Hadamard matrices

1 Introduction

A *Hadamard matrix* is an $n \times n$ real matrix H which satisfies $HH^\top = nI$.

The name derives from a theorem of Hadamard:

Theorem 1 *Let $X = (x_{ij})$ be an $n \times n$ real matrix whose entries satisfy $|x_{ij}| \leq 1$ for all i, j. Then $|\det(X)| \leq n^{n/2}$. Equality holds if and only if X is a Hadamard matrix.*

This is a nice example of a theorem which seems to lack any reasonable approach (we are asked to optimise a highly non-linear function over a multidimensional region), yet when looked at the right way it is very easy. Let $x_1 \ldots, x_n$ be the rows of X. Then by simple Euclidean geometry, $|\det(X)|$ is the volume of the parallelepiped with sides $x_1, \ldots, x_n$; so

$$|\det(X)| \leq |x_1| \cdots |x_n|,$$

where $|x_i|$ is the Euclidean length of x_i; equality holds if and only if $x_1, \ldots, x_n$ are mutually perpendicular. By hypothesis,

$$|x_i| = \left(x_{i1}^2 + \cdots + x_{in}^2\right)^{1/2} \leq n^{1/2},$$

with equality if and only if $|x_{ij}| = 1$ for all j. The result follows, since a Hadamard matrix is just a real matrix whose entries all have modulus 1 and whose rows are mutually perpendicular.

For which orders n do Hadamard matrices exist? There is a well-known necessary condition:

Theorem 2 *If a Hadamard matrix of order n exists, then $n = 1$ or 2 or $n \equiv 0 \pmod 4$.*

To see this, we observe first that changing the sign of every entry in a column of a Hadamard matrix gives another Hadamard matrix. So changing the signs of all columns for which the entry in the first row is $-$, we my assume that all entries in the first row are $+$. (We abbreviate $+1$ and -1 to $+$ and $-$ respectively.)

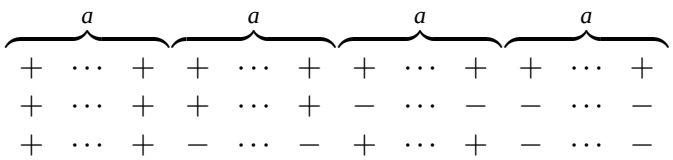

Figure 1: Three rows of a Hadamard matrix

Now, since every other row is orthogonal to the first, we see that each further row has m entries $+$ and m entries $-$, where $n = 2m$. Moreover, if $n > 2$, the first three rows are now as in Figure 1, with $n = 4a$.

It is conjectured that there is a Hadamard matrix of every order divisible by 4 (in other words, the above necessary condition is sufficient). The smallest multiple of 4 for which no matrix has been constructed is currently 428. We will see a few constructions in the following sections. See [2] for more.

2 Some constructions

The constructions given here by no means exhaust those known, but suffice to give a Hadamard matrix of each admissible order less than 52.

2.1 Sylvester matrices

The simplest construction of new Hadamard matrices from old is the Kronecker (or tensor) product. In general, if $A = (a_{ij})$ and $B = (b_{kl})$ are matrices of size $m \times n$ and $p \times q$ respectively, the *Kronecker product* $A \otimes B$ is the $mp \times nq$ matrix made up of $p \times q$ blocks, where the (i, j) block is $a_{ij}B$. Then we have the following result:

Theorem 3 *The Kronecker product of Hadamard matrices is a Hadamard matrix.*

The *Sylvester matrix* $S(k)$ of order 2^k is the iterated Kronecker product of k copies of the Hadamard matrix $\begin{pmatrix} + & + \\ + & - \end{pmatrix}$ of order 2. By the preceding theorem,

it is a Hadamard matrix. For example,

$$S(2) = \begin{pmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{pmatrix}.$$

The Sylvester matrices have many other descriptions. For example, if we index the rows and columns by all k-tuples over the binary field GF(2), we can take the entry in row $a = (a_1, \ldots, a_k)$ and column $b = (b_1, \ldots, b_k)$ to be $(-1)^{a \cdot b}$, where $a \cdot b = \sum a_i b_i$ is the usual dot product of vectors. We can regard the index $(a_1, \ldots, a_k)$ as being the base 2 representation of an integer $\sum a_i 2^{k-i}$ in the range $[0, 2^k - 1]$. Alternatively, $S(k)$ is the character table of the elementary abelian group of order 2^k.

2.2 Paley matrices

Let q be a prime power congruent to 3 mod 4. Recall that in the field GF(q), half the non-zero elements are quadratic residues or squares, and half are quadratic non-residues or non-squares; and in particular, $+1$ is a square and -1 is a non-square. The *quadratic character* of GF(q) is the function χ given by

$$\chi(x) = \begin{cases} 0 & \text{if } x = 0; \\ +1 & \text{if } x \text{ is a quadratic residue;} \\ \text{-1} & \text{if } x \text{ is a quadratic non-residue.} \end{cases}$$

Now let A be the matrix whose rows and columns are indexed by elements of GF(q), and having (x,y) entry $a_{xy} = \chi(y-x)$. The matrix A is skew-symmetric, with zero diagonal and ± 1 elsewhere, and satisfies the equation

$$A^2 = J - qI.$$

The matrix A is the adjacency matrix of the *Paley tournament*.

Now if we replace the diagonal zeros by -1s and border A with a row and column of $+1$s, we obtain a Hadamard matrix of order $q+1$ called a *Paley matrix*.

2.3 Order 36

The smallest order not settled by the above constructions is 36. Here are two completely different methods for constructing Hadamard matrices of order 36.

Construction from Latin squares Let $L = (l_{ij})$ be a Latin square of order 6: that is, a 6×6 array with entries $1, \ldots, 6$ such that each entry occurs exactly once in each row or column of the array. Now let H be a matrix with rows and columns indexed by the 36 cells of the array: its entry in the position corresponding to a pair (c, c') of distinct cells is defined to be $+1$ if c and c' lie in the same row, or in the same column, or have the same entry; all other entries (including the diagonal ones) are -1. Then H is a Hadamard matrix.

Steiner triple systems Let S be a Steiner triple system of order 15: that is, S is a set of "triples" or 3-element subsets of $\{1, \ldots, 15\}$ such that any two distinct elements of this set are contained in a unique triple. There are 35 triples, and two distinct triples have at most one point in common. Now let A be a matrix with rows and columns indexed by the triples, with entry in position (t, t') being -1 if t and t' meet in a single point; all other entries (including the diagonal ones)are $+1$. Now let H be obtained by bordering A by a row and column of $+1$s. Then H is a Hadamard matrix.

3 Equivalence of Hadamard matrices

The Sylvester and Paley matrices of orders 4 and 8 are equivalent – indeed there is essentially a unique matrix of each of these orders. For all larger orders for which both types exist (that is, $n = p + 1$, where p is a Mersenne prime), they are not equivalent. We proceed to make the sense of "equivalence" of Hadamard matrices precise.

There are several operations on Hadamard matrices which preserve the Hadamard property:

(a) permuting rows, and changing the sign of some rows;

(b) permuting columns, and changing the sign of some columns;

(c) transposition.

We call two Hadamard matrices H_1 and H_2 *equivalent* if one can be obtained from the other by operations of types (a) and (b); that is, if $H_2 = P^{-1}H_1Q$, where P and Q are *monomial matrices* (having just one non-zero element in each row or column) with non-zero entries ± 1.

Accordingly, the *automorphism group* of a Hadamard matrix H is the group consisting of all pairs (P, Q) of monomial matrices with non-zero entries ± 1

satisfying $P^{-1}HQ = H$; the group operation is given by $(P_1, Q_1) \circ (P_2, Q_2) = (P_1P_2, Q_1Q_2)$.

Note that there is always an automorphism $(-I, -I)$, which lies in the centre of the automorphism group.

This analysis is due to Marshall Hall [1]. He showed that there is, up to equivalence, a unique Hadamard matrix H of order 12. Moreover, if $G = \mathrm{Aut}(H)$, and Z is the central subgroup generated by $(-I, -I)$, then G/Z is isomorphic to the sporadic simple group M_{12} (the Mathieu group), and has its two 5-transitive representations on the rows and columns. Moreover, the map $(P, Q) \mapsto (Q, P)$ gives an outer automorphism of M_{12} interchanging these two representations.

4 Designs from Hadamard matrices

If we choose a row of a Hadamard matrix of order $n = 4a$, and normalise it to have entries $+1$, then each of the remaining $4a-1$ rows has $2a$ entries $+1$ and $2a$ entries -1. If we take the set of columns as points, and the sets of columns carrying $+1$s and -1s in all but the chosen row as blocks, we obtain a 3-$(4a, 2a, a-1)$ design. Different choices of row may or may not give isomorphic designs. The Hadamard matrix can be recovered uniquely (up to equivalence) from the design. The design obtained from the Sylvester matrix is the point-hyperplane design of affine space over $\mathrm{GF}(2)$.

Designs with parameters 3-$(4a, 2a, a-1)$ are necessarily affine, and any affine 3-design has this form. They are called *Hadamard* 3*-designs*.

If we choose a row and a column of a Hadamard matrix of order $n = 4a$, we can normalise both to consist of $+1$s. Then take the columns other than the distinguished one as points; for each row other than the distinguished one, take the set of columns where its $+1$ entries occur as the blocks. We obtain a square 2-$(4a-1, 2a-1, a-1)$ design. Different choices of row and column may or may not give isomorphic designs. The Hadamard matrix can be recovered uniquely (up to equivalence) from the design. The design obtained from the Sylvester matrix is the point-hyperplane design of projective space over $\mathrm{GF}(2)$.

Square designs with parameters 2-$(4a-1, 2a-1, a-1)$ are called *Hadamard* 2*-designs*.

For example, in the Paley matrix of order $q+1$, one row and column is already normalised to consist of $+1$s; the resulting design can be described as follows: the point set is $\mathrm{GF}(q)$; one block is the set S of non-zero squares (quadratic residues) in $\mathrm{GF}(q)$, and the others are its translates $S + x = \{s + x : s \in S\}$, for $x \in \mathrm{GF}(q)$.

This is the *Paley design*.

Yet another design can be obtained as follows. Let H be a Hadamard matrix of order $4a$. The points of the design are the columns of H; for each pair of rows of H, there are two blocks of size $2a$, the set of columns where the entries in the rows agree, and the set where they disagree. This is a 3-$(4a, 2a, 2a(a-1))$ design. Equivalent matrices give the same design. Remarkably it turns out that the design is a 4-design if and only if $a = 3$, in which case it is even a 5-design (specifically the 5-$(12, 6, 1)$ Steiner system, whose automorphism group is the Mathieu group M_{12} which we met above).

5 Symmetric matrices with constant row sum

If a Hadamard matrix H is symmetric with constant row sum, then its order is a square, say $4m^2$, and the row sum is either $2m$ or $-2m$. If we replace the entries -1 in the matrix by 0, we obtain the incidence matrix of a square 2-$(4m^2, 2m^2 \pm m, m^2 \pm m)$ design.

Any Sylvester matrix of square order is equivalent to a symmetric matrix with constant row sum, and thus gives rise to such designs; these can be constructed using quadratic forms on a vector space over GF(2).

The Hadamard matrices of order 36 constructed above from Latin squares are also of this form.

References

[1] M. Hall, Jr., Note on the Mathieu group M_{12}, *Arch. Math.* **13** (1962), 334–340.

[2] J. Seberry and M. Yamada, Hadamard matrices, sequences and block designs, pp. 431–560 in *Contemporary Design Theory: A Collection of Surveys* (ed. J. H. Dinitz and D. R. Stinson), Wiley, New York, 1992.

Peter J. Cameron

July 31, 2002