Can. J. Math., Vol. XXVIII, No. 6, 1976, pp. 1216–1223

CRITERIA FOR A HADAMARD MATRIX TO BE SKEW-EQUIVALENT

JUDITH Q. LONGYEAR

Introduction. A matrix H of order $n = 4t$ with all entries from the set $\{1, -1\}$ is *Hadamard* if $HH^t = 4tI$. The set of Hadamard matrices is $\mathscr{H}$. A matrix $H \in \mathscr{H}$ is of *type I* or is *skew-Hadamard* if $H = S - I$ where $S^t = -S$ (some authors also use $H = S + I$). The set of type I members of $\mathscr{H}$ is $\mathscr{T}$. A matrix P is a *signed permutation matrix* if each row and each column has exactly one non-zero entry, and that entry is from the set $\{1, -1\}$. The set of signed permutation matrices is $\mathscr{P}$, containing the two subsets $\mathscr{A}$, those with all non negative entries, and $\mathscr{M}$, those with zeros off the main diagonal. If H and K are in $\mathscr{H}$, then H is *equivalent* to K, or $H \equiv K$, whenever there exist P and $Q \in \mathscr{P}$ with $PH = KQ$. The set of members of H equivalent to members of $\mathscr{T}$ is $\mathscr{E}$. Note that if $H \equiv K \in \mathscr{E}$ then $H \in \mathscr{E}$.

For each $\mathscr{X} = \mathscr{H}, \mathscr{P}, \mathscr{T}, \mathscr{E}, \mathscr{A}, \mathscr{M}$, the symbol $\mathscr{X}(n)$ refers to the subset of $\mathscr{X}$ whose members all have order n.

The entry in the ith row and jth column of any matrix B is denoted by $B(i, j)$. Thus if $P \in \mathscr{P}(n)$ then there is a permutation σ on n letters for which $P(i, j) = \delta_{i,\sigma(j)}(-1)^{p(j)}$, where p is some mapping from $\{1, 2, \ldots, n\}$ to $\{0, 1\}$.

If $H \in \mathscr{H}$, then H is *skew-normal* if $H(i, 1) = -1$ for all i and $H(1, j) = 1$ for all $j > 1$. Every equivalence class of $\mathscr{H}$ contains a skew-normal representative.

The first criterion.

CRITERION 1. *For any $H \in \mathscr{H}$, $H \in \mathscr{E}$ if and only if there exists $P \in \mathscr{P}$ such that $H + 2P \in \mathscr{H}$.*

Proof. If $H + 2P \in \mathscr{H}$ then $nI = (H + 2P)^t(H + 2P) = H^tH + 2H^tP + 2P^tH + 4I = (n + 4)I + 2((P^tH)^t + P^tH)$. Thus $-2 = -2I(i, i) = ((P^tH)^t + (P^tH))(i, i) = 2(P^tH)(i, i)$, so $P^tH(i, i) = -1$. Also $0 = -2I(i, j)$ for $i \neq j$, so

$$(P^tH)(i, j) = -(P^tH)^t(i, j) = -P^tH(j, i)$$

and therefore $P^tH \in \mathscr{T}$.

If $H \in \mathscr{E}$ then there is some $K \in \mathscr{T}$ and some P and Q in $\mathscr{P}$ with $PHQ^t = K$. Since $K \in \mathscr{T}(n)$, $K = S - I$ with $S^t = -S$, thus $K + 2I$ satisfies

$$(K + 2I)^t(K + 2I) = K^tK + 2(K^t + K) + 4I = nI.$$

Received December 15, 1975 and in revised form, August 17, 1976.

Thus $PHQ^t + 2I \in \mathscr{H}$, whence

$$P^t(PHQ^t + 2I)Q = H + 2P^tQ \in \mathscr{H}.$$

COROLLARY. *$H \in \mathscr{E}$ if and only if there is some $P \in \mathscr{P}$ such that $P^tH \in \mathscr{E}$.*

LEMMA 2. *If H is skew-normal and $P^tH \in \mathscr{T}$ then the following are equivalent:*
1) *P^tH is skew-normal.*
2) *$P(1, 1) = 1$.*
3) *$p(i) = 0$ for all i.*

Proof. 1) $\Rightarrow$ 2) and 3). If P^tH is skew-normal then

$$-1 = (P^tH)(i, 1) = \sum_{k=1}^{n} P(k, i)H(k, 1)$$

$$= - \sum_{k=1}^{n} \delta_{k\sigma i}(-1)^{p(i)} = -(-1)^{p(i)}.$$

Thus $p(i) = 1$ for all i, so that $2P$ only adds to H in $H + 2P$. Since every position of the first row of H is positive except the first, $\sigma 1 = 1$, so that $P(1, 1) = 1$.

2) $\Rightarrow$ 3). If $P(1, 1) = 1$, denote row i of $H + 2P$ by $(H + 2P)(i)$, then for any $i \neq 1$,

$$(H + 2P)(1) = 1, 1, \ldots, 1$$
$$(H + 2P)(i) = H(i, 1), H(i, 2), \ldots, -H(i, \sigma^{-1}i), \ldots, H(i, n).$$

Since $H + 2P \in \mathscr{H}$,

$$\begin{aligned}(H + 2P)(1) \circ (H + 2P)(i) &= 0 \\ &= H(i, 1) + \ldots + H(i, \sigma^{-1}i - 1) - H(i, \sigma^{-1}i) + H(i, \sigma^{-1}i + 1) \\ &\quad + \ldots + H(i, n) \\ &= H(1)H(i) + 2H(i, 1) - 2H(i, \sigma^{-1}i) \\ &= 0 + 2(H(i, 1) - H(i, \sigma^{-1}i)) \\ &= 2(-1 - H(i, \sigma^{-1}i)).\end{aligned}$$

Thus $H(i, \sigma^{-1}i) = -1$, so $P(i, \sigma^{-1}i) = +1$.

3) $\Rightarrow$ 1). If $p(j) = 0$ for all j, then clearly $P(1, 1) = 1$ since H is skew-normal. Moreover $P^tH(i, 1) = \sum_{k=1}^{n} \delta_{k\sigma(i)}H(k, 1) = H(\sigma i, 1) = -1$.

Since $P^tH \in \mathscr{T}$, $P^tH(1, j) = -P^tH(j, i) = +1$ for $j \neq 1$, so P^tH is skew-normal.

Remark. Since $H \in \mathscr{E}$ if and only if H is equivalent to a skew-normal $K \in \mathscr{T}$, it would be most useful to be able to say that a skew-normal $H \in \mathscr{E}$ if and only if there is some $P \in \mathscr{A}$ with $H + 2P \in \mathscr{H}$, since this would lower the number of computations by a factor of $n2^n$. This is false, however, since the order 20 matrix N discussed below is a counterexample. There are no smaller counterexamples.

The second criterion. We now restrict the discussion to the case where $P \in \mathscr{A}$. Although the necessity for checking each row as first row is actually quite tedious in practice, this necessity imposes no theoretical restriction, since whenever $H + 2P \in \mathscr{H}$ for skew-normal H, the non-zero value of P in the first column must be positive. If this occurs in row i, let QH be skew normal and have row i of H for row 1. Then $QH + 2QP = Q(H + 2P) \in \mathscr{H}$ and $QP(1, 1) = 1$.

Definition 1. For $H \in \mathscr{H}$ and skew-normal we define two (v, k, λ)-designs. Let the order of H be $n = 4t$. The treatments of $E(H)$ are the rows $H_2, H_3, \ldots, H_n$, the blocks are the columns $\{2, 3, \ldots, n\}$, and row H_i is incident with j whenever $H(i, j) = +1$. Then $E(H)$ is a $(4t - 1, 2t - 1, t - 1)$-design, as is well known (see, for example, Hall [**4**, p. 103]). The treatments of $M(H)$ are the columns $\{2, \ldots, n\}$, the blocks the rows $H_2, \ldots, H_n$, with row i incident with j whenever $H(i, j) = -1$. $M(H)$ is the misère design of H (with respect to the fixed row 1 and column 1) and is easily seen to be a $(4t - 1, 2t, t)$-design. To avoid confusion, we write the blocks of $M(H)$ as $M_2, \ldots, M_n$ or $M_2(H), \ldots, M_n(H)$ if necessary.

Definition 2. Let D be any (b, v, r, k, λ) design with $k > \lambda$. Then D is said to have a (t, s, i) *cut down* if each treatment may be removed from t blocks in such a way that the new smaller blocks form a $(b, v, r - t, k - s, \lambda - i)$ design. Clearly, if a $(1, 1, i)$ cut down exists for D, then D is a (v, k, λ)-design. Since both $\lambda(v - 1) = k(k - 1)$ and $(\lambda - i)(v - 1) = (k - 1)(k - 2)$ must be satisfied, we see that $v = 4\lambda - 1$, that $k = 2\lambda$, and that $i = 1$. If a $(4t - 1, 2t, t)$-design D has a $(1, 1, 1)$ cut down we shall say that D *cuts down*, and denote the obtained $(4t - 1, 2t - 1, t - 1)$-design by D^*.

LEMMA 1. *If $H \in \mathscr{T}$ and H is skew-normal then $M(H)$ cuts down.*

Proof. The treatment i can be removed from M_i since $H = S - I$. Moreover, since $S^t = -S$, the treatment $i \in M_j$ if and only if $j \notin M_i$, so exactly one occurrence of the pair $\{i, j\}$ is destroyed by doing this.

LEMMA 2. *If $H \in \mathscr{H}$, if H is skew-normal, and if $H + 2P \in \mathscr{H}$ then $M(H)$ cuts down.*

Proof. Since H is skew-normal, $P(1, 1) = 1$ and so $P \in \mathscr{A}$. If $P(i, j) = \delta_{i,\sigma(j)}$, then $H(\sigma j, j) = -1$, so j may be removed from $M_{\sigma j}$. Moreover, $0 = (H + 2P)_{\sigma i} \circ (H + 2P)_{\sigma j} = H_{\sigma j} \circ H_{\sigma j} - 2H(\sigma i, i)H(\sigma i, j) - 2H(\sigma j, i)H(\sigma j, j) = 0 - 2\{-H(\sigma i, j) - H(\sigma j, i)\}$, whenever $i \neq j$. Thus $H(\sigma i, j) = -H(\sigma j, i)$ so that $i \in M_{\sigma j}$ if and only if $j \notin M_{\sigma i}$.

CRITERION 2. *$M(H)$ cuts down if and only if there is some $P \in \mathscr{A}$ for which $H + 2P \in \mathscr{H}$.*

COROLLARY. *$H \in \mathscr{E}$ if and only if H has some row such that $M(H)$ with respect to this row cuts down.*

LEMMA 3. *If $M = M(H)$ cuts down to M^*, then M^* and $E = E(H)$ are isomorphic designs.*

Proof. Let $E_2, \ldots, E_n$ be the treatments of E; in particular, E_2 is row 2 of H. Define the mapping f from M^* to E by $f(i) = E_{\sigma i}$ and $f(M^*_{\sigma j}) = j$. Clearly, f is a bijection taking the treatments of M^* to those of E and the blocks of M^* to those of E. To see that f preserves incidence, $i \notin M_{\sigma i}^*$, but i was removed from $M_{\sigma i}$ to get $M_{\sigma i}^*$, thus $H(\sigma i, i) = -1$, whence $f(i) = E_{\sigma i} \notin i = f(M_{\sigma i}^*)$ in $E(H)$. Also, if $i \neq j$ and $i \in M_{\sigma i}^*$ then $j \notin M_{\sigma i}^*$, so $H(\sigma i, j) = +1$ whence $f(i) = E_{\sigma i} \in j$ in $E(H)$. Since f preserves incidence, E and M^* are isomorphic as designs.

Definition 3. For any (v, k, λ)-design D the *derived design* $\delta D(B)$ is the $(v - 1, k, k - 1, \lambda, \lambda - 1)$-design consisting of the treatments in the fixed block B and the blocks $B_i' = B_i \cap B$ for all blocks $B_i \neq B$ of D. Thus for each row in H, the designs $\delta M^*(M_{\sigma i}^*)$ and $\delta E(i)$ are isomorphic $(4t - 2, 2t - 1, 2t - 1, t - 1, t - 2)$-designs.

CRITERION 3. *$H \in \mathscr{E}$ if and only if for some choice of normalizing row, $\delta E(2)$ has an incidence preserving injection to $\delta M(Mi)$, for some i.*

A negative application of the third criterion. In this section we will use Criterion 3 to show that several matrices of order 16 are not in $\mathscr{E}$, so that $\mathscr{E} \neq \mathscr{H}$. M. Hall, Jr. has shown in [**1**] that there are exactly 5 equivalence classes of matrices in $\mathscr{H}(16)$. He calls these 'group', '3/4 group', '1/2 group', 'first 3/8 group' and 'second 3/8 group.' He also shows that the automorphism group fixing the first row on each of these is transitive with respect to columns; thus, we will succeed in finding a cut down in the design for the first row if such a cut down exists for any design of the matrix.

'Group' belongs to the equivalence class containing the matrix H obtained from the elementary abelian group $G = \langle a, b, c, d \rangle$. The difference set $D = \{a, b, c, d, ab, cd\}$ in G generates a $(16, 6, 2)$-design with blocks $Dx = \{ax, bx, cx, dx, abx, cdx\}$ as x runs over G. A Hadamard matrix H is obtained by taking $H(x, y) = +1$ if and only if $y \in Bx$. To normalize H, eliminate the identity from all rows by replacing H_x with $-H_x$ whenever $x \in D$. Then replace columns a, b, c, d, ab, cd by $-a, -b, -c, -d, -ab, -cd$. If this skew-normal matrix is called K, then we again treat $K_a, \ldots, K_{abcd}$ as sets, in the same way that $H_1, \ldots, H_{abcd}$ represent sets in G.

$$K_x = \begin{cases} H_x \Delta H_1 & \text{if } x \in D = B_1 \\ H_x \Delta H_1^{\,c} & \text{if } x \notin D, \end{cases}$$

where Δ is symmetric difference and ^{c} is the complement in the set $G\backslash\{1\}$.

Thus $\delta E(2)$ is the design with blocks:

$X = c, d, cd$	d, ac, acd
a, c, ac	a, cd, acd
a, d, ad	c, ad, acd
$Y = c, d, cd$	d, ac, acd
a, c, ac	a, cd, acd
a, d, ad	ac, ad, cd
c, ad, acd	ac, ad, cd

All the blocks of $\delta E(2)$ come in pairs like X, Y, so if f were to inject $\delta E(2)$ into some $\delta M(i)$ then for each such pair, $|fX \cap fY| \geqq 3$, but there are no triples of blocks in M that meet in more than two elements. Since no such f is possible, 'group' cannot be a skew-equivalent matrix.

A positive application and a warning. Although it is well known [**2**] that all order 12 Hadamard matrices are equivalent, it is not always simple to determine just how. Consider the matrix H in Figure 1. With respect to this normalization, E and M have the following blocks:

E	M
a. $8t$ (016)	l. ($\bar{5}$ 6 7 8 9 t)
b. 27 (019)	e. 5 7 9 (23$\bar{4}$)
c. 47 (036)	h. $\bar{6}$ 9 t (024)
d. $2t$ (035)	a. 5 8 9 ($\bar{0}$14)
e. 48 (059)	i. $\bar{7}$ 6 9 (013)
l. (2 4 7 8 t)	c. 5 7 t (01$\bar{2}$)
g. 78 (135)	b. 5 6 t ($\bar{1}$34)
h. 28 (369)	j. 7 8 $\bar{t}$ (034)
i. 24 (156)	g. 8 $\bar{9}$ t (123)
j. $7t$ (569)	d. 5 6 8 (02$\bar{3}$)
k. $4t$ (139)	k. 6 7 $\bar{8}$ (124)

If δE is taken with respect to block 5, then the numbers in parentheses are removed, leaving ten 2-element blocks. The mapping $(2, 4, 7, 8, t) \to (6, 7, t, 9, 8)$ injects this simple design into $\delta M(l)$, taking block a to block a, etc. Moreover, it induces (0, 1, 6, 9, 3, 5) $\to$ (5, 4, 1, 3, 0, 2) which injects E into M, leaving the overscored numbers to be removed for a cut down of M.

It should be emphasized that not all injections of $\delta E(l)$ into some δM necessarily extend to E. For instance, it would have been more natural to take $\delta E(a)$ and $\delta M(l)$, and again an injection exists, namely $(0, 1, 6, 8, t) \to$

(9, 7, t, 6, 8); but in trying to extend this, one is faced with mapping

$$\{2, 7, 9\} \to \{2, 3, 4\}$$
$$\{3, 4, 7\} \to \{0, 2, 4\}$$
$$\{2, 3, 5\} \to \{0, 1, 4\}$$

which is impossible since the first three form a triangle on 2, 3, 7 but the second three are copunctual on 4.

	∞	1	1	2	3	4	5	6	7	8	9	t
∞	—	1	1	1	1	1	1	1	1	1	1	1
0	—	1	1	1	1	1	—	—	—	—	—	—
1	—	1	1	—	—	—	—	1	—	1	—	1
2	—	—	1	—	1	—	1	—	1	1	—	—
3	—	—	—	1	1	—	—	1	1	—	—	1
4	—	—	—	1	—	1	1	—	—	1	—	1
5	—	—	—	—	1	1	—	1	—	1	1	—
6	—	1	—	1	—	—	—	—	1	1	1	—
7	—	—	1	1	—	—	1	1	—	—	1	—
8	—	1	—	—	—	1	1	1	1	—	—	—
9	—	—	1	—	—	1	—	—	1	—	1	1
t	—	1	—	—	1	—	1	—	—	—	1	1

H

FIGURE 1

The remaining order 16 matrices. Since Hall [**1**] has shown that the group of automorphisms fixing row 1 is transitive on the columns for all order 16 Hadamard matrices, we need only consider the designs obtained by using row 1 for normalization. The matrix 'group' was discussed in the section 'a negative application of criterion 3', and shown not to be skew-equivalent. The agreement of 'group', '3/4 group' and '1/2 group' on all first 8 rows and 8 columns shows that when each is normalized by row 1 and δE taken with respect to row 2, the same design results, namely one in which the blocks come in identical pairs. As before, any injection f of such a pair X, Y to any $\delta M(i)$ requires $|fX \cap fY \cap \text{row}(i)| \geqq 3$. Thus the rows $\{2, 3, \ldots, i-1, i+1, \ldots, 16\}$ must be paired j, j^* so that $|\text{row } i \cap \text{row } j \cap \text{row } j^*| \geqq 3$. In M (group), each three rows intersect in 2 elements. In M (3/4 group), if $i \geqq 13$ then some pair $\{j, j^*\}$ has, say, $j \geqq 13$, but no pair of rows from $\{13, 14, 15, 16\}$ intersects any third row in more than 2 elements. If $i < 13$, then some pair $\{j, j^*\}$ have both $j, j^* < 13$, but then i, j, j^* are as in M (group), so again, it is impossible. Thus '3/4 group' $\notin \mathscr{E}$. In M (1/2 group), row 2 would need to be in some triple $\{i, j, j^*\}$, but row 2 meets each pair of other rows in 0 or 2 elements.

By contrast, in both M (3/8 group)'s, there is an abundance of the necessary triples, and both cut down as follows.

1st 3/8 group (1) (11, 13, 6, 7, 10, 4, 15, 16, 2, 8, 9, 3, 14, 2, 5)
2nd 3/8 group (1) (9, 14, 7, 15, 4, 12, 5, 11, 6, 16, 2, 13, 3, 10, 8).

Thus 11 is removed from block 2 and 13 from block 3 in M (1st 3/8 group).

These cut downs were obtained using criterion 2 on a computer, and used about three minutes each.

The order 20 matrices. In [**3**], Hall showed that there are exactly three equivalence classes of order 20 matrices, which he calls Q, P, N. The class Q contains the matrix obtained from the non-zero quadratic residues modulo 19, which is type I. The class N is new and is skew-equivalent. If N, as given on page 40 of [**3**] is normalized by row 5, then $M(N)$ cuts down by

(15, 9, 17, 2) (1) (12, 20, 7, 11, 14, 3, 8, 6, 10, 5, 19, 19, 16, 4, 13).

This cut down was obtained by the same computer program, taking about 20 minutes. It also reported that normalizations by rows 1, 2, 3, 4 have no cut downs. The same program, in 80 minutes, returned that $P \notin \mathscr{E}$, but there is no direct proof.

The class P contains both the Paley and Williamson matrices of order 20.

On difference sets.

Definition. A (v, k, λ)-*difference set* is a set of k of the residues mod v, say $D = \{x_1, x_2, \ldots, x_k\}$, such that every non-zero residue occurs exactly λ times as $x_i - x_j$. The blocks $D + i = \{x_1 + i, x_2 + i, \ldots, x_k + i\}$ for $i = 0, 1, \ldots, v - 1$ form a (v, k, λ)-design on $\{0, 1, \ldots, v - 1\}$, and the complementary blocks form a $(v, v - k, v - 2k + \lambda)$-design. Such a difference set D is called a *Hadamard difference set* if $v = 4t - 1$, $k = 2t - 1$, $\lambda = t - 1$, and is called a *skew-Hadamard difference set* if $D \cup \{0\}$ is a $(4t - 1, 2t, t)$-difference set.

Example. The difference set $D = \{1, 2, 4\}$ is a skew-Hadamard difference set. The misère difference set, $S = \{0, 3, 5, 6\}$ thus has the cyclic cut down $S(i)^* = (S + i)\backslash\{i\}$. It also has many non-cyclic cut downs such as

S	3	5	6	(0)	$S + 4$	0	2	(3)	4
$S + 1$	(4)	6	0	1	$S + 5$	1	3	4	(5)
$S + 2$	5	(0)	1	2	$S + 6$	(2)	4	5	6
$S + 3$	6	(1)	2	3					

Interestingly, if g is the mapping which assigns i to $S + g(i)$ in this cut down, then the mapping $i \to g(i)$ induces an injection from M^* to M so that the leftover treatments form a cyclic cutdown of M. It would be particularly nice to know if such is always the case, that is if whenever $i \to S + g(i)$ is a cut-down of M, then g acting on the elements of M^* induces a mapping from M^*

to M which leaves over a cyclic cutdown. This is not known. E. C. Johnson [**5**] has shown that if any Hadamard difference set extends by adding 0, then it must have been the quadratic residue set.

In combination with the truth of the statement about g, this would say that no Hadamard matrix constructed from a difference set was in $\mathscr{E}$, except the quadratic residue matrices, which are all in $\mathscr{T}$.

The author would like to thank John McKay for introducing her to the problem and for a most stimulating correspondence during the course of the work.

References

1. M. Hall, Jr. *Hadamard matrices of order* 16, J.P.L. Research summary No. 36-10, *1* (1961), 21–26.
2. ——— *Note on the Matthieu group* M_{12}, Arch. Math. *13* (1962), 334–340.
3. ——— *Hadamard matrices of order* 20, J.P.L. Technical Report No. 32-761 (1965), 1–41.
4. ——— *Combinatorial theory* (Ginn-Blaisdell, Waltham, Mass., 1967).
5. E. C. Johnson, *Skew-Hadamard abelian group difference sets*, J. Algebra *1* (1964), 388–402.

Wayne State University,
Detroit, Michigan