A Proper n-Dimensional Orthogonal Design of Order 8 on 8 Indeterminates

Warwick de Launey[1]

Cryptomathematics Research
c/o DVR2, 'A' Block, New Wing
Victoria Barracks
St Kilda Road
Victoria 3004
AUSTRALIA

Abstract. Let $x_1, x_2, \ldots, x_r$ be commuting indeterminates over the integers. We say a $\nu \times \nu \times \cdots \times \nu$ n-dimensional matrix is a proper n-dimensional orthogonal design of order ν and type $(s_1, s_2, \ldots, s_r)$ (written $OD^n(s_1, s_2, \ldots, s_r)$) on the indeterminates $x_1, x_2, \ldots, x_r$ if every 2-dimensional axis-normal submatrix is an $OD(s_1, s_2, \ldots, s_r)$ of order ν on the indeterminates $x_1, x_2, \ldots, x_r$. Constructions for proper $OD^n(1^2)$ of order and $OD^n(1^4)$ of order 4 are given in J. Seberry (1980) and J. Hammer and J. Seberry (1979,1981a), respectively. This paper contains simple constructions for proper $OD^n(1^2)$, $OD^n(1^4)$, and $OD^n(1^8)$ of orders 2, 4 and 8, respectively. Prior to this paper no proper higher dimensional OD on more than 4 indeterminates was known

1. Introduction

By a *proper n-dimensional orthogonal design of type* $(s_1, s_2, \ldots, s_r)$ *and order* ν *on the indeterminates* $x_1, x_2, \ldots, x_r$ (written $OD^n(s_1, s_2, \ldots, s_r)$), we mean an n-dimensional array $(a_{i_1 i_2 \ldots i_n})$ of order ν (here $1 \le i_j \le \nu$ and $1 \le j \le n$) where every $\nu \times \nu$ 2-dimensional sub-array obtained by fixing all but two indices is an $OD(s_1, s_2, \ldots, s_r)$ on the indeterminates $x_1, x_2, \ldots, x_r$. We will call these 2-dimensional sub-arrays 2-sections.

Since P. J. Shlichta's pioneering paper (1971), a number of authors, including S. Agaian (1981a,1981b), W. de Launey (1987,1989), W. de Launey and K. J. Horadam (1990), J. Hammer and J. Seberry (1979,1981a,1981b), J. Seberry (1980) and Yang Yi Xian (1986a,b,c) have studied higher dimensional Hadamard matrices, weighing matrices, and orthogonal designs. In particular, J.Seberry (1980) constructed proper $OD^n(1^2)$ of order 2, and J. Hammer and J. Seberry (1979,1981a) constructed proper $OD^n(1^4)$ of order 4. This paper contains simple constructions for proper $OD^n(1^2)$, $OD^n(1^4)$, and $OD^n(1^8)$ of orders 2, 4 and 8, respectively.

[1] Warwick de Launey is with the Defence Science and Technology Organization, Electronic Research Laboratory, Communications Division.

2. The Designs

2.1 Definition: Let D be an $OD(s_1, s_2, \ldots, s_r)$ (where $s_i > 0$) of order ν on the indeterminates $x_1, x_2, \ldots, x_r$, and let $x = \{x_1, x_2, \ldots, x_r\}$. Also, let H be an abelian group, and suppose that D may be indexed over H so that, for some maps $f: H \times H \to \{1, -1\}$ and $g: H \to X \cup \{0\}$,

(i) $D = (f(h_1, h_2)g(h_1 + h_2))$

(ii) for all $k \in H$, the design $(f(h_1, h_2)g(k + h_1 + h_2))$ is an orthogonal design.

Then we say D *is transversable over* H. Also, we say D is *transversable* if there is some group H over which D is transversable.

2.2 Example: Certain $OD(1^2)$, $OD(1^4)$, and $OD(1^8)$ are shown below with co-ordinatisations, which satisfy Definiton 2.1(i), over the respective groups Z_2^t, $t = 2, 3$. (The group $Z_2 = \{0, 1\}$ is written additively). The columns are indexed by h_1 and the rows are indexed by h_2. For example $g(00) = a$ and $f(011, 101) = -1$.

00	a	b	c	d
01	b	$-a$	$-d$	c
10	c	d	$-a$	$-b$
11	d	$-c$	b	$-a$
	00	01	10	11

000	a	b	c	d	e	f	g	h
001	b	$-a$	$-d$	c	$-f$	e	h	$-g$
010	c	d	$-a$	$-b$	$-g$	$-h$	e	f
011	d	$-c$	b	$-a$	$-h$	g	$-f$	e
100	e	f	g	h	$-a$	$-b$	$-c$	$-d$
101	f	$-e$	h	$-g$	b	$-a$	d	$-c$
110	g	$-h$	$-e$	f	c	$-d$	$-a$	b
111	h	g	$-f$	$-e$	d	c	$-b$	$-a$
	000	001	010	011	100	101	110	111

2.3 Lemma.

(i) *If the order of an OD D is the same as the order of X, then D is transversable if and only if there exists some group H and some maps $f: H \times H \to \{1, -1\}$ and $g: H \to X \cup \{0\}$ for which condition (i) of Definition 2.1 holds.*

(ii) *All Hadamard matrices are transversable over any abelian group of the same order.*

(iii) *If E is a Hadamard matrix of order t and D is a transversable $OD(s_1, s_2, \ldots, s_r)$ of order ν, then the direct product design $E \times D$ is transversable.*

Proof:

(i) The forward implication is immediate. Now suppose $D = (f(h_1, h_2)g(h_1 + h_2))(h_1, h_2 \in H)$ is an $OD(1^\nu)$ of order ν, and that $k \in H$; then $E_k = (f(h_1 + h_2)g(k + h_1 + h_2)) = (f(h_1, h_2)g(\pi(h_1 + h_2)))$ where π is a permutation on H. Hence, for all $k \in H$, E_k can be obtained from D by relabelling indeterminates, and E_k is therefore an $OD(1^\nu)$.

(ii) Given $E = (e_{ij})$ an Hadamard matrix of order ν, let $H = \{a_1, a_2, \ldots, a_\nu\}$ be an abelian group of order ν, and define $f: H \times H \to \{-1, +1\}$ so that $f(a_j, a_i) = e_{ij}$ and $g: H \to \{-1, +1\}$ so that, for all $h \in H$, $g(h) = 1$. Then $E = (f(h_1, h_2)g(h_1 + h_2))$ and part (ii) of Definition 2.1 is trivially satisfied because $g(k + h) = g(h)$ for all $h, k \in H$.

(iii) This is left to the interested reader.

It happens that all the $OD(1^2)$, $OD(1^4)$, and $OD(1^8)$ of the respective orders 2,4, and 8 (see J. Wallis (1970) for a discussion of these designs) satisfy Lemma 2.3(i) for the respective groups $Z_2^t = 1, 2, 3$; so they are all transversable. In particular, the designs shown in Example 2.2 are transversable.

2.4 Theorem. *Let $n \geq 2$ be an integer. Let H be a finite abelian group, let $X = \{x_1, x_2, \ldots, x_r\}$ be a set of commuting indeterminates, and let D_{ij} ($n \geq i > j \geq 1$) be $OD(s_1, s_2, \ldots, s_r)$ (where $s_i > 0$) of order ν on the indeterminates in X. Let $f_{ij}: H \times H \to \{1, -1\}$ ($n \geq 1 > j \geq 1$) and $g: H \to X \cup \{0\}$ be maps, and suppose $D_{ij} = (f_{ij}(h_1, h_2)g(h_1 + h_2))$ are all transversable over H (ie. for all $k \in H$, $E_{ijk} = (f_{ij}(h_1, h_2)g(k + h_1 + h_2))$ is an $OD(s_1, s_2, \ldots, s_{,r})$). For all $h_1, h_2, \ldots, h_n \in H$, put*

$$f(h_1, h_2, \ldots, h_n) = \prod_{n \geq i > j \geq 1} f_{ij}(h_i, h_j), \tag{2.1}$$

and let D be the n-dimensional design of order H where

$$D = (f(h_1, h_2, \ldots, h_n)g(h_1 + h_2 + \cdots + h_n)).$$

Then D is a proper $OD(s_1, s_2, \ldots, s_n)$ on the indeterminates in X.

Proof: Let i and j be integers such that $n \geq i > j \geq 1$. Let $A(h_1, \ldots, \hat{h}_j, \ldots, h_n)$ be the product of all the terms in (2.1) which do not depend on h_j, and let $B(h_1, \ldots, \hat{h}_i, \ldots, h_n)$ be the product of the terms in (2.1) which depend on h_j but not h_i; then

$$f(h_1, \ldots, h_j, \ldots, h_j, \ldots, h_n) = \\ A(h_1, \ldots, \hat{h}_j, \ldots, h_n)B(h_1, \ldots, \hat{h}_i, \ldots, h_n)f(h_i, h_j),$$

where $A(h_1, \ldots, \hat{h}_j, \ldots, h_n)$ and $B(h_1, \ldots, \hat{h}_j, \ldots, h_n)$ are independent of h_j and h_i, respectively. Note that the range of $A(h_1, \ldots, \hat{h}_j, \ldots, h_n)$ and $B(h_1, \ldots, \hat{h}_i, \ldots, h_n)$ is $\{-1, +1\}$; so any 2-section of D which is indexed by h_i and h_j is equivalent to a design of the form $(f_{ij}(h_i, h_j)\, g(k + h_i + h_j))$ where $k \in H$; so, by Definition 2.1, every section of D is an $OD(s_1, s_2, \ldots, s_r)$ on the indeterminates $x_1, x_2, \ldots, x_r$.

2.5 Example: We apply the theorem to the three transversable $OD(1^4)$ below. We use the indexing described for the $OD(1^4)$ in Example 2.2.

$$\begin{array}{rrrr} a & b & c & d \\ b & -a & -d & c \\ c & d & -a & -b \\ d & -c & b & -a \end{array} \qquad \begin{array}{rrrr} a & b & c & d \\ b & -a & d & -c \\ c & -d & -a & b \\ d & c & -b & -a \end{array} \qquad \begin{array}{rrrr} -a & b & c & d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & -a \end{array}$$

D_{21} $\qquad$ D_{31} $\qquad$ D_{32}

The following four 2-sections make up a proper $OD^3(1^4)$ of order 4.

$$\begin{array}{rrrr} -a & -b & -c & -d \\ b & -a & -d & c \\ c & d & -a & -b \\ d & -c & b & -a \end{array} \qquad \begin{array}{rrrr} b & -a & d & -c \\ a & b & -c & -d \\ -d & c & b & -a \\ c & d & a & b \end{array}$$

$h_3 = 00$ $\qquad$ $h_3 = 01$

$$\begin{array}{rrrr} c & -d & -a & b \\ d & c & b & a \\ a & -b & c & -d \\ -b & -a & d & c \end{array} \qquad \begin{array}{rrrr} d & c & -b & -a \\ -c & d & -a & b \\ b & a & d & c \\ a & -b & -c & d \end{array}$$

$h_3 = 10$ $\qquad$ $h_3 = 11$

2.6 Example: If we apply the theorem with $n = 3$ and $D_{2l} = D_{3l} = D_{32}$ equal to the $OD(1^8)$ given in Example 2.2, we obtain the $OD^3(1^8)$ with the following h_3-axis normal sections. (The rows are indexed by h_2 and columns by h_1; so the $(010, 101, 001)$th entry is $-e$ and the $(101, 010, 011)$th entry is e.)

$$\begin{array}{rrrrrrrr} a & b & c & d & e & f & g & h \\ b & -a & -c & d & -f & e & h & -g \\ c & d & -a & -b & -g & -h & e & f \\ d & -c & b & -a & -h & g & -f & e \\ e & f & g & h & -a & -b & -c & -d \\ f & -e & h & -g & b & -a & d & -c \\ g & -h & -e & f & c & -d & -a & b \\ h & g & -f & -e & d & c & -b & -a \end{array} \qquad \begin{array}{rrrrrrrr} b & -a & -d & c & -f & e & h & -g \\ -a & -b & -c & -d & -e & -f & -g & -h \\ d & -c & b & -a & h & -g & f & -e \\ -c & -d & a & b & -g & -h & e & f \\ f & -e & -h & g & b & -a & -d & c \\ -e & -f & g & h & a & b & -c & -d \\ -h & -g & -f & -e & d & c & b & a \\ g & -h & e & -f & -c & d & -a & b \end{array}$$

$h_3 = 000$ $\qquad$ $h_3 = 001$

$$\begin{array}{cccccccc}
c & d & -a & -b & -g & -h & e & f \\
-d & c & -b & a & -h & g & -f & e \\
-a & -b & -c & -d & -e & -f & -g & -h \\
b & -a & -d & c & f & -e & -h & g \\
g & h & -e & -f & c & d & -a & -b \\
h & -g & -f & e & -d & c & b & -a \\
-e & f & -g & h & a & -b & c & -d \\
-f & -e & -h & -g & b & a & d & c
\end{array}$$

$h_3 = 010$

$$\begin{array}{cccccccc}
d & -c & b & -a & -h & g & -f & e \\
c & d & -a & -b & g & h & -e & -f \\
-b & a & d & -c & -f & e & h & -g \\
-a & -b & -c & -d & -e & -f & -g & -h \\
h & -g & f & -e & d & -c & b & -a \\
-g & -h & -e & -f & c & d & a & b \\
f & e & -h & -g & -b & = a & d & c \\
-e & f & g & -h & a & -b & -c & d
\end{array}$$

$h_3 = 011$

$$\begin{array}{cccccccc}
e & f & g & h & -a & -b & -c & -d \\
-f & e & h & -g & -b & a & d & -c \\
-g & -h & e & f & -c & -d & a & b \\
-h & g & -f & e & -d & c & -b & a \\
-a & -b & -c & -d & -e & -f & -g & -h \\
b & -a & d & -c & -f & e & -h & g \\
c & -d & -a & b & -g & h & e & -f \\
d & c & -b & -a & -h & -g & f & e
\end{array}$$

$h_3 = 100$

$$\begin{array}{cccccccc}
f & -e & h & -g & b & -a & d & -c \\
e & f & -g & -h & -a & -b & c & d \\
-h & g & f & -e & d & -c & -b & a \\
g & h & e & f & -c & -d & -a & -b \\
-b & a & -d & c & f & -e & h & -g \\
-a & -b & -c & -d & -e & -f & -g & -h \\
-d & -c & b & a & -h & -g & f & e \\
c & -d & -a & b & g & -h & -e & f
\end{array}$$

$h_3 = 101$

$$\begin{array}{cccccccc}
g & -h & -e & f & c & -d & -a & b \\
h & g & f & e & -d & -c & -b & -a \\
e & -f & g & -h & -a & b & -c & d \\
-f & -e & h & g & b & a & -d & -c \\
-c & d & a & -b & g & -h & -e & f \\
d & c & -b & -a & h & g & -f & -e \\
-a & -b & -c & -d & -e & -f & -g & -h \\
-b & a & -d & c & -f & e & -h & g
\end{array}$$

$h_3 = 110$

$$\begin{array}{cccccccc}
h & g & -f & -e & d & c & -b & -a \\
-g & h & -e & f & c & -d & a & -b \\
f & e & h & g & -b & -a & -d & -c \\
e & -f & -g & h & -a & b & c & -d \\
-d & -c & b & a & h & g & -f & -e \\
-c & d & a & -b & -g & h & e & -f \\
b & -a & d & -c & f & -e & h & -g \\
-a & -b & -c & -d & -e & -f & -g & -h
\end{array}$$

$h_3 = 111$

2.7 Corollary. *Suppose there exists an Hadamard matrix of order t; then there exist proper $OD^n(t^2)$, $OD^n(t^4)$, and $OD^n(t^8)$ of the respective orders 2t, 4t, and 8t.*

Proof: The result follows from Lemma 2.3 (i), (ii), and (iii) and Theorem 2.4.

References

1. S. S. Agaian (1981a), *On three-dimensional Hadamard matrices of Williamson type, (Russian - Armenian summary)*, Akad. Nauk. Armyan. SSR Dokl. **72**, No. **3**, 131–134.
2. S. S. Agaian (1981b), *A new method for constructing Hadamard matrices and the solution of the Shlichta problem*, Sixth Hungarian Coll. Comb. **6-11**, 2–3.
3. W. de Launey (1987), $(0, G)$*-Designs and Applications*, Ph.d. thesis, University of Sydney.
4. W. de Launey (1989), *On the construction of n-dimensional designs from 2-dimensional designs*, Australasian Journal of Combinatorics **1**, 67–81.
5. W. de Launey and KJ. Horadam (1990), *An extended difference set construction from higher dimensional designs*, Designs, Codes and Crypography. (to appear).
6. J. Hammer and J. Seberry (1979), *Higher dimensional orthogonal designs and Hadamard matrices II*, Proceedings of the Ninth Manitoba Conference on Numerical Mathematics, Congressus Numerantium **XXVII**, 23–29.
7. J. Hammer and J. Seberry (1981a), *Higher dimensional orthogonal designs and applications*, IEEE Transactions on Information Theory **IT-27**, **6**, 772–779.
8. J. Hammer and J. Seberry (1981b), *Higher dimensional orthogonal designs and Hadamard matrices*, Congressus Numerantium **31**, 95–108.
9. J. Seberry (1980), *Higher dimensional orthogonal designs and Hadamard matrices*, Combinatorics VII: Proceedings of the Seventh Australasian Conference on Combinatorial Mathematics, Lecture Notes in Mathematics, Springer-Verlag **829**, 220–223.
10. J. Wallis (1970), *Hadamard designs*, Bull. Austral. Math. Soc. **2**, No. **1**, 45–54.
11. Yang Yi Xian (1986a), *The proofs of some conjectures on higher dimensional Hadamard matrices,*, Kexue Tongbao **31(24)**, 16–21.
12. Yang Yi Xian (1986b), *On the classification of 4-dimensional 2 order Hadamard matrices.* (preprint).
13. Yang Yi Xian (1986c), *On n-dimensional 2 order Hadamard matrices.* (preprint).