Proof

Since all the characteristic roots of T are equal to 1, there exists a basis $e_1, e_2, \ldots, e_n$ with respect to which T is represented by its Jordan normal form

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

which is a square matrix of order n. then we have

$$\left.\begin{aligned} T(e_1) &= e_1 \\ T(e_i) &= e_{i-1} + e_i \end{aligned}\right\} \quad \text{for } 2 \leq i \leq n$$

Let W be a k-dimensional T-invariant subspace of V and let T_1 be the endomorphism of W induced by T. Then the characteristic polynomial of T_1 divides the characteristic polynomial of T so that all the characteristic roots of T_1 are also equal to 1. Then there exists a basis w_1, $w_2, \ldots, w_k$ of W such that

$$\left.\begin{aligned} T_1(w_1) &= w_1 \\ T_1(w_i) &= w_{i-1} + w_i \end{aligned}\right\} \quad \text{for } 2 \leq i \leq k$$

For $1 \leq i \leq k$, let

$$w_i = \sum_{j=1}^{n} \alpha_{ij} e_j$$

Then

$$\begin{aligned} w_1 = T_1(w_1) &= \sum_{j=1}^{n} \alpha_{ij} T(e_j) \\ &= \alpha_{11} e_1 + \sum_{j=2}^{n} \alpha_{ij}(e_{j-1} + e_j) \\ &= \sum_{j=1}^{n-1} (\alpha_{1j} + \alpha_{1j+1}) e_j + \alpha_{1n} e_n \end{aligned}$$

Therefore

$$\alpha_{1j} = \alpha_{1j} + \alpha_{1j+1} \qquad 1 \leq j \leq n-1$$

which show that

$$\alpha_{12} = \alpha_{13} = \cdots = \alpha_{1n} = 0$$

and

$$w_1 = \alpha_{11} e_1$$

We claim that

$$w_i = \alpha_{11}(e_1 + e_2 + \cdots + e_i) \quad 1 \le i \le k \tag{10.1}$$

Suppose that we have proved the relation up to $i < k$. Then

$$\begin{aligned} w_i + w_{i+1} &= T(w_{i+1}) \\ &= \alpha_{i+1,1} e_1 + \sum_{j=2}^{n} \alpha_{i+1,j}(e_{j-1} + e_j) \end{aligned}$$

which on comparison of coefficients of e_j gives

$$\alpha_{ij} + \alpha_{i+1,j} = \alpha_{i+1,j} + \alpha_{i+1,j+1} \quad 1 \le j \le n-1$$

or

$$\alpha_{ij} = \alpha_{i+1,j+1} \quad 1 \le j \le n-1 \tag{10.2}$$

The relations (10.1) for i and (10.2) together show that

$$\alpha_{i+1,j} = 0 \quad \text{for } j > i+1$$

and

$$\alpha_{i+1,j} = \alpha_{11} \quad \text{for } 1 \le j \le i+1$$

This proves that

$$w_{i+1} = \alpha_{11}(e_1 + e_2 + \cdots + e_{i+1})$$

Thus (10.1) holds $\forall i$, $1 \le i \le k$. Since $\alpha_{11} \ne 0$ (otherwise T is singular), W is spanned by

$$e_1, e_1 + e_2, \ldots, e_1 + e_2 + \cdots + e_k$$

which is the same as the space spanned by $e_1, \ldots, e_k$.

Theorem 10.6
Suppose that $\mathscr{C}$ is a binary self dual code of length $n = 2^a b$, $a \ge 1$, $b \ge 1$ and b odd, that is fixed (setwise) by a permutation group G satisfying the conditions

(a) G is transitive on the n coordinate positions;
(b) G has a Sylow 2-subgroup which is cyclic of order 2^a.

Then $\mathscr{C}$ contains code words of weight congruent to 2 modulo 4.

Proof

Let P be the cyclic Sylow 2-subgroup of G with generator π. Since $O(P)=2^a$, $O(G)=2^a e$, where e is odd and divisible by b. Then G contains a normal subgroup H with $G/H\cong P$, $O(H)=e$ (Proposition 10.5).

Let

$$\mathscr{C}_0=\{u\in\mathscr{C}\,|\,uh=u\,\forall h\in H\}$$

Since $O(H)$ is odd and n is even, H is not transitive (by Lemma 10.1). Then it follows (from Theorem 10.2) that G is imprimitive with the orbits of H forming a complete block system of G. All the blocks of G have the same length, l (say), and suppose that there are m blocks. Then

$$lm=n=2^a b$$

Each block being an orbit of H, H is transitive on each block and, therefore, $l\,|\,O(H)$ (Proposition 10.3(i)). Then l is odd. Therefore $2^a\,|\,m$. From the definition of complete block system, it follows that π is transitive on the blocks so that $m\le 2^a$. Thus $m=2^a$ and the orbits of H consist of 2^a blocks of length b each.

Therefore, the fixed subspace $(\mathbb{B}^n)_0$ has dimension 2^a with one generator for each block. Relabel the n coordinates in such a way that the elements in every orbit of H are consecutively numbered. Then the generator matrix of $(\mathbb{B}^n)_0$ becomes

$$\begin{pmatrix} \overbrace{111}^{b} & 000 & \cdots & 000 \\ 000 & 111 & \cdots & 000 \\ \vdots & \cdots & \ddots & \vdots \\ 000 & 000 & \cdots & 111 \end{pmatrix}$$

It follows from Theorem 10.5 that $\dim\mathscr{C}_0$ is 2^{a-1}. Also the action of the generator π of the cyclic group P on the blocks is represented by the square matrix

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

of order 2^a. Since the determinant of a matrix remains unchanged except for a possible change of sign when some rows are interchanged, the characteristic roots of $\mathbf{A}$ are the same as the characteristic roots of the identity matrix $\mathbf{I}$ of order n. Hence the characteristic roots of $\mathbf{A}$ are all 1. Therefore, there is a basis

$$v_1, v_2, \ldots, v_{2^a}$$

for $\mathbb{B}^{2^a}$ w.r.t. which π is represented by its Jordan normal form (Theorem 10.4), which is the square matrix

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & & \cdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 1 \end{pmatrix}$$

of order 2^a. Then, $\forall k$, $1 \leq k \leq 2^a$, $\mathbb{B}^n$ has exactly one subspace of dimension k. The rows of $2^{a-1} \times n$ matrix

$$\begin{pmatrix} \overline{b} & & & & \overline{b} & & & \\ 111 & 000 & \cdots & 000 & 111 & 000 & \cdots & 000 \\ 000 & 111 & \cdots & 000 & 000 & 111 & \cdots & 000 \\ \vdots & \ddots & & & \vdots & & \ddots & \vdots \\ 000 & 000 & \cdots & 111 & 000 & 000 & \cdots & 111 \end{pmatrix}$$

in which each row has two blocks of b ones as shown are linearly independent. Therefore, the rows of this matrix generate a subspace of dimension 2^{a-1} which must be the unique subcode $\mathscr{C}_0$. Since b is odd, weight of each row of $\mathbf{A}$ is equivalent to 2(mod 4), i.e. $\mathscr{C}_0$ contains words of weight equivalent to 2(mod 4).

Corollary
No binary cyclic self dual code has all its weights divisible by 4.

Proof
Let $\mathscr{C}$ be a binary cyclic self dual code of length $n = 2^a b$, where b is odd. Since the length of a self dual code is even, $a \geq 1$. Let σ be a cyclic permutation fixing $\mathscr{C}$, and let $G = \langle \sigma \rangle$ be the cyclic group generated by σ. Then $P = \langle \sigma^b \rangle$ is a cyclic Sylow 2-subgroup of G with order 2^a. The result then follows from the above theorem.

11

Hadamard matrices and Hadamard codes

11.1 HADAMARD MATRICES

Definition 11.1
A **Hadamard matrix** $\mathbf{M}$ of order n is a square matrix of order n with every entry equal to 1 or -1 such that $\mathbf{M}\mathbf{M}^t = n\mathbf{I}$. (Here $\mathbf{M}^t$ denotes the transpose of the matrix $\mathbf{M}$.)

Remarks 11.1

Note (i)
Let $\mathbf{M}$ be a Hadamard matrix of order n. Then

$$\mathbf{M}\mathbf{M}^t = n\mathbf{I} \Rightarrow (\det \mathbf{M})^2 = n^n$$

so that $\det \mathbf{M} \neq 0$ and hence $\mathbf{M}$ is non-singular.
Also

$$\mathbf{M}\mathbf{M}^t = n\mathbf{I} \Rightarrow \mathbf{M}^{-1}\left(\frac{1}{n}\mathbf{M}\mathbf{M}^t\right) = \mathbf{M}^{-1}$$

i.e.

$$\mathbf{M}^{-1} = \frac{1}{n}\mathbf{M}^t$$

Therefore, $\mathbf{M}^t\mathbf{M} = n\mathbf{I}$. Hence $\mathbf{M}^t$ is also a Hadamard matrix of order n.

Note (ii)
Let $\mathbf{M}$ be a Hadamard matrix of order n. Let $\mathbf{R}_1, \mathbf{R}_2, \ldots, \mathbf{R}_n$ denote the rows of $\mathbf{M}$. Let $\mathbf{M}_1$ be the matrix obtained from $\mathbf{M}$ by multiplying every entry of the ith

row of $\mathbf{M}$ by -1. Since $\mathbf{M}\mathbf{M}^{t} = n\mathbf{I}$

$$\mathbf{R}_j\mathbf{R}_k^{t} = \begin{cases} 0 & \text{if } j \neq k,\ 1 \leq j,\ k \leq n \\ n & \text{if } j = k,\ 1 \leq j \leq n \end{cases} \tag{11.1}$$

Let $\mathbf{S}_1, \ldots, \mathbf{S}_n$ denote the rows of $\mathbf{M}_1$ so that $\mathbf{S}_j = \mathbf{R}_j$ if $j \neq i$ and $\mathbf{S}_i = -\mathbf{R}_i$. Then $\mathbf{M}_1\mathbf{M}_1^{t} = (\lambda_{jk})$, where

$$\begin{aligned} \lambda_{jk} &= \mathbf{S}_j\mathbf{S}_k^{t} \\ &= \begin{cases} \mathbf{R}_j\mathbf{R}_k^{t} & \text{if } j \neq i,\ k \neq i \\ -\mathbf{R}_i\mathbf{R}_k^{t} & \text{if } j = i,\ k \neq i \\ -\mathbf{R}_j\mathbf{R}_i^{t} & \text{if } j \neq i,\ k = i \\ \mathbf{R}_i\mathbf{R}_i^{t} & \text{if } j = k = i \end{cases} \\ &= \begin{cases} 0 & \text{if } j \neq k \\ n & \text{if } j = k \end{cases} \end{aligned}$$

Hence $\mathbf{M}_1\mathbf{M}_1^{t} = n\mathbf{I}$ and $\mathbf{M}_1$ is a Hadamard matrix of order n. Thus if every entry of some row of $\mathbf{M}$ is multiplied by -1, then the resulting matrix is a Hadamard matrix of order n. Similarly, if every entry of a column of $\mathbf{M}$ is multiplied by -1, the resulting matrix is again a Hadamard matrix of order n.

Note (iii)
Given a Hadamard matrix of order n, by a repeated application of Note (ii) above, we can obtain a Hadamard matrix of order n in which every entry in the first row and in the first column is $+1$.

Note (iv)
If any two rows or any two columns are interchanged in a Hadamard matrix, then the resulting matrix is again Hadamard.

Definition 11.2
A Hadamard matrix of order n in which every entry in the first row and in the first column is $+1$ is called a **normalized Hadamard matrix** of order n.

In view of Note (iii) above, observe that if a Hadamard matrix of order n exists, then so does a normalized Hadamard matrix of n.

Examples 11.1

Case (i)
If

$$\begin{pmatrix} 1 & 1 \\ 1 & a \end{pmatrix}^2 = 2\mathbf{I}$$

then $1 + a = 0$ so that $a = -1$ and

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

is a normalized Hadamard matrix of order 2.

We observe that

$$\begin{pmatrix} -1 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

are some of the other Hadamard matrices of order 2.

Case (ii)

Let

$$\mathbf{M} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & a & b \\ 1 & c & d \end{pmatrix}$$

be a normalized Hadamard matrix of order 3. Then $\mathbf{MM}^t = 3\mathbf{I}$ and $1 + a + b = 0$.

But this relation is not possible with $a = \pm 1$ and $b = \pm 1$. Thus, there is no normalized Hadamard matrix of order 3 and, hence, there does not exist any Hadamard matrix of order 3.

We next give a procedure for obtaining a Hadamard matrix of order $2n$ from a given Hadamard matrix of order n.

Proposition 11.1

If $\mathbf{M}$ is a Hadamard matrix of order n, then

$$\begin{pmatrix} \mathbf{M} & \mathbf{M} \\ \mathbf{M} & -\mathbf{M} \end{pmatrix}$$

is a Hadamard matrix of order $2n$.

Proof

$$\begin{aligned}
\begin{pmatrix} \mathbf{M} & \mathbf{M} \\ \mathbf{M} & -\mathbf{M} \end{pmatrix}\begin{pmatrix} \mathbf{M} & \mathbf{M} \\ \mathbf{M} & -\mathbf{M} \end{pmatrix}^t &= \begin{pmatrix} \mathbf{M} & \mathbf{M} \\ \mathbf{M} & -\mathbf{M} \end{pmatrix}\begin{pmatrix} \mathbf{M}^t & \mathbf{M}^t \\ \mathbf{M}^t & -\mathbf{M}^t \end{pmatrix} \\
&= \begin{pmatrix} \mathbf{MM}^t + \mathbf{MM}^t & \mathbf{MM}^t - \mathbf{MM}^t \\ \mathbf{MM}^t - \mathbf{MM}^t & \mathbf{MM}^t + \mathbf{MM}^t \end{pmatrix} \\
&= \begin{pmatrix} 2n\mathbf{I}_n & \mathbf{0} \\ \mathbf{0} & 2n\mathbf{I}_n \end{pmatrix} \\
&= 2n\begin{pmatrix} \mathbf{I}_n & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_n \end{pmatrix} \\
&= 2n\mathbf{I}_{2n}
\end{aligned}$$

Hence

$$\begin{pmatrix} \mathbf{M} & \mathbf{M} \\ \mathbf{M} & -\mathbf{M} \end{pmatrix}$$

is a Hadamard matrix of order $2n$. Note: $\mathbf{I}_k$ denotes the identity matrix of order k. ■

We can also similarly prove that if $\mathbf{M}$ is a Hadamard matrix of order n, then

$$\begin{pmatrix} \mathbf{M} & -\mathbf{M} \\ \mathbf{M} & \mathbf{M} \end{pmatrix} \quad \begin{pmatrix} \mathbf{M} & \mathbf{M} \\ -\mathbf{M} & \mathbf{M} \end{pmatrix} \text{ and } \begin{pmatrix} -\mathbf{M} & \mathbf{M} \\ \mathbf{M} & \mathbf{M} \end{pmatrix}$$

are Hadamard matrices of order $2n$.

Using the above procedure, we find that

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

are Hadamard matrices of order 4.

Exercise 11.1

1. Without using the procedure of Proposition 11.1 and the remark below it, obtain a normalized Hadamard matrix of order 4.
2. Obtain a Hadamard matrix of order 8.

Theorem 11.1
If a Hadamard matrix of order n exists, then $n = 1, 2$ or a multiple of 4.

Proof
The matrix (1) is trivially a (normalized) Hadamard matrix of order 1 and we have already obtained Hadamard matrices of order 2. Also, we have proved that there does not exist a Hadamard matrix of order 3. So, we suppose that $n \geq 4$ and that there exists a Hadamard matrix and, hence, a normalized Hadamard matrix $\mathbf{M}$ of order n.

Since every row of $\mathbf{M}$ from second row onward is orthogonal to the first, the number of $+1$s in any such row equals the number of -1s in it. This proves that n is even, say $n = 2m$. By permuting the columns of $\mathbf{M}$, if necessary, we can assume that the first m entries in the second row of $\mathbf{M}$ are $+1$. Among the first m entries of the third row, suppose that j of these are $+1$ and the remaining $m - j$ are -1. Then among the last m entries of the third row $m - j$ entries are $+1$ and j of them are -1. By the orthogonality of the second and third rows,