we then find

$$j-(m-j)-(m-j)+j=0$$

giving $m=2j$. Hence $n=4j$.

Definition 11.3
Two Hadamard matrices are said to be **equivalent** if one of them can be obtained from the other by permuting rows or columns or by multiplying rows or columns by -1.

Remarks 11.2

Note (i)
Observe that the relation of two Hadamard matrices being equivalent is an equivalence relation.

Note (ii)
There are only two Hadamard matrices (1) and (-1) of order 1 and these are clearly equivalent.

Note (iii)
There is only one normalized Hadamard matrix of order 2 and as every Hadamard matrix of order n is equivalent to a normalized Hadamard matrix of order n, it follows that any two Hadamard matrices of order 2 are equivalent.

Note (iv)
Let

$$\mathbf{M}=\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & a & b & c\\ 1 & d & e & f\\ 1 & g & h & i\end{pmatrix}$$

be a normalized Hadamard matrix of order 4. Then $\mathbf{MM}^t=4\mathbf{I}$ shows that

$$1+a+b+c=0$$

$$1+d+e+f=0$$

$$1+g+h+i=0$$

$$1+ad+be+cf=0$$

$$1+ag+bh+ci=0$$

$$1+dg+ch+fi=0$$

If $a=b=-1$, $c=1$, then $f=-1$, $i=-1$ and $d+e=0$, $g+h=0$, $dg+eh+2=0$. If $d=-1$, $e=1$, then $h=-1$, $g=1$ while if $d=1$, $e=-1$, then $g=-1$, $h=1$. Therefore, the choice of a, b, c as above gives two normalized matrices:

$$\mathbf{M}_1=\begin{pmatrix}1&1&1&1\\1&-1&-1&1\\1&-1&1&-1\\1&1&-1&-1\end{pmatrix}\quad \mathbf{M}_2=\begin{pmatrix}1&1&1&1\\1&-1&-1&1\\1&1&-1&-1\\1&-1&1&-1\end{pmatrix}$$

Clearly $\mathbf{M}_2$ can be obtained from $\mathbf{M}_1$ by interchanging the third and fourth rows and so $\mathbf{M}_1$ and $\mathbf{M}_2$ are equivalent.

If $a=c=-1$, $b=1$, then $e=-1=h$ and $d+f=0=g+i$, $dg+fi+2=0$. If $d=-1$, $f=1$, then $g=1$, $i=-1$ while if $d=1$, $f=-1$, then $g=-1$, $i=1$. Thus the present choice of a, b, c gives two normalized matrices:

$$\mathbf{M}_3=\begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&-1&-1&1\\1&1&-1&-1\end{pmatrix}\quad \mathbf{M}_4=\begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{pmatrix}$$

But $\mathbf{M}_3$ is obtained from $\mathbf{M}_1$ by interchanging the second and third rows while $\mathbf{M}_4$ is obtained from $\mathbf{M}_1$ by applying the permutation $(\mathbf{R}_2\mathbf{R}_4\mathbf{R}_3)$ to the rows of $\mathbf{M}_1$. Thus, both $\mathbf{M}_3$ and $\mathbf{M}_4$ are equivalent to $\mathbf{M}_1$.

If $a=1$, $b=c=-1$, then $d=g=-1$, $e+f=0=h+i$ and $eh+fi+2=0$. If $e=1$, $f=-1$, then $h=-1$, $i=1$ while if $e=-1$, $f=1$, then $h=1$, $i=-1$. Thus, the two possible normalized matrices in this case are:

$$\mathbf{M}_5=\begin{pmatrix}1&1&1&1\\1&1&-1&-1\\1&-1&1&-1\\1&-1&-1&1\end{pmatrix}\quad\text{and}\quad \mathbf{M}_6=\begin{pmatrix}1&1&1&1\\1&1&-1&-1\\1&-1&-1&1\\1&-1&1&-1\end{pmatrix}$$

The matrix $\mathbf{M}_6$ follows from $\mathbf{M}_5$ by interchanging the third and fourth rows. Thus, $\mathbf{M}_5$ and $\mathbf{M}_6$ are equivalent. Also clearly $\mathbf{M}_1$ and $\mathbf{M}_5$ are equivalent.

This exhausts all possible choices for a, b, c and, therefore, up to equivalence there is only one normalized Hadamard matrix of order 4. Hence, there is only one equivalence class of Hadamard matrices of order 4.

The above could alternatively and in a simpler way be obtained as follows: For a normalized Hadamard matrix of order 4, the second row has two -1s and two $+1$s. Thus there are three choices for the second row. Then, with each choice of the second row, there are two choices for the third row and once the second and third rows have been chosen, there is only one choice for the fourth row. Hence, there are only six normalized Hadamard matrices of order 4 and these are the matrices $\mathbf{M}_1$ to $\mathbf{M}_6$ as above. Equivalence of these matrices needs the same argument as above.

11.2 HADAMARD CODES

Definition 11.4

A matrix obtained from a Hadamard matrix $\mathbf{M}_n$ of order n by changing 1s into 0s and -1s into 1s is called a **binary Hadamard matrix** of order n.

Let $\mathbf{M}_n$ be a normalized Hadamard matrix of order n and $\mathbf{A}_n$ be the binary Hadamard matrix of order n obtained from $\mathbf{M}_n$. Since any two rows of $\mathbf{M}_n$ are orthogonal, therefore, any two rows of $\mathbf{M}_n$ agree in $n/2$ places and differ in the remaining $n/2$ places. It follows that:

(i) the distance between any two rows of $\mathbf{A}_n$ is $n/2$;
(ii) the weight of every non-zero row of $\mathbf{A}_n$ is $n/2$.

Also, clearly, every row of $\mathscr{A}_n$ has first entry 0.

Let $\mathscr{A}_n$ denote the set of all the rows of $\mathscr{A}_n$ with first entry deleted. The set $\mathscr{A}_n$ has n elements of length $n-1$ and the distance between any two elements of $\mathscr{A}_n$ is $n/2$.

Let $\mathscr{C}_n$ denote the set of all rows of $\mathscr{A}_n$ together with their complements. Then elements of $\mathscr{C}_n$ are words of length n, are $2n$ in number and the minimum of the distance between any two of them is $n/2$.

Let $\mathscr{B}_n$ denote the set of all elements of $\mathscr{A}_n$ together with their complements. The elements of $\mathscr{B}_n$ are words of length $n-1$, are $2n$ in number and distance between any two of them is at least

$$\frac{n}{2}-1$$

(for $n > 2$).

$\mathscr{A}_n$, $\mathscr{B}_n$ and $\mathscr{C}_n$ are called **Hadamard codes**. These are binary codes but none of $\mathscr{A}_n$, $\mathscr{B}_n$ and $\mathscr{C}_n$ is in general a group. Thus, these are non-linear codes in general. Observe that the codes $\mathscr{B}_n$ and $\mathscr{C}_n$ satisfy the Plotkin bound (Theorem 6.7) as every code should but it is attained in the case of $\mathscr{A}_n$.

We end this section and also the chapter by constructing Hadamard codes for $n = 2, 4, 8$.

Examples 11.2

Case (i)

Consider

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

It is a normalized Hadamard matrix of order 2 and gives the following three codes:

$$\mathscr{A}_2 = \{0, 1\} \qquad \mathscr{B}_2 = \{0, 1\} \qquad \mathscr{C}_2 = \{00, 01, 10, 11\}$$

Case (ii)
The normalized Hadamard matrix

$$\mathbf{M} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

gives the Hadamard codes

$$\mathscr{A}_4 = \{000, 101, 011, 110\}$$

$$\mathscr{B}_4 = \{000, 101, 011, 110, 111, 010, 100, 001\}$$

$$\mathscr{C}_4 = \{0000, 0101, 0011, 0110, 1111, 1010, 1100, 1001\}$$

Case (iii)
The matrix

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

is a normalized Hadamard matrix of order 8 and gives the following Hadamard codes:

$$\mathscr{A}_8 = \begin{matrix} \{0000000, 0001111, \\ 1010101, 1011010, \\ 0110011, 0111100, \\ 1100110, 1101001\} \end{matrix}$$

$$\mathscr{B}_8 = \begin{matrix} \{0000000, 1110000, \\ 1010101, 0100101, \\ 0110011, 1000011, \\ 1100110, 0010110, \\ 1111111, 0001111, \\ 0101010, 1011010, \\ 1001100, 0111100, \\ 0011001, 1101001\} \end{matrix}$$

$$\mathscr{C}_8 = \begin{matrix} \{00000000, 11111111, \\ 01010101, 10101010, \\ 00110011, 11001100, \\ 01100110, 10011001, \\ 00001111, 11110000, \\ 01011010, 10100101, \\ 00111100, 11000011, \\ 01101001, 10010110\} \end{matrix}$$

Exercise 11.2

1. Write another normalized Hadamard matrix of order (i) 4; (ii) 8, and obtain the corresponding Hadamard codes. Compare these codes with the codes obtained in Examples 11.2, Cases (ii) and (iii) above.
2. Determine the number of normalized Hadamard matrices of order 8. Also determine the number of equivalence classes of Hadamard matrices of order 8.
3. Do any two Hadamard matrices of order 8 give the same Hadamard codes? Justify your answer!

Bibliography

Assmus, E. F. and Mattson, H. F. (1963) Error correcting codes: an axiomatic approach. *Information and Control*, **6**, 315–30.

Assmus, E. F. Jr and Mattson, H. F. (1966) Perfect codes and Mathieu groups, *Arch. Math.*, **17**, 121–35.

Assmus, E. F. Jr and Mattson H. F. Jr (1967) On tactical configurations and error correcting codes. *J. Combinatorial Theory*, **2**, 243–57.

Assmus, E. F. Jr and Mattson, H. F. Jr (1969) New 5-designs. *J. Combinatorial Theory*, **6**, 122–51.

Assmus, E. F. Jr and Mattson, H. F. Jr (1972) On weights in quadratic residue codes. *Discrete Mathematics*, **3**, 1–20.

Assmus, E. F. Jr and Pless, V. (1983) On the covering radius of extremal self-dual codes. *IEEE Trans. Information Theory*, **29**, 359–63.

Beenker, G. F. M. (1984) A note on quadratic residue codes over GF(9) and their ternary images. *IEEE Trans. Information Theory*, **30**, 403–404.

Berlekamp, E. R. (1968) *Algebraic Coding Theory*, McGraw-Hill.

Berman, S. D. (1967) Semisimple cyclic and Abelian codes, II. *Cybernetics*, **3**, 17–23.

Birkhoff, G. and Bartee, T. C. (1970) *Modern Applied Algebra*, McGraw-Hill.

Blake, I. F. and Mullin, R. C. (1975) *The Mathematical Theory of Coding*, Academic Press.

Bose, R. C. and Ray-Choudhuri, D. K. (1960) On a class of error correcting binary group codes. *Information and Control*, **3**, 68–79.

Calderbank, R. (1983) A square root bound on the minimum weight in quasi-cyclic codes. *IEEE Trans. Information Theory*, **29**, 332–7.

Cohen, G. D., Karpovsky, M. G., Mattson, H. F. Jr and Schatz, J. R. (1985) Covering radius-survey and recent results. *IEEE Trans. Information Theory*, **31**, 328–43.

Coppersmith, D. and Seroussi, G. (1984) On the minimum distance of some quadratic residue codes. *IEEE Trans. Information Theory*, **30**, 407–11.

Dornhoff, L. L. and Hohn, F. E. (1978) *Applied Modern Algebra*, Macmillan.

Graham, R. L. and Sloane, N. J. A. (1985) On the covering radius of codes. *IEEE Trans. Information Theory*, **31**, 385–401.

Helleseth, T. (1978) All binary 3-error correcting BCH codes of length $2^m - 1$ have covering radius 5. *IEEE Trans. Information Theory*, **24**, 257–8.

Herstein, I. N. (1968) *Non-commutative Rings*, Carus Math. Monographs No. 15, Math. Assoc. Amer.

Herstein, I. N. (1976) *Topics in Algebra*, Vikas Publishing House, New Delhi.

Hocquenghem, A. (1959) Codes correcteurs d'erreurs. *Chiffres* (Paris), **2**, 147–56.

Kasami, T., Lin, S. and Peterson, W. W. (1968) Some results on cyclic codes which are invariant under the affine group and their applications. *Information and Control*, **11**, 475–96.

Lambek, J. (1966) *Lectures on Rings and Modules*, Ginn (Blaisdell), Boston, Massachusetts.

Lidl, R. and Niederreiter, H. (1986) *Introduction to Finite Fields and their Applications*, Cambridge University Press.

MacWilliams, F. J. and Sloane, N. J. A. (1978) *Theory of Error Correcting Codes*, North-Holland.

Manju Pruthi (1992) Primitive idempotents in semisimple group algebras of finite cyclic groups and cyclic codes over finite fields. PhD thesis, M.D. University, Rohtak, India.

McEliece, R. J. (1977) *The Theory of Information and Coding, Encyclopaedia of Mathematics and its Applications*, Vol. 3, Addison-Wesley.

Niven, I. and Zuckerman, H. S. (1972) *An Introduction to Number Theory*, Wiley Eastern.

Remijn, J. C. C. M. and De Vroedt, C. (1984) The minimum distance of the [38, 19] ternary extended QR-code is 11. *IEEE Trans. Information Theory*, **30**, 405–7.

Roos, C. (1983) A new lower bound for minimum bound of a cyclic code. *IEEE Trans. Information Theory*, **29**, 330–2.

Scott, W. R. (1964) *Group Theory*, Prentice-Hall.

Shaughnessy, E. P. (1971) Codes with simple automorphism groups. *Arch. Math.*, **22**, 459–66.

Sloane, N. J. A. (1973) Is there a (72, 36), $d = 16$ self-dual code? *IEEE Trans. Information Theory*, **19**, 251.

Sloane, N. J. A. (1975) *A Short Course on Error Correcting Codes*, Centre for Mechanical Sciences, Courses and Lectures No. 188, Springer-Verlag, Wien, New York.

Sloane, N. J. A. (1977) Error correcting codes and invariant theory: New applications of nineteenth century technique. 82–107.

Sloane, N. J. A. and Thompson, J. G. (1983) Cyclic self-dual codes. *IEEE Trans. Information Theory*, **29**, 364–6.

Solomon, G. and McEliece, R. (1966) Weights of cyclic codes. *J. Combinatorial Theory*, **1**, 459–75.

Spiegel, E. (1977) Codes of Z_m. *Information and Control*, **35**.

Spiegel, E. (1978) Codes over Z_m, revised. *Information and Control*, **37**.

Van Lint, J. H. (1971) *Coding Theory*, Lecture Notes in Mathematics, No. 201, Springer-Verlag, Berlin, Heidelberg, New York.

Van Lint, J. H. and MacWilliams, J. (1978) Generalised quadratic residue codes. *IEEE Trans. Information Theory*, **24**, 720–37.

Vermani, L. R. and Jindal, S. L. (1983) A note on maximum distance separable (MDS) codes. *IEEE Trans. Information Theory*, **29**, 136.

Vermani, L. R. and Yogesh Kumar, A note on quadratic residue codes (preprint).

Ward, H. N. (1974) Quadratic residue codes and symplectic groups. *J. Algebra*, **29**, 150–71.

Ward, H. N. (1983) Divisors of codeword weights. *IEEE Trans. Information Theory*, **29**, 337–42.

Zimmermann, K. H. (1992) On a complete decoding scheme for binary radical codes. *Arch. Math.*, **59**, 513–20.

Index