Constructing Hadamard matrices via orthogonal designs

Jennifer Seberry

University of Wollongong, jennie@uow.edu.au

Follow this and additional works at: https://ro.uow.edu.au/infopapers

Part of the Physical Sciences and Mathematics Commons

Recommended Citation

https://ro.uow.edu.au/infopapers/1027
Constructing Hadamard matrices via orthogonal designs

Abstract
Orthogonal designs were created to give a unifying approach to the construction of Hadamard matrices. Recent work has been concerned with Hadamard matrices of order $2^{tpq}$, where $t \leq 5$ and one of $p$ and $q$ is small. This paper obtains many new constructions for Hadamard matrices of such orders and works toward a more general construction theory.

Disciplines
Physical Sciences and Mathematics

Publication Details
Abstract. Orthogonal designs were created to give a unifying approach to the construction of Hadamard matrices. Recent work has been concerned with Hadamard matrices of order $2^tq$, where $t \leq 5$ and one of $p$ and $q$ is small. This paper obtains many new constructions for Hadamard matrices of such orders and works toward a more general construction theory.

1. Introduction

Let $A = [a_{ij}]$ be a matrix of order $n$ with $a_{ij} \in \{0,1,-1\}$. $A$ is called a weighing matrix of weight $p$ and order $n$ if $AA^T = A^TA = pI_n$, where $I_n$ denotes the identity matrix of order $n$. Such a matrix is denoted by $W(n,p)$. If squaring all its entries gives the incidence matrix of an SBIBD, then $W$ is called a balanced weighing matrix.

An orthogonal design (OD) of order $n$ and type $(s_1,s_2,\ldots,s_t)$ on the commuting variables $(\pm x_1,\ldots,\pm x_k,0)$ is a square matrix of order $n$ with entries $\pm x_k$ or $0$ and with $|x_k|$ occurring $s_k$ times in each row and column such that the rows are pairwise orthogonal.

In other words,

$$AA^T = (s_1x_1^2 + \ldots + s_kx_k^2)I_n.$$

This is denoted by $OD(n;s_1,s_2,\ldots,s_t)$.

An Hadamard matrix, $A = [a_{ij}]$, is either an OD(n,n) or a W(n,n), that is, it is a square matrix of order $n$ with entries $a_{ij} \in \{1,-1\}$ which satisfies

$$AA^T = A^TA = nI_n.$$

2. Constructions

LEMMA 1. Suppose there is an $OD(p+1;1,p)$ and a conference matrix of order $p+3$. Then there is an Hadamard matrix of order $2(p+1)(p+2)$ (divisible by 8).

Proof. The conference matrix has symmetric core $N$ such that

$$(N+I)^2 + (N-I)^2 = 2(p+3)I - 2J.$$

Use the OD to form an $OD(2(p+1);1,1,p,p)$. Then replace its variables by the suitable matrices of order $p+2$: $I, J - 2I, N+I, N - I$. Now

$$J^2 + (J - 2I)^2 + p(N+I)^2 + p(N-I)^2$$

$$= (p+2)I + 4I + (p-2)J + 2p(p+3)I - 2pJ$$

$$= 2(p+1)(p+2)I,$$

and we have the result.
LEMMA 2. Suppose there exists an $OD(2(p+1); 2, 2p)$ and a symmetric Hadamard matrix of order $p+3$. Then there is an Hadamard matrix of order $4(p+1)(p+2)$.

Proof. The symmetric Hadamard matrix has symmetric core $B$ of order $p+2$ satisfying $$B^2 = (p+3)I - J.$$ Use the $OD(2(p+1); 2, 2p)$ to form an $OD(4(p+1); 2, 2p+2)$. Replace the variables by the suitable matrices of order $p+2$: $J, J - 2I, B$. Now

$$2J^2 + 2(J - 2I)^2 + 4pB^2 = 2(p+2)J + 2(4I + (p - 2)J) + 4p((p + 3)I - J) = 4(p + 1)(p + 2)I,$$

and we have the result.

Example. A symmetric conference matrix of order 102 exists. Hence an $OD(204; 2, 202)$ exists. A symmetric Hadamard matrix of order 104 exists. Hence we have an Hadamard matrix of order 851.103 (which was previously known) even though an Hadamard matrix of order 4.103 is not yet known.

LEMMA 3. Suppose there is an $OD(3r+1; 1, 3r)$ and a symmetric Hadamard matrix of order $4r+4$ with core $B$ of order $4r+3$. Then there is an Hadamard matrix of order $4(3r+1)(4r+3)$ (divisible by 16).

Proof. The symmetric core satisfies

$$B^2 = (4r+4)I - J.$$ Use the $OD(3r+1; 1, 3r)$ to form an $OD(4(3r+1); 1, 12r+1)$. Replace the variables by the suitable matrices of order $4r+3$: $J, J - 2I, B$. Now

$$J^2 + 2(J - 2I)^2 + (12r+1)B^2 = (4r+3)J + 2(4I + (4r - 1)J) + (12r+1)((4r+4)I - J) = 4(3r+1)(4r+3)I,$$

and we have the result.

Example 1. A small interesting example is for $r = 13$ which gives an Hadamard matrix of order $440$.55 = $16 \times 275$. An Hadamard matrix of order $4 \times 275$ is already known.

Example 2. An Hadamard matrix of order 4.103 is not yet known but an $OD(76; 1, 75)$ exists and a symmetric Hadamard matrix of order 104. So there is an Hadamard matrix of order 16.19.103. The Hadamard matrix of order 16.19.103 is known but matrices are not yet known for orders 4 . 19 . 103 or 8 . 19 . 103.

LEMMA 4. Let $v$ be a prime, and $Q$ be a cyclic $(1, -1)$ incidence matrix of a $(v,k,\lambda)$. Suppose an $OD(s(t+1); s, st)$ exists. Then there exists an Hadamard matrix of order $s(t+1)v$ or $2s(t+1)v$ according as $v = 3(mod 4)$ or $1(mod 4)$.

Proof. $Q$ satisfies

$$QQ^T = 4(k-\lambda)I + (v-4(k-\lambda))J = 4(k-\lambda)I + J.$$ Since $v$ is prime, there exists a back circulant $BR$ ($jv = 3 (mod 4)$) which satisfies

$$(BR)^2 = (v+1)I - J$$ (a)
Thus we use the suitable matrices:

(a) \( Q, BR \) in the OD \((s (t+1);s, st)\) for \( v = 3 \mod (4) \) and note

\[
sQ^2 + st (BR)^2 = 4s(k-\lambda) + stt + st(v+1) - stt = sv(v+1)\; ;
\]

(b) \( Q, (X+1)R, (X-1)R \) in the OD \((2s (t+1);2s, st, st)\) for \( v = 1 \mod (4) \) and note

\[
2sQ^2 + st (XR+R)^2 + st (XR-R)^1 = 2sv(v+1)\; .
\]

This gives the result.

We can find more results using the back circulant incidence matrices, \( Q, \) of \((v, k, \lambda)\) designs, \( v \) prime, which satisfy

\[
Q^2 = 4(k-\lambda)I + tI, \ \text{where} \ t = v - 4(k-\lambda), \ (**)
\]

the circulant \((1,1)-\)incidence matrices \( B \) or \( X + I, X - I \) of the \((v,\sqrt{v} (v-1), v/2(v-3))\) difference set or \( 2 - (v/2 (v-1))/2; (v/2 (v-3)) \) supplementary difference sets, according as \( v \equiv 3 \mod (4) \) or \( v \equiv 1 \mod (4) \) and which satisfy

\[
BB^T = (v+1)I - J, v \equiv 3 \mod (4) \ \ (***)
\]

and

\[
(X + I)^2 + (X - I)^2 = 2(v+1)I - 2J, X^T = X, v \equiv 1 \mod (4) \ \ (***)
\]

In most cases the power of the theorem is limited by the knowledge of the existence of orthogonal designs.
THEOREM 5 Let \( v \) be a prime. Let \( Q \) be the back-circulant \((1,-1)\) incidence matrix of a 
\((v,k,\lambda)\) design \((k=\sqrt{v(\pm 1)})\), \( t \) as above. Suppose there exists an 
\( OD(4n; a, b, 4n - a - b) \). Then

(i) for \( v \equiv 3 \pmod{4} \) there exist Hadamard matrices of order \( 4nv \) when 
\( a(v + 1) + b(t + 1) = 4n \);
(ii) for \( v \equiv 1 \pmod{4} \) there exist Hadamard matrices of order \( 8nv \) when 
\( a(v + 1) + b(t + 1) = 4n \).

Proof. Use the suitable matrices \( Q, J, B \), in (i) and \( Q, J, X - I \), in the 
\( OD(8n; 2a, 2b, 4n - a - b, 4n - a - b) \) in (ii).

Order 13 is a special case for there is a back circulant \((1, 1)\) matrix \( Q \) of a \((13, 4, 1)\) design. So that we have

COROLLARY 6. Suppose there exists an \( OD(4t; 2t, t, t) \) design. Then there exists 
an Hadamard matrix of order \( 4t \). Such an \( OD \) exists for infinitely many \( t \).

Proof. Replace the variables of the \( OD(4t; 2t, t, t) \) by \( Q, X + I, X - I \).

Example. Let \( v = 31 \) and \( Q \) be obtained from the \((31, 6, 1)\) design so \( Q^2 = 20I + 11J \).

Now suppose an \( OD(76; 1, 2, 73) \) exists, then, using the suitable matrices \( Q, J, B \), we 
get an Hadamard matrix of order 4.19.31.

Using the \( OD(56; 1, 2, 53) \) and the suitable matrices \( J, Q, B \), we obtain the Hadamard 
matrix of order 8.7.31.

Many more results could follow. We tabulate some of the possibilities:

<table>
<thead>
<tr>
<th>( OD ) that needs to exist</th>
<th>Known or N.E.?</th>
<th>( Q, J, B )</th>
<th>( Q, J, B )</th>
<th>( Q, J, B )</th>
<th>( Q, J, B )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( OD(56; 1, 2, 53) )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
</tr>
<tr>
<td>( OD(76; 1, 2, 73) )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
</tr>
<tr>
<td>( OD(68; 1, 3, 64) )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
</tr>
<tr>
<td>( OD(108; 1, 3, 104) )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
</tr>
<tr>
<td>( OD(80; 1, 4, 73) )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
</tr>
<tr>
<td>( OD(140; 1, 4, 135) )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
</tr>
<tr>
<td>( OD(100; 2, 3, 95) )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
</tr>
<tr>
<td>( OD(120; 2, 3, 115) )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
</tr>
<tr>
<td>( OD(124; 2, 3, 117) )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
</tr>
<tr>
<td>( OD(184; 2, 3, 177) )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
</tr>
<tr>
<td>( OD(144; 3, 4, 137) )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
</tr>
<tr>
<td>( OD(164; 3, 4, 157) )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
<td>( Q, J, B )</td>
</tr>
</tbody>
</table>

References
