INVARIANT FACTORS OF COMBINATORIAL MATRICES

BY

MORRIS NEWMAN

ABSTRACT

The Smith normal forms of an Hadamard matrix of order $4m$ (m square-free), and of the incidence matrix of a (v, k, λ) configuration ($n=k-\lambda$ square-free $(n, \lambda) = 1$), are determined.

Introduction

In a recent article [3] it was shown that if H is a $v \times v$ Hadamard matrix where $v = 4m$ and m is odd and square-free, then the invariant factors of H are 1 (once), 2 ($2m-1$ times), $2m$ ($2m-1$ times), and $4m$ (once). Here we give a short proof of this result without the restriction that m be odd, which is unnecessary. Our results give a good deal of additional information on the possible Smith normal forms of an Hadamard matrix. We also derive some results on the invariant factors of (v, k, λ) configurations.

A good general reference on the Smith normal form and the theory of equivalence is [1]. If A is an $n \times n$ non-singular integral matrix, we denote the Smith normal form of A by

$$S(A) = \operatorname{diag}(s_1(A), s_2(A), \cdots, s_n(A)),$$

so that $s_k(A)$ is the kth invariant factor of A, $1 \leqq k \leqq n$. The transpose of A will be denoted by A^T. We quote two results; the first is proved in [2], the second is obvious.

(1) If A, B are $n \times n$ non-singular integral matrices, then $s_k(AB)$ is divisible by $s_k(A)$ and by $s_k(B)$, $1 \leqq k \leqq n$.

(2) $S(A^T) = S(A)$.

Received September 1, 1970 and in revised form January 5, 1971

Hadamard matrices

Suppose that H is a $v \times v$ Hadamard matrix ($v = 4m$), so that H has entries ± 1, and H satisfies

$$HH^T = vI.$$

Then

$$H^T = vH^{-1},$$

and so by (2),

$$S(H) = S(vH^{-1}).$$

It follows easily that if

$$S(H) = \operatorname{diag}(h_1, h_2, \cdots, h_v),$$

then

$$h_k = v/h_{v-k+1}, \quad 1 \leqq k \leqq v.$$

Thus we have that

$$S(H) = \operatorname{diag}(h_1, h_2, \cdots, h_{2m}, v/h_{2m}, v/h_{2m-1}, \cdots, v/h_1).$$

where

$$h_k \,|\, h_{k+1}, \quad 1 \leqq k \leqq 2m-1, \quad h_{2m}^2 \,|\, 4m.$$

Now suppose that m is square-free. Then $h_{2m}^2 | 4$, and so h_{2m} is either 1 or 2. Thus to determine $S(H)$ completely we need only know the rank of H if its entries are taken modulo 2. But this, clearly, is 1, since $H \equiv J \bmod 2$, where J is the $v \times v$ matrix all of whose entries are 1. Thus we have proved

THEOREM 1. *Suppose that $v = 4m$, where m is square-free, and let H be an Hadamard matrix of order v. Then the invariant factors of H are*

$$1\,(\textit{once}),\ 2\,(2m-1 \ \textit{times}),\ 2m\,(2m-1\ \textit{times}),\ 4m\,(\textit{once})$$

(v, k, λ) configurations. Now suppose that A is the incidence matrix of a (v, k, λ)-configuration: i.e., A is a $v \times v$ matrix of zeros and ones with precisely k ones in each row and column such that

$$AA^T = A^TA = nI + \lambda J,$$

where $n = k - \lambda$. Then $(v-1)\lambda = k(k-1)$ and it is of some interest to determine (if possible) the invariant factors of A. Two such configurations with corresponding incidence matrices A, B are said to be *isomorphic* if permutation matrices P, Q exist such that $B = PAQ$. The problem of deciding when two configurations are isomorphic is both difficult and important. An obvious necessary condition for this to happen is that their corresponding incidence matrices have the same invariant factors, making the Smith normal form an important tool. Another possible application of the Smith normal form might be to results on the non-existence of such configurations.

In the "projective plane" case ($\lambda = 1,\ k = n+1,\ v = n^2+n+1$) it was shown in [2] that if n is square-free then the invariant factors of A are

$$1\left(\frac{v+1}{2}\text{times}\right),\ n\left(\frac{v-3}{2}\text{times}\right),\ n(n+1)\ (\text{once}).$$

We generalize this result in what follows. We first prove

LEMMA 1. *Let* $(n,\lambda) = \Delta$. *Then*

$$S(nI + \lambda J) = \operatorname{diag}(\Delta, n, \cdots, n, nk^2/\Delta).$$

PROOF. Perform the following elementary operations on the matrix $nI + \lambda J$:

(3) Subtract row 1 from each of the other rows.

(4) Add all the columns but the first to the first column.

(5) Subtract column 2 from columns $3,\cdots,v$.

(6) Add rows $3,\cdots,v$ to row 2.

The result is the matrix

$$\begin{pmatrix} n+\lambda v & \lambda \\ 0 & n \end{pmatrix} \dotplus nI_{v-2},$$

where I_{v-2} denotes the identity matrix of order $v-2$. Now because

$$(n+\lambda v,\ \lambda,\ 0,\ n) = \Delta,$$

the 2×2 matrix is equivalent to

$$\begin{bmatrix} \Delta & 0 \\ 0 & \dfrac{n}{\Delta}(n+\lambda v) \end{bmatrix}$$

and the result follows, since $n + \lambda v = k^2$.

We also require

LEMMA 2. *Suppose that* n *is square-free. Let* $x_1, x_2, \cdots, x_r$ *be positive integers such that*

(7) $x_k \mid x_{k+1}, \quad 1 \leqq k \leqq r-1, \; x_r \mid n,$

(8) $x_1 x_2 \cdots x_r \; = \; n^t.$

Then

$$x_1 = 1, \; 1 \leqq i \leqq r-t; \; x_j = n, \; r-t+1 \leqq j \leqq r.$$

PROOF. Let p be any prime dividing n. Let e_p be the least value of k such that $p \mid x_k$, $1 \leqq k \leqq r$. Then, because the x_k are square-free and satisfy (7), the exact power of p dividing $x_1 x_2 \cdots x_r$ is p^{r-e_p+1}. But (8) implies that this is also p^t. It follows that $e_p = r-t+1$, so that e_p is independent of p. Applying this result for all primes p dividing n we deduce the result.

Let A be the incidence matrix of a (v,k,λ) configuration. We go on now to analyse $S(A)$. Write

$$S(A) = \operatorname{diag}(\alpha_1, \alpha_2, \cdots, \alpha_v).$$

Then by (1) and the previous lemma,

$$\alpha_1 \mid \Delta, \; \alpha_k \mid n, \; 2 \leqq k \leqq v-1, \; \alpha_v \mid nk^2/\Delta.$$

But the fact that $AJ = JA = kJ$ easily implies that $k \mid \alpha_v$. For if $A = US(A)V$, U, V unimodular, then

$$J\,US(A)V = JA = kJ,$$

and since V is unimodular,

$$J\,US(A) \equiv 0 \bmod k.$$

Since $\alpha_k \mid \alpha_v$, $1 \leqq k \leqq v$, it follows that

$$\alpha_v JU \equiv 0 \bmod k.$$

Again, since U is unimodular, it follows that $\alpha_v J \equiv 0 \bmod k$,

so that

$$\alpha_v \equiv 0 \bmod k,$$

as desired. Thus we can write

$$\alpha_v = k\alpha_v', \quad \alpha_v' \mid nk/\Delta.$$

Now note that

$$\alpha_1 \alpha_2 \cdots \alpha_v = n^{(v-1)/2} k$$

so that

$$\alpha_1 \alpha_2 \cdots \alpha_{v-1} \alpha_v' = n^{(v-1)/2}. \tag{9}$$

We now assume that

$$\Delta = 1.$$

Then because $\alpha'_v \mid nk$, $\alpha'_v \mid n^{(v-1)/2}$, and $(n,k) = 1$, we get that $\alpha'_v \mid n$. Similarly, since $\alpha_{v-1} \mid k\alpha'_v$ and $\alpha_{v-1} \mid n$, we get that $\alpha_{v-1} \mid \alpha'_v$. Thus we have that

$$\alpha_k \mid \alpha_{k+1}, \; 1 \leqq k \leqq v-2, \; \alpha_{v-1} \mid \alpha'_v, \; \alpha'_v \mid n. \tag{10}$$

Now assume that n is square-free. Then (9), (10), and Lemma 2 together imply that

$$\alpha_i = 1, \; 1 \leqq i \leqq \frac{v+1}{2}; \; \alpha_j = n, \; \frac{v+3}{2} \leqq j \leqq v-1; \; \alpha'_v = n.$$

Summarizing, we have proved

THEOREM. 2. *Suppose that A is the incidence matrix of a(v,k,λ) configuration, where $n = k-\lambda$ is square-free and $(n,\lambda) = 1$. Then the invariant factors of A are*

$$1\left(\frac{v+1}{2}\text{ times}\right), \; n\left(\frac{v-3}{2}\text{ times}\right), \; nk\,(\text{once}).$$

REFERENCES

1. C. C. MACDUFFEE, *The theory of matrices*, Reprint of first edition, Chelsea, New York, 1964.

2. M. NEWMAN, *On the Smith normal form*, To appear.

3. W. D. WALLIS AND J. WALLIS, *Equivalence of Hadamard matrices*, Israel J. Math. 7 (1969), 122–128.

NATIONAL BUREAU OF STANDARDS,
WASHINGTON, D. C. 20234