A NOTE ON A RESULT IN THE THEORY OF CODE CONSTRUCTION

by

R. C. Bose and S. S. Shrikhande

University of North Carolina

This research was supported by the United States Air Force through the Air Office of Scientific Research of the Air Research and Development Command, under Contract No. AF 49(638)-213. Reproduction in whole or in part is permitted for any purpose of the United States Government.

Institute of Statistics
Mimeograph Series No. 217
January 1959

A NOTE ON A RESULT IN THE THEORY OF CODE CONSTRUCTION[1]

R. C. Bose & S. S. Shrikhande

University of North Carolina

Summary. This paper establishes a connection between Hadamard matrices and a problem in the theory of code construction.

1. Introduction

A sequence

$$\alpha = (a_1, a_2, \ldots, a_n)$$

of n numbers, where $a_i = 0$ or 1 may be called an n-place message. The number of unities in α may be called the weight of α and will be denoted by $w(\alpha)$. The Hamming distance (Hamming, 1950) between α and β, denoted by $\delta(\alpha,\beta)$, is defined as the number of positions in which α and β differ. It is easily verified that

$$\delta(\alpha,\beta) = w(\alpha) + w(\beta) - 2(\alpha \cdot \beta) , \qquad (1)$$

where $(\alpha \cdot \beta)$ is the scalar product of the vectors α and β, and is, therefore, the number of positions simultaneously occupied by unity in α and β.

Two n-place messages will be called different, if they differ in at least one position, i.e. their Hamming distance is non-zero. It is important in the theory of symmetric

[1] This research was supported by the United States Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command, under Contract No. AF 49(638)-213. Reproduction in whole or in part is permitted for any purpose of the United States Government.

binary codes (Slepian, 1956) to determine the maximum number A(n,d), of different n-place messages that can be constructed such that the Hamming distance between any two of them is greater than or equal to a preassigned positive integer d. A set of m n-place messages, such that the distance between any two is greater than or equal to d, may be called an n-place code of length m and minimum distance d. Such a code will be denoted by M(n,d;m).

In an interesting paper Plotkin (1951) has proved the following results, which are also quoted in a paper by Joshi (1958).

Theorem A. For any positive integer t

$$\text{(i) } A(4t-2,\ 2t) \leq 2t\ ,$$

$$\text{(ii) } A(4t-1,\ 2t) \leq 4t\ ,$$

$$\text{(iii) } A(\ 4t\ ,\ 2t) \leq 8t\ .$$

Further if the equality holds in (iii), then it also holds in (i) and (ii).

Theorem B. If $4t-1$ is a prime, then

$$A(4t,\ 2t) = 8t\ .$$

When the equality holds in any one of the parts (i), (ii), (iii) of Plotkin's Theorem A, the corresponding code is maximal in the sense that no other codes with the same minimum distance and the same number of places has greater length. The main result of the present paper is the theorem proved in section 3 asserting the coexistence of the maximal codes M(4t, 2t; 8t), M(4t - 1, 2t, 4t), the balanced incomplete block design with parameters $v = b = 4t-1$, $r = k = 2t-1$, $\lambda = t-1$, and the Hadamard matrix H_{4t} of order 4t. In particular this theorem implies that Plotkin's Theorem B is true for all values of t for which a Hadamard matrix of order 4t exists, and conversely. Thus for $t \leq 50$, we always have $A(4t, 2t) = 8t$ and in consequence $A(4t-1, 2t) = 4t$, $A(4t-2, 2t) = 2t$, except possibly for the cases $t = 23, 29, 39, 46, 47$ which are undecided. It has been conjectured that a Hadamard matrix of order 4t exists for all positive integral values of t. If this conjecture is true, then the equality holds in (i), (ii), (iii) of Theorem A. The second part of Theorem A, and the Theorem B, would then be superfluous.

In section 2, we state briefly the main results known up to date regarding the existence of Hadamard matrices, and the corresponding balanced incomplete block designs. In the final section 4, the structure of the maximal codes $M(4t-2, 2t; 2t)$, $M(4t-1, 2t; 4t)$, $M(4t, 2t; 8t)$ is studied.

2. Hadamard matrices and balanced incomplete block designs

A square matrix H of order h is called a Hadamard matrix, if all its elements are +1 or -1.and if any two rows (and hence any two columns) of H are orthogonal. It is known (Paley,1933) that Hadamard matrices of order h can exist only for values $h = 2$ and $h = 4t$, where t is a positive integer. We denote a Hadamard matrix of order h by H_h. A Hadamard matrix can always be reduced to the standard form in which the initial row and column contain only +1, since by changing the sign of all elements in a row (column) orthogonality remains unaffected.

A balanced incomplete block design (Bose, 1939) is an arrangement of v objects into b sets satisfying the following conditions:

(i) Each set contains exactly k different objects

(ii) Each object occurs in exactly r different sets

(iii) Any pair of objects occurs in exactly λ different sets.

The integers v, b, r, k, λ are called the parameters of the design, and satisfy the relations

$$bk = vr, \quad \lambda(v-1) = r(k-1) \ .$$

The design is said to be symmetrical, if b = v and consequently k = r. These designs were first introduced into experimental studies by Yates (1936). In consequence of this use the objects are called "treatments" and the sets are called "blocks." The incidence matrix of a balanced incomplete block design with parameters v, b, r, k, λ is defined to be the matrix $N = (n_{ij})$, such that $n_{ij} = 1$ if the i-th treatment occurs in the j-th block, and is 0 otherwise. Clearly N is a $v \times b$ matrix of zeroes and ones, such that each row contains r unities, each column contains k unities, and any two rows have unities in corresponding positions exactly λ times. Conversely the existence of a matrix with these properties is equivalent to the existence of the design.

Todd (1933) has shown that the existence of a Hadamard matrix H_{4t} is equivalent to the existence of a symmetrical incomplete block design with parameters

$$v = b = 4t - 1, \quad r = k = 2t - 1, \quad \lambda = t - 1 \ .$$

Methods of constructing Hadamard matrices, or the equivalent balanced incomplete block designs, have been given by Bose (1939), Paley (1933), Williamson (1944, 1947), the latest results being due to Brauer (1953) and Stanton and Sprott (1958). The existence of Hadamard matrices H_h has been proved for the following values of h, where p denotes an odd prime:

I. $h = 2^k$,

II. $h = p^k + 1 \equiv 0 \pmod 4$,

III. $h = h_1(p^k + 1)$, where $h_1 \geq 2$ is the order of a Hadamard matrix,

IV. $h = h^*(h^* - 1)$ where h^* is a product of numbers of forms I and II,

V. $h = 172$,

VI. $h = h^*(h^* + 3)$ where h^* and $h^* + 4$ both are products of numbers of forms I and II,

VII. $h = h_1 h_2 (p^k + 1) p^k$, where $h_1 \geq 2$, $h_2 \geq 2$ are orders of Hadamard matrices,

VIII. $h = h_1 h_2 s(s + 3)$ where $h_1 \geq 2$, $h_2 \geq 2$ are orders of Hadamard matrices and where s and $s + 4$ are both of the form $p^k + 1$,

IX. $h = (q + 1)^2$, where both q and $q + 2$ are prime or prime powers,

X. h is a product of numbers of the form I-IX.

The above list is essentially taken from Brauer's paper with a slight modification to include the results of Stanton and Sprott. As mentioned in the introduction, the existence of H_{4t} has not been disproved for any integral t, and it has been conjectured that H_{4t} always exists.

3. Connection between Plotkin's maximal codes, Hadamard matrices, and balanced incomplete block designs

Given an n-place code M(n,d;m) of length m and minimum distance d, we can represent it by the matrix M, whose rows are the messages $\alpha_1, \alpha_2, \ldots, \alpha_m$ belonging to the code. Any permutation of $\alpha_1, \alpha_2, \ldots, \alpha_m$ merely permutes the rows of M, and obviously the new code is still an n-place minimum distance d code of length m. Again suppose we interchange 0 and 1 in the j-th position in each of the messages $\alpha_1, \alpha_2, \ldots, \alpha_m$ (i.e., interchange 0 and 1 for every element in the j-th column of M). This process leaves the distance between any two messages unchanged and may be called column inversion. Two n-place codes of length m and minimum distance d which can be obtained from one another by row permutation or column inversion are called equivalent.

The code M(n,d;m) is said to be in the standard form, if in the corresponding matrix M, the initial row consists of unities only, and the initial column consists of consecutive unities followed by consecutive zeroes. If M(n,d;m) is not in the standard form, then it can be brought to this form by making row permutations and column inversions.

We shall now prove the following Theorem:

Theorem 1. The following statements are equivalent:

(a) $A(4t, 2t) = 8t$, i.e., there exists a code $M_1(4t, 2t; 8t)$.

(b) $A(4t-1, 2t) = 4t$, i.e., there exists a code $M_2(4t-1, 2t; 4t)$.

(c) A symmetric balanced incomplete block design with parameters

$$v = b = 4t - 1, \quad r = k = 2t - 1, \quad \lambda = t - 1,$$

exists.

(d) A Hadamard matrix H_{4t} of order $4t$ exists.

The proof consists in showing that (a) → (b) → (c) → (d) → (a), and shall be carried out in several steps.

(i) Suppose $A(4t,2t) = 8t$, so that a 4t-place code $M_1(4t, 2t; 8t)$ of length 8t and minimum distance 2t exists. We can without loss of generality assume that this code is in the standard form, so that the initial row of the corresponding matrix M_1 consists of unities. Each column M_1 contains exactly 4t unities and 4t zeroes. If not suppose the j-th column contains $4t + i$ unities and $4t - i$ zeroes, where $i \neq 0$. If $i > 0$, then we first drop all rows of M_1 for which the j-th column contains zero. The distance between any two of the $4t + i$ retained rows is not less than 2t. The j-th column now consists of unities only, and the distance between two rows remains unchanged if we drop this column. The resulting matrix M_2 has $4t + i$ rows and $4t - 1$ columns and corresponds to a code $M(4t-1, 2t; 4t+i)$. It follows from Plotkin's Theorem A part (ii), that $i \leq 0$, which contradicts our hypothesis. Similarly if i were less than zero, we get a contradiction by retaining only those rows of M_1 for which the j-th column contains zero and then dropping the j-th column. This shows that $i = 0$. Hence every column of M_1 has exactly 4t unities and 4t zeroes. Since M_1 is in the standard form the first column consists of 4t unities followed by 4t zeroes. If we drop the first column, and retain only the first 4t rows, we obtain a matrix M_2 corresponding to a code $M_2(4t-1, 2t; 4t)$. Similarly by retaining the last 4t rows after dropping the first column of M_1 we obtain a matrix $\overline{M}_2$ corresponding to a code $\overline{M}_2(4t-1, 2t; 4t)$. Thus (a) → (b).

(ii) Suppose $A(4t-1, 2t) = 4t$, so that a $(4t-1)$-place code $M_2(4t-1, 2t; 4t)$ of length 4t and minimum distance 2t exists. Without loss of generality we can take this code in the standard form so that the first row of the corresponding matrix M_2 consists of unities.

Schützenberger (1953) has shown that for an n-place code of length m

$$n \operatorname{var}(k_j) = m \sum k_j - \frac{(\sum k_j)^2}{n} - \sum \delta(\alpha_i, \alpha_{i'}),$$

where k_j is the number of unities in the j-th column of M, $j = 1,2,\ldots,n$; and α_i and $\alpha_{i'}$ are the i-th and i'-th rows of M, $i < i' = 1,2,\ldots,m$. Let $\bar{k} = \sum k_j/n$ be the mean value of k_j and $\bar{\delta} = 2\sum \delta(\alpha_i, \alpha_{i'})/m(m-1)$ be the mean value of $\delta(\alpha_i, \alpha_{i'})$. Then

$$\bar{\delta} = \frac{mn}{2(m-1)} - \frac{2n}{m(m-1)} \{(\bar{k} - \frac{m}{2})^2 + \operatorname{var}(k_j)\} .$$

$$\therefore \bar{\delta} \leq \frac{mn}{2(m-1)} , \qquad (2)$$

and the equality holds when and only when $k_1 = k_2 = \ldots = k_n = m/2$.

For the code $M_2(4t-1, 2t; 4t)$, we therefore have

$$\bar{\delta} \leq 2t \ .$$

On the other hand, $\delta(\alpha_i, \alpha_{i'}) \geq 2t$ for every pair i,i'. It follows that the distance $\delta(\alpha_i, \alpha_{i'})$ between any two rows of M_2 is constant and equal to $2t$, and every column has exactly $2t$ unities. Since the first row of M_2 consists entirely of unities, every other row of M_2 has exactly $2t$ zeroes and $2t-1$ unities. Now from (1)

$$\delta(\alpha_i,\alpha_{i'}) = w(\alpha_i) + w(\alpha_{i'}) - 2(\alpha_i \cdot \alpha_{i'}) \ .$$

Hence if $1 < i < i' \leq 4t$,

$$2t = (2t-1) + (2t-1) - 2(\alpha_i \cdot \alpha_{i'}) \ ,$$

or

$$(\alpha_i \cdot \alpha_{i'}) = t - 1 \ .$$

Thus if N_2 is the matrix obtained from M_2 by deleting the first row, N_2 is a $(4t-1) \times (4t-1)$ matrix with zeroes and ones, such that each row and each column have $2t-1$ unities, and any two rows have unity in corresponding positions for exactly $t-1$ positions. Therefore N_2 is the incidence matrix of a symmetrical balanced incomplete block design with parameters

$$v = b = 4t-1, \quad r = k = 2t-1, \quad \lambda = t-1 \ .$$

Thus (b) → (c).

(iii) The coexistence of a symmetrical balanced incomplete block design with parameters $v = b = 4t-1$, $r = k = 2t-1$, $\lambda = t-1$, and the Hadamard matrix H_{4t} of order $4t$, has been shown by Todd (1933). In fact if N is the incidence matrix of the balanced incomplete block design, then it is easy to verify that a Hadamard matrix H_{4t} (in the standard form) is obtained from N by changing each zero to -1, and then bordering the resultant matrix by an initial row and column consisting entirely of unities. Thus (c) → (d).

(iv) If α is a row vector with n elements each of which is zero or unity, we define a corresponding vector α^* as the vector obtained from α by changing all the zeroes to -1. Conversely from a vector α^* whose elements are +1 or -1, we can get an α by changing all -1's to zero. The relation between α and α^* is clearly given by

$$\alpha^* = 2\alpha - \varepsilon_n \ , \quad \alpha = \tfrac{1}{2}(\alpha^* + \varepsilon_n) \ ,$$

where $\varepsilon_n = (1,1,\ldots,1)$

$$(\alpha^* \cdot \beta^*) = ((2\alpha - \varepsilon_n)\cdot(2\beta - \varepsilon_n))$$

$$= 4(\alpha\cdot\beta) - 2(\alpha\cdot\varepsilon_n) - 2(\beta\cdot\varepsilon_n) + (\varepsilon_n \circ \varepsilon_n) \ .$$

Using (1) and noting that $(\alpha\cdot\varepsilon_n) = w(\alpha)$, $(\beta\cdot\varepsilon_n) = w(\beta)$, we have

$$(\alpha^*\cdot\beta^*) = n - 2\delta(\alpha,\beta) \ . \qquad (3)$$

Suppose a Hadamard matrix H_{4t} is given, with rows $\alpha_1^*, \alpha_2^*, \ldots, \alpha_{4t}^*$. Let

$$\beta_i^* = -\alpha_i^* \qquad i = 1,2,\ldots,4t \ .$$

From the properties of Hadamard matrices

$$(\alpha_i^*\cdot\alpha_{i'}^*) = (\beta_i^*\cdot\beta_{i'}^*) = 0 \quad , \text{ if } i \neq i' \ ;$$

$$(\alpha_i^*\cdot\beta_{i'}^*) = 0 \quad , \text{ if } i \neq i' \ ;$$

$$(\alpha_i^*\cdot\beta_i^*) = -4t \ .$$

If we now set

$$\alpha_i = \frac{1}{2}(\alpha_i^* + \varepsilon_{4t}), \quad \beta_i = \frac{1}{2}(\beta_i^* + \varepsilon_{4t}) ,$$

then from (3)

$$\delta(\alpha_i,\alpha_{i'}) = \delta(\beta_i, \beta_{i'}) = 2t \quad \text{if } i \neq i' ;$$

$$\delta(\alpha_i,\beta_{i'}) = 2t \quad \text{if} \quad i \neq i' ;$$

$$\delta(\alpha_i,\beta_i) = 4t .$$

Hence, we have a maximal code $M(4t, 2t; 8t)$ by taking as our messages the row vectors $\alpha_1, \alpha_2, \ldots, \alpha_{4t}, \beta_1, \beta_2, \ldots, \beta_{4t}$. (The code will be in the standard form if we start from an H_{4t} in the standard form.) This shows that (d) → (a), and completes the proof of our theorem.

4. The structure of the maximal sets $M_3(4t-2, 2t; 2t)$, $M_2(4t-1, 2t; 4t)$ and $M_1(4t, 2t; 8t)$

(i) Given a maximal set $M_3(4t-2, 2t; 2t)$ in the standard form it follows from (2) that $\overline{\delta} \leq 2t$. Hence the distance between any two rows is constant and equal to 2t, and each column contains exactly t unities. It follows as in section 3(ii) that the matrix N_3 obtained by deleting the initial column of M_3 is the incidence matrix of the balanced incomplete block design

$$v = 2t-1, \; b = 4t-2, \; r = 2t-2, \; k = t-1, \; \lambda = t-2 .$$

We can write

$$M_3 = \begin{bmatrix} \varepsilon_{4t-2} \\ N_3 \end{bmatrix} .$$

(ii) Given a maximal set $M_2(4t-1, 2t; 4t)$ in the standard form, we have already shown in section 3(ii) that the result of deleting the first row is a matrix N_2, which is the incidence matrix of the balanced incomplete block design

$$v = b = 4t - 1, \quad r = k = 2t - 1, \quad \lambda = t - 1 \ .$$

We can write

$$M_2 = \begin{bmatrix} \varepsilon_{4t-1} \\ N_2 \end{bmatrix} .$$

(iii) Before discussing the structure of the maximal set $M_1(4t, 2t; 8t)$, we shall prove the following Lemma:

Lemma. If H_{4t} and $\overline{H}_{4t}$ are Hadamard matrices of order 4t, with rows $\alpha_1^*, \alpha_2^*, \ldots, \alpha_{4t}^*$ and $\beta_1^*, \beta_2^*, \ldots, \beta_{4t}^*$ such that

$$(\alpha_i^* \cdot \beta_j^*) \leq 0 \ , \qquad i,j = 1,2,\ldots,4t \ ;$$

then there exists a permutation matrix P_{4t} of order 4t such that

$$H_{4t} = -P_{4t}\overline{H}_{4t} \ .$$

In other words, $\overline{H}_{4t}$ is derivable from H_{4t} by everywhere interchanging +1 and -1, and then applying a suitable row permutation. Let

$$K_{4t} = \frac{1}{+2t^{\frac{1}{2}}} H_{4t} \ , \qquad \overline{K}_{4t} = \frac{1}{+2t^{\frac{1}{2}}} \overline{H}_{4t} \ .$$

Then K_{4t} and $\overline{K}_{4t}$ are orthogonal matrices, such that the scalar product of any row of K_{4t} with any row of $\overline{K}_{4t}$ is negative or zero. Let K'_{4t} denote the transpose of K_{4t}. Then

$$K_{4t}K'_{4t} = I_{4t} \ ,$$

where I_{4t} is the unit matrix of order 4t. Let

$$\overline{K}_{4t}K'_{4t} = C_{4t} = (c_{ij}) \ .$$

Then C_{4t} is an orthogonal matrix. The row vectors of I_{4t} and

C_{4t} have been derived from those of K_{4t} and $\overline{K}_{4t}$ by the application of an orthogonal transformation. Hence the scalar product of any two vectors is unchanged. It follows that the scalar product of any row vector of C_{4t} with any row vector of I_{4t} is negative or zero. Hence

$$c_{ij} \leq 0 \ , \qquad i,j = 0,1,2,\ldots,4t \ .$$

This combined with the fact that C_{4t} is an orthogonal matrix, shows that no column of C_{4t} can contain more than one non-zero element, since the scalar product of two rows which have non-zero elements in the same column would be positive and non-zero. Similarly no row of C_{4t} can contain more than one non-zero element. It now follows that each column and row of C_{4t} contains only one non-zero element, which must be -1. Hence

$$C_{4t} = -P_{4t} \ ,$$

where P_{4t} is a permutation matrix. Hence

$$\overline{K}_{4t} = -P_{4t}K_{4t} \ ,$$

or

$$\overline{H}_{4t} = -P_{4t}H_{4t} \ .$$

This proves the required Lemma.

Suppose a maximal set $M_1(4t, 2t; 8t)$ is given in the standard form. From what has been shown in section 3(i), it follows that we can write

$$M_1 = \begin{bmatrix} \varepsilon'_{4t}, & M_2 \\ \varphi'_{4t}, & \overline{M}_2 \end{bmatrix} ,$$

where ε_n' denotes a column vector with n unities, φ_n' denotes a column vector with n zeroes, and M_2 and $\overline{M}_2$ are the matrices corresponding to maximal codes $M_2(4t-1,\ 2t;\ 4t)$ and $\overline{M}_2(4t-1,\ 2t;\ 4t)$. Let

$$A = (\varepsilon_{4t}',\ M_2) \quad \text{and} \quad B = (\varphi_{4t}',\ \overline{M}_2)\ .$$

Let the rows of A be $\alpha_1, \alpha_2, \ldots, \alpha_{4t}$, and the rows of B be $\beta_1, \beta_2, \ldots, \beta_{4t}$. Since any row of A differs from the corresponding row of M_2, by the addition of an initial unity, the Hamming distance between any two rows of A is the same as the Hamming distance between the corresponding rows of M_2. It follows from what has been proved in section 3(ii) that

$$\delta(\alpha_i,\ \alpha_{i'}) = 2t\ ,\ i,i' = 1,2,\ldots,4t,\ i \neq i'\ .$$

A similar argument proves that

$$\delta(\beta_j,\ \beta_{j'}) = 2t\ ,\ j,j' = 1,2,\ldots,4t,\ j \neq j'\ .$$

Also since the Hamming distance between any two rows of M_1 is not less than 2t, we have

$$\delta(\alpha_i,\ \beta_j) \geq 2t \qquad i,j = 1,2,\ldots,4t\ .$$

Now let us set

$$\alpha_i^* = 2\alpha_i - \varepsilon_{4t}\ ,\ \beta_j^* = 2\beta_j - \varepsilon_{4t}\ ;\ i,j = 1,2,\ldots,4t.$$

Then from (3)

$$(\alpha_i^* \cdot \alpha_{i'}^*) = 0\ ,\ \text{if } i \neq i' = 1,2,\ldots,4t\ ;$$

$$(\beta_j^* \cdot \beta_{j'}^*) = 0\ ,\ \text{if } j \neq j' = 1,2,\ldots,4t\ ;$$

$$(\alpha_i^* \cdot \beta_j^*) \leq 0\ , \qquad i,j = 1,2,\ldots,4t\ .$$

Let H_{4t} and $\overline{H}_{4t}$ be matrices with rows $\alpha_1^*, \alpha_2^*, \ldots, \alpha_{4t}^*$ and $\beta_1^*, \beta_2^*, \ldots, \beta_{4t}^*$ respectively. Then H_{4t} and H_{4t}^* are Hadamard matrices satisfying the conditions of our Lemma. Hence

$$H_{4t} = -P_{4t}\overline{H}_{4t}$$

where P_{4t} is a permutation matrix. Let J_{4t} be a square matrix of order 4t all of whose elements are unity. Then

$$H_{4t} = 2A - J_{4t} , \quad \overline{H}_{4t} = 2B - J_{4t}$$

$$\therefore \quad A + P_{4t}B = J_{4t} .$$

If a suitable permutation is made on the last 4t rows of M_1 this relation simplifies to

$$A + B = J_{4t} .$$

Combining this with what has been proved in section 3(iii) regarding the structure of M_2 we can state the following:

Given a 4t-place maximal code of length 8t and minimum distance 2t, there exists an equivalent code with matrix M_1 such that

$$M_1 = \begin{bmatrix} A \\ J_{4t} - A \end{bmatrix} , \text{ where } A = \begin{bmatrix} 1 & \varepsilon_{4t-1} \\ \varepsilon'_{4t-1} & N_2 \end{bmatrix} ,$$

and N_2 is the incidence matrix of a balanced incomplete block design with parameters

$$v = b = 4t - 1, \quad r = k = 2t - 1, \quad \lambda = t - 1 .$$

Note that the last 4t rows of M_1 are obtained from the first 4t rows by everywhere interchanging 0 and 1.

REFERENCES

Bose, R.C. (1939). On the construction of balanced incomplete block designs. Annals of Eugenics, 9, 353-399.

Brauer, A. (1953). On a new class of Hadamard determinants. Math. Zeitschrift, 58, 219-225.

Joshi, D.D. (1958). A note on upper bounds for minimum distance codes. Information and control, 1, 289-295.

Hamming, R.W. (1950). Error detecting and error correcting codes. Bell System Tech. J., 29, 147-160.

Paley, R.E.A.C. (1933). On orthogonal matrices. J. of Math. and Phys., 12, 311-320.

Plotkin, M. (1951). Binary codes with specified minimum distance. Research Division Reprint 51-20. The University of Pennsylvania Moore School of Electrical Engineering, Philadelphia, Pennsylvania.

Schützenberger, M.P. (1953). Sur un problème du codage binaire. Publ. Inst. statist. Univ. Paris, 2, 125-127.

Slepian, D. (1956). A class of binary signalling alphabets. Bell System Tech. J., 35, 203-234.

Stanton, R.G., and D.A. Sprott. (1958). A family of difference sets. Canadian J. of Math., 10, 73-77.

Todd, J.A. (1933). A combinatorial problem. J. of Math. and Phys., 12, 321-333.

Williamson, J. (1944). Hadamard determinant theorem and sum of four squares. Duke Math. J., 11, 65-81.

---------(1947). Note on Hadamard's determinantal problem. Bull. Amer. Math. Soc., series 2, 53, 608-613.

Yates, F. (1936). Incomplete randomised blocks. Annals of Eugenics, Lond., 7, 121-140.