J. Austral. Math. Soc. 22 (Series A) (1976), 119–127.

USING CYCLOTOMY TO CONSTRUCT ORTHOGONAL DESIGNS

JOAN COOPER AND JENNIFER SEBERRY WALLIS

(Received 29 November 1974)

Communicated by W. D. Wallis

Dedicated to George Szekeres on his 65th birthday

Abstract

An orthogonal design of order n and type (s_1, s_2) on the commuting variables x_1, x_2 is a matrix of order n with entries from $\{0, \pm x_1, \pm x_2\}$ whose row vectors are formally orthogonal.

This note uses cyclotomy to construct orthogonal designs and finds several infinite families of new designs.

1. Introduction

Orthogonal designs in various guises have received attention lately [Baumert and Hall (1965), Cooper (1972), (1973), Cooper and Wallis (1972), Geramita, Geramita and Wallis (1975), Geramita and Wallis (1974), (1975), Hunt and Wallis (1972), Turyn (1972), (1974), Wallis (1973)] because they give insight into long standing problems on Hadamard matrices, weighing matrices and Baumert-Hall arrays. Ian Blake has noticed their application in coding theory and they are intimately related to the decomposition of integers into squares.

We shall assume all definitions which appear in the book by Wallis, Street and Wallis (1972) and give only those other definitions we need.

An orthogonal design of order n and *type* $(s_1, s_2, \cdots, s_l)(s_1 > 0)$ on the commuting variables $x_1, x_2, \cdots, x_l$ is an $n \times n$ matrix A with entries from $0, \pm x_1, \cdots, \pm x_l$ such that

$$AA^T = \sum_{i=1}^{l} (s_i x_i^2) I_n.$$

Alternatively, the rows of A are formally orthogonal and each row has precisely s_i entries of the variable $\pm x_i$.

In Geramita, Geramita and Wallis (1975), where this was first defined and

many examples and properties of such designs were investigated, it is mentioned that

$$A^T A = \sum_{i=1}^{l} (s_i x_i^2) I_n$$

and so the alternative description of A applies equally well to the columns of A. It was shown in the same paper of Geramita, Geramita and Wallis that $l \leqq \rho(n)$, where $\rho(n)$ (Radon's function) is defined by

$$\rho(n) = 8c + 2^d$$

when

$$n = 2^a \cdot b, b \text{ odd}, \quad a = 4c + d \quad 0 \leqq d < 4.$$

The identity matrix will be represented as I and the $v \times v$ matrix in which every entry is 1 will be J.

Let $v = ef + 1 = p^\alpha$ (a prime power) and consider the associated cyclic group G, of order $v - 1$, which is the multiplicative group of the Galois field $GF(P^\alpha)$. Then the associated cosets (or cyclotomic classes (the names are interchangeable see Storer (1967))) of G will be defined as

$$C_i = \{x^{ej+i} : 0 \leqq j \leqq f - 1\} \qquad 0 \leqq i \leqq e - 1,$$

where x is a primitive element of $GF(p^\alpha)$ and a generator of G. Write the elements of G as $0, z_1, z_2, \cdots, z_{ef}$.

The transpose of a coset, C_i^T, will be defined as $-C_i$ where

$$\begin{aligned} -C_i &= -\{x^{ej+i} : 0 \leqq j \leqq f - 1\} \\ &= \{-x^{ej+i} : 0 \leqq j \leqq f - 1\} \\ &= \{x^{em+i+k} : 0 \leqq j \leqq f - 1\} \end{aligned}$$

with $k = e/2$ for f odd and $k = 0$ for f even.

We will define $[C_i]$ the incidence matrix of the coset C_i by

$$C_{jl} = \begin{cases} 1 & \text{if } z_j - z_l \in C_i \\ 0 & \text{otherwise} \end{cases}$$

As $G = C_0 \cup C_1 \cup \cdots \cup C_{e-1} = GF(p^\alpha)/\{0\}$, its incidence matrix is $J - I$ (i.e., $\Sigma_{s=0}^{e-1}[C_s] = J - I$) and the incidence matrix of $GF(p^\alpha)$ is J. Therefore the incidence matrix of $\{0\}$ will be I.

Now if $[C_i]$ is incidence matrix of a coset of G then $[C_i^T] = [C_i]^T$ and

https://doi.org/10.1017/S1446788700013379 Published online by Cambridge University Press

(i) $[C_i]^T = [C_i]$ *if* f *is even:*

(ii) $[C_i]^T = [C_{i+\frac{e}{2}}]$ if f is odd.

The term $[C_i][C_j]$ will be taken to mean the ordinary matrix product of the incidence matrices of the cosets C_i and C_j.

$$[C_i][C_j] = \begin{cases} \sum_{s=0}^{e-1} a_s [C_s], & \text{if } C_j \neq C_i^T \text{ and} \\ \sum_{s=0}^{e-1} a_s [C_s] + fi, & \text{if } C_j = C_i^T \end{cases}$$

where the a_s are integers giving the coefficients of the matrices (for proof see Cooper (1972)).

2. Results

We shall consider various matrices obtained by taking linear combinations of the incidence matrices of cyclotomic classes. Part of this work appeared in the Ph.D. thesis of Joan Cooper (1974).

In every case p will be a prime power.

CASE 1: $p = 2f + 1$, f odd.

Consider

$$P = aI + b[C_0] + c[C_1] \tag{1}$$

where a, b, c are commuting variables. Now

$$PP^T = a^2 I + a(b[C_0] + c[C_1] + b[C_0]^T + c[C_1]^T) + b^2[C_0][C_0]^T + c^2[C_1][C_1]^T + bc([C_0][C_1]^T + [C_0]^T[C_1]).$$

Using the adapted cyclotomic array for $e = 2$ (in Hunt and Wallis (1973)) the Table 1 (writing ii for $[C_i][C_i]^T$ and ij for $([C_i][C_j]^T + [C_i]^T[C_j])$). We can calculate the coefficients

	C_0, C_1	$\{0\}$
00	$A = (f-1)/2$	f
11	$A = (f-1)/2$	f
01	$A + B = f$	0

Table 1

of the incidence matrices $[C_i]$ in PP^T from Table 1 obtaining:

https://doi.org/10.1017/S1446788700013379 Published online by Cambridge University Press

(i) the coefficient for $[C_0]$ is $(b^2+c^2+bc)A + bcB + ab + ac$;

(ii) the coefficient for $[C_1]$ is $(b^2+c^2+bc)A + bcB + ab + ac$.

As we are mainly interested in the situation where the coefficients of the $[C_i]$, $i = 1, 2, \cdots$ are equal we obtain

$$PP^T = (a^2 - ab - ac + \tfrac{1}{2}(b^2+c^2) + \tfrac{1}{2}(b-c)^2 f)I + (ab + ac - \tfrac{1}{2}(b^2+c^2) + \tfrac{1}{2}(b+c)^2 f)J. \tag{2}$$

Summarising

THEOREM 1. *Suppose $p = 2f+1$ (f odd) is a prime power and G the associated cyclic group $GF(p)/\{0\}$ of order $p-1$ with cosets C_0 and C_1 of order f. Then*

$$P = aI + b[C_0] + c[C_1],$$

a, b, c, commuting variables, is a square matrix satisfying (2).

COROLLARY 2. *Suppose $p = 2f+1$ (f odd) is a prime power. Then there exists an orthogonal integer matrix of order p.*

PROOF. Set $a = -\frac{1}{2}(f-1)c$, $b = 0$ and c any integer in Theorem 1.

We now use P to obtain orthogonal designs. Let X, Y, Z and W be derived from P given in (1) by setting
(i) $a = c = 0$, (ii) $a = -b, c = 0$, (iii) $a = b, c = 0$, (iv) $c = -b$ *respectively, then*

$$XX^T = b^2(\tfrac{1}{2}+\tfrac{1}{2}f)I + b^2(-\tfrac{1}{2}+\tfrac{1}{2}f)J$$
$$YY^T = b^2(5/2 + f/2)I + b^2(-3/2 + f/2)J$$
$$ZZ^T = b^2(\tfrac{1}{2}+\tfrac{1}{2}f)I + b^2(\tfrac{1}{2}+\tfrac{1}{2}f)J$$
$$WW^T = (a^2 + b^2 + 2b^2 f)I - b^2 J.$$

Then we have

THEOREM 3. *Let $I+S$ be a skew-Hadamard matrix of order* (i) $\frac{1}{2}(f+1)$ (ii) $\frac{1}{2}(f-1)$ (iii) $\frac{1}{2}(f+3)$ *respectively, where $p = 2f+1$ (f odd) is a prime power. Then with X, Y, Z, W, R as above* (i) $I \times XR + S \times W$ (ii) $I \times YR + S \times W$ (iii) $I \times ZR + S \times W$ *respectively are orthogonal designs of order*

(i) $\frac{1}{2}(f+1)(2f+1)$ *and type* $(\frac{1}{2}(f-1), f^2)$,

(ii) $\frac{1}{2}(f-1)(2f+1)$ *and type* $(\frac{1}{2}(f-3), (f-1)^2)$,

https://doi.org/10.1017/S1446788700013379 Published online by Cambridge University Press

(iii) $\frac{1}{2}(f+3)(2f+1)$ *and type* $(\frac{1}{2}(f+1), (f+1)^2)$,

respectively.

PROOF. Straightforward verification.

EXAMPLE. With $f = 5$ we see that the orthogonal design $(1, 16)$ exists in order 22 and $(3, 36)$ exists in order 44; while with $f = 9$ an orthogonal design $(3, 64)$ is obtained in order 76 and with $f = 13$ a $(7, 196)$ is obtained in order 216.

CASE 2: $p = 2f + 1$, $e = 2$, f even.

Again we use

$$P = aI + b[C_0] + c[C_1]$$

and obtain PP^T as before. However as f is even $C_i^T = C_i$, $i = 1, 2$ and

$$PP^T = a^2 I + 2ab[C_0] + 2ac[C_1] + b^2[C_0][C_0] + c^2[C_1][C_1] + 2bc[C_0][C_1].$$

From Storer (1967, p. 30) the cyclotomic matrix for $e = 2$, f even is

	0	1	
0	B	A	$B = \frac{1}{2}(f-2)$
1	A	A	$A = \frac{1}{2}f$.

Using Hunt and Wallis (1973) we see that expression $[C_i][C_j]$ is easily determined (see Table 2) and, since for f even $C_i^T = C_i$, the cyclotomic arrays can be used immediately to evaluate PP^T.

	C_0	{0}		
00	B	A	f	(writing ii for $[C_i][C_i]$
11	A	B	f	and ij for $[C_i][C_j]$).
01	A	A	0	

Table 2

Hence

$$PP^T = (a^2 + (b^2 + c^2)f)I + (2ab + \tfrac{1}{2}b^2(f-2) + \tfrac{1}{2}c^2 f + bcf)[C_0] + (2ac + \tfrac{1}{2}c^2(f-2) + \tfrac{1}{2}b^2 f + bcf)[C_1].$$

The coefficients of $[C_0]$ and $[C_1]$ are equal when

$$\text{(i)} \quad b = c \qquad \text{or} \qquad \text{(ii)} \quad 2a = b + c.$$

The case $b = c$ is trivial and the other case gives

https://doi.org/10.1017/S1446788700013379 Published online by Cambridge University Press

$$PP^T = (\tfrac{1}{4}(b-c)^2 + \tfrac{1}{2}(b-c)^2 f)I + (\tfrac{1}{2}(b+c)^2 f + bc)J.$$

Thus we have

THEOREM 4. *Let $p = 2f+1$ (f even) be a prime power and G the associated cyclic group of $GF(p)$ of order $p-1$ with cosets C_0 and C_1 of order f. Then*

$$P = \tfrac{1}{2}(b+c)I + b[C_0] + c[C_1],$$

where b and c are commuting variables, is a matrix satisfying

$$PP^T = (\tfrac{1}{4}(b-c)^2 + \tfrac{1}{2}(b-c)^2 f)I + (\tfrac{1}{2}(b+c)^2 f + bc)J.$$

To obtain orthogonal designs we will consider

$$P = aI + b[C_0] + c[C_1] \tag{3}$$
$$Q = aI + c[C_0] + b[C_1].$$

Now

$$PP^T + QQ^T = (a-b-c)^2 + a^2 - 2bc + (b-c)^2 f)I + (2a(b+c) - (b^2+c^2) + (b+c)^2 f)J.$$

Setting $c = -b$ we get M, N satisfying

$$MM^T + NN^T = 2(a^2 + b^2 + 2b^2 f)I - 2b^2 J.$$

Choosing $X = dI + b(J-I)$ and $Y = -dI + b(J-I)$ we have

$$XX^T + YY^T = 2(d^2+b^2)I + 2b^2(2f-1)J,$$

and hence, since M, N, X, Y are all symmetric, we have

THEOREM 5. *Let $p = 2f+1$ (f even) be a prime power. Suppose there exists a skew-Hadamard matrix, $I+S$, of order $2f$. Then*

$$I \times \begin{bmatrix} X & Y \\ -Y & X \end{bmatrix} + S \times \begin{bmatrix} M & N \\ N & -M \end{bmatrix}$$

is an orthogonal design of order $4f(2f+1)$ and type $(2, 2(f-1), 8f^2)$.

PROOF. By straightforward verification.

CASE 3: Now we consider $p = 4f+1$ (f even or odd) a prime power. As before G is the associated cyclic group of $GF(p)$ of order $p-1$ with cosets C_0, C_1, C_2 and C_3 of order f. Then

$$P = \tfrac{1}{2}(b+c) + b[C_0] + c[C_1] + b[C_2] + c[C_3],$$

where b and c are commuting variables, is a matrix satisfying

$$PP^T = (\tfrac{1}{4}(b-c)^2 + (b-c)^2 f)I + ((b+c)^2 f + bc)J.$$

To obtain orthogonal designs we will consider two cases

(a)
$$P = \tfrac{1}{2}(b+c)I + b[C_0] + c[C_1] + b[C_2] + c[C_3]$$
$$Q = \tfrac{1}{2}(b+c)I + c[C_0] + b[C_1] + c[C_2] + b[C_3]$$

(b)
$$P = aI + b[C_0] + c[C_1] + b[C_2] + c[C_3]$$
$$Q = aI + c[C_0] + b[C_1] + c[C_2] + b[C_3].$$

In case (a)

$$PP^T + QQ^T = (\tfrac{1}{2}(b-c)^2 + 2(b-c)^2 f)I + 2((b+c)^2 f + bc)J.$$

Setting $b = -c$ we get M, N satisfying

$$MM^T + NN^T = 2(b^2 + 4b^2 f)I - 2b^2 J.$$

Choosing

$$X = dI + b(J - I) \quad \text{and} \quad Y = -dI + b(J - I)$$

we have

$$XX^T + YY^T = 2(d^2 + b^2)I + 2b^2(4f - 1)J,$$

and hence, since M, N, X, Y are all symmetric we have

THEOREM 6. *Let $p = 4f + 1$ (f even or odd) be a prime power. Suppose there exists a skew-Hadamard matrix, $I + S$, of order $4f$. Then*

$$I \times \begin{bmatrix} X & Y \\ -Y & X \end{bmatrix} + S \times \begin{bmatrix} M & N \\ N & -M \end{bmatrix}$$

is an orthogonal design of order $8f(4f+1)$ and type $(2, 32f^2)$.

PROOF. By straightforward verification.

In case (b) we set $b = -c$ and we get M, N satisfying

$$MM^T + NN^T = 2(a^2 + b^2 + 4fb^2)I - 2b^2 J.$$

Choosing

$$X = dI + b(J - I) \quad \text{and} \quad Y = -dI + b(J - I)$$

we have

$$XX^T + YY^T = 2(d^2 + b^2)I + 2b^2(4f - 1)J$$

and hence, since M, N, X, Y are all symmetric we have

THEOREM 7. *Let $p = 4f + 1$ (f even or odd) be a prime power. Suppose there exists a skew-Hadamard matrix, $I + S$, of order $4f$. Then*

$$I \times \begin{bmatrix} X & Y \\ -Y & X \end{bmatrix} + S \times \begin{bmatrix} M & N \\ M & -M \end{bmatrix}$$

is an orthogonal design of order $8f(4f + 1)$ and type $(2, 2(4f - 1), 32f^2)$.

Clearly these methods can be extended to obtain similar results for other e.

References

L. D. Baumert and Marshall Hall, Jr. (1965), 'A new construction for Hadamard matrices', *Bull. Amer. Math. Soc.* **71**, 169–170.

Joan Cooper (1972), 'A binary composition for collections and sets', *Proceedings of the First Australian Conference on Combinatorial Mathematics*, 145–161, TUNRA, Newcastle.

Joan Cooper (1974), 'A note on Hadamard arrays', *Bull. Austral. Soc.* **10**, 15–21.

Joan Cooper and Jennifer Wallis (1972), 'A construction for Hadamard arrays', *Bull. Austral. Math. Soc.* **7**, 269–278.

Anthony V. Geramita, Joan Murphy Geramita and Jennifer Seberry Wallis (1975), 'Orthogonal designs', *Linear and Multilinear Algebra* **3**.

Anthony V. Geramita and Jennifer Seberry Wallis, 'Orthogonal designs II', *Aequationes Math.* (to appear).

Anthony V. Geramita and Jennifer Seberry Wallis (1974), 'Orthogonal designs III: weighing matrices', *Utilitas Math.* **6**, 209–236.

Anthony V. Geramita and Jennifer Seberry Wallis (1975), 'Orthogonal designs IV: existence questions', *J. Combinatorial Theory.* (Series A), **19**, 66–83.

J. M. Geothals and J. J. Seidel (1967), 'Orthogonal matrices with zero diagonal', *Canad. J. Math.* **19**, 1001–1010.

Marshall Hall, Jr. (1967), *Combinatorial Theory* (Blaisdell, [Ginn] Waltham, Massachusetts).

David C. Hunt and Jennifer Wallis (1973), 'Cyclotomy, Hadamard arrays and supplementary difference sets', *Proceedings of the Second Manitoba Conference on Numerical Mathematics*, 351–381, Congressus Numerantium 7, University of Manitoba, Winnipeg.

Thomas Storer (1967), *Cyclotomy and Difference Sets* (Lectures in Advanced Mathematics, 2. Markham, Chicago, Illinois).

Richard J. Turyn (1974), 'Hadamard matrices, Baumert-Hall units, four-symbol sequence, pulse compression and surface wave encodings', *J. Combinatorial Th.* (ser. A), **16**, 313–333.

Richard J. Turyn (1972), 'Hadamard matrices, algebras, and composition theorems', *Notices Amer. Math. Soc.* **19**, A–388.

Jennifer Wallis (1973), 'Hadamard matrices of order 28m, 36m, and 44m', *J. Combinatorial Theory* (Series A) **15**, 323–328.

W. D. Wallis, Anne Penfold Street, Jennifer Seberry Wallis (1972), *Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices* (Lecture Notes in Mathematics, Vol. 292, Springer-Verlag, Berlin-Heidelberg-New York).

Department of Mathematics
University of Newcastle
Australia

and

Department of Mathematics
Institute of Advanced Studies
Australian National University.