ORTHOGONAL MATRICES WITH ZERO DIAGONAL

J. M. GOETHALS AND J. J. SEIDEL

To H. S. M. Coxeter
on the occasion of his sixtieth birthday

1. Introduction. The central problem in the present paper is the construction of symmetric and of skew-symmetric (=skew) matrices C of order v, with diagonal elements 0 and other elements $+1$ or -1, satisfying

$$CC^T = (v-1)I.$$

The following necessary conditions are known: $v \equiv 2 \pmod 4$ and

$$v - 1 = a^2 + b^2,$$

a and b integers, for symmetric matrices C (Belevitch **(1, 2)**, Raghavarao **(14)**), and $v = 2$ or $v \equiv 0 \pmod 4$ for skew matrices C. However, the only matrices C that have been constructed so far are symmetric matrices of order

$$v = p^h + 1 \equiv 2 \pmod 4, \qquad p \text{ prime},$$

(Paley **(13)**), and skew matrices of order

$$v = 2^t \prod_{i=1}^{r} (p_i^{h_i} + 1), \qquad p_i^{h_i} + 1 \equiv 0 \pmod 4,$$

p_i odd primes; t, r, h_i non-negative integers (Williamson **(17)**).

In §2 Paley's construction is presented in a geometric setting, which enables us to prove, among other things, that any symmetric matrix of the Paley type is equivalent to a matrix of the form

$$\begin{bmatrix} A & B \\ B & -A \end{bmatrix}$$

with A and B symmetric and circulant. In §3 we consider representations of general symmetric matrices C. The existence of such matrices which are not equivalent to matrices of the Paley type is demonstrated in the case of order 26. The final section contains the construction of symmetric matrices C of certain orders which are not covered by the sufficient conditions mentioned above, for instance of the order 226. In addition, some series of new Hadamard matrices are obtained, for instance a Hadamard matrix of order 452. Results of Williamson **(17, 18)** are improved.

C-matrices appear in the literature at various places in connection with combinatorial designs in geometry, engineering, statistics, and algebra.

Received May 1, 1967.

Questions in the theory of polytopes, posed by Coxeter **(6)**, led Paley **(13)** to the construction of Hadamard matrices in which he used C-matrices. Recently, in connection with equilateral point sets in elliptic geometry, C-matrices were discussed by van Lint and Seidel **(11)**. Some 20 years ago, in the construction of networks for conference telephony, Belevitch **(1)** initiated the study of C-matrices, which he called conference matrices. In statistics they were treated in connection with weighing designs by Raghavarao **(14)**. They appear as adjacency matrices of association schemes of certain partially balanced incomplete block designs and strongly regular graphs (Bose **(3)**, Connor-Clatworthy **(5)**, Seidel **(16)**, and Mesner **(12)**, who attributes the name pseudocyclic to Bruck). There are relations to orthogonal latin squares (Bruck **(4)**). C-matrices may be interpreted as the adjacency matrices of the Δ-graphs of Erdös and Rényi **(8)** and of certain self-complementary graphs of Sachs **(15)**. Finally, but we do not claim any completeness, investigations on finite permutation groups by D. G. Higman **(9)** are related to C-matrices.

We use the following notations. I_k denotes the $k \times k$ unit matrix, J_k the $k \times k$ matrix consisting solely of 1's and j_k the $k \times 1$ matrix consisting solely of 1's. Subscripts are deleted if there is no fear of confusion. $\otimes$ denotes the Kronecker matrix product.

2. Paley matrices. Let V be a vector space of dimension 2 over $GF(q)$, the Galois field of order $q = p^k$, p prime, $p \neq 2$. Let χ denote the Legendre symbol, defined by $\chi(0) = 0$, $\chi(\alpha) = 1$ or -1 according as $\alpha \neq 0$ is or is not a square in GF(q). Then $\chi(-1) = 1$ or -1 according as $q \equiv 1$ or $-1 \pmod 4$. We consider the function χ *det*, where the determinant *det* denotes any alternating bilinear form on V. The $q + 1$ one-dimensional subspaces of V, which are the $q + 1$ projective points of the projective line PG$(1, q)$, are represented by the vectors $x_0, x_1, \ldots, x_q$, no two of which are dependent. We now define the *Paley matrix* C of the $q + 1$ vectors as follows:

$$C = [\chi \det(x_i, x_j)], \qquad i, j = 0, 1, \ldots, q.$$

In addition, we define the *line matrix* S of the q vectors $y_1, y_2, \ldots, y_q$, which are on a line not through the origin, as follows:

$$S = [\chi \det(y_i, y_j)], \qquad i, j = 1, 2, \ldots, q.$$

The following operations on square matrices:

(1) multiplication by -1 of any row and of the corresponding column,

(2) interchange of rows and, simultaneously, of the corresponding columns,

generate a relation, called *equivalence*. The second operation alone also generates a relation, called *permutation equivalence*.

THEOREM 2.1. *To the projective line* PG$(1, q)$ *there is attached a class of equivalent Paley matrices C of order $q + 1$, symmetric if $q + 1 \equiv 2 \pmod 4$ and skew if $q + 1 \equiv 0 \pmod 4$, with elements $c_{ii} = 0$, $c_{ij} = \pm 1$ for $i \neq j$, $i, j = 0, 1, \ldots, q$, satisfying $CC^T = qI$.*

Proof. The operations (1) and (2) on Paley matrices are effected by multiplication of any vector by a non-square element of GF(q) and by interchange of any two vectors respectively. Therefore, all Paley matrices of order $q + 1$ are equivalent. We only need to prove the property $CC^T = qI$ for one matrix C. To that end we consider the Paley matrix of the vectors x and $y + \alpha_i x$, where x and y are independent and α_i runs through GF(q):

$$C = \chi\det(x, y)\begin{bmatrix} 0 & j^T \\ j\chi(-1) & \chi(\alpha_i - \alpha_j) \end{bmatrix}, \qquad i, j = 1, \ldots, q.$$

The desired property then follows from Jacobsthal's formula (**(10)**, cf. **(17**, p. 66**)**):

$$\textstyle\sum_{\alpha\in GF(q)} \chi(\alpha)\chi(\alpha + \beta) = -1, \qquad \beta \in \mathrm{GF}(q), \beta \neq 0.$$

THEOREM 2.2. *All line matrices S of order q are permutation equivalent. They satisfy*

$$SS^T = qI - J, \qquad SJ = JS = 0.$$

They are permutation equivalent to a multicirculant matrix. They are permutation equivalent to a matrix of the form

$$\begin{bmatrix} 0 & j^T & -j^T \\ \chi(-1)j & A & B \\ -\chi(-1)j & \chi(-1)B^T & -A \end{bmatrix}$$

with circulant matrices A and B of order $\frac{1}{2}(q - 1)$.

Proof. The line matrix of the vectors $y + \alpha_1 x, \ldots, y + \alpha_q x$, where $\alpha_1, \ldots, \alpha_q$ denote the elements of GF(q), is

$$S = \chi\det(x, y)[\chi(\alpha_i - \alpha_j)], \qquad i, j = 1, \ldots, q.$$

If $\chi\det(x, y) = -1$, then for some non-square γ all $\alpha_i\gamma$ are distinct and S is permutation equivalent to $[\chi(\alpha_i - \alpha_j)]$. Hence all line matrices are permutation equivalent. The relations for S follow from

$$qI = CC^T = \begin{bmatrix} 0 & j^T \\ j\chi(-1) & S \end{bmatrix}\begin{bmatrix} 0 & j^T\chi(-1) \\ j & S^T \end{bmatrix}.$$

The multicirculant form is obvious for $q = p$ and readily follows for $q = p^k$; cf. **(2)**. The last standard form is obtained by taking $\chi\det(y, x) = 1$ and by arranging the vectors as follows:

$$y, \quad y + x\eta^2, \quad y + x\eta^4, \ldots, \quad y + x\eta^{q-1}, \quad y + x\eta, \quad y + x\eta^3, \ldots, \quad y + x\eta^{q-2}$$

where η denotes any primitive element of GF(q). Hence the theorem is proved.

Any linear mapping u: $V \to V$ satisfies

$$\det(u(x), u(y)) = \det u \cdot \det(x, y)$$

for all $x, y \in V$. We define linear mappings v and w, which will be used in the proof of Theorem 2.3. Let ϵ be any primitive element of GF(q^2), the quadratic extension of $GF(q)$. We choose any basis in V. With respect to this basis, v is defined by the matrix

$$(v) = \frac{1}{2}\begin{bmatrix} \epsilon^{q-1} + \epsilon^{1-q} & (\epsilon^{q-1} - \epsilon^{1-q})\epsilon^{\frac{1}{2}(q+1)} \\ (\epsilon^{q-1} - \epsilon^{1-q})\epsilon^{-\frac{1}{2}(q+1)} & \epsilon^{q-1} + \epsilon^{1-q} \end{bmatrix},$$

which indeed has its element in $\mathrm{GF}(q)$. Then $\det(v) = 1$ and the eigenvalues of v are ϵ^{q-1} and ϵ^{1-q}, both elements of $\mathrm{GF}(q^2)$ whose $\frac{1}{2}(q+1)$th power, and no smaller, belongs to $GF(q)$. Hence v acts on $\mathrm{PG}(1, q)$ as a permutation with period $\frac{1}{2}(q+1)$, without fixed points, which divides the points of $\mathrm{PG}(1, q)$ into two sets of transitivity each containing $\frac{1}{2}(q+1)$ points. In addition, w is defined by the matrix

$$(w) = \begin{bmatrix} 0 & \epsilon^{q+1} \\ 1 & 0 \end{bmatrix}.$$

Then $\chi \det(w) = -\chi(-1)$. The eigenvalues of w are $\pm\epsilon^{\frac{1}{2}(q+1)}$, elements of $\mathrm{GF}(q^2)$ whose square is in $\mathrm{GF}(q)$. Hence w acts on $\mathrm{PG}(1, q)$ as a permutation with period 2, which maps any point of one set of transitivity, defined above by v, into the other set. Indeed, for $i = 1, \ldots, \frac{1}{2}(q+1)$, the mapping $v^i w$ has no eigenvalue in $\mathrm{GF}(q)$. Finally we remark that $vw = wv$.

THEOREM 2.3. *The equivalence class of Paley matrices of order $q + 1$ contains a member of the form*

$$\begin{bmatrix} A & B \\ B & -A \end{bmatrix} \text{ or } \begin{bmatrix} A & B \\ -B & A \end{bmatrix},$$

according as $q + 1 \equiv 2$ or $0 \pmod 4$, with B symmetric, A and B circulant in the first case and skew-circulant in the second case.*

Proof. Represent the $q + 1$ points of $\mathrm{PG}(1, q)$ by the following $q + 1$ vectors in V:

$$x,\quad v(x),\quad v^2(x), \ldots,\quad v^{\frac{1}{2}(q-1)}(x),\quad w(x),\quad vw(x),\quad v^2w(x), \ldots,\quad v^{\frac{1}{2}(q-1)}w(x).$$

Observing that, for $i, j = 0, 1, \ldots, \frac{1}{2}(q-1)$,

$$\begin{aligned} \det(v^i w(x), v^j w(x)) &= \det(w) \cdot \det(v^i(x), v^j(x)) = \det(w) \cdot \det(x, v^{j-i}(x)), \\ \det(v^i(x), v^j w(x)) &= -\det(v^i w(x), v^j(x)) = \det(v^j(x), v^i w(x)), \\ \det(v^i(x), v^j(x)) &= -\det(v^{\frac{1}{2}(q+1)+i}(x), v^j(x)), \end{aligned}$$

we conclude that the Paley matrix belonging to these vectors has the desired form.

3. Symmetric C-matrices.

THEOREM 3.1. *Necessary conditions for the existence of a symmetric matrix C of order v with elements $c_{ii} = 0$; $c_{ij} = c_{ji} = \pm 1$ for $i \neq j$, $i, j = 1, \ldots, v$,*

*A matrix of order n is called skew-circulant if its elements satisfy $a_{i,j} = a_{1,j-i+1}$ if $j \geqslant i$ and $a_{i,j} = -a_{1,j-i+1+n}$ if $j < i$.

satisfying $C^2 = (v-1)I$, *are* $v \equiv 2 \pmod 4$ *and* $v - 1 = a^2 + b^2$, *a and b integers.*

This theorem was first conjectured by Belevitch **(1)** and first proved, with Hasse–Minkowski methods, by Raghavarao **(14)**. For elementary proofs we refer to **(2)** and **(11)**. The matrices described in Theorem 3.1 will be called *symmetric C-matrices.*

LEMMA 3.2. *Any symmetrically partitioned symmetric C-matrix of order v satisfies*

$$C = \begin{bmatrix} A & B \\ B^T & D \end{bmatrix} = \begin{bmatrix} P(A+aI) & PB+bQ \\ QB^T+bP & Q(D-aI) \end{bmatrix}^{-1} \times \begin{bmatrix} aI & bI \\ bI & -aI \end{bmatrix} \begin{bmatrix} P(A+aI) & PB+bQ \\ QB^T+bP & Q(D-aI) \end{bmatrix}$$

for any real square matrices P, Q and real numbers a, b with $v - 1 = a^2 + b^2$, *for which the transformation matrix is regular.*

Proof. For any square matrices C, D, R of equal order, which satisfy $C^2 = D^2 = (v-1)I$, we have $(RC + DR)C = D(RC + DR)$. This implies the statement in the lemma.

Remark. By taking P, Q, a, b rational, which is possible by Theorem 3.1, we obtain rational representations of symmetric C-matrices. Analogously, rational representations of skew C-matrices may be obtained, since for any order $v \equiv 0 \pmod 4$ skew integer matrices exist whose square equals $1 - v$ times the unit matrix.

THEOREM 3.3 (*Belevitch* **(1)**). *Any symmetric C-matrix is permutation equivalent to a matrix of the form*

$$\sqrt{v-1}\begin{bmatrix} 2(I+NN^T)^{-1} - I & -2(I+NN^T)^{-1}N \\ -2(I+N^TN)^{-1}N^T & I - 2(I+N^TN)^{-1} \end{bmatrix}$$

for some square matrix N whose elements have the form $r + s\sqrt{(v-1)}$, *r and s rationals.*

Proof. By suitable symmetric permutation we may write

$$C = \begin{bmatrix} A & B \\ B^T & D \end{bmatrix} = \begin{bmatrix} U & V \\ W & X \end{bmatrix} \begin{bmatrix} I\sqrt{v-1} & 0 \\ 0 & -I\sqrt{v-1} \end{bmatrix} \begin{bmatrix} U^T & W_T^T \\ V^T & X \end{bmatrix},$$

$$\begin{bmatrix} U & V \\ W & X \end{bmatrix} \begin{bmatrix} U^T & W^T \\ V^T & X^T \end{bmatrix} = I,$$

with non-singular $2\sqrt{(v-1)}\,UU^T = A + I\sqrt{(v-1)}$.

Then also

$$2\sqrt{(v-1)}XX^T = I\sqrt{(v-1)} - D$$

is non-singular. Applying Lemma 3.2 for $a = \sqrt{(v-1)}$, $b = 0$,

$$P = \{A + I\sqrt{(v-1)}\}^{-1}, \qquad Q = \{D - \sqrt{(v-1)}I\}^{-1},$$

https://doi.org/10.4153/CJM-1967-091-8 Published online by Cambridge University Press

and calling $PB = -N$, we obtain $QB^T = N^T$ and

$$C = \begin{bmatrix} A & B \\ B^T & D \end{bmatrix} = \sqrt{v-1}\begin{bmatrix} I & -N \\ N^T & I \end{bmatrix}^{-1}\begin{bmatrix} I & 0 \\ 0 & -I \end{bmatrix}\begin{bmatrix} I & -N \\ N^T & I \end{bmatrix}$$

$$= \sqrt{v-1}\begin{bmatrix} -I & 0 \\ 0 & I \end{bmatrix} + 2\sqrt{v-1}\begin{bmatrix} I & N \\ N^T & -I \end{bmatrix}^{-1}$$

which is the matrix mentioned in the theorem.

Remark. For symmetric C-matrices of the form of Theorem 3.3, which satisfy the special property

$$(*) \qquad NJ = N^TJ = nJ$$

for some real number n, it follows that

$$JA = AJ = -JD = -DJ = \frac{1-n^2}{1+n^2}\sqrt{v-1}\, J,$$

$$JB = BJ = \frac{2n}{1+n^2}\sqrt{v-1}\, J.$$

In both formulae the coefficient of J,

$$a = \frac{1-n^2}{1+n^2}\sqrt{v-1}, \qquad b = \frac{2n}{1+n^2}\sqrt{v-1},$$

respectively, is an integer. In fact, a is even and b is odd. Since $a^2 + b^2 = v - 1$, an interpretation of the integers a and b occurring in Theorem 3.1 is obtained for symmetric C-matrices with property (*). In addition, if any such matrix satisfies $a = 0$, then all row sums are equal. This applies to symmetric C-matrices with property (*) of order

$$v = p^{2k} + 1, \qquad p \equiv -1 \pmod 4,\ p \text{ prime},$$

since in this case the decomposition of $v - 1$ as a sum of two squares of integers is unique. The authors do not know any example of a symmetric C-matrix which is not equivalent to a C-matrix with property (*).

THEOREM 3.4 *Any symmetric Paley matrix of order $q + 1$ is equivalent to a matrix of the form*

$$\begin{bmatrix} A & B \\ B & -A \end{bmatrix} = \begin{bmatrix} I & -N \\ N & I \end{bmatrix}^{-1}\begin{bmatrix} aI & bI \\ bI & -aI \end{bmatrix}\begin{bmatrix} I & -N \\ N & I \end{bmatrix}$$

with symmetric, circulant, and rational N, where a and b are any rationals satisfying $a^2 + b^2 = q$ and $\det(A + aI) \neq 0$.

Proof. Using the matrix obtained in Theorem 2.3 we apply Lemma 3.2 for $P = -Q = (A + aI)^{-1}$. Putting $(A + aI)^{-1}(B - bI) = N$, we observe that N is symmetric and circulant because A and B have that property. This proves the theorem.

For the order $v = 26$ essentially two symmetric C-matrices are known **(1**, p. 243**)**, corresponding to the decompositions $25 = 4^2 + 3^2$ and $25 = 0^2 + 5^2$. They are both given in the form

$$\begin{bmatrix} A & B \\ B^T & -A \end{bmatrix}$$

with A and B circulant of order 13. The matrix with first row

$$0 - + + + - + + - + + + - , \qquad - + - - + + + + + + - - +$$

is a Paley matrix with $a = 4$, $b = 3$. The corresponding line matrix of order 25 is permutation equivalent to the matrix S which consists of the cyclically permuted blocks

$$I - J, \quad J - 2I - 2P, \quad J - 2I - 2P^2, \quad J - 2I - 2P^3, \quad J - 2I - 2P^4.$$

Here P, of order 5, is defined by $p_{ij} = 1$ if $j - i \equiv 1 \pmod 5$, $p_{ij} = 0$ otherwise. This S is the $(-1, 1)$ adjacency matrix of the net $(5, 3)$, that is, of the graph corresponding to one latin square of order 5.

We call the *exceptional* C-matrix of order 26 the matrix with first row

$$0 - + - - + + + + - - + - , \qquad - - + - + + + + + - + + + .$$

It has $a = 0$, $b = 5$, $A^2 = 13I - J$, $BB^T = 12I + J$. Here B, symmetric with respect to its odd diagonal, is the $(-1, 1)$ incidence matrix of the points and the lines of PG(2, 3).

THEOREM 3.4. *The exceptional C-matrix and the Paley matrix of order* 26 *are not equivalent.*

Proof. By equivalence operations the first and second row and column of the exceptional C-matrix of order 26 are transformed into

$$0 + + \ldots + + \ldots + , \qquad + 0 + \ldots + - \ldots - .$$

Then four submatrices of order 12 arise. Now equivalence with the Paley matrix would imply, in view of Theorem 2.2, that each of these submatrices can be permuted into a circulant matrix. Hence all rows of the square of any submatrix would have to consist of the same set of numbers. However, by inspection this is seen not to be the case.

4. C-matrices and Hadamard matrices. In this section we restrict our attention to symmetric and skew C-matrices of order v of the form

$$C_v = \begin{bmatrix} 0 & j^T \\ \pm j & S_{v-1} \end{bmatrix}$$

with adapted sign $\pm$. Here S_{v-1} of order $v - 1$ satisfies

$$SS^T = (v-1)I - J, \qquad SJ = JS = 0, \qquad S^T = \pm S,$$

and conversely determines C_v. We shall refer to the pair S_{v-1}, C_v, THEOREM 4.1. *If the pair S_n, C_{n+1} exists, then a pair of symmetric S_{n^2}, C_{n^2+1} exists.*

Proof. By a result due to Belevitch (**2**) the matrix

$$S_{n^2} = S_n \otimes S_n + I_n \otimes J_n - J_n \otimes I_n$$

has order n^2, has elements 0 on the diagonal and ± 1 elsewhere, is symmetric, and satisfies the relations for S mentioned above. These statements are obtained by straightforward calculation using the properties of the Kronecker product.

COROLLARY 4.1. *There exists a pair of symmetric* $S_{(N-1)^2}$, $C_{(N-1)^2+1}$ for $N = p^h + 1 \equiv 2 \pmod 4$ *and for*

$$N = 2^k \prod_{i=1}^{r} (p_i^{h_i} + 1), \qquad p_i^{h_i} + 1 \equiv 0 \pmod 4,$$

where p, p_i are odd primes, h, k, h_i are non-negative integers, $i = 1, \ldots, r$.

Proof. Paley (**13**) constructed symmetric C-matrices and Williamson (**17**) constructed skew C-matrices of the respective orders N. Hence the pair S_{N-1}, C_N exists and Theorem 4.1 can be applied.

The following theorem is only a slight extension of a theorem of Ehlich (**7**).

THEOREM 4.2. *If symmetric or skew C-matrices of order n and of order $n + 2$ exist, then a Hadamard matrix of order n^2 exists.*

Proof. If the pairs S_{n-1}, C_n and S_{n+1}, C_{n+2} exist, then one pair is symmetric and the other is skew. By straightforward computation it follows that the matrix

$$K = S_{n-1} \otimes S_{n+1} + I_{n-1} \otimes J_{n+1} - J_{n-1} \otimes I_{n+1} - I_{n-1} \otimes I_{n+1},$$

which has order $n^2 - 1$ and elements ± 1, satisfies $KK^T = n^2 I - J$, $KJ = JK = J$. Then

$$H = \begin{bmatrix} -1 & j^T \\ j & K \end{bmatrix}$$

is a Hadamard matrix of order n^2.

For future reference we introduce the generalized permutation matrices

$$P_m = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \otimes I_{\frac{1}{2}m}, \qquad K_m = \bar{K}_4 \otimes I_{\frac{1}{4}m}, \qquad L_m = \bar{L}_4 \otimes I_{\frac{1}{4}m},$$
$$M_m = \bar{M}_4 \otimes I_{\frac{1}{4}m},$$

where $\bar{K}$, $\bar{L}$, $\bar{M}$ are the quaternion matrices of order four (**17**, p. 68). P, K, L, M are skew and satisfy

$$PP^T = KK^T = LL^T = MM^T = I, \qquad KL = M, \qquad LM = K, \qquad MK = L.$$

The following theorem is a slight extension of a theorem of Williamson (**17**).

https://doi.org/10.4153/CJM-1967-091-8 Published online by Cambridge University Press

THEOREM 4.3. *If a Hadamard matrix of order $m > 1$ and a symmetric C-matrix of order n exist, then a Hadamard matrix of order mn exists.*

Proof. Let H_m be a Hadamard matrix, P_m the generalized permutation matrix, and C_n a systematic C-matrix. By straightforward calculation it follows that

$$H_{mn} = H_m \otimes C_n + P_m H_m \otimes I_n$$

is a Hadamard matrix of order mn.

COROLLARY 4.3. *If a Hadamard matrix of order $m > 1$ exists and if N is defined as in Corollary* 4.1, *then a Hadamard matrix of order* $m((N - 1)^2 + 1)$ *exists.*

THEOREM 4.4. *If a Hadamard matrix of order $m > 1$ and a symmetric C-matrix of order n exist, then a Hadamard matrix of order $mn(n - 1)$ exists.*

Proof. For a Hadamard matrix H_m, a generalized permutation matrix P_m, and a pair of symmetric S_{n-1}, C_n the matrix

$$K = H_m \otimes C_n \otimes S_{n-1} + P_m H_m \otimes C_n \otimes I_{n-1} + H_m \otimes I_n \otimes J_{n-1}$$

has order $mn(n - 1)$, has elements ± 1, and satisfies $KK^T = mn(n - 1)I$.

THEOREM 4.5. *If a Hadamard matrix of order $m > 2$ and symmetric C-matrices of orders n and $n + 4$ exist, then a Hadamard matrix of order $mn(n + 3)$ exists.*

Proof. For a Hadamard matrix H_m, generalized permutation matrices K_m, L_m, and pairs of symmetric S_{n-1}, C_n and S_{n+3}, C_{n+4} the matrix

$$K = H_m \otimes C_n \otimes S_{n+3} + K_m H_m \otimes C_n \otimes I_{n+3} + L_m H_m \otimes I_n \otimes (2I - J)_{n+3}$$

is a Hadamard matrix of order $mn(n + 3)$.

Remark. Theorems 4.3, 4.4, 4.5 are the counterparts of results of Williamson (**17**, **18**), who proved these theorems for skew instead of symmetric C-matrices, but without the restrictions $m > 1$ and $m > 2$. Theorems 4.4 and 4.5 improve results of Williamson (**17**, **18**), who proved these theorems for $m = n_1 n_2$, where $n_1 > 1$ and $n_2 > 1$ are orders of Hadamard matrices, and for n and $n + 4$ both of the form $p^h + 1 \equiv 2 \pmod 4$, p odd prime.

Some numerical results follow. For $N = 16$ Corollary 4.1 yields a new symmetric C-matrix of order 226, which is not a Paley matrix. New Hadamard matrices of orders 452 and 904 are then obtained from Corollary 4.3. Hadamard matrices of order $612 = 2 \times 17 \times 18$ and of order $1300 = 2 \times 25 \times 26$ are obtained from Theorem 4.4 and of order $3016 = 4 \times 26 \times 29$ from Theorem 4.5.

REFERENCES

1. V. Belevitch, *Theory of 2n-terminal networks with application to conference telephony*, Elect. Commun., *27* (1950), 231–244.
2. ——— *Conference networks and Hadamard matrices*, Proceedings of the Cranfield Symposium (1965), to be published.

https://doi.org/10.4153/CJM-1967-091-8 Published online by Cambridge University Press

3. R. C. Bose, *Strongly regular graphs, partial geometries and partially balanced designs*, Pacific J. Math., *13* (1963), 389–419.
4. R. H. Bruck, *Finite nets, II, Uniqueness and imbedding*, Pacific J. Math., *13* (1963), 421–457.
5. W. S. Connor and W. H. Clatworthy, *Some theorems for partially balanced designs*, Ann. Math. Statist., *25* (1954), 100–112.
6. H. S. M. Coxeter, *Regular compound polytopes in more than four dimensions*, J. Math. and Phys., *12* (1933) 334–345.
7. H. Ehlich, *Neue Hadamard-Matrizen*, Arch. Math., *16* (1965), 34–36.
8. P. Erdös and A. Rényi, *Asymmetric graphs*, Acta Math. Acad. Sci. Hungar., *14* (1963), 295–315.
9. D. G. Higman, *Finite permutation groups of rank 3*, Math. Z., *86* (1964), 145–156.
10. E. Jacobsthal, *Anwendung einer Formel aus der Theorie der quadratischen Reste*, Dissertation (Berlin, 1906).
11. J. H. van Lint and J. J. Seidel, *Equilateral point sets in elliptic geometry*, Kon. Ned. Akad. Wetensch. Amst. Proc. A, *69* (= Indag. Math. *28*) (1966), 335–348.
12. D. M. Mesner, *A note on the parameters of PBIB association schemes*, Ann. Math. Statist., *36* (1965), 331–336.
13. R. E. A. C. Paley, *On orthogonal matrices*, J. Math. Phys., *12* (1933), 311–320.
14. D. Raghavarao, *Some aspects of weighing designs*, Ann. Math. Statist., *31* (1960), 878–884.
15. H. Sachs, *Über selbstkomplementäre Graphen*, Publ. Math. Debrecen, *9* (1962), 270–288.
16. J. J. Seidel, *Strongly regular graphs of L_2-type and of triangular type*, Kon. Ned. Akad. Wetensch. Amst. Proc. A, *70* (= Indag. Math. *29*) (1967), 188–196.
17. J. Williamson, *Hadamard's determinant theorem and the sum of four squares*, Duke Math. J., *11* (1944), 65–81.
18. ——— *Note on Hadamard's determinant theorem*, Bull. Amer. Math. Soc., *53* (1947), 608–613.

M.B.L.E. Research Laboratory, Brussels, Belgium, and
Technological University, Eindhoven, Netherlands