Can. J. Math., Vol. XXXIII, No. 5, 1981, pp. 1043–1054

LIMITS ON PAIRWISE AMICABLE ORTHOGONAL DESIGNS

WARREN WOLFE

Introduction. An *orthogonal design in order n of type* $(u_1, \ldots, u_t)$ on the commuting variables $x_1, \ldots, x_t$ is an $n \times n$ matrix X with entries $0, \pm x_1, \ldots, \pm x_t$ such that

$$XX^t = (u_1x_1^2 + \ldots + u_tx_t^2)I_n.$$

In [**5**] Geramita and Wallis show that if $n = 2^{4a+b} \cdot n_0$, where n_0 is odd and $0 \leqq b < 4$, then $t \leqq \rho(n) = 8a + 2^b$. The result is essentially Radon's limit on the number of anti-commuting, real, anti-symmetric, orthogonal matrices in order n. Garamita and Pullman show that this limit is sharp for orthogonal designs: i.e., given n, there exists an orthogonal design in order n with $\rho(n)$ variables [**6**].

Two orthogonal designs, X and Y, are called *amicable* if $XY^t = YX^t$. Such pairs of orthogonal designs are especially useful in generating new orthogonal designs [**5**] or [**6**]. In [**9**] it is shown that the total number of variables which can appear in such a pair is bounded by $\rho(n) = 8a + 2b + 2$ and that this bound is sharp. In [**8**] Shapiro has found the same limiting functions on the dimensions of spaces of similarities of quadratic forms.

The interested reader is referred to [**7**] for a more complete discourse on orthogonal designs.

In this paper, a set of t pairwise amicable orthogonal designs in order n is considered. Such sets would again be productive generators of new orthogonal designs. It is shown that the total number of variables which can appear in such a set is bounded by $8a + 2b + t$. If $b = 0$, then this bound is always sharp. However, if $b = 1, 2$, or 3, there are cases when the limit is actually less than $8a + 2b + t$.

1. A generalized Hurwitz group. Suppose $X_1, \ldots, X_t$ are orthogonal designs in order n such that, if $i \neq j$, $X_iX_j^t = X_jX_i^t$. Let

$$X_i = \sum_{j=1}^{s(i)} A_{ij}x_{ij}$$

where the x_{ij}'s are distinct commuting variables and the A_{ij} are $(0, \pm 1)$ matrices such that $A_{ij}A_{ij}^t = u_{ij}I_n$: i.e., X_i is of type $(u_{i1}, \ldots, u_{is(i)})$.

Received September 11, 1979 and in revised form May 20, 1980.

https://doi.org/10.4153/CJM-1981-079-x Published online by Cambridge University Press

Let

$$\alpha_{ij} = \frac{1}{\sqrt{u_{ij}u_{11}}} A_{ij}A_{11}{}^{t}.$$

Then $\alpha_{11} = I_n$ and the set of real matrices $\{\alpha_{ij}, 1 \leqq i \leqq t, 1 \leqq j \leqq s(i)\}$ satisfy:

(i) $\alpha_{1j}{}^2 = -I_n, 2 \leqq j \leqq s(1); \alpha_{ij}{}^2 = I_n, i \neq 1, 1 \leqq j \leqq s(i)$;

(ii) $\alpha_{ij}\alpha_{ik} = -\alpha_{ik}\alpha_{ij}, 1 \leqq i \leqq t, j \neq k$;

(iii) $\alpha_{1j}\alpha_{ik} = -\alpha_{ik}\alpha_{1j}, i \neq 1, 2 \leqq j \leqq s(1), 1 \leqq k \leqq s(i)$;

(iv) $\alpha_{ij}\alpha_{kl} = \alpha_{kl}\alpha_{ij}, 2 \leqq i \neq k \leqq t, 1 \leqq j \leqq s(i), 1 \leqq l \leqq s(k)$.

Then consider a group which mimics the above structure.

Definition. If $\{s(1), \ldots, s(t)\}$ is an t-tuple of positive integers where $t \geqq 2$ and $s(1) \geqq 2$, then the *generalized Hurwitz group* $G = G\{s(1), \ldots s(t)\}$ is the group with generators $\epsilon, a_{12}, \ldots, a_{1s(1)}, \ldots, a_{t1}, \ldots, a_{ts(t)}$ and defining relations:

(i) $\epsilon^2 = 1, \epsilon \neq 1, \epsilon a = a\epsilon$ for every a in G;
(ii) $a_{1j}{}^2 = \epsilon, 2 \leqq j \leqq s(1); a_{ij}{}^2 = 1, i \neq 1, 1 \leqq j \leqq s(i)$;
(iii) $a_{ij}a_{ik} = \epsilon a_{ik}a_{ij}$ $\quad 1 \leqq i \leqq t, j \neq k$;
(iv) $a_{1j}a_{ik} = \epsilon a_{ik}a_{1j}$ $\quad i \neq 1, 2 \leqq j \leqq s(1), 1 \leqq k \leqq s(i)$;
(v) $a_{ij}a_{kl} = a_{kl}a_{ij}$ $\quad 2 \leqq i \neq k \leqq t, 1 \leqq j \leqq s(i), 1 \leqq l \leqq s(k)$.

Surely the set of normalized matrices obtained from the set of pairwise amicable orthogonal designs in order n is a matrix representation of a generalized Hurwitz group. The goal is to find the minimal degree of such a real representation, F, where $F(\epsilon) = -I_n$. The techniques were used by Eckmann in his description of the Hurwitz group [**2**]. The reader is referred to [**1**], [**3**] or [**4**] for the salient facts regarding group representation theory.

Note. If A is a set, then $|A|$ denotes the order of A.

Let $m = \sum_1^t s(i)$. It is clear that $|G| = 2^m$. Also an easy check will show that the commutator subgroup, G', is $\{1, \epsilon\}$. Let $c(G)$ be the number of conjugacy classes in G, let $J = \{i | 1 \leqq i \leqq t, s(i) \text{ is odd}\}$, and let $Z(G)$ denote the centre of the group G.

LEMMA 1.1. *If $s(i)$ is even for all i then $|Z(G)| = 4$. Otherwise $|Z(G)| = 2^{|J|}$.*

Proof. Let

$$a_1 = \prod_{j=2}^{s(1)} a_{1j} \quad \text{and} \quad a_i = \prod_{j=1}^{s(i)} a_{ij} \quad \text{for } i \neq 1.$$

Consider an element ω of $Z(G)$, the centre of G. Then assume without

https://doi.org/10.4153/CJM-1981-079-x Published online by Cambridge University Press

loss of generality that

$$\omega = \prod_{i=1}^{t} \prod_{j=1}^{\beta(i)} y_{ij}$$

where y_{ij} is in $\{a_{ik}\}$, $y_{ij} \neq y_{il}$, $0 \leqq \beta(i) \leqq s(i)$. Note that $\epsilon\omega$ is in $Z(G)$.

If $0 < \beta(1)$, then

$$y_{11}\omega = \omega y_{11} = \epsilon^{\Sigma\beta(i)-1} y_{11}\omega$$

and hence $\sum\beta(i)$ is odd. If $\beta(1) < s(1) - 1$, then for some a_{1k},

$$a_{1k} \notin \{y_{1j}\},\ a_{1k}\omega = \omega a_{1k} = \epsilon^{\Sigma\beta(i)} a_{1k}\omega$$

and hence $\sum\beta(i)$ is even. Thus either $\beta(1) = 0$ and $\sum\beta(i)$ is even or $\beta(1) = s(1) - 1$ and $\sum\beta(i)$ is odd.

For $i \neq 1$, a procedure as above yields that either $\beta(i) = 0$ and $\beta(1)$ is even or $\beta(i) = s(i)$ and $\beta(i) + \beta(1)$ is odd.

Now assume $\beta(1) = 0$. Then for $i \neq 1$, $\beta(i) = 0$ or $\beta(i) = s(i)$ is odd. Thus $\omega = \prod_{i \in I} a_i$, $1 \notin I \subset J$, $|I|$ even.

Finally assume that $\beta(1) = s(1) \neq 0$. Now if $s(1)$ is even then $\beta(1)$ is odd and $\beta(i) = s(i)$ is even for $i \neq 1$. Hence $\omega = \prod_{i=1}^{t} a_i$.

On the other hand, if $s(1)$ is odd then $\beta(1)$ is even and $\beta(i) = 0$ or $\beta(i) = s(i)$ is odd for $i \neq 1$. Then $\omega = \prod_{i \in I} a_i$, $I \subset J$, $|I|$ even.

The result follows by counting the elements in $Z(G)$.

By the theory of group representations G has 2^{m-1} irreducible complex representations of degree 1. The following lemma will provide a common degree for those representations of degree > 1, and appears as problem 2.13 in [**3**].

LEMMA 1.2. *If G is a group such that $|G| = 2^m$ and $|G'| = 2$ then all complex irreducible representations of G of degree > 1 have a common degree.*

Proof. Let $\mu_1, \ldots, \mu_t$ be the characters of all irreducible complex representations of G of degree 1 and let χ_i, $1 \leqq i \leqq s$ be the characters of those representations, F_i, of degrees $d_i > 1$.

By the orthogonality relations, see [**1**],

$$\sum_1^t |\mu_i(g)|^2 + \sum_1^s |\chi_j(g)|^2 = |C_G(g)|$$

where $C_G(g)$ is the centralizer of g. But, if $g \notin Z(G)$, then

$$\sum_1^t |\mu_i(g)|^2 = |G|/|G'| = 2^{m-1} \quad \text{and} \quad |C_G(g)| \leqq 2^{m-1}.$$

Hence $2^{m-1} + \sum_1^t |\chi_j(g)|^2 \leqq 2^{m-1}$ so $\chi_i(g) = 0$. Now if i is fixed,

$$|G| = \sum_{g \in G} |\chi_i(g)|^2 = \sum_{g \in Z(G)} |\chi_i(g)|^2.$$

https://doi.org/10.4153/CJM-1981-079-x Published online by Cambridge University Press

But if $g \in Z(G)$, $F_i(g)$ must be a scalar matrix $\alpha_g I_{d_i}$ where α_g is a root of unity. Thus

$$|G| = \sum_{g \in \Sigma(G)} d_i^2 = |Z(G)| d_i^2$$

i.e., $d_i^2 = |G|/|Z(G)|$ for $1 \leqq i \leqq s$. Thus for all i, j, $d_i = d_j$.

Consider the case when some $s(i)$ is odd. Then $c(G) = 2^{m-1} + 2^{|J|-1}$, and this is the number of equivalent irreducible complex representations of G. Since G has 2^{m-1} representations of degree 1, there must be $2^{|J|-1}$ irreducible complex representations of degree $n > 1$. In fact, the proof of the lemma shows that every such representation has degree d where

$$d^2 = \frac{|G|}{|Z(G)|} = \frac{2^m}{2^{|J|}}$$

i.e.,

$$d = 2^{(m-|J|)/2}.$$

LEMMA 1.3. *If $s(i)$ is even for all i, then there exist 2 irreducible complex representations of G of degree $2^{(m-2)/2}$.*

Otherwise there exist $2^{|J|-1}$ irreducible complex representations of G of degree $2^{(m-|J|)/2}$.

Proof. The second statement is proved above and the first follows similarly.

For the purpose at hand, it is necessary to find the degrees of real representations of G. If F is an irreducible complex representation of G of degree n, then ϕF is a real representation of G of degree $2n$ where ϕ is the usual representation of the complex numbers as 2×2 real matrices. However, it is often possible to do better. F is called *realizable* over **R** if the entries in the matrices of $F(G)$ are real complex numbers. The Frobenius Schur Lemma [**1**] states that a complex representation F is realizable over **R** if and only if $\sum_{g \in G} \chi(g^2) > 0$ where χ is the character of F. Note also that in the present case it is required that $F(\epsilon) = -I$. Then $\chi(\epsilon) = -n$.

Suppose g is in G and

$$g = \prod_{i=1}^{t} \prod_{j=1}^{\alpha(i)} y_{ij}$$

where $y_{ij} \in \{a_{ik}\}$, $y_{ij} \neq y_{il}$, and $0 \leqq \alpha(i) \leqq s(i)$. Let

$$\mu_g = \alpha(1)[\alpha(1) + 1] + \sum_{i=2}^{t} (2\alpha(1)\alpha(i) + \alpha(i)[\alpha(i) - 1]).$$

Then

$$(\epsilon g)^2 = g^2 = \epsilon^{\mu_g/2} = \begin{cases} 1 & \text{if } \mu_g \equiv 0 (\text{mod } 4) \\ \epsilon & \text{if } \mu_g \equiv 2 (\text{mod } 4) \end{cases}$$

and $\chi(g^2) = \pm n$, depending upon μ_g. Consequently $\sum_{g \in G} \chi(g^2) = 2nT$ where

$$T = |\{g|\mu_g \equiv 0 \pmod 4\}| - |\{g|\mu_g \equiv 2 \pmod 4\}|.$$

Now F is realizable over $\mathbf{R}$ if and only if $T > 0$.

A suitable counting device for T is suggested in [**2**]. If p is a positive integer, let $z_p = (1 + i)^p = x_p + iy_p$.

$$x_p = \binom{p}{0} - \binom{p}{2} + \binom{p}{4} \dots \quad y_p = \binom{p}{1} - \binom{p}{3} + \binom{p}{5} \dots$$

$$x_p + y_p = \binom{p}{0} + \binom{p}{1} - \binom{p}{2} - \binom{p}{3} + \dots$$

$$x_p - y_p = \binom{p}{0} - \binom{p}{1} - \binom{p}{2} + \binom{p}{3} + \dots.$$

The following table gives values $-$, $+$, or 0 for these numbers for various values of p.

TABLE 1.1

$p \pmod 8$	0	1	2	3	4	5	6	7
x_p	+	+	0	−	−	−	0	+
y_p	0	+	+	+	0	−	−	−
$x_p + y_p$	+	+	+	0	−	−	−	0
$x_p - y_p$	+	0	−	−	−	0	+	+

LEMMA 1.4.

$$T = x_{s(1)} \prod_{j=2}^{t} (x_{s(j)} + y_{s(j)}) - y_{s(1)} \prod_{j=2}^{t} (x_{s(j)} - y_{s(j)}).$$

Proof. There are $\binom{s(1) - 1}{\alpha(1)}$ ways of choosing a word of $\alpha(1)$ distinct elements from the set $\{a_{1j}\}$; $\binom{s(i)}{\alpha(i)}$ ways of choosing a word of $\alpha(i)$ distinct elements from $\{a_{ij}\}$ if $i \neq 1$.

Let T_i be the contribution to T by elements g, where $\alpha(1) \equiv i \pmod 4$, for $i = 0, 1, 2, 3$. There are

$$\left[\binom{s(1) - 1}{i} + \binom{s(1) - 1}{4 + i} + \dots\right]$$

such elements, and

$$\mu_g \equiv \left(i(i + 1) + \sum_{j=2}^{t} \alpha(j)[2i + \alpha(j) - 1]\right) \pmod 4.$$

Suppose $i = 0$; then

$$\mu_g = \sum_{j=2}^{t} \alpha(j)(\alpha(j) - 1) \equiv 0 (\text{mod } 4)$$

if and only if there are an even number of j's such that $\alpha(j) \equiv 2$ or 3 (mod 4). Now proceed by induction on t.

If $t = 2$, then $\mu_g \equiv 0 \pmod 4$ if and only if $\alpha(2) \equiv 0$ or $1 \pmod 4$. Hence

$$T_0 = \left[\binom{s(1) - 1}{0} + \binom{s(1) - 1}{4} + \dots \right] (x_{s(2)} + y_{s(2)}).$$

Now assume that for $t = k$

$$T_0 = \left[\binom{s(1) - 1}{0} + \binom{s(1) - 1}{4} + \dots \right] \times (x_{s(2)} + y_{s(2)}) \dots (x_{s(k)} + y_{s(k)}).$$

Let

$$g = \left(\prod_{i=1}^{k} \prod_{j=1}^{\alpha(i)} y_{ij} \right) \prod_{j=1}^{\alpha(k+1)} y_{(k+1)j} = g_k \prod_{j=1}^{\alpha(k+1)} y_{(k+1)j}.$$

Then $\mu_g = \mu_{g_k} + \alpha(k+1)(\alpha(k+1) - 1)$ and $\mu_g \equiv 0 \pmod 4$ if and only if

$$\mu_{g_k} \equiv \alpha(k+1)(\alpha(k+1) - 1) \pmod 4.$$

$$\begin{aligned} T_0 &= [\text{number of times } \mu_{g_k} \equiv 0 \pmod 4] (x_{s(k+1)} + y_{s(k+1)}) \\ &- [\text{number of times } \mu_{g_k} \equiv 2 \pmod 4] (x_{s(k+1)} + y_{s(k+1)}) \\ &= \left[\binom{s(1) - 1}{0} + \binom{s(1) - 1}{4} + \dots \right] \times (x_{s(2)} + y_{s(2)}) \dots (x_{s(k+1)} + y_{s(k+1)}). \end{aligned}$$

Similarly

$$T_1 = (-1) \left[\binom{s(1) - 1}{1} + \binom{s(1) - 1}{1} + \dots \right] \times (x_{s(2)} - y_{s(2)}) \dots (x_{s(t)} - y_{s(t)})$$

$$T_2 = (-1) \left[\binom{s(1) - 1}{2} + \binom{s(1) - 1}{6} + \dots \right] \times (x_{s(2)} + y_{s(2)}) \dots (x_{s(t)} + y_{s(t)})$$

$$T_3 = \left[\binom{s(1) - 1}{3} + \binom{s(1) - 1}{7} + \dots \right] \times (x_{s(2)} - y_{s(2)}) \dots (x_{s(t)} - y_{s(t)}).$$

https://doi.org/10.4153/CJM-1981-079-x Published online by Cambridge University Press

Then

$T = (T_0 + T_2) + (T_1 + T_3)$ and the lemma follows.

The lemma shows that T depends upon the values of the $s(i) \pmod 8$. Let

$$n_\alpha = |\{i|2 \leqq i \leqq t,\ s_i \equiv \alpha \pmod 8\}|,\ 0 \leqq \alpha \leqq 8.$$

Note from Table 1.1 that if for some $i, j \neq 1$, $s(i) \equiv 1 \pmod 4$ and $s(j) \equiv 3 \pmod 4$, then $T = 0$.

Begin by assuming $n_1 + n_5 > 0$ and $n_3 = n_7 = 0$. Then

$$T = x_{s(1)-1}(x_{s(2)} + y_{s(2)}) \dots (x_{s(t)} + y_{s(t)}).$$

Since $x_{s(i)} + y_{s(i)} > 0$ for all i such that $s(i) \equiv 0, 1$, or $2 \pmod 8$, and $x_{s(i)} + y_{s(i)} < 0$ for all j such that $s(j) \equiv 4, 5$, or $6 \pmod 8$, it is sufficient to assume that

$$T = (-1)^{n_4+n_5+n_6}x_{s(1)-1}.$$

Thus $T > 0$ if and only if either

1) $n_4 + n_5 + n_6$ is even, $s(1) \equiv 0, 1$, or $2 \pmod 8$;

or

2) $n_4 + n_5 + n_6$ is odd, $s(1) \equiv 4, 5$, or $6 \pmod 8$.

Similarly if $n_3 + n_7 > 0$ and $n_1 = n_5 = 0$, then $T > 0$ if and only if either

1) $n_2 + n_3 + n_4$ is even, $s(1) \equiv 0, 6$, or $7 \pmod 8$;

or

2) $n_2 + n_3 + n_4$ is odd, $s(1) \equiv 2, 3$, or $4 \pmod 8$.

Now suppose $n_1 = n_3 = n_5 = n_7 = 0$. By Table 1.1 we can assume that

$$T = (-1)^{n_4}[x_{s(1)-1}(x_{s(2)} + y_{s(2)}) \dots (x_{s(q)} + y_{s(q)}) - y_{s(1)-1}(x_{s(2)} - y_{s(2)}) \dots (x_{s(q)} - y_{s(q)})]$$

where $s(i) \equiv 2$ or $6 \pmod 4$ for $2 \leqq i \leqq q$, and $q = n_2 + n_6$.

Note that if $n_2 + n_6 = 0$ then $T = (-1)^{n_4}x_{(s(1)-1)} - y_{(s(1)-1)}$.

If $s(i) \equiv 2$ or $6 \pmod 4$ then $x_s(i) = 0$ and

$$\begin{aligned} T &= (-1)^{n_4}[x_{(s(1)-1)}y_{x(2)} \dots y_{x(q)} - y_{(s(1)-1)}(-y_{s(2)}) \dots (-y_{s(q)})] \\ &= (-1)^{n_4}y_{s(2)} \dots y_{s(q)}[x_{(s(1)-1)} + (-1)^{q+1}y_{(s(1)-1)}] \\ &= (-1)^{n_4+n_6}[x_{(s(1)-1)} + (-1)^{n_2+n_6+1}y_{(s(1)-1)}]. \end{aligned}$$

Under the assumption that $n_1 = n_3 = n_5 = n_7 = 0$, then $T > 0$ if and only if one of the following

1) $n_2 = n_6 = 0$ and either:

a) n_4 is even, $s(1) \equiv 0, 1, 7 \pmod 8$;

or

b) n_4 is odd, $s(1) \equiv 3, 4, 5 \pmod 8$;

2) $n_2 + n_6 > 0$ and either:

a) $n_4 + n_6$ is even, $n_2 + n_6$ is even, $s(1) \equiv 0, 1, 7 \pmod 8$

or

b) $n_4 + n_6$ is even, $n_2 + n_6$ is odd, $s(1) \equiv 1, 2, 3 \pmod 8$

or

c) $n_4 + n_6$ is odd, $n_2 + n_6$ is even, $s(1) \equiv 3, 4, 5 \pmod 8$

or

d) $n_4 + n_6$ is odd, $n_2 + n_6$ is odd, $s(1) \equiv 5, 6, 7 \pmod 8$.

Let d be the degree of a real representation of G of minimal degree > 1. Lemma 1.3 combines with the above calculations as follows:

Case 1. If $s(1)$ is odd and $s(i)$ is even for all i, $2 \leqq i \leqq t$, then $d = 2^{(m-1)/2}$ if

i) $n_2 + n_6$ is even, $n_4 + n_6$ is even, $s(1) \equiv 1, 7 \pmod 8$

or

ii) $n_2 + n_6$ is even, $n_4 + n_6$ is odd, $s(1) \equiv 3, 5 \pmod 8$

or

iii) $n_2 + n_6$ is odd, $n_4 + n_6$ is even, $s(1) \equiv 1, 3 \pmod 8$

or

iv) $n_2 + n_6$ is odd, $n_4 + n_6$ is odd, $s(1) \equiv 5, 7 \pmod 8$

and $d = 2^{(m+1)/2}$ otherwise.

Case 2. If $s(1)$ and $s(i)$ are odd for some i, $2 \leqq i \leqq t$, then

$d = 2^{(m-n_1-n_5-1)/2}$ if $n_1 + n_5 > 0$, $n_3 = n_7 = 0$

and either

i) $n_4 + n_5 + n_6$ is even, $s(1) \equiv 1 \pmod 8$

or

ii) $n_4 + n_5 + n_6$ is odd, $s(1) \equiv 5 \pmod 8$.

$d = 2^{(m-n_3-n_7-1)/2}$ if $n_3 + n_7 > 0$, $n_1 = n_5 = 0$

and either

i) $n_2 + n_3 + n_4$ is even, $s(1) \equiv 7 \pmod 8$

or

ii) $n_2 + n_3 + n_4$ is odd, $s(1) \equiv 3 \pmod 8$.

$d = 2^{(m-n_1-n_3-n_5-n_7+1)/2}$ otherwise.

Case 3. If $s(i)$ is even for all i, $1 \leqq i \leqq t$, then $d = 2^{(m-2)/2}$ if

i) $n_2 + n_6$ is even, $n_4 + n_6$ is even, $s(1) \equiv 0 \pmod 8$

or

ii) $n_2 + n_6$ is even, $n_4 + n_6$ is odd, $s(1) \equiv 4 \pmod 8$

or

iii) $n_2 + n_6$ is odd, $n_4 + n_6$ is even, $s(1) \equiv 2 \pmod 8$

or

iv) $n_2 + n_6$ is odd, $n_4 + n_6$ is odd, $s(1) \equiv 6 \pmod 8$.

$d = 2^{m/2}$ otherwise.

Case 4. If $s(1)$ is even and $s(i)$ is odd for some i, $a \leqq i \leqq t$, then

$d = 2^{(m-n_1-n_5)/2}$ if $n_1 + n_5 > 0$, $n_3 = n_7 = 0$,

and either

i) $n_4 + n_5 + n_6$ is even, $s(1) \equiv 0, 2 \pmod 8$

or

ii) $n_4 + n_5 + n_6$ is odd, $s(1) \equiv 4, 6 \pmod 8$.

$d = 2^{(m-n_3-n_7)/2}$ if $n_3 + n_7 > 0$, $n_1 = n_5 = 0$,

and either

i) $n_2 + n_3 + n_4$ is even, $s(1) \equiv 6, 0 \pmod 8$

or

ii) $n_2 + n_3 + n_4$ is odd, $s(1) \equiv 2, 4 \pmod 8$.

$d = 2^{(m-n_1-n_3-n_5-n_7+2)/2}$ otherwise.

2. Limits on the variables. Now given a t-tuple $[s(1), \ldots, s(t)]$ it is possible to find the minimal degree n such that there exists a set of t pairwise amicable orthogonal designs where $s(i)$ is the number of variables in the ith design for $1 \leqq i \leqq t$. Again let $m = \sum_1^t s(i)$.

https://doi.org/10.4153/CJM-1981-079-x Published online by Cambridge University Press

Let $\delta_t(n)$ be the maximum number of variables which can appear in t pairwise amicable orthogonal designs in order n. Set $n = 2^{4a+b}\cdot n_0$ where n_0 is odd, $0 \leqq b < 4$. Then it has been shown that $\delta_1(n) = 8a + 2^b$ and that $\delta_2(n) = 8a + 2b + 2$ [see Introduction]. Partial bounds for $\delta_t(n)$ can now be found by using Section 1.

THEOREM 2.1. *For* $t > 1$, $\delta_t(n) \leqq 8a + 2b + t$.

Proof. By the calculations in Section 1, it is clear that the degree of a representation of the group G corresponding to a set of pairwise amicable orthogonal designs must have degree $\geqq 2^{(m-t)/2}$.

In fact this situation will occur only if all the $s(i)$ are odd and congruent (mod 4). Then

$$2^{4a+b} \geqq 2^{(m-t)/2} \text{ and } \delta_t(n) = m \leqq 8a + 2b + t.$$

COROLLARY 2.2. *If* $b = 1$ *and* $t \not\equiv 3 \pmod 4$, *then* $\delta_t(n) \leqq 8a + t - 1$.

Proof. Assume that $\delta_t(n) = m = 8a + t + 2$. Then $m \equiv t + 2$ (mod 8) and all the $s(i)$ must be odd and congruent (mod 4).

Assume $s(i) \equiv 1 \pmod 4$ for all i, then let $s(i) = 4p_i + 1$. Then

$$m = \sum_{i=1}^{t} s(i) = \sum_{i=1}^{t} (4p_i + 1) = 4\left(\sum_{i=1}^{t} p_i\right) + t \equiv t \pmod 4.$$

This contradicts the conclusion that $m = t + 2$ (mod 8).

Assume $s(i) \equiv 3 \pmod 4$ for all i. Then

$$m \equiv s(1) + 3n_3 + 7n_7 \pmod 8.$$

(Recall: $n_\alpha = |\{i|2 \leqq i \leqq t, s_i \equiv \alpha \pmod 8\}|$). Hence

$$\begin{aligned} s(1) &\equiv m - 3n_3 + n_7 \pmod 8 \\ &\equiv (t + 2) - 3n_3 + (t - n_3 - 1) \pmod 8 \\ &\equiv 2t + 1 - 4n_3 \pmod 8. \end{aligned}$$

Now, if n_3 is odd, then by case 2 after Lemma 1.4, $s(1) \equiv 3 \pmod 8$. By the above calculation, $s(1) \equiv 2t + 5 \pmod 8$, and hence $t \equiv 3 \pmod 4$, contrary to hypothesis. If n_3 is even, the same contradiction is achieved.

Thus, the conclusion is that $\delta_t(n) \leqq 8a + t + 1$.

COROLLARY 2.3. *If* $b = 2$ *and* $t \not\equiv 2 \pmod 4$, *then* $\delta_t(n) \leqq 8a + t + 3$.

COROLLARY 2.4. *If* $b = 3$ *and* $t \equiv 1 \pmod 4$, *then* $\delta_t(n) \leqq 8a + t + 5$.

Both of the above corollaries are proven in a manner similar to that used for Corollary 2.2.

THEOREM 2.5. *If* $n = 2^{4a}\cdot n_0$, *where* n_0 *is odd, then for each* $t > 1$, $\delta_t(n) = 8a + t$.

Proof. In [**9**] it is shown that there exist $\rho(n/2) + 1 = 8a + 1$ anti-commuting, symmetric, orthogonal, disjoint, $(0, \pm 1)$ matrices in order n, say $A_1, \ldots, A_{8a+1}$.

Let $X_1 = I_n x_1, \ldots, X_{t-1} = I_n x_{t-1}$, $X_t = \sum A_i y_i$ where the x_i and y_j are distinct commuting variables. Then $\{X_1, \ldots, X_t\}$ is a set of pairwise amicable orthogonal designs in order n with $8a + t$ variables.

CONSTRUCTION 2.6. *If there exists a set of t pairwise amicable orthogonal designs in order n with p variables, then there exists a similar set in order* $2^4\cdot n$ *with* $p + 8$ *variables.*

Proof. Let $\{X_i = \sum_{j=1}^{s(i)} A_{ij}x_{ij}, 1 \leqq i \leqq t\}$ be the given set of designs in order n. Let Zu and $\sum_1^9 W_i v_i$ be the amicable orthogonal designs in order 2^4 constructed in [**9**]. Then let

$$\bar{X}_1 = (A_{11} \otimes Z)z_{11} + \sum_{j=2}^{s(1)} (A_{1j} \otimes W_1)z_{1j}$$

$$\bar{X}_2 = \sum_{j=1}^{s(2)} (A_{2j} \otimes W_1)z_{2j} + \sum_{k=2}^{9} (A_{11} \otimes W_k)w_{2k}$$

$$\bar{X}_i = \sum_{j=1}^{s(i)} (A_{ij} \otimes Z)z_{ij} \quad \text{for } 3 \leqq i \leqq t,$$

where the z_{ij}, w_{2k} are distinct commuting variables. Then $\{\bar{X}_1, \ldots, \bar{X}_t\}$ is a set of pairwise amicable orthogonal designs in order $2^4\cdot n$ with $\sum_{i=1}^t s(i) + 8 = p + 8$ variables.

THEOREM 2.7.

$$\delta_3(n) = \begin{cases} 4 & \text{if } a = 0,\ b = 1 \\ 8a + 3 & \text{if } b = 0 \\ 8a + 5 & \text{if } b = 1,\ a > 0 \\ 8a + 6 & \text{if } b = 2 \\ 8a + 8 & \text{if } b = 3. \end{cases}$$

Proof. If $a = 0$, $b = 1$ then a pair of amicable orthogonal designs exists in order n with 4 variables. Hence $4 \leqq \delta_3(n) \leqq 5$. Careful consideration of all possible values for $s(1)$, $s(2)$, and $s(3)$ will show that in fact $\delta_3(n) = 5$ is impossible.

If $b = 0$, then Theorem 2.5 shows that $\delta_3(n) = 8a + 3$.

https://doi.org/10.4153/CJM-1981-079-x Published online by Cambridge University Press

If $b = 1$, $a > 0$, then let

$$\begin{aligned}
&A_{00} = I_{32} && A_{11} = P \otimes P \otimes P \otimes P \otimes P \\
& && A_{21} = Q \otimes A \otimes Q \otimes A \otimes I_2 \\
&A_{01} = P \otimes A \otimes I_8 && A_{12} = P \otimes P \otimes P \otimes P \otimes Q \\
& && A_{22} = Q \otimes A \otimes I_2 \otimes Q \otimes A \\
&A_{02} = A \otimes I_{16} && A_{13} = P \otimes P \otimes P \otimes Q \otimes I_2 \\
& && A_{23} = Q \otimes A \otimes Q \otimes P \otimes A \\
& && A_{14} = P \otimes P \otimes Q \otimes I_4 \\
& && A_{15} = P \otimes Q \otimes I_8 \\
& && A_{16} = Q \otimes I_{16} \\
& && A_{17} = P \otimes P \otimes A \otimes Q \otimes A
\end{aligned}$$

where

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad P = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad Q = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Then $\{X_i = \sum_j A_{ij}x_{ij}\}$, where x_{ij} are distinct commuting variables, is a set of 3 pairwise amicable orthogonal designs in order 2^5 with 13 variables. Now by induction on a and Construction 2.6, $\delta_3(n) \geqq 8a + 5$. By Theorem 2.1, $\delta_3(n) \leqq 8a + 5$ so there is equality.

If $b = 2$, Corollary 2.2 shows that $\delta_3(n) \leqq 8a + 6$, but, since a pair of amicable orthogonal designs exist in order n with $8a + 6$ variables [**9**], $\delta_3(n) = 8a + 6$.

Similarly Corollary 2.3 and the construction given in [**9**] show that if $b = 3$, then $\delta_3(n) = 8a + 8$.

References

1. L. Dornhoff, *Group representation theory*, part A (Marcel Dekker, New York, 1971).
2. B. Eckmann, *Gruppentheoretischer Beweis des Satzes von Hurwitz-Radon über die Komposition quadratischer Formen*, Comment. Math. Helv. *15* (1943).
3. I. M. Isaacs, *Character theory of finite groups* (Academic Press, New York, 1976).
4. I. N. Herstein, *Non-commutative rings*, Carus Math. Mono. *15*, M.A.A. (Wiley, New York, 1968).
5. A. V. Geramita, J. M. Geramita and J. S. Wallis, *Orthogonal designs*, J. Linear and Multilinear Alg. *3* (1975/76).
6. A. V. Geramita and N. J. Pullman, *A theorem of Hurwitz and Radon and orthogonal projective modules*, Proc. A.M.S. *42* (1974).
7. A. V. Geramita and J. Seberry, *Orthogonal designs* (Marcel Dekker, New York, 1979).
8. D. Shapiro, *Spaces of similarities IV: (s, t) families*, Pac. J. Math. *69* (1977).
9. W. Wolfe, *Amicable orthogonal designs—existence*, Can. J. Math. *28* (1976).

Royal Roads Military College,
Victoria, British Columbia