h_{n-r} & \cdots & h_2 & h_1 & h_0 & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & h_{n-r} & \cdots & h_1 & h_0 \end{pmatrix}$$

Thus it follows (see Theorem 2.4) that code $\mathscr{C}^\perp$ is the polynomial code generated by

$$\begin{aligned} k(X) &= h_{n-r} + h_{n-r-1}X + \cdots + h_0 X^{n-r} \\ &= X^{n-r}(h_0 + h_1 X^{-1} + \cdots + h_{n-r}X^{-n+r}) \end{aligned}$$

Now

$$X^n - 1 = g(X)h(X) \Rightarrow X^{-n} - 1 = g(X^{-1})h(x^{-1})$$

or

$$1 - X^n = X^r g(X^{-1})k(X)$$

showing that $k(X) \mid X^n - 1$ as it should.

Theorem 6.2
Let $\mathscr{C}$ be a cyclic code of length n over F with generator polynomial $g(X)$ of degree r and $h(X)$ as its check polynomial. Then:

(i) the dual code $\mathscr{C}^{\perp}$ is also cyclic with $k(X) = X^{n-r}h(X^{-1})$ as a generator polynomial; and
(ii) the dual code $\mathscr{C}^{\perp}$ is equivalent to the code generated by $h(X)$.

Proof
We only have to prove (ii).

Consider the permutation matrix $\mathbf{P} = (p_{ij})$ where

$$p_{ij} = \begin{cases} 1 & \text{if } i + j = n + 1 \\ 0 & \text{otherwise} \end{cases}$$

Let $\mathbf{c}_1, \ldots, \mathbf{c}_n$ denote the columns of the generator matrix $\mathbf{H}_1$ of $\mathscr{C}^{\perp}$. Then

$$\begin{aligned} \mathbf{H}_1\mathbf{P} &= (\mathbf{c}_1 \quad \cdots \quad \mathbf{c}_n)P \\ &= \left(\sum_i \mathbf{c}_i p_{i1} \quad \sum \mathbf{c}_i p_{i2} \quad \cdots \quad \sum \mathbf{c}_i p_{in} \right) \\ &= (\mathbf{c}_n \quad \mathbf{c}_{n-1} \quad \cdots \quad \mathbf{c}_1) \\ &= \begin{pmatrix} h_0 & h_1 & \cdots & h_{n-r} & 0 & \cdots & \cdots & 0 \\ 0 & h_0 & \cdots & h_{n-r-1} & h_{n-r} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & h_0 & h_1 & \cdots & h_{n-r} \end{pmatrix} \end{aligned}$$

The linear code generated by $\mathbf{H}_1\mathbf{P}$ is thus the code $\langle h(X) + I \rangle$ generated by $h(X)$. But the code generated by $\mathbf{H}_1\mathbf{P}$ is equivalent to $\mathscr{C}^{\perp}$. Hence the result.

Exercise 6.2

1. Is a code equivalent to a cyclic code cyclic?
2. Determine the check polynomials and also parity check matrices of the cyclic codes constructed in Exercise 6.1.
3. Determine the duals of the codes constructed in Exercise 6.1.

6.3 BCH AND HAMMING CODES AS CYCLIC CODES

Let $\mathscr{C}$ be a cyclic code of length n over F (i.e. an ideal in $F[X]/I, I = \langle X^n - 1 \rangle$) with generator matrix $g(X)$ of degree r. Let $\alpha_1, \alpha_2, \ldots, \alpha_r$ be the roots of $g(X)$ in a suitable extension field of F. Then

$$g(X) = (X - \alpha_1) \cdots (X - \alpha_r)$$

Observe that $g(X)$ divides a polynomial $a(X)$ iff $\alpha_1, \ldots, \alpha_r$ are among the roots of $a(X)$. Therefore $a(X) + I$ is in $\mathscr{C}$ iff $\alpha_1, \ldots, \alpha_r$ are among the roots of $a(X)$.

Given a positive integer m, we defined a binary $(2^m - m - 1, 2^m - 1)$ Hamming code by taking $\mathbf{H}^t$ as the parity check matrix where $\mathbf{H}$ is the $m \times (2^m - 1)$ matrix the ith row of which, $1 \leq i \leq 2^m - 1$, is the binary representation of the number i and by insisting that in a code word $b_1 b_2 \cdots b_n$ $(n = 2^m - 1)$, $b_1, b_2, b_{2^2}, \ldots, b_{2^{m-1}}$ are the check symbols. If we do not insist on the condition about the position of the check symbols, we may define the **binary Hamming code** as the code with parity check matrix $\mathbf{H}^t$.

With the parity check matrix given, it is not easy to find the code words. For finding these, we observe that $\mathbf{H}^t$ contains m columns, a suitable permutation of which forms the identity matrix $\mathbf{I}_m$ of order m. Let σ be a permutation of the columns of $\mathbf{H}^t$ which, when applied, transforms $\mathbf{H}^t$ into $(\mathbf{A} \quad \mathbf{I}_m) = \mathbf{H}_1$. The corresponding generating matrix then becomes

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

An application of the permutation σ^{-1} to the columns of $\mathbf{G}_1$ gives a generator matrix $\mathbf{G}$ of the Hamming code. The code words of the Hamming code are then given by $a\mathbf{G}$, $a \in V(n-m, 2)$.

We illustrate this procedure for the case $m = 3$. Here,

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

Applying the permutation

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

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

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

The corresponding generator matrix is

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

Applying σ^{-1} to the columns of $\mathbf{G}_1$ gives the generator matrix of the code corresponding to $\mathbf{H}^t$ as

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