Can. J. Math., Vol. XXVIII, No. 5, 1976, pp. 1006–1020

AMICABLE ORTHOGONAL DESIGNS—EXISTENCE

WARREN WOLFE

1.

Definition. An *orthogonal design in order n and of type* $(u_1, \ldots, u_s)$ *on the commuting variables* $x_1, \ldots, x_s$ is an $n \times n$ matrix, X, with entries from the set $\{0, \pm x_1, \ldots, \pm x_s\}$ such that

$$XX^t = \left(\sum_1^s u_i x_i^2\right) I_n.$$

Alternately, each row of X has exactly u_i entries of the type $\pm x_i$ and the rows are formally orthogonal. A generic form of Hadamard arrays, orthogonal designs have been particularly useful for constructing Hadamard matrices and weighing matrices (see [**4**]).

If X is as above, let $X = \sum_1^s A_i x_i$. Then the A_i's are $n \times n$ matrices such that

(i) all entries are from $\{0, \pm 1\}$;

(ii) the A_i's are *disjoint*; i.e. if $*$ denotes the Hadamard product, $A_i * A_j = 0$ for $i \neq j$;

(iii) $A_i A_i^t = u_i I_n$;

(iv) $A_i A_j^t + A_j A_i^t = 0 \quad i \neq j$.

Using only (iii) and (iv) above, the authors of [**3**] show that $s \leqq \rho(n)$, where, if $n = 2^{4a+b} \cdot n_0$, n_0 odd, then $\rho(n) = 8a + 2^b$. The proof is based on Radon's work with sets of anti-commuting, skew-symmetric, orthogonal matrices.

In [**11**], as an attempt to further extract existence conditions from the algebraic properties of orthogonal designs, the following definition was made.

Definition. A *rational family in order n and of type* $[u_1, \ldots, u_s]$ is a family of $n \times n$ rational matrices, $\{A_1, \ldots, A_s\}$, where (iii) and (iv) above are satisfied.

Note that the type numbers of a rational family are positive rational numbers.

In [**11**], and to some extent in [**11**], it is shown that necessary and sufficient conditions for the existence of a rational family can be given in terms of the equivalence of two rational quadratic forms. As the Hasse-Minkowski theorem

Received September 29, 1975 and in revised form, May 26, 1976. This paper is based on the author's doctoral dissertation written at Queen's University, Kingston, under the supervision of Dr. A. V. Geramita.

gives a complete classification of such forms, the algebraic conditions for the existence of orthogonal designs are known and computable.

Even when a certain type of orthogonal design escapes extinction by the above results or by the rich combinatorial theory, there still remains the often difficult task of actually constructing an example of such a design. One of the most prolific generators of orthogonal designs has been the following construction:

THEOREM 1.1 (Geramita-Geramita-Wallis; see [**4**]). *Let X be an orthogonal design in order n and of type $(u_1, \ldots, u_s)$ on the variables $x_1, \ldots, x_s$. If $Y_1, \ldots, Y_s$ are orthogonal designs in order m on disjoint sets of variables, where Y_i is of type $(v_{i1}, \ldots, v_{ik_i})$ and $Y_iY_j^t = Y_jY_i^t$ for $i \neq j$, then there exists an orthogonal design in order $n \cdot m$ and of type $(u_1v_{11}, \ldots, u_1v_{1k_1}, \ldots, u_sv_{s1}, \ldots, u_sv_{sk_s})$.*

Proof. If $X = \sum_1^s A_ix_i$, then $Y = \sum_1^s (A_i \otimes Y_i)$ will be the required orthogonal design.

Essentially, the construction consists of replacing the variable x_i in X with the order m matrix Y_i. The relation $Y_iY_j^t = Y_jY_i^t$ is required to give orthogonality in the new orthogonal design and it became of interest to find pairs of matrices which satisfied this transpose commutativity. For the purpose of investigating the existence of such pairs, we have made the following definition:

Definition. Two orthogonal designs, X and Y, of the same order, will be said to be *amicable* if $XY^t = YX^t$.

Suppose X and Y are amicable orthogonal designs in order n, where X is of type $(u_1, \ldots, u_s)$ on the variables $x_1, \ldots, x_s$ and Y is of type $(v_1, \ldots, v_t)$ on the variables $y_1, \ldots, y_t$, and the x_i's and y_j's are distinct. Write

$$X = \sum A_ix_i \quad Y = \sum B_jy_j.$$

The A_i's form a rational family as do the B_j's and the union of these two families is called the *amicable family* obtained from X, Y. Note that

(0) $A_i * A_j = 0$ for $i \neq j$, $\quad B_k * B_l = 0$ for $k \neq l$

(i) $A_iA_i^t = u_iI_n \,\forall i$, $\quad B_jB_j^t = v_jI_n \,\forall j$

(ii) $A_iA_j^t + A_jA_i^t = 0$ for $i \neq j$, $\quad B_kB_l^t + B_lB_k^t = 0$ *for* $k \neq l$

(iii) $A_iB_j^t = B_jA_i^t \quad \forall i, \forall j$.

Certainly the A_i's, respectively the B_j's, must satisfy all the necessary conditions for the existence of a rational family; in particular s, respectively t, must not exceed $\rho(n)$. A preliminary exhaustive search in order 4 seemed to indicate that there were further restrictions and that $s + t < 8$. This led to a closer examination of the amicable families and their relations. In [**9**], Shapiro studies a form of amicable families of matrices (or (s, t)-families in his notation) over general fields and has so generalized the results achieved in this paper.

2. Extended Radon functions and Clifford algebras. Suppose $\{A_i, 0 \leqq i \leqq s; B_j, 1 \leqq j \leqq t\}$ is an amicable family of rational matrices obtained from two amicable orthogonal designs in order n of types $(u_0, \ldots, u_s)$ and $(v_1, \ldots, v_t)$.

Let

$$\alpha_i = \frac{1}{\sqrt{u_0 u_i}} A_i A_0^t \text{ for } 0 \leqq i \leqq s \quad \text{and} \quad \beta_j = \frac{1}{\sqrt{u_0 v_j}} B_j A_0^t \text{ for } 1 \leqq j \leqq t.$$

Then

$\alpha_0 = I_n$ and $\{\alpha_i 1 \leqq i \leqq s; \beta_j 1 \leqq j \leqq t\}$ is a family of *real* matrices where $\alpha_i = -\alpha_i^t$, $\beta_j = \beta_j^t$ and

$$(*)\begin{cases} \text{(i) } \alpha_i^2 = -I_n \,\forall i, \quad \beta_j^2 = I_n \,\forall j \\ \text{(ii) } \alpha_i\alpha_j + \alpha_j\alpha_i = 0 \text{ for } i \neq j, \quad \beta_k\beta_l + \beta_l\beta_k = 0 \text{ for } k \neq l \\ \text{(iii) } \alpha_i\beta_j + \beta_j\alpha_i = 0 \,\forall i, j. \end{cases}$$

Definition. A family of real matrices $\{\alpha_i \quad 1 \leqq i \leqq s; \beta_j \quad 1 \leqq j \leqq t\}$ will be called a *Hurwitz-Radon family of type* (s, t) (or, simply an H-$R(s, t)$ family) *in order* n if $\alpha_i = -\alpha_i^t \,\forall i$, $\beta_j = \beta_j^t \,\forall j$, and the relations $(*)$ are satisfied.

The relations $(*)$ are a form of the relations found by Clifford (see [**2**]) in his attempt to generalize the quaternions. Formal algebras over **R** which satisfy these relations are the so-called Clifford algebras and were used by Kawada and Iwahori (see [**5**]) in their study of sets of anti-commuting real and complex matrices.

Definition. A *Clifford algebra of type* (s, t) on **R**, denoted $C^{s,t}$, is an algebra over **R** with generators $\epsilon, a_1, \ldots, a_s, b_1, \ldots, b_t$ and fundamental relations

(i) $\epsilon^2 = \epsilon$, $\epsilon a_i = a_i\epsilon = a_i$ for $1 \leqq i \leqq s$

$\epsilon b_j = b_j\epsilon = b_j$ for $1 \leqq j \leqq t$

(ii) $a_i^2 = -\epsilon$ for $1 \leqq i \leqq s$, $\quad b_j^2 = \epsilon$ for $1 \leqq j \leqq t$

(iii) $a_i a_j = -a_j a_i$ for $i \neq j$, $\quad b_k b_l = -b_l b_k$ for $k \neq l$

(iv) $a_i b_j = -b_j a_i$ for $1 \leqq i \leqq s$, $1 \leqq j \leqq t$.

If $\epsilon = 1$, then $C^{s,t}$ is seen to be the Clifford algebra associated with the quadratic form $s \cdot \langle -1 \rangle \perp t \cdot \langle 1 \rangle$. For details of such Clifford algebras, we refer the reader to Witt (see [**10**]).

Our interest in such algebras is natural, since the existence of an H-$R(s, t)$ family in order n implies that the algebra $C^{s,t}$ has a matrix representation of degree n over **R**. Thus, if there is no representation of $C^{s,t}$ of degree n over **R**, then there is certainly no H-$R(s, t)$ family in order n.

On the other hand, every matrix representation of degree n of $C^{s,t}$ does not directly give rise to an H-$R(s, t)$ family in order n; for example, the images of the a_i's (respectively b_j's) need not be skew-symmetric (respectively symmetric) or even orthogonal. However, we shall see that the existence of such a representation of $C^{s,t}$ does indeed imply the existence of an H-$R(s, t)$ family.

Kawada and Iwahori describe completely the representation theory of $C^{s,t}$ (see [**5**]). In their connection with quadratic forms, these same algebras were investigated by Lam (see [**6**, pp. 126–139]).

If we let d be the degree of the irreducible matrix representation of $C^{s,t}$ over $\mathbf{R}$ of minimal degree >1, then the following theorems are restatements of the corresponding theorems of [**5**].

THEOREM 2.1. *If $s + t = 2k$, then $C^{s,t}$ is a central simple algebra over* $\mathbf{R}$, *and d (as defined above) is given as follows:*
(i) *if* $t - k \equiv 0$ *or* 1 (mod 4), *then* $d = 2^k$;
(ii) *if* $t - k \equiv 2$ *or* 3 (mod 4), *then* $d = 2^{k+1}$.

THEOREM 2.2. *If $s + t = 2k + 1$, then $C^{s,t}$ is a semi-simple algebra over* $\mathbf{R}$, *and d is given as follows:*
(i) *if* $t - k \equiv 0, 2,$ *or* 3 (mod 4), *then* $d = 2^{k+1}$;
(ii) *if* $t - k \equiv 1$ (mod 4), *then* $d = 2^k$.

If $s + t = 8h + p$, $0 \leqq p < 8$, then $d = 2^{4h+\delta}$ where δ is given by the following table:

TABLE I: Values of δ

t(mod 4) \ p	0	1	2	3	4	5	6	7
0	0	1	2	2	3	3	3	3
1	0	0	1	2	3	3	4	4
2	1	1	1	1	2	3	4	4
3	1	1	2	2	2	2	3	4

Definition. Let n, t be integers, $n > 0$, $t \geqq 0$. We define

$$\rho_t(n) = \max\{s \mid C^{s-1,t} \text{ has an irreducible matrix representation over } \mathbf{R} \text{ of degree } n\}.$$

By Radon's result previously metioned, it follows that $\rho_0(n) = \rho(n)$. Since the dimension of a Clifford algebra is always a power of 2, $\rho_t(2^a \cdot b) = \rho_t(2^a)$ if b is odd, and hence it suffices to consider $n = 2^a$. Further, the following relations may be observed:

PROPOSITION 2.3.

(i) $\rho_1(2) - 1 = 1$; $\rho_2(2) - 1 = 1$; $\rho_5(8) - 1 = 0$;
(ii) $\rho_t(2n) = \rho_{t-1}(n) + 1$;
(iii) $\rho_t(n) = \rho_{t+8}(2^4 n)$.

Proof. If $n = 2^{4a+b}$, $0 \leqq b < 4$, then $\rho_t(n) - 1 = 8a - t + \lambda$ where λ is given by the table below:

TABLE II: Values of λ

$t \pmod 4$ \ b	0	1	2	3
0	0	1	3	7
1	1	2	3	5
2	−1	3	4	5
3	−1	1	5	6

(i) follows immediately from the table.

(ii). Suppose $n = 2^{4h}$. If $t \equiv 0 \pmod 4$, then $\rho_t(2n) - 1 = 8h - t + 1$. Now $t - 1 \equiv 3 \pmod 4$ and $\rho_{t-1}(n) - 1 = 8h - (t - 1) - 1 = 8h - t$. If $t \equiv 1 \pmod 4$, then $\rho_t(2n) - 1 = 8h - t + 2$ and $\rho_{t-1}(n) - 1 = 8h - (t - 1) = 8h - t + 1$. If $t \equiv 2 \pmod 4$, then $\rho_t(2n) - 1 = 8h - t + 3$ and $\rho_{t-1}(n) - 1 = 8h - (t - 1) + 1 = 8h - t + 2$. If $t \equiv 3 \pmod 4$, then $\rho_t(2n) - 1 = 8h - t + 1$ and $\rho_{t-1}(n) - 1 = 8h - (t - 1) - 1 = 8h - t$.

The proof is similar for other values of n.

(iii) is proven in the same manner as (ii).

Note that the $\rho_t(n)$ are in fact completely determined by $\rho(l)$ and the above proposition. This is illustrated by the following table. Note the 8-periodicity. (The beginning of the second period is indicated by the dotted line.)

We appear to have considered only one side of the problem, i.e. given t *symmetric*, anti-commuting orthogonal matrices of order n, $\rho_t(n) - 1$ is the maximum number of *skew-symmetric*, anti-commuting orthogonal matrices of order n which anti-commute with the given t matrices. One could just as well begin with skew-symmetric matrices and ask for a limit on the number of anti-commuting symmetric orthogonal matrices. Let us consider this approach.

Definition. Let n and s be integers, $n > 0$, $s \geqq 0$. Define

$$\sigma_s(n) = \max\{t | C^{s,t-1} \text{ has an irreducible matrix representation over } \mathbf{R} \text{ of degree } n\}.$$

Indeed, $\sigma_s(n) - 1$ is the maximum number of anti-commuting symmetric orthogonal matrices in order n which one might find that anti-commute with a given set of s anti-commuting skew-symmetric orthogonal matrices.

Lam shows that, if $n = 2^{4a+b} \cdot n_0$, where n_0 is odd, $0 \leqq b < 4$, then $\sigma_0(n) = 8a + b + [b/3] + 2$ (Bracket denotes the integral part of rational numbers, see [**6**, p. 132]).

Adams et al. looked at sets of symmetric matrices of order n, such that non-zero linear combinations of the matrices were always non-singular (see [**1**]). If

https://doi.org/10.4153/CJM-1976-099-5 Published online by Cambridge University Press

TABLE III

n	$\rho_0(n)-1$	$\rho_1(n)-1$	$\rho_2(n)-1$	$\rho_3(n)-1$	$\rho_4(n)-1$	$\rho_5(n)-1$	$\rho_6(n)-1$	$\rho_7(n)-1$	$\rho_8(n)-1$	$\rho_9(n)-1$	$\rho_{10}(n)-1$	$\rho_{11}(n)-1$	$\rho_{12}(n)-1$
2	1	1	1	—									
2^2	3	2	2	2	—								
2^3	7	4	3	3	3	0	—						
2^4	8	8	5	4	4	4	1	0	0	0	—		
2^5	9	9	9	6	5	5	5	2	1	1	1	—	
2^6	11	10	10	10	7	6	6	6	3	2	2	2	—
2^7	15	12	11	11	11	8	7	7	7	4	3	3	3
2^8	16	16	13	12	12	12	9	8	8	8	5	4	4
2^9	17	17	17	14	13	13	13	10	9	9	9	6	5
2^{10}	19	18	18	18	15	14	14	14	11	10	10	10	7
2^{11}	23	20	19	19	19	16	15	15	15	12	11	11	11
2^{12}	24	24	21	20	20	20	17	16	16	16	13	12	12
2^{13}	25	25	25	22	21	21	21	18	17	17	17	14	13

$\mathbf{R}_s(n)$ is the maximum number of such real matrices which form a set with the above property, then they show that $\mathbf{R}_s(n) = \rho(n/2) + 1$.

If $\{A_i, 1 \leqq i \leqq t\}$ is an H-$R(0, t)$ family in order n, then for any t-tuple $(c_1, \ldots, c_t)$ of elements of $\mathbf{R}$

$$(c_1A_1 + \ldots + c_tA_t)^2 = (c_1^2 + \ldots + c_t^2)I_n.$$

Hence, if $(c_1, \ldots, c_t) \neq 0$, then $c_1A_1 + \ldots + c_tA_t$ is non-singular and $\{A_i, 1 \leqq i \leqq t\}$ is one of the families that Adams considered.

On the other hand, $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ is a family with Adams' property but it is not an H-$R(0, 1)$ family. However it is interesting to note how Adams' number $\mathbf{R}_s(n)$ is related to $\sigma_0(n)$. First we prove two lemmas. Let

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

LEMMA 1. *If* $\{M_i, 1 \leqq i \leqq t\}$ *is an* $H - R(t, 0)$ *family in order* n, *then*

$$\{A \otimes M_i, 1 \leqq i \leqq t, P \otimes I_n, Q \otimes I_n\}$$

is an H-$R(0, t + 2)$ *family in order* $2n$.

Proof. By tensoring each of the M_i with A, we have constructed symmetric orthogonal matrices which anti-commute because the M_i's do. That the other two matrices are symmetric orthogonal, and anti-commute properly follow from properties of A, P, and Q.

LEMMA 2. *If* $\{N_j, 1 \leqq j \leqq t\}$ *is an* H-$R(0, t)$ *family in order* n, *then* $\{A \otimes Q \otimes I_2 \otimes N_j, 1 \leqq j \leqq t, I_2 \otimes A \otimes I_{2n}, A \otimes P \otimes Q \otimes I_n, Q \otimes Q \otimes A \otimes I_n, P \otimes Q \otimes A \otimes I_n, I_2 \otimes P \otimes A \otimes I_n, A \otimes P \otimes P \otimes I_n\}$ *is an* H-$R(t + 6, 0)$ *family in order* $8n$.

Proof. Again follows from the properties of A, P, Q, and the N_j's.

PROPOSITION 2.4. $\sigma_0(n) = \rho(n/2) + 2$.

Proof. By Lemmas 1 and 2, $\sigma_0(n) \geqq \rho(n/2) + 2$ and $\rho(8n) \geqq \sigma_0(n) + 6$. Thus,

$$\rho(n/2) \leqq \sigma_0(n) - 2 \leqq \rho(8n) - 8.$$

But by the explicit form of ρ, we have

$$\rho(8n) - 8 = \rho(n/2).$$

Hence $\sigma_0(n) = \rho(n/2) + 2$.

This then gives a description of $\sigma_0(n)$ in terms of $\rho(l)$. Now consider $\sigma_s(n)$ for $s > 0$.

PROPOSITION 2.5. (i) $\sigma_1(2) - 1 = 2$; $\sigma_3(4) - 1 = 0$; $\sigma_5(8) - 1 = 0$; $\sigma_6(8) - 1 = 0$; $\sigma_7(8) - 1 = 0$.

(ii) $\sigma_s(2n) = \sigma_{s-1}(n) + 1$.
(iii) $\sigma_s(n) = \sigma_{s+8}(2^4 n)$.

Proof. If $n = 2^{4a+b}$, $0 \leqq b < 4$, then $\sigma_s(n) - 1 = 8a - s + \eta$ where η is given by the table below:

TABLE IV: Values of η

$s \pmod 4$ \ b	0	1	2	3
0	1	2	3	5
1	−1	3	4	5
2	−1	1	5	6
3	0	1	3	7

As in Proposition 2.3, the proof consists of considering various cases. We leave those verifications to the reader.

Now $\sigma_s(n) - 1$ is completely determined by $\sigma_0(l) - 1$ (and hence $\rho(l/2)$) and the above proposition.

Finally, one might ask, for a given n, what is the maximum total number of anti-commuting skew-symmetric and symmetric orthogonal matrices of order n.

Definition. Let $n > 0$ be an integer. Define

$$\tau(n) = \max\{\rho_t(n) + t | t \geqq 0\}.$$

PROPOSITION 2.6. *If $n = 2^a \cdot n_0$, where n_0 is odd, then $\tau(n) = 2a + 2$.*

Proof. We first chart some values of $\tau(n)$ for various n. For example, if $n = 2^{4h}$, by looking at Table II, one sees that the maximum value for $\rho_t(n) - 1 + t$ is $8h + 1$. Thus $\tau(2^{4h}) = 8h + 2 = 2(4h) + 2$.

n	2^{4h}	2^{4h+1}	2^{4h+2}	2^{4h+3}
$\tau(n)$	$2(4h) + 2$	$2(4h + 1) + 2$	$2(4h + 2) + 2$	$2(4h + 3) + 2$

Clearly one could have defined $\tau(n)$ as the maximum of $\sigma_s(n) + s$, $s \geqq 0$. But, from Table IV, one sees the numbers would coincide exactly.

Our results in this section lead us to the following theorem.

THEOREM 2.7. *Given $n > 0$, if there exists an H-R(s, t) family in order n, then*
(i) $s + t \leqq \tau(n) - 1$
(ii) $s \leqq \rho_t(n) - 1$, $t \leqq \sigma_s(n) - 1$.

COROLLARY 1. *If there exists a pair of amicable designs X and Y of types*

$(u_0, \ldots, u_s)$ and $(v_1, \ldots, v_t)$ respectively in order n, then $s \leqq \rho_t(n) - 1$. Similarly $t \leqq \sigma_s(n) - 1$.

Proof. We have already seen that if X and Y exist they give rise to an H-$R(s, t)$ family in order n and hence $s \leqq \rho_t(n) - 1$.

COROLLARY 2. *If X and Y exist as in Corollary 1, then $s + t \leqq \tau(n) - 1$.*

Indeed, the bounds $\tau(n)$, $\rho_t(n)$, and $\sigma_s(n)$ are sharp limits on the numbers of variables in an amicable pair of designs. Our purpose now is to show that, given $n > 0$, $t \geqq 0$, there does indeed exist an H-$R(\rho_t(n) - 1, t)$ family in order n and hence an H-$R(s, t)$ family exists in order n for $s \leqq \rho_t(n) - 1$. First we need two building lemmas.

Let A, P, and Q be the 2×2 matrices as defined before Lemma 1.

LEMMA (Slide). *If $\{M_i, 1 \leqq i \leqq i \leqq s; N_j, 1 \leqq j \leqq t\}$ is an H-$R(s, t)$ family in order n, then $\{P \otimes M_k, 1 \leqq i \leqq s, A \otimes I_n; P \otimes N_j, 1 \leqq j \leqq t, Q \otimes I_n\}$ is an H-$R(s + 1, t + 1)$ family in order $2n$.*

Proof. Orthogonality, symmetry, skew-symmetry, and anti-commutativity follow from the properties of A, P, Q, M_i's, and N_j's.

LEMMA (Jump). *If $\{M_i, 1 \leqq i \leqq s; N_j, 1 \leqq j \leqq t\}$ is an H-$R(s, t)$ family in order n, then $\{(A \otimes P \otimes A \otimes Q \otimes M_i, 1 \leqq i \leqq s; A \otimes P \otimes A \otimes Q \otimes N_j, 1 \leqq j \leqq t, Q \otimes Q \otimes Q \otimes Q \otimes I_n, P \otimes I_4 \otimes Q \otimes I_n, Q \otimes P \otimes I_2 \otimes Q \otimes I_n, Q \otimes Q \otimes P \otimes Q \otimes I_n, I_8 \otimes P \otimes I_n, P \otimes Q \otimes A \otimes A \otimes I_n, I_2 \otimes P \otimes A \otimes A \otimes I_n)\}$ is an H-$R(s, t + 8)$ family in order 2^4n.*

Proof. The proof is tedious but follows directly.

THEOREM 2.8. *For any positive integer n, there exists an H-$R(\rho_t(n) - 1, t)$ family in order n where $0 \leqq t$. Indeed, the matrices may be assumed to have integer entries.*

Proof. (i) $\{A; Q, P\}$ is an H-$R(1, 2)$ family in order 2.

(ii) $\{P \otimes P \otimes P, P \otimes P \otimes Q, P \otimes Q \otimes I_2, A \otimes Q \otimes A, Q \otimes I_2 \otimes I_2\}$ is an H-$R(0, 5)$ family in order 8.

(iii) $A \otimes P \otimes A \otimes Q, Q \otimes Q \otimes Q \otimes Q, P \otimes I_4 \otimes Q, Q \otimes P \otimes I_2 \otimes Q, Q \otimes Q \otimes P \otimes Q, I_8 \otimes P, P \otimes Q \otimes A \otimes A, I_2 \otimes P \otimes A \otimes A, P \otimes A \otimes I_2 \otimes A\}$ is an H-$R(0, 9)$ family in order 16.

Theorem 1 of [**3**] gives H-$R(\rho_0(n), 0)$ families in order n for all n. Now, working within the first period of Table III, one sees that, by using these families and (i), (ii), (iii), one can find big enough families by sliding down the diagonals with the slide lemma. For example, (i) gives an H-$R(\rho_1(2) - 1, 1)$ family in order 2. By repeated use of the slide lemma, one constructs from this family an H-$R(\rho_2(4) - 1, 2)$ family in order 4, an H-$R(\rho_3(8) - 1, 3)$ family in order 8, an H-$R(\rho_4(16) - 1, 4)$ family in order 16, . . . etc.

https://doi.org/10.4153/CJM-1976-099-5 Published online by Cambridge University Press

Using the jump lemma one can jump from period to period in Table III, constructing large enough families. Again, for example, from the family in (i) one can jump to an $H\text{-}R(\rho_9(2^5) - 1, 9)$ family in order 2^5, then to an $H\text{-}R(\rho_{17}(2^9) - 1, 17)$ family in order 2^9, . . . etc.

COROLLARY 1. *For any positive integer n, there exists an $H\text{-}R(s, t)$ family of integer matrices in order n for $s \leqq \rho_t(n) - 1$.*

Proof. We just throw away skew-symmetric matrices from the big family in the theorem.

COROLLARY 2. *In order n there exists a pair of amicable designs, X and Y, of types $(1, \ldots, 1)$ and $(1, \ldots, 1)$ on the variables $x_0, \ldots, x_s$ and $y_1, \ldots, y_t$ respectively if and only if $s \leqq \rho_t(n) - 1$.*

Proof. By Corollary 1 to Theorem 2.7, $s \leqq \rho_t(n) - 1$.

Conversely, suppose $\{A_i, 1 \leqq i \leqq s; B_j, 1 \leqq j \leqq t\}$ is one of the $H\text{-}R(s, t)$ families in order n we constructed in Theorem 2.8. We note that all the matrices have entries from $\{0, \pm 1\}$. We claim that the A_i's (and the B_j's) are disjoint. This follows from the easily proven property that if A, B, C, and D are matrices of the same order then $(A \otimes B) * (C \otimes D) = (A * C) \otimes (B * D)$. For example, in the slide lemma, if we assume that the M_i's are already disjoint, then $(P \otimes M_i) * (P \otimes M_j) = 0$.

Let

$$X = I_n x_0 + A_1 x_1 + \ldots + A_s x_s$$
$$Y = B_1 y_1 + \ldots + B_t y_t.$$

Then X and Y are amicable designs of the required type.

Note that the corollary also shows that X and Y exist if and only if $t \leqq \sigma_s(n) - 1$, for Corollary 2 asserts that every possible pair (s, t) is obtained and hence surely the maximum t for a given s is obtained.

COROLLARY 3. *Given $0 < k \leqq n$, then there exists a pair of amicable designs, X, Y, of types $(u_1, \ldots, u_s)$ and $(v_1, \ldots, v_t)$ where $\sum u_i \leqq k$, $\sum v_i \leqq$* $\max\{p_k(n), \sigma_{k-1}(n) - 1\}$.

Proof. Case (i): If $\rho_k(n) \geqq \sigma_{k-1}(n) - 1$, then we construct an $H\text{-}R(\rho_k(n) - 1, k)$ family in order n. As in Corollary 2, this family gives us a pair of amicable designs of types $(1, 1, \ldots, 1)$ and $(1, 1, \ldots, 1)$ on the variables $x_1, \ldots, x_{\rho_k(n)}$ and $y_1, \ldots, y_k$. Now by equating variables or setting variables equal to zero we will get all tuples $(u_1, \ldots, u_s)$ and $(v_1, \ldots, v_t)$ which satisfy the conditions in the statement of the theorem.

Case (ii): If $\sigma_{k-1}(n) - 1 > \rho_k(n)$, then we construct an $H\text{-}R(k - 1, \sigma_{k-1}(n) - 1)$ family in order n and proceed as before to find pairs of amicable designs.

3. Rational families and amicable pairs. In many orders, looking at the algebraic properties, by way of the rational families, does not give any information on the existence of amicable orthogonal designs. If n is odd and a^2 and b^2 are in Q, then let $A = aI_n$, $B = bI_n$. Then $AA^t = a^2 I_n$, $BB^t = b^2 I_n$ and $AB^t = BA^t$. Is the same possible for $(0, \pm 1)$ matrices?

In order $n \equiv 2 \pmod 4$, if there exists an orthogonal design of type (a, b), then a and b are sums of two squares and ab is a square (see [**4**]). So, suppose a, b and c, d are two pairs of rational numbers such that a, b, c, and d are sums of two squares and ab and cd are squares. Then, let $a = a_1^2 + a_2^2$, $b = au^2$, $c = c_1^2 + c_2^2$, and $d = cv^2$. Now let

$$A = \begin{bmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{bmatrix}, B = u\begin{bmatrix} -a_2 & a_1 \\ -a_1 & -a_2 \end{bmatrix}, C = \begin{bmatrix} c_1 & c_2 \\ c_2 & -c_1 \end{bmatrix}, D = v\begin{bmatrix} c_2 & -c_1 \\ -c_1 & -c_2 \end{bmatrix}.$$

$\{A, B\}$ is a rational family in order 2 of type $[a, b]$, $\{C, D\}$ is a rational family in order 2 of type $[c, d]$, and $XY^t = YX^t$ for X in $\{A, B\}$ and Y in $\{C, D\}$. We could tensor these families with I_n to achieve similar families in any order $2 \cdot n$.

This would indicate that we cannot hope to achieve any new existence theorems for amicable orthogonal designs *in these orders* using the methods of rational families. Any non-existence statements for pairs of amicable orthogonal designs would appear to have to be combinatorial. We shall give examples of such results in orders $2 \cdot n$, where n is odd. Recall the following results in [**11**].

THEOREM 3.1. *If $n \equiv 4 \pmod 8$, then there exists a rational family in order n and of type:*

(i) $[a, b, c, d]$ *if and only if $abcd$ is a square and, at every prime p, $s_p(\langle a, b, c, d\rangle) = 1$;*

(ii) $[a, b, c]$ *if and only if, at every prime p, $s_p(\langle a, b, c, abc\rangle) = 1$;*

(iii) $[a, b]$ *if and only if ab is a sum of three squares;*

(iv) $[a]$ *always.*

Note. $s_p(f)$ is the p-adic Hasse-invariant of the rational quadratic form f.

Now, suppose $X = \sum_1^s A_i x_i$ and $Y = \sum_1^t B_j y_j$ are amicable orthogonal designs in order n and of types $(a_1, \ldots, a_s)$ and $(b_1, \ldots, b_t)$ where $s \geqq 2$. Consider the family of matrices $\{A_1 A_2{}^t B_i,\ 1 \leqq i \leqq t,\ A_3, \ldots, A_s\}$. It is easy to verify that this set is a rational family in order n and of type $[a_1 a_2 b_1, \ldots, a_1 a_2 b_t, a_3, \ldots, a_s]$.

THEOREM 3.2. *If there exist amicable orthogonal designs in order n, where $n \equiv 4 \pmod 8$ and of types:*

(i) (a_1, a_2, a_3) *and* (b_1, b_2, b_3), *then $a_1a_2a_3b_1b_2b_3$ is an integer square;*

(ii) (a_1, a_2, a_3) *and* (b_1, b_2), *then, at every prime p, $s_p(\langle a_1a_2b_1, a_1a_2b_2, a_3, a_3b_1b_2\rangle) = 1$.*

Proof. (i) As in the remarks preceding the theorem, the amicable family obtained from the pair may be translated into a rational family in order n and

https://doi.org/10.4153/CJM-1976-099-5 Published online by Cambridge University Press

of type $[a_1a_2b_1, a_1a_2b_2, a_1a_2b_3, a_3]$. The result now follows by application of Theorem 3.1.

(ii) Follows similarly.

Examples of amicable orthogonal designs which are eliminated by the above theorems are easily found. No pair of types $(1, 1, 1)$ and $(1, 1, 2)$ can exist in order $4 \cdot n_0$, n_0 odd, since the product of all type numbers is not a square. Since the necessary condition of (ii) fails at the prime 3, amicable orthogonal designs of types $(1, 1, 1)$ and $(1, 3)$ does not exist in order $4 \cdot n_0$, n_0 odd.

In order $n \equiv 8 \pmod{16}$, a pair of amicable orthogonal designs can have at most 8 variables, namely 4 variables in each. The translation method used above and a result analogous to Theorem 3.1 will give results only in a few special cases. However, these results are now superseded by the results of Shapiro who has completely determined the question of the existence of amicable families. Translating his language of similarities of quadratic forms to one of orthogonal designs, we find the following result.

THEOREM 3.3. *If there exists amicable orthogonal designs in order* $n = 2^m \cdot n_0$, *where* n_0 *is odd, and of types* $(a_1, \ldots, a_{m+1})$ *and* $(b_1, \ldots, b_{m+1})$, *then* $\prod_1^{m+1} a_i \prod_1^{m+1} b_j$ *is a square and at every prime,* p, $s_p(\langle a_1, \ldots, a_{m+1} \rangle) = s_p(\langle b_1, \ldots, b_{m+1} \rangle)$.

Similar conditions can be given for the existence of amicable orthogonal designs with fewer than $\tau(n)$ variables. Thus the algebraic nature of pairs of amicable orthogonal designs is completely understood.

4. Further existence conditions. Disjointness and 0, ± 1 entries in the coefficient matrices of amicable orthogonal designs have led to some curious combinatorial results and prophesize a rich theory of this vein.

PROPOSITION 4.1. *There is no symmetric design of type* $(2, 2)$ *in order* n, $n \equiv 2 \pmod 4$.

Proof. We require the following lemma:

LEMMA. *If there exists a symmetric* $(0, \pm 1)$ *matrix,* A, *in order* n *which has zero diagonal and* $AA^t = 2I_n$, *then* $n \equiv 0 \pmod 4$.

Proof of Lemma. We simply note that, by applying suitable simultaneous row and column operations, such a matrix can be put in the form

$$\oplus \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{bmatrix},$$

To prove the proposition, we let $n = 4s + 2$ and proceed by induction on s. Assume there is a 6×6 symmetric orthogonal design A of type $(2, 2)$ on the variables x, y. We must assume x occurs in the diagonal by the lemma, and by simultaneous row and column operations we may put A in the form

$$A = \begin{bmatrix} x & x & y & y & 0 & 0 \\ x & -x & a & & & \\ y & & & & & \\ y & & & & & \\ 0 & & & & & \\ 0 & & & & & \end{bmatrix}$$

If $a = \pm y$, then $A = \begin{bmatrix} A' & 0 \\ 0 & B \end{bmatrix}$ where A' is 4×4 and B is 2×2. But this is nonsense since $BB^t = (2x^2 + 2y^2)I_2$.

If $a = 0$, then

$$A = \begin{bmatrix} x & x & y & y & 0 & 0 \\ x & -x & 0 & 0 & y & y \\ y & 0 & & & & \\ y & 0 & & & & \\ 0 & y & & & & \\ 0 & y & & & & \end{bmatrix}$$

and we are unable to put any more y-entries in the third column.

So now assume the proposition is true for $s > 1$ and further assume that there exists a symmetric orthogonal design, A, of type $(2, 2)$ in order $4(s + 1) + 2$ on the variables x and y. Again we may assume A is of the form

$$A = \begin{bmatrix} x & x & y & y & 0 & \cdots \\ x & -x & a & & & \\ y & & & & & \\ y & & & & & \\ y & & & & & \\ \cdot & & & & & \\ \cdot & & & & & \\ \cdot & & & & & \end{bmatrix}$$

If $a = \pm y$, then $A = \begin{bmatrix} A' & 0 \\ 0 & B \end{bmatrix}$ where A' is 4×4 and B is now an orthogonal design of type $(2, 2)$ in order $4s + 2$, contradictory to the inductive hypothesis.

So $a = 0$. Using row and column operations, we can put A in the form $A = \begin{bmatrix} A' & 0 \\ 0 & B \end{bmatrix}$ where A' is 8×8 and B is an orthogonal design of type $(2, 2)$ in order $4(s - 1) + 2$, again an impossibility.

PROPOSITION 4.2. *Suppose X and Y are amicable orthogonal designs in order $n \equiv 0 \pmod 4$ where X is of type $(1, 1, 1, a_1, \ldots, a_s)$ and Y is of type $(b_1, \ldots, b_t)$. Then there exists an orthogonal design in order n of type $(1, b_1, \ldots, b_t)$.*

Proof. Let $X = \sum_1^{s+3} A_i x_i$. Then by applying row and column operations to X and Y simultaneously, we can assume that

$$A_1 = \bigoplus_{n/4} \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}, \quad A_2 = \bigoplus_{n/4} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix},$$

$$A_3 = \bigoplus_{n/4} \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}.$$

The relations $A_i Y^t = Y A_i^t$ $i = 1, 2, 3$ now will force Y to be skew-symmetric and $I_n x + Y$ is the required orthogonal design.

This is the first combinatorial result on the types of amicable orthogonal designs in order n, $n \equiv 0 \pmod 4$. It precludes the existence of certain amicable pairs which are not eliminated by algebraic techniques. For example, a pair of orthogonal designs of type (1, 1, 1) and (1, 1, 16) in order 20 does not contradict the condition of Theorem 3.2. Yet, the existence of such an amicable pair would, by the proposition, imply that there exists an orthogonal design of type (1, 1, 1, 16) in order 20 and this is impossible. The existence problem for amicable pairs certainly has the di-polarity between algebraic and combinatorial properties that we noted for orthogonal designs. To date we have found only a few results in the spirit of the above proposition, but each one seems so unique that we believe that there is a rich and complex combinatorial theory in this area.

PROPOSITION 4.3. *Suppose X is an orthogonal design in order n, $n \equiv 0 \pmod 4)$, $n \neq 4$, and of type $(1, 1, n-2)$. If Y is an orthogonal design in order n and of type $(u_1, \ldots, u_s)$ and such that $XY^t = YX^t$, then $u_i \neq 1$ for any i.*

Proof: Write $X = A_1x_1 + A_2x_2 + A_3x_3$, $Y = \sum_1^s B_j y_j$ where $A_i A_i^t = I_n$, $i = 1, 2$, $A_3 A_3^t = (n-2) I_n$ and $B_j B_j^t = u_j I_n$. We may assume that $A_1 = \bigoplus \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ and $A_2 = \bigoplus \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Careful consideration of the relations $A_3 A_i^t + A_i A_3^t = 0$ and $B_j A_i^t = A_i B_j^t$ for $i = 1, 2$ will lead the patient and persistent reader to conclude that A_3 and all the B_j's are split into blocks of 2×2 matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$. Under the usual representation of the complex numbers as 2×2 matrices, this matrix corresponds to the complex number $a + bi$. Thus, we may identify A_3 and B_j, $j = 1, \ldots, s$ with matrices of order $n/2$ and with entries $a + bi$, a, b in the set $\{0, \pm 1\}$. The reader should also observe that, then,

(i) $A_3 = -A_3^t$, $B_j = B_j^t$ $\quad j = 1, \ldots, s$
(ii) $A_3 A_3^* = (n-2) I_{n/2}$, $B_j B_j^* = u_j I_{n/2}$ $\quad j = 1, \ldots, s$
(iii) $A_3 B_j^* = B_j A_3^*$ $\quad j = 1, \ldots, s$.

https://doi.org/10.4153/CJM-1976-099-5 Published online by Cambridge University Press

Note that (i) and (ii) assert that, if $a + bi$ is an entry in A_3 not on the diagonal, then neither a nor b is a zero.

Assume that one of the u_i's, say u_1, is 1. Then the entries in B_1 must be from the set $\{0, \pm 1, \pm i\}$ with one non-zero entry in each row and column. We claim that B_1 must be a diagonal matrix. For suppose there is a non-zero entry in the i, j position and let z_{ij} be the corresponding entry in A_3. Then, from (iii), we find that $z_{ij} = \pm \bar{z}_{ij}$ and hence is either real or pure imaginary. But, as we have noted, the only such entries in A_3 are the zero diagonal entries and hence z_{ij} occurs on the diagonal i.e. $i = j$.

Now we attempt to construct the matrix B_1. We may assume the first diagonal entry is 1. Then, if x is the next diagonal entry, $x = \pm 1$ or $\pm i$ and (iii) implies $z_{12}\bar{x} = -\bar{z}_{12}$ where z_{12} is the entry in A_3. We see that $x \neq \pm 1$ and so $x = \pm i$. Let y be the third diagonal entry. Now (iii) will give that $z_{13}\bar{y} = -\bar{z}_{13}$ and $z_{23}\bar{y} = \pm i\bar{z}_{23}$, clearly an impossible situation.

The above proposition arose from the false hope that, for $n = 2^a$, one could always find a pair of amicable designs in order n both of type $(1, 1, 2, 4, \ldots, 2^{a-1})$. These pairs would be especially nice as they use the maximum number of variables for an amicable pair in order n and give a double binary system for finding all possible pairs of amicable orthogonal designs, each with two variables. However, the existence of the pair both of type $(1, 1, 2 \ldots, 2^{a-1})$ would imply the existence of a pair of types $(1, 1, 2^a - 2)$ and $(1, k)$ which is impossible for $a > 2$. The amicable orthogonal designs of types $(1, 1)$ in order 2 and types $(1, 1, 2)$ in order 4 are the only exceptions.

References

1. J. F. Adams, P. D. Lax, and J. S. Phillips, *On matrices whose real linear combinations are non-singular*, Proc. A.M.S. *16* (1965), 318–322.

2. W. K. Clifford, *Applications of Grassman's extensive algebra*, Amer. J. Math. *1* (1878), 350–358.

3. A. V. Geramita, and N. J. Pullman, *A theorem of Hurwitz and Radon and orthogonal projective modules*, Proc. A.M.S. *42* (1974), 51–58.

4. A. V. Geramita, J. M. Geramita, and J. S. Wallis, *Orthogonal designs*, to appear, Journal of Linear and Multilinear Algebra.

5. Y. Kawada, and N. Iwahori, *On the structure and representations of Clifford algebra*, J. Math. Soc. Japan *2* (1950), 34–43.

6. T. Y. Lam, *The algebraic theory of quadratic forms*, Math. Lecture Notes Series (Benjamin, Reading, Mass., 1973).

7. Dan Shapiro, *Rational spaces of similarities*, unpublished.

8. ——— *Spaces of similarities I: the Hurwitz problem*, pre-print.

9. ——— *Spaces of similarities IV: (s, t) families*, pre-print.

10. E. Witt, *Theorie der quadratischen Formen in beliebigen Korpern*, Crellee J. *176* (1937), 31–44.

11. W. Wolfe, *Rational quadratic forms and orthogonal designs*, to appear, J. Number Theory.

University of Alberta,
Edmonton, Alberta