Can. J. Math., Vol. XXIII, No. 3, 1971, pp. 531–535

ON C-MATRICES OF ARBITRARY POWERS

RICHARD J. TURYN

A C-matrix is a square matrix of order $m + 1$ which is 0 on the main diagonal, has ± 1 entries elsewhere and satisfies $C' = \epsilon C$, $CC' = mI$. Thus, if $\epsilon = -1$, $I + C$ is an Hadamard matrix of skew type [**3**; **6**] and, if $\epsilon = 1$, $iI + C$ is a (symmetric) complex Hadamard matrix [**4**]. For $m > 1$, we must have $\epsilon = (-1)^{(m+1)/2}$. Such matrices arise from the quadratic character χ in a finite field, when m is an odd prime power, as $[\chi(a_i - a_j)]$ suitably bordered, and also from some other constructions, in particular those of skew type Hadamard matrices. (For $\epsilon = 1$ we must have $m = a^2 + b^2$, a, b integers.) Goldberg [**2**] showed that if a skew Hadamard matrix of order $m + 1$ exists then one of order $m^3 + 1$ also exists, i.e. the theorem of this paper for $\epsilon = -1$, $n = 3$. Goethals and Seidel ([**1**]) pointed out an early result of Belevitch, the theorem for $\epsilon = \pm 1$, $n = 2$. J. Wallis [**5**] pointed out that both of these results hold for $\epsilon = \pm 1$ and gave a proof of the theorem for $n = 5$ and 7. It is clear that it is sufficient to prove the theorem for n prime. In this paper we finish the theorem by proving it for all odd primes p. The construction here is a direct generalization of the ones given by Wallis; it coincides with Goldberg's for $n = 3$. As a consequence of the theorem we have some (presumably) new Hadamard matrices, and skew type Hadamard matrices. The smallest candidates for new (skew type) orders of Hadamard matrices are $15^{11} + 1$ and $15^{13} + 1$.

If we start with an arbitrary C-matrix of order $m + 1$ we may form an equivalent one with first row all $+1$, first column ϵ, except the 0 on the main diagonal. The remaining core matrix of order m, say W, satisfies $JW = WJ = 0$, $W' = \epsilon W$, $WW' = mI - J$, with J the matrix with all entries $= 1$. Conversely, given W which satisfies these conditions, we can border it and get a C-matrix. In the remainder of the paper we assume that p is an odd prime, and W a matrix satisfying the conditions above. Define a G-string to be a sequence of p symbols, each I, J or W, such that each I is followed by a J and each J preceded by an I, where the last symbol is considered to be followed by the first one for the purpose of deciding which sequences are G-strings. Any sequence of length p of symbols I, J, W, is to represent the Kronecker product G of the corresponding matrices, i.e. a matrix of order m^p. The matrix of order m^p we construct is the sum of all the G-strings.

LEMMA 1. *If G_1 and G_2 are different G-strings then there is a position in which G_1 has W and G_2 has J or vice-versa.*

Received October 14, 1970.

Proof. If all the positions which have a W in either string have a W in the other, the two strings are identical, since each must be completed uniquely from the set of W's in it by adding consecutive pairs I, J in the vacant places. Thus assume that G_1 has a W in a position (which we may write as the first) in which G_2 does not have a W. If G_2 has a J there, we are done, so assume

$$G_1 = W \times \ldots \quad \text{and}$$
$$G_2 = I \times J \times \ldots,$$

since a J must follow an I. Then the second position in G must have an I, as otherwise we are finished, and thus the third a J. We now have

$$G_1 = W \times I \times J \times \ldots \quad \text{and}$$
$$G_2 = I \times J \times \ldots,$$

so that the third position in G_2 must have an I, etc. Since each G-string has at least one W, p being odd, G_2 has a W somewhere; the smallest index for which G_1 or G_2 has a W corresponds to a J in the other.

LEMMA 2. *If G_1 and G_2 are different G-strings there is a position in which G_1 has a W and G_2 an I, or conversely.*

Proof. This follows from Lemma 1 by interchanging I and J and reading backwards.

LEMMA 3.
(1) $G' = \epsilon G$.
(2) $G_i G_j = 0$ if $G_i \neq G_j$.
(3) $G_i * G_j = 0$ if $G_i \neq G_j$, *i.e. different G_i and G_j do not have non-zero entries in the same place* (*Hadamard product*).

Proof. The first statement follows from the fact that each G-string has an odd number of W's and $W' = \epsilon W$, $I' = I$, $J' = J$. The second follows from Lemma 1 since $JW = WJ = 0$, and the third from Lemma 2 since $W * I = 0$.

We let W_p be the matrix of order m^p which corresponds to the sum of all the G-strings, so that e.g.

$$W_3 = W \times W \times W + I \times J \times W + W \times I \times J + J \times W \times I.$$

This is Goldberg's original construction but as restated by Wallis (Goldberg considered the corresponding 0,1 matrix). For the exceptional case $p = 2$ we have the Belevitch construction

$$W_2 = W \times W - I \times J + J \times I.$$

We now have $W_p' = \epsilon W_p$ and from Lemma 3 we know that $W_p W_p' = \sum G_i G_i'$, the sum taken over all G-strings.

LEMMA 4. *W_p has ± 1 entries except 0 on the main diagonal.*

Proof. From part 3 of Lemma 3 we know that all entries of W_p are 0, $+1$ or -1, and clearly W_p is zero on the main diagonal as all G_t are. We will now show that all other entries are $+1$ or -1. A pair of subscripts (row and column) for W_p consists of two p-tuples $(i_1, \ldots, i_p)$, $(j_1, \ldots, j_p)$ with $1 \leqq i_k, j_k \leqq m$. If $i_k \neq j_k$ for all k then $W \times W \times \ldots \times W$ is not zero in that entry. If $i_k = j_k$ but $i_{k-1} \neq j_{k-1}$ ($k \bmod p$) then we take the kth symbol in a G-string as I and the $(k+1)$th as J. In general, for each block of exactly t consecutive ($\bmod p$) indices such that

$$i_{k+r} = j_{k+r},\ 0 \leqq r \leqq t-1,$$

we let the kth, $(k+2)$th, $(k+4)$th, ... symbols be I, the symbols following I be J, and complete to a G-string with W in all other positions. We thus get a G-string which has a non-zero entry in the desired position.

As a corollary, we note some interesting numerical identities.

COROLLARY.

(1) $$m^p - 1 = (m-1)^p + p \sum_{k=1}^{p-1/2} \frac{m^k (m-1)^{p-2k}}{k} \binom{p-k-1}{k-1}$$

(2) $$\sum_{k \geqq 1} \binom{k}{i-k} \binom{p-k-1}{k-1} \frac{p}{k} = \binom{p}{i}$$

(3) $$\sum_{k \geqq 1} \frac{\binom{i}{i-k}\binom{p-i}{2k-i}}{\binom{p-1}{k}} = 1$$

Proof. The second statement is equivalent to the first (expand m^p as $((m-1)+1)^p$), and the third is a modification of the second, the sums being taken for $k \geqq 1$, $i \leqq 2k \leqq 2i$, for the binomial coefficients to be defined. The first statement of the corollary is a count of the non-zero entries in a row of W_p: a G-string with $k > 0$ pairs $I \times J$ in it, which starts with an I will correspond to the p G-strings obtained by translating it ($\bmod p$); all the resulting G-strings are distinct because p being prime, there can be no periodicities. Each such G-string arises in this way from k different G-strings with an initial I, i.e. there are k choices for the initial I. Each row of W has $m-1$ nonzero entries, each row of J has m. Finally, there are $\binom{p-k-1}{k-1}$ G-strings which start with I and have $k-1$ other I's: treating $I \times J$ as one symbol we have two symbols and want to use $k-1$ times $I \times J$ and $p-2k$ times W, in the remainder of the G-string. Since the count applies for any W which is zero on the main diagonal and ± 1 elsewhere, e.g. $J - I$, the statement is true for all $m > 0$, and thus all m.

LEMMA 5. $W_p W_p' = m^p I_p - J_p$ *(I_p and J_p are of order m^p).*

https://doi.org/10.4153/CJM-1971-056-0 Published online by Cambridge University Press

Proof. We have $WW' = mI - J$, $JJ' = mJ$, $II' = I$. It is therefore clear that W_pW_p' can be expressed as a linear combination of the various p-fold Kronecker products of I and J. We know that $W_pW_p' = \sum G_iG_i'$ and that $G_1 = W \times W \times \ldots \times W$ contributes $m^pI_p - J_p$ (plus other terms) to W_pW_p', and that I_p and J_p cannot arise in any other product G_iG_i'.

We now ask how any other p-fold product P of I and J, one containing at least one I and at least one J, can arise from G_iG_i'. If P contains J (I) in position j it cannot appear in a product G_iG_i' if G_i has an I (J) in position j. This is the only type of restriction there is. Thus, assume P has exactly b blocks of consecutive J's, $b > 0$, and that it has a total of c J's which are preceded by J. Then P contains b I's followed by J and $p - c - 2b$ I's followed by I; if P occurs in GG' we have

$$\begin{array}{rccc}
 & P & G & GG' \\
b: & I \times J & W \times W & (mI - J) \times (mI - J) \\
 & & \text{or} \quad I \times J & I \times mJ \\
c: & (J)J & W & mI - J \\
p - c - 2b: & I(I) & W & mI - J.
\end{array}$$

There are $\binom{b}{j}$ G-strings which have $I \times J$ pairs in j of the positions corresponding to the b $I \times J$ pairs in P, so that the coefficient of P in $\sum G_iG_i'$ is

$$(-1)^c m^{p-c-2b} \left\{ \sum_j \binom{b}{j} m^{b-j} (-1)^{b-j} m^j \right\} = 0.$$

The $(-1)^c$ factor arises from the c non-initial J's, m^{p-c-2b} arises from the non-final I's, m^j arises from the j $I \times J$ pairs and $(-1)^{b-j} m^{b-j}$ from the $b - j$ $W \times W$ pairs.

We have thus shown:

THEOREM. *If there is a C-matrix of order $m + 1$ there is a C-matrix of order $m^n + 1$ for every integer n.*

COROLLARY. *If there is a (real) Hadamard matrix of skew type of order $m + 1$ and n is odd there is an Hadamard matrix of skew type of order $m^n + 1$ and a (symmetric) complex Hadamard matrix of order $m^t + 1$, $t = 2^i n$, $i \geqq 1$.*

We note that different matrices W can be used, provided they are of the same order and the same matrix W is used consistently in each position, so that $W \times W' \times W'' + I \times J \times W'' + J \times W' \times I + W \times I \times J$ would work equally well for W_3 if W, W', W'' are cores of C-matrices of the same order. The assumption that p is a prime is used only in the calculation of the corollary and could be omitted. Thus, the theorem automatically gives us somewhat different possible constructions for composite odd n: the matrix for $n = 9$ obtained by applying the cube construction twice is not the same as the matrix W_9, and is not equivalent to it under a permutation of the nine Kronecker product coordinates.

References

1. J. M. Goethals and J. J. Seidel, *Orthogonal matrices with zero diagonal*, Can. J. Math. *19* (1967), 1001–1010.
2. K. Goldberg, *Hadamard matrices of order cube plus one*, Proc. Amer. Math. Soc. *17* (1966), 744–746.
3. Marshall Hall, Jr., *Combinatorial theory* (Blaisdell, Waltham, Mass., 1967).
4. R. Turyn, *Complex Hadamard matrices*, Combinatorial structures and their applications (Gordon and Breach, New York, 1970).
5. J. Wallis, *On integer matrices obeying certain matrix equations*, to appear in J. Combinatorial Theory.
6. J. Williamson, *Hadamard's determinant theorem and the sum of four squares*, Duke J. Math. *11* (1944), 65–81.

Raytheon Company,
Sudbury, Massachusetts