Can. J. Math., Vol. XXIII, No. 5, 1971, pp. 816–832

ORTHOGONAL MATRICES WITH ZERO DIAGONAL. II

P. DELSARTE, J. M. GOETHALS, AND J. J. SEIDEL

1. Introduction. C-matrices appear in the literature at various places; for a survey, see [**11**]. Important for the construction of Hadamard matrices are the symmetric C-matrices, of order $v \equiv 2 \pmod 4$, and the skew C-matrices, of order $v \equiv 0 \pmod 4$. In § 2 of the present paper it is shown that there are essentially no other C-matrices. A more general class of matrices with zero diagonal is investigated, which contains the C-matrices and the matrices of (v, k, λ)-systems on k and $k + 1$ in the sense of Bridges and Ryser [**6**]. Skew C-matrices are interpreted in § 3 as the adjacency matrices of a special class of tournaments, which we call strong tournaments. They generalize the tournaments introduced by Szekeres [**24**] and by Reid and Brown [**21**]. In § 4 we introduce the notion of negacyclic C-matrices, analogous to the similar notion introduced by Berlekamp in the setting of coding theory (cf. [**4**, p. 211]). Eigenvalues of negacyclic matrices are characterized and standard forms are obtained. Negacyclic C-matrices are interpreted in § 5 as the matrices of a special class of the relative difference sets introduced by Butson [**7**]. Exploiting some results of Elliott and Butson [**10**], we obtain a "multiplier theorem" for negacyclic C-matrices, and adapting a result of [**2**], we show that any negacyclic C-matrix has a nontrivial multiplier. Necessary conditions for the existence of a negacyclic C-matrix of order v are obtained in § 6. The nonexistence of negacyclic C-matrices of all orders $v \leqq 226$, $v \neq 1 + p^k$, with p prime, has been verified. This leads to the conjecture that they do not exist, unless $v = 1 + p^k$. Paley [**19**] constructed C-matrices of all orders $v = 1 + p^k$, p prime. In § 7 it is shown that every Paley matrix is equivalent to a negacyclic C-matrix, a fact that was pointed out to us by R. Turyn (private communication). It would be interesting to know if there exists a negacyclic C-matrix not equivalent to a Paley matrix. Using the standard forms of Theorem 4.3, we take the opportunity to correct an error in Theorem 2.3 of our previous paper [**11**], which was pointed out to us by V. Belevitch.

As for the notations, I and J denote, as usual, the unit and all-one matrices, and j is the all-one column vector. The matrix A^T denotes the transpose of A and, unless otherwise specified, all vectors and matrices are of order v.

2. C-matrices. A C-matrix of order v is a square matrix C with diagonal elements 0, and other elements $+1$ or -1, satisfying

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

Received February 22, 1971 and in revised form, May 18, 1971.

This equation is not altered if some rows and columns of C are multiplied by -1. Hence C can be transformed into a matrix of the form

$$C = \begin{bmatrix} 0 & j^T \\ j & S \end{bmatrix}, \tag{2.1}$$

where j is the all-one vector of order $v - 1$, and S is a square matrix of order $v - 1$ satisfying

$$Sj = 0, \qquad SS^T = (v - 1)I - J. \tag{2.2}$$

Conversely, if a square matrix S of order $v - 1$ exists, satisfying (2.2), then the matrix (2.1) is a C-matrix. These matrices constitute a particular class of the set of square matrices M of order v, with 0 on the diagonal and $+1$ or -1 elsewhere, satisfying

$$MM^T = mI + (v - 1 - m)J, \tag{2.3}$$

where m is some integer.

We shall begin with a discussion of this matrix relation. We first observe that equation (2.3) is not altered if some columns of M are multiplied by -1. For given parameters v and m, multiplication on the right by a diagonal matrix Δ of diagonal elements $+1$ or -1 generates an equivalence relation on the set of matrices M. Accordingly, we shall say that two matrices M_1 and M_2, with the same parameters v and m, are equivalent whenever there exists a diagonal matrix Δ with diagonal elements ± 1 such that $M_1 = M_2\Delta$.

THEOREM 2.1. *Given v and m, with $m \neq v - 1$, the equivalence class of matrices M contains a matrix B satisfying*

$$\begin{aligned} BB^T &= B^TB = mI + (v - 1 - m)J, \\ Bj &= B^Tj = bj, \\ b^2 &= (v - 1)(v - m), \\ B^T &= (-1)^{(m-1)/2}B. \end{aligned} \tag{2.4}$$

This normal matrix B is unique up to multiplication by $-I$.

Proof. Since $m \neq v - 1$, the eigenvalues of MM^T are m with multiplicity $v - 1$, and $(v - 1)(v - m)$ with multiplicity 1. The matrix M^TM has the same eigenvalues with the same multiplicities, whence $M^TM - mI$ is a symmetric rational matrix of rank 1. Let us write

$$M^TM - mI = (v - 1 - m)xx^T,$$

with $x^T = (x_1, x_2, \ldots, x_v)$. Now, since M has zero on the diagonal and $+1$ or -1 elsewhere, all diagonal elements of M^TM are $v - 1$, whence $x_i^2 = 1$ for $i = 1, 2, \ldots, v$. Therefore, we may write $x = \Delta j$, where Δ is a diagonal matrix of diagonal elements $+1$ or -1. It is then easily verified that the matrix $B = M\Delta$ satisfies (2.4), from which we obtain

$$BB^TBj = (v - 1)(v - m)Bj.$$

https://doi.org/10.4153/CJM-1971-091-x Published online by Cambridge University Press

Hence Bj is necessarily a multiple of j, since j is the only eigenvector of BB^T associated with the eigenvalue $(v-1)(v-m)$. The same argument applied to B^Tj leads to the conclusion that

$$Bj = B^Tj = bj,$$

with $b^2 = (v-1)(v-m)$. It remains to be shown that $B^T = (-1)^{(m-1)/2}B$. To that end, we consider the scalar product of any two distinct rows of B, $(b_{i,1}, b_{i,2}, \ldots, b_{i,v})$ and $(b_{j,1}, b_{j,2}, \ldots, b_{j,v})$; and we denote by n_0, n_1, n_2, n_3, respectively, the number of indices k for which the ordered pair $(b_{i,k}, b_{j,k})$ equals $(1, 1)$, $(1, -1)$, $(-1, 1)$, $(-1, -1)$, respectively. Then, from the equations for B, we have

$$\begin{aligned} n_0+n_1+n_2+n_3 &= v-2 \qquad \text{whence } 4n_0 = 2v-3-m+2b-(b_{i,j}+b_{j,i}) \\ n_0+n_1-n_2-n_3 &= b-b_{i,j} \qquad\qquad 4n_1 = m-1-(b_{i,j}-b_{j,i}) \\ n_0-n_1+n_2-n_3 &= b-b_{j,i} \qquad\qquad 4n_2 = m-1+(b_{i,j}-b_{j,i}) \\ n_0-n_1-n_2+n_3 &= v-1-m, \qquad\qquad 4n_3 = 2v-3-m-2b+(b_{i,j}+b_{j,i}). \end{aligned}$$

Since $b_{i,j} \pm b_{j,i}$ equals $0, +2$, or -2, we conclude that $m-1$ is even, and that $b_{i,j} - b_{j,i} \equiv m-1 \pmod 4$, which proves the formulae for B. Finally, if B_1 and $B_2 = B_1\Delta$ are two normal matrices, satisfying (2.3) and belonging to the same equivalence class, it readily follows that

$$B_1B_1^T = \Delta B_1^TB_1\Delta = \Delta B_1B_1^T\Delta,$$

whence, from (2.3), $\Delta J\Delta = J$, which is only possible for $\Delta = \pm I$. This completes the proof of the theorem.

COROLLARY 2.2. *Any C-matrix of order $v > 2$ is equivalent, under multiplication of rows and columns by -1, to a symmetric or to a skew-symmetric C-matrix, according as v satisfies $v \equiv 2 \pmod 4$ or $v \equiv 0 \pmod 4$.*

Proof. Under multiplication of rows and columns by -1, any C-matrix can be transformed into a matrix C of the form (2.1), where S is normal and satisfies (2.2). It then follows from Theorem 2.1 that S is symmetric or skew, according as $v \equiv 2 \pmod 4$ or $v \equiv 0 \pmod 4$, which proves the corollary.

Remarks. (i) For the state of affairs concerning the construction of symmetric and skew C-matrices, we refer to [**11**; **12**; **15**; **25**]. The smallest undecided cases are $v = 46$ and $v = 92$, respectively.

(ii) The cases $m = v$ or $m = v-1$ lead either to matrices S or to C-matrices. They exist simultaneously. For $m \neq v-1$, skew matrices B are only possible if $b = 0$, that is, $v = m \equiv -1 \pmod 4$ (cf. Theorem 2.1). In all remaining cases, B is symmetric and satisfies

$$B^2 - mI = (v-1-m)J, \qquad Bj = bj,$$

with $b^2 = (v-1)(v-m) > 0$. The symmetric matrix A of order v, with elements 0 and 1, defined by $B = J - I - 2A$, satisfies

$$A^2 + A = (k-\lambda)I + \lambda J, \qquad AJ = kJ,$$

where $k = (v - 1 - b)/2$ and $k - \lambda = (m - 1)/4$. Hence A is the matrix of a (v, k, λ)-*system on* k *and* $k + 1$, as defined in [**6**]. It can be shown that m has to be the square of an integer s (cf. [**6**]), and that s necessarily divides $16\lambda^2 - 1$ (cf. [**5**]). Thus, for each λ, there are finitely many such systems. For the state of affairs concerning these systems, we refer to [**5**], where a (243, 22, 2)-system on 22 and 23 is constructed.

3. Strong tournaments. A *tournament* of order v is described by the pair $\{V, A\}$ of the set V of its v vertices and its adjacency matrix A, which is defined by its elements $a_{x,x} = 0$, $a_{x,y} = -a_{y,x} = 1$ if $x \in V$ dominates $y \in V$. A special class of tournaments was treated in [**24**], under the name of extreme $T_{2,m}$ tournaments, and in [**21**] under the name of doubly regular tournaments. Instead, we propose the name of strongly regular tournaments and, in addition, we introduce the notion of strong tournaments, in analogy to the notions of strongly regular and strong graphs (cf. [**22**; **23**]).

Definitions. (*a*) A tournament of order v is *strong* if and only if there exists an integer n such that

$$n(x, y) + n(y, x) = n; \quad \text{for all } x \in V, y \in V, x \neq y,$$

where $n(x, y)$ denotes the number of vertices that dominate x and are dominated by y.

(*b*) A tournament of order v is *strongly regular* if and only if there exist integers l and m such that: (i) the number of vertices dominating each vertex is l, and (ii) the number of vertices dominating each pair of vertices is m.

Obviously, a strongly regular tournament is strong, with $n = 2(l - m) - 1$.

THEOREM 3.1. (Cf. [**21**; **24**].) *A tournament* $\{V, A\}$ *of order* v *is strongly regular if and only if*

$$AA^T = vI - J.$$

It is strong, but not strongly regular, if and only if A *is a skew C-matrix.*

Proof. Let $\{V, A\}$ be a strong tournament. From the definition it follows that, in the scalar product of any two distinct rows of A, two elements are 0, n elements are -1, and $v - 2 - n$ elements are $+1$. Therefore, A satisfies

$$AA^T = (2n + 1)I + (v - 2 - 2n)J.$$

Since A is skew, hence normal, it follows from Theorem 2.1 that the tournament is strongly regular with

$$Aj = aj, \qquad a^2 = (v - 1)(v - 1 - 2n),$$

unless $v = 2n + 2$, in which case A is a skew C-matrix. In the former case, we have $a = 0$ since A is skew, whence $v = 2n + 1$, $l = n$, $m = (n - 1)/2$. This proves the theorem.

4. Negacyclic C-matrices. Let P be the square matrix of order v, whose elements $p_{i,j}$ are defined as follows:

$$p_{i,i+1} = 1,\ i = 0, 1, \ldots, v-2;$$
$$p_{v-1,0} = -1;$$
$$p_{i,j} = 0, \text{ otherwise.}$$

Then, P satisfies

$$P^v = -I, \qquad P^T = -P^{v-1}, \qquad PP^T = I.$$

Any square matrix A of order v, such that $AP = PA$, is called *negacyclic*. Its elements $a_{i,j}$, $0 \leqq i, j \leqq v-1$, satisfy

$$a_{i+1,0} = -a_{i,v-1};$$
$$a_{i+1,j} = a_{i,j-1},\ j = 1, 2, \ldots, v-1,$$

for $i = 0, 1, \ldots, v-2$. Hence all elements are determined by the first row $(a_0, a_1, \ldots, a_{v-1})$, with $a_i = a_{0,i}$. In fact, one has

$$A = a_0 I + a_1 P + a_2 P^2 + \ldots + a_{v-1} P^{v-1}.$$

The set of all negacyclic matrices of order v constitutes an algebra, which is isomorphic to the algebra of polynomials

$$a(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{v-1} x^{v-1}, \tag{4.1}$$

modulo $x^v + 1$, over the field of coefficients a_i. This isomorphism maps A onto $a(x)$ and A^T onto $a(x^{-1})$. Therefore, for a negacyclic C-matrix mapped onto $c(x)$, we have

$$c(x)c(x^{-1}) \equiv v - 1 \pmod{x^v + 1},$$

with

$$c(x) = c_0 + c_1 x + \ldots + c_{v-1} x^{v-1},\ c_0 = 0,\ c_i = \pm 1\ (i \neq 0). \tag{4.2}$$

Let A be a negacyclic matrix of order v with first row $(a_0, a_1, \ldots, a_{v-1})$ and polynomial (4.1). On the other hand, let ω be a complex $2v$th root of unity. Then, it is easily verified that one has

$$A\Omega = \Omega\Lambda,$$

where $\Omega = [\Omega_{i,j} = (\omega^{2j+1})^i;\ i, j = 0, 1, \ldots, v-1]$, and $\Lambda = \operatorname{diag}[a(\omega^{2j+1});\ j = 0, 1, \ldots, v-1]$. Hence the eigenvalues of A are the values

$$\lambda_j = a(\omega^{2j+1}),\ j = 0, 1, \ldots, v-1,$$

taken by $a(x)$ at the v distinct roots of $x^v + 1$. We emphasize that the matrix A is completely determined by the ordered v-tuple $(\lambda_0, \lambda_1, \ldots, \lambda_{v-1})$ of its eigenvalues. Indeed, taking the first row in the matrix equation

$$A = \Omega\Lambda\Omega^{-1},$$

https://doi.org/10.4153/CJM-1971-091-x Published online by Cambridge University Press

we readily obtain

$$a_i = \frac{1}{v}\,\omega^{-i}\sum_{j=0}^{v-1}\lambda_j\omega^{-2ij}, \qquad i = 0, 1, \ldots, v-1.$$

We further observe that, for integers a_i, the eigenvalues λ_j are algebraic integers in the cyclotomic field $Q[\omega]$, and that $\lambda_j \equiv 0 \pmod{n}$ for $j = 0, 1, \ldots, v-1$, implies that $va_i \equiv 0 \pmod{n}$, whence $a_i \equiv 0 \pmod{n/(n,v)}$ for $i = 0, 1, \ldots, v-1$. This result is a basic tool in the proof of Theorem 5.4.

The following theorem, due to Belevitch [**2**], shows that the coefficients c_i of the polynomial $c(x)$ of a negacyclic C-matrix are not independent.

THEOREM 4.1 (Belevitch [**2**]). *The polynomial $c(x)$ of a negacyclic C-matrix of order v satisfies*

$$c(x^{v-1}) \equiv (-1)^{(v-2)/2}c(x) \pmod{(x^v + 1)}.$$

Proof. Let C be a negacyclic C-matrix of order v, with polynomial (4.2). Then the coefficient of x^j, $j \neq 0$, in $c(x)c(x^{-1})$, $\bmod(x^v + 1)$, is

$$\sum_{i=1}^{v-j-1} c_i c_{j+i} + \sum_{i=1}^{j-1}(-c_i c_{v-j+i}) = 0.$$

There are $v - 2$ terms in the above sum, each of which is $+1$ or -1. Thus, there are $(v-2)/2$ terms equal to -1, and their product must be $(-1)^{(v-2)/2}$. But it is easily seen that each c_i, $i = 1, 2, \ldots, v-1$, appears twice in the product, except for c_j and c_{v-j}, each of which appears once. On the other hand, $j - 1$ coefficients c_i appear with a minus sign. Hence the product is

$$(-1)^{j-1}c_j c_{v-j} = (-1)^{(v-2)/2},$$

from which it follows that $c_{v-j} = (-1)^{v/2+j}c_j$ and that

$$\begin{aligned} c(x^{v-1}) &\equiv \sum_{j=1}^{v-1}(-1)^{j-1}c_{v-j}x^j \\ &\equiv (-1)^{(v-2)/2}c(x) \pmod{(x^v + 1)}. \end{aligned}$$

This proves the theorem.

In order to give a better insight into negacyclic C-matrices and to correct a mistake in a theorem of [**11**], we now prove the following result.

THEOREM 4.2. *Any negacyclic C-matrix of order $v = rn$, r odd, $n = 2^m$, is equivalent to a C-matrix of the form*

$$B = \begin{bmatrix} B_0 & B_1 & B_2 & \ldots & B_{n-1} \\ -B_{n-1} & B_0 & B_1 & \ldots & B_{n-2} \\ \vdots & & & & \\ -B_1 & -B_2 & -B_3 & \ldots & B_0 \end{bmatrix}, \tag{4.3}$$

https://doi.org/10.4153/CJM-1971-091-x Published online by Cambridge University Press

where $B_0, B_1, \ldots, B_{n-1}$ *are cyclic matrices of order* r *and satisfy*

$$B_0^T = (-1)^{n/2-1}B_0;$$
$$B^T{}_{n-\lambda} = (-1)^{n/2+\lambda}B_\lambda, \lambda = 1, 2, \ldots, n-1.$$

Proof. Let $c(x)$ be the polynomial (4.2) of the given C-matrix. Since n and r are relatively prime, the set of integers $\lambda r + \mu n$, $\lambda = 0, 1, \ldots, n-1$, and $\mu = 0, 1, \ldots, r-1$, constitutes a complete system of residues modulo $v = rn$. It readily follows that $c(x)$ can be represented in the form

$$c(x) \equiv \sum_{\lambda=0}^{n-1} x^{\lambda r} b_\lambda(-x^n) \pmod{(x^v + 1)}, \tag{4.4}$$

or equivalently, if we set $y = -x^n$ and $z = x^r$, by

$$b(y, z) = \sum_{\lambda=0}^{n-1} z^\lambda b_\lambda(y) \pmod{(z^n + 1, y^r - 1)}. \tag{4.5}$$

Let $\lambda r + \mu n = qv + t$, with $0 \leqq t < v$. Then the coefficient of y^μ in $b_\lambda(y)$ is given by

$$b_{\lambda,\mu} = (-1)^{q+\mu}c_t. \tag{4.6}$$

Defining B_λ as the cyclic matrix with first row $(b_{\lambda,0}, b_{\lambda,1}, \ldots, b_{\lambda,r-1})$, we observe that the element in row $\alpha r + \beta$ and column $\gamma r + \delta$ of the matrix (4.3) is given by the coefficient of $y^\delta z^\gamma$ in the polynomial

$$y^\beta z^\alpha b(y, z) \pmod{(y^r - 1, z^n + 1)},$$

which, according to (4.4), is congruent to

$$(-1)^\beta x^{\alpha r + \beta n} c(x) \pmod{(x^v + 1)}.$$

Since, on the other hand, the element in row i and column j of the matrix C is given by the coefficient of x^j in the polynomial

$$x^i c(x) \pmod{(x^v + 1)},$$

it easily follows from (4.6) that the matrices B and C are equivalent under permutation and multiplication by -1 of rows and columns.

Finally, by Theorem 4.1, one has $c(x^{-1}) \equiv (-1)^{(v-2)/2}c(-x) \pmod{(x^v + 1)}$, whence

$$b(y^{-1}, z^{-1}) \equiv (-1)^{(n-2)/2}b(y, -z) \pmod{(z^n + 1, y^r - 1)}.$$

Using (4.5), one obtains

$$b_0(y^{-1}) \equiv (-1)^{(n-2)/2}b_0(y) \pmod{(y^r - 1)},$$
$$b_{n-\lambda}(y^{-1}) \equiv (-1)^{n/2+\lambda}b_\lambda(y) \pmod{(y^r - 1)},$$

for $\lambda = 1, 2, \ldots, n-1$. This completes the proof of the theorem.

By specialization of Theorem 4.2 for $n = 2$ and $n = 4$, respectively, we have the following results.

THEOREM 4.3. (i) *Any negacyclic C-matrix of order* $v \equiv 2 \pmod 4$ *is equivalent to a C-matrix of the form*

$$B = \begin{bmatrix} B_0 & B_1 \\ -B_1 & B_0 \end{bmatrix},$$

where B_0 and B_1 are symmetric cyclic matrices of order $v/2$ and

$$v - 1 = \rho_0^2 + \rho_1^2, B_\lambda J = \rho_\lambda J, \lambda = 0, 1. \tag{4.7}$$

(ii) *Any negacyclic C-matrix of order* $v \equiv 4 \pmod 8$ *is equivalent to a C-matrix of the form*

$$B = \begin{bmatrix} B_0 & B_1 & B_2 & -B_1^T \\ B_1^T & B_0 & B_1 & B_2 \\ -B_2 & B_1^T & B_0 & B_1 \\ -B_1 & -B_2 & B_1^T & B_0 \end{bmatrix},$$

where B_0, B_1 *and* B_2 *are cyclic matrices of order* $v/4$, B_2 *is symmetric*, B_0 *is skew and*

$$v - 1 = 2\rho_1^2 + \rho_2^2, B_\lambda J = \rho_\lambda J, \lambda = 1, 2. \tag{4.8}$$

Proof. Application of Theorem 4.2 yields the standard form. The necessary conditions for the order v follow from

$$BB^T J = (v - 1)J.$$

5. Negacyclic *C*-matrices, relative difference sets and multipliers. The concept of a relative difference set was first introduced in [**7**] and later extended in [**10**]. It is defined as follows. Let G be a finite additive group of order sv and H any normal subgroup of G, of order s. Then a set D of k distinct elements of G,

$$D = \{g_1, g_2, \ldots, g_k\},$$

is called a *difference set relative to* H *in* G if, among the $k(k-1)$ differences $g_i - g_j, i \neq j, 1 \leqq i, j \leqq k$, each element of the difference $G \backslash H$ occurs exactly λ times and no element of H occurs. We shall make use of the notation $(s; v, k, \lambda)$ for such a relative difference set (R.D.S.).

An obvious necessary condition for the existence of a $(s; v, k, \lambda)$ R.D.S. is

$$k(k-1) = \lambda s(v-1).$$

It is also clear from the definition that any two distinct elements of D belong to distinct cosets of G with respect to H, since otherwise their difference is an element of H. Hence $v \geqq k \geqq \lambda s$ and the homomorphic image of D, under the natural homomorphism which maps G onto the factor group G/H, is an ordinary $(v, k, \lambda s)$ difference set in G/H.

From now on, we assume that G is the additive cyclic group of integers modulo sv, in which case D is called a *cyclic relative difference set*. It easily follows from the definition that the formal polynomial

$$d(x) = \sum_{g \in D} x^g$$

satisfies

$$d(x)d(x^{-1}) \equiv k + \lambda j_s(x^v)[j_v(x) - 1] \pmod{(x^{sv} - 1)}, \tag{5.1}$$

where

$$j_n(x) = 1 + x + x^2 + \ldots + x^{n-1}. \tag{5.2}$$

We also observe that, when reduced $\bmod(x^v - 1)$, (5.1) becomes

$$d(x)d(x^{-1}) \equiv (k - \lambda s) + \lambda s j_v(x) \pmod{(x^v - 1)}, \tag{5.3}$$

which is a well-known property of an ordinary cyclic $(v, k, \lambda s)$ difference set. On the other hand, for ω a primitive complex sth root of unity, we have $j_s(\omega) = 0$, whence (5.1) reduces to

$$d(x)d(x^{-1}) \equiv k \pmod{(x^v - \omega)}. \tag{5.4}$$

THEOREM 5.1. *There exists a negacyclic C-matrix of order v if and only if there exists a cyclic* $(2; v, v - 1, (v - 2)/2)$ *relative difference set.*

Proof. Let D be a $(2; v, v - 1, (v - 2)/2)$ cyclic R.D.S. with polynomial $d(x)$. Then, (5.4) with $\omega = -1$ yields

$$d(x)d(x^{-1}) \equiv v - 1 \pmod{(x^v + 1)}, \tag{5.5}$$

and (5.3) yields

$$d(x)d(x^{-1}) \equiv 1 + (v - 2)j_v(x) \pmod{(x^v - 1)}. \tag{5.6}$$

Since $d(x)$ has coefficients 0 or $1 \bmod(x^{2v} - 1)$, it follows that the coefficients are 0, $+1$ or $-1 \bmod(x^v + 1)$. Since there are $k = v - 1$ nonzero coefficients, only one, d_i say, is zero. Hence $x^{-i}d(x)$, which still satisfies (5.5), is of the form (4.2) and corresponds to a negacyclic C-matrix. Conversely, let $c(x)$ be the polynomial (4.2) of a negacyclic C-matrix and let us write

$$c(x) = c_1(x) - c_2(x),$$

where all coefficients in $c_1(x)$ and $c_2(x)$ are 0 or 1. Then, $d(x) = c_1(x) + x^v c_2(x)$ satisfies

$$d(x) \equiv c(x) \pmod{(x^v + 1)},$$

and

$$\begin{aligned} d(x) &\equiv c_1(x) + c_2(x) \\ &\equiv j_v(x) - 1 \pmod{(x^v - 1)}. \end{aligned}$$

It easily follows that $d(x)$ satisfies (5.5) and (5.6), whence

$$d(x)d(x^{-1}) \equiv v - 1 + \frac{v - 2}{2}(1 + x^v)[j_v(x) - 1] \pmod{(x^{2v} - 1)},$$

which proves the theorem.

The concept of a multiplier was introduced in [**13**] for ordinary difference sets and later applied to R.D.S. in [**10**]. For cyclic R.D.S., it can be defined as follows. The integer t, $(t, sv) = 1$, is called a *multiplier* of the cyclic $(s; v, k, \lambda)$ relative difference set D with polynomial $d(x)$ if

$$d(x^t) \equiv x^i d(x) \pmod{(x^{sv} - 1)},$$

for an integer i. It easily follows from the definition that the set of multipliers of a given cyclic R.D.S. forms a group under multiplication mod sv.

THEOREM 5.2. *Let C be a negacyclic C-matrix of order v with polynomial $c(x)$ and let D be the associated cyclic $(2; v, v-1, (v-2)/2)$ R.D.S. Then the integer t, with $(t, 2v) = 1$, is a multiplier of D if and only if*

$$c(x^t) \equiv (-1)^{(t-1)/2} c(x) \pmod{(x^v + 1)}.$$

Proof. Let us define $d(x)$ as in Theorem 5.1, that is,

$$d(x) \equiv c(x) \pmod{(x^v + 1)}, \tag{5.7}$$

and

$$d(x) \equiv j_v(x) - 1 \pmod{(x^v - 1)},$$

and let t be a multiplier of D. Then, necessarily, $(t, 2v) = 1$ and (5.7) yields

$$c(x^t) \equiv x^i c(x) \pmod{(x^v + 1)}, \tag{5.8}$$

and

$$j_v(x^t) - 1 \equiv x^i (j_v(x) - 1) \pmod{(x^v - 1)}. \tag{5.9}$$

Since $j_v(x^t) \equiv j_v(x) \pmod{(x^v - 1)}$, it follows from (5.9) that $i \equiv 0 \pmod{v}$; whence, from (5.8),

$$c(x^t) \equiv \pm c(x) \pmod{(x^v + 1)}.$$

The sign is then uniquely determined from the fact that the coefficient of $x^{v/2}$ in $c(x)$ is non-zero, while

$$x^{tv/2} = x^{v(t-1)/2} x^{v/2} \equiv (-1)^{(t-1)/2} x^{v/2} \pmod{(x^v + 1)}.$$

Hence we have

$$c(x^t) \equiv (-1)^{(t-1)/2} c(x) \pmod{(x^v + 1)}. \tag{5.10}$$

Conversely, with $d(x)$ defined by (5.7) and assuming that (5.10) holds, we readily obtain

$$d(x^t) \equiv x^{v(t-1)/2} d(x) \pmod{(x^{2v} - 1)},$$

hence proving that t is a multiplier of D.

We shall say that t is a *multiplier of the negacyclic C-matrix* whenever (5.10) holds. Accordingly, Theorem 4.1 can be restated as follows.

https://doi.org/10.4153/CJM-1971-091-x Published online by Cambridge University Press

THEOREM 5.3. *The integer $v - 1$ is a multiplier of any negacyclic C-matrix of order v.*

Using methods of Mann (cf. [**18**, Chapter 7]), Elliott and Butson were able to extend Hall's multiplier theorem to relative difference sets (cf. [**10**, Theorem 7.1]). A slight variation of the latter yields the following multiplier theorem for negacyclic C-matrices.

THEOREM 5.4. *Let there exist, for all prime divisors p_i of $v - 1$, suitably chosen exponents f_i and multipliers t_i of a negacyclic C-matrix of order v such that*

$$t_i p_i^{f_i} \equiv t \pmod{2v},$$

where t is a fixed integer. Then t and $p_i^{f_i}$ are multipliers of the negacyclic C-matrix.

The proof proceeds along the same lines as in [**10**, Theorem 7.1] and will be omitted. We immediately get two important corollaries.

COROLLARY 5.5. *If $v - 1 = p^k$, where p is a prime, then p is a multiplier of any negacyclic C-matrix of order v.*

Proof. This is immediate from Theorem 5.4.

COROLLARY 5.6. *If $v - 1 = p^i q^j$, where p and q are distinct primes, then p^i and q^j are multipliers of any negacyclic C-matrix of order v.*

Proof. Let k be the order of q mod $2v$. Then, multiplying both members of $v - 1 = p^i q^j$ by q^{k-j}, we obtain

$$(v - 1)q^{k-j} \equiv p^i \pmod{2v}.$$

The result then follows from Theorems 5.3 and 5.4.

Remark. We observe that, for $v - 1 = p^k$ or $v - 1 = pq$, p and q primes, all divisors of $v - 1$ are multipliers for any negacyclic C-matrix of order v. In trying to prove that this property holds generally, we encountered difficulties similar to those arising in Hall's multiplier theorem (cf. [**15**, Theorem 11.4.1]). It is rather easy to show that, for $v - 1 = p^k n$, with $(n, p) = 1$, we have

$$c(x^p)c(x^{-1}) \equiv p^k m(x) \pmod{(x^v + 1)},$$

where $m(x)$ has integer coefficients and

$$m(x)m(x^{-1}) \equiv n^2 \pmod{(x^v + 1)}.$$

But, unless $n = 1$, the latter equation does not imply that $m(x) \equiv nx^i \pmod{(x^v + 1)}$, from which it would follow that p is a multiplier. For example, for $n = 3$ and $v \equiv 0 \pmod 4$, the polynomial

$$m(x) = 1 + 2x^{v/4} + 2x^{3v/4}$$

satisfies $m(x)m(x^{-1}) \equiv 9 \pmod{(x^v + 1)}$.

6. Necessary conditions for the existence of negacyclic *C*-matrices. The following theorem is an application to negacyclic *C*-matrices of [**10**, Theorem 8.1], which itself is a generalization of [**18**, Theorem 7.2]. We shall not repeat the proof.

THEOREM 6.1. *Let p be any prime divisor of $v - 1$ and let d be any odd divisor of v. Let further t be a multiplier of a negacyclic C-matrix of order v, such that*

$$tp^f \equiv -1 \pmod{(2v/d)},$$

for some integer f. Then $v - 1$ must be exactly divisible by an even power of p, p^{2h} say, and

$$c(x) \equiv 0 \pmod{\text{dd } p^h, (x^{v/d} + 1)}.$$

As a consequence of Theorem 6.1, we obtain the necessary conditions of Theorem 6.2.

THEOREM 6.2. *Let $v = 2^m r$, where r is an odd integer, and let there exist a negacyclic C-matrix of order v. Then any prime p dividing the square-free part of $v - 1$ must satisfy*

$$p \equiv 1 \text{ or } p \equiv 2^m - 1 \pmod{2^{m+1}}.$$

Proof. If $p \equiv -1 \pmod{2^{m+1}}$, it follows from Theorem 6.1, with $t = 1$ and $d = r$, that p divides $v - 1$ to an even power, which is a contradiction. From now on, let us assume that $m \geqq 2$ and $p \not\equiv -1, +1$ or $2^m - 1 \pmod{2^{m+1}}$. We shall then show that there exists an integer $l \geqq 1$ such that

$$p^{2^{l-1}} \equiv 2^m + 1 \pmod{2^{m+1}}.$$

Indeed, let k, necessarily of the form $k = 2^l$, $l \geqq 1$, be the order of $p \bmod 2^{m+1}$ and let

$$p^{2^{l-1}} \equiv a \pmod{2^{m+1}}.$$

Then $a^2 \equiv 1 \pmod{2^{m+1}}$, where a is odd. Let us write $a = 2i + 1$. It then follows that

$$i(i + 1) \equiv 0 \pmod{2^{m-1}},$$

whence $i \equiv 0$, or $i + 1 \equiv 0 \pmod{2^{m-1}}$. If $i \equiv 0 \pmod{2^{m-1}}$, then $a \equiv 2^m + 1 \pmod{2^{m+1}}$, which was to be shown. If $i + 1 \equiv 0 \pmod{2^{m-1}}$, then $a \equiv -1 \pmod{2^m}$, whence

$$p^{2^{l-1}} \equiv -1 \pmod{2^m},$$

which is possible only for $l = 1, p \equiv -1 \pmod{2^m}$, and contradicts our assumption. Therefore, there exists an integer $f = 2^{l-1}$ such that

$$p^f \equiv 2^m + 1 \pmod{2^{m+1}},$$

whence

$$(v - 1)p^f \equiv -1 \pmod{2^{m+1}}.$$

https://doi.org/10.4153/CJM-1971-091-x Published online by Cambridge University Press

Applying now Theorem 6.1, with $t = v - 1$ and $d = r$, we are led to a contradiction. This proves the theorem.

We add some comments.

(1) For $m = 1$, that is, $v \equiv 2 \pmod 4$, Theorem 6.2 says that the square-free part of $v - 1$ is divisible only by primes of the form $p \equiv 1 \pmod 4$, which is equivalent to $v - 1 = a^2 + b^2$, a and b integers. This is known to be a necessary condition for the existence of any (not necessarily negacyclic) C-matrix of order v (cf. [**3**; **11**; **17**; **20**]).

For $m = 2$, that is $v \equiv 4 \pmod 8$, these conditions state that the square-free part of $v - 1$ is divisible only by primes p of the form $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$, which is equivalent to $v - 1 = a^2 + 2b^2$, a and b integers. This excludes, for example, 36 as an order for a negacyclic C-matrix. Note, however, that there does exist a C-matrix of that order (cf. [**12**]). Thus, for $m \geqq 2$, the conditions of Theorem 6.2 are more severe than the conditions for the existence of any C-matrix of order v. For instance, orders $v = 16, 36, 40, 56, 64, 88, 92, 96$, for $v \leqq 100$, are excluded by Theorem 6.2, although the first undecided case for the existence of a C-matrix of order $v \equiv 0 \pmod 4$ is $v = 92$.

For $m = 1, 2$, we point out that the numbers a and b appearing above in the decomposition of $v - 1$ into a sum of squares, are related to the standard forms of Theorem 4.3 (cf. equations (4.7) and (4.8)).

(2) For $v - 1 = q = p^k$, where p is a prime, the conditions of Theorems 6.1 and 6.2 are always satisfied. On the other hand, the existence of a cyclic $(2; q + 1, q, (q - 1)/2)$ R.D.S. is assured by a construction of Elliott and Butson (cf. [**10**, Corollary 5.1.1]), and this implies the existence of a negacyclic C-matrix of order $v = 1 + p^k$ (cf. Theorem 5.1). It can be shown that the construction of Elliott and Butson leads to a C-matrix equivalent to the Paley matrix of order $v = 1 + p^k$, which can always be put into a negacyclic form, as we shall show in the next section.

(3) For the remaining orders, no complete answer is known. We announce the following theorem.

THEOREM 6.3. *No negacyclic C-matrix exists of an order v, with $v \leqq 226$, $v \neq 1 + p^k$, p prime.*

The proof is based on the existence of multipliers assured by Corollary 5.7 and uses some manipulations involving the standard form of Theorem 4.2. It is not reproduced here because of the ad hoc character of the theorem. Trying to remove the condition $v \leqq 226$, we are led to the following questions.

(i) Do there exist negacyclic C-matrices of order $v \neq 1 + p^k$, p prime?

(ii) Do there exist negacyclic C-matrices of order $v = 1 + p^k$ that are not equivalent to Paley matrices?

We conjecture that at least question (i) has a negative answer.

7. Paley matrices. Paley [**19**] constructed C-matrices of order $v = q + 1$, with $q = p^k$, p an odd prime, by use of the Legendre symbol χ of the Galois

field GF(q). A variation of this construction (cf. [**11**]) readily leads to a negacyclic form for the Paley matrices. This was pointed out to us by Turyn in private communication. Here, this result is obtained as a corollary to a theorem involving the automorphism group of a Paley matrix. We make use of the equivalence relation on the set of all C-matrices of order v, which is generated by the following operations: multiplication by -1 of any row; multiplication by -1 of any column; and simultaneous interchange of any two rows and of the corresponding columns. These operations generate the group of all generalized permutations of degree v.

Let X be any set of $q+1$ pairwise independent vectors of $V(2, q)$, the 2-dimensional vector space over GF(q). The Paley matrix associated with X is defined by

$$C_X = [\chi \det(\xi, \eta); \xi, \eta \in X],$$

where χ is the Legendre symbol of GF(q) and where $\det(\xi, \eta)$ is the determinant of the vectors ξ and η over GF(q). All Paley matrices C_X of order $q+1$ are easily shown to be equivalent (cf. [**11**]).

It is well known (cf., for instance, [**8**, p. 272]) that the set of substitutions of the form

$$\xi \to \xi' = A\xi^{p^i}, \quad 0 \leqq i < k, \tag{7.1}$$

where A is a nonsingular square matrix of order 2 over GF(q) and where ξ^p is the vector whose components are the pth powers of the components of ξ, acts as a triply transitive permutation group of order $kq(q^2-1)$ on the $q+1$ elements of a set X. The permutation associated with (7.1) maps ξ onto $\delta_\xi \xi'$, where δ_ξ is the unique element of GF(q) such that $\delta_\xi \xi'$ belongs to X when ξ belongs to X. This group is usually denoted by $\mathrm{P\Gamma L}_2(q)$ (cf. [**9**, p. 31]).

The following theorem is a slight generalization of a result due to Hall [**14**].

THEOREM 7.1. *The group* $\mathrm{P\Gamma L}_2(q)$ *induced by the substitutions* (7.1), *acting as a generalized permutation group on the rows and columns of a Paley matrix* C_X, *transforms* C_X *into* C_X *or* $-C_X$, *according as* $\det(A)$ *is a square or a non-square in* GF(q).

Proof. Since the permutation on X associated with (7.1) maps ξ onto $\delta_\xi A \xi^{p^i}$ and since in GF(q)

$$\det(\xi^{p^i}, \eta^{p^i}) = [\det(\xi, \eta)]^{p^i},$$

we readily deduce that

$$QC_XQ^{-1} = [\chi(\delta_\xi)\chi(\delta_\eta)\chi \det(A)\chi \det(\xi, \eta); \xi, \eta \in X],$$

where Q is the permutation matrix associated with (7.1). Hence, defining the diagonal matrix Δ by

$$\Delta = \mathrm{diag}[\chi(\delta_\xi); \xi \in X],$$

https://doi.org/10.4153/CJM-1971-091-x Published online by Cambridge University Press

we obtain

$$(\Delta Q)C_X(\Delta Q)^{-1} = \epsilon_A C_X, \tag{7.2}$$

where $\epsilon_A = \chi \det(A) = \pm 1$. This proves the theorem.

Remark. Theorem 7.1 shows that the group of generalized permutations induced by the set of substitutions (7.1) with determinant 1, acting on the rows and columns of C_X, is contained in the automorphism group Γ_X of the Paley matrix. From a theorem of [**16**] (cf. also [**1**]), it can be shown that, for $q \equiv -1 \pmod 4$, $\Gamma_X/\{I, -I\}$ contains no other operation. In that case, $H_X = C_X + I$ is a skew Hadamard matrix, called Paley Hadamard matrix, whose automorphism group Γ_X' obviously contains Γ_X as a subgroup. Quite surprisingly, Kantor [**16**] proved in fact that $\Gamma_X' = \Gamma_X$ for $q \equiv -1 \pmod 4$, $q \geqq 19$. For $q = 11$, $\Gamma_X'/\{I, -I\}$ is the Mathieu group M_{12} (cf. [**14**]).

COROLLARY 7.2. *Any Paley matrix is equivalent to a negacyclic C-matrix.*

Proof. Let A be the matrix of the trinomial

$$z^2 - (\epsilon + \epsilon^q)z + \epsilon^{q+1},$$

where ϵ is a primitive element in an extension field $\mathrm{GF}(q^2)$ of $\mathrm{GF}(q)$. Then, $A^{q+1} = \omega I$, where $\omega = \epsilon^{q+1}$ is a primitive root in $\mathrm{GF}(q)$ and the vectors

$$\xi_j = A^j\xi_0, j = 0, 1, \ldots, q,$$

are pairwise independent over $\mathrm{GF}(q)$ whenever ξ_0 is a nonzero vector. Taking $X = \{\xi_0, \xi_1, \ldots, \xi_q\}$, we consider the substitution (7.1), with $i = 0$. It clearly acts as a cyclic permutation on X so Q and Δ, defined in Theorem 7.1, are in this case

$$Q = \mathrm{circ}(0, 1, 0, \ldots, 0),$$
$$\Delta = \mathrm{diag}(1, 1, \ldots, 1, -1).$$

It is easily seen that $P = \Delta Q$ is in fact the generalized negacyclic permutation matrix introduced in § 4. Equation (7.2) becomes

$$PC_XP^{-1} = -C_X,$$

since $\det(A) = \omega$ is a non-square. Finally, defining $\Gamma = \mathrm{diag}(1, -1, 1, -1, \ldots)$, one has $\Gamma P = -P\Gamma$ so the matrix $C = \Gamma C_X$ satisfies $PCP^{-1} = C$ and, therefore, is a negacyclic C-matrix equivalent to C_X.

Remark. The polynomial $c(x)$ of the negacyclic Paley C-matrix is

$$c(x) = \sum_{j=0}^{q} \chi \det(\xi_0, A^j\xi_0)x^j.$$

It can be shown that the substitution $x \to x^p \pmod{(x^{q+1} + 1)}$ in the polynomial $c(x)$ corresponds to a generalized permutation on the rows and columns of C, which in fact belongs to the group $\mathrm{P\Gamma L}_2(q)$. This is in agreement with Corollary 5.5, in which it is shown that p is a multiplier of C.

Finally, we correct an error in [**11**]. As was pointed out to us by Belevitch, [**11**, Theorem 2.3] is valid only if $q + 1 \equiv 2 \pmod 4$. For $q + 1 \equiv 0 \pmod 4$, the proof breaks down. Indeed, referring to [**11**, p. 1004], we observe that in this case the $q + 1$ vectors

$$x, v(x), v^2(x), \ldots, v^{(q-1)/2}(x); w(x), vw(x), v^2w(x), \ldots, v^{(q-1)/2}w(x)$$

do not represent the $q + 1$ points of $PG(1, q)$, since we have

$$v^{(q+1)/4}(x) = -\epsilon^{-q-1}w(x).$$

The correct statement of [**11**, Theorem 2.3] is as follows.

THEOREM 7.3. *The equivalence class of Paley matrices of order* $q + 1 \equiv 2 \pmod 4$ *contains a member of the form*

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

with square symmetric cyclic submatrices A *and* B.

The proof of [**11**] is valid. A second proof is obtained by application of Corollary 7.2 and Theorem 4.3 of the present paper. Theorem 4.2 provides a contribution to what is happening for $q + 1 \equiv 0 \pmod 4$.

REFERENCES

1. E. F. Assmus, Jr., and H. F. Mattson, Jr., *On the automorphism groups of Paley-Hadamard matrices*, Combinatorial mathematics and its applications, R. C. Bose and T. A. Dowling (Ed.), (University of North Carolina Press, Chapel Hill, 1969), 98–103.
2. V. Belevitch, *Synthesis of four-wire conference networks and related problems*, Proc. symp. on modern network synthesis, Polytechnic Institute of Brooklyn (1955), 175–195.
3. ——— *Conference networks and Hadamard matrices*, Ann. Soc. Sci. Bruxelles Sér. 1 *82* (1968), 13–32.
4. E. R. Berlekamp, *Algebraic Coding Theory* (McGraw-Hill, New York, 1968).
5. E. R. Berlekamp, J. H. van Lint and J. J. Seidel, *A strongly regular graph derived from the perfect ternary Golay code* (to appear).
6. W. G. Bridges and H. J. Ryser, *Combinatorial designs and related systems*, J. Algebra *13* (1969), 432–446.
7. A. T. Butson, *Relations among generalized Hadamard matrices, relative difference sets, and maximal length linear recurring sequences*, Can. J. Math. *15* (1963), 42–48.
8. R. D. Carmichael, *Introduction to the theory of groups of finite order* (Dover, London, 1956).
9. P. Dembowski, *Finite Geometries* (Springer-Verlag, New York, 1968).
10. J. E. H. Elliott and A. T. Butson, *Relative difference sets*, Illinois J. Math. *10* (1966), 517–531.
11. J. M. Goethals and J. J. Seidel, *Orthogonal matrices with zero diagonal*, Can. J. Math. *19* (1967), 1001–1010.
12. ——— *A skew Hadamard matrix of order 36*, J. Australian Math. Soc. *11* (1970), 343–344.
13. M. Hall, Jr., *Cyclic projective planes*, Duke Math. J. *14* (1947), 1079–1090.
14. ——— *Note on the Mathieu group* M_{12}, Arch. Math. *13* (1962), 334–340.
15. ——— *Combinatorial theory* (Blaisdell, Waltham, Mass., 1967).
16. W. M. Kantor, *Automorphism groups of Hadamard matrices*, J. Combinatorial Theory *6* (1969), 279–281.

17. J. H. van Lint and J. J. Seidel, *Equilateral point sets in elliptic geometry*, Nederl. Akad. Wetensch. Proc. Ser. A *69* (1966), 335–348.
18. H. B. Mann, *Addition theorems* (Wiley, New York, 1965).
19. R. E. A. C. Paley, *On orthogonal matrices*, J. Math. and Phys. *12* (1933), 311–320.
20. D. Raghavarao, *Some aspects of weighing designs*, Ann. Math. Statist. *31* (1960), 878–884.
21. K. B. Reid and E. Brown, *Doubly regular tournaments are equivalent to skew Hadamard matrices* (to appear).
22. J. J. Seidel, *Strongly regular graphs with* (−1, 1, 0) *adjacency matrix having eigenvalue 3*, Linear Algebra and Appl. *1* (1968), 281–298.
23. ——— *Strongly regular graphs*, Recent progress in combinatorics, W. T. Tutte (Ed.), Proc. Third Waterloo Conference on Combinatorics, 185–198 (Academic Press, New York, 1969).
24. G. Szekeres, *Tournaments and Hadamard matrices*, Enseignement. Math. *15* (1969), 269–278.
25. J. Wallis, *Some* (1, −1) *Matrices*, J. Combinatorial Theory Ser. B *10* (1971), 1–11.

M.B.L.E. Research Laboratory,
Brussels, *Belgium;* (P.D. and J.M.G.)
Technological University,
Eindhoven, *Netherlands* (J.J.S.)