PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 32, Number 1, March 1972

HADAMARD DESIGNS

EDWARD SPENCE[1]

ABSTRACT. It has already been shown, using a combinatorial argument, that a Hadamard design with each letter repeated once and only once can exist for 2, 4 and 8 letters only. In this paper the same result is proved by a different method which utilizes the underlying algebraic structure of such a Hadamard design.

A *Hadamard design* is a square array of letters which commute in pairs, and to which signs are attached, so that the scalar product of any two distinct rows, considered as vectors, is zero. In [1] Hadamard designs on n letters (or n-letter designs) were studied. These are Hadamard designs with n distinct letters where each letter occurs once and only once in each row and column. It was shown that such a design could exist for $n=2$, 4 or 8 only.

Clearly, if H is an n-letter design, we may suppose that the sign associated with each element in the first row and column is positive (by changing the sign of each element in a row or column, if necessary) and that the first row and column are identical (interchange rows and columns, if necessary). Suppose therefore that H satisfies the above conditions on the letters $a_1, a_2, \cdots, a_n$ and write $-H$ for the design obtained by changing the sign of every letter in H. Then we have the following

LEMMA 1.

$$\begin{bmatrix} H & -H \\ -H & H \end{bmatrix} \tag{1}$$

is the multiplication table of a loop L of order $2n$ with elements $a_1, a_2, \cdots, a_n, -a_1, -a_2, \cdots, -a_n$.

PROOF. Since each letter $a_1, a_2, \cdots, a_n$ occurs once and only once in each row and column of H, the array (1) is certainly a latin square. Also,

Received by the editors March 9, 1971.

AMS 1970 *subject classifications*. Primary 05B20; Secondary 20N05.

Key words and phrases. Hadamard design, Cayley numbers.

[1] This paper was written while the author held a Visiting Lectureship at the University of Illinois, Urbana, Illinois 61801.

since its first row and column are identical, it has an identity, and hence is a loop.

In the case $n=2$ it is easy to verify that L is a cyclic group of order 4 and so for the rest of the paper we assume $n>2$.

Suppose that a_1 is the identity of L and write $a_1=1$. It is immediate from (1) that $(-1)a_i=-a_i=a_i(-1)$ and $(-1)^2=1$, and hence $\{1, -1\}\subseteq Z$, the center of L. Also, from the orthogonality of distinct rows of H, we have the following condition:

(2) if $a_i \neq \pm a_j$, $a_k \neq \pm a_l$, then $a_ia_k = a_ja_l \Rightarrow a_ja_k = -(a_ia_l)$.

Consequences of (2).

I. $Z=\{1, -1\}$. For $1a_i=a_i1$ and if $a_i\neq\pm 1$, (2) implies that $a_i^2=-1$. Thus if $a_ix=xa_i$ for *all* $x\in L$, we must have for some $x\neq\pm 1$, $\pm a_i$ (such exists since $2n\geqq 6$), $a_i^2=-x^2=1$, i.e. $a_i=\pm 1$ which proves the assertion.

II. *If* x, $y\in L$, *then* $xy\neq yx\Rightarrow xy=-yx$. Since $xy\neq yx$ we may suppose

$$x \neq \pm 1, y \neq \pm 1 \quad \text{and} \quad x \neq \pm y. \tag{3}$$

Given x, $y\in L$ there exists a unique $t\in L$ such that $xy=tx$, whence, since $x\neq\pm t$, as is easily shown from (3), $ty=-x^2=1$. However $(-y)y=1$ and cancellation yields $t=-y$, i.e. $xy=-yx$.

III. *Any two elements of L generate a subgroup.* To prove this all we need verify are the following associative laws

(a) $x(xy)=x^2\cdot y$,

(b) $(xy)x=x(yx)$,

(c) $(yx)x=y\cdot x^2$.

Since these are trivial when $x=\pm 1$ or $y=\pm 1$ or $x=\pm y$ we may assume that none of these equalities is satisfied. Write $x(xy)=1\cdot z$ so that, by (2), $xy=-xz=x(-z)$. Cancellation gives $y=-z$, i.e. $z=-y$ so that $x(xy)=-y=x^2y$ which proves (a). (b) and (c) are proved using II and (a) above.

IV. *If* $xy\neq yx$ *then* x *and* y *generate a quaternion group.* For $xy\neq yx\Rightarrow xy=-yx$ by II, and the result follows using III.

V. *If* $x(yz)=(xy)z$ *then* x, y *and* z *generate a subgroup.* Suppose that

(4) u, v, $w\notin Z$ and all lie in different cosets of Z in L.

There exists a unique $t\in L$ such that $uv=tw=v(-u)$, and hence (2) yields $vw=-t(-u)=-ut$, and $u(vw)=u(-ut)=-u^2t$ (by III)$=t$ since $u\notin Z$. But $(uv)w=(tw)w=-t$, i.e. $(uv)w=-u(vw)$ if u, v, w satisfy (4). Thus if $(xy)z=x(yz)$, then at least one of x, y, $z\in Z$ or $x=\pm y$ or $x=\pm z$ or $y=\pm z$. It follows from III that x, y and z generate a subgroup.

Collecting all this information together, we have

THEOREM 2. *The loop L defined in Lemma* 1 ($n>2$) *satisfies the following* *conditions*:

(i) *The center Z has order two and elements* 1, -1 *where* $(-1)^2=1$, $1\neq -1$.

(ii) *If $x\notin Z$, then $x^2=-1$.*

(iii) *If $xy\neq yx$ then $xy=-yx$ and x, y generate a quaternion group.*

(iv) *If $x(yz)=(xy)z$, then x, y, z generate a subgroup.*

However, it is known that a loop satisfying the conditions of Theorem 2 must either be a quaternion group or a Cayley loop [**2**, Theorem 7.2 and the remarks following]. Since a quaternion group has order 8 and a Cayley loop has order 16, it is immediate that $n=4$ or 8.

In the opposite direction, it is straightforward to verify that the designs obtained from these loops as in (1) are n-letter designs. Consequently,

THEOREM 3. *There are n-letter designs only for* $n=2$, 4 *or* 8.

REFERENCES

1. Jennifer Wallis, *Hadamard designs*, Bull. Austral. Math. Soc. **2** (1970), 45–54. MR **41** #3304.

2. R. H. Bruck, *A survey of binary systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete, N.F., Band 20, Springer-Verlag, Berlin, 1958. MR **20** #76.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GLASGOW, GLASGOW, W.2., SCOTLAND