J. Austral. Math. Soc. (Series A) 30 (1981), 297–306

INTEGRAL QUADRATIC FORMS AND ORTHOGONAL DESIGNS

PETER EADES

(Received 1 May 1980)

Communicated by W. D. Wallis

Abstract

Warren W. Wolfe obtained necessary conditions for the existence of orthogonal designs in terms of rational matrices. In this paper it is shown that these necessary conditions can be obtained in terms of integral matrices. In the integral form, Wolfe's theory is more useful in the construction of orthogonal designs.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): primary 05 B 20.

0. Introduction

An $n \times n$ matrix A with entries from the commuting variables 0, $\pm x_1, \pm x_2, \ldots, \pm x_u$, is called an *orthogonal design* of type $(s_1, s_2, \ldots, s_u)$ and order n if

$$AA^t = \sum_{i=1}^{u} s_i x_i^2 I_n.$$

The study of orthogonal designs has arisen from problems in Hadamard matrices, weighing matrices and Baumert-Hall arrays (see [4]). Most of this study is directed toward a solution of the existence problem: given parameters $n, s_1, s_2, \ldots, s_u$, does there exist an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order n? This problem is clearly equivalent to finding $n \times n$ matrices $A_1, A_2, \ldots, A_u$, which satisfy

(0.1) $A_i * A_j = 0$ for $i \neq j$ ($*$ denotes Hadamard product),

(0.2) the entires of each A_i are from $\{0, 1, -1\}$,

https://doi.org/10.1017/S1446788700017195 Published online by Cambridge University Press

(0.3) $A_iA_i^t = s_iI_n$ for $1 \leqslant i \leqslant u$,

(0.4) $A_iA_j^t + A_jA_i^t = 0$ for $i \neq j$.

The equations (0.3) and (0.4) reflect the algebraic properties of orthogonal designs. Radon [9] showed that if $A_1, A_2, \ldots, A_u$ are real $n \times n$ matrices satisfying (0.3) and (0.4), then $u \leqslant \rho(n)$, where ρ (the *Radon function*) is defined as follows. Suppose that $n = 2^ab$, and $a = 4c + d$, where b is odd and $0 \leqslant d \leqslant 3$. Then $\rho(n) = 8c + 2^d$.

A rational family of type $(s_1, s_2, \ldots, s_u)$ *and order* n is a set $\{A_1, A_2, \ldots, A_u\}$ of $n \times n$ rational matrices which satisfy (0.3) and (0.4).

The following theorem uses rational families to give a necessary condition for the existence of orthogonal designs. The theorem follows from the results of Wolfe [11] and Shapiro [10].

(0.5) Rational Family Theorem [4]. *Suppose that $n = 2^ab$ where b is odd and $0 \leqslant a \leqslant 3$. Then there is a rational family of type $(s_1, s_2, \ldots, s_u)$ and order n if and only if*

(0.6) *there is a $u \times 2^a$ rational number P such that*

$$PP^t = \operatorname{diag}(s_1, s_2, \ldots, s_u).$$

Wolfe showed how the Hasse–Minkowski classification of rational quadratic forms can be applied to (0.6) to provide a useful necessary condition for the existence of orthogonal designs. Much effort has been spent in attempting to determine precisely when (0.6) is sufficient for the existence of an orthogonal design (see [4]).

A rational family which consists of integral matrices shall be called an *integral family*. An integral familly shall be called *combinatorial* if it satisfies (0.1). A necessary and sufficient condition for the existence of an integral family of order not divisible by 16 is given in this paper. This condition is shown to be often sufficient for the existence of a combinatorial integral family. This is of interest because a combinatorial integral family is not very different from an orthogonal design. If $\{A_1, A_2, \ldots, A_u\}$ is a combinatorial integral family of type $(s_1, s_2, \ldots, s_u)$ and $x_1, x_2, \ldots, x_u$, are commuting variables, then $A = \Sigma_{i-1}^u x_iA_i$ has entries from $\{mx_i: m \in Z, 1 \leqslant i \leqslant u\}$ and

$$AA^t = \Sigma_{i=1}^u s_ix_i^2I.$$

Precisely, the following two theorems are proved.

(0.7) Main Theorem A. *Suppose that $s_1, s_2, \ldots, s_u$, are positive integers, b is an odd positive integer, and $0 \leqslant a \leqslant 3$. Then a necessary and sufficient condition for the existence of an integral family of type $(s_1, s_2, \ldots, s_u)$ and order 2^ab is*

https://doi.org/10.1017/S1446788700017195 Published online by Cambridge University Press

(0.8) *there is a* $u \times 2^a$ *integral matrix* Q *such that*

$$QQ' = \operatorname{diag}(s_1, s_2, \ldots, s_u).$$

(0.9) Main Theorem B. *If* $0 \leqslant a \leqslant 2$ *and* $b \geqslant u$ *then* (0.8) *is a necessary and sufficient condition for the existence of a combinatorial integral family of type* $(s_1, s_2, \ldots, s_u)$ *and order* $2^a b$.

Necessity in the two main theorems is proved in Section 1 by showing that for $0 \leqslant a \leqslant 3$, (0.6) implies (0.8). Sufficiency is proved in Section 2.

(0.10) Remark. The Radon number bound shows that the added hypothesis $b \geqslant u$ in Main Theorem B excludes only combinatorial integral families of order less than 16. These excluded cases are of little interest since the existence problem for orthogonal designs is completely solved for such orders.

(0.11) Remark. The integral condition (0.8) has at least two advantages over its rational counterpart (0.6). Firstly, it is often easier to construct an integral matrix Q satisfying $QQ' = \operatorname{diag}(s_1, s_2, \ldots, s_u)$ than to prove that such a matrix exists by using the Hasse–Minkowski theory. Secondly, the integral matrix Q can be used as a starting point in an algorithm to construct the orthogonal design in question. This algorithm, described in [1], has been used successfully to construct many orthogonal designs of orders 20 and 28.

1. The integer matrix conjecture

The following conjecture originally arose from a study of the Goethals–Seidel method for constructing orthogonal designs (see [1]).

(1.1) Integer Matrix Conjecture. *Suppose that* $s_1, s_2, \ldots, s_u$, *are positive integers. If the matrix equation*

$$XX' = \operatorname{diag}(s_1, s_2, \ldots, s_u) \tag{1.2}$$

has a rational $u \times n$ *solution then it has an integral* $u \times n$ *solution.*

In this section we prove

(1.3) Proposition. *The Integer Matrix Conjecture is true for* $u \leqslant n \leqslant 8$.

It follows that for $a \in \{0, 1, 2, 3\}$ the conditions (0.6) and (0.8) are equivalent, and necessity in Main Theorem A and B is established.

https://doi.org/10.1017/S1446788700017195 Published online by Cambridge University Press

The author does not know whether the Integer Matrix Conjecture holds for any value $n \geqslant 9$. However, for $n \leqslant 7$, a stronger result may be proved.

(1.4) Proposition. *Suppose that A is a nonsingular integral matrix and the matrix equation*

$$XX^t = A \tag{1.5}$$

has a rational $u \times n$ solution, where $u \leqslant n \leqslant 7$. Then (1.4) *has an integral $u \times n$ solution.*

(1.6) Remarks. The proof given below for Proposition (1.4) was presented by Gordon Pall at the Conference on Quadratic Forms at Queen's University, Kingston, Ontario, in 1976. The author is grateful to Professor Pall for his kind permission to use his work.

J. S. Hsia [6] has independently obtained proofs of Propositions (1.3) and (1.4) using the language of lattices. In fact, Hsia's results give information about the case $n \geqslant 8$ as well.

The proof of Propositions (1.3) and (1.4) uses the classical theory of integral quadratic forms. We shall begin by revising some terminology. The rational quadratic forms are *rationally equivalent* if there is a nonsingular rational linear transformation which takes one to the other. Thus, for instance, if there is a $u \times u$ rational matrix P such that $PP^t = \operatorname{diag}(s_1, s_2, \ldots, s_u)$, then the form $x_1^2 + x_2^2 + \cdots + x_u^2$ is rationally equivalent to $s_1x_1^2 + s_2x_2^2 + \cdots + x_ux_u^2$. Two integral quadratic forms are *integrally equivalent* or in the *same class*, if there is a nonsingular integral linear transformation of determinant 1 which takes one to the other.

A form shall be called *classic* if it has an integral matrix. A classic form f shall be called *c-reducible* if there is an integral linear transformation which takes a classic form g to f, where $|\det g| < |\det f|$. In matrix terms, the form f with matrix F is c-reducible if there is an integral matrix G and a nonsingular integral matrix T such that $F = TGT^t$ and $|\det F| > |\det G|$. A classic form which is not c-reducible is c-irreducible.

The following lemma is central to the proof of Proposition (1.4).

(1.7) Lemma. *If two c-irreducible forms are rationally equivalent, then they have the same determinant.*

Because the proof of this proposition is long and tedious, it is left until the end of this section. First we show how to obtain Proposition (1.3) and (1.4).

Consider the case $u = n \leqslant 7$. Suppose that there is a $u \times u$ rational solution to (1.4), that is, the form f with matrix A is rationally equivalent to $x_1^2 + x_2^2 + \cdots + x_u^2$. Since f is classic, there is a c-irreducible form g and a nonsingular

https://doi.org/10.1017/S1446788700017195 Published online by Cambridge University Press

integral linear transformation which takes g to f. Clearly g is rationally equivalent to $x_1^2 + x_2^2 + \cdots + x_u^2$; hence, by Proposition (1.6), g has determinant 1. Now a theorem of Hermite (Jones [7], p. 60) implies that there is only one class of positive definite classic forms of determinant 1 with $u \leqslant 7$ variables. So g is integrally equivalent to $x_1^2 + x_2^2 + \cdots + x_u^2$. The composition of this equivalence transformation with the transformation from g to f has an integral matrix Q which satisfies $QQ' = A$.

Now suppose that $u < n \leqslant 7$, and P is a rational $u \times n$ solution to (1.5). Let m be an integer such that mP is integral. Let V be an $(n - u) \times n$ matrix whose rows form a basis of the orthogonal complement of the rowspace of P in rational n-space. Suppose that k is an integer such that kV is integral. If U denotes the $n \times n$ integral matrix whose transpose is (P', mkV'), then UU' is integral. From the case $u = n$ proved above there is an $n \times n$ integral matrix Y such that $YY' = UU'$. The first u rows of Y form an integral $u \times n$ solution to (1.5). This completes the proof of Proposition (1.4) (except for the proof of Lemma (1.7)).

There is more than one class of positive definite classic forms of determinant 1 with 8 variables [8]. However, it is well known (see [8]) that an integral form is integrally equivalent to $x_1^2 + x_2^2 + \cdots + x_8^2$ if and only if it represents an odd number. So using the same argument as in the case $n < 8$, we can show that if one s_i, $1 \leqslant i \leqslant 8$, is odd, then the existence of an 8×8 rational solution to (1.2) implies the existence of an 8×8 integral solution. To prove the Integer Matrix Conjecture (1.1) for $n = u = 8$, only 8-tuples $(s_1, s_2, \ldots, s_8)$ of even integers need be considered. Clearly the s_i can be assumed to be squarefree, and so we consider only the case $s_i \equiv 2 \pmod 4$ for $1 \leqslant i \leqslant 8$. A standard Hasse-symbol argument shows that $s_1x_1^2 + s_2x_2^2 + \cdots + s_8x_8^2$ is rationally equivalent to $\frac{1}{2}(s_1x_1^2 + s_2x_2^2 + \cdots + s_8x_8^2)$. So, if there is a rational 8×8 solution to (1.2), then there is a rational 8×8 matrix P such that $PP' = \frac{1}{2}\operatorname{diag}(s_1, s_2, \ldots, s_8)$. Because $\frac{1}{2}s_1$ is odd, there is an 8×8 integral matrix S such that $SS' = \frac{1}{2}\operatorname{diag}(s_1, s_2, \ldots, s_8)$. The product Q of S with

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times I_4 \quad \text{(Kronecker product)}$$

satisfies $QQ' = \operatorname{diag}(s_1, s_2, \ldots, s_8)$.

The case $u < n = 8$ follows since any set of mutually orthogonal vectors in rational 8-space can be completed to an orthogonal basis.

It remains only to prove Lemma 1.7.

Suppose that f is a c-irreducible form. We will show that

(1.8) $\det f$ is not divisible by 4;

and if p is an odd prime then

(1.9) p^3 does not divide $\det f$,

https://doi.org/10.1017/S1446788700017195 Published online by Cambridge University Press

and

(1.10) if p^2 divides $\det f$ then $c_p(f) = -1$,

and

(1.11) if p does not divide $\det f$ then $c_p(f) = 1$.

(The Hasse symbol at p is denoted by c_p.)

A theorem of Hasse–Minkowski implies that if f_1 and f_2 are rationally equivalent forms, then the squarefree parts of $\det f_1$ and $\det f_2$ are equal and $c_p(f_1) = c_p(f_2)$ for each prime p. If f_1 and f_2 are c-irreducible then it follows from (1.8) to (1.11) that $\det f_1 = \det f_2$.

Firstly we prove (1.8). Suppose that 4 divides $\det f$, and choose r so that the largest power of 2 dividing $\det f$ is less than 2^r. Now f is integrally equivalent to a form g such that

$$g \equiv a_1h_1 + a_2h_2 + \cdots + a_mh_m \pmod{2^n}, \tag{1.12}$$

where the a_i are integers and each h_i has shape either $2xy$, $2x^2 + 2xy + 2y^2$ or x^2, and the variables of distinct h_i's are distinct (Jones [7], p. 110). (By $f_1 \equiv f_2 \pmod{v}$ we mean that the corresponding coefficients of f_1 and f_2 are equal modulo v.)

Now each term in (1.12) has odd determinant; if 4 divides $\det f$ then one of the following must hold. Either

(1.13) 2 divides a_i for some h_i of shape $2xy$;

or

(1.14) 4 divides a_i for some h_i of shape x^2;

or

(1.15) 2 divides a_i for some h_i of shape $2x^2 + 2xy + 2y^2$

or

(1.16) $a_i \equiv a_j \equiv 2 \pmod 4$ for some diagonal components h_i and h_j.

It is clear that neither (1.13) nor (1.14) can hold for the c-irreducible form f.

Suppose that (1.15) holds. The transformation T with matrix

$$\begin{bmatrix} 2 & 0 \\ 1 & 1 \end{bmatrix}$$

takes $x^2 + 3y^2$ to $4x^2 + 4xy + 4y^2$. Since T has determinant 2 and f contains a term $4x^2 + 4xy + 4y^2 \pmod{2^r}$, f is c-reducible, contrary to hypothesis. A similar argument shows that (1.16) is impossible.

Hence 4 does not divide $\det f$.

For (1.9), (1.10) and (1.11) a similar method may be employed. Suppose that p is an odd prime. Choose r so that the highest power of p which divides $\det f$ is less than p^r. Now f is integrally equivalent to a form g which is diagonal modulo p^r (see Jones [7], p. 110). Since f is c-irreducible, p^2 does not divide any of the diagonal coefficients of g. Using elementary methods we can show that a diagonal form with coefficients prime to p is integrally equivalent to a form

https://doi.org/10.1017/S1446788700017195 Published online by Cambridge University Press

which has shape $x_1^2 + x_2^2 + \cdots + kx_3^2$ modulo p^r, where $(k, p) = 1$. Thus the form

$$(1.17) \quad h = x_1^2 + x_2^2 + \cdots + x_{s-1}^2 + kx_s^2 + p(y_1^2 + y_2^2 + \cdots + y_{w-1}^2 + ly_2^2)$$

is considered, where k and l are prime to p. Now h has many of the properties of f: a power of p divides det h if and only if it divides det f; f is c-reducible if h is c-reducible by a transformation of determinant $\pm p$; and $c_p(f) = c_p(h)$.

Suppose that (1.9) is false, that is, p^3 divides det f. Then $w \geqslant 3$ and integers a and b can be found such that the form

$$h' = px^2 - 2axz + pz^2 - 2byz + (a^2 + b^2 + l)z^2/p$$

is classic. The transformation

$$\begin{bmatrix} 1 & & a \\ & 1 & b \\ & & p \end{bmatrix}$$

has determinant p and takes h to h'. Thus $w \geqslant 3$ is impossible and p^3 does not divide det f.

Suppose that p^2 divides det f; then $w = 2$. If $c_p(f) = 1$, then an easy calculation shows that $-l$ is a square modulo p^r. Hence there is an integer d such that

$$px^2 + ply^2 \equiv px^2 - d^2py^2 \pmod{p^r}.$$

Since $(l, p) = 1$, $d \not\equiv 0 \pmod{p^r}$, and so there are integers e and q such that $de = 1 + qp$. The transformation with matrix

$$\begin{bmatrix} d & p \\ 1 & 0 \end{bmatrix}$$

has determinant $-p$ and takes the classic form

$$d^2px^2 - 2d^2xy + ey^2$$

to $px^2 - d^2py^2$. Hence f is c-reducible contrary to assumption; so $c_p(f) = -1$.

Finally, if p does not divide det f then $w = 0$ and an easy calculation shows that $c_p(f) = 1$.

This completes the proof of Lemma 1.7.

2. Combinatorial integral families

Geramita and Pullman [3] showed that for each n there is an orthogonal design of type $(1, 1, \ldots, 1)$ and order n on $p(n)$ variables. Sufficiency in Main Theorem A may be deduced using the following method. Suppose that $n = 2^a b$ where $0 \leqslant a \leqslant 3$ and b is odd; for convenience denote 2^a by r. Note that $p(n) = r$. Let $\{P_1, P_2, \ldots, P_r\}$ be the rational family corresponding to the

Geramita–Pullman orthogonal design. Suppose that Q is a $u \times r$ integral matrix such that

$$QQ^t = \operatorname{diag}(s_1, s_2, \ldots, s_u).$$

If q_{ij} is the ijth entry of Q then the matrices

$$\sum_{i=1}^{r} q_{ij} P_j, \qquad 1 \leqslant i \leqslant u,$$

form an integral family of type $(s_1, s_2, \ldots, s_u)$ and order n.

For $a = 0$ it is trivial that the integral family above is combinatorial. For $a > 0$ and $b \geqslant u$ consider the sequences

$$c_j = (q_{ij}x_1, q_{2j}x_2, \ldots, q_{uj}x_u, 0_{b-u}),$$

where the x_i are commuting variables and 0_{b-u} denotes a sequence of $b - u$ zeros. Denote by A_j the $b \times b$ circulant matrix with first row c_j. It is easy to check that

$$\text{(2.1)} \qquad \sum_{j=1}^{r} A_j A_j^t = \sum_{i=1}^{u} s_i x_i^2 I_b.$$

Let R denote the backdiagonal matrix, that is, R has 1 in the $(i, b - i + 1)$th position for $1 \leqslant i \leqslant b$, and zeros elsewhere. In the case $a = 1$, consider the $2b \times 2b$ matrix

$$M = \begin{bmatrix} A_1 & A_2R \\ -A_2R & A_1 \end{bmatrix}.$$

From (2.1), $MM^t = \Sigma_{i=1}^{u} s_i x_i^2 I_{2b}$, and M has entries from $\{mx_i : m \in Z, 1 \leqslant i \leqslant u\}$. Hence M gives a combinatorial integral family of type $(s_1, s_2, \ldots, s_u)$ and order $2b$. For $a = 2$, the Goethals–Seidel array [5]

$$\begin{bmatrix} A_1 & A_2R & A_3R & A_4R \\ -A_2R & A_1 & A_4^tR & -A_3^tR \\ -A_3R & -A_4^tR & A_1 & A_2^tR \\ -A_4R & A_3^tR & -A_2^tR & A_1 \end{bmatrix}$$

can be used to obtain a combinatorial integral family of type $(s_1, s_2, \ldots, s_u)$ and order $4b$.

Finally we give a combinatorial condition to determine when combinatorial integral families constructed by the method above are orthogonal designs.

(2.2) PROPOSITION. *Suppose* $X_1, X_2, \ldots, X_u$, *are integral circulant* $b \times b$ *matrices such that*

$$\text{(2.3)} \qquad \sum_{i=1}^{u} X_i X_i^t = cI_B.$$

https://doi.org/10.1017/S1446788700017195 Published online by Cambridge University Press

Write $X_i = Y_i - Z_i$, where Y_i and Z_i have nonnegative entries, and denote by y_i and z_i the rowsums of Y_i and Z_i respectively. Then

$$c = \sum_{i=1}^{u} (y_i - z_i)^2 \tag{2.4}$$

and the X_i have entries from $\{0, 1, -1\}$ if and only if

$$c = \sum_{i=1}^{u} (y_i + z_i). \tag{2.5}$$

Proof. A standard rowsum argument gives (2.4), and, if the X_i have entries from $\{0, 1, -1\}$, then (2.5) is immediate. Conversely, suppose that (2.5) holds, and let $x_i = (x_{1i}, x_{2i}, \ldots, x_{bi})$ denote the first row of X_i. Clearly

$$y_i + z_i = \sum_{j=1}^{b} |x_{ji}|.$$

Hence by (2.5),

$$c = \sum_{i=1}^{u} \sum_{j=1}^{b} |x_{ji}|,$$

but also

$$c = \sum_{i=1}^{u} \sum_{j=1}^{b} |x_{ji}|^2$$

by considering the scalar products the first row of each X_i with itself. Hence

$$\sum_{i=1}^{u} \sum_{j=1}^{b} |x_{ji}|(|x_{ji}| - 1) = 0.$$

But each term in this sum is nonnegative. Hence $x_{ji} \in \{0, 1, -1\}$ for $1 \leqslant j \leqslant b$ and $1 \leqslant i \leqslant u$.

References

[1] P. Eades (1977), 'Orthogonal designs constructed from circulants', *Utilitas Math.* **11**, 43–55.

[2] D. Estes and G. Pall (1970), 'The definite octonary quadratic forms of determinant 1', *Illinois J. Math.* **14**, No. 1.

[3] A. V. Geramita and N. J. Pullman (1974), 'A theorem of Hurwitz and Radon and orthogonal projective modules', *Proc. Amer. Math. Soc.* **42**, 51–56.

[4] A. V. Geramita and J. Seberry (1979), *Orthogonal designs* (Lecture Notes in Pure and Applied Mathematics 45, Marcel Dekker, New York and Basel).

[5] J. M. Goethals and J. J. Seidel (1970), 'A skew-Hadamard matrix of order 36', *J. Austral. Math. Soc.* **11**, 343–344.

[6] J. S. Hsia (1977–78), 'Two theorems on integral matrices', *Linear and Multilinear Algebra* **5**, 257–264.

https://doi.org/10.1017/S1446788700017195 Published online by Cambridge University Press

[7] B. W. Jones (1950), *The arithmetic theory of quadratic forms*, Carus Mathematical Monographs 10 (John Wiley and Sons).

[8] M. Kneser (1957), 'Klassenzahlen definiter quadratischer Formen', *Arch. Math.* **8**, 241–250.

[9] J. Radon (1922), 'Linear scharen orthogonaler matrixen', *Abh. Math. Sem. Univ. Hamburg.* **1**, 1–14.

[10] D. Shapiro (1974), *Similarities, quadratic forms and Clifford algebras* (Ph.D. Thesis, University of California, Berkeley).

[11] W. Wolfe (1977), 'Rational quadratic forms and orthogonal designs', *Number theory and algebra* edited by H. Zassenhaus (Academic Press, New York, San Franciso, London).

Department of Pure Mathematics
School of General Studies
Australian National University
Box 4, Canberra, A.C.T. 2600
Australia

Department of Computer Science
University of Queensland
St. Lucia
Queensland 4067
Australia

https://doi.org/10.1017/S1446788700017195 Published online by Cambridge University Press