ON THE EXISTENCE OF ORTHOGONAL DESIGNS

Peter Eades

A thesis submitted for the degree of

Doctor of Philosophy

at the

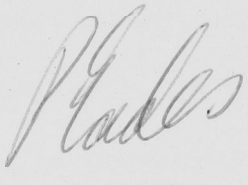
Australian National University

Canberra

July 1977

STATEMENT

The results presented in this thesis are my own, except where otherwise stated.



Peter Eades

ACKNOWLEDGEMENTS

It is a great pleasure to thank my supervisor Jennifer Seberry for her constant help, advice and encouragement during my research. I am also grateful to John Cossey, Peter J. Robinson and many other mathematicians at the Australian National University for providing a stimulating atmosphere in which to work.

I also acknowledge the financial support of the Australian Government and the Australian National University.

I extend special thanks to Mrs Barbara Geary for her skilful typing.

Finally I would like to thank my wife Diana without whose support this thesis would not have been possible.

ABSTRACT

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

$$AA^t = \left(\sum_{i=1}^{u} s_i x_i^2\right) I \ .$$

The existence question for orthogonal designs stems from many problems originating in fields as diverse as algebraic topology and coding theory. A brief history of the existence question is included in the Introduction.

Wolfe [79] and Shapiro [63] have recently found effective necessary and sufficient conditons for the existence of orthogonal designs in terms of rational matrices. Subsequent research has been directed mainly toward the question of determining precisely when these necessary conditions suffice for existence.

This question is answered in many particular cases by the direct construction of orthogonal designs in Chapter 2. A method which searches for an orthogonal design of given parameters is presented. This method has been implemented by hand and by computer to construct a large number of previously unknown orthogonal designs. Some related techniques are used to construct infinite families of orthogonal designs.

In Chapter 3 two different asymptotic existence results are proved. Firstly, it is shown that if all of $n, s_1, s_2, \ldots, s_u$ are sufficiently divisible by 2, then often the existence of an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order n can be deduced. Secondly, the Wolfe-Shapiro necessary conditions are shown to be often sufficient for the existence of orthogonal designs with few nonzero entries.

A kind of integral analogue to the Wolfe-Shapiro theory is presented in

Chapter 4. As a consequence, it is shown that the Wolfe-Shapiro necessary conditions suffice for the existence of an $n \times n$ matrix A with entries from $\{mx_i : 1 \leq i \leq u, m \in \mathbb{Z}\}$ such that $AA^t = \left(\sum_{i=1}^{u} s_i x_i^2\right) I$. This is important because such a matrix resembles an orthogonal design.

In Chapter 5 the power of the results in previous chapters, especially Chapter 2, is illustrated by the tabulation of numerical results.

Many of the results in this thesis can be found in the published papers of the author.

TABLE OF CONTENTS

INTRODUCTION

THE EXISTENCE PROBLEM

The following definition was formulated in 1973 by Geramita, Geramita and Wallis [24] in order to unify some algebraic and combinatorial concepts.

DEFINITION. *An orthogonal design of order* n *and type* $(s_1, s_2, \ldots, s_u)$ *on the commuting variables* $x_1, x_2, \ldots, x_u$, *is an* $n \times n$ *matrix* A *with entries from* $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ *such that*

$$AA^t = \left(\sum_{i=1}^{u} s_i x_i^2\right) I \ . \tag{0.0.1}$$

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

Special kinds of orthogonal designs were studied for many years before 1973. Jacques Hadamard [36] in 1893 showed that the determinant of a real $n \times n$ matrix with entries from the interval $[-1, 1]$ has absolute value at most $n^{\frac{1}{2}n}$. Matrices which achieve this bound have subsequently been called *Hadamard matrices*. It is clear from (0.0.1) that an orthogonal design of type (n) and order n gives an example of an Hadamard matrix. Hadamard proved the converse: every Hadamard matrix has mutually orthogonal rows and entries from $\{-1, 1\}$. Also, he showed that the order of an Hadamard matrix is either $1, 2$, or divisible by 4. The question of whether there is an Hadamard matrix for each order divisible by 4 is open. This problem has received a great deal of attention in recent years because of its implications in other areas of combinatorics, such as balanced incomplete block designs [38], tournaments ([52], [66]) and codes [7].

An orthogonal design of type $(1, 1, 1, 1)$ and order 4,

$$\begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ -x_2 & x_1 & x_4 & -x_3 \\ -x_3 & -x_4 & x_1 & x_2 \\ -x_4 & x_3 & -x_2 & x_1 \end{bmatrix} \tag{0.0.2}$$

was used by Williamson in 1944 to construct Hadamard matrices. If X_1, X_2, X_3, X_4, are $v \times v$ matrices with entries from $\{-1, 1\}$ such that $X_i X_j^t = X_j X_i^t$ for $1 \le i < j \le 4$ and $X_1X_1^t + X_2X_2^t + X_3X_3^t + X_4X_4^t = 4vI$, then replacing the variable x_i by X_i in (0.0.2) yields an Hadamard matrix of order $4v$. Baumert and Hall [4] used orthogonal designs of type (b, b, b, b) and order $4b$ in a similar fashion to construct Hadamard matrices of order $4vb$. Such orthogonal designs have subsequently been called *Baumert-Hall arrays*, and have received considerable attention (see [75], [10]). Turyn [68] has shown that constructions for Baumert-Hall arrays are related to problems in signal detection.

Another special kind of orthogonal design was introduced by Raghavarao [50] in 1959 in connection with a weighing problem. A *weighing matrix of weight* k *and order* n is an $n \times n$ matrix with entries from $\{0, 1, -1\}$ such that $WW^t = kI$. Thus a one variable orthogonal design gives a weighing matrix; in particular, an Hadamard matrix of order n is a weighing matrix of weight n and order n. Raghavarao demonstrated that a weighing matrix describes a method of weighing n objects k at a time to obtain an error distribution with small variance. Taussky [67] suggested the study of weighing matrices as a natural extension of the study of Hadamard matrices. In recent years weighing matrices have been used in connection with Pless symmetry codes [6], in designing telephone conference networks [5], and in the design of masks for optical spectrometers ([65], [43]). Also, weighing matrices are related to problems in finite projective

geometry ([37], [35]) and graph theory [34].

Geramita and Pullman [25] introduced orthogonal designs of type $(1, 1, 1, \ldots, 1)$ in 1973 as a realization of the maximal number of independent vector fields on the n sphere. The problem was solved completely by the topologist J.F. Adams [1] in 1962. However, it can be stated in terms of an earlier problem of Hurwitz [42] and Radon [49] as follows (see [2]): *What is the maximal number of real skew-symmetric* $n \times n$ *matrices* A_i *such that* $A_i^2 = -I$ *for each* i *and* $A_iA_j = -A_jA_i$ *for each* $i \neq j$? Now suppose that A is an orthogonal design of type $(1, 1, 1, \ldots, 1)$ and order n on the variables $x_1, x_2, \ldots, x_u$. Write A as $x_1P_1 + x_2P_2 + \ldots + x_uP_u$ where the entries of the P_i are from $\{0, 1, -1\}$. Then the equation

$$AA^t = \left(\sum_{i=1}^{u} x_i^2\right) I$$

ensures that the matrices $A_i = P_1^{-1}P_i$ $(2 \leq i \leq u)$ satisfy the requirements above. Hence by finding orthogonal designs of type $(1, 1, 1, \ldots, 1)$ on a maximal number of variables, Geramita and Pullman gave a neat combinatorial solution to the Hurwitz-Radon problem.

Some other special kinds of orthogonal designs are discussed by Taussky [67]. In particular, she notes that the orthogonal designs

$$\begin{bmatrix} x_1 \end{bmatrix},$$

$$\begin{bmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{bmatrix},$$

$$\begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ -x_2 & x_1 & x_4 & -x_3 \\ -x_3 & -x_4 & x_1 & x_2 \\ -x_4 & x_3 & -x_2 & x_1 \end{bmatrix},$$

$$\begin{bmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ -x_2 & x_1 & x_4 & -x_3 & x_6 & -x_5 & x_8 & -x_7 \\ -x_3 & -x_4 & x_1 & x_2 & x_7 & -x_8 & -x_5 & x_6 \\ -x_4 & x_3 & -x_2 & x_1 & -x_8 & -x_7 & x_6 & x_5 \\ -x_5 & -x_6 & -x_7 & x_8 & x_1 & x_2 & x_3 & -x_4 \\ -x_6 & x_5 & x_8 & x_7 & -x_2 & x_1 & -x_4 & -x_3 \\ -x_7 & -x_8 & x_5 & -x_6 & -x_3 & x_4 & x_1 & x_2 \\ -x_8 & x_7 & -x_6 & -x_5 & x_4 & x_3 & -x_2 & x_1 \end{bmatrix},$$

give representations of the real numbers, complex numbers, quaternions and Cayley numbers respectively. The fact that these four are essentially the only orthogonal designs of type $(1, 1, \ldots, 1)$ and order n on n variables is related to the theorem of Bott and Milnor [9] which says that the only division algebras over the reals have dimensions $1, 2, 4$ and 8.

The *existence question* is central to all the particular studies of orthogonal designs mentioned above:

(0.0.3) *For which 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 thesis is motivated primarily by the search for an answer to this question. Of course the question is open; for example it includes the problem of Hadamard matrices. However, recent algebraic and combinatorial results have provided some insights on the existence question. The most significant of these results are outlined below.

Using a theorem of Radon [49], Geramita, Geramita and Wallis [24] observed that the number of variables of an orthogonal design of order n is at most $\rho(n)$, where ρ (the *Radon* function) is defined as follows. Suppose that $n = 2^{4c+d}b$, where b is odd and $0 \leq d < 4$. Then $\rho(n) = 8c + 2^d$ (see also [67]). The proof of this fact uses the observation

that an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order n can be written as $\sum_{i=1}^{u} x_i A_i$, where

(0.0.4) $$A_i A_i^t = s_i I \quad \text{for} \quad 1 \le i \le u ;$$

(0.0.5) $$A_i A_j^t + A_j A_i^t = 0 \quad \text{for} \quad 1 \le i < j \le u ;$$

(0.0.6) the entries of each A_i are from $\{0, 1, -1\}$;

(0.0.7) $$A_i * A_j = 0 \quad \text{for} \quad 1 \le i < j \le u \quad \text{(see (1.1.11))}.$$

A set $\{A_1, A_2, \ldots, A_u\}$ of rational $n \times n$ matrices which satisfy (0.0.4) and (0.0.5) is called a *rational family* of type $(s_1, s_2, \ldots, s_u)$ and order n. Thus the existence of an orthogonal design implies the existence of a rational family of the same order and type. The observation that the algebraic properties of an orthogonal design are reflected in the associated rational family motivates the following theorem.

(0.0.8) **THEOREM** (Rational Family Theorem) [24], [63], [78]. *Suppose that* $n = 2^a b$ *where* b *is odd. Then there is a rational family of type* $(s_1, s_2, \ldots, s_u)$ *and order* n *if and only if*

(0.0.9) $$u \le \rho(n)$$

and

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

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

The Rational Family Theorem as stated above summarizes many results in the literature. A full exposition is given by Geramita and Seberry [26].

The conditions (0.0.9) and (0.0.10) are called the *algebraic necessary conditions* for the existence of an orthogonal design. For many values of a and u, the Hasse-Minkowski classification of rational quadratic forms (see Serre [62], p. 41) gives an efficient algorithm for deciding whether (0.0.10)

holds for given values of $s_1, s_2, \ldots, s_u$ (see Wolfe [79]). Robinson (private communication) has used a computer to determine all 4-tuples (s_1, s_2, s_3, s_4) with $s_1 + s_2 + s_3 + s_4 \leq 100$ such that (0.0.10) holds with $a = 2$. In some cases the algebraic necessary conditions can be stated in terms of sums of squares. For instance it follows from (0.0.10) and a theorem of Davenport and Cassels (Serre [62], p. 46) that the existence of a weighing matrix of weight k and order $2^a b$, b odd, implies that k can be written as a sum of 2^a squares of integers. Also, the existence of an orthogonal design of type (s_1, s_2) and order $2^a b$ implies that $a > 0$ and the product $s_1 s_2$ can be written as a sum of $2^a - 1$ squares of integers.

An important concept for the theory of orthogonal designs is the fact that the algebraic necessary conditions weaken as the order becomes more divisible by 2. That is, if (0.0.9) and (0.0.10) hold for parameters $n, s_1, s_2, \ldots, s_u$, then they hold when n is replaced with $2n$.

A kind of integral analogue to the Rational Family Theorem is proved in Chapter 4. In particular, we show that the algebraic necessary conditions for the existence of an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order n often suffice to ensure the existence of an $n \times n$ matrix A which has entries from $\{mx_i : m \in \mathbb{Z}, 1 \leq i \leq u\}$ and satisfies the same equation as an orthogonal design, that is,

$$AA^t = \left(\sum_{i=1}^{u} s_i x_i^2\right) I .$$

Sufficient conditions are given for the matrix A to be an orthogonal design, that is, for the entries of A to be from $\{\pm x_i : 1 \leq i \leq u\}$.

However, the algebraic necessary conditions are not always sufficient for the existence of orthogonal designs. Clearly $s_1 + s_2 + \ldots + s_u \leq n$

is also required for the existence of an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order n. The following three theorems give further combinatorial necessary conditions for existence.

(0.0.11) THEOREM [24]. *Suppose that there is a weighing matrix of weight k and order n.*

(a) If $n \equiv 2 \pmod 4$ then either $n = 2$ or $n \geq k+1$.

(b) If n is odd then $n \geq k + \sqrt{k} + 1$ with equality only if there is a projective plane of order $n - k - 1$. □

(0.0.12) THEOREM (Geramita-Verner Theorem) [27]. *Suppose that there is an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order n and $s_1 + s_2 + \ldots + s_u = n - 1$. Then n is even and*

(a) $n \equiv 2 \pmod 4$ implies that there is a symmetric orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order n;

(b) $n \equiv 0 \pmod 4$ implies that there is a skew-symmetric orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order n. □

(0.0.13) THEOREM (Robinson's Theorem) [53]. *If there is an orthogonal design of type $(1, 1, 1, 1, 1, n-5)$ and order n then $n \leq 32$.* □

To illustrate the use of Theorems (0.0.12) and (0.0.13) consider the possibility that there is an orthogonal design of type $(1, 1, 1, 1, 51)$ and order 56. Note that these parameters satisfy the algebraic necessary conditions since $\rho(56) = 8$ and

$$P = \begin{bmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \\ & & & 1 & & & \\ & & & & 1 & 5 & 5 \end{bmatrix}$$

satisfies $PP^t = \mathrm{diag}(1, 1, 1, 1, 51)$. But the Geramita-Verner Theorem implies that if such an orthogonal design exists, then there is a skew-symmetric orthogonal design A with the same parameters. It is not

difficult to verify that $yI_{56} + A$ must be an orthogonal design of type (1, 1, 1, 1, 1, 51) ; but by Robinson's Theorem, this is impossible.

The three combinatorial theorems above indicate that the algebraic necessary conditions may not be sufficient for the existence of full or almost full orthogonal designs (see (1.1.8)). However, numerical evidence suggests that if n is sufficiently larger than $s_1 + s_2 + \ldots + s_u$, then the algebraic necessary conditions imply existence.

(0.0.14) ASYMPTOTIC SUFFICIENCY CONJECTURE. *Suppose that a is a non-negative integer and $s_1, s_2, \ldots, s_u$, are positive integers such that $u \leq \rho(2^a)$ and there is a $u \times 2^a$ rational matrix P such that $PP^t = \mathrm{diag}(s_1, s_2, \ldots, s_u)$. Then there is an integer N such that an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order $2^a n$ exists for each $n \geq N$.*

The case $a = 0$ of this conjecture was first proved by Geramita and Wallis [31]. In Chapter 3 of this thesis the conjecture is discussed for $0 \leq a \leq 3$. In particular it is proved for weighing matrices, for skew-symmetric weighing matrices, and for orthogonal designs of order equivalent to 2 modulo 4. Partial results for other cases are obtained. The numerical evidence on which the conjecture is based is given in Chapter 5.

Conjecture (0.0.14) claims that existence can be established at the cost of fullness. This cost is considerable, since orthogonal designs have greater significance in applications if they are full or almost full. Robinson and Seberry [60] have investigated the existence problem for full orthogonal designs. They conjecture that existence of full orthogonal designs with a limited number of variables can be established for orders which are a power of 2.

(0.0.15) ROBINSON-SEBERRY CONJECTURE. *If* $u \leq 5$ *and* $s_1 + s_2 + \ldots + s_u = 2^a$, *then there is an orthogonal design of type* $(s_1, s_2, \ldots, s_u)$ *and order* 2^a.

Remark. Robinson's Theorem (0.0.13) prevents the extension of this conjecture to the case $u = 6$. Note also that the algebraic necessary conditions are not relevant to this conjecture, since if $u \leq 5$ and $a \geq 3$ then $u \leq \rho(2^a)$ and for every u-tuple $(s_1, s_2, \ldots, s_u)$ of positive integers there is a $u \times 2^a$ rational matrix P such that $PP^t = \mathrm{diag}(s_1, s_2, \ldots, s_u)$ (see [79]).

The Robinson-Seberry conjecture has been proved by Wallis for $u \leq 3$ [70], and there is extensive numerical evidence which suggests that it is true for $u \leq 4$ [60].

In a similar vein, Wallis [70] has proved the following asymptotic result for Hadamard matrices.

(0.0.16) THEOREM (Wallis' Theorem [70]). *If* v *is a positive integer then there is an Hadamard matrix of order* $2^a v$ *for all* $a \geq [2 \log_2(v-3)]$. □

In Chapter 3 we show that for some values of v, Theorem (0.0.16) can be generalized to orthogonal designs. That is, if all of $n, s_1, s_2, \ldots, s_u$, are sufficiently divisible by 2 then there is an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order n.

These asymptotic results leave many existence questions untouched. For example, the methods of Chapter 3 imply that an orthogonal design of type (4, 9) and order $2n$ exists for all $n \geq 11430$ (using the proof of Theorem (3.2.2)). We would like to know whether there is an orthogonal design of type (4, 9) and order $2n$ for $7 \leq n < 11430$. This prompts

three questions.

Suppose that $u \leq \rho(2^a)$ *and there is a* $u \times 2^a$ *rational matrix* P *such that* $PP^t = \mathrm{diag}(s_1, s_2, \ldots, s_u)$.

(0.0.17) *What is the smallest integer* N *such that an orthogonal design of type* $(s_1, s_2, \ldots, s_u)$ *and order* $2^a n$ *exists for all* $n \geq N$ *?*

(0.0.18) *What is the smallest odd integer* l *such that an orthogonal design of type* $(s_1, s_2, \ldots, s_u)$ *and order* $2^a l$ *exists?*

(0.0.19) *For which integers* m *between* l *and* N *does there exist an orthogonal design of type* $(s_1, s_2, \ldots, s_u)$ *and order* $2^a m$ *?*

In this thesis we attempt to answer these questions by direct construction of orthogonal designs. The principal method is an array used first by Goethals and Seidel [33] to construct a skew-symmetric weighing matrix of weight 35 and order 36 . In Chapter 2 an algorithm is presented for using this array to construct orthogonal designs of order equivalent to 4 modulo 8 . The array is generalized in the second section of Chapter 2, and the existence of infinite families of orthogonal designs is deduced. The power of the results of Chapter 2 is illustrated by the numerical results in Chapter 5.

The existence question (0.0.3) is only partially answered by this thesis. Many problems are raised but not solved; even more are left untouched.

A list of significant unsolved problems forms an appendix.

CHAPTER 1

PRELIMINARIES

(1.1) Notation, conventions, and jargon

(1.1.1) $\mathbb{Z}$ denotes the ring of integers and $\mathbb{Q}$ denotes the field of rational numbers.

(1.1.2) The *order* of an $n \times n$ matrix is n.

(1.1.3) The identity matrix of order n is denoted by I_n and the $n \times n$ matrix with every entry 1 is denoted by J_n. The subscripts are omitted where convenient.

(1.1.4) A diagonal matrix may be denoted by $\operatorname{diag}(a_1, a_2, \ldots, a_n)$.

(1.1.5) A blank entry in a matrix represents zero. Thus

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

denotes

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

(1.1.6) The largest integer no bigger than a real number q is denoted by $[q]$.

(1.1.7) The number of elements of a finite set S is denoted by $|S|$.

(1.1.8) A matrix is *full* if all its entries are nonzero. A matrix may be referred to as *almost full* if only a small number of entries are zero. A matrix with a large number of zero entries is referred to as *sparse*.

(1.1.9) The transpose of a matrix A is denoted by A^t. The multiplicative inverse of A^t is written A^{-t} if this causes no ambiguity.

(1.1.10) The matrix whose entries are the absolute values of the entries of A is denoted by $\operatorname{abs}(A)$.

(1.1.11) If $A = (a_{ij})$ and $B = (b_{ij})$ are two $n \times m$ matrices then the

Hadamard product of A and B is written $A * B$ and is an $n \times m$ matrix with ijth entry $a_{ij}b_{ij}$. If $A * B = 0$ then A and B are said to be *disjoint*.

(1.1.12) The symbols $x, x_1, x_2, \ldots, y, y_1, y_2, \ldots$, are reserved for use as formal commuting variables. To make this notion mathematically precise we may consider these variables as elements of the polynomial ring $\mathbb{Q}[x, x_1, x_2, \ldots, y, y_1, y_2, \ldots]$.

(1.1.13) If A is an $n \times n$ matrix and B is an $m \times m$ matrix with ijth entry b_{ij}, then their *kronecker product* $B \times A$ is the $mn \times mn$ matrix

$$\begin{bmatrix} b_{11}A & b_{12}A & \ldots & b_{1m}A \\ b_{21}A & b_{22}A & \ldots & b_{2m}A \\ \vdots & \vdots & & \vdots \\ b_{m1}A & b_{m2}A & \ldots & b_{mm}A \end{bmatrix}.$$

The relevant properties of the kronecker product are given in [75].

(1.2) Elementary constructions

Suppose that there is an orthogonal design A of type $s_1, s_2, \ldots, s_u$ and order n. Then other orthogonal designs may be constructed as follows (from [24]). Replacing the variable x_u by zero throughout given an orthogonal design of type $(s_1, s_2, \ldots, s_{u-1})$. An orthogonal design of type $(s_1+s_2, s_3, \ldots, s_u)$ may be obtained by *equating variables*, that is, replacing x_1 by x_2 throughout. Note that a weighing matrix of weight $s_1 + s_2 + \ldots + s_u$ may be obtained in this way.

If there is another orthogonal design B of type $(s_1, s_2, \ldots, s_u)$ and order m, then the $(m+n) \times (m+n)$ matrix

$$\begin{bmatrix} A & \\ & B \end{bmatrix}$$

is an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order $m + n$. Note that it follows that if w and v are nonnegative integers and $mw + nv \neq 0$ then there is an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order $mw + nv$. The significance of this is due to the fact that if m is prime to n and $r \geq (m-1)(n-1)$ then r can be written as $mw + nv$ where m and n are nonnegative. This simple observation is used in Chapter 3.

Suppose that A is skew-symmetric, that is, $A = -A^t$. Then the diagonal of A is zero and we can verify that $yI + A$ is an orthogonal design of type $(1, s_1, s_2, \ldots, s_u)$ and order n. In particular, the existence of a skew-symmetric weighing matrix of weight k is equivalent to the existence of an orthogonal design of type $(1, k)$ and the same order.

(1.3) Amicable orthogonal designs

A u-tuple $(A_1, A_2, \ldots, A_u)$ of orthogonal designs of the same order is called *amicable* if $A_i A_j^t = A_j A_i^t$ for $1 \leq i < j \leq u$. Amicable u-tuples, especially pairs, have been studied extensively for the following reason. Suppose that there is an orthogonal design B of type $(s_1, s_2, \ldots, s_u)$ and order n, and $(A_1, A_2, \ldots, A_u)$ is amicable, where each A_i has order m and type $(a_{1i}, a_{2i}, \ldots, a_{v_i i})$. Then replacing the variable x_i by A_i in B gives an orthogonal design of type

$$(s_1 a_{11}, s_1 a_{21}, \ldots, s_1 a_{v_1 1}, s_2 a_{12}, \ldots, s_2 a_{v_2 2}, \ldots, s_u a_{v_u u})$$

and order mn. The knowledge of amicable u-tuples of orders 2, 4, and 8 has proved invaluable in the construction of full orthogonal designs (see

[56]).

Amicable u-tuples of order 2 have been found which establish the following theorems.

(1.3.1) THEOREM [24]. *If there is an orthogonal design of type* $(s_1, s_2, \ldots, s_u)$ *and order* n *and* $\varepsilon_i \in \{1, 2\}$ *for* $1 \le i \le u$, *then there are orthogonal designs of types* $(s_1, s_1, \varepsilon_1 s_2, \varepsilon_1 s_3, \ldots, \varepsilon_1 s_u)$ *and* $(\varepsilon_1 s_1, \varepsilon_2 s_2, \ldots, \varepsilon_u s_u)$ *and order* $2n$. □

(1.3.2) THEOREM [24]. *If there is an orthogonal design of type* (s_1, s_2) *and order* n *then there is an orthogonal design of type* (s_1, s_1, s_2, s_2) *and order* $2n$. □

Wallis [70] used Theorem (1.3.1) to prove the following result for orthogonal designs of order a power of 2.

(1.3.3) THEOREM [70]. *(a) If* s_1, s_2, s_3, *are positive integers with sum* 2^a *then there is an orthogonal design of type* (s_1, s_2, s_3) *and order* 2^a.

(b) If s_1 *and* s_2 *are positive integers with sum at most* 2^a *then there is an orthogonal design of type* (s_1, s_2) *and order* 2^a. □

For weighing matrices the kronecker product provides a construction similar in effect to the constructions given by amicable orthogonal designs.

(1.3.4) THEOREM [75]. *If* W *and* V *are weighing matrices of weights* k *and* l *and orders* m *and* n *respectively then* $W \times V$ *is a weighing matrix of weight* kl *and order* mn. □

(1.4) Circulant matrices

An $n \times n$ matrix (a_{ij}) is *circulant* if $a_{ij} = a_{0,j-i}$, where the subscripts range over a reduced residue system modulo n. It is not

difficult to prove that the circulant matrices over a commutative ring form a commutative ring.

Let S_n denote the group of permutation matrices of order n, and suppose that T is the permutation matrix which represents the n-cycle $(1\ 2\ \ldots\ n)$; that is

$$T = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & & 0 \\ 0 & 0 & 0 & & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & & 0 & 1 \\ 1 & 0 & \ldots. & 0 & 0 \end{bmatrix}.$$

If the first row of the circulant matrix A is $(a_{11}, a_{12}, \ldots, a_{1n})$, then

$$A = a_{11}I + a_{12}T + \ldots + a_{1n}T^{n-1}.$$

This expansion makes algebraic manipulation of circulant matrices easier.

The element R of S_n which represents

$$(1, n)(2, n-1) \ldots \left([\tfrac{1}{2}(n+1)], [\tfrac{1}{2}(n+2)]\right)$$

is called the backdiagonal matrix of order n. Note that

$$R = \begin{bmatrix} & & & & 1 \\ & & & 1 & \\ & & 1 & & \\ & \iddots & & & \\ 1 & & & & \end{bmatrix}.$$

A matrix is *backcirculant* if it can be written as AR where A is circulant. The fact that backcirculant matrices are symmetric is important in Chapter 2.

It can be shown easily that there are no circulant orthogonal designs with more than one variable, but there is an infinite family of circulant weighing matrices.

(1.4.1) THEOREM [74]. *If q is a prime power then there is a circulant weighing matrix of weight q^2 and order $q^2 + q + 1$.* □

These circulant weighing matrices are used extensively in Chapter 3 and section (2.3).

The reader is referred to [17] for details on the problem of existence of circulant weighing matrices.

(1.5) Complementary sequences

The sequences

$$a_1 = (a_{11}, \ldots, a_{1v}),\ a_2 = (a_{21}, \ldots, a_{2v}),\ \ldots,\ a_u = (a_{u1}, \ldots, a_{uv})$$

are *complementary* if

$$\sum_{i=1}^{u} \sum_{j=1}^{v-l} a_{ij} a_{i,j+l} = 0 , \tag{1.5.1}$$

for each $l \in \{1, 2, \ldots, v-1\}$. For example if a, b, c, d , are integers then

$$(a, b, c, d) ,$$
$$(-b, a, d, -c) ,$$
$$(-c, -d, a, b) ,$$
$$(-d, c, -b, a) ,$$

are complementary.

A straightforward computation using (1.5.1) shows that if B_i is the circulant matrix with first row a_i , then

$$\sum_{i=1}^{u} B_i B_i^t = \left(\sum_{i=1}^{u} \sum_{j=1}^{v} a_{ij}^2 \right) I \tag{1.5.2}$$

(see [26]). Equations of this form are significant in the construction of orthogonal designs, especially in Chapter 2.

Note that the sequences $a_1', a_2', \ldots, a_u'$, where

$$a_i' = (a_{i1}, a_{i2}, \ldots, a_{iv}, 0)$$

are complementary. Thus for each $m \geq v$ there are $m \times m$ circulant matrices $A_1, A_2, \ldots, A_u$, such that

$$\sum_{i=1}^{u} A_i A_i^t = \left(\sum_{i=1}^{u} \sum_{j=1}^{v} a_{ij}^2 \right) I .$$

This fact is important in Chapters 4 and 5.

Complementary sequences have extensive applications in both pure and applied combinatorics. The reader is referred to [61], [68], [3], [26], for further details.

(1.6) Miscellaneous

Several mathematical ideas other than the theory of orthogonal designs are used in this thesis.

The classification of rational quadratic forms by Hasse and Minkowski is invoked in section (3.2) and often in section (4.2). An exposition of this theory is beyond the scope of this thesis, and the reader is referred to Serre [62] (part 1).

The classical theorems on sums of squares of integers are used throughout. Siérpinski [64] lists all the necessary theorems.

The language of algebraic structures (groups, rings etc.) is used in various places. In particular, some facts about permutation groups are used. Herstein [60] covers this area sufficiently.

Cyclic difference sets are used in section (2.2); details are in Baumert [3].

CHAPTER 2

THE GOETHALS-SEIDEL ARRAY AND SIMILAR CONSTRUCTIONS

Circulant matrices have been used to reproduce orthogonal designs in the following way. Suppose that there is an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order n on the variables $x_1, x_2, \ldots, x_u$, and $X_1, X_2, \ldots, X_u$, are $v \times v$ circulant matrices with entries from $\{0, \pm y_1, \pm y_2, \ldots, \pm y_l\}$ such that

$$\sum_{i=1}^{u} s_i X_i X_i^t = \left(\sum_{j=1}^{l} m_j y_j^2 \right) I \,, \tag{2.0.1}$$

and

$$X_i X_j^t = X_j X_i^t \quad \text{for} \quad 1 \le i < j \le u \,. \tag{2.0.2}$$

(Note that (2.0.2) is satisfied if each X_i is symmetric, or if each X_i is skew-symmetric.)

Then an orthogonal design of type $(m_1, m_2, \ldots, m_l)$ and order nv may be obtained by replacing each variable x_i in A by X_i.

The difficulty here is the requirement (2.0.2). For example, it can be shown that a skew-symmetric weighing matrix of weight 35 and order 36 cannot be constructed using an orthogonal design of type (1, 1, 1, 1) and order 4. Goethals and Seidel produced such a weighing matrix by using a construction which overcame the problem (2.0.2).

(2.0.3) THEOREM (Goethals-Seidel construction) [33]. *Suppose that* A_1, A_2, A_3, A_4, *are* $v \times v$ *circulant matrices with entries from* $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ *and*

$$\sum_{i=1}^{4} A_i A_i^t = \left(\sum_{j=1}^{u} s_j x_j^2 \right) I \,. \tag{2.0.4}$$

If R *denotes the backdiagonal matrix of order* v *then*

$$\begin{bmatrix} A_1 & A_2R & A_3R & A_4R \\ -A_2R & A_1 & A_4^tR & -A_3^tR \\ -A_3R & -A_4^tR & A_1 & A_2^tR \\ -A_4R & A_3^tR & -A_2^tR & A_1 \end{bmatrix} \tag{2.0.5}$$

is an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ *and order* $4v$. □

The array (2.0.5) has subsequently been called the *Goethals-Seidel array*. Theorem (2.0.3) has proved to be the most productive method of constructing orthogonal designs of order equivalent to 4 modulo 8 .

A similar array for two circulant matrices is well known.

(2.0.6) THEOREM (Two-circulant construction) [26]. *Suppose that* A_1 *and* A_2 *are* $v \times v$ *circulant matrices with entries from* $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ *and*

$$A_1A_1^t + A_2A_2^t = \left(\sum_{i=1}^{u} s_i x_i^2\right) I \ .$$

If R *denotes the* $v \times v$ *backdiagonal matrix then*

$$\begin{bmatrix} A_1 & A_2R \\ -A_2R & A_1 \end{bmatrix} \tag{2.0.7}$$

is an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ *and order* $2v$. □

The two-circulant construction is useful for the construction of orthogonal designs of order equivalent to 2 modulo 4 . The array (2.0.7) is called the *two-circulant array*.

A method for finding solutions of (2.0.4) is described in section (2.1) following.

Generalizations of the Geothals-Seidel array are presented in section (2.2). Section (2.3) illustrates techniques for using the Geothals-Seidel array and its generalizations to produce infinite families of orthogonal

designs.

The results of sections (2.1) and (2.3) have provided a substantial amount of information about the questions (0.0.17), (0.0.18) and (0.0.19) posed in the introduction to this thesis. The extent of this information is indicated in the tables of numerical results in Chapter 5.

The limitations of constructions such as the Goethals-Seidel array are discussed in section (2.9).

(2.1) A method for constructing orthogonal designs by using circulant matrices

The method outlined in this section has been used successfully to compute 4 variable orthogonal designs of order 20 and 2 variable orthogonal designs of order 28 . Some success has been achieved with weighing matrices of orders 18, 22, 26, 30, 44 , and 52 . The results of this computation are included in the tables of numerical results in Chapter 5. The author believes that the method can be extended to construct 3 and 4 variable orthogonal designs of order 28 and 2 variable orthogonal designs of order 36 , but so far this has not been done.

The method is presented as it applies to the Geothals-Seidel construction (2.0.3), but there are no difficulties in extending the results for more general circulant constructions, such as those mentioned in section (2.2).

Specifically, for positive integers $s_1, s_2, \ldots, s_u$, and odd v the method searches for four circulant matrices X_1, X_2, X_3, X_4 , of order v with entries from $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ such that

$$\sum_{i=1}^{u} X_i X_i^t = \left(\sum_{i=1}^{u} s_i x_i^2 \right) I \ . \tag{2.1.1}$$

The existence of an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order $4v$ follows from the Goethals-Seidel construction (2.0.3).

Remark. The restriction that v is odd is not necessary for most of the results which follow. However, the restriction is made because we are principally interested here in constructing orthogonal designs of order not divisible by 8. Orthogonal designs of order divisible by a large power of 2 can be constructed using other methods (see [55], [57], and section (3.1)).

Equation (2.1.1) has v^2 components, but since $X_i X_i^t$ is circulant and symmetric, at most $\frac{1}{2}(v+1)$ of these components are independent. The next two definitions are made to isolate the independent components.

If A_1, A_2, A_3, A_4, are $v \times v$ circulant matrices with entries from $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ and the first row of A_j has m_{ij} entries of the kind $\pm x_i$, then the $u \times 4$ matrix $M = (m_{ij})$ is called the *entry matrix* of (A_1, A_2, A_3, A_4).

Suppose that A is a $v \times v$ circulant matrix with rows $r_1, r_2, \ldots, r_v$, and denote $\frac{1}{2}(v-1)$ by w. Then the *IPV (inner product vector)* of A is $\left(r_1 r_2^t, r_1 r_3^t, \ldots, r_1 r_w^t\right)$. Note that if $(d_1, d_2, \ldots, d_v)$ is the first row of AA^t, then the IPV of A is $(d_2, d_3, \ldots, d_w)$.

It is clear that $(X_1, X_2, X_3, X_4) = (A_1, A_2, A_3, A_4)$ is a solution of (2.1.1), if and only if

$$\sum_{j=1}^{4} m_{ij} = s_i \quad \text{for} \quad 1 \le i \le u , \tag{2.1.2}$$

and

$$\sum_{j=1}^{4} b_j = 0 , \text{ where } b_j \text{ is the IPV of } A_j . \tag{2.1.3}$$

In other words, to find a solution of (2.1.1) we need four circulant matrices with entries from $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ whose entry

matrix has ith row adding to s_i for $1 \le i \le u$ and whose IPV's add to zero.

The *content* of a circulant matrix A with entries from $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ is the set of pairs $(\varepsilon x_i, m)$ where εx_i $(\varepsilon = \pm 1)$ occurs a nonzero number m times in the first row of A. Our next task is to show how the contents of solutions of (2.1.1) may be determined from the knowledge of the parameters $v, s_1, s_2, \ldots, s_u$.

Suppose that the rowsum of A_i is $\sum_{i=1}^{u} p_{ij}x_j$ for $1 \le j \le 4$. Then the $u \times 4$ integral matrix $P = (p_{ij})$ is called the *sum matrix* of (A_1, A_2, A_3, A_4). The *fill matrix* of (A_1, A_2, A_3, A_4) is $M - \mathrm{abs}(P)$. The content of A_i is determined by the ith columns of the sum and fill matrices.

The following Theorem may be used to find the sum matrix of a solution of (2.1.1).

(2.1.4) **THEOREM** (Sum Matrix Theorem). *The sum matrix P of a solution of* (2.1.1) *satisfies*

$$PP^t = \mathrm{diag}(s_1, s_2, \ldots, s_u) . \tag{2.1.5}$$

Proof. Suppose that A is a $v \times v$ circulant matrix with rowsum a, and denote by b the sum of the squares of the first row of A, and by c the sum of the entries of the IPV of A. Then

$$(JA)(A^tJ^t) = a^2JJ^t = a^2vJ$$

(see (1.1.3)). But also

$$\begin{aligned}(JA)(A^tJ^t) &= J(AA^t)J^t \\ &= (b+2c)JJ^t \\ &= v(b+2c)J .\end{aligned}$$

Hence $a^2 = b + 2c$. Thus if (p_{ij}) and (m_{ij}) are the sum and entry matrices of a solution of (2.1.1), then since the sum of the sums of the entries of the IPV's is zero, it follows that

$$\sum_{i=1}^{4} \left(\left(\sum_{j=1}^{u} p_{ij} x_i \right)^2 - \left(\sum_{j=1}^{u} m_{ij} x_j^2 \right) \right) = 0 .$$

Expanding this equation and equating coefficients of $x_i x_j$ gives (2.1.5). □

(2.1.6) **REMARKS.** (a) Note that the Sum Matrix Theorem (2.1.4) implies that a necessary condition for the existence of an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order $4v$ constructed by using the Goethals-Seidel array is the existence of a $u \times 4$ integral matrix P satisfying (2.1.5). The similarity between this result and the Rational Family Theorem (0.0.8) was the original motivation for much of Chapter 4.

(b) Suppose that P and Q are the sum and fill matrices of a solution $(X_1, X_2, X_3, X_4) = (A_1, A_2, A_3, A_4)$ of (2.1.1). If B and C are permutation matrices of orders u and 4 respectively, then BPC and BQC are the sum and fill matrices of another solution of (2.1.1) formed by permuting the indices of the A_i and the x_j . Hence BPC and BQC are regarded as essentially the same as P and Q . Similarly, if P' is formed from P by multiplying some rows and columns by -1 , then P' is regarded as essentially the same as P .

We state the first step of the method.

STEP 1. *Use the Sum Matrix Theorem to find a sum matrix of a solution of* (2.1.1).

If the algebraic necessary conditions ((0.0.9) and (0.0.10)) for the existence of an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order $4v$ hold, then the existence of a solution to (2.1.5) is guaranteed by Proposition (4.2.3). In most cases if the s_i are small (for instance

$s_1 + s_2 + \ldots + s_u \leq 28$) then the solution of (2.1.5) is essentially unique and can be found easily by hand.

It is clear that if Q is the fill matrix of a solution of (2.1.1) then

(2.1.7) the entries of Q are even nonnegative integers,

and if $M = (m_{ij}) = \text{abs}(P) + Q$ then M satisfies (2.1.2) and

(2.1.8) the sum of a column of M is at most v .

There may be a large number of matrices which satisfy (2.1.2), (2.1.7) and (2.1.8) (see Example (2.1.11)), but the next two lemmas may be used to reduce the number of possibilities.

(2.1.9) **LEMMA.** *Suppose that A is a circulant matrix of odd order v , with entries from $\{0, 1, -1\}$ and with k nonzero entries in each row.*

(a) If $k \geq v-1$ then each entry of the IPV of A is odd.

(b) If each entry of the IPV of A is even then $v \geq k + \sqrt{k} + 1$.

Proof. Part (a) can be proved by an elementary parity check. For part (b), a standard counting argument may be employed as follows. Suppose that the ijth entry of A is a_{ij} and denote by B_i the set

$$\{j : 1 \leq j \leq v \text{ and } a_{ij} = 0\} ,$$

for $1 \leq i \leq v$. Each B_i contains $v - k$ elements. Also, since each column of A contains k nonzero entries, each integer in $\{1, 2, \ldots, v\}$ occurs in $v - k$ of the B_i . It follows that each element of B_1 occurs in $v - k - 1$ of the B_i for $i \geq 2$; hence

$$\sum_{i=2}^{v} |B_1 \cap B_i| = (v-k)(v-k-1) .$$

But since the inner product of each pair of distinct rows of A is even and v is odd, $|B_1 \cap B_i|$ is odd for $2 \leq i \leq v$. In particular $|B_1 \cap B_i| \geq 1$. Hence

$$\sum_{i=2}^{v} |B_1 \cap B_i| \geq v - 1 ,$$

and so

$$(v-k)^2 - (v-k) \geq v - 1 .$$

Completing the square gives

$$(v-k-1)^2 \geq k .$$

By part (a), $v > k \geq 0$ and so $v \geq k + \sqrt{k} + 1$. □

(2.1.10) **LEMMA.** *Suppose that the entry matrix of a solution* $(X_1, X_2, X_3, X_4) = (A_1, A_2, A_3, A_4)$ *of* (2.1.1) *is*

$$\begin{bmatrix} V & \\ & W \end{bmatrix}$$

where V *is* $l \times r$ *and* W *is* $(u-l) \times (4-r)$. *Then*

$$\sum_{j=1}^{r} A_j A_j^t = \left(\sum_{i=1}^{l} s_i x_i^2 \right) I$$

and

$$\sum_{j=r+1}^{4} A_j A_j^t = \left(\sum_{i=l+1}^{u} s_i x_i^2 \right) I . \quad \square$$

The proof of this lemma is straightforward and thus omitted.

Before the use of these lemmas is illustrated with an example, the second step of the method is stated explicitly.

STEP 2. *Using* (2.1.2), (2.1.7), (2.1.8) *and Lemmas* (2.1.9) *and* (2.1.10), *find all possible fill matrices which could accompany the sum matrix found in Step* 1.

If v and the s_i are small, then there are usually very few possible fill matrices, and they can be found easily without a computer.

(2.1.11) **EXAMPLE.** The existence of an orthogonal design of type (1, 5, 5, 9) and order 20 is listed in [31] as being undetermined. To construct such an orthogonal design, we require four 5×5 circulant matrices

B_1, B_2, B_3, B_4 , with entries from $\{0, \pm x_1, \pm x_2, \pm x_3, \pm x_4\}$, such that

$$\sum_{i=1}^{4} B_i B_i^t = \left(x_1^2+5x_2^2+5x_3^2+9x_4^2\right) I \ . \tag{2.1.12}$$

Now $1 = 1^2$, $5 = 1^2 + 2^2$, $9 = 3^2 = 2^2 + 2^2 + 1^2$, are essentially the only ways of writing 1, 5, 9 , as sums of at most 4 squares, and so it is not difficult to show that (essentially) the only 4×4 integral matrix P which satisfies $PP^t = \mathrm{diag}(1, 5, 5, 9)$ is

$$P = \begin{bmatrix} 1 & & & \\ & 1 & 2 & \\ & -2 & 1 & \\ & & & 3 \end{bmatrix} . \tag{2.1.13}$$

(See Remark (2.1.6) (b).)

Now there are eight 4×4 integral matrices which, on the basis of (2.1.2), (2.1.7) and (2.1.8), could be fill matrices.

(a) $\begin{bmatrix} 2 & & & \\ 2 & & & \\ 2 & 2 & 2 & \end{bmatrix}$, (b) $\begin{bmatrix} 2 & & & \\ & 2 & & \\ 2 & & 2 & \end{bmatrix}$, (c) $\begin{bmatrix} 2 & & & \\ & & 2 & \\ 2 & 2 & & \end{bmatrix}$, (d) $\begin{bmatrix} 2 & & & \\ & & & 2 \\ 2 & 2 & 2 & \end{bmatrix}$,

(2.1.14)

(e) $\begin{bmatrix} & 2 & & \\ & & 2 & \\ 4 & & & 2 \end{bmatrix}$, (f) $\begin{bmatrix} & & 2 & \\ & 2 & & \\ 4 & & & 2 \end{bmatrix}$, (g) $\begin{bmatrix} & 2 & & \\ & & & 2 \\ 4 & & 2 & \end{bmatrix}$, (h) $\begin{bmatrix} & & 2 & \\ & & & 2 \\ 4 & 2 & & \end{bmatrix}$.

However, four of these matrices can be discounted as possible fill matrices by using Lemmas (2.1.9) and (2.1.10).

Suppose that (B_1, B_2, B_3, B_4) has sum matrix P above (2.1.13) and fill matrix (2.1.14) (b). Then the entry matrix is

$$\begin{bmatrix} 1 & & & \\ 2 & 1 & 2 & \\ & 4 & 1 & \\ 2 & & 2 & 5 \end{bmatrix}$$

which satisfies (2.1.2) and (2.1.8). But the (3, 2)th entry of this entry matrix indicates by Lemma (2.1.9) that every entry of the IPV of B_2 has a term in x_3^2 with odd coefficient. But x_3 occurs at most once in each row of each of the other circulant matrices, and it follows that the IPV's of the other circulant matrices have no terms in x_3^2. Hence it is impossible for the IPV's of the B_i to add to zero; so (2.1.14) (b) is not the fill matrix of the B_i.

Suppose that (2.1.14) (f) is the fill matrix of (B_1, B_2, B_3, B_4); this gives entry matrix

$$\begin{bmatrix} 1 & & & \\ & 1 & 4 & \\ & 4 & 1 & \\ 4 & & & 5 \end{bmatrix}.$$

If this is the entry matrix of (B_1, B_2, B_3, B_4) then

$$\begin{bmatrix} 1 & & & \\ 4 & 5 & & \\ & & 1 & 4 \\ & & 4 & 1 \end{bmatrix}$$

is the entry matrix of another solution (C_1, C_2, C_3, C_4) of (2.1.13) (see Remark (2.1.6) (b)). It follows by Lemma (2.1.10) that

$$C_1C_1^t + C_2C_2^t = \left(x_1^2+9x_2^2\right)I_5 ,$$

and thus, using the two-circulant construction (2.0.6), there is an orthogonal design of type (1, 9) and order 10. This is impossible (see Theorem (0.0.11)) and so (2.1.14) (f) is not the fill matrix of (B_1, B_2, B_3, B_4).

Similarly it can be shown that (2.1.14) (h) and (2.1.14) (e) are not possible.

Each of the possible fill matrices (2.1.14) (a), (c), (d), (g), could specify the contents of a solution of (2.1.12). For each of these possibilities, we need to search through the circulant matrices whose contents are thus specified, until we find a combination whose IPV's add to zero. For instance, for (2.1.14) (a) we need to find four 5×5 permutation matrices M_1, M_2, M_3, M_4, such that

$$(x_1, x_2, -x_2, x_3, -x_3)M_1 ,$$

$$(x_2, -x_3, -x_3, x_4, -x_4)M_2 ,$$

$$(x_2, x_2, x_3, x_4, -x_4)M_3 ,$$

$$(x_4, x_4, x_4, x_4, -x_4)M_4 ,$$

are the first rows of circulant matrices whose IPV's add to zero. If this search fails then we consider circulant matrices with contents specified by (2.1.4) (c), and so on. Note that there are a large number (about 2×10^8) of 4-tuples (M_1, M_2, M_3, M_4) of 5×5 permutation matrices; however, only a small proportion of these need be considered, as we shall presently see.

Once the sum and fill matrices have been chosen, the final steps of the method may be executed.

STEP 3. *For each* $i \in \{1, 2, 3, 4\}$ *write down a circulant matrix* A_i *with contents specified by the* i*th columns of the sum and fill matrices.*

Step 3 can be executed easily either by hand or by computer. Of course, the circulant matrices A_i can be represented by their first rows.

Two circulant matrices with the same content are *isometric* if they have the same IPV.

STEP 4. *For each* $i \in \{1, 2, 3, 4\}$ *write a list* L_i *of non-isometric circulant matrices with the same contents as* A_i. *Attach to each*

circulant matrix its IPV.

The problem of executing the fourth step is considered next. Given two circulant matrices with the same content, how do we determine whether they are isometric (without the time consuming calculation of IPV's)? How large are the lists L_i ? Useful necessary and sufficient conditions for isometry are, in general, unknown, but one obvious sufficient condition can be described as follows. Denote by S_v the group of $v \times v$ permutation matrices, and suppose that $T \in S_v$ represents the v-cycle $(1\ 2\ \ldots\ v)$. Let R denote the $v \times v$ backdiagonal matrix (see section (1.3)). The subgroup S_v generated by T and R is denoted by $\langle T, R \rangle$. If A and B are $v \times v$ circulant matrices with first rows a and aK for some $K \in \langle T, R \rangle$ then it can be seen immediately that A and B are isometric. It follows that the number of non-isometric circulant matrices with the same content is at most the index of $\langle T, R \rangle$ in S_v , that is, $(v\text{-}1)!/2$. Thus the lists L_i in Step 4 contain at most $(v\text{-}1)!/2$ entries. A complete set of distinct coset representatives of $\langle T, R \rangle$ in S_v is easily seen to be

$E = \{M \in S_v : M$ represents a permutation

θ on $\{1, 2, \ldots, v\}$ which satisfies $v\theta = v$ and $1\theta \leq \frac{1}{2}(v\text{-}1)\}$.

Thus to compute the list L_i in step 4 we first write out the elements of

$S = \{B : B$ is a circulant matrix with first row $a_i M$ for some $M \in E\}$

where a_i denotes the first row of the circulant matrix A_i chosen at step 3. This can be done easily either automatically or by hand.

Of course S may contain isometric elements. But it can be shown (as follows) that if $a_i = (x_1, x_2, \ldots, x_v)$ then no two distinct elements of S are isometric.

(2.1.15) **LEMMA.** *If* $a_i = (x_1, x_2, \ldots, x_v)$ *and* B_1 *and* B_2 *are elements*

of S *with first rows* $a_i M_1$ *and* $a_i M_2$ *where* M_1 *and* M_2 *are* $v \times v$ *permutation matrices, then* B_1 *and* B_2 *are isometric if and only if they are equal.*

Proof. The first entries of the IPV's of B_1 and B_2 are equal, that is,

$$a_i M_1 T^{-1} M_1^{-1} a_i^t = a M_2 T^{-1} M_2^{-1} a_i^t .$$

Symmetrizing gives

$$a_i M_1 (T+T^{-1}) M_1^{-1} a_i^t = a_i M_2 (T+T^{-1}) M_2^{-1} a_i^t .$$

Since $a_i = (x_1, x_2, \ldots, x_v)$ we obtain

$$T + T^{-1} = MTM^{-1} + MT^{-1}M^{-1}$$

where M denotes $M_1^{-1} M_2$. A simple combinatorial argument using the fact that v is odd shows that $T + T^{-1}$ can be written uniquely as a sum of two permutation matrices (see [14]). Hence either $T = MTM^{-1}$ or $T^{-1} = MTM^{-1}$. In either case, since the subgroup of S_v generated by T is self centralizing (see [76]), we can deduce that $M \in \langle T, R \rangle$. Thus M_1 and M_2 are in the same coset of $\langle T, R \rangle$; but both are elements of S ; so $M_1 = M_2$.

The converse is immediate. □

This lemma implies that sometimes the list L_i achieves its maximum size $(v\text{-}1)!/2$. However this is rare. For instance, if the content of A_i is $\{(\varepsilon x_i, n_{\varepsilon i}) : 1 \le i \le u, \varepsilon = \pm 1\}$ then the subgroup

$$L = \{M \in S_v : a_i M = a_i\}$$

of S_v has order

$$m = \left(\prod_{i=-u}^{u} n_i!\right)\left(v - \sum_{i=-u}^{u} n_i\right)! \ .$$

Hence there are at most $v!/m$ entries of the list L_i, and often $v!/m < (v-1)!/2$. However, the coset representatives of L in S_v are more difficult to deal with by computer than the representatives of $\langle T, R \rangle$. Hence L is used only in hand calculations. When a computer is used the sort-merge package program may be used to eliminate isometric elements of the set S.

The final step of the method is to search the lists L_i for an answer.

STEP 5. *Search for one circulant matrix C_i with IPV c_i from each list L_i $(1 \le i \le 4)$ such that $c_1 + c_2 + c_3 + c_4 = 0$.*

In the implementations for orthogonal designs of orders 20 and 28, there was no difficulty in using a naive algorithm for the search at step 5 because the lists L_i were relatively small. However, to extend the method to higher orders it seems that a sophisticated search algorithm would need to be employed.

Two notes on the execution of steps 4 and 5 are presented next.

Firstly, suppose that C_1, C_2, C_3, C_4, are circulant matrices whose sum and fill matrices satisfy (2.1.2), (2.1.5), (2.1.7) and (2.1.8). Then the sum of the sums of the entries of the IPV's of the C_i is zero (see proof of Theorem (2.1.4)). That is, if $(c_{i1}, c_{i2}, \ldots, c_{iw})$ is the IPV of C_i $(1 \le i \le 4)$ then

$$\sum_{i=1}^{4} \sum_{j=1}^{w} c_{ij} = 0 \ .$$

Hence if

$$\sum_{i=1}^{4} c_{ij} = 0 \quad \text{for} \quad 1 \le j \le w\text{-}1$$

then

$$\sum_{i=1}^{4} c_{ij} = 0 \quad \text{for} \quad 1 \le j \le w \ .$$

Hence only $\frac{1}{2}(v\text{-}3)$ of the $\frac{1}{2}(v\text{-}1)$ components of the IPV's need to add to zero for (2.1.1) to hold. This saves time and space in computer implementation and provides a simple error checking device for hand calculations.

Secondly, we note that the IPV's of non-isometric circulant matrices may be dependent, in the following way. Suppose that $N \in S_v$ normalizes the subgroup $\langle T \rangle$ of S_v generated by T. Note that there is an integer d prime to v such that $NT^iN^{-1} = T^{id}$ for $0 \le i < v$. Now if the circulant matrix A has first row a then the ith entry of the IPV of A is $aT^{-i}a^t$. Hence the IPV of the circulant matrix B with first row aN has ith entry $aNT^{-i}N^{-1}a^t$, that is, $aT^{-id}a^t$. Hence the IPV of B is a permutation of the IPV of A, described as follows. Suppose that the IPV of A is $(h_1, h_2, \ldots, h_w)$ and $(id)^*$ denotes the image of id in $\{0, 1, \ldots, v\text{-}1\}$ modulo v. Then the IPV of B is $(h_{1\theta}, h_{2\theta}, \ldots, h_{w\theta})$ where θ is the permutation on $\{1, 2, \ldots, w\}$ defined by

$$\text{(2.1.16)} \qquad \theta : i \mapsto \begin{cases} (id)^* & \text{if } 1 \le (id)^* \le w \ , \\ v - (id)^* & \text{otherwise.} \end{cases}$$

Note that $\theta = 1$ if and only if $N \in \langle T, R \rangle$. Hence the index of the normalizer of $\langle T \rangle$ in S_v is $v\phi(v)$, where ϕ is the Euler function. If v is prime then the set E' of $v \times v$ permutation matrices which represent a permutation on $\{1, 2, \ldots, v\}$ which fixes v and $v - 1$ is a

complete set of distinct coset representatives of the normalizer of $\langle T \rangle$ in S_v .

For automatic computation this means that one of the lists, say L_1 , may consist of elements

$S' = \{B : B$ is a circulant matrix with first row $a_1 M$ for some $M \in E'\}$.

This produces a considerably shorter list, and the search (step 5) may be proportionally shorter in time.

The use of the normalizer of $\langle T \rangle$ in hand calculations is illustrated in the completion of Example (2.1.11) below. Firstly, however, we show how the facts above may be used to construct a certain 4 variable orthogonal design of order 28 .

(2.1.17) **EXAMPLE.** An orthogonal design of type (1, 1, 1, 25) and order 28 can be constructed as follows. We want four 7×7 circulant matrices V_1, V_2, V_3, V_4 , with entries from $\{0, \pm x_1, \pm x_2, \pm x_3, \pm x_4\}$ such that

$$\sum_{i=1}^{4} V_i V_i^t = \left(x_1^2+x_2^2+x_3^2+25x_4^2\right) I \ . \tag{2.1.18}$$

The conditions (2.1.2), (2.1.5), (2.1.7), (2.1.8), imply that the sum and fill matrices of (V_1, V_2, V_3, V_4) must be diag(1, 1, 1, 5) and

$$\begin{bmatrix} & & & \\ & & & \\ & & & \\ 6 & 6 & 6 & 2 \end{bmatrix}$$

respectively. Hence V_4 must be $(J-2I)x_4$ up to isometry (see (1.1.3)); thus V_4 has IPV $\left(3x_4^2, 3x_4^2, 3x_4^2\right)$. Choose a skew-symmetric 7×7 matrix C_1 with entries from {0, 1, -1} and precisely one zero in each row; denote its IPV by (d_1, d_2, d_3) . Now the normalizer of $\langle T \rangle$ in S_7 acts cyclically on (d_1, d_2, d_3) by (2.1.16), and further, it preserves skew-

symmetry. Hence there are skew-symmetric circulant matrices C_2 and C_3 with IPV's (d_2, d_3, d_1) and (d_3, d_1, d_2) respectively. For $1 \le i \le 3$ denote $x_i I + x_4 C_i$ by V_i. It is clear that the IPV's of the V_i, $1 \le i \le 4$, add to (f, f, f), where $f = (d_1+d_2+d_3+3)x_4^2$. But since the sum and fill matrices of (V_1, V_2, V_3, V_4) satisfy (2.1.2), (2.1.5), (2.1.7), (2.1.8), it follows that $f + f + f = 0$, that is, $f = 0$. Hence the IPV's of the V_i add to zero, and thus the V_i satisfy (2.1.18).

Example (2.1.11) completed. The index of the normalizer of $\langle T \rangle$ in S_5 is 6, and so there are at most 6 circulants of order 5 with the same contents whose IPV's differ by more than just a permutation. A complete set of distinct coset representatives of this subgroup is

$$F = \{1, (12), (23), (34), (45), (51)\} .$$

Suppose that a solution (B_1, B_2, B_3, B_4) of (2.1.12) has sum matrix P (2.1.13) and fill matrix (2.1.14) (a). Using the set F, a list L_i of circulants with contents thus specified and essentially different IPV's can be made, for each $i \in \{1, 2, 3, 4\}$. A short search reveals that if B_1, B_2, B_3, B_4, have first rows

$$(x_1, x_2, -x_3, x_3, -x_2) ,$$

$$(x_2, x_4, -x_3, -x_3, -x_4) ,$$

$$(x_3, x_2, x_4, -x_4, x_2) ,$$

$$(-x_4, x_4, x_4, x_4, x_4)$$

respectively, then the B_i satisfy (2.1.12).

(2.2) Generalized Goethals-Seidel arrays

Denote by U_v the multiplicative group of generalized permutation

matrices of order v, that is, the elements of U_v are $v \times v$ matrices with entries from $\{0, 1, -1\}$ such that each row and column contains precisely one nonzero entry. If T denotes the permutation matrix which represents $(1\ 2\ \ldots\ v)$ then the circulant matrices of order v over a commutative ring K with identity are the elements of the group ring $K\langle T\rangle$.

If H is an abelian subgroup of U_v and there is an element R of U_v such that $R^2 = I$ and $R^{-1}AR = A^{-1}$ for all $A \in H$, then we shall call KH a GC-*ring* (*generalized circulant ring*).

The elements of a GC-ring may be used in the Goethals-Seidel array in the same way as circulant matrices. That is, if A_1, A_2, A_3, A_4, are elements of a GC-ring such that

$$\sum_{i=1}^{4} A_i A_i^t = mI \,, \tag{2.2.1}$$

then the rows of

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

are orthogonal.

Wallis and Whiteman [73] showed essentially that if H is an abelian group of permutation matrices, then KH is a GC-ring. The elements of KH are called *type 1 matrices on* H.

Delsarte, Goethals and Seidel [11] introduced another GC-ring. If D denotes the $v \times v$ matrix $\mathrm{diag}(1, 1, \ldots, 1, -1)$, then DT generates a cyclic subgroup L of U_v of order $2v$. The group ring KL is a GC-ring and its elements are called *negacyclic matrices*.

Remarks. (a) Mullin and Stanton [46] use the term *group matrix* rather than *type 1 matrix*.

(b) The definition of type 1 matrix by Wallis and Whiteman in fact only includes the case where H represents a transitive permutation group. However, the extension to the intransitive case is not difficult (see Wielandt [76], pp. 1-10).

(c) Suppose that b is odd and N denotes the $b \times b$ matrix $\mathrm{diag}(1, -1, 1, -1, \ldots, -1, 1)$. Then a $b \times b$ matrix A is circulant if and only if $N^{-1}AN$ is negacyclic. Hence an equation of the form (2.2.4) (or (2.0.1)) has a solution consisting of negacyclic matrices of order b if and only if it has a solution consisting of circulant matrices of order b. (The author is grateful to Dr L.G. Kovács for this observation. See also Theorem 4.2 of [11].)

The Goethals-Seidel array itself may be generalized as follows. Let G denote the group

$$\left\langle r, x_1, x_1^t, x_2, x_2^t, \ldots \mid x_i x_j = x_j x_i,\ x_i x_j^t = x_j^t x_i \text{ for } i, j \in \{1, 2, \ldots\},\ r^2 = 1,\ r x_i r = x_i^t \right\rangle .$$

Denote by S the subset

$$\left\{0, \pm x_1, \pm x_1^t, \pm r x_1, \pm r x_1^t, \pm x_2, \pm x_2^t, \pm r x_1, \pm r x_2^t, \ldots\right\}$$

of the integral group ring $\mathbb{Z}G$. The notion of transpose may be abstracted by defining an operation $(\ )^t$ on $\mathbb{Z}G$ by $(x_i)^t = x_i^t$, $\left(x_i^t\right)^t = x_i$, $r^t = r$, and extending to $\mathbb{Z}G$ in the obvious fashion. If $A = (a_{ij})$ is an $n \times n$ matrix with entries from $\mathbb{Z}G$ then A^* denotes the $n \times n$ matrix with ijth entry a_{ji}^t. If A has entries from S and

$$AA^* = \left(\sum_{i=1}^{u} s_i x_i x_i^t\right) I$$

then A is called a GGS *array (generalized Goethals-Seidel array) of type* $(s_1, s_2, \ldots, s_u)$ *and order* n .

For example, the Goethals-Seidel array itself, written as

$$\begin{bmatrix} x_1 & rx_2^t & rx_3^t & rx_4^t \\ -rx_2^t & x_1 & rx_4 & -rx_3 \\ -rx_3^t & -rx_4 & x_1 & rx_2 \\ -rx_4^t & rx_3 & -rx_2 & x_1 \end{bmatrix}$$

is a GGS array of type $(1, 1, 1, 1)$ and order 4 .

The essential use of GGS arrays is immediate. Suppose that there is a GGS array A of type $(s_1, s_2, \ldots, s_u)$ and order n , and $X_1, X_2, \ldots, X_u$ are $v \times v$ matrices from some GC-ring such that the entries of the X_i are from $\{0, \pm y_1, \pm y_2, \ldots, \pm y_l\}$ and

$$\sum_{i=1}^{4} s_i X_i X_i^t = \left(\sum_{j=1}^{l} m_j y_j^2 \right) I \ .$$

Then replacing the entries of A with the appropriate matrices yields an orthogonal design of type $(m_1, m_2, \ldots, m_l)$ and order nv . Examples of orthogonal designs constructed in this way are given in the next section and in Chapter 5.

More importantly, GGS arrays may be used to produce more GGS arrays.

(2.2.2) **THEOREM.** *Suppose that there is a GGS array of type* $(s_1, s_2, \ldots, s_u)$ *and order* n , *and the* $v \times v$ *matrices* $A_1, A_2, \ldots, A_u$ *are from some GC-ring and have entries from* $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$. *If*

$$\sum_{i=1}^{4} s_i A_i A_i^* = \left(\sum_{j=1}^{l} m_j x_j x_j^t \right) I$$

then there is a GGS array of type $(m_1, m_2, \ldots, m_l)$ *and order* nv .

Proof. Suppose that A is a GGS array of type $(s_1, s_2, \ldots, s_u)$ and

order v , and the following replacements are made:

$$0 \longmapsto \text{zero matrix of order } v \ ;$$

$$\pm x_i \longmapsto \pm A_i \ ;$$

$$\pm x_i^t \longmapsto \pm A_i^t \ ;$$

$$\pm r x_i \longmapsto \pm r R A_i \ ;$$

$$\pm r x_i^t \longmapsto \pm r R A_i^* \ .$$

Then the resulting matrix B has entries from S and

$$BB^* = \left(\sum_{i=1}^{u} s_i A_i A_i^* \right) \times I_n$$

$$= \left(\sum_{j=1}^{l} m_j x_j x_j^t \right) I_{nv} \ . \qquad \square$$

To illustrate this theorem a GGS array of type (2, 2) and order 6 is constructed. The two-circulant construction (2.0.6) gives a GGS array of type (1, 1) and order 2 :

$$\begin{bmatrix} x_1 & r x_2^t \\ -r x_2^t & x_1 \end{bmatrix} \ .$$

The circulant matrices

$$A_1 = \begin{bmatrix} x_1 & x_2 & \\ & x_1 & x_2 \\ x_2 & & x_1 \end{bmatrix} \quad \text{and} \quad A_2 = \begin{bmatrix} x_1 & -x_2 & \\ & x_1 & -x_2 \\ -x_2 & & x_1 \end{bmatrix}$$

satisfy $A_1 A_1^* + A_2 A_2^* = 2\left(x_1 x_1^t + x_2 x_2^t \right) I$. Following the replacements in the proof of Theorem (2.2.2), a GGS array of type (2, 2) and order 6 is obtained:

$$\begin{bmatrix} x_1 & x_2 & & & -rx_2^t & rx_1^t \\ & x_1 & x_2 & -rx_2^t & rx_1^t & \\ x_2 & & x_1 & rx_1^t & & -rx_2^t \\ & rx_2^t & -rx_1^t & x_1 & x_2 & \\ rx_2^t & -rx_1^t & & & x_1 & x_2 \\ -rx_1^t & & rx_2^t & x_2 & & x_1 \end{bmatrix} .$$

Note that the theorem could be applied a times to obtain a GGS array of type $(2^a, 2^a)$ and order $3^a.2$.

The existence of a GGS array clearly implies the existence of an orthogonal design of the same type and order, but the converse is false (see section (2.4)). In many cases, however, the converse is true. An important fact is that every orthogonal design on 2 variables can be made into a GGS array by replacing the second variable x_2 by rx_2^t . The following proposition gives some infinite families of GGS arrays with 4 variables.

(2.2.3) PROPOSITION. *Suppose that a is a positive integer and l is a product of at least a positive integers, that is, $l = l_1 l_2 \ldots l_j$ where $j \geq a$.*

(a) If $l_i \geq 2$ for $1 \leq i \leq j$ then there is a GGS array of type $(2^a, 2^a, 2^a, 2^a)$ and order $4l$.

(b) If $l_i \geq 4$ for $1 \leq i \leq j$ then there are GGS arrays of type $(3^a, 3^a, 3^a, 3^a)$ and $(4^a, 4^a, 4^a, 4^a)$ and order $4l$.

Proof. For $l_1 \geq 2$ consider the sequences $a_1 = (x_1, x_2, {}^0l_1{}^{-2})$, $a_2 = (x_1, -x_2, {}^0l_1{}^{-2})$, $a_3 = (x_3, -x_4, {}^0l_1{}^{-2})$, $a_4 = (x_3, x_4, {}^0l_1{}^{-2})$, where ${}^0l_1{}^{-2}$ denotes a sequence of $l_1 - 2$ zeros. These sequences are

complementary, and further, if A_i is the circulant matrix with first row a_i then

$$\sum_{i=1}^{4} A_i A_i^* = 2\left(\sum_{i=1}^{4} x_i x_i^t\right) I \ .$$

Using Theorem (2.2.2) and the Goethals-Seidel array, a GGS array of type $(2, 2, 2, 2)$ and order $4l_1$ may be obtained. Repeating this procedure a times gives (a). For (b) the following complementary sequences may be used in a similar fashion:

$(3, 3, 3, 3)$: $(0, -x_2, -x_3, -x_4)$, $(x_1, 0, -x_3, x_4)$,

$(x_1, x_2, 0, -x_4)$, $(x_1, -x_2, x_3, 0)$,

$(4, 4, 4, 4)$: $(x_1, -x_2, -x_3, -x_4)$, $(x_1, x_2, -x_3, x_4)$,

$(x_1, x_2, x_3, -x_4)$, $(x_1, -x_2, x_3, x_4)$. □

A numerical investigation of GGS arrays of order 12 has been made and the results are listed in section (5.7). These GGS arrays have been used to construct orthogonal designs of orders 36 and 60 . Examples are given in section (5.4).

GGS arrays with 2 variables have been used successfully for constructing orthogonal designs of highly composite orders equivalent to 2 modulo 4 . Examples are given in section (5.3). (See also [70].)

Finally, we note that there are several other methods of using circulant matrices to construct orthogonal designs (see [72]). However, it seems that GGS arrays are the most powerful method for orders not divisible by 8 .

(2.3) Some infinite families of orthogonal designs

The Goethals-Seidel array and its generalizations have been used to construct many infinite families of orthogonal designs. Some examples are

listed in [19] and [13]. The theorems below illustrate some of the techniques involved.

(2.3.1) THEOREM. *If there is a GGS array of type* $(s_1, s_2, \ldots, s_u)$ *and order* n *then there is an orthogonal design of type* $(s_1, s_1, s_2, s_2, \ldots, s_u, s_u)$ *and order* $2n$.

Proof. The negacyclic matrix

$$X_i = \begin{bmatrix} x_i & y_i \\ -y_i & x_i \end{bmatrix}$$

is an orthogonal design of type $(1, 1)$. Hence

$$\sum_{i=1}^{u} s_i X_i X_i^t = \left(\sum_{i=1}^{u} s_i \left(x_i^2 + y_i^2 \right) \right) I \ . \qquad \square$$

The combination of Theorem (2.3.1) and Proposition (2.2.3) gives a large collection of orthogonal designs. For example, for each $a > 0$ there is an orthogonal design of type $(4^a, 4^a, 4^a, 4^a, 4^a, 4^a, 4^a, 4^a)$ and order 8.5^a .

(2.3.2) THEOREM. *Suppose that* q *is a prime power of the form* $3m + 1$. *Then there is a skew symmetric weighing matrix of weight* q^2 *and order* $4(q^2+q+1)/3$.

Proof. For each v denote the $v \times v$ permutation matrix which represents $(1\ 2\ \ldots\ v)$ by T_v . Since $q = 3m + 1$, 3 divides $q^2 + q + 1$ but 9 does not divide $q^2 + q + 1$. Hence the group S_1 of permutation matrices generated by T_{q^2+q+1} is isomorphic to the group generated by $T_{3m^2+3m+1} \times T_3$. Both these groups represent transitive permutation groups and it follows (see [16]) that they are conjugate. Hence for each circulant matrix W of order $q^2 + q + 1$ there is a permutation

matrix N of order $q^2 + q + 1$ such that $N^{-1}WN$ has the form

$$\begin{bmatrix} X_1 & X_2 & X_3 \\ X_3 & X_1 & X_2 \\ X_2 & X_3 & X_1 \end{bmatrix}$$

where the X_i are circulant matrices of order $3m^2 + 3m + 1$. If W is a circulant weighing matrix of weight q^2 (see section (1.4)) then the X_i have entries from $\{0, 1, -1\}$ and

$$X_1X_1^t + X_2X_2^t + X_3X_3^t = q^2I .$$

Thus x_1I, x_2X_1, x_2X_2, x_2X_3, may be used in the Goethals-Seidel array to obtain an orthogonal design of type $(1, q^2)$ and order $4(3m^2+3m+1)$. □

(2.3.3) THEOREM. *Suppose that there is a skew symmetric weighing matrix of weight k and order n, and $4k - 1$ is prime. Then there is a skew symmetric weighing matrix of weight $4k^2$ and order $(4k-1)n$.*

Proof. Since $4k - 1$ is prime there is a cyclic difference set D with parameters $(v, k, \lambda) = (4k-1, 2k, k)$. Further, D may be chosen so that $0 \in D$ and for $x \neq 0$, $x \in D$ if and only if $-x \notin D$. (Baumert [3] has details on difference sets.) Denote the incidence matrix of this difference set by B. The circulant matrices $A_1 = x_2B$ and $A_2 = x_1I + x_2(B-J-I)$ satisfy

$$A_1A_1^t + kA_2A_2^t = \left(x_1^2+4k^2x_2^2\right)I_{4k-1} .$$

The theorem follows since a skew symmetric weighing matrix of weight k may be used as a GGS array of type $(1, k)$. □

(2.3.4) THEOREM. *Suppose that q is a prime power and $q^2 + q + 1$ is a prime of the form $4m - 1$. Then there are orthogonal designs of types*

$(1, 1, 2q^2, 2(q+1)^2)$ *and* $(1, 1, q^2+(q+1)^2, q^2+(q+1)^2)$ *and order* $4(q^2+q+1)$.

Proof. Suppose that W is a circulant weighing matrix of weight q^2 and order $q^2 + q + 1$ (see (1.4)). Denote J - abs(W) by B . It can be shown that B is the incidence matrix of a cyclic projective plane of order q (see [34]); hence $BB^t = qI + J$. If $q^2 + q + 1 = 4m - 1$ and is prime, then there is a cyclic difference set E with parameters $(4m-1, 2m-1, m-1)$ such that $0 \notin E$, and for $x \neq 0$, $x \in E$ if and only if $-x \notin E$ [3]. (In fact E is the complement of the difference set in the proof of the previous theorem.) If F is the incidence matrix of E , then $A = 2F - J$ is skew-symmetric and $AA^t = (q^2+q+1)I - J$. The circulant matrices

$$X_1 = x_1 I + x_3 A ,$$

$$X_2 = x_2 I + x_4 A ,$$

$$X_3 = x_3 W + x_4 B ,$$

$$X_4 = x_4 W - x_3 B ,$$

satisfy

$$\sum_{i=1}^{4} X_i X_i^t = \left(x_1^2+x_2^2+(2q^2+2q+1)\left(x_3^2+x_4^2\right)\right) I .$$

The circulant matrices

$$Y_1 = x_1 I + x_4 A ,$$

$$Y_2 = x_2 I + x_4 A ,$$

$$Y_3 = x_3 W + x_4 B ,$$

$$Y_4 = x_3 W - x_4 B ,$$

satisfy

$$\sum_{i=1}^{4} Y_i Y_i^t = \left(x_1^2+x_2^2+2q^2x_3^2+2(q+1)^2x_4^2\right) I . \qquad \square$$

Remark. It is not known whether Theorem (2.3.4) generates an infinite family of orthogonal designs. The first few primes in

$$\{q^2+q+1 : q \text{ is a prime power and } q^2+q+1 \equiv 3 \pmod 4\}$$

are 7, 31, 307, 1723, 8011, 9507.

(2.3.5) THEOREM. *Suppose that* q *is a prime power and* $v \geq 6$. *Then there are orthogonal designs of types* $(5, 5q^2)$, $(5q^2, 5q^2)$, $(10, 10q^2)$, $(5(q^2+1), 5(q^2+1))$ *and order* $2v(q^2+q+1)$.

Proof. The existence of an orthogonal design of type (5, 5) and order $2v$ is established in [21]. Hence there is a GGS array of type (5, 5) and order $2v$. The circulant weighing matrices of weight q^2 and order $q^2 + q + 1$ may be used to complete the proof. □

(2.4) Limitations

There are two ways in which the use of GGS arrays for constructing orthogonal designs is limited.

Firstly, little is known about the existence of GGS arrays. The numerical investigation of GGS arrays of order 12 (see section (5.7)) shows that existence of a GGS array is harder to establish than existence of the corresponding orthogonal design. Further, it can be deduced from Theorem (2.3.1) that the number of variables of a GGS array of order n is at most $[\frac{1}{2}\rho(2n)]$. If 8 divides n then $[\frac{1}{2}\rho(2n)] < \rho(n)$ and so there are many orthogonal designs for which a corresponding GGS array does not exist. Note also that if 16 divides n then $[\frac{1}{2}\rho(2n)] > 4$, but no GGS array with more than 4 variables is known.

Secondly, it can be proved that not all orthogonal designs can be constructed using GGS arrays. There is an orthogonal design of type (4, 9) and order 14 (see [23]). However, using the methods of section (2.2), it can be shown that there is no orthogonal design of type (4, 9) and order

14 constructed by using two 7×7 circulant matrices in the two-circulant construction. Using the same methods it can be shown that there are no orthogonal designs of types (3, 7, 8), (1, 3, 6, 8), (1, 4, 4, 9), or (2, 2, 5, 5) and order 20 constructed using GGS arrays (see [14], [15]). However it is not known whether there are any orthogonal designs of order equivalent to 4 modulo 8 which cannot be constructed using GGS arrays. The existence of orthogonal designs of types (3, 7, 8), (1, 3, 6, 8), (1, 4, 4, 9), (2, 2, 5, 5) and order 20 is undetermined and the author knows of no efficient method of solving this problem.

CHAPTER 3

ASYMPTOTIC EXISTENCE RESULTS

Geramita and Pullman [25] proved that for every positive integer n there is an orthogonal design of type $(1, 1, 1, \ldots, 1)$ and order n on $\rho(n)$ variables. Since the function $a \mapsto \rho(2^a)$ is strictly increasing, an asymptotic result may be immediately deduced.

(3.0.1) THEOREM. *If $s_1, s_2, \ldots, s_u, b$, are positive integers then there is an integer N such that there is an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order $2^a b$ for all $a \geq N$.* □

For example, it is not known whether there is an orthogonal design of type $(1, 3, 6, 8)$ and order 20, but the existence of an orthogonal design of this type and order $2^a.5$ may be obtained for large a as follows. If $a \geq 10$ then $\rho(2^a) \geq 18 = 1 + 3 + 6 + 8$. Hence there is an orthogonal design of type $(1, 1, 1, \ldots, 1)$ and order $2^a.5$ on 18 variables for all $a \geq 10$. Equating variables gives an orthogonal design of type $(1, 3, 6, 8)$ and order $2^a.5$ for all $a \geq 10$.

However this result is unsatisfactory. It is not useful in applications because the orthogonal designs obtained are very sparse - the ratio of the number of nonzero entries per row to the order in the example above is less than $.004$. In section (3.1) an asymptotic result which preserves fullness is obtained. This result is related to the Robinson-Seberry conjecture (0.0.15) and Wallis' Theorem (0.0.16).

Also, Theorem (3.0.1) sheds no light on the question of sufficiency of the algebraic necessary conditions (0.0.9) and (0.0.10). This is because the power of 2 dividing the order of the orthogonal design is allowed to vary considerably. Asymptotic existence results for orders divisible by a

fixed power of 2 are proved in section (3.2). Several cases of the Asymptotic Sufficiency Conjecture (0.0.14) are obtained.

(3.1) Asymptotic existence of full orthogonal designs

If the positive integers $n, s_1, s_2, \ldots, s_u$, are all highly divisible by 2, then in many cases the existence of an orthogonal design of type $s_1, s_2, \ldots, s_u$ and order n may be established. Specifically, we prove:

(3.1.1) THEOREM. *Suppose that r and n are positive integers, $b_1, b_2, \ldots, b_l$, are powers of 2, and there is an orthogonal design of type $(b_1, b_2, \ldots, b_l)$ and order $2^r n$. If $s_1, s_2, \ldots, s_u$, are positive integers with sum $2^d(b_1 + b_2 + \ldots + b_l)$ for some $d \geq 0$, then there is an integer N such that an orthogonal design of type $\left(2^a s_1, 2^a s_2, \ldots, 2^a s_u\right)$ and order $2^{a+d+r}n$ exists for each $a \geq N$.*

Before a proof of this theorem is given, we present a corollary which gives full orthogonal designs of order $2^a n$ for small n.

(3.1.2) COROLLARY. *Suppose that $1 \leq n \leq 8$ and $s_1, s_2, \ldots, s_u$, are positive integers with sum $2^d n$ for some $d \geq 0$. Then there is an integer N such that an orthogonal design of type $\left(2^a s_1, 2^a s_2, \ldots, 2^a s_u\right)$ and order $2^{a+d}n$ exists for each $a \geq N$.*

Proof. There are full orthogonal designs of type (1) and order 1, type (1, 1, 2, 8) and order 12, type (4, 4, 8) and order 20, and type (4, 4, 4, 16) and order 28 (see [24], [31], [19]). The corollary follows for $n = 1, 3, 5$ and 7. For n even, write n as $2^c n_1$ where n_1 is odd. □

Remark. The case $n = 1$ of this corollary is proved in [18].

Proof of Theorem (3.1.1). Theorem (1.3.1) implies that if there is an orthogonal design of type $(a_1, a_2, \ldots, a_v)$ and order m, then there are orthogonal designs of types $(2a_1, 2a_2, \ldots, 2a_v)$ and $(a_1, a_1, 2a_2, 2a_3, \ldots, 2a_v)$ and order $2m$. This result is used extensively below.

Suppose that there is an orthogonal design of type $(b_1, b_2, \ldots, b_l)$ and order $2^r n$ where each b_i is a power of 2. Denote the sum of the b_i by f. If d is a nonnegative integer then denote the sequence $\left(2^d b_1, 2^d b_2, \ldots, 2^d b_l\right)$ by B. By Theorem (1.3.1) there is an orthogonal design of type B and order $2^{d+r} n$. If 2^j is the highest power of 2 which occurs in B and $j > 0$, then replace one occurrence of 2^j with $(2^{j-1}, 2^{j-1})$ to form a sequence B' of length $l + 1$. Using Theorem (1.3.1), there is an orthogonal design of type $2B'$ and order 2^{d+r+1}. Again, if 2^i is the highest power of 2 occurring in B' and $i > 0$, then replace one occurrence of 2^i with $(2^{i-1}, 2^{i-1})$ to form a sequence B''; there is an orthogonal design of type $4B''$ and order 2^{d+r+2}. Continuing in this fashion, an orthogonal design A of type $2^N(1, 1, 1, \ldots, 1)$ and order $2^{d+r+N} n$ on $2^d f$ variables may be obtained, where N denotes $2^d f - l$. If $s_1, s_2, \ldots, s_u$ are positive integers with sum $2^d f$, then equating variables in A gives an orthogonal design of type $2^N(s_1, s_2, \ldots, s_u)$ and order $2^{d+r+N} n$. Using Theorem (1.3.1), an orthogonal design of type $2^a(s_1, s_2, \ldots, s_u)$ and order $2^{d+r+a} n$ may be obtained for all $a \geq N$. □

The above proof is chosen for its simplicity and generality. Other methods give smaller values of N in particular cases.

For example, if d is an integer greater than 2 then denote by N_d the smallest integer such that an orthogonal design of type $(2^a, 2^a, 2^a, 2^a, 2^a, 2^a(2^d-5))$ and order 2^{a+d} exists for each $a \geq N_d$. The existence of N_d is assured by Corollary (3.1.2), and Robinson's Theorem (0.0.13) shows that for $d > 5$, $N_d \neq 0$. Following through the proof of Theorem (3.1.1) above it can be shown that N_d is at most $2^d - 1$. However, the methods of [18] can be used as follows to obtain $N_d \leq 3$ for all $d \geq 3$.

There is an orthogonal design of type (1) and order 1 and repeated applications of Theorem (1.3.1) give orthogonal designs

of type $(1, 1)$ and order 2,

of type $(1, 1, 2)$ and order 4,

of type $(1, 1, 2, 4)$ and order 8,

$\vdots \quad \vdots \quad \vdots \quad \vdots$

of type $(1, 1, 2, 4, 8, 16, \ldots, 2^{d-1})$ and order 2^d,

of type $(2, 2, 4, 4, 4, 16, 32, \ldots, 2^d)$ and order 2^{d+1},

of type $(4, 4, 4, 4, 8, 8, 32, 64, \ldots, 2^{d+1})$ and order 2^{d+2},

of type $(8, 8, 8, 8, 8, 8, 16, 64, 128, \ldots, 2^{d+2})$ and order 2^{d+3}.

Now $8 + 16 + 64 + 128 + \ldots + 2^{d+2} = 8(2^d-5)$. Hence by equating variables an orthogonal design of type $(8, 8, 8, 8, 8, 8(2^d-5))$ and order 2^{d+3} may be obtained. From Theorem (1.3.1) we deduce that $N_d \leq 3$.

Remark. Using sophisticated constructions Robinson [58] has established the existence of an orthogonal design of type $(1, 1, 1, 1, 2, 2, 4, 4, \ldots, 2^{d-2}, 2^{d-2})$ and order 2^d for each $d > 2$. Methods similar to those above may be applied to this orthogonal design to

obtain $N_d \leq 1$. Hence for $d > 5$, $N_d = 1$. For $2 < d < 5$ Robinson [57] has shown that $N_d = 0$. The case $d = 5$ remains open.

(3.2) Asymptotic sufficiency of the algebraic necessary conditions

The conjecture (0.0.14) that the algebraic necessary conditions ((0.0.9), (0.0.10)) are asymptotically sufficient for existence is discussed in this section. The main results are Theorems (3.2.1), (3.2.2), (3.2.3) and (3.2.6) below.

Suppose that there is a weighing matrix of weight k and order $2^a b$ where b is odd. Then it follows from the algebraic necessary conditions that k can be written as a sum of 2^a squares. Similarly, the existence of a skew symmetric weighing matrix of weight k and order $2^a b$ implies that $a > 0$ and k can be written as a sum of $2^a - 1$ squares. These necessary conditions are asymptotically sufficient.

(3.2.1) **THEOREM.** *(a) Suppose that k can be written as a sum of 2^a squares. Then there is an integer N such that a weighing matrix of weight k and order $2^a n$ exists for each $n \geq N$.*

(b) Suppose that $a > 0$ and k can be written as a sum of $2^a - 1$ squares. Then there is an integer N such that a skew symmetric weighing matrix of weight k and order $2^a n$ exists for each $n \geq N$.

Remark. Geramita and Wallis [31] have also obtained the case $a = 0$ of Theorem (3.2.1) (a).

For orders equivalent to 2 modulo 4 , the existence of an orthogonal design of type (s_1, s_2) implies the existence of a rational 2×2 matrix P such that $PP^t = \mathrm{diag}(s_1, s_2)$. This condition is asymptotically sufficient for existence.

(3.2.2) THEOREM. *Suppose that* s_1 *and* s_2 *are positive integers such that there is a* 2×2 *rational matrix* P *satisfying* $PP^t = \mathrm{diag}(s_1, s_2)$. *Then there is an integer* N *such that an orthogonal design of type* (s_1, s_2) *and order* $2n$ *exists for each* $n \geq N$.

If b is odd then $\rho(4b) = 4$ and so an orthogonal design of order $4b$ has at most 4 variables. The existence of an orthogonal design of type (s_1, s_2, s_3, s_4) implies the existence of a rational 4×4 matrix P such that $PP^t = \mathrm{diag}(s_1, s_2, s_3, s_4)$. With some added hypotheses, this condition is asymptotically sufficient.

(3.2.3) THEOREM. *Suppose that* s_1, s_2, s_3, s_4 , *are positive integers and there is a* 4×4 *rational matrix* P *such that* $PP^t = \mathrm{diag}(s_1, s_2, s_3, s_4)$. *Denote the squarefree part of* s_i *by* t_i *for* $1 \leq i \leq 4$. *Further suppose that either*

(3.2.4) $$t_1 = t_2 = t_3 = t_4$$

or

(3.2.5) $t_1 = t_2$ *and every prime factor of* $\gcd(t_1, t_3)$ *is either* $2, 3$, *or of the form* $4m + 1$.

Then there is an integer N *such that an orthogonal design of type* (s_1, s_2, s_3, s_4) *and order* $4n$ *exists for all* $n \geq N$.

Remark. Similar partial results may be obtained for asymptotic existence of two and three variable orthogonal designs of order equivalent to 4 modulo 8 . The extent to which these partial results cover types $(s_1, \ldots, s_u)$ with $u \in \{2, 4\}$ and $s_1 + \ldots + s_u \leq 36$ is indicated in sections (5.4) and (5.5).

If $s_1, s_2, \ldots, s_u$, are positive integers with $u \leq 5$, then there is

a rational $u \times 8$ matrix P such that $PP^t = \text{diag}(s_1, s_2, \ldots, s_u)$ (see [79]). Hence the algebraic necessary conditions for the existence of orthogonal designs of order divisible by 8 with less than 6 variables are always satisfied. For two variables, an asymptotic result may be obtained.

(3.2.6) THEOREM. *If s_1 and s_2 are positive integers then there is an integer N such that an orthogonal design of type (s_1, s_2) and order $8n$ exists for each $n \geq N$.*

The proofs of the theorems above occupy the rest of this section. Three lemmas are used.

The first lemma establishes the existence of type 1 weighing matrices which can be used as building blocks in the constructions to follow.

(3.2.7) LEMMA. *Suppose that $k_1, k_2, \ldots, k_u$, are square integers. Then for some group H of permutation matrices of odd order there are mutually disjoint type 1 weighing matrices $W_1, W_2, \ldots, W_u$, on H such that W_i has weight k_i.*

Proof. Suppose that $k_j = q_1^2 q_2^2 \ldots q_m^2$ where each q_i is a prime power. If L_i is a circulant weighing matrix of weight q_i^2 and order $q_i^2 + q_i + 1$ for $1 \leq i \leq m$ (see section (1.4)) then the kronecker product $V_j = L_1 \times L_2 \times \ldots \times L_m$ is a type 1 weighing matrix of weight k_j on a group G_j of odd order $m_j = \prod_{i=1}^{m} \left(q_i^2+q_i+1\right)$. For each $j \in \{1, 2, \ldots, u\}$ denote

$$I_{m_1} \times I_{m_2} \times \ldots \times I_{m_{j-1}} \times V_j \times I_{m_{j+1}} \times \ldots \times I_{m_u}$$

by V_j'. Note that for every $j \in \{1, 2, \ldots, u\}$, V_j' is a type 1 weighing

matrix of weight k_j on the group

$$G = \{M_1 \times M_2 \times \ldots \times M_u : M_r \in G_r\}$$

of permutation matrices of odd order $m_1 m_2 \ldots m_u$. Let v be an odd integer at least as large as u, and denote the $v \times v$ permutation matrix which represents $(1\ 2\ \ldots\ v)$ by T. For $1 \le j \le u$ denote $T^j \times V_j'$ by W_j. It is clear that W_j is a type 1 weighing matrix of weight k_j on the group

$$H = \{M \times T^i : 0 \le i < v,\ M \in G\}$$

of permutation matrices of odd order $m_1 m_2 \ldots m_u v$. For $i \ne j$, $T^i * T^j = 0$ and so $W_i * W_j = 0$. □

The second lemma reduces the problem of asymptotic existence to finding orthogonal designs of a particular order.

(3.2.8) LEMMA. *Suppose that there is an orthogonal design of type* $(s_1, s_2, \ldots, s_u)$ *and order* $2^a b$ *where* b *is odd. Then there is an integer* N *such that an orthogonal design of type* $(s_1, s_2, \ldots, s_u)$ *and order* $2^a n$ *exists for each* $n \ge N$.

Proof. For sufficiently large d there is an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order 2^d given by Theorem (3.0.1). We can assume that $d > a$, for if $d \le a$ then the existence of an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order 2^{a+1} is assured by elementary constructions (see section (1.2)). Since b is odd it is prime to 2^{d-a} and so every integer at least as large as $(b-1)(2^{d-a}-1)$ can be written as $bm + 2^{d-a}l$ for nonnegative integers m and l. Using elementary constructions (section (1.2)) it can be deduced that if $N = (b-1)(2^{d-a}-1)$,

then there is an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order $2^a n$ for each $n \geq N$.

Remark. The use of Theorem (3.0.1) in the proof of Lemma (3.2.8) means that the integer d must be at least $\frac{1}{2}(s_1 + s_2 + \ldots + s_u)$. This implies that N depends exponentially on the sum of the s_i and thus is very large. However, in many cases other existence results for orthogonal designs of order a power of two (e.g. Theorem (1.3.3)) may be used to obtain a smaller value of N. The numerical results of Chapter 5 seem to indicate that N may be bounded by a linear function of $s_1, s_2, \ldots, s_u$, but we have been unable to prove this.

The third lemma shows that only types $(s_1, s_2, \ldots, s_u)$ where each s_i is squarefree need to be considered.

(3.2.9) **LEMMA.** *Suppose that $k_1, k_2, \ldots, k_u$, are square integers and there is an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order n. Then there is an odd integer v such that an orthogonal design of type $(k_1 s_1, k_2 s_2, \ldots, k_u s_u)$ and order nv exists.*

Proof. Suppose that q^2 is a prime power which divides k_1 and W is a circulant weighing matrix of weight q^2 and order $q^2 + q + 1$. If R is the backdiagonal matrix of order $q^2 + q + 1$ then WR is symmetric (see section (1.4)). Hence the u-tuple $(x_1 WR, x_2 I, x_3 I, \ldots, x_u I)$ is amicable (see section (1.3)) and so there is an orthogonal design of type $\left(q^2 s_1, s_2, \ldots, s_u\right)$ and order $n(q^2+q+1)$. Note that $q^2 + q + 1$ is odd. This process may be continued to achieve the desired result. □

Theorem (3.2.6) may be deduced from the lemmas above as follows. If

s_1 and s_2 are integers then there are squares $k_1, k_2, \ldots, k_e$, $l_1, l_2, \ldots, l_f$ such that $s_1 = k_1 + k_2 + \ldots + k_e$ and $s_2 = l_1 + l_2 + \ldots + l_f$, and e and f are each at most 4 (see [64]). There is an orthogonal design of type $(1, 1, \ldots, 1)$ and order 8 on $e + f$ variables [24]. Hence by Lemma (3.2.9) there is an orthogonal design of type $(k_1, k_2, \ldots, k_e, l_1, l_2, \ldots, l_f)$ and order $8v$ for some odd v. Using Lemma (3.2.8) and equating variables, we obtain Theorem (3.2.6).

Note that Theorem (3.2.6) implies the case $a \geq 3$ of Theorem (3.2.1). The case $a < 3$ of Theorem (3.2.1) may be obtained in a similar fashion, by constructing orthogonal designs of types $\left(m_1^2, m_2^2, \ldots, m_u^2\right)$ and order $2^a v$ for v odd, and equating variables.

The case (3.2.4) of Theorem (3.2.3) can be established by using Lemma (3.2.7) and a construction from [68] and [10] as follows. If m is a positive integer then there are integer squares k_1, k_2, k_3, k_4, such that $m = k_1 + k_2 + k_3 + k_4$ [64]. Denote the type 1 weighing matrices of weights k_1, k_2, k_3, k_4, obtained in Lemma (3.2.7) by W_1, W_2, W_3, W_4. (If $k_i = 0$, then the zero matrix may be used for W_i.) Suppose that

$$A_1 = x_1W_1 + x_2W_2 + x_3W_3 + x_4W_4 ,$$

$$A_2 = -x_2W_1 + x_1W_2 + x_4W_3 - x_3W_4 ,$$

$$A_3 = -x_3W_1 - x_4W_2 + x_1W_3 + x_2W_4 ,$$

$$A_4 = -x_4W_1 + x_3W_2 - x_2W_3 + x_1W_4 .$$

Then the A_i are type 1 matrices of odd order b with entries from $\{0, \pm x_1, \pm x_2, \pm x_3, \pm x_4\}$ such that

$$\sum_{i=1}^{4} A_i A_i^t = \left(\sum_{i=1}^{4} mx_i^2\right) I .$$

Using the Goethals-Seidel construction (2.0.3) an orthogonal design of type (m, m, m, m) and order $4b$ may be obtained. If l_1, l_2, l_3, l_4, are squares then Lemma (3.2.9) may be used to establish the existence of an orthogonal design of type (l_1m, l_2m, l_3m, l_4m) and order equivalent to 4 modulo 8. Using Lemma (3.2.8) the case (3.2.4) of Theorem (3.2.3) may be obtained.

For the case (3.2.5) of Theorem (3.2.3), suppose that P is a 4×4 rational matrix such that $PP^t = \text{diag}(s_1, s_2, s_3, s_4)$. If t_i denotes the squarefree part of s_i, then by dividing the ith row of P by $\sqrt{s_i/t_i}$ for $1 \leq i \leq 4$ we obtain a 4×4 rational matrix P_1 such that $P_1P_1^t = \text{diag}(t_1, t_2, t_3, t_4)$. If $t_1 = t_2$, then a consideration of determinants yields $t_3 = t_4$.

Denote $\gcd(t_1, t_3)$ by g, t_1/g by r_1 and t_3/g by r_3. A standard Hasse invariant argument, using the fact that r_1 is prime to r_3, shows that both r_1 and r_3 can be written as sums of two squares. We next show that it follows that there are type 1 matrices B_1, B_2, B_3, B_4 of odd order such that

$$\sum_{i=1}^{4} B_iB_i^t = \left(r_1x_1^2+r_1x_2^2+r_3x_3^2+r_3x_4^2\right)I \quad . \tag{3.2.10}$$

In fact we claim something stronger, namely that if k_1, k_2, k_3, k_4 are squares then there are type 1 matrices A_1, A_2, A_3, A_4 of odd order and with entries from $\{0, \pm x_1, \pm x_2, \pm x_3, \pm x_4\}$ such that

$$\sum_{i=1}^{4} A_iA_i^* = \left((k_1+k_2)\left(x_1x_1^t+x_2x_2^t\right)+(k_3+k_4)\left(x_3x_3^t+x_4x_4^t\right)\right)I \tag{3.2.11}$$

(see section (2.2) for the definition of A^*). For suppose that

W_1, W_2, W_3, W_4 are the type 1 weighing matrices of weights k_1, k_2, k_3, k_4 obtained in Lemma (3.2.7). If

(3.2.12)
$$A_1 = x_1W_1 + x_2W_2 ,$$
$$A_2 = x_2W_1^t - x_1W_2^t ,$$
$$A_3 = x_3W_3 + x_4W_4 ,$$
$$A_4 = x_4W_3^t - x_3W_4^t ,$$

then the A_i satisfy (3.2.11). If $r_1 = k_1 + k_2$ and $r_2 = k_3 + k_4$, then we have (3.2.10).

If each prime factor of g is either 2, 3, or of the form $4m + 1$ then the existence of a GGS array of type (g, g, g, g) and order equivalent to 4 modulo 8 may be deduced. For if $l \geq 0$ and 3^l is the highest power of 3 which divides g then there is a GGS array of type $(3^l, 3^l, 3^l, 3^l)$ and order 4.5^l (see Proposition (2.2.3)). Since $g/3^l$ has no factors equivalent to 3 modulo 4, $g/3^l$ can be written as a sum of two squares (see [64], p. 351). Hence using the type 1 matrices (3.2.11) above with $g/3^l = k_1 + k_2 = k_3 + k_4$, there is a GGS array of type (g, g, g, g) and order equivalent to 4 modulo 8 (see Theorem (2.2.2)). Using the matrices B_i which satisfy (3.2.10) in this GGS array gives an orthogonal design of type (t_1, t_2, t_3, t_4) and order equivalent to 4 modulo 8. Hence, by Lemma (3.2.9), there is an orthogonal design of type (s_1, s_2, s_3, s_4) and order $4b$, b odd. This case (3.2.5) of Theorem (3.2.3) follows by Lemma (3.2.8).

Theorem (3.2.2) can be proved in a similar fashion. If there is a 2×2 rational matrix P such that $PP^t = \mathrm{diag}(s_1, s_2)$, then there are

integers m_1, m_2, m_3, m_4 such that $s_1 = m_1^2\left(m_3^2+m_4^2\right)$ and $s_2 = m_2^2\left(m_3^2+m_4^2\right)$.

A construction similar to (3.2.11) gives an orthogonal design of type $\left(m_3^2+m_4^2,\ m_3^2+m_4^2\right)$ and order equivalent to 2 modulo 4. Theorem (3.2.2) follows by using the lemmata.

CHAPTER 4

INTEGRAL SOLUTIONS

(4.1) Introduction and the main theorems

An integral analogue to the Rational Family Theorem (0.0.8) is provided in this chapter.

Recall that a *rational family* F 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

(4.1.1) $$A_i A_i^t = s_i I \quad \text{for} \quad 1 \le i \le u \ ;$$

(4.1.2) $$A_i A_j^t + A_j A_i^t = 0 \quad \text{for} \quad 1 \le i < j \le u \ .$$

If F also satisfies

(4.1.3) $$A_i * A_j = 0 \quad \text{for} \quad 1 \le i < j \le u \ ,$$

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

then $\sum_{i=1}^{u} x_i A_i$ is an orthogonal design.

A rational family which consists of integral matrices shall be called an *integral family*. An integral family shall be called *combinatorial* if it satisfies (4.1.3), that is, if its elements are mutually disjoint.

A necessary and sufficient condition for the existence of integral families of order not divisible by 16 is obtained in this chapter. 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 $(s_1, s_2, \ldots, s_u)$ then $A = \sum_{i=1}^{u} x_i A_i$ has entries from

$\{mx_i : 1 \le i \le u,\ m \in \mathbb{Z}\}$ and $AA^t = \left(\sum_{i=1}^{u} s_i x_i^2\right) I$. An orthogonal design of type $(s_1, s_2, \ldots, s_u)$ satisfies the same equation and has entries from $\{mx_i : 1 \le i \le u,\ m = 0, \pm 1\}$.

Precisely we prove:

(4.1.5) THEOREM. *Suppose that* b *is odd and* $0 \le a \le 3$. *Then a necessary and sufficient condition for the existence of an integral family of type* $(s_1, s_2, \ldots, s_u)$ *and order* $2^a b$ *is that*

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

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

(4.1.7) THEOREM. *Suppose that* b *is an odd integer at least as large as* u *and* $0 \le a \le 2$. *Then* (4.1.6) *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 these two theorems is established in section (4.2) by showing that for $0 \le a \le 3$ and b odd the algebraic necessary conditions ((0.0.9) and (0.0.10)) for the existence of an orthogonal design of order $2^a b$ are equivalent to (4.1.6).

We note that (4.1.6) has at least two advantages over the algebraic necessary conditions in determining existence of orthogonal designs of order not divisible by 16 . Firstly, it is often easier to construct by hand an integral solution of the matrix equation

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

than to use the Hasse-Minkowski theory to prove that a rational solution exists. Secondly, the constructive approach yields the *sum matrix* discussed in section (2.1), and so defines a useful starting point in the search for

the orthogonal design in question.

Note that for $0 \le a \le 3$ and b odd, $\rho(2^a b) = 2^a$. Hence the condition $u \le \rho(2^a)$ (see (0.0.9)) is not necessary in Theorems (4.1.5) and (4.1.7). It also follows that the condition $b \ge u$ in Theorem (4.1.7) excludes only orders less than 16. These excluded cases are of little interest since the existence problem for orthogonal designs of order less than 16 is largely solved (see Chapter 5).

Sufficiency in Theorems (4.1.5) and (4.1.7) is established in section (4.3). This section also contains a condition to determine whether certain combinatorial integral families in fact yield orthogonal designs.

(4.2) The conjecture on integral matrices

The following conjecture originally arose from the observation that the Sum Matrix Theorem (2.1.4) and the Rational Family Theorem (0.0.8) are related (see [14]).

(4.2.1) INTEGER MATRIX CONJECTURE. *Suppose that* $s_1, s_2, \ldots, s_u$ *are positive integers. If the matrix equation*

$$XX^t = \operatorname{diag}(s_1, s_2, \ldots, s_u) \tag{4.2.2}$$

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

In this section we prove

(4.2.3) PROPOSITION. *The Integer Matrix Conjecture* (4.2.1) *is true for* $u \le n \le 8$.

This proposition implies that (4.1.6) is a necessary condition for the existence of an integral family of order $2^a b$, where b is odd and $0 \le a \le 3$.

In fact, if $n \le 7$ then a stronger result is proved.

(4.2.4) PROPOSITION. *Suppose that* A *is a nonsingular integral matrix and*

$$XX^t = A \tag{4.2.5}$$

has a rational $u \times n$ *solution, where* $u \leq n \leq 7$. *Then* (4.2.5) *has an integral* $u \times n$ *solution.*

Remark. The author is indebted to Gordan Pall for the proof of Proposition (4.2.4) presented below (see [47]), and to John Cossey and Jonathan A. Hillman for helping with the details of the proof. J.S. Hsia [41] has independently obtained both Propositions (4.2.3) and (4.2.4) using the language of lattices.

Both the Integer Matrix Conjecture and Proposition (4.2.4) may be interpreted as statements within the theory of quadratic forms. Some of the machinery of this theory is required. (Jones [44] is a good reference.)

Unless otherwise stated, all quadratic forms discussed below are assumed to have full rank.

Two rational 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 solution to (4.2.2), then the form $x_1^2 + x_2^2 + \ldots + x_u^2$ is rationally equivalent to $s_1x_1^2 + s_2x_2^2 + \ldots + s_ux_u^2$.

Two integral forms are *integrally equivalent*, or of the same *class* if there is a nonsingular integral linear transformation of determinant 1 which takes one form 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 the determinant of f is greater than the determinant of g . 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 form is *c-irreducible* if it is classic but not c-reducible.

The following proposition is central to the proof of Proposition (4.2.4).

(4.2.6) PROPOSITION. *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, Propositions (4.2.3) and (4.2.4) are deduced.

Consider the case $u = n \leq 7$. Suppose that there is a $u \times u$ rational solution to (4.2.6), that is, the form f with matrix A is rationally equivalent to $x_1^2 + x_2^2 + \ldots + x_u^2$. Since f is classic, there is a non-singular integral linear transformation which takes f to a c-irreducible form g. Clearly g is rationally equivalent (through f) to $x_1^2 + x_2^2 + \ldots + x_u^2$; hence $\det g = 1$ by Proposition (4.2.6). Now a theorem of Hermite (see Jones [44], p. 60) implies that there is only one class of positive definite classic forms of determinant 1 with $u \leq 7$ variables. Hence g is integrally equivalent to $x_1^2 + x_2^2 + \ldots + x_u^2$. The composition of this equivalence transformation with the transformation from g to f provides an integral matrix Q such that $QQ^t = A$.

Now suppose that $u < n \leq 7$, and P is a rational $u \times n$ solution to (4.2.5). Let m be an integer such that mP is integral, and denote the $(n-u) \times n$ matrix of ones by V. If U denotes the transpose of the $n \times n$ matrix (P^t, mV), then UU^t is integral. From the case $u = n$ proved above there is an $n \times n$ integral matrix Y such that $YY^t = UU^t$. The first u rows of Y form an integral $u \times n$ solution of (4.2.5). This completes the proof of Proposition (4.2.4) (except for the proof of Proposition (4.2.6)).

There are two classes of positive definite classic forms of determinant 1 with 8 variables (see [45]). However, a classic form with 8 variables is in the same class as $x_1^2 + x_2^2 + \ldots + x_8^2$ if and only if it

represents an odd number (see [22]). So by using the same argument as in the case $n < 8$ above, we can show that if one of the s_i is odd then the existence of an 8×8 rational solution of (4.2.2) implies the existence of an 8×8 integral solution. Hence only 8-tuples $(s_1, s_2, \ldots, s_8)$ of even integers need to be considered to prove the Integer Matrix Conjecture (4.2.1) for $u = n = 8$. Clearly the s_i can be assumed to be squarefree, and so we need only consider the case $s_i \equiv 2 \pmod 4$ for $1 \le i \le 8$. A standard Hasse invariant computation shows that $s_1x_1^2 + s_2x_2^2 + \ldots + s_8x_8^2$ is rationally equivalent to $\frac{1}{2}\left(s_1x_1^2 + s_2x_2^2 + \ldots + s_8x_8^2\right)$. This means that if there is an 8×8 rational solution to (4.2.2) then there is an 8×8 rational matrix P such that $PP^t = \frac{1}{2}\,\mathrm{diag}(s_1, s_2, \ldots, s_8)$. Since $\frac{1}{2}s_1$ is odd there is an 8×8 integral matrix S such that $SS^t = \frac{1}{2}\,\mathrm{diag}(s_1, s_2, \ldots, s_8)$. The product of S with

$$\begin{bmatrix} 1 & 1 & & & & & & \\ 1 & -1 & & & & & & \\ & & 1 & 1 & & & & \\ & & 1 & -1 & & & & \\ & & & & 1 & 1 & & \\ & & & & 1 & -1 & & \\ & & & & & & 1 & 1 \\ & & & & & & 1 & -1 \end{bmatrix}$$

is an 8×8 solution to (4.2.2). This proves the case $u = n = 8$ of the Integer Matrix Conjecture.

The case $u < n = 8$ follows by observing that every set of u mutually orthogonal vectors in 8 dimensional rational space Q^8 can be completed to an orthogonal basis of Q^8.

Only Proposition (4.2.6) remains to be proved.

The classification of rational quadratic forms by Hasse and Minkowski is used (see Serre [62], p. 39). Let c_p denote the Hasse invariant at the prime p. The Hasse-Minkowski theory implies that two positive definite rational forms f and g are rationally equivalent if and only if $c_p(f) = c_p(g)$ for each prime p, and the squarefree parts of the determinants of f and g are equal.

Let f be a c-irreducible form. We show that

(4.2.7) $\qquad 4$ does not divide $\det f$;

and, if p is an odd prime then

(4.2.8) $\qquad p^3$ does not divide $\det f$;

and either

(4.2.9) $\qquad p$ does not divide $\det f$ and $c_p(f) = 1$,

or

(4.2.10) $\quad p$ divides $\det f$ and p^2 does not divide $\det f$,

or

(4.2.11) $\qquad p^2$ divides $\det f$ and $c_p(f) = -1$.

Proposition (4.2.6) follows immediately from the Hasse-Minkowski theory.

We prove (4.2.7) first. Suppose that 4 divides $\det f$, and choose r so that the largest power of 2 which divides $\det f$ is less than 2^r. Now f is integrally equivalent to a form g such that

(4.2.12) $\qquad g \equiv a_1h_1 + a_2h_2 + \ldots + a_mh_m \pmod{2^r}$

where the a_i are integers and h_i has shape either

(4.2.13) $\qquad x^2$,

or

(4.2.14) $\qquad 2xy$,

or

(4.2.15) $$2x^2 + 2xy + 2y^2 ,$$

and the variables of distinct h_i's are distinct (see Jones [44], p. 110). (If f_1 and f_2 are two integral forms then $f_1 \equiv f_2 \pmod{v}$ means that the corresponding coefficients of f_1 and f_2 are equivalent modulo v .)

Since each of the terms (4.2.13), (4.2.14) and (4.2.15) has odd determinant and 4 divides $\det f$, at least one of the following must hold.

(4.2.16) For some h_i of shape $2xy$, a_i is even.

(4.2.17) For some h_i of shape $2x^2 + 2xy + 2y^2$, a_i is even.

(4.2.18) For some diagonal (4.2.13) h_i , 4 divides a_i .

(4.2.19) For some $i \neq j$, $a_i \equiv a_j \equiv 2 \pmod 4$ for two diagonal components (4.2.13) h_i and h_j .

The next lemma is used to show that none of (4.2.16)-(4.2.19) is possible.

(4.2.20) LEMMA. *Suppose that* $r > 2$ *and* $f_1 \equiv f_2 \pmod{p^r}$ *for some prime* p . *If there is a classic form* h *and an integral linear transformation of determinant* $\pm p$ *which takes* h *to* f_2 , *then* f_1 *is c-reducible.*

Proof. Let F_1 and F_2 denote the matrices of f_1 and f_2 respectively, and suppose that the transformation from h to f_1 has matrix T . Now $T^{-1}F_2T^{-t}$ is integral, but $F_1 = F_2 + L$, where each entry of L is divisible by p^r . Since the denominator of each entry of T^{-1} is at most p , it follows that $T^{-1}F_1T^{-t}$ is integral. □

Now consider the case (4.2.17). The transformation with matrix

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

has determinant 2, and sends $x^2 + 3y^2$ to $2(2x^2+2xy+2y^2)$. (That is,

$$\begin{bmatrix} 2 & \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & \\ & 3 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ & 1 \end{bmatrix} = \begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix}.)$$

By Lemma (4.2.20), f is c-reducible, contrary to hypothesis.

For (4.2.19) suppose that a and b are odd and note that the transformation with matrix

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

takes the classic form $2ax^2 - 2axy + \frac{1}{2}(a+b)y^2$ to $2ax^2 + 2ay^2$. Hence (4.2.19) is impossible.

Similarly the transformation $x \mapsto 2x$ may be used to show that (4.2.16) and (4.2.18) are impossible.

Hence we have (4.2.7), that is, 4 does not divide $\det f$.

For an odd prime p a similar method may be used to establish (4.2.8)-(4.2.11). In particular, we need to use the fact that each positive integer is a sum of two squares modulo p^r. That is, if k and r are positive integers then there are integers c and d such that $k \equiv c^2 + d^2 \pmod{p^r}$. To prove this, we can assume that k is odd, because $(c+d)^2 + (c-d)^2 = 2c^2 + 2d^2$. If $k \equiv 1 \pmod 4$ then consider the sequence with the mth term $4mp^r + k$. The celebrated theorem of Dirichlet (see [8], p. 338) implies that this sequence contains a prime, and this prime can be written as a sum of two squares (see [64], p. 360). If $k \equiv 3 \pmod 4$ then the sequence with mth term $4mp^r + 2p^r + k$ may be used in a similar fashion.

Now choose r so that the highest power of p dividing $\det f$ is

less than p^r . It can be shown (see Jones [44], p. 110) that f is integrally equivalent to a form g which is diagonal modulo p^r . If p^2 divides one of the diagonal coefficients in g , then f is c-reducible by Lemma (4.2.20). Thus

$$g \equiv g_1 + pg_2 \pmod{p^r} \tag{4.2.21}$$

where g_1 and g_2 are diagonal forms with coefficients prime to p and no variables in common.

Next we show that each g_i is integrally equivalent to a form h_i such that

$$h_i \equiv x_1^2 + x_2^2 + \ldots + x_{s-1}^2 + kx_s^2 \pmod{p^r}$$

where k is prime to p . It is clearly sufficient to prove this for forms $ax^2 + by^2$, where a and b are integers prime to p . Some arithmetic of integers modulo p^r is required and the reader is referred to Hardy and Wright [39], p. 67, for details of such things as quadratic residues. Suppose that there is an integer α such that $a = \alpha^2 \pmod{p^r}$. Let β be an integer such that $\alpha\beta = 1 + mp^{2r}$ for some integer m . The transformation with matrix

$$\begin{bmatrix} \beta & p^r \\ mp^r & \alpha \end{bmatrix}$$

has determinant 1 and takes $ax^2 + by^2$ to a form which is $x^2 + aby^2$ modulo p^r .

If neither a nor b is a quadratic residue of p^r then $a^{-1}b$ is a quadratic residue, where a^{-1} denotes the inverse of a modulo p^r . There are integers γ and δ such that $b^{-1} \equiv \gamma^2 + \delta^2 \pmod{p^r}$. Suppose that ε is an integer such that $a^{-1}b\gamma^2 \equiv \varepsilon^2 \pmod{p^r}$. Since b^{-1} is not a

quadratic residue of p^r , $\varepsilon \not\equiv 0 \pmod{p^r}$. Writing δ as $\varepsilon(\varepsilon^{-1}\delta)$ makes it clear that there is an integer ψ such that $\delta + \psi p^r$ is prime to ε . Now if ϕ denotes $\delta + \psi p^r$ then

$$a\varepsilon^2 + b\phi^2 \equiv b\gamma^2 + b\delta^2 \pmod{p^r}$$

$$\equiv bb^{-1} \equiv 1 \pmod{p^r}$$

and so there is an integer ξ such that $a\varepsilon^2 + b\phi^2 = 1 + \xi p^r$. Since ε is prime to ϕ , there are integers μ and ν such that $\xi = \mu\varepsilon + \nu\phi$. The transformation with matrix

$$\begin{bmatrix} \varepsilon & \phi \\ \nu p^r - b\phi & a\varepsilon - \mu p^r \end{bmatrix}$$

has determinant 1 and takes $ax^2 + by^2$ to a form which is $x^2 + aby^2$ modulo p^r .

Thus we have proved that $g_1 + pg_2$ (4.2.21) is integrally equivalent to a form which is

$$h = x_1^2 + x_2^2 + \ldots + x_{s-1}^2 + kx_s^2 + p\left(y_1^2 + y_2^2 + \ldots + y_{w-1}^2 + ly_w^2\right)$$

modulo p^r , where k and l are prime to p . Note that h has many of the properties of f which we seek to investigate. A power of p divides $\det h$ if and only if it divides $\det f$. If h is c-reducible by a transformation of determinant $\pm p$, then f is c-reducible. And the Hasse invariant of f is the same as that of h .

If p does not divide $\det h$ then $w = 0$, and a simple calculation shows that $c_p(f) = 1$.

Suppose that $w \geq 3$. Integers α and β can be found such that $l \equiv \alpha^2 + \beta^2 \pmod{p}$; then the form

$$h' = px^2 - 2\alpha xz + py^2 - 2\beta yz + \left(\alpha^2+\beta^2+l\right)z^2/p$$

is classic. The transformation with matrix

$$\begin{bmatrix} 1 & & \\ & 1 & \\ \alpha & \beta & p \end{bmatrix}$$

has determinant p and takes h' to $p(x^2+y^2+lz^2)$. So by Lemma (4.2.20), f is c-reducible, contrary to hypothesis. Hence $w < 3$ and we have (4.2.8).

If p^2 divides $\det f$ then $w = 2$ and a simple Hasse invariant argument shows that $c_p(f) = 1$ if and only if $-l$ is a quadratic residue of p (and thus of p^r). If γ is an integer such that $\gamma^2 \equiv -l \pmod{p^r}$ then denote the inverse of γ modulo p^r by δ. The transformation with matrix

$$\begin{bmatrix} \delta & p \\ 1 & \end{bmatrix}$$

has determinant $-p$ and takes the classic form

$$-\gamma^2 px^2 + 2\gamma^2\delta xy + (1-\gamma^2\delta^2)y^2/p$$

to a form which is equivalent to $p(x^2+ly^2)$ modulo p^r. Hence if p^2 divides $\det f$ then $c_p(f) = -1$, and we have (4.2.11).

This completes the proof of Proposition (4.2.6).

(4.3) The construction of combinatorial integral families

Suppose that the algebraic necessary conditions for the existence of an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order n hold, where $n = 2^a b$ and b is odd; that is, $u \le \rho(n)$ and there is a $u \times 2^a$ rational matrix P such that $PP^t = \operatorname{diag}(s_1, s_2, \ldots, s_u)$. If $a \le 3$ then Proposition (4.2.3) ensures the existence of an integral $u \times 2^a$ matrix Q such that $QQ^t = \operatorname{diag}(s_1, s_2, \ldots, s_u)$. The matrix Q can be used as the sum matrix in an algorithm (section (2.1)) for constructing an orthogonal

design of type $(s_1, s_2, \ldots, s_u)$ and order n. However, this algorithm may not be successful (see section (2.4)). In the present section, it is demonstrated that Q can always be used to construct an integral family and if $a \leq 2$ and $b \geq u$, then Q gives a combinatorial integral family. This establishes sufficiency in Theorems (4.1.5) and (4.1.7).

The first construction follows a construction of Wolfe [79]. Denote the ijth entry of Q by q_{ij}, and denote $\rho(2^a)$ by r. Suppose that $\{P_1, P_2, \ldots, P_r\}$ is the integral family which corresponds to the Geramita-Pullman [25] orthogonal design of type $(1, 1, 1, \ldots, 1)$ and order $2^a b$ on r variables. Using the relations

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

$$P_i P_i^t = I \quad \text{for} \quad 1 \leq i \leq u ,$$

$$P_i P_j^t + P_j P_i^t = 0 \quad \text{for} \quad 1 \leq i < j \leq u ,$$

a simple computation shows that

$$\left\{ \sum_{j=1}^{r} q_{ij} P_j \, : \, 1 \leq i \leq u \right\}$$

is an integral family of type $(s_1, s_2, \ldots, s_u)$ and order $2^a b$.

For $a = 0$ it is trivial that the integral family above is combinatorial. For $a > 0$ note that the sequences

$$c_j = (q_{1j}x_1, q_{2j}x_2, \ldots, q_{uj}x_u) , \quad 1 \leq j \leq 2^a ,$$

are complementary (see section (1.5)). Hence for every $b \geq u$ there are $b \times b$ circulant matrices A_j, $1 \leq j \leq 2^a$, with entries from $\{mx_i \, : \, 1 \leq i \leq u, \, m \in \mathbb{Z}\}$ such that

$$\sum_{j=1}^{2^a} A_j A_j^t = \left(\sum_{i=1}^{u} s_i x_i^2 \right) I_b .$$

If a is 1 or 2, then these circulant matrices may be used in the two-circulant construction (2.0.6) or the Goethals-Seidel construction (2.0.3) to form a combinatorial integral family of type $(s_1, s_2, \ldots, s_u)$ and order $2^a b$.

This completes the proof of sufficiency in Theorems (4.1.5) and (4.1.7).

Finally we give a combinatorial condition to determine whether a combinatorial integral family constructed using GGS arrays is in fact an orthogonal design.

(4.3.1) PROPOSITION. *Suppose that* $A_1, A_2, \ldots, A_u$, *are integral* $b \times b$ *matrices and* $s_1, s_2, \ldots, s_u$ *are positive integers such that*

$$\sum_{i=1}^{u} s_i A_i A_i^t = aI .$$

For $1 \le i \le u$, *write* $A_i = B_i - C_i$, *where* B_i *and* C_i *have nonnegative entries, and denote by* l_i *and* m_i *the rowsums of* B_i *and* C_i *respectively. Then*

$$a = \sum_{i=1}^{u} s_i (l_i - m_i)^2 \tag{4.3.2}$$

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

$$a = \sum_{i=1}^{u} s_i (l_i + m_i) . \tag{4.3.3}$$

Proof. A standard rowsum argument gives (4.3.2); if the A_i have entries from $\{0, 1, -1\}$ then (4.3.3) is immediate.

Conversely, suppose that (4.3.3) holds and let

$$a_i = (a_{1i}, a_{2i}, \ldots, a_{bi})$$

denote the first row of A_i for $1 \le i \le u$. Now it is clear that

$$l_i + m_i = \sum_{j=1}^{b} |a_{ji}| \ .$$

Hence using (4.3.3) we obtain

$$a = \sum_{i=1}^{u} s_i \sum_{j=1}^{b} |a_{ji}| \ ;$$

but also

$$a = \sum_{i=1}^{u} s_i \sum_{j=1}^{b} |a_{ji}|^2$$

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

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

But each term in this sum is nonnegative, and the s_i are positive. Hence $|a_{ji}| \in \{0, 1\}$ for $1 \le j \le b$ and $1 \le i \le u$, that is, the A_i have entries from $\{0, 1, -1\}$. □

CHAPTER 5

NUMERICAL RESULTS

The purpose of this chapter is to present numerical results to complement the theory in Chapters 2 and 3.

Much of the information is compiled in tables using results from the literature as well as unpublished results of the author.

In general, proofs are not given, but sometimes a few examples which illustrate the techniques involved are outlined.

Not all currently known numerical existence results are listed here. Notably absent are results for skew symmetric weighing matrices, 3 variable orthogonal designs, and orthogonal designs of order divisible by 8 . Geramita and Seberry [26] have more comprehensive lists.

In this chapter the formal commuting variables

$$x_1, x_2, x_3, \ldots, -x_1, -x_2, -x_3, \ldots ,$$

are denoted by

$$a, b, c, \ldots, \bar{a}, \bar{b}, \bar{c}, \ldots ,$$

respectively.

(5.1) Weighing matrices of odd order

If k is a square integer then denote by $N(k)$ the smallest integer such that a weighing matrix of weight k and order n exists for all $n \geq N(k)$. The argument (k) may be omitted if there is no fear of ambiguity.

The existence of N is assured by Theorem (3.2.1). It follows from Theorem (0.0.11) that $N \geq k + \sqrt{k} + 1$. An upper bound for N can be calculated as follows.

Suppose that the decomposition of k into prime powers is

$k = q_1^2 q_2^2 \ldots q_m^2$; denote $\prod_{i=1}^{m} \left(q_i^2+q_i+1\right)$ by $\tau(k)$. By taking kronecker products of the circulant weighing matrices of weight q_i^2 and order $q_i^2 + q_i + 1$, a weighing matrix of weight k and order $\tau(k)$ may be obtained. (See Theorem (1.3.4) and the proof of Lemma (3.2.7).) Also, from Theorem (1.3.3) it follows that there is a weighing matrix of weight k and order 2^w where $2^{w-1} < k \leq 2^w$. Now $\tau(k)$ is prime to 2^w and so each integer at least as large as $\left(\tau(k)-1\right)\left(2^w-1\right)$ may be written as $\tau(k)m_1 + 2^w m_2$ where m_1 and m_2 are nonnegative integers. Hence there is a weighing matrix of weight k and order n for each $n \geq \left(\tau(k)-1\right)\left(2^w-1\right)$. Thus we obtain

$$N(k) \leq \left(\tau(k)-1\right)(2k-1) .$$

A familiar arithmetic function may be used to estimate this bound. Denote the sum of the divisors of k by $\sigma(k)$. If $q_i = p_i^{e_i}$ for $1 \leq i \leq m$ and the p_i are prime, then the following expression for σ may be obtained (Hardy and Wright [39], p. 239):

$$\sigma(k) = \prod_{i=1}^{m} \left(\frac{p_i^{2e_i+1} - 1}{p_i - 1} \right) .$$

It follows that $\tau(k) \leq \sigma(k)$ with equality if and only if $\sqrt{k}$ is square-free. Now for each positive real number ε there is a real number B such that $\sigma(k) \leq Bk^{1+\varepsilon}$ (Hardy and Wright [39], p. 266). Hence there is a real number A such that $N \leq Ak^{2+\varepsilon}$. This means that the order of N is at most a little larger than quadratic.

If k is a prime power then a more accurate estimate for $N(k)$ may be obtained. In this case $N(k) \geq \tau(k) = k + \sqrt{k} + 1$. If k is even then

there is an Hadamard matrix of order k, and if k is odd then there is a weighing matrix of weight k and order $k+1$ (see [75]). Note that $\tau(k)$ is prime to both k and $k+1$. Hence if k is even then

$$k + \sqrt{k} + 1 \leq N(k) \leq (k+\sqrt{k})(k-1)$$

and if k is odd then

$$k + \sqrt{k} + 1 \leq N(k) \leq (k+\sqrt{k})k .$$

However, numerical evidence suggests that N is not much larger than a linear function of k. In fact it seems that $N(k) \leq M(k)$, where $M(k)$ is $\tau(k) + k - 1$ if k is even and $\tau(k) + k$ if k is odd, but the author has not been able to prove this.

It can be shown that $N(4) = 10 = M(4)$. For there are weighing matrices of weight 4 and orders 7 and $2n$ for each $n \geq 2$. It follows that $N(4) \leq 10$. If $N(4) < 10$ then there is a weighing matrix of weight 4 and order 9. An elementary combinatorial argument (due to J. Verner; see [26]) can be employed to show that no such weighing matrix exists.

Preliminary results from a computer program lead us to conjecture that $N(9) = 22 = M(9)$. However, there is a circulant weighing matrix of weight 16 and order 31 (with first row

$$- 0 0 0 0 - 0 + 0 - - + 0 + + 0 0 0 - + - + + 0 0 + + 0 + 0 0$$

where + indicates +1 and - indicates -1). This suggests that $N(16)$ could be less than $M(16) = 36$.

Apart from the results mentioned above, very little is known about the behaviour of $N(k)$. The following table lists results for $k \leq 49$. For this table $\underline{N}$ denotes the largest integer for which it is known that $N \geq \underline{N}$, and $\overline{N}$ denotes the smallest integer for which it is known that $\overline{N} \leq N$. The smallest odd order for which it is known that a weighing matrix of weight k exists is denoted by $l(k)$.

(5.1.1) TABLE

k	$\tau(k)$	$M(k)$	$\underline{N}(k)$	$\overline{N}(k)$	$l(k)$	Orders for which the existence problem is unsolved
4	7	10	10	10	7	nil
9	13	22	13	22	13	15, 17, 19, 21
16	21	36	21	36	21	23, 25, 27, 29, 33, 35
25	31	56	31	83	31	many
36	91	126	44	163	91	many
49	53	102	53	200	53	many

(5.2) Two variable orthogonal designs of order equivalent to 2 modulo 4

Suppose that there is a 2×2 rational matrix P such that $PP^t = \mathrm{diag}(s_1, s_2)$. Denote by $N(s_1, s_2)$ the smallest integer such that an orthogonal design of type (s_1, s_2) and order $2n$ exists for each $n \geq N(s_1, s_2)$. The arguments (s_1, s_2) are omitted where there is no fear of ambiguity. The existence of N is assured by the fact that the algebraic necessary conditions ((0.0.9) and (0.0.10)) are asymptotically sufficient for existence (Theorem (3.2.2)).

Denote the sum of s_1 and s_2 by s. Using methods similar to those of the previous section it can be shown that for every positive real number ε there is a real constant A such that

$$N(s_1, s_2) \leq As^{3+\varepsilon} .$$

However, numerical evidence suggests that N is bounded by a linear function of s_1 and s_2. The following table lists the current status of the existence problem for orthogonal designs of type (s_1, s_2) and order equivalent to 2 modulo 4 such that $s_1 + s_2 \leq 38$.

The column headings are defined in a similar way to those in Table (5.1.1): l denotes the smallest odd integer such that it is known that an orthogonal design of type (s_1, s_2) and order $2l$ exists; $\underline{N}$ denotes the largest integer for which it is known that $N \geq \underline{N}$; $\overline{N}$ denotes the smallest integer for which it is known that $N \leq \overline{N}$.

(5.2.1) TABLE

s_1, s_2	$2\underline{N}$	$2\overline{N}$	$2l$	Orders for which the existence problem is unsolved
1, 1	2	2	2	nil
1, 4	6	6	6	nil
1, 9	12	28	14	18, 22
1, 16	20	40	22	30, 34, 38
1, 25	28	92	62	many
1, 36	38	220	182	many
2, 2	4	4	6	nil
2, 8	12	12	14	nil
2, 18	20	40	26	22, 30, 34, 38
2, 32	36	80	42	many
4, 4	8	8	10	nil
4, 9	14	28	14	18, 22, 26
4, 16	20	20	22	nil
4, 25	30	1300	434	many
5, 5	12	12	14	nil
5, 20	26	68	42	26, 30, 34, 38, 46, 50, 58, 62, 66
8, 8	16	16	18	nil
8, 18	28	208	182	many
9, 9	20	46	26	22, 30, 34, 38, 42
9, 16	28	220	182	many
9, 25	36	932	806	many
10, 10	20	20	22	nil
13, 13	28	28	30	nil
16, 16	32	32	34	nil
17, 17	36	104	42	many
18, 18	36	112	78	many

The techniques involved in proving the results in Table (5.2.1) are illustrated with an example.

(1, 16) : Geramita and Verner proved that there is no orthogonal design of type (1, 16) and order 18 (see [26]). Hence $N(1, 16) \geq 20$. The 11×11 circulant matrices A_1 and A_2 with first rows

(5.2.2) $$b\bar{a}aaa\bar{a}\bar{a}\bar{a}\bar{a}\bar{a}\bar{a} \quad , \quad aa0aaa000a0$$

satisfy $A_1A_1^t + A_2A_2^t = (b^2+16a^2)I$, and so using the two-circulant construction (2.0.6) an orthogonal design of type (1, 16) and order 22 exists. Similarly

(5.2.3) $$ba0a\bar{a}0000a\bar{a}0\bar{a} \quad , \quad a\bar{a}\bar{a}00aa0aa\bar{a}\bar{a}a$$

give an orthogonal design of type (1, 16) and order 26. Now there is an orthogonal design of type (1, 1, 8, 8) and order $4n$ for all $n \geq 5$ (see section (5.4)); equating variables gives an orthogonal design of type (1, 16) for these orders. Thus, by elementary constructions, $N(1, 16) \leq 40$, leaving only the orders 30, 34 and 38 unsolved.

Remark. The circulants with first rows (5.2.2) and (5.2.3) were found by implementing the method described in section (2.1) on the Australian National University U1100/42 Univac computer.

To illustrate the use of GGS arrays in constructing orthogonal designs of highly composite order, the following table gives the present status of the existence problem for 2 variable orthogonal designs of orders 42, 50, 54. A tick "√" indicates that the orthogonal design exists, a dash "-" indicates that it does not exist and a blank space indicates that the existence question is unsolved.

(5.2.4) TABLE

type	Order 42	Order 50	Order 54
1, 1	√	√	√
1, 4	√	√	√
1, 9	√	√	√
1, 16	√	√	√
1, 25			
1, 36			
1, 49	-	-	
2, 2	√	√	√
2, 8	√	√	√
2, 18	√		
2, 32	√		
2, 50	-	-	
4, 4	√	√	√
4, 9	√	√	√
4, 16	√	√	√
4, 25			
4, 36			
4, 49	-	-	
5, 5	√	√	√
5, 20	√		√
5, 45			
8, 8	√	√	√
8, 18			
8, 32			√
9, 9			
9, 16			
9, 25			
9, 36	-		
10, 10	√	√	√
10, 40	-	-	
13, 13	√	√	√
16, 16	√	√	√
16, 25	-		
16, 36	-	-	
17, 17	√		
18, 18			
18, 32	-	-	
20, 20	√	√	√
25, 25	-	-	
26, 26	-	-	

We give an example which illustrates the methods of proof for these results.

The sequences

(5.2.5) $$a0abb\bar{b} \ , \quad b0b\bar{a}\bar{a}a \ ,$$

are complementary (see section (1.5)) and hence, using the two-circulant construction, there is an orthogonal design of type (5, 5) and order $2n$

for each $n \geq 6$. Hence there is a GGS array of type (5, 5) and order $2n$ for each $n \geq 6$. The sequences

$$ba\bar{b} \ , \quad b0b \ ,$$

are complementary, and so for each $v \geq 3$ there are circulant matrices A_1 and A_2 such that

$$A_1A_1^t + A_2A_2^t = (a^2+4b^2)I \ .$$

These circulant matrices may be used in the GGS array of type (5, 5) and order $2n$ to obtain an orthogonal design of type (5, 20) and order $2nv$ whenever $n \geq 6$ and $v \geq 3$.

(5.3) Weighing matrices of order equivalent to 2 modulo 4

For each integer k which can be written as a sum of 2 squares denote by $N(k)$ the smallest integer such that a weighing matrix of weight k and order $2n$ exists for all $n \geq N(k)$. The argument is omitted where convenient.

Using the same methods as in section (5.1) it can be shown that for every positive real number ε there is a real constant A such that $N(k) \leq Ak^{3+\varepsilon}$ for each k which can be written as a sum of 2 squares. Again, however, numerical evidence suggests that N is much smaller.

It follows from Theorem (0.0.11) that $N(k) \geq M(k)$, where $M(k)$ is defined by

$$M(k) = \begin{cases} \frac{1}{2}k & \text{if } k \equiv 0 \pmod 4 \ , \\ \frac{1}{2}(k+1) & \text{if } k \equiv 1 \pmod 4 \ , \\ \frac{1}{2}(k+2) & \text{if } k \equiv 2 \pmod 4 \ . \end{cases}$$

(Since M is defined only for integers which can be written as a sum of 2 squares, the case $k \equiv 3 \pmod 4$ does not arise.)

In fact $N(k) = M(k)$ for $k \leq 16$ and it is conjectured that

$N(k) = M(k)$ for each k which can be written as a sum of 2 squares ([19]).

The following table presents the current status of the existence problem for weighing matrices of order equivalent to 2 modulo 4 and weight $k \leq 29$.

The integers l and $\overline{N}$ are defined in the same way as these symbols in Table (5.2.1).

(5.3.1) TABLE

k	$2M$ (M is the conjectured value for N)	$2\overline{N}$	$2l$	Orders for which the existence problem is unsolved
2	2	2	2	nil
4	4	4	6	nil
5	6	6	6	nil
8	8	8	10	nil
9	10	10	10	nil
10	12	12	14	nil
13	14	14	14	nil
16	16	16	18	nil
17	18	36	18	34
18	20	40	22	34, 38
20	20	20	22	nil
25	26	52	26	34, 38, 46, 50
26	28	28	30	nil
29	30	62	30	34, 38, 42, 46, 50, 54, 58

(5.4) Four variable orthogonal designs of order equivalent to 4 modulo 8

Suppose that s_1, s_2, s_3, s_4 are positive integers with sum s , and b is an odd integer such that $s \leq 4b$. Then the existence of an orthogonal design of type (s_1, s_2, s_3, s_4) and order $4b$ implies that

(5.4.1) $s \neq 4b - 1$ (by the Geramita-Verner Theorem (0.0.12));

(5.4.2) there is a 4×4 rational matrix P such that

$PP^t = \mathrm{diag}(s_1, s_2, s_3, s_4)$ (the algebraic necessary condition (0.0.10)).

It is well known that if $s \leq 12$ then (5.4.2) is sufficient for the existence of an orthogonal design of type (s_1, s_2, s_3, s_4) and order $4n$ for all $n \geq 3$ (see [31], [21]).

The results of [31] together with the methods of section (2.1) can be used to show that orthogonal designs of order 20 and type (s_1, s_2, s_3, s_4) exist for all 4-tuples (s_1, s_2, s_3, s_4) which satisfy (5.4.1), (5.4.2), and $s \leq 20$, except for (2, 2, 5, 5), (1, 3, 6, 8) and (1, 4, 4, 9). (See [15] and section (2.4).)

It is conjectured that (5.4.2) is sufficient for the existence of an integer N such that an orthogonal design of type (s_1, s_2, s_3, s_4) and order $4n$ exists for each $n \geq N$ (see (0.0.14)). Using the methods of section (3.2), this conjecture has been verified for 4-tuples with sum s at most 28, and, with 3 exceptions, for 4-tuples with $s \leq 36$.

The following table gives the status of the existence problem for $12 < s \leq 28$. The column headings are defined in the same way as in previous tables: l denotes the smallest odd integer for which it is known that an orthogonal design of type (s_1, s_2, s_3, s_4) and order $4l$ exists; $\overline{N}$ denotes the smallest integer for which it is known that an orthogonal design of type (s_1, s_2, s_3, s_4) and order $4n$ exists for each $n \geq \overline{N}$.

Most of the orthogonal designs listed in this table may be constructed using the methods of section (2.1), together with elementary constructions and results listed in [57], [55], [19]. Three examples are given after the table.

(5.4.3) TABLE

$12 < s \leq 16$

s_1, s_2, s_3, s_4	$4l$	$4\overline{N}$	Orders for which the existence problem is unsolved
1, 1, 4, 9	20	16	nil
1, 2, 2, 9	20	16	nil
1, 2, 4, 8	20	16	nil
1, 4, 4, 4	20	16	nil
1, 4, 5, 5	20	16	nil
2, 2, 2, 8	20	16	nil
2, 2, 5, 5	28	24	20
2, 3, 4, 6	20	16	nil
4, 4, 4, 4	20	16	nil

$16 < s \leq 20$

1, 1, 1, 16	28	24	nil
1, 1, 8, 8	20	20	nil
1, 1, 9, 9	20	20	nil
1, 2, 8, 9	20	40	36
1, 3, 6, 8	28	48	20, 36, 44
1, 4, 4, 9	28	48	20, 36, 44
1, 5, 5, 9	20	40	36
2, 2, 4, 9	20	40	28, 36
2, 2, 8, 8	20	20	nil
2, 3, 6, 9	20	40	28, 36
2, 5, 5, 8	20	20	nil
3, 3, 6, 6	20	20	nil
4, 4, 5, 5	20	20	nil
5, 5, 5, 5	20	20	nil

$20 < s \leq 24$

1, 1, 2, 18	28	48	36, 44
1, 1, 4, 16	28	24	nil
1, 1, 10, 10	28	40	36
1, 2, 2, 16	28	48	36, 44
1, 2, 6, 12	28	24	nil
1, 4, 8, 8	36	32	28
1, 4, 9, 9	52	72	28, 36, 44, 60, 68
2, 2, 2, 18	28	48	44
2, 2, 4, 16	28	24	nil
2, 2, 9, 9	28	24	nil
2, 2, 10, 10	28	24	nil
2, 4, 6, 12	28	24	nil
2, 4, 8, 9	140	168	many
3, 3, 3, 12	28	48	36, 44
3, 4, 6, 8	28	56	24, 36, 44, 52
4, 4, 4, 9	84	112	many
4, 4, 8, 8	28	24	nil
4, 5, 5, 9	140	168	many
6, 6, 6, 6	28	24	nil

(5.4.3) Table (Continued)

$24 < s \leq 28$

s_1, s_2, s_3, s_4	$4l$	$4\overline{N}$	Orders for which the existence problem is unsolved
1, 1, 1, 25	28	56	36, 44, 52
1, 1, 5, 20	84	144	many, including 56
1, 1, 8, 18	28	56	36, 44, 52
1, 1, 9, 16	252	280	many
1, 1, 13, 13	28	56	36, 44, 52
1, 2, 4, 18	52	80	28, 36, 44, 60, 68, 76
1, 2, 8, 16	84	112	many
1, 3, 6, 18	156	464	many, including 40, 56, 72
1, 4, 4, 16	44	40	28, 36
1, 4, 10, 10	44	40	28, 36
1, 5, 5, 16	84	160	many
1, 6, 8, 12	84	160	many
1, 8, 8, 9	52	80	28, 36, 44, 52, 60, 68, 76
1, 9, 9, 9	52	80	28, 36, 44, 52, 60, 68, 76
2, 3, 6, 16	140	216	many, including 40 and 72
2, 4, 4, 18	36	48	28, 44
2, 8, 8, 8	28	28	nil
2, 8, 9, 9	52	80	28, 36, 44, 60, 68, 76
3, 6, 8, 9	140	416	many, including 40, 56, 72
3, 6, 6, 12	60	80	28, 36, 44, 52, 68, 76
4, 4, 4, 16	28	28	nil
4, 4, 9, 9	28	48	36, 44
4, 4, 10, 10	28	28	nil
5, 5, 8, 8	36	32	28
5, 5, 9, 9	52	80	28, 36, 44, 60, 68, 76
7, 7, 7, 7	28	28	nil

(2, 3, 6, 9) : The 5×5 circulants A_1, A_2, A_3, A_4, with first rows

$$abd\bar{d}c \ , \quad a\bar{b}d\bar{d}\bar{c} \ , \quad bdc\bar{c}\bar{d} \ , \quad ddc\bar{c}d \ ,$$

respectively satisfy

$$\sum_{i=1}^{4} A_i A_i^t = \left(2a^2+3b^2+6c^2+9d^2\right) I$$

and so, using the Goethals-Seidel construction, there is an orthogonal design of type (2, 3, 6, 9) and order 20 . Robinson ([55], [57]) gives orthogonal designs of this type and orders 24 and 32 . Hence if m_1, m_2, m_3 are nonnegative integers then there is an orthogonal design of type

$(2, 3, 6, 9)$ and order $20m_1 + 24m_2 + 32m_3$, using elementary constructions (see section (1.2)). This implies that $N \leq 40$, and the only orders for which existence is unknown are 28 and 36.

$(1, 1, 1, 25)$: The existence of an orthogonal design of type $(1, 1, 1, 25)$ and order 28 is established in section (2.1) (example (2.1.17)). It follows from results in [57] that there is an orthogonal design of order 32 and $(1, 1, 1, 25)$. Also from [57], there is an orthogonal design of type $(1, 1, 1, 1, 2, 6)$ and order 16. The 3×3 circulants A_i, $1 \leq i \leq 6$, with first rows

$$a00 \ , \ b00 \ , \ c00 \ , \ d00 \ , \ ddd \ , \ \bar{d}dd$$

are symmetric and satisfy

$$A_1A_1^t + A_2A_2^t + A_3A_3^t + A_4A_4^t + 2A_5A_5^t + 6A_6A_6^t = (a^2+b^2+c^2+25d^2)I \ .$$

Hence there is an orthogonal design of type $(1, 1, 1, 25)$ and order 48 (see introduction of Chapter 2 or [72]). Similarly, 5×5 circulants with first rows

$$a0000 \ , \ b0000 \ , \ ddddd \ , \ 0dd\bar{d}\bar{d} \ , \ 0d\bar{d}d\bar{d}$$

may be used in an orthogonal design of type $(1, 1, 1, 1, 2, 2)$ and order 8 to give an orthogonal design of type $(1, 1, 1, 25)$ and order 40. It follows that $N \leq 40$.

$(2, 4, 4, 18)$: There is a GGS array of type $(2, 2, 4, 4)$ and order 12 (see section (5.7)). The 3×3 circulant matrices A_1, A_2, A_3, A_4, with first rows

$$ad\bar{d} \ , \ ddd \ , \ bd\bar{d} \ , \ c00 \ ,$$

respectively satisfy

$$2A_1A_1^t + 2A_2A_2^t + 4A_3A_3^t + 4A_4A_4^t = (2a^2+4b^2+4c^2+18d^2)I \ .$$

Hence there is an orthogonal design of type $(2, 4, 4, 18)$ and order 36.

There is a circulant weighing matrix W of weight 9 and order 13 (see Theorem (1.4.1)) and W may be chosen with zero diagonal. The matrices

$A_1 = aI + dW$, $A_2 = aI - dW$, satisfy $A_1A_1^t + A_2A_2^t = (2a^2+18d^2)I$. The sequences

$$ccb\bar{b} \ , \quad bb\bar{c}c \ ,$$

(from [21]) are complementary, and so there are 13×13 circulant matrices A_3 and A_4 such that $A_3A_3^t + A_4A_4^t = (4c^2+4d^2)I$. Using A_1, A_2, A_3, A_4 in the Goethals-Seidel array (2.0.5) there is an orthogonal design of type (2, 4, 4, 18) and order 52 .

Similarly, using a GGS array of type (2, 2, 2, 2) and order 12 an orthogonal design of type (2, 4, 4, 18) and order 60 may be obtained.

Since there is an orthogonal design of type (1, 2, 2, 9) and order $4n$ for all $n \geq 4$, there is an orthogonal design of type (2, 4, 4, 18) and order $8n$ for all $n \geq 4$ (by Theorem (1.3.1)).

It follows that $N \leq 48$.

The following table gives values of l and $\overline{N}$ for $28 < s \leq 36$. The double asterisk "**" indicates that an orthogonal design of this type is not known for any order equivalent to 4 modulo 8 .

Two examples are given to illustrate the calculations involved in preparing Table (5.4.4).

(1, 5, 5, 25) : There is a circulant weighing matrix W of weight 25 and order 31 (Theorem (1.4.1)). If $A_1 = aI_{31}$ and $A_4 = dW$ then $A_1A_1^t + A_4A_4^t = (a^2+25d^2)I$. Also, there are complementary sequences which give 31×31 circulant matrices A_2 and A_3 such that $A_2A_2^t + A_3A_3^t = (5b^2+5c^2)I$ (see (5.2.5)). The matrices A_1, A_2, A_3, A_4 may be used in the Goethals-Seidel array (2.0.5) to construct an orthogonal design of type (1, 5, 5, 25) and order 124 . There are orthogonal designs of this type and orders 64 [57] and 96 [55]. It can be deduced that $N \leq 492$.

(5.4.4) TABLE

$28 < s \leq 32$

s_1, s_2, s_3, s_4	4λ	$4\bar{N}$	s_1, s_2, s_3, s_4	4λ	$4\bar{N}$
1, 1, 4, 25	124	368	2, 3, 10, 15	**	
1, 2, 2, 25	84	112	2, 4, 8, 16	44	40
1, 2, 3, 24	84	248	2, 5, 5, 18	52	80
1, 2, 9, 18	52	84	2, 6, 9, 12	140	416
1, 4, 5, 20	84	248	2, 8, 10, 10	44	40
1, 4, 8, 18	196	272	3, 3, 12, 12	60	80
1, 4, 9, 16	52	80	3, 4, 6, 18	156	216
1, 4, 13, 13	60	56	4, 5, 5, 16	44	40
1, 9, 10, 10	52	80	4, 6, 8, 12	60	80
2, 2, 5, 20	84	248	4, 8, 8, 9	140	184
2, 2, 8, 18	52	80	4, 9, 9, 9	156	184
2, 2, 9, 16	140	168	5, 5, 10, 10	44	40
2, 2, 13, 13	60	56	8, 8, 8, 8	36	32

$32 < s \leq 36$

1, 1, 2, 32	84	160	2, 8, 13, 13	60	56
1, 1, 9, 25	364	1088	3, 3, 3, 27	60	120
1, 1, 16, 16	84	80	3, 3, 6, 24	60	96
1, 1, 17, 17	68	64	3, 3, 15, 15	60	96
1, 2, 6, 27	156	464	3, 6, 8, 16	140	232
1, 2, 8, 25	124	368	3, 6, 9, 18	60	120
1, 2, 11, 22	**		3, 8, 10, 15	**	
1, 3, 8, 24	84	248	4, 4, 5, 20	84	248
1, 4, 4, 25	124	184	4, 4, 8, 18	60	140
1, 5, 5, 25	124	492	4, 4, 9, 16	140	416
1, 8, 8, 16	84	160	4, 4, 13, 13	60	56
1, 8, 9, 18	156	248	4, 8, 8, 16	44	40
1, 9, 13, 13	364	456	5, 5, 8, 18	260	336
2, 2, 4, 25	372	448	5, 5, 13, 13	60	56
2, 2, 16, 16	60	96	6, 6, 12, 12	60	96
2, 3, 6, 25	372	1112	8, 8, 9, 9	52	128
2, 4, 9, 18	156	192	8, 8, 10, 10	44	40
2, 6, 7, 21	**		9, 9, 9, 9	36	36
2, 6, 12, 16	84	160			
2, 8, 8, 18	84	160			

(3, 3, 15, 15) : Proposition (2.2.3) gives a GGS array of type (3, 3, 3, 3) and order 20 . The 3×3 circulant matrices A_1, A_2, A_3, A_4 , with first rows

$$ac\bar{c} \ , \ bd\bar{d} \ , \ cdd \ , \ \bar{d}cc$$

satisfy

$$\sum_{i=1}^{4} 3A_i A_i^t = \left(3a^2+3b^2+15c^2+15d^2\right) I \ ,$$

and so there is an orthogonal design of type (3, 3, 15, 15) and order 60 (see section (2.2)). From table (5.4.3) there is an orthogonal design of type (3, 3, 6, 6) and order $4n$ for each $n \geq 5$. Equating variables gives an orthogonal design of type (3, 15) for these orders. Using Theorem (1.3.2) an orthogonal design of type (3, 3, 15, 15) and order $8n$ for each $n \geq 5$ may be obtained. Using elementary constructions (section (1.2)) it follows that $N \leq 96$.

Remark. The author is grateful to Peter J. Robinson for permission to use his list of 4-tuples which satisfy (5.4.2).

(5.5) Two variable orthogonal designs of order equivalent to 4 modulo 8

Suppose that s_1 and s_2 are positive integers and with sum s, and b is an odd integer with $4b \geq s$. Then the existence of an orthogonal design of type (s_1, s_2) and order $4b$ implies that

(5.5.1) $s_1 s_2$ is a sum of 3 squares, and

(5.5.2) if $s = 4b - 1$ then there is a 2×3 integral matrix P such that $PP^t = \mathrm{diag}(s_1, s_2)$.

These two conditions follow from the Rational Family Theorem (0.0.8) and the Geramita-Verner Theorem (0.0.12).

For $s \leq 28$, (5.5.1) and (5.5.2) are sufficient for existence.

(5.5.3) **THEOREM.** *Suppose that $b \leq 7$ and s_1 and s_2 are positive integers which satisfy* (5.5.1) *and* (5.5.2). *Then there is an orthogonal design of type (s_1, s_2) and order $4b$.*

Proof. The table (5.5.4) gives the first rows of circulant matrices which can be used in the Goethals-Seidel array to obtain orthogonal designs

of order 28 and the types listed. (These circulant matrices were found by implementing the method of section (2.1) on the Univac U1100/42 computer at the Australian National University.) For types and orders other than those in this table the theorem is proved in [19], [31], [55], [57]. □

(5.5.4) TABLE

(4, 19)	$aaaaaa\bar{a}\bar{a}$,	$aa0\bar{a}aa0$,	$a\bar{a}aa\bar{a}ab\bar{b}$,	$bb0a0\bar{a}0$
(5, 21)	$aab\bar{a}ab\bar{b}$,	$a\bar{a}\bar{a}aa\bar{a}bb$,	$aaa\bar{a}\bar{a}\bar{a}a0$,	$aaaa\bar{a}a0$
(6, 17)	$aaaa\bar{a}b\bar{b}$,	$a\bar{a}aaa\bar{a}ab$,	$\bar{a}b0\bar{a}000$,	$bbaa\bar{a}\bar{a}0$
(6, 20)	$aa\bar{a}\bar{a}aa\bar{a}b$,	$aaaa\bar{a}a\bar{b}$,	$ababa\bar{a}0$,	$\bar{a}\bar{a}ba\bar{b}a0$
(1, 6, 21)	$b\bar{b}b\bar{b}b\bar{b}c$,	$bbbb\bar{b}\bar{b}a$,	$bb\bar{a}bba\bar{a}$,	$b\bar{b}\bar{b}bbaa$
(7, 15)	$\bar{a}\bar{a}\bar{a}aaa\bar{a}b$,	$b\bar{a}0b000$,	$ababa\bar{b}0$,	$aab\bar{a}aa0$
(7, 19)	$aa\bar{b}aab\bar{b}$,	$aaa\bar{a}b\bar{a}0$,	$aba\bar{a}a\bar{a}0$,	$a\bar{a}\bar{a}aabb$
(1, 10, 14)	$0b\bar{b}b\bar{b}bb$,	$\bar{b}aaa\bar{a}a0$,	$b\bar{a}bcba0$,	$bba\bar{b}\bar{a}b0$
(9, 16)	$bbbab\bar{a}\bar{b}$,	$aaaa\bar{b}b0$,	$aa\bar{a}\bar{a}b\bar{b}0$,	$a\bar{a}a\bar{a}\bar{a}a0$
(8, 17)	$a\bar{a}aa\bar{a}\bar{a}a0$,	$aabbbb\bar{b}0$,	$ab\bar{a}\bar{a}\bar{a}b0$,	$aca\bar{a}aab\bar{b}$
(11, 15)	$b\bar{a}bbb\bar{b}b0$,	$ba\bar{b}\bar{b}bb0$,	$aaa\bar{a}\bar{a}aab$,	$aaaa\bar{a}a\bar{a}$
(11, 17)	$bbbaa\bar{b}\bar{b}$,	$bbb\bar{b}aa\bar{b}$,	$a\bar{a}\bar{a}\bar{a}\bar{a}ab$,	$aaa\bar{a}aaa\bar{a}$
(12, 14)	$ababab\bar{b}$,	$\bar{a}bb\bar{a}\bar{a}a0$,	$a\bar{a}b\bar{a}bb\bar{b}$,	$aa\bar{a}\bar{a}b\bar{b}0$
(9, 17)	$ab\bar{a}bbb\bar{b}$,	$aa\bar{b}baa0$,	$\bar{a}\bar{a}abaa\bar{b}$,	$a\bar{a}a\bar{a}\bar{a}a0$
(11, 12)	$bb\bar{b}b0b0$,	$a\bar{a}aa000$,	$abab\bar{b}\bar{b}$,	$\bar{a}\bar{a}\bar{a}aa\bar{a}b$

It is conjectured (0.0.14) that (5.5.1) suffices for the existence of an integer N such that an orthogonal design of type (s_1, s_2) and order $4n$ exists for each $n \geq N$. For $s \leq 36$, this is true with only two exceptions.

(5.5.5) THEOREM. *Suppose that* s_1 *and* s_2 *are positive integers such that* $s_1 + s_2 \leq 36$ *and* $s_1 s_2$ *is a sum of* 3 *squares. If* $(s_1, s_2) \neq (11, 23)$ *or* $(15, 19)$ *then there is an integer* N *such that an orthogonal design of type* (s_1, s_2) *and order* $4n$ *exists for each* $n \geq N$. □

This theorem may be proved by considering each pair (s_1, s_2) separately, and using the methods of section (3.2).

(5.6) Weighing matrices of order equivalent to 4 modulo 8

For each positive integer k denote by $N(k)$ the smallest integer such that a weighing matrix of weight k and order $4n$ exists for each $n \geq N(k)$. The argument is omitted where convenient. Using similar methods as in section (5.1), it can be shown that if ε is a positive real number then there is a real constant A such that $N(k) \leq Ak^{5+\varepsilon}$ for all k .

However, numerical evidence suggests that $N(k)$ is much smaller. It has been conjectured [69] that $N(k) = [(k+3)/4]$. This conjecture has been verified for $k \leq 45$. For $46 \leq k \leq 60$, the following table gives an upper bound $\overline{N}$ for N .

(5.6.1) TABLE

k	$4\overline{N}$	$4[(k+3)/4]$	k	$4\overline{N}$	$4[(k+3)/4]$
46	104	48	54	108	56
47	48	48	55	108	56
48	48	48	56	56	56
49	104	52	57	120	60
50	52	52	58	60	60
51	52	52	59	60	60
52	52	52	60	60	60
53	60	56			

(5.7) GGS arrays of order 12

There are GGS arrays of order 12 and the following types:

4 variables: (1, 1, 1, 1), (1, 1, 2, 2), (2, 2, 2, 2), (2, 2, 4, 4) ;

3 variables: (1, 1, 1), (1, 1, 2), (1, 1, 4), (1, 1, 5), (1, 2, 2), (1, 2, 3), (2, 2, 2), (2, 2, 4), (2, 2, 5), (2, 2, 8), (2, 4, 4), (2, 4, 6), (3, 3, 3), (4, 4, 4) ;

2 variables: (1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (1, 8), (1, 9), (1, 10), (1, 11), (2, 2), (2, 3), (2, 4), (2, 5), (2, 6), (2, 7), (2, 8), (2, 9), (2, 10), (3, 3), (3, 4),

(3, 6), (3, 7), (3, 8), (3, 9), (4, 4), (4, 5), (4, 6), (4, 8), (5, 5), (5, 7), (6, 6) .

All but (1, 8), (1, 9), (1, 10), (1, 11), (3, 4), (3, 8), (3, 9), (5, 7) can be constructed by using 3×3 matrices in the Goethals-Seidel array (2.0.5) (see Theorem (2.2.2)). The first rows of some of these circulants are listed below, and others can be obtained by elementary constructions (section (1.2)). The two variable GGS arrays may be made from orthogonal designs of the same type (see section (2.2)).

(5.7.1) TABLE

type	circulant matrices
(1, 1, 1, 1)	$a00$, $b00$, $c00$, $d00$
(1, 1, 2, 2)	$a00$, $b00$, $cd0$, $c\bar{d}0$
(2, 2, 2, 2)	$ab0$, $a\bar{b}0$, $cd0$, $c\bar{d}0$
(2, 2, 4, 4)	abc , $a\bar{b}\bar{c}$, $db\bar{c}$, $d\bar{b}c$
(1, 1, 5)	$a00$, $b00$, $\bar{c}cc$, $0cc$
(2, 2, 5)	$ab0$, $\bar{a}b0$, $\bar{c}cc$, $0cc$
(3, 3, 3)	abc , $a\bar{b}0$, $a0\bar{c}$, $0b\bar{c}$
(2, 9)	$ab\bar{b}$, $a\bar{b}b$, bbb , $0b\bar{b}$
(3, 7)	$ab0$, $a0b$, $a\bar{b}\bar{b}$, $\bar{b}bb$
(5, 5)	$ab\bar{b}$, $0aa$, $ba\bar{a}$, $0bb$
(5, 6)	abb , $\bar{b}aa$, $\bar{b}bb$, $0a\bar{a}$.

GGS arrays of the following types are not known to exist, even though the corresponding orthogonal designs exist.

4 variables: (1, 1, 1, 4), (1, 1, 1, 9), (1, 1, 2, 8), (1, 1, 4, 4), (1, 1, 5, 5), (1, 2, 2, 4), (1, 2, 3, 6), (3, 3, 3, 3) ;

3 variables: (1, 1, 9), (1, 1, 10), (1, 2, 4), (1, 2, 6), (1, 2, 8), (1, 3, 6), (1, 3, 8), (1, 4, 4), (1, 4, 5), (1, 5, 5), (2, 3, 4), (2, 3, 6), (2, 3, 7), (2, 5, 5), (3, 3, 6) .

REFERENCES

[1] J.F. Adams, "Vector fields on spheres", *Ann. of Math.* (2) 75 (1962), 603-632.

[2] M.F. Atiyah, "The role of algebraic topology in mathematics", *J. London Math. Soc.* 41 (1966), 63-69.

[3] Leonard D. Baumert, *Cyclic Difference Sets* (Lecture Notes in Mathematics, 182. Springer-Verlag, Berlin, Heidelberg, New York, 1971).

[4] L.D. Baumert and Marshall Hall Jr., "A new construction for Hadamard matrices", *Bull. Amer. Math. Soc.* 71 (1965), 169-170.

[5] V. Belevitch, "Theory of $2n$-terminal networks with applications to to conference telephony", *Electr. Commun.* 273 (1950), 231-244.

[6] Ian F. Blake, "On a generalization of the Pless symmetry codes", *Information and Control* 27 (1975), 369-373.

[7] Ian F. Blake and R.C. Mullin, *The Mathematical Theory of Coding* (Academic Press, New York, San Francisco, London, 1975).

[8] Z.I. Borevich and I.R. Shafarevich, *Number Theory* (Academic Press, New York and London, 1966).

[9] R. Bott and J. Milnor, "On the parallizability of the spheres", *Bull. Amer. Math. Soc.* 64 (1958), 87-89.

[10] Joan Cooper and Jennifer Wallis, "A construction for Hadamard arrays", *Bull. Austral. Math. Soc.* 7 (1972), 269-278.

[11] P. Delsarte, J.M. Goethals, and J.J. Seidel, "Orthogonal matrices with zero diagonal. II", *Canad. J. Math.* 23 (1971), 816-832.

[12] Peter Eades, "Some asymptotic existence results for orthogonal designs", *Ars Comb.* 1 (1976), 109-118.

[13] Peter Eades, "Some new constructions for orthogonal designs using circulants", *Proc. Fifth Austral. Conf. Combinatorics*, Melbourne 1976 (to appear).

[14] Peter Eades, "Orthogonal designs constructed from circulants", *Utilitas Math.* 11 (1977), 43-55.

[15] Peter Eades, "A note on orthogonal designs of order 20 ", (unpublished note).

[16] Peter Eades, "A note on the Hadamard conjecture", submitted.

[17] Peter Eades and Richard M. Hain, "On circulant weighing matrices", *Ars Comb.* 2 (1976), 265-284.

[18] Peter Eades, Peter J. Robinson, Jennifer Seberry Wallis and Ian S. Williams, "An algorithm for orthogonal designs", *Proc. Fifth Manitoba Conference on Numerical Mathematics*, Manitoba, 1975 (Congressium Numerantium, XVI, 279-292. Utilitas Math., Winnipeg, 1976).

[19] Peter Eades and Jennifer Seberry Wallis, "An infinite family of skew weighing matrices", *Combinatorial Mathematics IV* (Proc. Fourth Austral. Conf. Combinatorial Mathematics, Adelaide, 1976. Lecture Notes in Mathematics, 560, 27-40. Springer-Verlag, Berlin, Heidelberg, New York, 1977).

[20] Peter Eades and Jennifer Seberry Wallis, "Some asymptotic results for orthogonal designs: II", *Colloque sur Problèmes Combinatoures et Theorie des Graphes*, Orsay, France, 1976.

[21] Peter Eades, Jennifer Seberry Wallis and Nicholas Wormald, "A note on asymptotic existence results for orthogonal designs", *Proc. Fifth Austral. Conf. Combinatorics*, Melbourne, 1976 (to appear).

[22] Dennis Estes and Gordon Pall, "The definite octonary quadratic forms of determinant 1 ", *Illinois J. Math.* 14 (1970), 159-163.

[23] Anthony V. Geramita and Joan M. Geramita, "Complex orthogonal designs", Queen's Math. Preprints, No. 1975-10, Queen's University, Kingston, Ontario, 1975.

[24] Anthony V. Geramita, Joan Murphy Geramita and Jennifer Seberry Wallis, "Orthogonal designs", *J. Lin. Multilin. Algebra* 3 (1975/76), 281-306.

[25] A.V. Geramita and N.J. Pullman, "A theorem of Radon-Hurwitz and orthogonal projective modules", *Proc. Amer. Math. Soc.* 42 (1974), 51-66.

[26] A.V. Geramita and Jennifer R. Seberry, *Orthogonal Designs* (in preparation).

[27] A.V. Geramita and J.H. Verner, "Orthogonal designs with zero diagonal", *Canad. J. Math.* 28 (1976), 215-224.

[28] Anthony V. Geramita and Jennifer Seberry Wallis, "A survey of orthogonal designs", *Proc. Fourth Manitoba Conference on Numerical Mathematics*, Manitoba, 1974 (Congressium Numerantium, XII, 121-168. Utilitas Math., Winnipeg, 1975).

[29] Anthony V. Geramita and Jennifer Seberry Wallis, "Orthogonal designs II", *Aequationes Math.* 13 (1975), 299-313.

[30] Anthony V. Geramita and Jennifer Seberry Wallis, "Orthogonal designs III: weighing matrices", *Utilitas Math.* 6 (1974), 209-236.

[31] Anthony V. Geramita and Jennifer Seberry Wallis, "Orthogonal designs IV: existence questions", *J. Combinatorial Theorem Ser. A* 19 (1975), 66-83.

[32] J.M. Goethals and J.J. Seidel, "Orthogonal matrices with zero diagonal", *Canad. J. Math.* 19 (1967), 1001-1010.

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

[34] J.M. Goethals and J.J. Seidel, "Strongly regular graphs derived from combinatorial designs", *Canad. J. Math.* 22 (1970), 597-614.

[35] D. Glynn, Draft of PhD thesis.

[36] J. Hadamard, "Résolution d'une question rélative aux déterminants", *Darboux Bull.* (2) 17 (1893), 240-256.

[37] Richard Martin Hain, "Circulant weighing matrices", (MSc thesis, Australian National University, Canberra, 1977).

[38] Marshall Hall Jr., *Combinatorial Theory* (Blaisdell [Ginn and Co.], Waltham, Mass., 1967).

[39] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers* (Claredon Press, Oxford, 1960).

[40] I.N. Herstein, *Topics in Algebra* (Blaisdell, Waltham, Mass., 1964).

[41] J.S. Hsia, "Two theorems on integral matrices", *J. Lin. Multilin. Algebra* (to appear).

[42] A. Hurwitz, "Über die Komposition der quadratischen Formen", *Math. Ann.* 88 (1923), 1-25.

[43] R.N. Ibbett, D. Aspinall and J.F. Grainger, "Real-time multiplexing of dispersed spectra in any wavelength region", *Appl. Optics* 7 (1968), 1089-1093.

[44] Burton W. Jones, *The Arithmetic Theory of Quadratic Forms* (Carus Monographs, 10. John Wiley & Sons, New York, 1950).

[45] M. Kneser, "Klassenzahlen definiter quadratischer Formen", *Arch. Math.* 8 (1957), 241-250.

[46] R.C. Mullin and R.G. Stanton, "Group matrices and balanced weighing designs", *Utilitas Math.* 8 (1975), 277-301.

[47] Gordon Pall and Peter Eades, "Integral quadratic forms and orthogonal designs", unpublished manuscript.

[48] R.E.A.C. Paley, "On orthogonal matrices", *J. Math. Phys.* 12 (1933), 311-320.

[49] J. Radon, "Lineare Scharen orthogonaler Matrizen", *Abh. Math. Sem. Hamburg. Univ.* 1 (1922), 1-14.

[50] D. Raghavarao, "Some optimum weighing designs", *Ann. Math. Stat.* 30 (1959), 295-303.

[51] D. Raghavarao, "Some aspects of weighing designs", *Ann. Math. Stat.* 31 (1960), 878-884.

[52] K.B. Reid and Ezra Brown, "Doubly regular tournaments are equivalent to skew-Hadamard matrices", *J. Combinatorial Theory Ser. A* 12 (1972), 332-338.

[53] Peter J. Robinson, "A non-existence theorem for orthogonal designs", *Utilitas Math.* 10 (1976), 179-184.

[54] Peter J. Robinson, "Amicable orthogonal designs", *Bull. Austral. Math. Soc.* 14 (1976), 303-314.

[55] Peter J. Robinson, "Orthogonal design in order 24 ", *Proc. Fifth Austral. Conf. Combinatorics*, Melbourne, 1976 (to appear).

[56] Peter J. Robinson, "Concerning the existence and construction of orthogonal designs" (PhD thesis, Australian National University, Canberra, 1977).

[57] Peter J. Robinson, "Orthogonal designs in order 16 ", *Ars Combinatoria* (to appear).

[58] Peter J. Robinson, "Using product designs to construct orthogonal designs", *Bull. Austral. Math. Soc.* 16 (1977), 297-305.

[59] Peter J. Robinson and Jennifer Seberry, "On the structure and existence of some amicable orthogonal designs", *J. Austral. Math. Soc. Ser. A* (to appear).

[60] Peter J. Robinson and Jennifer Seberry, "Orthogonal designs in powers of two", *Ars Combinatoria* (to appear).

[61] Peter J. Robinson and Jennifer Seberry Wallis, "A note on using sequences to construct orthogonal designs", *Colloq. Math. Soc. Janos Bolyai* (to appear).

[62] Jean-Pierre Serre, *A Course in Arithmetic* (Graduate Texts in Mathematics, 7. Springer-Verlag, New York, Heidelberg, Berlin, 1973).

[63] D. Shapiro, "Similarities, quadratic forms and Clifford algebras", (PhD thesis, University of California, Berkeley, 1974).

[64] W. Siérpinski, *Elementary Theory of Numbers* (Panstwowe wydawnictwo Nautowe, Warszawa, 1964).

[65] Neil J.A. Sloane and Martin Harwitt, "Masks for Hadamard transform optics", *Appl. Optics* 15 (1976), 107-114.

[66] G. Szekeres, "Tournaments and Hadamard matrices", *Enseignement Math.* 15 (1969), 269-278.

[67] Olga Taussky, "(1, 2, 4, 8)-sums of squares and Hadamard matrices", *Proc. Symp. Pure Math. Combinatorics*, 229-234 (Amer. Math. Soc., Providence, Rhode Island, 1971).

[68] Richard J. Turyn, "Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression and surface wave encodings", *J. Combinatorial Theory Ser. A* 16 (1974), 313-333.

[69] Jennifer Wallis, "Orthogonal (0, 1, -1) matrices", *Proc. First Austral. Conf. Comb. Math.*, 61-84 (TUNRA, Newcastle, Australia, 1972).

[70] Jennifer Seberry Wallis, "On the existence of Hadamard matrices", *J. Combinatorial Theory Ser. A* 21 (1976), 444-451.

[71] Jennifer Seberry Wallis, "Constructions for amicable orthogonal designs", *Bull. Austral. Math. Soc.* 12 (1975), 179-182.

[72] Jennifer Seberry Wallis, "Orthogonal designs V: orders divisible by eight", *Utilitas Math.* 9 (1975), 263-281.

[73] Jennifer Wallis and Albert Leon Whiteman, "Some classes of Hadamard matrices with constant diagonal", *Bull. Austral. Math. Soc.* 7 (1972), 233-249.

[74] Jennifer Seberry Wallis and Albert Leon Whiteman, "Some results on weighing matrices", *Bull. Austral. Math. Soc.* 12 (1975), 433-447.

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

[76] Helmut Wielandt, *Finite Permutation Groups* (Academic Press, New York and London, 1964).

[77] John Williamson, "Hadamard's determinant theorem and the sum of four squares", *Duke Math. J.* 11 (1944), 65-81.

[78] Warren W. Wolfe, "Orthogonal designs - amicable orthogonal designs - some algebraic and combinatorial techniques" (PhD thesis, Queen's University, Kingston, 1975).

[79] Warren W. Wolfe, "Rational quadratic forms and orthogonal designs", Queen's Math. Preprints, No. 1975-22. (Queen's University, Kingston, 1975.) To appear *J. Number Theory*.

APPENDIX

SOME UNSOLVED PROBLEMS

The following problems are selected on two criteria.

Firstly, the author considers these problems to be solvable - no questions of immense difficulty are included.

Secondly, solutions to these problems would enhance the results of this thesis.

(Q1). In section (2.4) it is shown that there are at most $[\frac{1}{2}\rho(2n)]$ variables in a GGS array of order n. If 16 divides n, then $[\frac{1}{2}\rho(2n)] \geq 5$; are there any GGS arrays with 5 variables?

(Q2). Suppose that H and G are transitive abelian subgroups of the symmetric group, and θ is an isomorphism from H onto G. Then it can be shown [16] that there is a permutation ϕ such that $\psi\theta = \phi^{-1}\psi\phi$ for each $\psi \in H$. Hence type 1 matrices on transitive groups are classified up to conjugacy by isomorphism. Can a similar theorem be proved for GC-rings in general?

(Q3). GGS arrays of type (m, m, m, m) and order equivalent to 4 modulo 8 play an important role in Chapters 2, 3 and 5. However the only such arrays known for $m \equiv 3 \pmod 4$ have m a power of 3 (Proposition 2.2.3). Are there any GGS arrays of type (m, m, m, m) and order equivalent to 4 modulo 8 where $m \neq 3$ is squarefree and equivalent to 3 modulo 4 ?

(Q4). Are there orthogonal designs of types (3, 7, 8), (1, 3, 6, 8), (1, 4, 4, 9), (2, 2, 5, 5), and order 20 ? (An answer to this question cannot be found by using GGS arrays (see section (2.4)), and could lead to new methods for constructing orthogonal designs of order equivalent to 4 modulo 8 .)

(Q5). Theorem (4.1.7) is proved using a great deal of heavy machinery. Is there a direct combinatorial proof?

(Q6). Is there a weighing matrix of weight 9 and order 15 ?

(Q7). Is there a real number r between 0 and 1 such that if $s_1, s_2, \ldots, s_u$ are positive integers with sum less than $2^a r$, then there is an orthogonal design of type $(s_1, s_2, \ldots, s_u)$ and order 2^a ? (A positive answer to this question would lower the bounds in the asymptotic results of section (3.2) - see the remark after Lemma (3.2.7).)

(Q8). Are there any weighing matrices of weight 36 and odd order n such that $45 \leq n \leq 89$?