Jennifer Seberry

Orthogonal Designs

Hadamard Matrices, Quadratic Forms and Algebras

Springer

Orthogonal Designs

Jennifer Seberry

Orthogonal Designs

Hadamard Matrices, Quadratic Forms and Algebras

Springer

Jennifer Seberry
School of Computing and Information
Technology
University of Wollongong
Wollongong, NSW
Australia

ISBN 978-3-319-59031-8 ISBN 978-3-319-59032-5 (eBook)
DOI 10.1007/978-3-319-59032-5

Library of Congress Control Number: 2017945720

Original publication: "Orthogonal Designs: Hadamard matrices and quadratic forms" - A.V. Geramita, J. Seberry. 1979. Marcel Deckker Press - Taylor & Francis, US.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

This book is dedicated, with the greatest respect, to Anthony V Geramita who has now gone to the Erdos' great SF. I thank Joan Geramita, his friend, colleague and heir, for permission to use Tony's work in this updated volume.

Preface

Problems concerned with the structure and existence of various kinds of matrices with elements from 0,1,-1, for example, Hadamard matrices and their generalization to weighing matrices, have long been of interest to workers in combinatorics and also applied statisticians, coding theorists, signal processors and other applied mathematicians. A first volume, "Orthogonal Designs: quadratic forms and Hadamard matrices" (Ed 1), was written jointly by Anthony V. Geramita and Jennifer Seberry and published by Marcel Dekker in 1979, but never reprinted. This 1979 volume, devoted to a ground-breaking approach, illuminated the connections between these various kinds of matrices and exposed new connections with several other areas of mathematics. The current volume, "Orthogonal Designs: Hadamard matrices, quadratic forms and algebras", is the revision and update of the initial volume created using research theses and papers written in the intervening years. This more recent research has led to new ideas for many areas of mathematics, signal processing and non-deterministic computer programming in computational mathematics. These approaches are through the investigation of orthogonal designs: roughly speaking, special matrices with indeterminate entries.

Originally this subject had been discussed in our research papers and those of our colleagues and students. The discovery of the intimate relationship between orthogonal designs and rational quadratic forms had not appeared in print before 1973. The finding of numerous constructions and interesting objects that appeared fundamental to the study of Hadamard matrices (and their generalizations) finally prompted Geramita and Seberry to look afresh at the work that had already appeared. They recast their work and their collaborators and students in the light of their new discoveries. This present updated and new work continues the previous book and introduces more recent material by collaborators, colleagues and students. It leads to new algebras, techniques and existence results.

As will be clear in the text, orthogonal designs is a heavy "borrower" of mathematics. The reader will find us using results from, for example, algebraic number theory, quadratic forms, difference sets, representation theory, coding

theory, finite geometry, elementary number theory, cyclotomy, the theory of computation and signal processing. The reader is not expected to be conversant with all these areas; the material is presented in such a way that even the novice to these areas will understand why and how we intend to use the results stated, even if the proofs in some cases remain a mystery. In those cases where detailed explanation would take too long, references are given so the interested reader can fill out their background. Thus the original volume and this volume can be profitably read both by experts and by people new to this area of discrete mathematics and combinatorics.

To dispel any notion that this book closes the area for further research, many problems are highlighted, all unsolved, and directions in which further research is possible are suggested. These problems vary in depth: some are seemingly very simple, others are major.

Some comments on how this volume is organized: the organization is, in part, directed by the Janus-like features of the study. In the first three chapters, which largely remain untouched and are heavily underpinned by the farsighted work of Anthony V. Geramita, the nature of the problem at hand is described, and some remarks made on the ingredients of a solution. After some preliminaries, a rather deep foray is made into the algebra side of the question. In broad terms, the algebra there described allows us to identify the first set of non-trivial necessary conditions on the problem of existence of orthogonal designs. Chapter 4 concentrates, and with the necessary conditions as a guide, on attempts to satisfy these conditions. Many different methods of construction are described and analysed. Chapter 5 focusses on one of these construction methods and analyses it in detail, both algebraically and combinatorially. Here again, the interplay between classical algebra and combinatorics is shown to have striking consequences. Chapter 6 deeply studies two construction methods introduced but not analysed in the original book. The result is new algebras which have been developed to encompass these combinatorial concepts. Chapter 7 deviates to give some of the theory and existence results for areas of number theory and discrete applied mathematics which have proved, over the past forty to fifty years, to have been somewhat forgotten by those not studying orthogonal designs. In Chapter 8 a very strong non-existence theorem for orthogonal designs is proved. The "Asymptotic Hadamard Existence Theorem" and related wonderful asymptotic consequences and questions, which are central to Chapter 9, are due to a number of authors. Chapter 10 reminds us that we have not finished with number theoretic consequences and other combinatorial features of orthogonal designs by commencing the study of non-real fields. Finally, in the Appendices, we tabulate numerous calculations we have made in specific orders.

Acknowledgements

No book this size could be the child of one or two parents. Many people are owed a debt of deep gratitude. For the original book Dan Shapiro (Ohio State) helped immensely with his work on similarities. The 1970's students Peter Robinson (ANU, Canberra), Peter Eades (ANU, Canberra) and Warren Wolfe (Queens', Kingston) had major input; the 1980's students of Seberry, Deborah J. Street (Sydney), Warwick de Launey (Sydney) and Humphrey Gastineau-Hills (Sydney), and the 2000's students Chung Le Tran (Wollongong) and Ying Zhao (Wollongong) have contributed conspicuously to the volume. Many, many colleagues such as Marilena Mitrouli (Athens), Christos Koukouvinos (NTUA, Athens) and his students Stelios Georgiou and Stella Stylianou, Hadi Kharghani (Lethbridge), Wolf Holzmann (Lethbridge), Rob Craigen (Winnipeg), Ilias Kotsireas (WLU), Dragomir Đoković (Waterloo), Sarah Spence Adams (Olin, Boston), Behruz Tayfeh-Rezaie (IPM, Tehran) and Ebrahim Ghaderpour (York, Toronto) have helped shape and correct our work. I acknowledge that at times I might have written utter rubbish without their knowledge and thoughts. I leave writing this book knowing it is an unfinished work, knowing that I have included many errors large and small. I acknowledge the generous proofing help for the original volume by Joan Geramita and Chuck Weibel. I acknowledge the LaTeXing proofing, and exceptional research assistance given me over the past ten years by Max Norden. I came to today with the help of the University of Wollongong Library and the provision of an office to me as Emeritus Professor.

From the original preface "Finally, a word of our experience writing this book. We approached the problems herein from quite different backgrounds. It became evident that Geramita was more interested in the connections with algebra, while Seberry was more interested in actually making the objects that could be made. The inevitable tensions that arise from these differing viewpoints (will), we hope, make this book more interesting to read."

Wollongong, Australia *Jennifer Seberry*
November 2016

Contents

About the Author

Emeritus Professor Jennifer Seberry is an Australian cryptographer, mathematician, and computer scientist, now at the University of Wollongong. A graduate of UNSW and LaTrobe, she has taught at the Universities of Newcastle, Sydney, UNSW (ADFA) and Wollongong. Her areas of research include discrete and combinatorial mathematics, Hadamard matrices and bent functions for cryptology, and orthogonal designs. She has published over 400 papers and 7 books. She was the first person in Australia to teach computer security to university students. She is highly respected and has been made a Fellow of the International Association for Cryptologic Research and a Chartered Mathematician by the Institute of Mathematics and its Applications.

List of Tables

List of Figures

Chapter 1
Orthogonal Designs

An orthogonal design of order n, type $(s_1,\ldots,s_\ell)$, denoted, $OD(n;s_1,\ldots,s_\ell)$, s_i positive integers, is an $n\times n$ matrix X, with entries from $0,\pm x_1,\ldots,\pm x_\ell$ (the x_i commuting indeterminates) satisfying:

$$XX^\top = \left(\sum_{i=1}^{\ell} s_i x_i^2\right) I_n\,.$$

Alternatively, each row of X has s_i entries of the type $\pm x_i$ and the rows are orthogonal under the Euclidean inner product.

We may view X as a matrix with entries in the field of fractions of the integral domain $\mathbb{Z}[x_\ell,\ldots,x_\ell]$, ($\mathbb{Z}$ the rational integers), and then if we let $f=\sum_{i=1}^{\ell} s_i x_i^2$, X is an inversible matrix with inverse $\frac{1}{f}X^\top$. Thus, $X^\top X = fI_n$, and so our alternative description of the rows of X applies equally well to the columns of X.

The task to which this text is addressed can be simply described as follows: Find necessary and sufficient conditions on the set of integers $n;s_1,\ldots,s_\ell$ such that there exists an orthogonal design in order n of type $(s_1,\ldots,s_\ell)$, $OD(n;s_1,\ldots,s_\ell)$.

The generality of the question is such that it includes many other problems which have been extensively studied and provides an umbrella under which these problems may be considered simultaneously. Also, in this generality the connections between these classical combinatorial problems and some of the great mathematics of the past century are illuminated. More particularly, the general approach shows the close connection the combinatorial problems studied have with the classification theorems of quadratic forms over $\mathbb{Q}$, the rational numbers. These classification theorems, largely the work of Minkowski, are among the few complete mathematical triumphs of this century. The fact that a partial solution to our general question is embedded in this beautiful theory gives us hope that there will now continue a deeper investigation

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5_1

of these combinatorial problems and the still unresolved problem of the classification of quadratic forms over $\mathbb{Z}$.

1.1 Generalities on Hurwitz-Radon families to prove that there exist orthogonal designs of type $(1,1,\ldots,1)$

If X is an $OD(n;s_1,\ldots,s_\ell)$ on the indeterminates $x_1,\ldots,x_\ell$, we may write:

$$X = A_1x_1 + \cdots + A_\ell x_\ell \tag{1.1}$$

where the A_i are $0,1,-1$ matrices of size $n\times n$. If we let $A*B$ denote the Hadamard product of the matrices A and B (the (i,j) entry of this product is the product of the (i,j) entry of A with the (i,j) entry of B), then the fact that the entries in X were linear monomials in the x_i (or zero) gives us

(i) $A_i * A_j = 0$ if $i \neq j$.
If we write out the fact that $XX^\top = \sum_{i=1}^{\ell} s_i x_i^2 I_n$, using (1.1), and compare coefficients, we find that:
(ii) $A_iA_i^\top = s_iI_n$ $1\leq i\leq \ell$,
(iii) $A_iA_j^\top + A_jA_i^\top = 0$, $1\leq i\neq j\leq \ell$.

We can obviously reverse this procedure, and we state that precisely.

Proposition 1.1. *A necessary and sufficient condition that there exists an $OD(n;s_1,\ldots,s_\ell)$, is that there exist matrices $A_1,\ldots,A_\ell$, satisfying:*

(0) the A_i are $0,1,-1$ matrices, $1\leq i\leq \ell$:
(i) $A_i * A_j = 0$ for $1\leq i\neq j\leq \ell$:
(ii) $A_iA_i^\top = s_iI_n$, $1\leq i\leq \ell$:
(iii) $A_iA_j^\top + A_jA_i^\top = 0$, $1\leq i\neq j\leq \ell$.

The first focus of our attack on the general problem concerns the maximum number of distinct variables that can appear in an orthogonal design of order n.

The last proposition shows that if the orthogonal design involves $\ell-$ variables, we get a collection of ℓ matrices, $A_1,\ldots,A_\ell$ satisfying (0)–(iii). Form the real matrices $B_i = \frac{1}{\sqrt{s_i}}A_i$. Then the B_i satisfy

(a) $B_iB_i^\top = I_n$, $1\leq i\leq \ell$,
(b) $B_iB_j^\top + B_jB_i^\top = 0$, $1\leq i\neq j\leq \ell$.

If we normalize the collection $B_1,B_2,\ldots,B_\ell$ by multiplying each member, on the right, by $B_1^\top$ and let $C_\ell = B_\ell B_1^\top$, then $C_1 = I$ and the remaining $C_2,\ldots,C_\ell$ are orthogonal, anti-commuting, skew-symmetric matrices, as is easily checked.

The question: How many real orthogonal anti-commuting skew-symmetric matrices there can be in order n is a question that was completely settled in the early twentieth century by J. Radon [162]. Radon's work (extending earlier work by A. Hurwitz [111]) was centred around a proposition concerning the composition of quadratic forms. The question Radon dealt with was given n, find the maximal m so that

$$(x_1^2+\cdots+x_n^2)(y_1^2+\cdots+y_m^2)=f_1^2+\cdots+f_n^2$$

where the f_i are real bilinear functions of the x_i and y_j. We shall not go into the connections between this problem and its relation to orthogonal matrices here, but just shall be content to quote the relevant facts. For a discussion of this Radon-Hurwitz problem, we suggest (Herstein [99], Curtis [38] or Lam [142]).
For ease in exposition we make the following definition.

Definition 1.1. A family $A_1,\ldots,A_s$ of real orthogonal matrices of order n satisfying:

(1) $A_i=-A_i^\top$, $1\le i\le s$,
(2) $A_iA_j=-A_jA_i$, $1\le i\ne j\le s$,

will be called a Hurwitz-Radon family (H-R family).

Now if an n is a positive integer, write $n=2^ab$, b odd, and then set $a=4c+d, 0\le d<4$. If we denote by $\rho(n)$ the number $8c+2^d$, the main theorem of Radon [1] states:

Theorem 1.1. *(1) Any H-R family of order n has fewer than $\rho(n)$ members. (2) There is an H-R family of order n having exactly $\rho(n)-1$ members.*

We thus immediately have:

Corollary 1.1. *The maximum number of variables in an orthogonal design of order n is $\le\rho(n)$.*

Unfortunately, Radon's theorem is not suitable, directly, for use with Proposition 1.1 since we need 0,1,-1 matrices.

If, however, we look for integer H-R families, this will automatically give us 0,1,-1 matrices, since an integer orthogonal matrix can only have entries from 0,1,-1. The fact that (2) of Theorem 1.1 could be improved in this direction was noted independently by Geramita-Pullman [78] and Gabel [62].

We need to make a few remarks about the function $\rho(n)$. First observe that when $n=2^ab$, b odd, then $\rho(n)=\rho(2^a)$. Let $n_1=2^{4s+3}$, $n_2=2^{4(s+1)}$, $n_3=2^{4(s+1)+1}$, $n_4=2^{4(s+1)+2}$ and $n_5=2^{4(s+1)+3}$; then

$$\begin{aligned}\rho(n_2)&=\rho(n_1)+1,\\ \rho(n_3)&=\rho(n_1)+2,\\ \rho(n_4)&=\rho(n_1)+4,\\ \rho(n_5)&=\rho(n_1)+8.\end{aligned}$$

We shall assume that the reader is familiar with the elementary properties of tensor products for matrices (see Marcus and Minc [151] or Kronecker).

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

Proposition 1.2. *(a) $\{A\}$ is an H-R family of $\rho(2)-1$ integer matrices of order 2.*
(b) $\{A\otimes I_2, P\otimes A, Q\otimes A\}$ is an H-R family of $\rho(4)-1$ integer matrices of order 4.
(c) $\{I_2\otimes A\otimes I_2,\ I_2\otimes P\otimes A,\ Q\otimes Q\otimes A,\ P\otimes Q\otimes A,\ A\otimes P\otimes Q,\ A\otimes P\otimes P,\ A\otimes Q\otimes I_2\}$ is an H-R family of $\rho(8)-1$ integer matrices of order 8.

Proof. A tedious check using the symmetries of A, P, Q and I_2 and the behaviour of these symmetries with respect to $\otimes$. □

Theorem 1.2. *There is an H-R family of integer matrices of order n having $\rho(n)-1$ members.*

Proof. The proposition above handles the cases $n = 3t, 4t, 8t, t$ odd (just tensor with I_t). The reader may easily verify that if $\{M,\ldots,M_s\}$ is an H-R family of integer matrices of order n, then
(1) $A\otimes I_n \cup Q\otimes M_i \mid i=1,\ldots,s$ is an H-R family of $s+1$ integer matrices of order $2n$.
If, in addition, $\{L_1,\ldots,L_m\}$ is an H-R family of integer matrices of order k, then
(2) $\{P\otimes I_k\otimes M_i \mid 1\le i\le s\}\cup\{Q\otimes L_j\otimes I_n \mid 1\le j\le m\}\cup\{A\otimes I_{nk}\}$ is an H-R family of $s+m+1$ integer matrices of order $2nk$. □

Let $n_1,\ldots,n_5$ be as before 1.2, and we may proceed by induction: Starting with the fact that (c) in 1.2 gives us the case $n_\ell = 2^3$. (Note that the nature of $\rho(n)$ allows us to only consider $n = 2^\ell$).

Now (l) gives us the transition from n_1 to n_2; if we now use (2), letting $k = n_1, n = 2$ (and hence by (a) of 1.2, $s = 1$), we get the transition from n_1 to n_3. We then use (2) (this time with (b) and (c) of the Proposition) to get the two remaining transitions n_1 to n_4, n_1 to n_5. That completes the proof.

To apply this theorem to orthogonal designs, we need one observation. If A, B are two members of an integral H-R family, then A and B are each $\{0,1,-1\}$ matrices and $A*B=0$. The orthogonality of A (and B) and the fact that the entries are integers shows immediately that A and B are $\{0,1,-1\}$ matrices with precisely one non-zero entry in each row and column. From the anticommutativity of A and B it follows that $(A+B)(A+B)^\top = 2I$, and so $A+B$ has exactly two non-zero entries in each row and column, and hence $A*B=0$. With the aid of 1.1, we sum this up by stating:

Theorem 1.3. *Given any natural number n, then*

(i) any orthogonal design in order n can involve at most $\rho(n)$ variables;

(ii) there is an orthogonal design in order n involving $\rho(n)$ variables.

Proof. Only (b) requires a small comment. If $A_1, \ldots, A_{\rho(n)-1}$ is an integral H-R family of order n then $\{I_n, A_1, \ldots, A_{\rho(n)-1}\}$ is a family of matrices satisfying the conditions of Proposition 1.1 and gives an orthogonal design of type $\underbrace{1,1,\ldots,1}_{\rho(n)-tuple}$ in order n. □

Thus, we have found the restrictions that must be placed on the number of variables in an orthogonal design, and we may rephrase our original question: Given n and $\ell \leq \rho(n)$, find necessary and sufficient conditions on $\{s_1, \ldots, s_\ell\}$ such that there exists an $OD(n : s_1, \ldots, s_\ell)$.

Remark 1.1. In cases $n = 2$, or $n = 4$, they come from the usual representations of the complex numbers and quaternions in 2×2 and 4×4 matrices respectively. For $n = 8$ the matrices are derived from the usual method of describing the multiplication table for the Cayley numbers (see, for example, Schafer [173]).

Chapter 2
Some Algebraic and Combinatorial Non-existence Results

In this chapter we intend to explain some easily obtained non-existence theorems for orthogonal designs. Many of these results will be generalized in later chapters, but we feel that these simpler special cases will give the reader an idea as to how the subject developed and what sorts of propositions might be expected.

2.1 Weighing Matrices

To help in the development, and because of independent interest, we make a new definition.

Definition 2.1. A weighing matrix of weight k and order n is an $n \times n$ $\{0,1,-1\}$ matrix A such that $AA^\top = kI_n$. (Note: $A^\top A = AA^\top = kI_n$).

Such matrices have already appeared naturally as the "coefficient" matrices of an orthogonal design. (See Raghavarao [163] or [164] for why these are called weighing matrices and why there is interest in them by statisticians. See also J. Wallis [232].) We shall refer to such a matrix as a $W(n,k)$.

Hadamard [95] showed that $H(n) = W(n,n)$ only exist if $n = 1,2$, or $\equiv 0 \pmod 4$. It is an easy exercise to show:

Proposition 2.1. *In order that a $W(n,n)$ exist, $n = 1,2$ or $4|n$.*

The proof uses, in an essential way, the fact that entries in an Hadamard matrix are $\{\pm 1\}$, and the statement would be false without that, since $(3I_9)(3I_9)^\top = 9I_9$, for example.

Now, when n is odd, $\rho(n) = 1$, and an orthogonal design on one variable is nothing more than a weighing matrix.

We shall next attempt to find some necessary conditions on the type of an orthogonal design in order n. We shall only consider a few special cases here: namely, n odd and $n = 2b$, b odd. We shall come back to the general problem later.

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5_2

2.2 Odd Order

We have already seen that $\rho(n) = 1$, and we need only consider orthogonal designs on one variable, that is, weighing matrices.

Proposition 2.1 already tells us something: If n is odd and a $W(n,k)$ exists, then $k \neq n$.

Proposition 2.2. *If X is a $W(n,k)$, n odd, then $k = a^2$ for some $a \in \mathbb{Z}$.*

Proof. More generally, if X is a matrix of odd order n with rational entries and $XX^\top = qI_n$, then $q = r^2$ with $r \in \mathbb{Q}$; for $\det(X)^2 = q^2$ and since q^n is a square and n is odd, q is already a square. The proposition follows from the observation that if an integer is the square of a rational number, it is the square of an integer. □

This proposition by itself does not to begin to tell the whole story in odd order, as the following example shows:

Example 2.1. There is no $W(5,4)$.

The property of being a weighing matrix is unaffected by row (or column) permutations. Multiplications of a row (or column) by -1 also does not affect the property of being a weighing matrix. Thus, there is no loss in generality if we assume a $W(5,4)$ has first row [11110]. The inner product of rows 1 and 2 of our matrix is zero, and so there are an even number of non-zero entries under the 1's of the first row. There must, then, be a zero in the second row, last column. This then allows only three non-zero entries in the last column; a contradiction.

This example can be generalized.

Proposition 2.3. *If n is odd, then a necessary condition that a $W(n,k)$ exists is that $(n-k)^2 - (n-k) \geq n-1$.*

Proof. (We are indebted to P. Eades for this proof, which is much more illuminating than the proof we gave in Geramita-Geramita-Wallis [77].)

We start with a preliminary observation: If M is an $n \times n$ $\{0,1\}$ matrix with exactly k non-zero entries in each row and column, and if we number the rows of M by $r_1, \ldots, r_n$, then, for any $1 \leq j \leq n$,

$$\sum_{\substack{i=1 \\ i \neq j}}^{n} r_i \cdot r_j = k^2 - k \tag{2.1}$$

To see this let J be the $n \times n$ matrix of ones. Then $MJ = kJ = M^\top J$, and hence $MM^\top J = k^2 J$, and so

$$\sum_{i=1}^{n} r_i \cdot r_j = k^2$$

Since $r_j \cdot r_j = k$, equation (2.1) is then clear.

To see the relevance of this observation, suppose n is odd and W is a $W(n,k)$, and set $X = W * W$. Then X is a $\{0,1\}$-matrix with exactly k non-zero entries in every row and column. An additional fact about X is that the inner product of any two of its rows is even.

Let $Y = J - X$, and note that Y has exactly $n-k$ non-zero entries in every row and column and, since n is odd, the inner product of any pair of rows of Y is odd and so ≥ 1.

Applying our preliminary observation to Y, we obtain $(n-k)^2 - (n-k) \geq n-1$, as was to be shown. □

Remark 2.1. We conclude that $W(5,4)$, $W(11,9)$, $W(19,16)$, $W(29,25)$, $W(41,36)$, and so on, do not exist. This remark does not exclude $W(7,4)$, $W(13,9)$, $W(31,25),\ldots,W(111,100)$, among others.

This proposition is far from the last word on non-existence, as the following example shows:

Example 2.2. There is no $W(9,4)$. (This proof is due to J. Verner.)(Note that here we do have $(n-k)^2 - (n-k) = 5^2 - 5 = 20 > 8 = n-1$).

We now consider $W(2t+1,t)$ for integers $t \geq 2$. We see that

$$(n-k)^2 - (n-k) = (t+1)^2 - (t+1) = t^2 + t \ \geq 2t = n-1$$

but using Verner's method we have

Lemma 2.1. *There does not exist a $W = W(2t+1,t)$ for $t > 2$ (although a $W(2t+1,t)$ satisfies the known necessary conditions for t, a square).*

Proof. We use 'e' to denote an even number of elements and 'o' to denote an odd number of elements. We notice that orthogonality requires that an even number of non-zero elements overlap in any pair of rows. We use 'x' to denote a non-zero element.

We permute the rows and columns of W until the first row has its first k elements $+1$. We permute the columns so the second row has non-zero elements first. Similarly and other row can be permuted so its first elements are non-zero.

Let k be odd. Thus diagrammatically any three rows are

$$\overbrace{\underbrace{1\ldots\ldots\ldots\ldots\ldots 1}_{o}\ \underbrace{0\ldots\ldots\ldots\ldots\ldots 0}_{e}}$$

$$\begin{array}{llllllll}
1\ldots\ldots\ldots\ldots\ldots & 1 & 0\ldots\ldots\ldots\ldots\ldots & 0 \\
x\ldots\ldots\ \ x\,0\ldots\ldots & 0 & x\ldots\ldots\ \ x\,0\ldots\ldots & 0 \\
\underbrace{x\ldots x}_{e}\ \underbrace{0\ldots 0}_{e} & \underbrace{x\ldots x}_{e}\ \underbrace{0\ldots 0}_{o} & \underbrace{x\ldots x}_{e}\ \underbrace{0\ldots 0}_{e} & \underbrace{x\ldots x}_{o}\ \underbrace{0\ldots 0}_{o}
\end{array}$$

Thus it is always possible to force the last column to contain a zero. Again the last column is all zeros which contradicts the definition of a weighing matrix.

Problem 2.1 (Research Problem). What other restrictions can be found for the non-existence of $W(n,k)$ k odd?

Let k be even. Thus diagrammatically any three rows are

$$\begin{array}{cccccccc}
\overbrace{\qquad\qquad\qquad\qquad}^{e} & & & & \overbrace{\qquad\qquad\qquad\qquad}^{o} & & & \\
1\ \ldots\ldots\ldots\ldots\ldots & & & 1 & 0\ \ldots\ldots\ldots\ldots\ldots & & & 0 \\
x\ \ldots\ldots & & x\,0\ \ldots\ldots & 0 & x\ \ldots\ldots & & x\,0\ \ldots\ldots & 0 \\
\underbrace{x\ldots x}_{e} & \underbrace{0\ldots 0}_{e} & \underbrace{x\ldots x}_{e} & \underbrace{0\ldots 0}_{e} & \underbrace{x\ldots x}_{e} & \underbrace{0\ldots 0}_{e} & \underbrace{x\ldots x}_{e} & \underbrace{0\ldots 0}_{o}
\end{array}$$

Thus it is always possible to force the last column to contain a zero. Thus the last column is all zeros which contradicts the definition of a weighing matrix. □

The "boundary" values of proposition 2.3 are of special interest, that is, when $n=(n-k)^2-(n-k)+1$. An inspection of the proof shows that if A is a $W(n,k)$ for such an n and k and if we set $B=J-A*A$ (where J is the $n\times n$ matrix of 1's), then $BB^\top=(n-k-1)I_n+J$; that is B is the incidence matrix of a projective plane of order $n-k-1$ (see Hall [97]).

Thus, for example, the existence of $W(111,100)$ would imply the existence of a projective plane of order 10. Lam showed the projective plane of order 10 does not exist [141]. We shall not go into projective planes here but will sum up this discussion by stating:

Proposition 2.4. *A $W(m^2+m+1,m^2)$ exists only if a projective plane of order m exists.*

It is worth mentioning now, and we shall prove in Section 4.4, that for those m where it is currently known that a projective plane of order m exists, then it is also known that a $W(m^2+m+1,m^2)$ also exists. It is hard to believe that the additional structure in a weighing matrix will not make its existence more difficult than the existence of a projective plane, yet there is no evidence to the contrary. Clearly the existence problem for $W(m^2+m+1,m^2)$ merits considerable attention.

There is little more we can do to the non-existence problem for weighing matrices of odd order, and so we shall leave that subject now. This last tantalising connection between weighing matrices of odd order and projective planes has made us wonder what other combinatorial structures may be related to the non-boundary values of Proposition 2.3. This area is wide open for further study.

We have seen that $\rho(n)=2$ in this case, and so our investigation of orthogonal designs in these orders must centre about one-variable designs (that is, weighing matrices) and two-variable designs.

For our first theorem in these orders, we shall need a classical theorem about quadratic forms. The theorem can be stated for matrices without any reference to quadratic forms, however, and since we intend to come back to quadratic forms later, we shall for now just state the theorem in its unmotivated form.

Definition 2.2. Let R be any commutative ring with identity, and let A, B be two $n \times n$ symmetric matrices with entries in R. We say that A and B are *congruent* if there is an invertible matrix P, with entries in R, such that $PAP^\top = B$.

Notation: If A is an $n \times n$ matrix over the ring R and B is an $m \times m$ matrix over R, then $A \oplus B$ is the $(n+m) \times (n+m)$ matrix $\left[\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right]$ where 0 stands for the appropriate-sized matrix of zeros.

Theorem 2.1 (Witt Cancellation Theorem). *Let F be a field of characteristics $\neq 2$, and let A and B be symmetric $n \times n$ matrices over F. Let X be any symmetric matrix over F. If $A \oplus X$ is congruent to $B \oplus X$, then A is congruent to B.*

Proof. See Lam [142]. □

We now apply this to orthogonal designs.

Theorem 2.2 (Raghavarao-van Lint-Seidel). *Let $n \equiv 2 \pmod 4$, and let A be a rational matrix of order n with $AA^\top = kI_n$, $k \in \mathbb{Q}$. Then $k = q_1^2 + q_2^2$, $q_1, q_2 \in \mathbb{Q}$.*

Proof. (This theorem was first provided by Raghavarao in [163] and another proof later given by van Lint-Seidel in [150]. The proof we give here is different from both and is based on a suggestion of H. Ryser [171].)

It is a well known theorem of Lagrange that every rational number is the sum of four squares of rational numbers, so let $k = k_1^2 + k_2^2 + k_3^2 + k_4^2$.

From the matrix

$$M = \begin{bmatrix} k_1 & k_2 & k_3 & k_4 \\ -k_2 & k_1 & -k_4 & k_3 \\ -k_3 & k_4 & k_1 & -k_2 \\ -k_4 & -k_3 & k_2 & k_1 \end{bmatrix}$$

It is easy to check that

$$MM^\top = kI_4. \tag{2.2}$$

The hypothesis of the theorem asserts that

$$AA^\top = kI_n. \tag{2.3}$$

Thus, from (2.2) we obtain that I_4 is congruent to kI_4 over $\mathbb{Q}$ and from (2.3) that I_n is congruent to kI_n over $\mathbb{Q}$.

By Witt's Cancellation Theorem, applied $\frac{n-2}{4}$ times, and the fact that the $n \equiv 2 \pmod 4$, we obtain I_2 is congruent to kI_2 over $\mathbb{Q}$; that is, there is a 2×2 rational matrix B such that $BB^\top = kI_2$. From this it is obvious that k is a sum of two squares in $\mathbb{Q}$. □

Corollary 2.1. *Let $n \equiv 2 \pmod 4$. If X is*

(a) a $W(n,k)$ or
(b) an orthogonal design of type (s_1, s_2) in order n,

then each of k, s_ℓ, s_2, $s_1 + s_2$ is a sum of two squares in $\mathbb{Z}$.

Proof. (a) From the theorem we obtain that k is a sum of two squares of rational numbers. It is a famous theorem of Fermat (see, for example, Samuel [172]) that if n is an integer and $n = c^2 d$ d square-free ($c, d \in \mathbb{Z}$), then n is a sum of two squares of integers if and only if whenever p is a prime and $p|d$, then $p = 2$ or $p = 1 \pmod 4$. It follows easily from this that if an integer is the sum of two squares of rational numbers, then it is the sum of two squares of integers.

(b) If X is $OD(n; s_1, s_2)$, then $X = A_1 x_1 + A_2 x_2$. Then A_i is a $W(n, s_i)$, and setting $x_1 = x_2 = 1$ we find $A_1 + A_2$ is a $W(n, s_1 + s_2)$. The result now follows from (a). □

Proposition 2.5. *Let $n \equiv 2 \pmod 4$, and let A be a rational matrix of order n satisfying:*

(i) $A = -A^\top$;
(ii) $AA^\top = kI_n$.

Then $k = r^2$, $r \in \mathbb{Q}$.

Proof. Since $AA^\top = kI_n$, we have $\det = (k^n)^{1/2}$. For $n \equiv 2 \pmod 4$, $\frac{n}{2} = s$ is odd. Now, since A is skew symmetric, $\det = q^2$ where $q =$ Pfaffian of A (see Artin [12]). Thus, $q^2 = k^s$, and since s is odd, $k = r^2$ for some $r \equiv \mathbb{Q}$. □

Corollary 2.2. *If $n \equiv 2 \pmod 4$ and X is an $OD(n; s_1, s_2)$, then $s_1 s_2$ is a square in $\mathbb{Z}$.*

Proof. Let

$$X = A_1 x_1 + A_2 x_2 ;$$

then $A_i A_i^\top = s_i I_n$ and $A_1 A_2^\top + A_2 A_1^\top = 0$.
Let

$$B_1 = \frac{1}{s_1} A_1^\top A_1 , \qquad B_2 = \frac{1}{s_1} A_1^\top A_2 .$$

Then $B_1 = I_n$ and $B_1 B_2^\top + B_2 B_1^\top = 0$; that is, $B_2 = -B_2^\top$. Also, $B_2 B_2^\top = \frac{s_2}{s_1} I_n$.

Thus, by the proposition, $\frac{s_2}{s_1}$ is a square in $\mathbb{Q}$; but then so is $s_1^2(\frac{s_2}{s_1}) = s_1 s_2$. However, if an integer is the square of a rational number, it is the square of an integer. □

So far, all the conditions that we have found necessary for the existence of an orthogonal design in order $n \equiv 2 \pmod 4$ have not depended on the fact that the matrices we want should have entries $\{0, 1, -1\}$. In fact, we have proven half of the following:

Theorem 2.3. *Let $n \equiv 2 \pmod 4$. A necessary and sufficient condition that there exist two rational matrices A and B of order n such that $AA^\top = q_1 I_n$, $BB^\top = q_2 I_n$, and $AB^\top + BA^\top = 0$ is that q_1, q_2 each be a sum of two squares in $\mathbb{Q}$ and that $q_1 q_2$ be a square in $\mathbb{Q}$.*

Proof. We have already seen the necessity of three conditions, and so it remains only to show that they are sufficient.

Write $q_1 = r_1^2 u$, $q_2 = r_2^2 v$ where $r_1, r_2 \in \mathbb{Q}$ $u, v \in \mathbb{Z}$, and u and v are square-free. Since $q_1 q_2$ is a square, we obtain $u = v$. Since q_1 and q_2 are each a sum of two squares, we find that $u = v = s^2 + t^2$. Now $q_1 = (r_1 s)^2 + (r_1 t)^2$ and $q_2 = (r_2 s)^2 + (r_2 t)^2$.

Let

$$A_1 = \begin{bmatrix} r_1 s & r_1 t \\ -r_1 t & r_1 s \end{bmatrix}, \qquad B_1 = \begin{bmatrix} -r_2 t & r_2 s \\ -r_2 s & -r_2 t \end{bmatrix};$$

then if $n = 2m$, m odd, one easily checks that $A = A_1 \otimes I_m$, $B = B_1 \otimes I_m$ are the required matrices. □

We can get one additional fact from knowing that in an orthogonal design the coefficient matrices are special.

2.3 Algebraic Problem

Proposition 2.6. *If $n \equiv 2 \pmod 4$, $(n > 2)$ and X is an $OD(n; s_1, \ldots, s_\ell)$ then $s_1 + s_2 < n$.*

Proof. If $s_1 + s_2 = n$, then by setting the variables in the design equal to one, we would obtain an Hadamard matrix, that is, a $W(n, n)$. This contradicts Proposition 2.1. □

This last proposition says, for example, that there is no $OD(10; 1, 9)$, although the existence of such an orthogonal design would not contradict Corollary 2.1 or Corollary 2.2.

2.4 Orthogonal Designs' Algebraic Problem

It has already become apparent that two separate kinds of theorem are being proved. If we glance back at the statement of Proposition 2.1, we see that the existence of an $OD(n; s_1, \ldots, s_\ell)$ depended on finding a collection of ℓ matrices, $A_1, \ldots, A_\ell$, satisfying two rather different types of conditions, which we shall label combinatorial and algebraic; namely,

$$\left\{ \begin{array}{c} \text{combinatorial} \\ \text{conditions} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{ll} \text{(0)} & \text{the } A_i \text{ are } \{0, 1, -1\} \text{ matrices, } 1 \le i \le \ell \\ \text{(i)} & A_i * A_j = 0, 1 \le i \ne \ell; \end{array} \right.$$

$$\left\{\begin{array}{l}\text{algebraic}\\ \text{conditions}\end{array}\right\} \leftrightarrow \left\{\begin{array}{ll}\text{(ii)} & A_iA_i^\top = s_iI_n, 1 \le i \le \ell\\ \text{(iii)} & A_iA_j^\top + A_jA_i^\top = 0, 1 \le i \ne j \le \ell.\end{array}\right.$$

When we looked at an orthogonal design in odd order (that is, a weighing matrix), the algebraic conditions yielded the simple statement that the weight had to be a square integer, while the combinatorial condition, in this case only (0), turned out to be the more mystifying and to have the deeper significance (re: the connection with finite projective planes).

In orders $n \equiv 2 \pmod 4$ the algebraic conditions are somewhat more substantial, and the only general combinatorial fact we know to date arose from the simple result that (apart from order 2) a Hadamard matrix can only exist in orders divisible by 4. In Geramita-Verner [82], by a rather tedious and un-instructive argument, it is shown that there is no $OD(18;1,16)$. This fact is not covered by any general theorem and appears to us to be but the tip of an iceberg, indicating what promises to be a rich source of possible combinatorial relations. The entire question of what combinatorial facts prohibit the existence of orthogonal designs in these orders $\equiv 2 \pmod 4$ is virtually untouched.

Theorem 2.3, however, opens up the possibility that the algebraic part of the problem may be tractable. This turns out to be the case and will occupy much of our efforts.

We state the algebraic problem after a definition.

Definition 2.3. A rational family of order n and type $[s_1,\ldots,s_\ell]$, where the s_i are positive rational numbers, is a collection of ℓ rational matrices of order $n, A_1,\ldots,A_\ell$, satisfying:

(a) $A_iA_i^\top = s_iI_n$, $1 \le i \le \ell$;
(b) $A_iA_j^\top + A_jA_i^\top = 0$, $1 \le i \ne j \le \ell$.

Algebraic Problem: Find necessary and sufficient conditions on n and $s_1,\ldots,s_\ell$ in order that there exists a rational family of order n and type $(s_1,\ldots,s_\ell)$.

Clearly, an orthogonal design gives rise to a rational family, but the converse is obviously not true. Nonetheless, if one wants to know if there is an $OD(n;s_1,\ldots,s_\ell)$ and one has proved there can be no rational family in order n of type $[s_1,\ldots,s_\ell]$, then ones knows there can be no orthogonal design of that order and type.

We may, in fact, rephrase many of the results so far proved for orthogonal designs in terms of rational families. For example, we have proved:

Proposition 2.7. *A rational family in order n cannot consist of more than $\rho(n)$ members; furthermore, there are rational families in order n consisting of ℓ members for every $\ell \le \rho(n)$.*

Proof. Examine the discussion after Proposition 1.1 and the proof of Theorem 1.1. □

We have also shown:

Proposition 2.8. *A necessary and sufficient condition that there exists a rational family of*

(a) type $[s]$ *in order* n*, if* n *is odd, is that* s *be a square in* $\mathbb{Q}$*.*
(b) type $[s]$ *in order* n*, if* $n \equiv 2 \pmod 4$*, is that* s *be a sum of two squares in* $\mathbb{Q}$*;*
(c) type $[s_1, s_2]$ *in order* n*, if* $n \equiv 2 \pmod 4$*, is that* $s_1 s_2$ *each be a sum of two squares in* $\mathbb{Q}$ *and* $s_1 s_2$ *be a square in* $\mathbb{Q}$*.*

We shall pursue this algebraic problem in greater depth in the next chapter. For now we shall concentrate on trying to find other combinatorial facts about orthogonal designs.

2.5 Geramita-Verner Theorem Consequences

The major combinatorial result so far found is motivated by the following theorem.

Theorem 2.4 (Delsarte-Goethals-Seidel [39]). *Let* A *be a* $W(n, n-1)$ *with the rows reordered so that the diagonal consists of zeros.*

(a) If $n \equiv 2 \pmod 4$*, then multiplication by* -1 *of rows (or columns) of* A *as necessary yields a matrix* $\bar{A}$ *with* $\bar{A} = \bar{A}^\top$*.*
(b) If $n \equiv 0 \pmod 4$*, then multiplication by* -1 *of rows (or columns) of* A *as necessary yields a matrix* $\bar{A}$ *with* $\bar{A} = -\bar{A}^\top$*.*

Proof. See Delsarte-Goethals-Seidel [39]. □

This result may be generalized to orthogonal designs as follows.

Theorem 2.5 (A. Geramita-J. Verner [82]). *Let* X *be* $OD(n; s_1, \ldots, s_\ell)$ *with* $\sum_{i=1}^{\ell} s_i = n - 1$*.*

(a) If $n \equiv 2 \pmod 4$*, there is an* $OD(n; s_1, \ldots, s_\ell)$ *where* $\bar{X}$ *has zero-diagonal and* $\bar{X} = \bar{X}^\top$*.*
(b) If $n \equiv 0 \pmod 4$*, there is an* $OD(n; s_1, \ldots, s_\ell)$ *where* $\bar{X}$ *has zero-diagonal and* $\bar{X} = -\bar{X}^\top$*.*

Proof. If necessary, reorder the rows (or columns) so that the orthogonal design X has 0-diagonal. In this form if x_1 (say) occurs in position (i, j), $i < j$, then position (j,i) contains $\pm x_1$.

For suppose not, and assume, without loss of generality, that position (j,i) contains $\pm x_2$. Consider the various incidences between the i-th and j-th rows.

Count all occurrences of $\binom{\pm x_1}{\pm x_1}$, and assume there are t_1 of these; similarly, assume there are a total of t_2 occurrences of $\binom{\pm x_1}{\pm x_2}$ and $\binom{\pm x_2}{\pm x_1}$ and a total of t_3 occurrences of $\binom{\pm x_1}{\pm x_k}$ and $\binom{\pm x_k}{\pm x_1}$, $k \neq 1, 2$.

Since rows i and j are orthogonal it follows that each of t_1, t_2 and t_3 must be even.

Observe also that these incidences account for all but one of the x_ℓ's in rows i and j, namely, that occurring as $\binom{x_1}{0}$.

Thus, $2t_1 + t_2 + t_3 = 2s_\ell - 1$, and this is a contradiction. □

Now suppose $n \equiv 2 \pmod 4$, and multiply rows and columns of the orthogonal design by -1, as necessary, so that each variable in the first row and column appears with coefficient $= +1$. Call the resulting matrix $\bar{X}$, and replace every variable in it by $+1$ to obtain the $W(n, n-1)$,

$$\begin{bmatrix} 0 & 1 & \dots & 1 \\ 1 & \ddots & * & \\ \vdots & * & \ddots & \\ 1 & & & 0 \end{bmatrix}$$

By Theorem 2.4 part (a), multiplication of appropriate rows and columns of this matrix by -1 will make it symmetric. However, as the first row and column are already symmetric, it follows that the entire matrix is symmetric. Hence, $\bar{X} = \bar{X}^\top$, as was to be shown.

For $n \equiv 0 \pmod 4$, multiply the rows and columns of X so that each variable in the first row appears with coefficient $= +1$ and each variable in the first column appears with coefficient $= -1$. Call the resulting matrix $\bar{X}$, and set each variable $= +1$. The argument above, with Theorem 2.4 part (b) implies $\bar{X} = -\bar{X}^\top$.

Corollary 2.3. *Let $n \equiv 0 \pmod 4$. There is an $OD(n; s_1, \dots, s_\ell)$ with $\sum_{i=1}^{\ell} s_i = n-1$ if and only if there is an $OD(n; 1, s_1, \dots, s_\ell)$ with $1 + \sum_{i=1}^{\ell} s_i = n$.*

Proof. The sufficiency is evident.

To establish the necessity, one observes that in view of Theorem 2.5 part(b) if there is an orthogonal design of the type described, then there is one $\bar{X}$ where $\bar{X} = -\bar{X}^\top$ on the variables $x_1, x_2, \dots, x_\ell$. It is then easily verified that $Y = yI + \bar{X}$ is an $OD(n; 1, s_1, s_2, \dots, s_\ell)$. □

Corollary 2.4. *If $n \neq 1, 2, 4, 8$, then there is a $\rho(n)$-tuple, $(s_1, \dots, s_{\rho(n)})$ with $s_i > 0$ and $\sum_{i=1}^{\rho(n)} s_i \leq n$ which is not the type of an orthogonal design of order n.*

Proof. If n is odd, $n > 1$, there is no $W(n, 2)$ since 2 is not a square.

If $n \equiv 2 \pmod 4, n > 2$, there is no orthogonal design of type (1,2) in order n, by Corollary 2.2.

So let $n \equiv 0 \pmod 4, n \neq 4, 8$. In this case $n - \rho(n) > 0$. So we may consider the $\rho(n)$-tuple $(1, 1, \ldots, n - \rho(n)$. The sum of the entries in this tuple is $n - 1$, and so by Corollary 2.3 there is an orthogonal design on $\rho(n) + 1$ variables. This contradicts Theorem 1.3 part (a). □

The full strength of Corollary 2.4 will best be realised after the algebraic question of orthogonal designs is dealt with in greater depth. We come back to this theorem again at the end of the next chapter.

Chapter 3
Algebraic Theory of Orthogonal Designs

As we saw in the last chapter, it is possible to obtain some non-trivial necessary conditions for the existence of orthogonal designs just by considering the equations that the coefficient matrices of an orthogonal design must satisfy. The *ad-hoc* procedures we give in the last chapter can, with difficulty, be pursued further. However, these procedures quickly become inadequate. To properly describe the solution to the "algebraic problem of orthogonal designs", it is necessary to discuss the theory of quadratic and bilinear forms. Only then can the "algebraic problem" be put in proper perspective. It is possible to highlight this theory fairly quickly, and we do that in this chapter. References for all omitted proofs are included.

Following the general discussion of quadratic and bilinear spaces, we restrict ourselves to the field of rational numbers and develop the theory of similarities of a bilinear space in detail. It is in the study of similarities that the connections with orthogonal designs is revealed.

The major source for this work is the Berkeley-thesis of Dan Shapiro [190] and the papers Shapiro [192], [193], [194] and his subsequent unpublished manuscript "Rational Spaces of Similarities". Shapiro first pointed out the connections between the problems we were studying and his work on similarities. He subsequently solved the algebraic problem of orthogonal designs. Special cases of the solution had first been given in Geramita-Geramita-Wallis [77], Geramita-Wallis [81], and Wolfe [247], [248].

3.1 Generalities on Quadratic and Bilinear Forms

We recall here some elementary notion about quadratics and bilinear forms. In addition to reminding the reader of these ideas, this introduction will serve to establish the notation we shall use. Most proofs are omitted, and we refer the reader to any of the following excellent sources for further information: (Lam [142], Scharlau [174], O'Meara [159], Serre [189], Bourbaki [27]).

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5_3

Definition 3.1. Let k denote a field and V a vector space over k. A function $B : V \times V \mapsto k$ is called a *bilinear form* if, for every $v \in V$, the maps $B_v : V \mapsto k$ and ${}_vB : V \mapsto k$, defined by $B_v(x) = B(x,v)$ and ${}_vB(x) = B(v,x)$, are linear maps. If, in addition, $B_v =_v B$ for all $v \in V$, then B is called a *symmetric bilinear form*.

We shall be exclusively concerned with symmetric bilinear forms and so shall usually drop the adjective "symmetric" when referring to them.

Definition 3.2. A function $q : V \mapsto k$ is called a *quadratic form* on V if

(i) $q(\alpha v) = \alpha^2 q(v)$, for all $\alpha \in k$, vvV, and
(ii) the map from $V \times V \mapsto k$ given by

$$(v_1, v_2) \mapsto q(v_1 + v_2) - q(v_1) - q(v_2)$$

is a (symmetric) bilinear form.

The pair (V,B) will be called a *bilinear space*, and the pair (V,q) will be called a *quadratic space*. If k is a field of characteristic not equal to 2, these two notions are intimately connected.

To see this, let (V,q) be a quadratic space, and define $B_q : V \times V \mapsto k$ by $B_q(x,y) = (\frac{1}{2})(q(x+y) - q(x) - q(y))$. Then B_q is a bilinear form on V by definition of (V,q). Thus, to the quadratic space (V,q) we can make correspond the bilinear space (V,B_q).

On the other hand, let (V,B) be a bilinear space, and define $q_B : V \mapsto k$ by $q_B(x) = B(x,x)$. It is easy to see that q_B is a quadratic form on V since $q_B(\alpha x) = B(\alpha x, \alpha x) = \alpha^2 B(x,x) = \alpha^2 q_B(x)$ and the map from $V \times V \mapsto k$ given by $(x,y) \mapsto q_B(x+y) - q_B(x) - q_B(y)$ is a bilinear form.

It is not hard to show that these two processes are inverse to each other; that is, given (V,B), form (V,q_B) and then construct (V,B_{q_B}).

Then (V,B) and (V,B_{q_B}) are the same bilinear space; that is, $B = B_{q_B}$. To see this, observe that $B_{q_B}(x,y) = (\frac{1}{2})(q_B(x+y) - q_B(x) - q_B(y))$, where $q_B(v) = B(v,v)$. Thus,

$$B_{q_B}(x,y) = \left(\frac{1}{2}\right)[B(x+y,x+y) - B(x,x) - B(y,y)] = B(x,y).$$

On the other hand, starting with (V,q), form (V,B_q) and then (V,q_{B_q}). Then (V,q) and (V,q_{B_q}) are the same quadratic space; that is, $q = q_{B_q}$. To see this, note that

$$q_{B_q}(x) = B_q(x,x) = \left(\frac{1}{2}\right)(q(x+x) - q(x) - q(x)) = q(x).$$

We shall now assume characteristic not 2 and thus, in view of the correspondence outlined above, freely interchange the notions of quadratic and bilinear space.

3.2 The Matrix Formulation

Let V be a finite-dimensional vector space over k (say of dimension n), and let $\{e_i\}$, $1 \le i \le n$, be a basis for V. If $v \in V$ and

$$v = \sum_{i=1}^{n} \alpha_i e_i,$$

then we shall denote v by the column vector

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = col(\alpha_1, \ldots, \alpha_n).$$

Definition 3.3. If B is a bilinear form on V, then we form the $n \times n$ matrix $A = (a_{ij})$ as follows: $a_{ij} = B(e_i, e_j)$. It is easy to check that if $x = col(\alpha_1, \ldots, \alpha_n), y = col(\beta_1, \ldots, \beta_n)$, then $B(x, y) = x^\top Ay$ ("$\top$" denotes matrix transpose). We call *A the matrix of the form B with respect to the basis* $\{e_i\}$. (Note that A is a symmetric matrix.)

If (V, q) is a quadratic space, then the matrix of q with respect to the basis $\{e_i\}$ is the matrix of B_q (as defined earlier) with respect to the basis $\{e_i\}$.

On the other hand, if V is an n-dimensional vector space over k, with a fixed basis $\{e_i\}$, $1 \le i \le n$, and A is any $n \times n$ symmetric matrix, then we can define a bilinear form on V by means of A. Namely, if $x = col(\alpha_1, \ldots, \alpha_n)$, $y = col(\beta_1, \ldots, \beta_n), x, y \in V$, define a map from $V \times V \mapsto k$ by $(x, y) \mapsto x^\top Ay$. This is clearly a bilinear form on V, and its matrix with respect to the basis $\{e_i\}$ is clearly A.

Thus, for a fixed basis of V the distinct bilinear forms on V are in one-to-one correspondence with the $n \times n$ symmetric matrices.

If (V, B) is a bilinear space and $\{e_i\}, 1 \le i \le n$, and $\{e'_i\}, 1 \le i \le n$, are two sets of bases for V, it is natural to ask how the matrices of B with respect to each of these bases are related. The formulation turns out to be relatively simple.

Let P be the (invertible) $n \times n$ matrix whose i-th column expresses the coordinates of e_i with respect to the bases $\{e_i\}$. Then, if $v \in V$ and $v = col(\alpha_1, \ldots, \alpha_n)$ with respect to the basis $\{e_i\}$ then

$$P = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} \alpha'_1 \\ \vdots \\ \alpha'_n \end{bmatrix}$$

gives the coordinates of v with respect to the basis $\{e_i\}$.

If we let A and A' denote the matrices of B with respect to the bases $\{e_i\}$ and $\{e'_i\}$, respectively, then it is easy to check that

$$A = P^\top A' P \tag{3.1}$$

Thus A and A' are congruent (see Definition 2.2).

On the other hand, if (V, B) is a bilinear space whose matrix, with respect to some basis, is X and if P is any invertible matrix, then $Y = P^\top X P$ is also the matrix of (V, B), but with respect to a different basis.

The notion of congruence is easily seen to be an equivalence relation on the set of symmetric $n \times n$ matrices.

Definition 3.4. The bilinear space (V, B) is called *non-degenerate* if the map from $V \mapsto V^*$ (dual space) given by $x \mapsto B(x, -)$ is an isomorphism of vector spaces.

In matrix terms, (v, B) is non-degenerate if the matrix of B with respect to any basis is invertible, as is easily shown. (In view of equation (3.1), if the matrix of B with respect to the one basis is invertible, so is the matrix of B with respect to any basis.)

3.3 Mapping Between Bilinear Spaces

Let (V_1, B_1) and $V_2, B_2)$ be two bilinear spaces.

Definition 3.5. A linear transformation $f : v_1 \mapsto V_2$ is called a *similarity* with *similarity factor* $\sigma(f) \in k$ if for any pair of vectors $u, w \in V_1$ we have

$$B_2(f(u), f(w)) = \sigma(f) B_1(u, w)\,.$$

In matrix terms, if we choose bases for V_1 and V_2, respectively, and, with respect to these chosen bases, let A be the matrix for B_1, A' the matrix for B_2,and X the matrix for f, then

$$\sigma(f) A = X^\top A' X.$$

If $\sigma(f) = 1$, then f is usually called a *linear morphism*, and if in addition $V_1 = V_2$, f is called a *isometry*.

If (V, B) is non-degenerate, then the isometries of (V, B) form a group under composition which is called the *orthogonal group* of the bilinear space. Also, the similarities of a non-degenerate bilinear space, with non-zero similarity factors, form a group. We shall investigate this in more detail later.

Finally, if (V, B_1) and (V, B_2) are two non-degenerate bilinear spaces, then (V, B_1) is *isometric* to (V, B_2) if and only if there is an isometry from (V, B_1) to (V, B_2); equivalently, if and only if the matrices of B_1 and B_2, with respect to any basis of V, are congruent.

Thus the classification of non-degenerate bilinear spaces of dimension n over a field k (up to isometry) is equivalent to classifying the congruence classes of invertible $n \times n$ symmetric matrices over k.

We shall spend some time in understanding this classification over a few fields. In general, such a classification involves a deep understanding of the arithmetic structure of k.

3.4 New Spaces From Old

Let (V, B) be a bilinear space, and let $W \subset V$ be a subspace. Then, since $B\colon W \times W \mapsto k$ is a bilinear map, we may consider (W, B) as a bilinear space in this way. The inclusion map from W to V is then a linear morphism. In the same way, if (V, q) is a quadratic space, then $q\,|_W\colon W \mapsto k$ is a quadratic form on W and $(W, q\,|_W)$ is a quadratic space.

Let (V_1, B_1) and (V_2, B_2) be two bilinear spaces.

Definition 3.6. Let $V = V_1 \oplus V_2$; we make V into a bilinear space as follows: Let $x, y \in V$, $x = x_1 \oplus x_2$, $y = y_1 \oplus y_2$, x_i, $y_i \in V_i$, and define $B(x, y) = B_1(x_1,\, y_1) + B_2 x_2,\, y_2)$. It is easy to verify that (V, B) is a bilinear space, and we call (V, B) the *orthogonal sum* of (V_1, B_1) and (V_2, B_2) and write $(V, B) = (V_1, B_1) \perp (V_2, B_2)$.

If (V, B) is any bilinear space, then way sat that $x, y \in V$ are *orthogonal* if $B(x, y) = 0$ and extend this definition to two subspaces V_1, V_2 of V if every vector in V_1 is orthogonal to every vector in V_2. In the orthogonal sum the subspaces that we can naturally identify with V_1 and V_2 are orthogonal.

Now suppose that (V, B) is a bilinear space and that (U, B) and (W, B) are subspaces which are orthogonal and $U + W = V$. It is easy to see that:

Proposition 3.1. *(V, B) and $(U, B) \perp (W, B)$ are isometric bilinear spaces.*

We may carry through this entire discussion for quadratic spaces by defining $(V_1, q_1) \perp (V_2, q_2) = (V, q)$ by setting $q(v_1 + v_2) = q_1(v_1) + q_2(v_2)$ where $v_i \in V_i$. It is routine to check that (V, q) is a quadratic space and that the correspondence between bilinear and quadratic spaces respects orthogonal sums.

In matrix terms: If we choose bases for V_1 and V_2 and let A_i be the matrix for B_i with respect to this basis of V_i $(i = 1, 2)$, then, with respect to the basis for $V_1 \oplus V_2$ obtained by taking the "union" of the two given bases, the matrix of B (the orthogonal sum) is

$$\begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}.$$

(Recall that this is the matrix we have denoted $A_1 \oplus A_2$).

There is one further construction we need to consider. As before, let (V_1, B_1) and (V_2, B_2) be two bilinear spaces and now set $V = V_1 \otimes V_2$. We make V into a bilinear space by defining $B : V \times V \mapsto k$ to be the unique bilinear map satisfying: $B(u_1 \otimes u_2,\, w_1 \otimes w_2) = B_1(u_1, w_1)B_2(u_2, w_2)$, where $u_i, w_i \in V_i$, and call this space the *product* of (V_1, B_1) and (V_2, B_2).

In matrix terms: Let $\{e_i\}$, $1 \le i \le n$, be a basis for V_1 and $\{f_j\}$, $1 \le j \le m$, a basis for V_2. Suppose $A = (a_{ij})$ is the matrix for B_1 with respect to the $\{e_i\}$ and $C = (c_{rs})$ is the matrix for B_1 with respect to the $\{f_j\}$. Then, if we consider the ordered basis for $V_1 \otimes V_2$ to be

$$\{e_1 \otimes f_1, \ldots, e_1 \otimes f_m, \ldots, e_n \otimes f_1, \ldots, e_n \otimes f_m\},$$

the matrix for B with respect to this basis is

$$\begin{bmatrix} a_{11}C & a_{12}C & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{n1} & \ldots & a_{nn}C \end{bmatrix}.$$

In similar fashion we can define the *tensor product of quadratic* spaces in such a way that the correspondence between bilinear and quadratic forms is respected (see Lam [142] for a complete discussion).

3.5 Bilinear Spaces Classification Theorems

We have already seen that the classification (up to isometry) of non-degenerate quadratic or bilinear spaces of dimension n over a field k is equivalent to classifying equivalence classes (under congruence) of invertible symmetric $n \times n$ matrices over k.

Let k^* denote the non-zero elements of k, and $(k^*)^2$ the subgroup of squares of k^*. Then one invariant of a congruence class lies in the quotient group, $k^*/(k^*)^2$. More specifically:

Definition 3.7. If A is an invertible $n \times n$ matrix over k and $\det A = d$, then $\bar{d} \in k^*/(k^*)^2$ is called the *discriminant* of A and denoted *discA*.

A major step toward the classification of bilinear spaces is the following:

Theorem 3.1. *If A is an invertible symmetric $n \times n$ matrix, then A is congruent to a diagonal matrix, $diag(a_1, \ldots, a_n)$.*

Proof. See any of the references on quadratic forms mentioned at the beginning of Definition 3.1. □

Thus every congruence class contains at least one diagonal matrix. So the problem of classifying quadratic spaces reduces to the question of when two invertible diagonal matrices are congruent.

Notation. In view of the previous theorem, we shall adopt the following standard notation. Let (V,q) be a quadratic space, and suppose that with respect to some basis for V the associated matrix is $\mathrm{diag}(a_1,\ldots,a_n)$. We shall refer to the quadratic space (or the isometry class of the quadratic space) as $\langle a_1,\ldots,a_n\rangle$ and drop the space V when no confusion (hopefully) can occur. If $\mathrm{diag}(a_1,\ldots,a_n)$ is congruent to $\mathrm{diag}(b_1,\ldots,b_n)$, then $\langle a_1,\ldots,a_n\rangle = \langle b_1,\ldots,b_n\rangle$ (and conversely).

Clearly $\langle a_1,\ldots,a_n\rangle = \langle a_{\sigma(1)},\ldots,a_{\sigma(n)}\rangle$ for any permutation σ, since, on the matrix level, this just amounts to re-ordering the basis, which is an isometry. Also, $\langle a_1 s_1^2,\ldots,a_n s_n^2\rangle = \langle a_1,\ldots,a_n\rangle$ for any $s_i \upsilon k^*$.

This last observation has as immediate corollaries:

Theorem 3.2. *If k is any algebraically closed field, then any two invertible symmetric $n\times n$ matrices are congruent.*

Proof. In an algebraically closed field everything is a square, so $\langle a_1,\ldots,a_n\rangle = \langle 1.b_1^2,\ldots,1.b_n^2\rangle = \langle 1,\ldots,1\rangle$. Thus every non-degenerate bilinear space is congruent to a fixed bilinear space of the same dimension. □

Theorem 3.3. *If $k=\mathbb{R}$ (the real numbers), then*

$$\langle a_1,\ldots,a_n\rangle = \langle \underbrace{1,\ldots,1}_{\ell}, \underbrace{-1,\ldots,-1}_{s}\rangle$$

for some $0\le \ell, s\le n$.

Proof. In $\mathbb{R}$ everything ($\neq 0$) is either a square or the negative of a square. □

Now if $k=\mathbb{R}$ and if an invertible symmetric $n\times n$ matrix A is congruent to $\langle \underbrace{1,\ldots,1}_{\ell}, \underbrace{-1,\ldots,-1}_{s}\rangle$, we call the integer $\ell - s$ the *signature* of A and write $sgn(A)$.

Theorem 3.4 (Sylvester's Law of Inertia [204]). *The signature of a real symmetric invertible matrix A is well defined and is an invariant of the congruence class containing A. Furthermore, if A and B are real symmetric invertible $n\times n$ matrices, A is congruent to B if and only if $sgn(A)=sgn(B)$.*

3.6 Classification of Quadratic Forms Over $\mathbb{Q}$

Let F be the field with p elements (p a prime). We shall describe a procedure for deciding when an element of F is a square. We may as well assume $p\neq 2$ since in any finite field of characteristic two, everything is a square.

Now $F^* = F\backslash\{0\}$ is a cyclic group of order $p-1$ (which is even) and hence has a unique subgroup of index 2 which consists of the squares of F^*.

Let the two-element group $F^*/(F^*)^2$ be denoted by the group {1,-1} under multiplication.

The map $\chi : F^* \mapsto \{1,-1\}$, which is the natural map onto a quotient, satisfies

$$\chi(a) = \begin{cases} 1 & \text{if } a \text{ is a square in } F^*, \\ -1 & \text{if } a \text{ is not a square in } F^*. \end{cases}$$

The map χ is usually denoted $(\bar{p})$; that is, $(\bar{p})\,(a) = \chi(a) = (\frac{a}{p})$ and is called the *Legendre character*.

We would like a way of calculating $\chi(a)$. The decisive procedures for such a calculation is given by Gauss's celebrated *Law of Quadratic Reciprocity.*

Theorem 3.5 (Gauss). *Let p and q be distant primes, both different from 2. Then*

(i) $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).(-1)^{\left(\frac{(p-1)}{2}\right)\cdot\left(\frac{(q-1)}{2}\right)}$ *reciprocity,*

(ii) $\left(\frac{-1}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8, \\ -1 & \text{if } p \equiv \pm 5 \pmod 8, \end{cases}$

(iii) $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$

We illustrate how to use this theorem by an example.

Example 3.1. Is $n = 2^3.3.7$ a square in $\mathbb{Z}_{67}$? Let $p = 67, n = 2^3.3.7$. Find $(\frac{n}{p})$.

Since the Legendre character is a group homomorphism, we have $(n/p) = \left(2^3/p\right)\,(3/p)\,(7/p)$.

$\left(2^3/p\right) = \left(2^2/p\right)(2/p)$, 2^2 is clearly a square, $\mod p$, so $(2^3/p) = (2/p)$.

Since $67 \equiv -5 \pmod 8$, $(2/67) = -1$.

Now

$$(3/67) = (67/3)(-1)^{33} = -(67/3) = -(1/3) = -1$$

and

$$(7/67) = (67/7)(-1)^{99} = -(67/7) = -(4/7) = -(2^2/7) = -1$$

therefore $(n/67) = -1$ and so n is not a square in $\mathbb{Z}_{67}$. □

Let p be a prime integer, and let $\mathbb{Q}_p$ denote the field of p-adic numbers. If $a, b \in \mathbb{Q}_p$, $a, b \neq 0$, then the *p-adic Hilbert symbol* $(a,b)_p$ is defined by:

$$(a,b)_p = \begin{cases} 1 & \text{if there are } p\text{-adic numbers } x,y, \text{ with } ax^2 + by^2 = 1, \\ -1 & \text{otherwise.} \end{cases}$$

The Hilbert symbols can be shown to have the following properties:

(i) $(a,b)_p = (b,a)_p, (a,c^2)_p = 1$;
(ii) $(a,-a)_p = 1$ and $(a,1-a)_p = 1$;

(iii) $(aa',b)_p = (a,b)_p(a',b)_p$ (bilinearity);
(iv) $(a,b)_p = (a,-ab)_p = (a,(1-a)b)_p$.

The importance of the Hilbert symbols is illustrated by the following theorem.

Theorem 3.6. *Let $\langle a_1,\ldots,a_n\rangle$ be a quadratic form over the field $\mathbb{Q}_p$, and let $s_p(\langle a_1,\ldots,a_n\rangle) = \prod_{i<j}(a_i,a_j)_p$; then*

(1) $s_p(\langle a_1,\ldots,a_n\rangle)$ is an invariant of the quadratic form and is called the Hasse-invariant at p;
(2) the non-degenerate quadratic forms $\langle a_1,\ldots,a_n\rangle$ and $\langle b_1,\ldots,b_n\rangle$ over $\mathbb{Q}_p$ are congruent (over $\mathbb{Q}_p$) if and only if they have the same discriminant and the same Hasse-invariant.

We are now ready to state the crowning achievement of the theory.

If $\langle a_1,\ldots,a_n\rangle$ is a quadratic form over $\mathbb{Q}$, then it may be viewed as a quadratic form over $\mathbb{Q}_p$ for any prime p and over $\mathbb{R}$, the real numbers. If two quadratic forms over $\mathbb{Q}$ are congruent over $\mathbb{Q}$, they are obviously also congruent over $\mathbb{Q}_p$ for ever p and over $\mathbb{R}$. The amazing thing is that the reverse is true.

Theorem 3.7 (Hasse-Minkowski). *If $\langle a_1,\ldots,a_n\rangle$ and $\langle b_1,\ldots,b_n\rangle$ are non-degenerate quadratic forms over $\mathbb{Q}_p$, then they are congruent over $\mathbb{Q}$ if and only if they are congruent over $\mathbb{Q}_p$ (for every p) and over $\mathbb{R}$.*

We have already seen how easy it is to decide congruence over $\mathbb{R}$; we just need to calculate the signature. All that is left to make this classification theorem work is an algorithm for calculating the Hasse-invariants, that is, to calculate the Hilbert symbols.

Suppose $\langle a_1,\ldots,a_n\rangle$ is a quadratic form over $\mathbb{Q}$; we can multiply each a_i by squares in $\mathbb{Q}$ and not change the congruence class of our form. Thus there is no loss in assuming the a_i are square-free integers.

Property (iii) of the Hilbert symbols implies that all we really need is a way to calculate $(r,s)_p$ where r,s are ± 1 or primes, and p is a prime. The prime $p=2$ will require special comment.

Theorem 3.8. *Let $p \neq 2$ be a prime. Then*

(i) $(r,s)_p = 1$ if r and s are relatively prime to p;
(ii) $(r,p)_p = \left(\frac{r}{p}\right)$, the Legendre symbol, if r and p are relatively prime;
(iii) $(p,p)_p = \left(\frac{-1}{p}\right)$.

Remarks. (iii) is easily derived from (ii) and the formal properties of the Hilbert symbols; the major part of this theorem is (i)and (ii).

Note also that (i) has as a corollary the comforting fact in checking if $\langle a_1,\ldots,a_n\rangle$ and $\langle b_1,\ldots,b_n\rangle$ are congruent over $\mathbb{Q}$, we need only check the

Hasse-invariants at the *finite* collection of the primes that divide the $a_i's$ and $b_j's$.

We are left only with the calculation of $(r,s)_2$. This is just a bit more complicated to explain (see Serre [189], for example). But, for our purposes this calculation will not be necessary. To see why, we first define $(r,s)_\infty$ by:

$$(r,s)_\infty = \begin{cases} 1 & \text{if there are real numbers } x \text{ and } y \text{ such that } rx^2+sy^2=1. \\ -1 & \text{otherwise.} \end{cases}$$

Note that $(r,s)_\infty = 1$ unless r and s are **both** negative.

With this definition we have:

Theorem 3.9 (Product Formula).

$$\prod_{\substack{p \, prime \\ p=\infty}} (r,s)_p = 1$$

for any r and s.

Corollary 3.1.

$$\prod_{\substack{p \, prime \\ p=\infty}} s_p(\langle a_1,\ldots,a_n\rangle) = 1.$$

It follows from this that if two quadratic forms over $\mathbb{Q}$ have the same discriminant and the same Hasse invariant at every prime p (including $p=\infty$) except perhaps one, then they have the same Hasse invariant at the prime also. Thus we may with impunity, ignore the prime $p=2$.

We would like to show, by considering some examples, how easy it is to use this criterion for any congruence over $\mathbb{Q}$.

Example 3.2. (a) $\langle 1,1,5,5,\rangle = \langle 1,1,1,1\rangle$ over $\mathbb{Q}$

Proof. They have the same discriminant since $1.1.5.5 = 25 = 1.1.1.1 \pmod{(\mathbb{Q}^*)^2}$. Also both have the same signature and the same Hasse invariant at ∞. The only other prime at which we need to check is $p=5$. Now $s_5(\langle 1,1,1,1\rangle) = 1$, clearly, and

$$\begin{aligned} s_5(1,1,5,5) &= \underbrace{(1,1)_5}_{=1}\underbrace{(1,5)_5(1,5)_5(1,5)_5(1,5)_5}_{[(1,5)_5]^4=1}(5,5)_5 \\ &= (5,5)_5 = \left(\frac{-1}{5}\right) = 1 \text{ for } 5 \equiv 1 \pmod 4. \end{aligned}$$

Therefore, the two quadratic forms are congruent over $\mathbb{Q}$. □

(b) $\langle 1,3,6,8\rangle = \langle 1,1,1,1\rangle$ over $\mathbb{Q}$.

Proof. The only primes we need consider are $2,3,\infty$. The two forms have the same discriminant and signature and the same Hasse-invariant at $p=\infty$. By our remarks we can ignore $p=2$ and just consider $p=3$.
Now $\langle 1,3,6,8\rangle = \langle 1,3,6,2\rangle$ by eliminating squares, and

$$s_3(\langle 1,3,6,2\rangle) = (1,3)_3(1,6)_3(1,2)_3(3,6)_3(3,2)_3(6,2)_3.$$

Since 1 is a square,

$$s_3(\langle 1,3,6,2\rangle) = (3,6)_3(3,2)_3(6,2)_3.$$

Using bilinearity, we have

$$s_3(\langle 1,3,6,2\rangle) = (3,2)_3(3,3)_3(3,2)_3(3,2)_3(2,2)_3.$$

Since the Hilbert symbol only takes on the value ± 1,

$$s_3(\langle 1,3,6,2\rangle) = (3,2)_3(3,3)_3(2,2)_3.$$

Now $(2,2)_3 = 1$ since 2 and 3 are relatively prime. Also $(3,3)_3 = (\frac{-1}{3}) = -1$ for $3 \equiv 3 \pmod 4$, and $(3,2)_3 = (\frac{2}{3}) = -1$ for $3 \equiv -5 \pmod 8$. Therefore, $s_3(\langle 1,3,6,2\rangle) = 1$.
Thus by the Corollary to the Product Formula, $s_p(\langle 1,3,6,2\rangle) = 1$ for every prime p (including $p=2$), and so we are done. □

(c) $\langle 1,2,7,14\rangle \neq \langle 1,1,1,1\rangle$.

Proof. Now $s_p(\langle 1,1,1,1\rangle) = 1$ for every p (including $p=\infty$), $disc(\langle 1,1,1,1\rangle) = \bar{1}$ and $sgn(\langle 1,1,1,1\rangle) = 4$. Now $s_\infty(\langle 1,2,7,14\rangle) = 1$, $disc(\langle 1,2,7,14\rangle) = \bar{1}$ and $sgn(\langle 1,2,7,14\rangle) = 4$. The only primes we need check are $p = 2,7$ (and we ignore 2).
Now $s_7(\langle 1,2,7,14\rangle) = (2,7)_7(2,2)_7(7,7)_7$ after some easy reductions.
But

$$(2,7)_7 = \left(\tfrac{2}{7}\right) = 1 \text{ for } 7 \equiv -1 \pmod 8,$$
$$(2,2)_7 = 1 \text{ since 2 and 7 are relatively prime,}$$

and

$$(7,7)_7 = \left(\tfrac{-1}{7}\right) = -1 \text{ for } 7 \equiv 3 \pmod 4.$$

Therefore

$$s_7(\langle 1,2,7,14\rangle) = -1 \neq (\langle 1,1,1,1\rangle.$$

Thus the two forms are not congruent over $\mathbb{Q}$. □

It is hoped that these few examples illustrate the power and ultimate simplicity of the classification theory for quadratic forms over $\mathbb{Q}$.

3.7 The Similarities of a Bilinear Space

From now on our discussion will always assume that our field k is $\mathbb{Q}$, the rational numbers. This hypothesis is not necessary for most of what we say, but it does avoid some difficulties, and it is the only field with which we are, in this text, eventually concerned. The interested reader should consult D. Shapiro' s papers [192] and [193] for the general discussion.

Recall that if (V_1, q_1) and (V_2, q_2) are two non-degenerate quadratic spaces with associated bilinear spaces (V_1, B_1) and (V_2, B_2), then the linear transformation $f\colon V_1 \mapsto V_2$ is a similarity with similarity factor $\sigma(f) \in \mathbb{Q}$ if for any $x, y \in V_1$ we have $B_2(f(x), f(y)) = \sigma(f) \ldots B_1(x, y)$.

The set of all similarities of a fixed non-degenerate bilinear (quadratic) space (V, B) will be abusively denoted $\boldsymbol{Sim(V)}$ when there is no danger of losing sight of the fact that B gives the underlying bilinear structure on V. Clearly, $Sim(V)$ is closed under composition and scalar multiplication.

Define $Sim^*(V) = \{f \in Sim(V) \,|\, \sigma(f) \neq 0\}$. Then it is easy to see that $Sim^*(V)$ is a group under composition, and the map $\sigma\colon Sim^*(V) \mapsto \mathbb{Q}^*$ by

$$\sigma\colon f \mapsto \sigma(f)$$

is a homomorphism of groups, and $ker\,\sigma = O(V)$, the orthogonal group of (V, B)

Definition 3.8. The bilinear spaces (V_1, B_1) and (V_2, B_2) are *similar* if there is a similarity $f\colon V_1 \mapsto V_2$ with $\sigma(f) \neq 0$.

It is not, in general, true that the sum of two similarities of the bilinear space (V, B) is again a similarity.

Example 3.3. Let $V = \mathbb{Q}^2$, and, with respect to the usual basis of $\mathbb{Q}^2$, assume B has matrix I_2. Let $g\colon V \mapsto V$ be the identity map; then g is a similarity, and $\sigma(g) = 1$.

Let $f\colon V \mapsto V$ have matrix $\left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$ with respect to the fixed basis. Then f is a similarity; for if $x = col(\alpha_1, \alpha_2)$, $y = col(\beta_1, \beta_2)$, then $f(x) = col(\alpha_1, -\alpha_2)$ and $f(y) = col(\beta_1, -\beta_2)$ and

$$B(x, y) = \alpha_1\beta_1 + \alpha_2\beta_2 = B(f(x), f(y)) = \alpha_1\beta_1 + (-\alpha_2)(-\beta_2).$$

Now $f + g$ has matrix $\left[\begin{smallmatrix} 2 & 0 \\ 0 & 0 \end{smallmatrix}\right]$ and we leave it to the reader to check that this is not a similarity.

The question as to when a subset of $Sim(V)$ is closed under addition is of paramount importance in our investigation. We consider that question in some detail in the next section.

3.8 Linear Subspaces of $Sim(V)$

Let (V, B) be a fixed non-degenerate bilinear space, and let $End(V)$ be the $\mathbb{Q}$-algebra of all endomorphisms of V, that is, all $\mathbb{Q}$-linear maps from V to V.

Definition 3.9. The *adjoint map* $\sim: End(V) \mapsto End(V)$ is defined by: If $f \in End(V)$, then $\tilde{f}$ is the unique map such that $B(f(x), y) = B(x, \tilde{f}(y))$, for all $x, y \in V$.

In matrix terms, choose a basis for V, and let X be the matrix for B with respect to this basis, A the matrix for f; then $\sim: A \mapsto X^{-1}A^{\top}X = \tilde{A}$. To see this let $x = col(\alpha_1, \ldots, \alpha_n)$, $y = col(\beta_1, \ldots, \beta_n)$; then

$$\begin{aligned} B(f(x), y) &= (Ax)^{\top} Xy \\ &= x^{\top} A^{\top} Xy \\ &= x^{\top} \left(XX^{-1}\right) A^{\top} Xy \\ &= x^{\top} X \left(X^{-1} A^{\top} Xy\right) \\ &= B\left(x, \tilde{f}(y)\right). \end{aligned}$$

It is easy to check that $\sim$ is a $\mathbb{Q}$-algebra anti-homomorphism; that is,

Proposition 3.2. *In matrix terms,*

(i) $\widetilde{(A+C)} = \tilde{A} + \tilde{C}$;
(ii) $\widetilde{(\alpha A)} = \alpha \tilde{A}$ *and* $\tilde{I} = I$;
(iii) $\widetilde{(AC)} = \tilde{C}\tilde{A}$;
(iv) $\tilde{\tilde{A}} = A$.

The adjoint map gives an easy way to identify similarities.

Proposition 3.3. *Let (V, B) be a non-degenerate bilinear space and $f \in End(V)$. f is a similarity with similarity factor $\sigma(f) = \sigma$ if and only if $\tilde{f}f = \sigma.1_V$ (where 1_V denotes the identity map of V).*

Proof. f is a similarity with similarity factor σ

$$\begin{aligned} &<=> B(f(x), f(y)) = \sigma.B(x, y) \text{ for all } x, y \in V, \\ &<=> B\left(x, \tilde{f}f(y)\right) = \sigma.B(x, y) \text{ for all } x, y \in V. \end{aligned}$$

Since B is non-degenerate, this last holds if and only if $\tilde{f}f = \sigma.1_V$. □

If $\sigma \neq 0$, then f is invertible and $\tilde{f} = \left(\frac{1}{\sigma}f\right)^{-1}$, and so $f\tilde{f} = \sigma 1_V$ also.

From this proposition we can see how the adjoint map also allows a method for deciding when the sum of two elements of $Sim(V)$ is again in $Sim(V)$.

Proposition 3.4. *Let (V,B) be a non-degenerate bilinear space, and suppose $f,g \in Sim(V)$. Then the following are equivalent:*

(1) $f+g \in Sim(V)$;
(2) $\alpha f+\beta g \in Sim(V)$ *for all* $\alpha,\beta \in \mathbb{Q}$;
(3) $\tilde{f}g+\tilde{g}f = c1_V$ *for some* $c \in \mathbb{Q}$.

Proof. (1) $\Leftrightarrow$ (3). $f+g \in Sim(V)$ if and only if $\widetilde{(f+g)}(f+g) = d1_V$, where $d = \sigma(f+g)$ by Proposition 3.3.

Using Proposition 3.2, this in turn is equivalent to $\tilde{f}f+\tilde{g}f+\tilde{f}g+\tilde{g}g = d1_V$ if and only if $\tilde{f}g+\tilde{g}f = (d-\sigma(f)-\sigma(g))1_V$.

(2) $\Rightarrow$ (1). Obvious

(1) and (3) $\Rightarrow$ (2).

$$\begin{aligned}\widetilde{(\alpha f+\beta g)}(\alpha f+\beta g) &= \alpha^2\tilde{f}f+\alpha\beta\tilde{f}g+\beta\alpha\tilde{g}f+\beta^2\tilde{g}g\\ &= \alpha^2\sigma(f)1_V+\alpha\beta c1_V+\beta^2\sigma(g)1_V\\ &= \left(\alpha^2\sigma(f)+\alpha\beta c+\beta^2\sigma(g)\right)1_V,\end{aligned}$$

and so, by Proposition 3.3, $\alpha f+\beta g \in Sim(V)$. □

If, in addition, $\sigma(f+g) \neq 0$, we could then add $g\tilde{f}+f\tilde{g} = c1_V$ to the list of equivalences above.

Definition 3.10. If $f,g \in Sim(V)$ satisfy any of the equivalent conditions of the preceding proposition, then we say that f and g are *compatible similarities.*

If $f_1,\ldots,f_r \in Sim(V)$ are mutually compatible similarities, then the entire $\mathbb{Q}$-linear span of the f_i lie in $Sim(V)$, and we obtain a linear subspace of $Sim(V)$.

Example 3.4. Let V be an n-dimensional vector space over $\mathbb{Q}$ with basis $\{e_i\}, 1 \leq i \leq n$, and suppose that with respect to this basis the matrix for the bilinear form B on V is I_n. Then $End(V)$ is the set of $n \times n$ matrices over $\mathbb{Q}$, which we denote $M_n(\mathbb{Q})$, and the adjoint map $\sim: M_n(\mathbb{Q}) \mapsto M_n(\mathbb{Q})$ is nothing more than $\sim: A \mapsto A^\top$; that is, $\tilde{A} = A^\top$.

Applying the last two propositions, we find that A is a similarity if and only if $A^\top A = dI_n$ for some $d \in \mathbb{Q}$, and if A and B are similarities, $A+B$ is a similarity if and only if $A^\top B+B^\top A = cI$ for some $c \in \mathbb{Q}$.

In this case, the only similarity with similarity factor equal to 0 is the matrix of all zeros. So, if A and B are similarities and $A+B$ is a similarity and $A+B \neq 0$, then $BA^\top+AB^\top = cI$ also.

If we look back at the definition of a rational family (Definition 2.3), we see that a rational family gives rise to a collection of mutually compatible similarities of the bilinear space of this example.

Linear subspaces of $Sim(V)$ have a naturally defined quadratic structure which relates to the quadratic structure on V. More precisely:

Proposition 3.5. *Let (V,B) be a non-degenerate bilinear space. The similarity factor map $\sigma\colon Sim(V)\mapsto\mathbb{Q}$ is a quadratic form on any linear subspace of $Sim(V)$.*

Proof. Let $S\subseteq Sim(V)$ be a linear subspace. If $f\in S$ and $\alpha\in\mathbb{Q}$ then $\sigma(\alpha f)=\alpha^2\sigma(f)$ is clear, and so it remains only to show that the map $B: S\times S\mapsto\mathbb{Q}$ given by $B(f,g)=\sigma(f+g)-\sigma(f)-\sigma(g)$, is bilinear. It obviously suffices to show that

$$B(\alpha_1 f_1+\alpha_2 f_2,g)=\alpha_1 B(f_1,g)+\alpha_2 B(f_2,g). \tag{3.2}$$

We need to compute $\sigma(\alpha_1 f_1+\alpha_2 f_2+g),\sigma(\alpha_1 f_1+\alpha_2 f_2),\sigma(f_1+g)$ and $\sigma(f_2+g)$. We may use Propositions 3.3 and 3.4. Set $\tilde{f}_1 g+\tilde{g}f_1=c_1 1_V$, and $\tilde{f}_1 f_2+\tilde{f}_2 f_1=c_3 1_V$; then a simple computation shows:

$$\begin{aligned}\sigma(\alpha_1 f_1+\alpha_2 f_2+g)&=\alpha_1^2\sigma(f_1)+\alpha_2^2\sigma(f_2)+\sigma(g)+\alpha_2 c_2+\alpha_1 c_1+\alpha_1\alpha_2 c_3,\\ \sigma(\alpha_1 f_1+\alpha_2 f_2)&=\alpha_1^2\sigma(f_1)+\alpha_2^2\sigma(f_2)+\alpha_1\alpha_2 c_3,\\ \sigma(f_1+g)&=\sigma(f_1)+\sigma(g)+c_1,\\ \sigma(f_2+g)&=\sigma(f_2)+\sigma(g)+c_2.\end{aligned}$$

The verification of equation (3.2) is now complete after a routine further calculation. □

Thus (S,σ) is a quadratic space, and the associated bilinear space is (S,B_σ), where $B_\sigma\colon S\times S\mapsto\mathbb{Q}$ is given by

$$B_\sigma(f,g)=\left(\frac{1}{2}\right)(\sigma(f+g)-\sigma(f)-\sigma(g)).$$

Note that $\tilde{f}g+\tilde{g}f=2B_\sigma(f,g)1_V$ for any f,g in a linear subspace of $Sim(V)$.

From now on, whenever we speak of a subspace of $Sim(V)$, we shall assume it is a quadratic (or bilinear) space with the quadratic structure we have just described.

Example 3.5. This is a continuation of Example 3.2. *Let* $A_1,\ldots,A_\ell$ be a rational family of type $(s_1,\ldots,s_\ell)$ in order n. As we have already noted, $A_1,\ldots,A_\ell$ span a linear subspace of $Sim(V)$. We first observe that the subspace spanned by these matrices has dimension equal to ℓ. For suppose $\alpha_1 A_1+\cdots+\alpha_\ell A_\ell=0$, where $a_i\in\mathbb{Q}$. Then we claim:

The a_i are all equal to 0.

Proof. It will be enough to show $a_1=0$. The claim then follows by induction on ℓ.

Since

$$\alpha_1 A_1+\alpha_2 A_2+\cdots+\alpha_\ell A_\ell=0, \tag{3.3}$$

we may multiply (3.3) by $A_1^\top$, on the left, to obtain

$$\alpha_1 A_1^\top A_1 + \alpha_2 A_1^\top A_2 + \cdots + \alpha_\ell A_1^\top A_\ell = 0. \tag{3.4}$$

By definition of a rational family, this is equal to

$$\alpha_1 s_1 I_n - \alpha_2 A_2^\top A_1 - \cdots - \alpha_\ell A_\ell^\top A_1 = 0 \tag{3.5}$$

Now take the transpose of (3.2), and multiply the result on the right by A_1 to get

$$\alpha_1 s_1 I_n + \alpha_2 A_1^\top A_1 + \cdots + \alpha_\ell A_\ell^\top A_1 = 0 \tag{3.6}$$

Adding (3.5) and (3.6) gives $2\alpha_1 s_1 I_1 = 0$, and so $2\alpha_1 s_1 = 0$. But since $s_1 \neq 0$, we get $a_1 = 0$, as claimed. □

Now we have seen that this subspace of $Sim(V)$ has a quadratic structure. The A_i are a basis for this subspace, and since $A_i A_j^\top + A_j A_i^\top = 0\,(i \neq j)$ we have that the A_i are mutually orthogonal

$$(\tilde{f}g + \tilde{g}f = 2B_\sigma)(f,g)1_V, \text{ so } B_\sigma(A_i, A_j) = 0$$

Furthermore, the A_i have similarity factors s_i, and thus we see that the rational family gives rise to the quadratic space (S,q), where $q = \langle s_1, \ldots, s_\ell \rangle$, and S is the subspace of $Sim(V)$ spanned (independently) by $A_1, \ldots, A_\ell$. Note further that since the $s_i > 0$, this is a non-degenerate quadratic space and the only 0-similarity is the zero matrix.

Since 0-similarities are troublesome in the general theory, we shall from now on consider only linear subspaces S of $Sim(V)$ which are non-degenerate quadratic spaces and whose only 0-similarity is the zero matrix. As the example above shows, these are, in fact, the linear subspaces of $Sim(V)$ that we are most interested in. (For the more general discussion, see Shapiro [192]).

So now let (V,B) be a non-degenerate bilinear space and (S,B_σ) a non-degenerate subspace of $Sim(V)$ as specified above. How are these two spaces related? The next proposition is crucial to our understanding (S,B_σ).

Proposition 3.6. *Let (V,B) be a non-degenerate bilinear space of dimension n, and (S,B_σ) a non-degenerate subspace of $Sim(V)$. Then (S,B_σ) is similar to a subspace of (V,B).*

Proof. Pick $x \in V$ with $B(x,x) \neq 0$, and define $\phi : S \mapsto$ by $\phi(f) = f(x)$. Clearly ϕ is a linear transformation from S to V, and since S is a non-degenerate subspace of $Sim(V)$ in which the 0-map is the only 0-similarity, we have that the only non-invertible similarity in S is the 0-map. Thus ϕ is one-to-one. If we let $W = \{f(x) \,|\, f \in S\} \subseteq V$, then W is a subspace of V, and we want to show that ϕ is a similarity between (S,B_ϕ) and (W,B).

Choose a basis for V, and let A denote the matrix of B with respect to this basis. Let $f,g \in S$, and suppose they have matrices X and Y, respectively, with respect to the basis chosen for V. We have seen that $\tilde{f}g + \tilde{g}f = 2B_\sigma(f,g)1_V$, so in matrix terms we have:

$$A^{-1}X^\top AY + A^{-1}Y^\top AX = 2B_\sigma(f,g)I_n\,;$$

that is,

$$X^\top AY = 2B_\sigma(f,g)A - Y^\top AX\,.$$

Now let $x \in V$ be as above, and write $x = col(\alpha_1,\ldots,\alpha_n)$ (with respect to the chosen basis); then

$$x^\top(X^\top AY)x = 2B_\sigma(f,g)x^\top Ax - x^\top(Y^\top AX)x\,;$$

that is,

$$B(f(x),g(x)) = 2B_\sigma(f,g)q_B(x) - B(g(x),f(x))\,.$$

Since B is symmetric, we have $B(f(x),g(x)) = q_B(x)B_\sigma(f,g)$. This proves the proposition. □

We obtained a bit more out of the proof than is stated in the proposition. Not only do we have a similarity between the two spaces considered, we even have a nice form for the similarity factor. In particular, if there were an $x \in V$ such that $q_B(x) = 1$, we would have an isometry between (S,B_σ) and (W,B). This fact is important enough to isolate, but first a definition.

Definition 3.11. Let (V,B) be a bilinear space and (V,q_B) the associated quadratic space. Let D equal the range of q_B, $q_B\colon V \mapsto k$. We say that q_B *represents* $\alpha \in k$ if $\alpha \in D$.

This definition is a bit unorthodox since 0 always belongs to the range of q_B. It is more usual to say that q_B represents 0 if there is a $v \neq 0$ with $q_B(v) = 0$. This should cause no confusion, however, since if we say "q_B represents 0", we shall mean in the non-trivial sense.

Corollary 3.2. *Let (V,B) be a non-degenerate bilinear space and (S,B_σ) a non-degenerate subspace of $Sim(V)$. If q_B represents 1, then (S,B_σ) is isometric to a subspace of (V,B).*

Example 3.6. This is a continuation of Examples 3.4 and 3.5. In those examples, $q_B = \langle 1,1,\ldots,1\rangle$, and q_B, therefore, always represents 1. Thus the corollary above applies to the examples. We state that fact separately.

Proposition 3.7. *If there is a rational family of type $[s_1,\ldots,s_\ell]$ in order n, then there is a subspace $(S,\langle s_1,\ldots,s_\ell\rangle)$ of $Sim(V)$, and $(S\langle s_1,\ldots,s_\ell\rangle)$ is isometric to a subspace of $(V,\langle 1,\,1,\ldots,1\rangle)$.*

3.9 Relations Between Rational Families in the Same Order

In Proposition 2.8 we completely characterised rational families in odd orders and in orders $n \equiv 2 \pmod 4$. Thus our interest will be mainly in orders n such that $4 \mid n$.

In this case we can make a simplification of our problem which will be useful later.

Proposition 3.8. *Let $n \equiv 0 \pmod 4$. There is a rational family of type $[s_1, \ldots, s_\ell]$ in order n if and only if there is a rational family of type*

$$\left[1, \tfrac{s_2}{s_1}, \ldots, \tfrac{s_\ell}{s_1}\right]$$

in order n.

Proof. Let $A_1, \ldots, A_\ell$ be the rational family of type $[s_1, \ldots, s_\ell]$ in order n. It is easy to see that

$$\frac{1}{s_1} A_1^\top A_1, \frac{1}{s_1} A_1^\top A_2, \ldots, \frac{1}{s_1} A_1^\top A_\ell$$

is a rational family in order n of type

$$\left[1, \tfrac{s_2}{s_1}, \ldots, \tfrac{s_\ell}{s_1}\right]$$

Conversely, let $B_1, \ldots, B_\ell$ be the rational family in order n of type

$$\left[1, \tfrac{s_2}{s_1}, \ldots, \tfrac{s_\ell}{s_1}\right]$$

It is easy to see that if X is a rational matrix of order n and $XX^\top = s_1 I_n$, then $XB_1, XB_2, \ldots, XB_\ell$ is a rational family of type $[s_1, \ldots, s_\ell]$ in order n. So it suffices to construct such a matrix X.

By a theorem of Lagrange, every positive rational number is the sum of four squares of rational numbers; so let $s_1 = q_1^2 + q_2^2 + q_3^2 + q_4^2$. Consider the 4×4 matrix

$$M = \begin{bmatrix} q_1 & q_2 & q_3 & q_4 \\ -q_2 & q_1 & -q_4 & q_3 \\ -q_3 & q_4 & q_1 & -q_2 \\ -q_4 & -q_3 & q_2 & -q_1 \end{bmatrix}$$

then $MM^\top = s_1 I_4$. By hypothesis, $4 \mid n$, and so $n = 4u$. If we let $X = M \otimes I_u$, then X is a matrix of the desired type. This completes the proof of the proposition. □

With this proposition proved we see that the study of rational families in orders divisible by 4 is equivalent to the study of rational families of type $[1, \ldots]$.

But given a rational family in order n of type $[1, s_2, \ldots, s_\ell]$, there is certainly another rational family (maybe the one we already have) of the same order and type for which the first matrix is the identity matrix.

Thus we may always assume we are dealing with a rational family in which the first matrix is the identity.

3.10 Clifford Algebras

Let (V,q) be a quadratic space over the field k, and let A be a $k-algebra$ which contains V as a linear subspace. A is said to be *compatible* with q if whenever $x \in V, x^2 = q(x).1$.

Definition 3.12. An algebra $C \supset (V,q)$ which is compatible with q is called a *Clifford Algebra for* (V,q) if it has the following universal property: If $A \supset V$ is compatible with q, then there is a unique $k-algebra$ homomorphism $\phi\colon C \mapsto A$ such that $\phi(x) = x$ for all $x \in V$.

The usual nonsense for universal objects shows that if the Clifford Algebra exists, it is unique up to canonical isomorphism. Thus existence is the only problem.

Clifford Algebras always exist, and their algebra structure has been extensively studied. It would take us very far afield to go into these matters here. We shall just be content to list a few properties and to refer the reader to an excellent account of this subject in Lam [142].

Let (V,q) be a quadratic space over k where $\dim V < \infty$, and let $C(V)$ be its Clifford Algebra.

Theorem 3.10. *(1) $C(V)$ is a finite-dimensional algebra over k and is generated by V.*
(2) If $\dim_k V = n$, then $\dim_k C(V) = 2^n$.
(3) If $\dim_k V$ is odd, then $C(V)$ is a semi-simple algebra (that is, a direct sum of matrix rings over division rings containing k).
(4) If $\dim_k V$ is even, then $C(V)$ is a simple algebra with centre k (that is, a matrix ring over a division ring whose centre is k).
(5) All irreducible (left) modules (that is, no proper sub-modules) for a Clifford Algebra have the same dimension (over k) which is a power of 2.

Example 3.7. (i) Let V be a 1-dimensional vector space, and let $q = \langle a \rangle$. Then

$$C(V) \backsimeq \frac{k[x]}{(x^2 - a)}$$

(Note that if "a" is a square in k, then $C(V) \backsimeq k \times k$, and if "$a$" is not a square, $x^2 - a$ is irreducible in $k[x]$, and so $C(V)$ is a field which is a 2-dimensional vector space over k).

(ii) Let, $a,b \in k$, and consider the 4-dimensional algebra, denoted $\left(\frac{a,b}{k}\right)$, with basis $1,i,j,ij$ where $i^2 = a, j^2 = b, ij = -ji$.
This algebra is called a *quaternion algebra* ($a = b = -1, k = \mathbb{R}$ (reals) gives the usual quaternions). If V is 2-dimensional and $q = \langle a,b\rangle$, then $C(V) \backsimeq \left(\frac{a,b}{k}\right)$.

Now, by part (4) of theorem 3.10 above, $\left(\frac{a,b}{k}\right)$ is either a division ring with centre k or 2×2 matrices over k. We shall need to be able to distinguish these two general cases, and we state the relevant fact here.

Proposition 3.9. $\left(\frac{a,b}{k}\right)$ *is* ***not*** *a division ring if and only if there are* $x,y \in k$ *such that* $ax^2 + by^2 = 1$.

Notice that if $k = \mathbb{Q}_p$, $\left(\frac{a,b}{k}\right)$ is **not** a division ring if and only if $s_p(a,b) = 1$.

For a thorough discussion of quaternion algebras, including a proof of the fact that they are Clifford Algebras, we refer the reader again to Lam [142]. A proof of Wedderburn's theorem on semi-simple algebras (which we shall use implicitly) may be found, for example, in Scharlau [174].

3.11 Similarity Representations

Definition 3.13. Let (V,B) be a non-degenerate bilinear space over $\mathbb{Q}$ of dimension n, and let (V,q_B) be the associated quadratic space. We say that (V,q_B) (or (V,B)) is *positive definite* if $q_B(x) > 0$ for every $X \neq 0, x \in V$.

Clearly, if $q_B = \langle a_1,\ldots,a_n\rangle$, then (V,q_B) is positive definite if and only if $a_i > 0, i = 1,\ldots,n$; alternatively, the signature of $q_B = n$.

Note also that in our investigation of rational families, the only spaces we have seen are positive definite. Thus from now on, unless we specifically state otherwise, all quadratic spaces we consider will be positive definite over $\mathbb{Q}$.

Definition 3.14. Let (V,B) be an arbitrary bilinear space, and let $W \subset V$ be a subspace. The *orthogonal complement* of W, denoted $W^{\perp}$, is $\{x \in V \,|\, B(x,w) = 0 \text{ for all } w \in W\}$.

Warning! In general, the orthogonal complement of a subspace is no "complement" in the usual sense; it is quite possible, even in a non-degenerate bilinear space, for $W = W^{\perp}$.

For positive definite spaces, though, this cannot occur.

Proposition 3.10. *Let* (V,q) *be a positive definite space and* $W \subset V$ *a subspace. Then*

(i) $W \cap W^{\perp} = 0$;

(ii) $W + W^{\perp} = V$;
(iii) $(W, q\,|_W) \perp (W^{\perp}, q\,|_{W^{\perp}}) \backsimeq (V, q)$, *where all spaces are again positive definite.*

Now if (V, B) is a positive definite space and $f \in Sim(V, B)$ is not a 0-similarity, then $\sigma(f) > 0$. Thus any non-degenerate subspace of $Sim(V, B)$ is automatically positive definite. So let S be a non-degenerate linear subspace of $Sim(V, B)$, where (V, B) is positive definite, and let us suppose $1_V \in S$. (By Section 3.9, this is all we need consider for rational families.) We denote, as usual by σ the quadratic form on S, and let $S_1 \subset S$ be the orthogonal complement of 1_V in S.

Proposition 3.11. *The inclusion $S_1 \mapsto End(V)$ is compatible with the quadratic form $-\sigma$ on S_1.*

Proof. Now since $(S_1, \sigma\,|_{S_1})$ is a quadratic space, so is $(S_1, -\sigma)$. Let $f \in S_1$ then f is orthogonal to 1_V so $B_\sigma(f, 1_V) = 0$; that is, $f + \tilde{f} = 0$; that is, $f = -\tilde{f}$. Now $f\tilde{f} = \sigma(f).1_V$ in general, and so $f^2 = -\sigma(f).1_V$, proving the proposition. □

In view of this proposition and the universal property of Clifford Algebras, there is a unique $\mathbb{Q} - algebra$ homomorphism $\pi\colon C(S_1, -\sigma) \mapsto End(V)$. However, this is just another way of saying that V is a (left)-module for the algebra $C(S_1, -\sigma)$; that is, the algebra $C(S_1, -\sigma)$ is represented on the vector space V.

Proposition 3.12. *Let (V, B) and S_1 be as above, and let $W \subset V$ be a subspace which is also a sub-module of the $C(S_1, -\sigma)$-module V. Then $W^{\perp}$ is also a sub-module of V.*

Proof. Let $\Pi : C(S_1, -\sigma) \mapsto End(V)$ be as above. To say that W is a sub-module of V means that for every $z \in C(S_1, -\sigma)$, $\pi(z)\colon W \mapsto W$. In view of the fact that S_1 generates $C(S_1, -\sigma)$, this is equivalent to saying that $\pi(x)\colon W \mapsto W$ for all $x \in S_1$. Thus to show that $W^{\perp}$ is also a sub-module, it will be enough to show that

$$\pi(x)\colon W^{\perp} \mapsto W^{\perp} \text{ for all } 0 \neq x \in S_1\,;$$

that is,

$$B(\pi(x)(v), w) = 0 \text{ for every } w \in W, v \in W^{\perp}\,.$$

Now $x \in S_1$ implies $\widetilde{\pi(x)} = -\pi(x)$; thus $\widetilde{\pi(x)}\colon W \mapsto W$, and so $\widetilde{\pi(x)}(w) = w' \in W$. We thus have $B\left(v, \widetilde{\pi(x)}(w)\right) = B\,(v, w') = 0$. □

The importance of this proposition to our discussion is now evident: We started with (V, B) a positive definite space and (S, σ) a positive definite subspace of $Sim(V)$. We then showed that V could be considered a module

for the Clifford Algebra $C(S_1, -\sigma)$. Now if W is a sub-module of V, then the proposition showed that $W^\perp$ is also a sub-module for V. Thus, by Proposition 3.9, we can write $(V,B) = (W,B) \perp (W^\perp, B)$, and each summand is a module for $C(S_1, -\sigma)$, and both summands are again positive definite spaces.

We may continue this process, as long as any of the summands has a $C(S_1, -\sigma)$-sub-module. We conclude, then, that $(V,B) = (V_1,B) \perp \cdots \perp (V_r,B)$, where the (V_i,B) are each $C(S_\ell, -\sigma)$-modules which have no non-trivial $C(S_1, -\sigma)$- sub-modules; that is, the (V_i,B) are *irreducible* $C(S_1, -\sigma)$-modules.

It is easy to understand what we have done here: for, let $1_V, f_1, \ldots, f_k$ be a basis for S; these are a collection of endomorphisms of V. The subspaces V_i we have found are nothing more than subspaces of V that are invariant under all the f_i (any subspace is invariant under 1_V). We have used the fact that V is a positive definite space to show that the complement of an invariant subspace is again invariant. In matrix terms this amounts to being able to choose a basis for V in such a way that the f_i become block diagonal matrices. The fact that we can recognise these invariant subspaces of V as irreducible modules for a certain Clifford Algebra will be important because then we shall be able to discuss the sizes of these blocks, the irreducible modules for Clifford Algebras being so completely understood.

With this discussion and the notation above, the following proposition is evident.

Proposition 3.13. *(S, B_σ) is isometric to a linear subspace of $Sim(V_i, B)$.*

(1) *Notation.* If $(V_1 B_1)$ is isometric to a subspace of (V_2, B_2), we write $(V_1, B_1) < (V_2, B_2)$. The analogous notation will be used for quadratic spaces.
(2) Let $(V_1, B_1) < (V_2, B_2)$. We say that (V_1, B_1) *divides* (V_2, B_2) if $(V_2, B_2) = (V_1, B_1) \otimes (U, B)$ for some (U, B). In the quadratic case, when there can be no misunderstanding about the spaces being considered, we abusively write $q_1 \,|\, q_2$.

3.12 Some Facts About Positive Definite Forms Over $\mathbb{Q}$

We write $n\langle a\rangle$ for the quadratic form $\underbrace{\langle a, a, \ldots, a\rangle}_{\text{n-times}}$.

Proposition 3.14. *Let (V,q) be a positive definite quadratic space over $\mathbb{Q}$.*

(1) If $dim V \geq 4$, q represents every element of $\mathbb{Q}^+$ ($\mathbb{Q}^+$ equals positive rationals).
(2) If $q \simeq \langle 1, a, b, ab\rangle$, $a, b \in \mathbb{Q}^+$ then for every $x \in \mathbb{Q}^+$, $xq = \langle x, xa, xb, xab\rangle \simeq \langle 1, a, b, ab\rangle$.
(3) If $4 \,|\, n$ and $q \simeq n\langle 1\rangle$, then $xq \simeq q$, for all $x \in \mathbb{Q}^+$.

(4) For any $a,b,x,y \in \mathbb{Q}^+$, $\langle 1,a,b,ab\rangle \otimes \langle x,y\rangle \simeq 8\langle 1\rangle$

Proof. (1) This generalises the theorem of Lagrange that $\langle 1,1,1,1\rangle$ represents every element of $\mathbb{Q}^+$ and can be found in Serre [189].

(2), (3), and (4) all follow from the Hasse-Minkowski Theorem 3.7. □

Corollary 3.3. *Let* $(S,\sigma) < Sim(V,q)$*, where* q *is positive definite and* $dimS = dimV = 4$*. Then* $(S,\sigma) \simeq (V,q)$*.*

Proof. By Proposition 3.13(1) above, q represents 1. Thus, by Corollary 3.2, (S,σ) is isometric to a subspace of (V,q). But, since $dimS = dimV$, that subspace must be all of (V,q). □

The next proposition is a special case of something true over general fields (see Shapiro [192]). However, over $\mathbb{Q}$, an *ad hoc* proof can be given.

Proposition 3.15. *Let* $n = 2^m t$*,* t *odd,* $a,b \in \mathbb{Q}^+$*. Then*

(i) $n\langle 1\rangle \simeq n\langle a\rangle \Leftrightarrow 2^m\langle 1\rangle \simeq 2^m\langle a\rangle$,
(ii) $\langle 1,a\rangle \mid n\langle 1\rangle \Leftrightarrow \langle 1,a\rangle \mid 2^m\langle 1\rangle$,
(iii) $\langle 1,a,b,ab\rangle \mid n\langle 1\rangle \Leftrightarrow \langle 1,a,b,ab\rangle \mid 2^m\langle 1\rangle$.

Proof. (i) If $m \geq 2$, then all isometries are true by (3) of Proposition 3.13. So we need only consider $m = 0,1$.

$$m = 0\colon\ t\langle 1\rangle \simeq t\langle a\rangle \Leftrightarrow \langle 1\rangle \simeq \langle a\rangle\,.$$

If: Obvious.
Only If: The isometry implies both have the same discriminant; that is, a^t is a square in $\mathbb{Q}$. But t odd implies $a = q^2$ for some $q \in \mathbb{Q}$. □

$$m = 1\colon\ 2t\langle 1\rangle \simeq 2t\langle a\rangle \Leftrightarrow 2\langle 1\rangle \simeq \langle a\rangle\,.$$

Proof. If: Obvious.
Only If: In this case we must have $s_p(2t\langle a\rangle) = 1$ for every prime p. But $s_p(2t\langle a\rangle) = ((a,a)_p)^x$, where

$$x = \sum_{j=1}^{2t-1} j = \frac{(2t-1)(2t)}{2} = t(2t-1)$$

which is odd since t is odd. Thus $((a,a)_p)^x = (a,a)_p = 1$ for every prime p. This is enough to prove that $\langle 1,1\rangle \simeq \langle a,a\rangle$, since the signatures and discriminants are obviously the same. □

(ii) We first note that $\langle 1,a\rangle \mid n\langle 1\rangle$ always if $m \geq 3$, since $8\langle 1\rangle \simeq \langle 1,a\rangle \otimes \langle 1,b\rangle \otimes \langle x,y\rangle$ for any $a,b,x,y \in \mathbb{Q}^+$ by (4) of Proposition 3.13. Also $\langle 1,a\rangle \mid n\langle 1\rangle$ implies that $m \geq 1$. So we need only consider $m = 1$, $m = 2$.

$$m = 1\colon\ \langle 1,a\rangle \mid 2t\langle 1\rangle \Leftrightarrow \langle 1,a\rangle \mid 2\langle 1\rangle\,.$$

Proof. If: Obvious.
Only If: The discriminant of $\langle 1,a\rangle \otimes \alpha$ is $a^t = 1$. Since t is odd, "a" is a square, and so $\langle 1,a\rangle \simeq \langle 1,1\rangle$. □

$$m = 2\colon \langle 1,a\rangle \mid 4t\langle 1\rangle \Leftrightarrow \langle 1,a\rangle \mid 4\langle 1\rangle .$$

Proof. If: Obvious.
Only If: $\langle 1,a\rangle \mid 4t\langle 1\rangle$ implies $\langle 1,a\rangle \otimes \langle \alpha_1,\ldots,\alpha_{2t}\rangle = 4t\langle 1\rangle$. If $t > 1$, we have, by repeated application of Proposition 3.14 part (i), that

$$\langle \alpha_1,\ldots,\alpha_{2t}\rangle \simeq \langle 1,1,\ldots,1,u,v,w\rangle = \alpha .$$

Comparing Hasse-Invariants, we find $(a,uvwa)_p(-1,uvw)_p = 1$ for every prime p. Let $d = uvw$. Then $d = disc\alpha$, and we have that $(a,da)_p(-1,d)_p = 1$ for every prime p. But this is enough to guarantee that $\langle 1,a\rangle \otimes \langle 1,d\rangle \simeq 4\langle 1\rangle$. □

(iii) Notice that by (4) of Proposition 3.13 we have $\langle 1,a,b,ab\rangle \mid n\langle 1\rangle$ always, if $m \geq 3$. Also $\langle 1,a,b,ab\rangle \mid n\langle 1\rangle$ implies $m \geq 2$. So we need only consider the case $m = 2$; that is, $\langle 1,a,b,ab\rangle \mid 4t\langle 1\rangle \Leftrightarrow \langle 1,a,b,ab\rangle \mid 4\langle 1\rangle$.

Proof. If: Obvious.
Only If: Suppose $\langle 1,a,b,ab\rangle \otimes \langle \alpha_1 \ldots \alpha_t\rangle = 4t\langle 1\rangle$, where t is odd, $t > 1$. By (4) of Proposition 3.13 and the Witt Cancellation Theorem 2.1, we obtain $\langle 1,a,b,ab\rangle \otimes \langle \alpha\rangle \simeq 4\langle 1\rangle$, which completes the proof. □

Proposition 3.16. *Let $(S,\sigma) < Sim(V,q)$ where $dimV = n, q$ is positive definite and $dimS \geq 5$. Then $8 \mid n$.*

Proof. We already know that if $q = n\langle 1\rangle$, then $8 \mid n$ by the Radon-Hurwitz Theorem.

Since $dimS \geq 5$, we know, by Proposition 3.13 part (1), that σ represents 1; that is, there is a similarity in S with similarity factor equal to 1, which we call f. It is an easy exercise to show that $(\tilde{f} \circ S,\sigma)$ is another subspace of $Sim(V,q)$ which is isometric to (S,σ) and that $\tilde{f} \circ S$ contains 1_V, So with no loss of generality we may assume $1_V \in S$.

Let $(T,\tau) < (S,\sigma)$, where $dimT = 5$ and $1_V \in T$, and let τ_1 be the form on the orthogonal complement of 1_V in T. Then, as we have seen, $C(V,-\tau_1)$ is represented on V. By Theorem 3.10 we know that $C(V,-\tau_1)$ is a simple algebra with centre equal to $\mathbb{Q}$ and of dimension 16 over $\mathbb{Q}$. By Wedderburn's theorem $C = C(V,-\tau_1)$ is either

(a) a 16-dimensional division ring with center equal to $\mathbb{Q}$,
(b) 2×2 matrices over K, where K is a division ring, centre $(K) = \mathbb{Q}$ and $[K\colon \mathbb{Q}] = 4$,
(c) 4×4 matrices over $\mathbb{Q}$.

Now, in each case we know precisely the dimensions of the irreducible modules; in cases (a) and (b) we know that every irreducible module has dimension divisible by 8, so if C is either (a) or (b), we shall have that $8 \mid n$.

It remains only to show that (c) cannot occur. In case (c) *every* irreducible module has dimension 4 over $\mathbb{Q}$. So if $(W,\tilde{q})$ is an irreducible sub-module of (V,q), we have, by Proposition 3.12, that (T,τ) is isometric to a linear subspace of $Sim(W,\tilde{q})$. But, since $dimW = 4$ and $\tilde{q}$ is positive definite, we have, by Proposition 3.13 part (1), that q represents 1 and so, by Corollary 3.3, that (T,τ) is isometric to a subspace of $(W,\tilde{q})$. But $dimT = 5 > dimW = 4$, which is a contradiction. Thus we have that $8\,|\,n$. □

3.13 Reduction of Algebraic Problem of Orthogonal Designs to Orders a Power of 2

As already seen, the existence of a rational family of type $[1,s_2,\ldots,s_\ell]$ in order n is equivalent to the existence of a linear sub-space (S,σ) of $Sim(\mathbb{Q}^n, n\langle 1\rangle)$ where $1_{\mathbb{Q}^n} \in S$ and $\sigma = \langle 1,s_2,\ldots,s_\ell\rangle$.

Proposition 3.17. *Let (S,σ) be a positive definite quadratic space. Then $(S,\sigma) < Sim(\mathbb{Q}^4, 4\langle 1\rangle) \Leftrightarrow (S,\sigma) < (\mathbb{Q}^4, 4\langle 1\rangle)$.*

Proof. Only If: Since $4\langle 1\rangle$ represents 1, obviously we are done by Corollary 3.2.

If: Since $(S,\sigma) < (\mathbb{Q}^4, 4\langle 1\rangle)$, we know $\dim S \le 4$. So we have to consider separately the cases $\dim S = 1,2,3,4$. They are all proved in the same way, so we shall just exhibit the proof for $s = 2$. Let $\sigma = \langle a,b\rangle$. Then we can find u,v such that $\langle a,b,u,v\rangle \simeq \langle 1,1,1,1\rangle$. In matrix terms, there is a 4×4 matrix P with $PP^\top = diag(a,b,u,v)$. Now, by Proposition 1.2, there is an integer Radon-Hurwitz family of order 4. Call the matrices in that family A_1,A_2,A_3,A_4. If $P = (p_{ij})$, let

$$X_1 = \sum_{j=1}^{4} p_{1j}A_j\,, \qquad X_2 = \sum_{j=1}^{4} p_{2j}A_j\,.$$

It is easy to check that X_1, X_2 form a rational family of type $[a,b]$ in order 4 and thus span the appropriate linear subspace of $Sim(\mathbb{Q}^4, 4\langle 1\rangle)$. □

Proposition 3.18. *Let (S,σ) be a positive definite quadratic space.*

(i) $(S,\sigma) < Sim\left(\mathbb{Q}^8, 8\langle 1\rangle\right) \Leftrightarrow (S,\sigma) < \left(\mathbb{Q}^8, 8\langle 1\rangle\right)$.
(ii) $(S,\sigma) < Sim\left(\mathbb{Q}^2, 2\langle 1\rangle\right) \Leftrightarrow (S,\sigma) < \left(\mathbb{Q}^2, 2\langle 1\rangle\right)$.

Proof. Exactly like Proposition 3.17, using the existence of Radon-Hurwitz family of eight integer matrices of order 8 (or for (ii) the same fact for order 2). □

Proposition 3.19. *Let $a,b > 0$, and let q be positive definite.*

(i) $(S,\langle 1,a\rangle) < Sim(V,q) \Rightarrow \langle 1,a\rangle\,|\,q$.

(ii) $(S, \langle 1, a, b\rangle) < Sim(V, q) \Leftrightarrow (S', \langle 1, a, b, ab\rangle) < Sim(V, q)$.
(iii) $(S, \langle 1, a, b\rangle) < Sim(V, q) \Rightarrow \langle 1, a, b, ab\rangle \,|\, q$.

Proof. (i) Since $(S, \langle 1, a\rangle) < Sim(V, q)$, we have a representation of $C(S_1, \langle -a\rangle)$ on V. Now, we noted that $C(S_1, \langle -a\rangle) \simeq \frac{\mathbb{Q}[x]}{x^2+a}$. Since $x^2 + a$ is irreducible in $\mathbb{Q}[x]$, $\frac{\mathbb{Q}[x]}{x^2+a} = K$, a field, and $\dim_{\mathbb{Q}} K = 2$. Now, an irreducible K-module is a 1-dimensional K vector space. So $(V, q) \simeq (V_1, q_1) \perp \ldots \perp (V_\top, q_\top)$, where the V_i are 1-dimensional over K; that is, 2-dimensional over $\mathbb{Q}$. By Propositions 3.13 and 3.6 we conclude that $(S, \langle 1, a\rangle)$ is similar to a subspace of (V_i, q_i). Since both S and V_i are 2-dimensional, we must have $q_i = \alpha_i\langle 1, a\rangle$. Hence $q = \langle 1, a\rangle \otimes \langle \alpha_1, \ldots, \alpha_\top\rangle$, as was to be shown. □

Proof. (ii) If: Obvious.

Only If: There is no loss in assuming that $1_V \in S, f_1, f_2 \in S, \sigma(f_1) = a$, $\sigma(f_2) = b$ and $B_\sigma(f_1, f_2) = 0 = B_\sigma(1_V, f_1) = B_\sigma(1_V, f_2)$. It is an easy matter, then, to check that $1_V, f_1, f_2, f_1 f_2$ span a space, S', and that they are orthogonal (under B_σ) and that $\sigma(f_1 f_2) = ab$. □

Proof. (iii) Now $(S, \langle 1, a, b\rangle) < Sim(V, q)$ implies that V is a module for $C = C(S_1, \langle -a, -b\rangle)$. By Proposition 3.9 we have that C is a division ring which is 4-dimensional over $\mathbb{Q}$. Now an irreducible module for a division ring is always 1-dimensional, hence 4-dimensional over $\mathbb{Q}$. Thus

$$(V, q) = (V_1, q_1) \perp \cdots \perp (V_t, q_t),$$

where each V_i is 4-dimensional over $\mathbb{Q}$. Now, by Proposition 3.13 again, we have that $(S, \langle 1, a, b\rangle) < Sim(V_i, q_i), 1 \le i \le t$. Now, by (ii) of this proposition, we obtain $(S', \langle 1, a, b, ab\rangle) < Sim(V_i, q_i)$. Now use Proposition 3.14 part (1) to note that q_i represents 1, and so, by Corollary 3.2, we have that $(S', \langle 1, a, b, ab\rangle) < (V_i, q_i)$. But since $\dim_{\mathbb{Q}} S' = \dim V_i$ we have $q_i \simeq \langle 1, a, b, ab\rangle$. Thus $q \simeq \underbrace{\langle 1, \ldots, 1\rangle}_{\text{t-times}} \otimes \langle 1, a, b, ab\rangle$. □

We have obtained a bit more out of the proof of (iii). Notice that if t is even, we may invoke Proposition 3.13 to assert that $q \simeq 4t\langle 1\rangle$. With this remark in mind we may improve Proposition 3.16.

Proposition 3.20. *Let* $(S, \sigma) < Sim(V, q)$ *where* $\dim V = n$, q *is positive definite and* $\dim S \ge 5$. *Then* $8 \,|\, n$ *and* $q \simeq n\langle 1\rangle$.

Proof. The interesting fact here is that we have forced q to be $n\langle 1\rangle$. No other positive definite form has a 5-dimensional space of similarities.

We have already proved $8 \,|\, n$, and, in the proof of Proposition 3.16, we have seen that $(U, \langle 1, a, b\rangle) < Sim(V, q)$. The remark before this Proposition finishes the proof, since if $8 \,|\, n$, t must be even. □

Theorem 3.11 (Shapiro [191]). *Let $n = 2^m t$ where t is odd, and let (S,σ) be a positive definite quadratic space where σ represents 1. Then*

$$(S,\sigma) < Sim(\mathbb{Q}^n, n\langle 1\rangle) \Leftrightarrow (S,\sigma) < Sim\left(\mathbb{Q}^{2^m}, 2^m\langle 1\rangle\right).$$

Proof. First note that in Proposition 2.8 we proved this for $m = 0, 1$. So we may assume $m \geq 2$. The fact that we are interested in rational families and the discussion in Section 3.9 shows that our assumption that σ represents 1 is no drawback. Note also that "If" is obvious, since, in matrix terms, we can just tensor with I_t.

$m = 2$: We need only consider $\dim S = 2$, 3 and 4.

Case 1. $\sigma = \langle 1, a\rangle$. By Proposition 3.19 part (i), we have that $\langle 1, a\rangle \,|\, n\langle 1\rangle$ and hence, by Proposition 3.15, $\langle 1, a\rangle \,|\, 4\langle 1\rangle$; that is, $(S, \langle 1, a\rangle) < (\mathbb{Q}^4, 4\langle 1\rangle)$. Now use Proposition 3.17 to assert $(S, \langle 1, a\rangle) < Sim(\mathbb{Q}^4, 4\langle 1\rangle)$.

Case 2. $\sigma = \langle 1, a, b\rangle$. The route is pretty much the same as in Case 1. By Proposition 3.19 part (iii), we have $\langle 1, a, b, ab\rangle \,|\, n\langle 1\rangle$ and hence, by Proposition 3.15, $\langle 1, a, b, ab\rangle \,|\, 4\langle 1\rangle$. Hence $(S, \langle 1, a, b\rangle) < (\mathbb{Q}^4, 4\langle 1\rangle)$. Now use Proposition 3.17 to get $(S, \langle 1, a, b\rangle) < Sim(\mathbb{Q}^4, 4\langle 1\rangle)$.

Case 3. $\sigma = \langle 1, a, b, c\rangle$. We postpone this case for a moment.

$m \geq 3$, $\dim \sigma = 2$. Let $\sigma = \langle 1, a\rangle$. Now $\langle 1, a\rangle \,|\, 8\langle 1\rangle$ for any "a" by Proposition 3.14 part (4). Thus $(S,\sigma) < (\mathbb{Q}^8, 8\langle 1\rangle)$. Now use Proposition 3.18 to get $(S,\sigma) < (\mathbb{Q}^8, 8\langle 1\rangle)$. But clearly, then $(S,\sigma) < Sim(\mathbb{Q}^{2^m}, 2^m\langle 1\rangle)$ for any $m \geq 3$.

$m \geq 3$, $\dim \sigma = 3$. Let $\sigma = \langle 1, a, b\rangle$. Again using Proposition 3.14 part(4), we have $\langle 1, a, b, ab\rangle \,|\, 8\langle 1\rangle$ and so $(S, \langle 1, a, b\rangle) < (\mathbb{Q}^8, 8\langle 1\rangle)$. By Proposition 3.18 we get $(S, \langle 1, a, b\rangle) < Sim(\mathbb{Q}^8, 8\langle 1\rangle)$ and thus isometric to a linear subspace of $Sim(\mathbb{Q}^{2^m}, 2^m\langle 1\rangle)$ for any $m \geq 3$. We are left with considering the case where $\dim \sigma \geq 4$.

$\dim \sigma \geq 5$. Let $(S,\sigma) < Sim(\mathbb{Q}^{2^{m_t}}, 2^{m_t}\langle 1\rangle) = Sim(V, q)$. The usual Clifford Algebra techniques give $(V, q) \simeq (V_1, q_1) \perp \cdots \perp (V_\ell, q_\ell)$. By Proposition 3.20 we know $8 \,|\, \dim V_i$ and $q_i = n_i\langle 1\rangle$, $n_i = \dim V_i$. Since the dimension (over $\mathbb{Q}$) of an irreducible module for a Clifford Algebra is always a power of 2 (Theorem 3.10), we know that $n_i = 2^s$, $s \geq 3$. Since $2^s \ell = \sum_{i=1}^{\ell} n_i = 2^m t$, we have $s \leq m$. We now invoke Propositions 3.13 and 3.20 to finish.

We are left only with the case $\dim \sigma = 4$.

We proceed as in the case for $\dim \sigma \geq 5$, and, using the notation there, we get $(S,\sigma) < Sim(V_i, q_i)$ where $\dim V_i = 2^s$ and $s \leq m$.

Case 1. $s \geq 3$. Let $\sigma = \langle 1, a, b, c\rangle$. We may proceed exactly as in the case $m \geq 3$, $\dim \sigma = 3$, to conclude that $q_i = 2^s\langle 1\rangle$, in which case we are done.

Case 2. $s = 2$, $\sigma = \langle 1, a, b, c\rangle$. Now we get $(S', \langle 1, a, b\rangle) < Sim(V_i, q_i)$, but Proposition 3.19 part (ii) implies $(T, \langle 1, a, b, ab\rangle) < Sim(V_i, q_i)$. By Proposition 3.14 part (1), q_i represents 1, so $(T, \langle 1, a, b, ab\rangle) < (V_i, q_i)$. Since $\dim V_i =$

$\dim T = 4$, we have $q_i \simeq \langle 1, a, b, ab\rangle$. But, for exactly the same reasons, we have $q_i \simeq \sigma$; that is, $\sigma = \langle 1, a, b, ab\rangle$.

Thus we are reduced to considering the case $\dim \sigma = 4$ and $\sigma = \langle 1, a, b, ab\rangle$. But now, by Proposition 3.19, we have

$$\big(S', \langle 1, a, b, ab\rangle\big) < Sim\,(\mathbb{Q}^n, n\langle 1\rangle) \Leftrightarrow (S, \langle 1, a, b\rangle) < Sim\,(\mathbb{Q}^n, n\langle 1\rangle)\,,$$

reducing us to the case where $\dim \sigma = 3$, which we have already handled. □

Corollary 3.4. *There is a rational family in order $n = 2^m t$, t odd, of type $[s_1, \ldots, s_\ell]$ if and only if there is a rational family of the same type in order 2^m.*

3.14 Solution of the Algebraic Problem of Orthogonal Designs in orders $4t$, $8t$ (t odd)

In this section we propose to classify the rational families that exist in orders $4t$ and $8t$ (t odd). By Theorem 3.11, this amounts to a classification of the rational families that can exist in orders 4 and 8.

3.14.1 Order 4

Since $p(4) = 4$, we have, by the results of Section 3.9, only to consider the conditions which allow there to exist rational families of types $[1, s_1]$, $[1, s_1, s_2]$ and $[1, s_1, s_2, s_3]$ in order 4.

Case 1: $[1, s_1]$.

Proposition 3.21 (Geramita-Seberry Wallis [81]). *A necessary and sufficient condition that there be a rational family of type $[1, s_1]$ in order 4 is that s_1 be a sum of three squares in $\mathbb{Q}$.*

Proof. To show the necessity, observe that by the results of Section 3.9 we may assume the rational family is $\{I_4, A\}$, where $A = -A^\top$ and $AA^\top = s_1 I$. The fact that A is skew-symmetric forces its diagonal entries to all be zero, and hence, evidently, s_1 is a sum of three rational squares.

For the sufficiency, let $s_1 = q_1^2 + q_2^2 + q_3^2$ where $q_i \in \mathbb{Q}$. If

$$A = \begin{bmatrix} 0 & q_1 & q_2 & q_3 \\ -q_1 & 0 & -q_3 & q_2 \\ -q_2 & q_3 & 0 & -q_1 \\ -q_3 & -q_2 & q_1 & 0 \end{bmatrix},$$

then it is easily checked that $\{I_4, A\}$ is a rational family of type $[1, s_1]$. □

Corollary 3.5. *A necessary and sufficient condition that there be a rational family of type* $[s_1, s_2]$ *in order 4 is that* $\frac{s_1}{s_2}$ *be a sum of three squares in* $\mathbb{Q}$.

Proof. See Section 3.9. □

Note that $\frac{m}{n} = \frac{mn}{n^2} = (\frac{1}{n})^2(mn)$, and so $\frac{m}{n}$ is a sum of three rational squares if and only if mn is a sum of three rational squares. Now it is well known (see, for example, Serre [189]) that a positive integer is the sum of three rational squares if and only if it is the sum of three integer squares if and only if (Gauss) it is *not* of the form $4^a(8b+7)$.

Thus, for example, there is no rational family of type $[k, 7k]$ or $[3s, 5s]$ in order 4.

Case 2: $[1, s_1, s_2]$.

We will not have to treat this case separately, as the following proposition shows.

Proposition 3.22. *There is a rational family of type* $[1, s_1, s_2]$ *in order 4 if and only if there is a rational family of type* $[1, s_1, s_2, s_1s_2]$ *in order 4.*

Proof. If: Obvious.

Only If: By Section 3.9 there is no loss in assuming the rational family is $\{I_4, A, B\}$. It is a routine verification that $\{I_4, A, B, AB\}$ is a rational family of type $[1, s_1, s_2, s_1s_2]$. □

Case 3: $[1, s_1, s_2, s_3]$.

This situation is completely settled by:

Proposition 3.23. *There is a rational family of type* $[1, s_1, s_2, s_3]$ *in order 4 if and only if* $\langle 1, s_1, s_2, s_3\rangle \simeq \langle 1, 1, 1, 1\rangle$ *over* $\mathbb{Q}$.

Proof. By Proposition 3.17 we see that there is a rational family of type $[1, s_1, s_2, s_3]$ in order 4 if and only if $\langle 1, s_1, s_2, s_3\rangle < 4\langle 1\rangle$. (Note the abusive notation). Since both forms have dimension four, this is true if and only if $\langle 1, s_1, s_2, s_3\rangle \simeq 4\langle 1\rangle$ over $\mathbb{Q}$. □

Corollary 3.6. *There is a rational family of type* $[1, s_1, s_2]$ *in order 4 if and only if* $\langle 1, s_1, s_2, s_1s_2\rangle \simeq 4\langle 1\rangle$.

It is now clear how the Hasse-Minkowski classification of quadratic forms comes into play. The algorithmic nature of the criteria for congruence over $\mathbb{Q}$ makes it extremely amenable to machine analysis, in specific orders. (The print-outs in the appendices verify this.)

We now list a few corollaries which had been obtained by quite different methods in Geramita-Seberry Wallis [81].

Corollary 3.7. *Let* $a, b \in \mathbb{Q}^+$. *There is a rational family of type* $[a, a, a, b]$ *in order 4 if and only if* $\frac{b}{a}$ *is a square in* $\mathbb{Q}$.

Proof. By Section 3.9 such a rational family exists if and only if a rational family of type $[1,1,1,\frac{b}{a}]$ exists in order 4. By Proposition 3.22 this occurs if and only if $\langle 1,1,1,\frac{b}{a}\rangle \simeq 4\langle 1\rangle$ over $\mathbb{Q}$. By Witt Cancellation, this occurs if and only if $\langle \frac{b}{a}\rangle \simeq \langle 1\rangle$, that is, if and only if $\frac{b}{a}$ is a square in $\mathbb{Q}$. □

Corollary 3.8. *Let $a,b \in \mathbb{Q}^+$. There is a rational family of type $[a,a,b]$ in order 4 if and only if $\frac{b}{a}$ is a sum of two squares in $\mathbb{Q}$.*

Proof. As in the previous corollary, such a rational family exists if and only if there is a rational family of type $[1,1,\frac{b}{a}]$ in order 4. By Corollary 3.6, this exists if and only if $\langle 1,1,\frac{b}{a},\frac{b}{a}\rangle \simeq 4\langle 1\rangle$. By the Witt Cancellation Theorem this is true if and only if $\langle \frac{b}{a},\frac{b}{a}\rangle \simeq \langle 1,1\rangle$.

Now two isometric forms represent the same elements of $\mathbb{Q}^*$, and so $\frac{b}{a}$ is represented by $\langle 1,1\rangle$; hence $\frac{b}{a}$ is a sum of two squares.

On the other hand, if $\frac{b}{a}$ is a sum of two squares in $\mathbb{Q}$, then $\frac{b}{a}$ is represented by $\langle 1,1\rangle$, and so $\langle 1,1\rangle \simeq \langle \frac{b}{a},x\rangle$ for some $x \in \mathbb{Q}^+$. Thus if we compare discriminants, we see that $(\frac{b}{a})x = u^2$, $u \in \mathbb{Q}$; that is, $x = (\frac{b}{a})v^2$, $v \in \mathbb{Q}$, and so $\langle \frac{b}{a},x\rangle \simeq \langle \frac{b}{a},\frac{b}{a}\rangle$, as was to be shown. □

There is another way to see that $\langle \frac{b}{a},\frac{b}{a}\rangle \simeq \langle 1,1\rangle$ if and only if $\frac{b}{a}$ is a sum of two squares in $\mathbb{Q}$.

First note that $\langle \frac{b}{a},\frac{b}{a}\rangle \simeq \langle (\frac{b}{a})a^2,(\frac{b}{a})a^2\rangle \simeq \langle ab,ab\rangle$.

Since the signatures and discriminants of the forms $\langle ab,ab\rangle$ and $\langle 1,1\rangle$ are the same, the two forms are congruent if and only if $s_p(\langle ab,ab\rangle) = 1$ for all primes p.

Now $(ab,ab)_p = (-1,ab)_p$. Write

$$ab = 2^{\alpha}p_1^{\alpha_1}\dots p_s^{\alpha_s}\,q_1^{\beta_1}\dots q_t^{\beta_t},$$

p_i, q_j primes, and where the $p_i \equiv 1 \pmod 4$ and the $q_j \equiv 3 \pmod 4$. Now, since -1 is a square modulo p only for $p = 2$ and $p \equiv 1 \pmod 4$, we see that the α_i may be even or odd. Since -1 is *not* a square modulo q if $q \equiv 3 \pmod 4$, we shall have $(-1,ab)_{q_j} = -1$ for $q_j \mid ab$, $q_j \equiv 3 \pmod 4$ unless β_j is even. But this, then, is precisely the condition that ensures that ab is a sum of two squares (Fermat).

3.14.2 Order 8

We know that $\rho(8) = 8$, so we must consider rational families having at most 8 members. The key result we need here is Proposition 3.17, which asserts that there is a rational family of type $[1,s_1,\dots,s_\ell]$ $(1 \le \ell \le 7)$ in order 8 if and only if $\langle 1,s_1,\dots,s_\ell\rangle = \sigma < 8\langle 1\rangle$.

Case 1. Much of the work is covered by the following:

Proposition 3.24. *For any $s_1s_2, s_3, s_4 \in \mathbb{Q}^+$ there is a rational family of type $[1, s_1s_2, s_3, s_4]$ in order 8.*

Proof. We need to show that:

$$\langle 1, s_1s_2, s_3, s_4\rangle = \sigma < 8\langle 1\rangle\,.$$

By Proposition 3.14 part (4),

$$\langle 1, s_1, s_2, s_1s_2\rangle \otimes \langle 1, s_3\rangle \simeq 8\langle 1\rangle\,;$$

that is,

$$\tau = \langle 1, s_1, s_2, s_1s_2, s_3, s_1s_3, s_2s_3, s_1s_2s_3\rangle \simeq 8\langle 1\rangle\,.$$

But

$$\tau = \langle 1, s_1, s_2, s_3\rangle \perp \langle s_1s_2, s_1s_3, s_2s_3, s_1s_2s_3\rangle = \langle 1, s_1, s_2, s_3\rangle \perp q\,.$$

Now q is positive definite of dimension 4, and so, by Proposition 3.14 part (1) q represents s_4. Thus $q \simeq \langle s_4, u, v, w\rangle$ for some $u, v, w \in \mathbb{Q}^+$. Thus $8\langle 1\rangle \simeq \langle 1, s_1, s_2, s_3, s_4\rangle \perp \langle u, v, w\rangle$. □

Case 2. $[1, s_1, s_2, s_3, s_4, s_5, s_6]$.

We need not consider this case separately from the case of 8-members, as the following proposition shows.

Proposition 3.25. *Let $s_i \in \mathbb{Q}^+$, $1 \le i \le 6$. There is a rational family of type $[1, s_{1,\ldots}, s_6]$ in order 8 if and only if there is a rational family of type*

$$\left[1, s_{1,\ldots}, s_6, \prod_{i=1}^{6} s_i\right]$$

in order 8.

Proof. If: Obvious.

Only If: As always, we may assume the rational family is $\{I_8, A_1, \ldots, A_6\}$ It is routine to check that

$$\left\{I_8, A_1, \ldots, A_6, \prod_{i=1}^{6} A_i\right\}$$

is the required rational family. □

Case 3. $[1, s_1, s_2, s_3, s_4, s_5, s_6, s_7]$.

Proposition 3.26. *Let $s_i \in \mathbb{Q}^+, 1 \le i \le 7$. There is a rational family of type $[1, s_1, \ldots, s_7]$ in order 8 if and only if $\langle 1, s_1, \ldots, s_7\rangle \simeq 8\langle 1\rangle$ over $\mathbb{Q}$.*

Proof. Exactly as in Proposition 3.23. □

Corollary 3.9. *Let $s_i \in \mathbb{Q}^+, 1 \le i \le 6$. There is a rational family of type $[1, s_1, \ldots, s_6]$ in order 8 if and only if*

$$\left\langle 1, s_1, \ldots, s_6, \prod_{i=1}^{6} s_i \right\rangle \simeq 8\langle 1\rangle$$

over $\mathbb{Q}$.

Proof. Exactly as in Corollary 3.6. □

We can further deduce, as in Corollaries 3.7 and 3.8,

Corollary 3.10. *There is a rational family of type*

(i) $[a,a,a,a,a,a,a,b]$ in order 8, $(a,b \in \mathbb{Q}^+)$ if and only if $\frac{b}{a} \in (\mathbb{Q}^*)^2$;
(ii) $[a,a,a,a,a,a,b]$ in order 8, $(a,b \in \mathbb{Q}^+)$ if and only if $\frac{b}{a}$ is a sum of two squares in $\mathbb{Q}$.

Case 4. $[1, s_1, s_2, s_3, s_4, s_5]$.

As we have noted before, this amounts to deciding when $\langle 1, s_1, \ldots, s_5\rangle = \sigma < 8\langle 1\rangle$.

Proposition 3.27. *If $\sigma = \langle 1, s_1, \ldots, s_5\rangle, s_i \in \mathbb{Q}^+$ and d equals the discriminant of σ, $\sigma < 8\langle 1\rangle$ if and only if there is a $u \in \mathbb{Q}^+$ such that $s_p(\sigma) = (-1,d)_p(-1,u)_p(u,d)_p$ for every prime p.*

Proof. $\sigma < 8\langle 1\rangle$ if and only if there are $u, v \in \mathbb{Q}^+$ with $\sigma \perp \langle u, v\rangle \simeq 8\langle 1\rangle$. Comparing discriminants, we have $duv = 1$ in $\frac{\mathbb{Q}^*}{(\mathbb{Q}^*)^2}$; that is, $v = du$ in $\frac{\mathbb{Q}^*}{(\mathbb{Q}^*)^2}$. Thus $\sigma \perp \langle u, du\rangle \simeq 8\langle 1\rangle$.

By the Hasse-Minkowski Theorem, this can happen if and only if $s_p(8\langle 1\rangle) = 1 = s_p(\sigma \perp \langle u, du\rangle)$ for all primes p. An easy calculation shows that $s_p(\sigma \perp \langle u, du\rangle) = s_p(\sigma)(d,d)_p(u,u)_p(u,d)_p$. This product is 1 at every prime p if and only if $s_p(\sigma) = (-1,d)_p(-1,u)_p(u,d)_p$. □

In practice, this proposition seems difficult to use. One may be lucky in finding the appropriate u, but it seems difficult to assert when no u exists. The next two propositions give some easy criteria when no u exists.

Proposition 3.28. *There is a rational family of type $[a,a,a,a,a,b]$ $(a,b \in \mathbb{Q}^+)$ in order 8 if and only if $\frac{b}{a}$ is a sum of three squares in $\mathbb{Q}$.*

Proof. Such a family exists if and only if one of type $[1,1,1,1,1,\frac{b}{a}]$ exists in order 8. By Proposition 3.27 this happens if and only if there is a $u \in \mathbb{Q}^+$ such that $\langle 1,1,1,1,1,\frac{b}{a}, u, (\frac{b}{a})u\rangle \simeq 8\langle 1\rangle$. Applying Witt's Cancellation Theorem, this is equivalent to saying

$$\left\langle \frac{b}{a}, u, \left(\frac{b}{a}\right)u \right\rangle \simeq \langle 1,1,1\rangle .$$

The congruence implies that $\frac{b}{a}$ is represented by $\langle 1,1,1\rangle$, so $\frac{b}{a}$ is a sum of three squares in $\mathbb{Q}$. This proves "Only If".

To show "If", we have that $\frac{b}{a}$ is represented by $\langle 1,1,1\rangle$; hence $\langle 1,1,1\rangle \simeq \langle \frac{b}{a}, x, y\rangle$ for some $x, y \in \mathbb{Q}^+$. Comparing discriminants, we have that $y = (\frac{b}{a})x$ in $\frac{\mathbb{Q}^*}{(\mathbb{Q}^*)^2}$, which finishes the proof. □

More generally, we have:

Proposition 3.29 (Wolfe [247]). *There is a rational family of type* $[a_1, a_2, a_3, a_4, a_5, a_6]$ *in order 8 where* $a_1a_2a_3a_4 = q^2$ *for some* $q \in \mathbb{Q}$ *and* $s_p(\langle a_1, a_2, a_3, a_4\rangle) = 1$ *for all primes* p *if and only if* a_5a_6 *is a sum of three squares in* $\mathbb{Q}$.

Proof. The hypothesis gives that $\langle a_1, a_2, a_3, a_4\rangle \simeq 4\langle 1\rangle$. Thus $\sigma = \langle a_1, \ldots, a_6\rangle < 8\langle 1\rangle$ if and only if $4\langle 1\rangle \perp \langle a_5, a_6\rangle < 8\langle 1\rangle$. By Witt's Cancellation Theorem this happens if and only if $\langle a_5, a_6\rangle < 4\langle 1\rangle$ if and only if $\langle 1, a_5a_6\rangle < 4\langle 1\rangle$ if and only if $\langle a_5a_6\rangle < 3\langle 1\rangle$ (Witt again!) if and only if a_5a_6 is a sum of three squares in $\mathbb{Q}$. □

This last proof applies notably to rational families of type $[a, a, a, a, b, c]$ in order 8.

There are other special cases one can handle easily for families of six members in order 8. We mention, and leave the proof to the reader; one more:

Proposition 3.30. *Let* $a, b, c \in \mathbb{Q}^+$. *There is a rational family of type* $[a, a, a, b, b, c]$ *in order 8 where* ab *is a sum of two squares in* $\mathbb{Q}$ *if and only if* c *is a sum of three squares in* $\mathbb{Q}$.

3.15 Solution of the Algebraic Problem of Orthogonal Designs in Orders $16t$ (t Odd)

Up to this point we have asked the patient reader to accept many unproved and deep statements from the classical theory of quadratic forms over $\mathbb{Q}$. This, we have felt, is not unreasonable, since many excellent sources for the material exist, and a full exposition here would have taken us too far afield.

In this section, however, the discussion of full proofs is even more difficult. Vast new amounts of background must be introduced to get each new proposition. Thus, we shall, albeit reluctantly, usually not give proofs of these deeper statements but just refer the reader to the imaginative arguments of Shapiro.

In spite of this disclaimer, there is still much we can say for these orders with only a small number of additional facts.

Definition 3.15. (1) Let (V,q) be a quadratic space over the field k. If $x \neq 0$, $x \in V$ and $q(x) = 0$, then x is called an *isotropic vector*.
(2) If there is an isotropic vector in (V,q), then (V,q) is called *isotropic* (not isotropic equals anisotropic).
(3) We say that (V,q) is *universal* if q represents every element $a \in k$.

Proposition 3.31. *Let (V,q) be a 2-dimensional non-degenerate quadratic space. The following are equivalent:*

(i) (V,q) is isotropic;
(ii) there is a basis for V such that the matrix of B_q with respect to this basis is $\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$;
(iii) there is a basis for V such that the matrix of B_q with respect to this basis is $\left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$;
(iv) the discriminant of q is equal to -1.

Proof. The proof is elementary; see Scharlau [174]. □

This unique (up to isometry) 2-dimensional isotropic space is usually called a *hyperbolic plane* and denoted H.

Proposition 3.32. *A hyperbolic plane is universal.*

Proof. Again, elementary; see Scharlau [174]. □

Corollary 3.11. *If (V,q) is a non-degenerate isotropic quadratic space, then (V,q) is universal.*

Proof. (V,q) has a hyperbolic plane as an orthogonal summand, and so the corollary is clear from Proposition 3.32. □

Definition 3.16. Let (V,q) be a non-degenerate quadratic space over $\mathbb{Q}$. We say that (V,q) is *indefinite* if there are $x, y \in V$ with $q(x) > 0$ and $q(y) < 0$.

One of the nicer consequences of the Hasse-Minkowski theory is the following.

Theorem 3.12 (Meyer's Theorem). *Any indefinite quadratic space (non-degenerate) over $\mathbb{Q}$ of dimension greater than or equal to 5 is isotropic.*

With these facts in hand, we can now consider rational families in order $16t$ (t odd). By Theorem 3.11, we must, equivalently, consider linear subspaces $(S,\sigma) < Sim(\mathbb{Q}^{16}, 16\langle 1\rangle)$. We shall continue to abusively refer to this as considering $\sigma\langle Sim(16\langle 1\rangle)$.

We proved, Proposition 2.7, that $p(16) = 9$, and so a rational family in order 16 cannot involve more than 9 members.

3.15.1 Case 1: 9-member rational families.

Lemma 3.1. *Let $V = \mathbb{Q}^2$, and let $q = \langle 1, a\rangle$, $a \in \mathbb{Q}^+$. Then*

$$\begin{bmatrix} 0 & -a \\ 1 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = A \in Sim(V,q)\,.$$

Furthermore, $\tilde{A} = A$.

Proof. A simple application of the definitions. □

Proposition 3.33. *Let $a \in \mathbb{Q}^+$ and let $\sigma = 8\langle 1\rangle \perp \langle a\rangle$. Then $\sigma < Sim(16\langle 1\rangle)$.*

Proof. Let $A_1, \ldots, A_7$ be the H-R family of order 8, constructed in Proposition 1.2. Recall that $A_i \in Sim(\mathbb{Q}^8, 8\langle 1\rangle)$ and that $\tilde{A}_i = -A_i$ (in this example "$\sim$" was "$\top$"). It is then an easy matter to check that

$$\left\{ I_2 \otimes I_8 = I_{16},\ \begin{bmatrix} 0 & -a \\ 1 & 0 \end{bmatrix} \otimes I_8 = f_1,\ \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \otimes A_i = f_{i+1},\ i = 1, \ldots, 7 \right\}$$

is in $Sim(\mathbb{Q}^2 \otimes \mathbb{Q}^8 = V, \langle 1, a\rangle \otimes 8\langle 1\rangle = q)$ and that $f_i\tilde{f}_j + f_j\tilde{f}_i = 0$, $i \neq j$, and $\tilde{f}_i = -f_i$, $i = 1, \ldots, 8$. Also $f_1\tilde{f}_1 = a1_V$ and $f_j\tilde{f}_j = 1_V$ for $j = 2, \ldots, 8$. Thus we have $\sigma = 8\langle 1\rangle \perp \langle a\rangle < Sim(q)$. But, by Proposition 3.14 part (4), $q \simeq 16\langle 1\rangle$, and so we are done. □

This is a generalization of part (1) in the proof of Theorem 1.2 and was noted by Shapiro [191].

Theorem 3.13 (Shapiro [191]). *Let $\sigma < Sim(16\langle 1\rangle)$, $\dim \sigma = 9$. Then there is an $a \in \mathbb{Q}^+$ such that $\sigma = 8\langle 1\rangle \perp \langle a\rangle$.*

Proof. We shall postpone our remarks about this proof until the end of this section. □

Corollary 3.12. *There is a rational family of type $[s_1, \ldots, s_9]$ in order 16 if and only if $s_p(\langle a_1, \ldots, a_9\rangle) = 1$ for every prime p.*

Example 3.8. There is a rational family of type $[a, a, a, a, a, a, a, b, b]$ in order 16 if and only if ab is a sum of two squares in $\mathbb{Q}$.

3.15.2 Case 2: 7-member rational families.

Proposition 3.34. *Any 7-member rational family exists in order 16.*

Proof. By Proposition 3.33 it would be enough to show that if σ is positive definite and $\dim \sigma = 7$, then there is an $a \in \mathbb{Q}^+$ with $\sigma < 8\langle 1\rangle \perp \langle a\rangle$.

By repeated use of Proposition 3.14 part (1), we may assume $\sigma = 4\langle 1\rangle \perp \langle u,v,w\rangle$ for some $u,v,w \in \mathbb{Q}^+$. By Witt's Cancellation Theorem it will be enough to find $a \in \mathbb{Q}^+$ with $\langle u,v,w\rangle < 4\langle 1\rangle \perp \langle a\rangle$.

Let $\tau = \langle u,v,w\rangle$; then $u\tau \simeq \langle 1,y,z\rangle$, and suppose $u\tau < 4\langle 1\rangle \perp \langle d\rangle$ for some $d \in \mathbb{Q}^+$ Then $\tau < 4\langle u\rangle \perp \langle ud\rangle$. But $4\langle u\rangle \simeq 4\langle 1\rangle$, and letting $a = ud$ would finish the proof.

Thus there is no loss in assuming $\tau = \langle 1,y,z\rangle$. Consider $\langle 1,1,1,-y,-z\rangle$. By Meyer's Theorem this is isotropic, and so $\langle 1,1,1,-y,-z\rangle \simeq \langle 1,-1\rangle \perp \langle -e,s,t\rangle$ for some $e,s,t \in \mathbb{Q}^+$. Add $\langle y,z,e\rangle$ to both sides, and observe that $\langle \ell,-\ell\rangle \simeq \langle 1,-1\rangle$ (unique hyperbolic plane!) for any $\ell \in \mathbb{Q}$. Hence

$$\begin{array}{ccc} \langle 1,1,1,-y,-z\rangle \perp \langle y,z,e\rangle & \simeq & \langle 1,-1\rangle \perp \langle -e,s,t\rangle \perp \langle y,z,e\rangle \\ \wr & & \wr \\ \langle 1,1,1\rangle \perp H \perp H \perp \langle e\rangle & \simeq & H \perp H \perp \langle s,t,y,z\rangle \end{array}$$

Using Witt's Cancellation Theorem again, to cancel the hyperbolic planes, gives $\langle 1,1,1,e\rangle \simeq \langle s,t,y,z\rangle$. Adding $\langle 1\rangle$ to both sides gives the desired result. □

3.15.3 Case 3: 8-member rational families.

This is the only case we have yet to consider. There is one easy part of this discussion and one difficult part. We prove the easy part.

Proposition 3.35. *Let σ be a positive definite 8-dimensional form over $\mathbb{Q}$, and suppose $disc\sigma = 1$. Then $\sigma < Sim(16\langle 1\rangle)$.*

Proof. Let $\sigma = 5\langle 1\rangle \perp \langle u,v,w\rangle$, without loss of generality. Since $disc\sigma = 1$, $w = uv$ in $\frac{\mathbb{Q}^*}{(\mathbb{Q}^*)^2}$, and so $\sigma = 5\langle 1\rangle \perp \langle u,v,uv\rangle$.

Let $\tau = 5\langle 1\rangle \perp \langle u,v\rangle$; by Proposition 3.34, $\tau < Sim(16\langle 1\rangle)$; that is, there is a rational family of type $[1,1,1,1,1,u,v]$ in order 16. By Section 3.9 we may assume this rational family is $\{I_{16}, A_1, \ldots, A_6\}$. It is an easy matter to check that $\{I_{16}, A_1, \ldots, A_6, \prod_{i=1}^{6} A_i\}$ is a rational family of type $[1,1,1,1,1,u,v,uv]$, and hence $\sigma < Sim(16\langle 1\rangle)$. □

The case where the discriminant is not equal to 1 is deeper.

Theorem 3.14. *Let (S,σ) be a non-degenerate linear subspace of $Sim(\mathbb{Q}^{16}, 16\langle 1\rangle)$ where $\dim\sigma = 8$ and $disc\sigma \neq 1$. Then $(S,\sigma) \subset (S',\sigma')$ where $\dim\sigma' = 9$ and $(S',\sigma') < Sim(\mathbb{Q}^{16}, 16\langle 1\rangle)$.*

Proof. See Shapiro [192]. □

Thus 8-dimensional subspaces of $Sim(l6\langle 1\rangle)$ are **not** maximal if their discriminant is not equal to 1.

Corollary 3.13. *Let σ be a positive definite quadratic form where* $\dim\sigma = 8$ *and disc$\sigma \neq 1$. Then $\sigma < Sim(16\langle 1\rangle)$ if and only if there is an $a,b \in \mathbb{Q}^+$ with $\sigma \perp \langle a\rangle \simeq 8\langle 1\rangle \perp \langle b\rangle$.*

Proof. This is immediate from Theorems 3.14 and 3.13. □

If $\sigma \perp \langle a\rangle \simeq 8\langle 1\rangle \perp \langle b\rangle$, and if $d = \text{disc } \sigma \neq 1$, then $da = b$ in $\frac{\mathbb{Q}^*}{(\mathbb{Q}^*)^2}$; that is, $\sigma \perp \langle db\rangle \simeq 8\langle 1\rangle \perp \langle b\rangle$. By Hasse-Minkowski $s_p(\sigma \perp \langle db\rangle) = 1$ for all primes p. An easy calculation shows that

$$s_p(\sigma \perp \langle db\rangle) = s_p(\sigma)(d,-b)_p = 1\,.$$

Thus $s_p(\sigma) = (d,-b)_p$ for all primes p. Thus, we may restate the last corollary.

Corollary 3.14. *Let σ be a positive definite quadratic form where* $\dim\sigma = 8$ *and* disc $\sigma = d \neq 1$. *Then $\sigma < Sim(16\langle 1\rangle)$ if and only if there is $ab \in \mathbb{Q}^+$ with $s_p(\sigma) = (d,-b)_p$ for any prime p.*

We conclude this section with a short discussion of what is involved in the proof of Theorem 3.13.

Let $\dim\sigma = 9, (S,\sigma) < Sim(V, 16\langle 1\rangle)$, and write $\sigma = \langle 1\rangle \perp \sigma_1$, and let $C =$ Clifford Algebra of $-\sigma_1$.

Since $\dim(-\sigma_1) = 8$, C is a simple algebra. Let $\phi : C \mapsto End(V)$ be the usual similarity representation. Then C simple implies ϕ is one-to-one, and a dimension count ($\dim C = 2^8, \dim_{\mathbb{Q}} End(V) = 16 \times 16 = 2^8$) shows ϕ is an isomorphism.

If we call the *Witt Invariant* of $-\sigma_1$ the class of C in the Brauer group of $\mathbb{Q}$ and denote it $c(-\sigma_1)$, $C \tilde{=} End_{\mathbb{Q}} V$ implies that this is the trivial element of the Brauer group; that is, $c(-\sigma_1) = 1$. (See Lam [142, p. 120].)

Now the Hilbert symbol (a,b) may also be interpreted as the class of the quaternion algebra $\left(\frac{a,b}{\mathbb{Q}_p}\right)^p$ in the Brauer group of $\mathbb{Q}_p$ in the following way: Since there is only one non-trivial quaternion algebra over $\mathbb{Q}_p$, $\left(\frac{a,b}{\mathbb{Q}_p}\right)^p = 1$ if the quaternion algebra is 2×2 matrices over $\mathbb{Q}_p$ and -1 if it is the other quaternion algebra over $\mathbb{Q}_p$. The p-adic Hasse-invariant s_p of the quadratic form is then just the appropriate product of quaternion algebras in the Brauer group of $\mathbb{Q}_p$.

We can define a global Hasse-invariant of the quadratic form $\sigma = \langle a_1, \ldots, a_n\rangle$, $a_i \in Q$ as $s(\sigma)$, where $s(\sigma)$ is in the Brauer group of $\mathbb{Q}$ by $s(\sigma) = \prod_{i<j} \left[\left(\frac{a_i,a_j}{\mathbb{Q}}\right)\right]$ where $\left[\left(\frac{a_i,a_j}{\mathbb{Q}}\right)\right]$ denotes the class of the quaternion algebra in the Brauer group.

This global invariant (it is invariant of σ) is closely related to the Witt Invariant, and, in fact, in (Lam, [142]) the exact connections are given. In the case we're considering, $\dim(-\sigma_1) = 8$, the calculation gives

$$c(-\sigma_1) = 1 = s(-\sigma_1) \cdot \left(\frac{-1, \delta}{\mathbb{Q}} \right)$$

where $\delta =$ disc of $-\sigma_1$. In our usual terminology $1 = s_p(-\sigma_1)(-1,\delta)_p$ for all primes p.

Now since $\delta = disc(-\sigma_1) = disc(\sigma_1)$ (since $\dim(-\sigma_1) = 8$) and since $\sigma = \langle 1 \rangle \perp \sigma_1$, we have $\delta =$ disc σ.

Furthermore, $s_p(-\sigma_1) = (-1,\delta)_p s_p(\sigma_1)$, as a simple calculation shows. Now $s_p(\sigma_1) = s_p(\sigma)$. Thus we have

$$\begin{aligned} 1 = s_p(-\sigma)(-1,\delta) &= (-1,\delta)_p s_p(\sigma_1) \cdot (-1,\delta) \\ &= s_p(\sigma_1) = s_p(\sigma) \end{aligned}$$

for all primes p. Hence, if $\tau = 8\langle 1 \rangle \perp \langle \delta \rangle$, we see that $s_p(\sigma) = s_p(\tau)$ for all primes p; they have the same discriminant and same signature, and by the Hasse-Minkowski Theorem they are isometric.

3.16 Solution of the Algebraic Problem of Orthogonal Designs in Orders $32t$ (t-odd)

As usual, we are interested in finding conditions on the positive definite form σ in order that $\sigma < Sim(32\langle 1 \rangle)$. Since $\rho(32) = 10$, we know $\dim \sigma \leq 10$.

Proposition 3.36. *For any $a, b \in \mathbb{Q}^+$, $\sigma = 8\langle 1 \rangle \perp \langle a, b \rangle < Sim(32\langle 1 \rangle)$.*

Proof. We have already seen that for any $b \in \mathbb{Q}^+, 8\langle 1 \rangle \perp \langle b \rangle < Sim(16\langle 1 \rangle)$. By the same proof as in Proposition 3.33 we conclude that

$$8\langle 1 \rangle \perp \langle b \rangle \perp \langle a \rangle < Sim(\langle 1, a \rangle \otimes 16\langle 1 \rangle \simeq 32\langle 1 \rangle) . \square$$

With just this proposition we may prove

Proposition 3.37. *If σ is positive definite,* $\dim \sigma = 9$, *then $\sigma < Sim(32\langle 1 \rangle)$.*

Proof. We may write $\sigma = 6\langle 1 \rangle \perp \tau$ where $\dim \tau = 3$ and τ is positive definite. Consider $\tau \perp \langle -1, -1 \rangle = \mu$. Since μ is indefinite and $\dim \mu = 5$, we know, by Meyer' s Theorem, that μ represents 0 non-trivially. But this is just another way of saying that τ and $\langle 1, 1 \rangle$ represent a common value c. In that case $\tau = \langle a, b \rangle \perp \langle c \rangle = \langle a, b, c \rangle$ and $\langle 1, 1 \rangle \simeq \langle c, ? \rangle$, but by checking the invariants we see $\langle 1, 1 \rangle \simeq \langle c, c \rangle$. Thus

$$\tau < \langle a, b, c \rangle \perp \langle c \rangle = \langle a, b, c, c \rangle \simeq \langle a, b, 1, 1 \rangle$$

for some $a, b \in \mathbb{Q}^+$. Thus $6\langle 1 \rangle \perp \tau < 8\langle 1 \rangle \perp \langle a, b \rangle$ for some $a, b \in \mathbb{Q}^+$. $\square$

Thus we are left only with considering the case where $\dim \sigma = 10$.

Theorem 3.15 (Shapiro [191]). *If* $\dim\sigma = 10$ *and* σ *is positive definite,* $\sigma < Sim(32\langle 1\rangle)$ *if and only if* $\sigma \simeq 8\langle 1\rangle \perp \langle a,b\rangle$.

Proof. We have shown "If". We again omit the proof. It is similar, in spirit, to the (omitted) proof of Theorem 3.13. □

3.17 The Periodicity Theorem and the General Solution of the Algebraic Problem of Orthogonal Designs

In this section we omit all proofs and refer the reader to Shapiro [192].

Proposition 3.38. *Let* σ *be a positive definite form and* $\sigma = \langle 1\rangle \perp \sigma_1$. *Let* C *be the Clifford Algebra of* $-\sigma_1$, *and let* V *be any* C*-module. Then there is a positive definite form* q *on* V *where* $\sigma < Sim(V,q)$.

If $\dim\sigma \geq 5$, then $\sigma = \langle 1\rangle \perp \sigma_1$ automatically, and by Proposition 3.20 this gives that $q \simeq n\langle 1\rangle$ where $8 \mid n$ and $n = \dim V$.

Theorem 3.16 (Periodicity). *Let* σ *be positive definite and suppose* $\sigma = 8\langle 1\rangle \perp \tau$, *where* τ *represents 1. Then* $\sigma < Sim\left(2^{m+4}\langle 1\rangle\right)$ *if and only if* $\tau < Sim(q)$ *for some* 2^m*-dimensional positive definite quadratic form* q.

Proof. We shall only remark that the proof rests on Proposition 3.38 and the classical periodicity theorems for Clifford Algebras. □

Corollary 3.15. *Suppose* σ *is positive definite and* $\sigma = 8\langle 1\rangle \perp \tau$ *where* $\dim\tau \geq 5$*; then*

$$< Sim\left(2^{m+4}\langle 1\rangle\right) \Leftrightarrow \tau < Sim(2^m\langle 1\rangle).$$

Proof. This corollary just comes from the theorem and the remark preceding it. □

We are still not in a position to use the full force of this periodicity theorem. The fact that we still have restrictions on 10-dimensional σ in order 2^5 gives trouble in order 2^6.

The case of 2^6. Now $p(2^6) = 12$. Suppose $\dim\sigma = 12$. Write $\sigma = 8\langle 1\rangle \perp \tau$, $\dim\tau = 4$. By periodicity, $\tau < Sim(q)$, where q is 4-dimensional. By Corollary 3.3 we have $\tau < Sim(q)$ if and only if $\tau \simeq q$, and an easy application of Proposition 3.19 part (ii) shows $\tau \simeq q \simeq \langle 1, a.b, ab\rangle$ for some $a,b \in \mathbb{Q}^+$, and so $disc\tau = 1$. In summary, $\tau < Sim(q)$ if and only if $disc\tau = 1$. For later reference:

Proposition 3.39. *Let* σ *be a positive definite form of dimension 12.* $\sigma < Sim(2^6\langle 1\rangle)$ *if and only if* $disc\sigma = 1$.

If $\dim\sigma = 11$, then, for $11 \equiv 3 \pmod 4$, we may use the proofs of Corollary 3.6 or (equivalently) Corollary 3.9 to see that if d equals the discriminant of σ, then $\sigma < Sim(2^6\langle 1\rangle)$ if and only if $\sigma \perp \langle d\rangle < Sim(2^6\langle 1\rangle)$. Since the discriminant of $\sigma \perp \langle d\rangle = 1$, we may apply Proposition 3.39 to obtain:

Proposition 3.40. *Let σ be a positive definite form of dimension 11. Then $\sigma < Sim(2^6\langle 1\rangle)$.*

The case of 2^7. Now $p(2^7) = 16$. The periodicity handles $\dim\sigma = 16$, 15, 14, 13. So we need only consider $\dim\sigma = 12$. If we can show that every σ of dimension 12 is $< Sim(2^7\langle 1\rangle)$, then we need never consider dimension 12 (or less) again. Thus we may always use the periodicity.

But for $\dim\sigma = 12$, write $\sigma = 8\langle 1\rangle \perp \tau$, the periodicity implies $\sigma < Sim(2^7\langle 1\rangle)$ if and only if $\tau < Sim(q)$ where $\dim q = 8$. But τ represents 1, so $\langle 1, a, b\rangle < \tau$ for some $a, b \in \mathbb{Q}^+$, and hence, by Proposition 3.19 part (iii), $\langle 1, a, b, ab\rangle \,|\, q$. Applying Proposition 3.14 part (4), we obtain $q \simeq 8\langle 1\rangle$. We may now invoke Proposition 3.24 to see that since $\dim\tau = 4$, $\tau < Sim(8\langle 1\rangle)$ is always possible.

We summarize all the major results from Sections 3.15 on.

Theorem 3.17. *Let σ be a positive definite form over $\mathbb{Q}$, d equal the discriminant of σ, and $m \geq 3$.*

(A) If $\dim\sigma < 2m$, then $\sigma < Sim(2^m\langle 1\rangle)$.
(B) If $2m \leq \dim\sigma \leq p(2^m)$, then:

- *(i) if $m \equiv 0 \pmod 4$, $p(2^m) = 2m+1$ and*
  - *(a) $\dim\sigma = 2m+1$; $\sigma < Sim(2^m\langle 1\rangle)$ if and only if $s_p(\sigma) = 1$ for all primes p;*
  - *(b) $\dim\sigma = 2m$; if $d = 1$, $\sigma < Sim(2^m\langle 1\rangle)$ always; if $d \neq 1$, $\sigma < Sim(2^m\langle 1\rangle)$ if and only if there is a $b \in \mathbb{Q}^+$ with $s_p(\sigma) = (d, -b)_p$ for all primes p;*
- *(ii) if $m \equiv 1 \pmod 4$, $\rho(2^m) = 2m$; $\dim\sigma = 2m$; $\sigma < Sim(2^m\langle 1\rangle)$ if and only if there are $a, b \in \mathbb{Q}^+$ with $\sigma \simeq 2(m-1)\langle 1\rangle \perp \langle a, b\rangle$ if and only if $s_p(\sigma) = (-d, a)_p$ for some $a \in \mathbb{Q}^+$, and all primes p;*
- *(iii) if $m \equiv 2 \pmod 4$, $\rho(2^m) = 2m$; $\dim\sigma = 2m$; $\sigma < Sim(2^m\langle 1\rangle)$ if and only if $d = 1$;*
- *(iv) if $m \equiv 3 \pmod 4$, $p(2^m) = 2m+2$;*
  - *(a) $\dim\sigma = 2m+2$, $\sigma < Sim(2^m\langle 1\rangle)$ if and only if $d = 1$ and $s_p(\sigma) = 1$ for all primes p;*
  - *(b) $\dim\sigma = 2m+1$, $\sigma < Sim(2^m\langle 1\rangle)$ if and only if $s_p(\sigma) = (-1, d)_p$ for all primes p;*
  - *(c) $\dim\sigma = 2m$, $\sigma < Sim(2^m\langle 1\rangle)$ if and only if there is an $a \in \mathbb{Q}^+$ with $s_p(\sigma) = (d, -a)_p(a, -1)_p$ for every prime p.*

3.18 Combining the Algebraic Solution with Combinatorial Facts

One of the strongest combinatorial facts we discovered was Theorem 2.5. It, combined just with the algebraic restriction on the number of variables in an orthogonal design of order n, was enough to eliminate many $p(n)$-tuples as the types of orthogonal designs in order n. We now combine it with the new algebraic information to eliminate more tuples (even those of length less than $p(n)$).

We illustrate, by some examples, how the two types of information may be combined.

Example 3.9. We want to know if it is possible for an orthogonal design $OD(20;1,1,17)$ to exist.

Since $p(20)=4$, we get no contradiction just from the number of variables involved. Since $17=1^2+4^2$, we know there is a rational family of type $[1,1,17]$ in order 20. Now use Corollary 2.3 to note that if an orthogonal design of type (1,1,17) exists in order 20, then there is an orthogonal design of type (1,1,1,17) in order 20. Hence there is a rational family of type $[1,1,1,17]$ in order 20 and thus, by Theorem 3.11, in order 4. Thus $\langle 1,1,1,17\rangle \simeq \langle 1,1,1,1\rangle$, which is a contradiction since the discriminants are not equal. So there is no orthogonal design $OD(20;1,1,17)$.

Exactly the same procedure may be used to show that there is no orthogonal design $OD(20;7,12)$.

Similarly, there are no orthogonal designs of types $OD(72;1,1,1,1,1,66)$, $OD(72;1,1,1,1,1,1,65)$ or $OD(72;1,1,1,1,1,1,1,64)$.

These examples indicate how we may modify Theorem 3.17. The examples also show how the proof should be constructed and so shall be omitted.

Theorem 3.18. *Let* $n\equiv 0 \pmod 4$, $n=2^m b$, b *odd. Let* $\Delta=(a_1,\ldots,a_\ell)$ *where* $\ell<p(n)$ *and* $\sum_{i=1}^{\ell} a_i = n-1$. *The following give necessary conditions for* Δ *to be the type of an orthogonal design in order* n. *(Let* $\sigma=\langle a_1,\ldots,a_\ell\rangle$ $d=disc\,\sigma$*)*

(A) $m=2$.

$\ell=2$; $(-1,a_1a_2)_p(a_1a_2)_p=1$ for all primes p.

$\ell=3$; $a_1a_2a_3$ is a square, and $1=(a_1a_2)_p(-1,a_1a_2)_p$ for all primes p.

(B) $m\geq 3$.

(i) $m \equiv 0 \pmod 4$; $\ell = 2m$; $s_p(\sigma) = 1$ for all primes p.
$\ell = 2m-1$; if $d \neq 1$, then there is a $b \in \mathbb{Q}^+$ with $s_p(\sigma) = (d,-b)_p$ for all primes p.

(ii) $m \equiv 1 \pmod 4$; $\ell = 2m-1$; there is a $b \in \mathbb{Q}^+$ with $s_p(\sigma) = (-d,b)$ for all primes p.

(iii) $m \equiv 2 \pmod 4$; $\ell = 2m-1$; $d = 1$.

(iv) $m \equiv 3 \pmod 4$; $\ell = 2m+1$; $d = 1$ and $s_p(\sigma) = 1$ for all primes p.
$\ell = 2m$; $s_p(\sigma) = (-1,d)_p$ for all primes p.
$\ell = 2m-1$; there is an $a \in \mathbb{Q}^+$ with $s_p(\sigma) = (d,-a)_p(a,-1)_p$ for all primes p.

Example 3.10. (A) As we have seen, (A) eliminates $(7,12)$ and $(1,1,17)$ in order 20.

(B) (i) Consider if there is an orthogonal design $OD(48;1,1,1,1,3,3,36) = 3.16$. This is not eliminated by Theorem 3.17 part (B).(i).(b) since if $\sigma = 5\langle 1\rangle \perp \langle 3,3,36\rangle$, $disc\,\sigma = 1$. But $s_3(\sigma) = (3,3)_3 = (-1,3)_3 = -1$. So it is eliminated by Theorem 3.18 part (B).(i) above.

(ii) We have not found anything yet that this eliminates.

(iii) This one is easy to use; for example; there is no orthogonal design $OD(64;2,2,2,2,2,2,2,2,2,2,43)$, i.e. $OD(64;2_{10},43)$.

(iv) Parts of this are easy to use, especially $\ell = 2m+1$, $\ell = 2m$; the other part is not so easy.

We have not explored yet which designs are eliminated (in general) by this theorem. Later, when we consider the possibilities of orthogonal designs in various orders, we shall make use of these theorems.

In this chapter, then, we have dealt at some length with finding necessary conditions for the existence of orthogonal designs in various orders. The conditions, of course, then amount to eliminating various tuples as the types of orthogonal designs. In general, what we have found is (algebraically) if the length of tuple is "small" compared to $p(n)$, the tuple exists as the type of a rational family. Hence, in general, we have no algebraic conditions on small tuples. On the other hand, the combinatorial results tell us to exercise care when the orthogonal design we are after is almost full (that is, few zeros per row).

In the next chapter we take a more positive (depending on your point of view) approach. We give many constructions and examples of orthogonal designs and give some indication of the scope of possibilities that exist.

3.18.1 Alert

Since this chapter was originally written and published in 1979 there has been growing literature in the field of *Classification of Algebras*. We do not delve into this here but recommend the deeper scholar to also study this area of classification.

Chapter 4
Constructions for Orthogonal Designs via Plug In and Plug Into Matrices

4.1 Introduction

In previous chapters we have studied some necessary conditions for the existence of orthogonal designs. We now turn to the task of actually constructing such designs. The ideas and methods we use are quite varied, and many have been used in the construction of Hadamard matrices. There is one unifying theme in the constructions presented in this chapter. They revolve, in the main, around finding plug-in matrices with prescribed properties or discovering the obstructions to finding such matrices. Then we study arrays which these matrices may be plugged into. There are several methods of obtaining the appropriate collections of plug-in matrices (circulants, negacyclics, type 1, type 2 and blocks). The ways they may be used often depend on how we obtained them. In general, the more control we attempt to exert on the internal structure of the plug-in matrices, the more interesting the ways we can use them.

4.2 Some Orthogonal Designs Exist

Proposition 1.2 actually gives a construction for orthogonal designs. We review that proposition and add a remark about uniqueness in the following.

Theorem 4.1. *There are* $OD(1;1)$*,* $OD(2;1,1)$*,* $OD(4;1,1,1,1)$ *and* $OD(8;1,1,1,1,1,1,1,1)$*. These are equivalent under the equivalence operations*

(a) interchange rows or columns;
(b) multiply rows or columns by -1*;*
(c) replace any variable by its negative throughout the design; to one of the arrays of appropriate order in Table 4.1.

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5_4

Table 4.1 Examples: $OD(1;1)$, $OD(2;1,1)$, $OD(4;1,1,1,1)$ and $OD(8;1,1,1,1,1,1,1,1)$

$$[x], \quad \begin{bmatrix} x & y \\ y & -x \end{bmatrix}, \quad \begin{bmatrix} a & b & c & d \\ -b & a & d & -c \\ -c & -d & a & b \\ -d & c & -b & a \end{bmatrix} \text{ or } \begin{bmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{bmatrix},$$

$$\left[\begin{array}{cccc|cccc} a & b & c & d & e & f & g & h \\ -b & a & d & -c & f & -e & -h & g \\ -c & -d & a & b & g & h & -e & -f \\ -d & c & -b & a & h & -g & f & -e \\ \hline -e & -f & -g & -h & a & b & c & d \\ -f & e & -h & g & -b & a & -d & c \\ -g & h & e & -f & -c & d & a & -b \\ -h & -g & f & e & -d & -c & b & a \end{array}\right]$$

Proof. By tedious systematic elimination. The uniqueness of the orthogonal design of order 8 under Hadamard equivalence operations is shown in [239]. □

Here we leave the question of equivalence of orthogonal designs, except to say that Lakein and Wallis [140] have briefly considered inequivalence of Baumert-Hall arrays of small order (see Section 4.12 for definition), and Hain [96] conjectured and Eades [52] established that there are exactly two equivalence classes of circulant weighing matrices of order 13. The existence of circulant weighing matrices has attracted considerable interest. See [6, 7, 9–11, 153] papers and Section 4.4, Ohmori [156–158] has studied the equivalence of weighing matrices, $W(n,k)$ and Kimura [124], the equivalence of Hadamard matrices.

We believe equivalence of orthogonal designs is an area worthy of study. We refer any interested reader to the work of M. Hall Jnr, W. D. Wallis and others described in J. Cooper [31], J. Wallis [231, pp 408-425], B. Gordon [92], C. Koukouvinos and colleagues, H. Kharaghani, W. Holzmann and W.D. Wallis on equivalence of Hadamard matrices.

In Chapter 1 we gave a construction for H-R families (see Theorem 1.2). It is possible to generalize that result to orthogonal designs.

Theorem 4.2. *If there exists* $OD(n;u_1,u_2,\ldots,u_s)$*, then there exists an orthogonal design of type*

(i) $OD(2n;u_1,u_2,\ldots,u_{s-1},u_s,u_s)$ *with* $s+1$ *variables,*
(ii) $OD(4n;u_1,u_2,\ldots,u_{s-1},u_s,u_s,u_s)$ *with* $s+2$ *variables,*
(iii) $OD(8n;u_1,u_2,\ldots,u_{s-1},u_s,u_s,u_s,u_s,u_s)$ *with* $s+4$ *variables,*
(iv) $OD(16n;u_1,u_2,\ldots,u_{s-1},u_s,u_s,u_s,u_s,u_s,u_s,u_s,u_s,u_s)$ *with* $s+8$ *variables.*

Proof. In each case we replace each of the first $s-1$ variables by $x_i I_m$, where $m = 2, 4, 8, 16$, respectively. In cases (i), (ii), (iii) and (iv) the last variable is replaced by

$$\begin{bmatrix} x & y \\ y & -x \end{bmatrix}, \quad \begin{bmatrix} x & y & z & 0 \\ y & -x & 0 & -z \\ z & 0 & -x & y \\ 0 & -z & y & x \end{bmatrix}, \quad X \text{ and } W,$$

respectively, where X and W are given in Table 4.2. □

Table 4.2 Values for X and W

$$W = \begin{bmatrix} X & Y \\ Y^\top & Z \end{bmatrix}$$

$$= \left[\begin{array}{cccc|cccc|cccc|cccc} x & y & z & 0 & a & 0 & 0 & -b & c & 0 & 0 & d & 0 & -e & f & 0 \\ y & -x & 0 & -z & 0 & -a & b & 0 & 0 & -c & -d & 0 & e & 0 & 0 & -f \\ z & 0 & -x & y & 0 & -b & -a & 0 & 0 & d & -c & 0 & -f & 0 & 0 & -e \\ 0 & -z & y & x & b & 0 & 0 & a & -d & 0 & 0 & c & 0 & f & e & 0 \\ \hline a & 0 & 0 & b & -x & y & z & 0 & 0 & -e & f & 0 & -c & 0 & 0 & -d \\ 0 & -a & -b & 0 & y & x & 0 & -z & e & 0 & 0 & -f & 0 & c & d & 0 \\ 0 & b & -a & 0 & z & 0 & x & y & -f & 0 & 0 & -e & 0 & -d & c & 0 \\ -b & 0 & 0 & a & 0 & -z & y & -x & 0 & f & e & 0 & d & 0 & 0 & -c \\ \hline c & 0 & 0 & -d & 0 & e & -f & 0 & -x & y & z & a & 0 & 0 & 0 & -b \\ 0 & -c & d & 0 & -e & 0 & 0 & f & y & x & 0 & -z & 0 & -a & b & 0 \\ 0 & -d & -c & 0 & f & 0 & 0 & e & z & 0 & x & y & 0 & -b & -a & 0 \\ d & 0 & 0 & c & 0 & -f & -e & 0 & 0 & -z & y & -x & b & 0 & 0 & a \\ \hline 0 & e & -f & 0 & -c & 0 & 0 & d & a & 0 & 0 & b & x & y & z & 0 \\ -e & 0 & 0 & f & 0 & c & -d & 0 & 0 & -a & -b & 0 & y & -x & 0 & -z \\ f & 0 & 0 & e & 0 & d & c & 0 & 0 & b & -a & 0 & z & 0 & -x & y \\ 0 & -f & -e & 0 & -d & 0 & 0 & -c & -b & 0 & 0 & a & 0 & -z & y & x \end{array}\right]$$

Corollary 4.1. *There exists an orthogonal design of type $OD(n;1,\ldots,1)$ with $\rho(n)$ variables in order $n = 2^a.b$ (b odd).*

Proof. This follows immediately from Theorem 1.2. □

We now note that orthogonal designs of the same order but different types can be easily made by setting variables equal to zero or to one another. For easy reference, this is stated in the following lemma:

Lemma 4.1 (Equate and Kill Theorem). *If A is $OD(n;u_1,\ldots,u_s)$ on variables $x_1,\ldots,x_s$, then there is $OD(n;u_1,\ldots,u_i+u_j,\ldots,u_s)$ and $OD(n;u_1,\ldots,u_{j-1},u_{j+1},\ldots,u_s)$ on $s-1$ variables $x_1\ldots,\hat{x}_j,\ldots,x_s$.*

Proof. Set the variables $\hat{x}_j = x_i = x_j$ in the first case and $\hat{x}_j = 0$ in the second. □

Corollary 4.2. *An* $OD(n;u_1,\ldots,u_s)$ *exists if* $\sum_{i=1}^{s} u_i \le \rho(n)$ *for any integer* $n = 2,4,8$*, orthogonal designs of order* n *and any type exist.*

Proof. The proof follows by using the designs of type $(1,1,\ldots,1)$ in Corollary 4.1. □

Example 4.1.

$$\begin{bmatrix} x & y & z & w \\ -y & x & w & -z \\ -z & -w & x & y \\ -w & z & -y & x \end{bmatrix}$$

is $OD(4;1,1,1,1)$. We can make designs $OD(4;1,1,2)$ by (for example) setting $z = w = v$ and of type $OD(4;1,1,1)$ by (for example) setting $y = 0$.

$$\begin{bmatrix} x & y & v & v \\ -y & x & v & -v \\ -v & -v & x & y \\ -v & v & -y & x \end{bmatrix}$$

is an $OD(4;1,1,2)$, and

$$\begin{bmatrix} x & 0 & z & w \\ 0 & x & w & -z \\ -z & -w & x & 0 \\ -w & z & 0 & x \end{bmatrix}$$

is an $OD(4;1,1,1)$.

Another method of finding orthogonal designs, already foreshadowed by the proof of Theorem 4.2, is to replace variables by suitable matrices of variables. Similar methods were first used extensively by J. Wallis [231] in constructing Hadamard matrices. The results now quoted are due to Joan Murphy Geramita, Kounias, Koukouvinos, Holzmann, Kharaghani, Ming-yuan Xia, ourselves and many of our students.

The next lemma is given for easy reference. The remaining lemmas of this section are of far-reaching consequences and great power in constructing orthogonal designs.

Lemma 4.2. *If* A *is an* $OD(n;u_1,\ldots,u_s)$ *on* $x_1\ldots,x_s$*, then there exists* $OD(mn;u_1,\ldots,u_s)$ *on* $x_1,\ldots,x_s$ *for any integer* $m \ge 1$.

Proof. Replace each variable x_i of A by $x_i I_m$. □

The next result is most useful, and part of it first appeared in Geramita-Geramita-Wallis [77]. It was the start of what is now amicable orthogonal designs (see Chapter 5).

Lemma 4.3. *If there is* $OD(n;a,b)$*, there is an*

$OD(2n;a,a,b,b)$ $\quad$ $OD(4n;a,a,2a,b,b,2b)$
$OD(8n;a,a,2a,2a,2a,8b)$ $\quad$ $OD(8n;a,2a,2a,3a,2b,6b)$

Proof. To obtain the required designs in order $2n$, $4n$ and $8n$, respectively, the two variables of the design $OD(n;a,b)$ in order n should be replaced by the matrices of commuting variables (we use $\bar{x}_i$ for $-x_i$ and $\bar{y}_j$ for $-y_j$) given in Table 4.3 respectively. This is possible because $X_i Y_i^\top = Y_i X_i^\top$, $i = 1,2,3,4$, that is, X_i and Y_i are amicable. □

Table 4.3 Amicable designs in order $2n$, $4n$, $8n$ using $\bar{x}_i$ for $-x_i$, $\bar{y}_j$ for $-y_j$

$$X_1 = \begin{bmatrix} x_1 & x_2 \\ \bar{x}_2 & x_1 \end{bmatrix}, \quad \begin{bmatrix} y_1 & y_2 \\ y_2 & \bar{y}_1 \end{bmatrix} = Y_1$$

$$X_2 = \begin{bmatrix} x_1 & x_2 & x_3 & x_3 \\ \bar{x}_2 & x_1 & x_3 & \bar{x}_3 \\ \bar{x}_3 & \bar{x}_3 & x_1 & x_2 \\ \bar{x}_3 & x_3 & \bar{x}_2 & x_1 \end{bmatrix}, \quad \begin{bmatrix} y_1 & y_2 & y_3 & y_3 \\ y_2 & \bar{y}_1 & y_3 & \bar{y}_3 \\ y_3 & y_3 & \bar{y}_2 & \bar{y}_1 \\ y_3 & \bar{y}_3 & \bar{y}_1 & y_2 \end{bmatrix} = Y_2$$

$$X_3 = \begin{bmatrix} x_0 & x_1 & x_2 & x_3 & x_2 & x_4 & x_3 & x_4 \\ \bar{x}_1 & x_0 & x_3 & \bar{x}_2 & x_4 & \bar{x}_2 & x_4 & x_3 \\ \bar{x}_2 & \bar{x}_3 & x_0 & x_1 & x_3 & \bar{x}_4 & \bar{x}_2 & x_4 \\ \bar{x}_3 & x_2 & \bar{x}_1 & x_0 & \bar{x}_4 & \bar{x}_3 & x_4 & x_2 \\ \bar{x}_2 & \bar{x}_4 & \bar{x}_3 & x_4 & x_0 & x_1 & x_2 & \bar{x}_3 \\ \bar{x}_4 & x_2 & x_4 & x_3 & \bar{x}_1 & x_0 & \bar{x}_3 & \bar{x}_2 \\ \bar{x}_3 & \bar{x}_4 & x_2 & \bar{x}_4 & \bar{x}_2 & x_3 & x_0 & x_1 \\ \bar{x}_4 & x_3 & \bar{x}_4 & \bar{x}_2 & x_3 & x_2 & \bar{x}_1 & x_0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & - & 1 & - & - & 1 & - \\ 1 & - & 1 & 1 & - & 1 & - & - \\ - & 1 & - & - & - & 1 & - & - \\ 1 & 1 & - & 1 & 1 & 1 & - & 1 \\ - & - & - & 1 & 1 & 1 & 1 & - \\ - & 1 & 1 & 1 & 1 & - & - & - \\ 1 & - & - & - & 1 & - & - & - \\ - & - & - & 1 & - & - & - & 1 \end{bmatrix} = Y_3$$

$$X_4 = \begin{bmatrix} x_0 & x_2 & x_3 & x_3 & x_3 & x_2 & \bar{x}_1 & \bar{x}_1 \\ \bar{x}_2 & x_0 & x_3 & \bar{x}_3 & x_2 & \bar{x}_3 & \bar{x}_1 & x_1 \\ \bar{x}_3 & \bar{x}_3 & x_0 & x_2 & \bar{x}_1 & \bar{x}_1 & \bar{x}_2 & \bar{x}_3 \\ x_3 & x_3 & \bar{x}_2 & x_0 & \bar{x}_1 & x_1 & \bar{x}_3 & x_2 \\ \bar{x}_3 & \bar{x}_2 & x_1 & x_1 & x_0 & x_2 & x_3 & x_3 \\ \bar{x}_2 & x_3 & x_1 & \bar{x}_1 & \bar{x}_2 & x_0 & x_3 & \bar{x}_3 \\ x_1 & x_1 & x_2 & x_3 & \bar{x}_3 & \bar{x}_3 & x_0 & x_2 \\ x_1 & \bar{x}_1 & x_3 & \bar{x}_2 & \bar{x}_3 & x_3 & \bar{x}_2 & x_0 \end{bmatrix}, \quad \begin{bmatrix} y_2 & y_1 & \bar{y}_2 & \bar{y}_2 & \bar{y}_2 & y_1 & \bar{y}_2 & \bar{y}_2 \\ y_1 & \bar{y}_2 & y_2 & \bar{y}_2 & \bar{y}_1 & \bar{y}_2 & \bar{y}_2 & y_2 \\ \bar{y}_2 & y_2 & \bar{y}_1 & y_2 & \bar{y}_2 & \bar{y}_2 & \bar{y}_2 & y_1 \\ \bar{y}_2 & \bar{y}_2 & y_2 & y_1 & \bar{y}_2 & y_2 & \bar{y}_1 & \bar{y}_2 \\ \bar{y}_2 & \bar{y}_1 & \bar{y}_2 & \bar{y}_2 & \bar{y}_2 & y_1 & y_2 & y_2 \\ y_1 & \bar{y}_2 & \bar{y}_2 & y_2 & y_1 & y_2 & \bar{y}_2 & y_2 \\ \bar{y}_2 & \bar{y}_2 & \bar{y}_2 & \bar{y}_1 & y_2 & \bar{y}_2 & \bar{y}_1 & \bar{y}_2 \\ \bar{y}_2 & y_2 & y_1 & \bar{y}_2 & y_2 & y_2 & \bar{y}_2 & y_1 \end{bmatrix} = Y_4 .$$

Corollary 4.3. *If there are $OD(n;1,k)$, $1 \le k \le j$, then there are $OD(2n;1,m)$ for $1 \le m \le 2j+1$. In particular, if there are $OD(n;1,k)$, $1 \le k \le n-1$, then there are $OD(2^t n;1,m)$, $1 \le m \le 2^t n - 1$, t a positive integer.*

Example 4.2. Since there is an $OD(2;1,1)$, there exist, using Corollary 4.3, orthogonal designs $OD(2^t;1,k)$, $1 \le k \le 2^t - 1$, in every order 2^t, t a positive integer.

The following lemma is crucial to the powerful results on Hadamard matrices we will obtain later.

Theorem 4.3 (Doubling Theorem). *If there exists an* $OD(n; s_1, s_2, \ldots, s_u)$, *then there exist orthogonal designs of type*

(i) $OD(2n; e_1 s_1, e_2 s_2, \ldots, e_u s_u)$ *where* $e_i = 1$ *or* 2,
(ii) $OD(2n; s_1, s_1, f s_2, \ldots, f s_u)$ *where* $f = 1$ *or* 2.

Proof. (i) Replace each variable by $\begin{bmatrix} x_i & 0 \\ 0 & x_i \end{bmatrix}$ if $e_i = 1$ and by $\begin{bmatrix} x_i & x_i \\ x_i & -x_i \end{bmatrix}$ if $e_i = 2$. (ii) Replace the variable x_1 by $\begin{bmatrix} x_0 & x_1 \\ -x_1 & x_0 \end{bmatrix}$ and the variable x_i, $i \neq 1$, by $\begin{bmatrix} 0 & x_i \\ x_i & 0 \end{bmatrix}$ or $\begin{bmatrix} x_i & x_i \\ x_i & -x_i \end{bmatrix}$ according as f is 1 or 2. □

4.3 Some Basic Matrix Results

One of the most useful constructive methods for orthogonal designs has been that using two or more circulant matrices. Later in Section 4.5 we discuss the alternative plug-in matrices, nega-cyclic matrices, which are especially useful for even orders. In this section we give some results about circulant matrices starting with the more general concept of type 1; then we develop some existence results.

First we give some definitions and elementary results. We use the following notation:

Notation 4.1. A $(1, -1)$ matrix is a matrix whose only entries are $+1$ or -1. We use similar notation for a $(0, 1, -1)$ matrix, (a, b, c) matrix, etc. We use J_n for the $n \times n$ matrix with every entry $+1$. (We shall sometimes drop the subscript if the order is obvious.)

Definition 4.1. (a) Let G be an additive abelian group of order t, and order the elements of G as $z_1, \ldots, z_t$. Let ψ and ϕ be two functions from G into a commutative ring. We define two matrices $M = (m_{ij})$ and $N = (n_{ij})$, of order t, as follows:

$$m_{ij} = \psi(z_j - z_i) \text{ and } n_{ij} = \phi(z_j + z_i).$$

M and N are called *type 1* and *type 2* matrices, respectively.

Remark 4.1. The words "type 1" used to describe these matrices leaves out information: the way the elements of G are ordered and which functions ψ and ϕ are being used. One should say, e.g., in describing M, "type 1 with respect to the following ordering of G and the function ϕ"; however, this cumbersome phrase will be omitted since the ordering for G is usually understood and fixed, while the functions ψ and ϕ are usually explicit.

(b) Let G be as above with its elements ordered as above. Let X be a subset of G, and suppose $0 \notin X$. If ψ and ϕ are defined by:

$$\psi(x)=\begin{cases} a, & x=0 \\ b, & x\in X \\ c, & x\notin X\cup\{0\} \end{cases}, \qquad \phi(x)=\begin{cases} d, & x=0 \\ e, & x\in X \\ f, & x\notin X\cup\{0\} \end{cases},$$

then M will be called the *type 1* (a,b,c) *incidence matrix generated by* X, and N the *type 2* (d,e,f) *incidence matrix generated by* X.

Remark 4.2. If we drop the restriction that $0\notin X$ and let

$$\psi(x)=\phi(x)=\begin{cases} 1 & \text{if } x\in X \\ -1 & \text{if } x\notin X \end{cases},$$

we obtain the type i $(i=1,2)$ $(1,-1)$ *incidence matrix generated by* X, and if we let

$$\psi(x)=\phi(x)=\begin{cases} 1 & \text{if } x\in X \\ 0 & \text{if } x\notin X \end{cases},$$

then we obtain the type i $(i=1,2)$ $(1,0)$ *incidence matrix generated by* X.

Notice that these latter two "incidence" matrices are really special cases of Definition 4.1 part (b) where we let $a=b$ or $a=c$ depending on whether $0\in X$ or $0\notin X$.

Example 4.3. Consider the field $\frac{Z_3[x]}{(x^2-x-1)}=GF(3^2)$. We order the elements $g_1=0,\ g_2=1,\ g_3=2,\ g_4=x,\ g_5=x+1,\ g_6=x+2,\ g_7=2x,\ g_8=2x+1,$ $g_9=2x+2$. Define the set

$$\begin{aligned} X&=\{y\colon y=z^2 \text{ for some } z\in GF(3^2),\ z\neq 0\} \\ &=\{x+1,2,2x+2,1\}. \end{aligned}$$

Then the type 1 and type 2 $(0,1,-1)$ incidence matrices generated by X are given by A and B, respectively:

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

$$B = \begin{bmatrix} 0 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 0 & 1 & -1 & -1 & -1 & 1 & -1 \\ 1 & 0 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 0 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & 0 \\ -1 & -1 & 1 & 1 & -1 & -1 & 1 & 0 & 1 \\ -1 & -1 & 1 & 0 & 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & 1 & 0 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 0 & 1 & -1 & -1 & 1 \end{bmatrix}.$$

If the additive abelian group in Definition 4.1 is the cyclic group Z_t of integers modulo t with the usual ordering $0,1,2,\ldots,t-1$, then the type 1 and type 2 matrices are very familiar.

Definition 4.2. (a) A circulant matrix $A = (a_{ij})$ of order n is one for which $a_{ij} = a_{1,j-i+1}$ where $j-i+1$ is reduced modulo n to $0,1,2,\ldots,n-1$. For example:

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

(b) A set $D = \{x_1, x_2, \ldots, x_k\} \subset \{0,1,2,\ldots,n-1\}$ will be said to *generate a circulant* $(1,-1)$ matrix if the first row of the circulant matrix is defined by

$$a_{1x} = \begin{cases} +1, & x \in D \\ -1, & x \notin D \end{cases}.$$

(c) A matrix $A = (a_{ij})$ of order n will be called *back circulant* if $a_{ij} = a_{1,i+j-1}$ where $i+j-1$ is reduced modulo n. For example:

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

Remark 4.3. (i) Any type 1 matrix defined on Z_t (with its usual ordering) is circulant since:

$$m_{ij} = \psi(j-i) = \psi(j-i+1-1) = m_{1,j-i+1}.$$

(ii) Any type 2 matrix defined on Z_t (with its usual ordering) is back circulant since:

$$n_{ij} = \phi(i+j) = \phi(i+j-1+1) = n_{1,i+j-1}.$$

Clearly, any circulant matrix is a type 1 matrix, and any back circulant matrix is a type 2 matrix. In any case:

- A type 1 matrix is analogous to a circulant matrix;
- A type 2 matrix is analogous to a back circulant matrix.

Thus, all propositions proved about type 1 and type 2 matrices have corollaries about circulant and back circulant matrices.

Lemma 4.4. *Suppose G is an additive abelian group of order v with elements ordered $z_1, z_2, \ldots, z_v$. Let ϕ, ψ, and μ be functions from G to some commutative ring R.*

Define $A = (a_{ij})$, $B = (b_{ij})$ and $C = (c_{ij})$ by $a_{ij} = \phi(z_j - z_i)$, $b_{ij} = \psi(z_j - z_i)$ and $c_{ij} = \mu(z_j + z_i)$. Then

$$\text{(i)} \quad C^\top = C, \qquad \text{(ii)} \quad AB = BA, \qquad \text{(iii)} \quad AC^\top = CA^\top.$$

Proof. (i) $c_{ij} = \mu(z_j + z_i) = \mu(z_i + z_j) = c_{ji}$.

(ii) $(AB)_{ij} = \sum_{g \in G} \phi(g - z_i)\psi(z_j - g)$.

Putting $h = z_i - z_j - g$, it is clear that as g ranges through G, so does h, and the above expression becomes

$$\sum_{h \in G} \phi(z_j - h)\psi(h - z_i) \;=\; \sum_{n \in G} \psi(h - z_i)\phi(z_j - h)$$

(since R is commutative); this is $(BA)_{ij}$.

$$\begin{aligned} \text{(iii)}\ (AC^\top)_{ij} &= \textstyle\sum_{g \in G} \phi(g - z_i)\psi(z_j + g) \\ &= \textstyle\sum_{h \in G} \phi(h - z_j)\mu(z_i + h) \qquad (h = z_j + g - z_i) \\ &= (CA^\top)_{ij}. \end{aligned}$$

□

Corollary 4.4. *If X and Y are type 1 matrices and Z is a type 2 matrix, all defined on the same abelian group with a fixed ordering, then (i) $Z^\top = Z$, (ii) $XY = YX$, (iii) $XZ^\top = ZX^\top$.*

Lemma 4.5. *(i) If X is a type 1, $i = 1, 2$, matrix, then so is $X^\top$.*
(ii) If X and Y are type 1 matrices, $i = 1, 2$, both defined on the same abelian group with a fixed ordering, then so is $X + Y$ and $X - Y$.

Proof. (i.a) If $X = (x_{ij})$ is type 2 defined using a function ϕ, then $X_{ij} = \phi(z_i + z_j) = \phi(z_j + z_i) = X_{ji}$. So $X^\top$ is also defined as type 2 using ϕ.

(i.b) If $X = (x_{ij})$ is of type 1 defined using ψ, then $x_{ij} = \psi(z_j - z_i)$. Now define a type 1 matrix $M = (m_{ij})$ using μ, where $\mu(x) = \psi(-x)$. Then $m_{ij} = \mu(z_j - z_i) = \psi(z_i - z_j) = x_{ji}$. Thus $M = X^\top$.

(ii.a) If X and Y are type 2 defined using ϕ_1 and ϕ_2, then the type 2 matrices defined using $\phi_1+\phi_2$ and $\phi_1-\phi_2$ respectively, give $X+Y$ and $X-Y$, respectively.

(ii.b) Similarly, if X and Y are type 1 defined using ψ_1 and ψ_2, define type 1 matrices using $\mu_1+\mu_2$ and $\mu_1-\mu_2$, respectively, to obtain $X+Y$ and $X-Y$, respectively, where $\mu_i(x)=\psi_i(-x)$. □

Corollary 4.5. *(i) If X and Y are type 1 matrices, defined on the same abelian group with a fixed ordering, then*

$$\begin{array}{ll} XY=YX & XY^\top=Y^\top X \\ X^\top Y=YX^\top & X^\top Y^\top=Y^\top X^\top \end{array}.$$

(ii) If P is a type 1 matrix and Q is a type 2 matrix, both defined on the same abelian group with a fixed ordering, then

$$\begin{array}{ll} PQ^\top=QP^\top & P^\top Q^\top=QP \\ PQ=Q^\top P^\top & P^\top Q=Q^\top P \end{array}.$$

We now summarize the most used results for circulants.

Corollary 4.6. *(i) Two circulant matrices of the same order commute.*
(ii) A back circulant matrix is symmetric.
(iii) The product of a back circulant matrix with a circulant matrix of the same order is symmetric. In particular, if B is back circulant and A is circulant,

$$AB^\top=BA^\top.$$

A and B are amicable matrices (see Chapter 5)

Remark. From now on, whenever we refer to a collection of type 1 and type 2 matrices all defined on the same abelian group G, we shall assume that the ordering of the group elements has been fixed.

Lemma 4.6. *(i) Let X and Y be type 2 (d,e,f) incidence matrices generated by subsets A and B of an additive abelian group G. Suppose, further, that*

$$a\in A\Rightarrow -a\in A \quad \textit{and} \quad b\in B\Rightarrow -b\in B\,.$$

Then,

$$XY=YX \quad \textit{and} \quad XY^\top=YX^\top\,.$$

(ii) The same result holds if X and Y are type 1.

Proof. (i) Since X and Y are symmetric, we only have to prove that $XY^\top=YX^\top$. Suppose $X=(x_{ij})$ and $Y=(y_{ij})$ are defined by

$$x_{ij}=\phi(z_i+z_j), \qquad y_{ij}=\psi(z_i+z_j)\,,$$

where $z_1, z_2, \ldots$ are the elements of G. Then

$$\begin{aligned}
(XY^\top)_{ij} &= \sum_k \phi(z_i + z_k)\psi(z_k + z_j) \\
&= \sum_k \phi(-z_i - z_k)\psi(z_k + z_j) && \text{since } a \in A \Rightarrow -a \in A \\
&= \sum_\ell \phi(z_j + z_\ell)\psi(-z_\ell - z_i - z_j + z_j) && z_\ell = -z_k - z_i - z_j \\
&= \sum_\ell \phi(z_j + z_\ell)\psi(z_\ell + z_i) && \text{since } b \in B \Rightarrow -b \in B \\
&= (YX^\top)_{ij}\,.
\end{aligned}$$

(ii) The additional hypotheses on A and B force X and Y to be symmetric. The proof, then, is similar to (i), and we leave it to the reader as an easy exercise. □

Lemma 4.7. *Let $R = (r_{ij})$ be the permutation matrix of order n, defined on an additive abelian group $G = \{g_i\}$ of order n by*

$$r_{k,j} = \begin{cases} 1 & \text{if } g_k + g_j = 0 \\ 0 & \text{otherwise.} \end{cases}$$

(i) If M is a type 1 matrix defined on G, then MR is a type 2 matrix defined on G.
(ii) If N is a type 2 matrix defined on G, then NR is a type 1 matrix defined on G.
(iii) If X is a subset of G where $0 \notin X$ and M is the type 1 (a,b,c) incidence matrix generated by X, then MR is the type 2 (a,b,c) incidence matrix generated by $-X$.
(iv) If X is as in (3) and N is the type 2 (a,b,c) incidence matrix generated by X, then NR is the type 1 (a,b,c) incidence matrix generated by $-X$.

Proof. 1.) Let $M = (m_{ij})$ be defined by $m_{ij} = \psi(g_j - g_i)$, and let $\mu(x) = \psi(-x)$. We claim that MR is the type 2 matrix defined by μ, for

$$\begin{aligned}
(MR)_{ij} &= \sum_k m_{ik} r_{kj} = m_{i\ell}, \text{ where } g_\ell + g_j = 0, \\
&= \psi(g_\ell - g_i) = \psi(-g_j - g_i) = \mu(g_j + g_i)\,.
\end{aligned}$$

2.) follows from a similar argument.
3.) and 4.) are clear from 1.) and 2.) and the relationship between ψ and μ. □

Corollary 4.7. *Let G be an additive abelian group and X a subset of G where $0 \notin X$. Let M be the type 1 (a,b,c) incidence matrix generated by X, and N the type 2 (a,b,c) incidence matrix generated by $-X$. Then*

$$MM^\top = NN^\top .$$

Proof. Lemma 4.7 gives that $M = NR$, where R is the permutation matrix appropriate to G. The corollary follows since $RR^\top = 1$. □

4.3.1 Supplementary Difference Sets, their Incidence Matrices and their Uses as Suitable Matrices

Definition 4.3. Let $S_1, S_2, \ldots, S_n$ be subsets of V, an additive abelian group of order v. Let $|S| = k_i$ and $S_i = s_{i1}, s_{i2}, \ldots, s_{ik_i}$. If the equation

$$g = s_{ij} - s_{im}$$

has exactly λ solutions for each non-zero element g of V, then $S_1, S_2, \ldots, S_n$ will be called $n - \{v; k_l, k_2, \ldots, k_n; \lambda\}$ *supplementary difference sets* or sds. If $k_1 = k_2 = \cdots = k_n = k$, we write $n - \{v; k; \lambda\}$ sds.

Lemma 4.8. *Suppose $A_1, \ldots, A_n$ are the type 1 $(0,1)$ incidence matrices generated by $S_1, \ldots, S_n$, where $S_1, \ldots, S_n$ are $n - \{v; k; \lambda\}$ sds. Then*

$$\sum_{i=1}^{n} A_i A_i^\top = \left(\sum_{i=1}^{n} k_i - \lambda \right) I + \lambda J .$$

Proof. This follows from the definition by a simple counting argument. (See Wallis [231, p.290] for a fuller proof.) □

Example 4.4. $S_1 = \{0,2,3\}$ and $S_2 = \{0,1,4\}$ are $2 - \{5;3;3\}$ sds in Z_5. Their type 1 $(1,0)$ incidence matrices are the circulants

$$A_1 = \begin{bmatrix} 1\,0\,1\,1\,0 \\ 0\,1\,0\,1\,1 \\ 1\,0\,1\,0\,1 \\ 1\,1\,0\,1\,0 \\ 0\,1\,1\,0\,1 \end{bmatrix} \quad \text{and} \quad A_2 = \begin{bmatrix} 1\,1\,0\,0\,1 \\ 1\,1\,1\,0\,0 \\ 0\,1\,1\,1\,0 \\ 0\,0\,1\,1\,1 \\ 1\,0\,0\,1\,1 \end{bmatrix}$$

which satisfy

$$A_1 A_1^\top + A_2 A_2^\top = 3I + 3J .$$

We observe that for these subsets of Z_5, $x \in S_i \Rightarrow -x \in S_i$. So, if R is the back diagonal matrix of order 5 (see Lemma 4.7), we see $A_1 R = B_1$ and $A_2 R = B_2$ are the type 2 $(1,0)$ incidence matrices generated by S_1 and respectively.

$$B_1 = A_1R = \begin{bmatrix} 1\,0\,1\,1\,0 \\ 0\,1\,1\,0\,1 \\ 1\,1\,0\,1\,0 \\ 1\,0\,1\,0\,1 \\ 0\,1\,0\,1\,1 \end{bmatrix} \quad \text{and} \quad B_2 = A_2R = \begin{bmatrix} 1\,1\,0\,0\,1 \\ 1\,0\,0\,1\,1 \\ 0\,0\,1\,1\,1 \\ 0\,1\,1\,1\,0 \\ 1\,1\,1\,0\,0 \end{bmatrix}.$$

Using Lemma 4.6 (or directly), we obtain

$$B_1B_2 = B_2B_1 \text{ and } B_1B_2^\top = B_2B_1^\top.$$

Also

$$A_1A_2 = A_2A_1 \text{ and } A_1A_2^\top = (B_1R)(B_2R)^\top = B_2B_1^\top.$$

We also observe that

$$A_1B_2^\top = B_2A_1^\top \text{ and } A_iA_i^\top = B_iB_i^\top.$$

Lemma 4.9. *Let $A_1,\ldots,A_n$ be type 1 $(1,0)$ incidence matrices generated by $S_1,\ldots,S_n$ where $S_1,\ldots,S_n$ are $n-\{v;k_1,\ldots,k_n;\lambda\}$ sds.*

Let $B_i = A_i - J$. Then

$$\sum_{i=1}^{n} B_iB_i^\top = 4\left(\sum_{j=1}^{n} k_j - \lambda\right) I + \left[nv - 4\left(\sum_{j=1}^{n} k_j - \lambda\right)\right] J.$$

We are constantly searching for $(0,1,-1)$ matrices to substitute for the variables in an orthogonal design. We shall be precise about what is needed.

Definition 4.4. A set of m $(0,1,-1)$ matrices $A_1, A_2, \ldots, A_m$ of order n will be called *suitable plug-in matrices* for the orthogonal design of type $OD(n; s_1, s_2, \ldots, s_m)$ if

$$\begin{aligned} &1) \quad A_iA_j^\top = A_jA_i^\top, \quad 1 \le i, \quad j \le m; \\ &2) \quad \sum_{i=1}^{m} s_iA_iA_i^\top = kI_n. \end{aligned}$$

2) is called the *additive property*. So suitable matrices are pairwise amicable and satisfy the additive property.

Theorem 4.4. *Let S_1, S_2, S_3, S_4 be $4-\{t;k_1,k_2,k_3,k_4;\sum_{j=1}^{4} k_j - t\}$ sds for which $x \in S_i \Rightarrow -x \in S_i$, and let A_l, A_2, A_3, A_4 be the type 1 $(1,-1)$ incidence matrices of these sets. Then A_1, A_2, A_3, A_4 are suitable matrices for an orthogonal design $OD(4st; s, s, s, s)$.*

Proof. Since $x \in S_i \Rightarrow -x \in S_i$ we see that A_i, $i = 1,2,3,4$, are symmetric and commuting. Using Lemma 4.9, we have

$$\sum_{i=1}^{4} A_i A_i^\top = 4\left(\sum_{j=1}^{4} k_j - \sum_{j=1}^{4} k_j + t\right) I + \left(4t - 4\left(\sum_{j=1}^{4} k_j - \sum_{j=1}^{4} k_j + t\right)\right) J$$
$$= 4tI.$$

In particular,

$$\sum_{i=1}^{4} sA_i A_i^\top = 4stI\,.$$

If the variables of the orthogonal design are replaced by the A_i, $i = 1,2,3,4$, we have a weighing matrix of weight $4st$. □

If the orthogonal design of the theorem is of order $4s$, then the weighing matrix obtained will be of order $4st$ and weight $4st$, in other words, an Hadamard matrix of order $4st$. In this case the symmetric matrices of Theorem 4.4 are a special kind of what will be called Williamson matrices (see also Definition 4.16).

4.4 Existence of Weighing Matrices

In 1972 at the first Australian conference on Combinatorial Mathematics, Seberry Wallis gave her first paper on weighing matrices [232]. Weighing matrices also caused interest at Queen' s University that year. It was observed that in order to establish existence in all orders for a given weight we needed to consider weighing matrices in odd orders.

We noticed that there was a circulant $W(7,4)$. It has first row -110100.

Then D. Gregory found a non-circulant $W(13,9)$. After observing that the zeros of this matrix give the incidence matrix of a finite projective plane, we found a circulant $W(13,9)$ with first row $0010111-01-1$.

At the Fifth South-eastern Conference on Combinatorics, Graph Theory and Computing in Boca Raton, Florida, in 1972, Rick Wilson and R.C. Mullin said they thought $W(q^2+q+1,q^2)$ might exist when q was a prime power.

At that time Mullin [153] was writing a book on Coding Theory with Ian Blake [23], who quickly saw the possibilities of using weighing matrices and especially circulant matrices W to form generator matrices $[I,W]$ of codes over $GF(3)$ which would generalise the Pless symmetry codes.

Wallis and Whiteman (Theorem 4.6) finally showed that circulant $W(q^2+q+1,q^2)$ existed when q was a prime power.

In writing this section it seemed that the proof of Wallis and Whiteman was too circuitous and a prettier, more direct proof was desirable. Our colleague, L.G. Kovacs, has given three proofs; the second is illustrated by Example

4.8 and we feel is intrinsically very beautiful. The first proof is illustrated by Example 4.9. The proof we have given here is the shortest, but hides to some extent the delightful intimacy between circulant weighing matrices and cyclic projective planes. The work of David Glynn gives more insight. (See Glynn [87].)

It was Kovacs' work that allowed Hain and Eades [54] to establish that there are only two equivalence classes of circulant $W(13,9)$. Many others [6, 7, 9–11, 153, 201, 252] have continued this study of circulant weighing matrices, but the full story is not yet known.

If A is a $W(n,k)$, then $(\det A)^2 = k^n$. Thus if n is odd and a $W(n,k)$ exists, then k must be a perfect square.

In Proposition 2.3 it is shown that

$$(n-k)^2 - (n-k) + 2 > n$$

must also hold. It is noted there that the "boundary" values of this condition are of special interest, that is, if

$$(n-k)^2 - (n-k) + 1 = n,$$

for in this case the zeros of A occur such that the incidence between any pair of rows is exactly one. So if we let $B = J_n - AA^\top$, B satisfies

$$BB^\top = (n-k-1)I_n + J_n, \quad BJ_n = (n-k)J_n;$$

that is, B is the incidence matrix of the projective plane of order $n-k-1$.

Thus the non-existence of the projective plane of order $n-k-1$ implies the non-existence of the $W(n,k)$ when $n = (n-k)^2 - (n-k) + 1$. So we rewrite the Bruck-Ryser-Chowla Theorem from Hall [97, p.107–112] to allow us to consider the non-existence of projective planes.

Theorem 4.5 (Bruck-Ryser). *If there exists a projective plane of order s, then the Diophantine equation*

$$x^2 = sy^2 + (-1)^{\frac{(s^2+2)}{2}} z^2$$

has a solution in the integers not all zero. That is, the Hilbert symbol

$$\left((-1)^{\frac{(s^2+2)}{2}}, s \right)_p = +1$$

for all primes p, including $p = \infty$.

Example 4.5. Consider $s = n-k-1 = 6$, $s^2+s+1 = n = 43$, $s^2 = k = 36$. The Bruck-Ryser Theorem says that there is a projective plane only if

$$\left(-1^{21}, 6\right)_p = (-1, 6)_p = +1 \quad \text{at all primes } p.$$

But at $p = 3$

$$(-1,6)_3 = (-1,2)_3(-1,3)_3 = \left(\tfrac{2}{3}\right) = -1\,.$$

So there is no projective plane of order 6 and no $W(43,36)$.

Similarly, if $s = 2t = n-k-1$, $s^2+s+1 = n$, $s^2 = k$, where $t \equiv 3 \pmod 4$ is a prime, there is no projective plane of order $2t$ and no $W(4t^2+2t+1, 4t^2)$.

Before we prove our result on circulant weighing matrices, we prove the following more general result.

Lemma 4.10 (Blake [23]). *Let q be the power of an odd prime and k any integer $k \geq 3$. Then there exists a*

$$W\left(\frac{(q^k-1)}{q-1}, q^{k-1}\right).$$

Proof. Let G be a $kX(q^k-1)$ matrix whose columns contain all the distinct non-zero k-tuples over the finite field $GF(q)$. In coding terms, the row space of G, denoted by C, is equivalent to a maximum length cyclic code. It is known that the weight of every non-zero codeword in C is $(q-1)q^{k-1}$. If G^1 is the $k \times (q^k-1)$ matrix whose rows are any set of k linearly independent codewords of C, then every non-zero k-tuple over $GF(q)$ appears as a column of G^1.

Let H be a $k \times n$ submatrix of G, $n = \frac{q^k-1}{q-1}$, with the property that any two of its columns are linearly independent. We assume that H is normalized in the sense that the first non-zero element in each column is unity. Let A be an $n \times n$ matrix whose rows are chosen from the non-zero vectors of the row space of H and have the property that any two distinct rows are linearly independent. Assume for convenience that the first k rows of A are rows of H. It follows readily from observations on G that every row of A has weight q^{k-1}. It is not difficult to show that if H is the $(0,1)$ matrix obtained from H by replacing each non-zero element by unity, then the rows of H^1 are the incidence vectors of the compliments of the hyperplanes of the geometry $PG(k-1,q)$.

Let x_1 and x_2 be two distinct rows of A. Since they are independent, they can be extended to a basis x_i , $i = 1,\ldots,k$, each vector of which is a row of A. Let B be the $k \times n$ matrix whose i-th row is x_i, $i = 1,\ldots,k$. Assume B has been normalized by multiplying each column so that the first non-zero element in each column is unity. let B^1 be the $k \times q^{k-1}$ submatrix of B consisting of those columns with unity in the first row. Every $(k-1)$-tuple over $GF(q)$, including the a1l-zeros $(k-1)$-tuple, appears in the columns of B in rows 2 through k. Each element of $GF(q)$ appears q^{k-2} times in the second row of B. In the matrix A, replace $\alpha \in GF(q)$ by $\chi(\alpha)$, where χ is the usual quadratic character, and call the resulting matrix $S(q^{k1})$. We now show that over the real numbers

$$S\left(q^{k-1}\right) S\left(q^{k-1}\right)^t = q^{k-1} I_n$$

and thus that $S(q^{k-1})$ is the required $W\left(\frac{q^k-1}{q-1}, q^{k-1}\right)$.

Since every row of A is of weight q^{k-1} and each non-zero element of $GF(q)$ is either a square or a non-square, the inner product over the reals of any row of $S(q^{k-1})$ with itself is q^{k-1}. Let $x_1 = (\alpha_l, \ldots, \alpha_n)$, $x_2 = (\beta_1, \ldots, \beta_n)$ be two distinct rows of A. If $y_1 = (\chi(\beta_1), \ldots, \chi(\beta_n))$ and $y_2 = (\chi(\alpha_1), \ldots, \chi(\alpha_n))$ are the corresponding rows of $S(q^{k-1})$, then the inner product of y_1 and y_2 over the reals is the number of non-zero coordinate positions for which $\chi(\alpha_i) = \chi(\beta_i)$ less the number of non-zero coordinate positions for which $\chi(\alpha_i) \neq \chi(\beta_i)$. Since χ is multiplicative, i.e. , $\chi(\alpha)\chi(\beta) = \chi(\alpha\beta)$, multiplication of a coordinate position by a non-zero element of $GF(q)$ does not change the agreement or disagreement between coordinate positions of y_1 and y_2. As before, assume that x_1 and x_2 are the first two rows of the matrix B, which is assumed in normalized form. In the non-zero positions of x_1, each element of $GF(q)$ appears in x_2, q^{k-2} times. Thus the inner product of the corresponding vectors y_1 and y_2 is zero, which completes the lemma. □

We now show how to construct circulant weighing matrices based on the fact that an oval in a projective plane can meet a line in only one of three ways: 0 (it misses it entirely), 1 (it is a tangent), 2 (it intersects the oval). This observation is true for any projective plane of prime power order (even or odd). These will be used extensively in later theorems.

Theorem 4.6 (Wallis-Whiteman [242], proof by L. G. Kovacs). *Let q be a prime power. Then there is a circulant $W(q^2+q+1, q^2)$.*

Proof. Let D be a cyclic planar difference set with parameters $(q^2+q+1, q+1, 1)$. (See Baumert [16] for definition.) These always exist for q a prime power, and the incidence matrix of D is the incidence matrix of the projective plane of order q.

Without loss of generality, we assume $0 \in D$. We note that d and $-d$ cannot both be in D because $d - 0 = 0 - (-d)$, contradicting the uniqueness of differences in D.

Let

$$\psi(x) = \sum_{d \in D} x^d$$

be the Hall polynomial of D. (see Baumert [16, p.8]) Then

$$\psi^2(x) = \sum_{d \in D} x^{2d} + 2 \sum_{\substack{e,f \in D \\ e \neq f}} x^{e+f}$$

We wish to show the coefficients of x^i in $\chi^2(x)$ are 0, 1, 2, i.e. , that $2d \neq 2e$ unless $d = e$, $e + f \neq e' + f'$ unless $e = e'$ and $f = f'$, and $2d \neq e + f$ unless $d = e = f$.

Clearly, $2d \neq 2e$ for $d \neq e$. If $e + f = e' + f'$, then $e - e' = f - f'$, and by the uniqueness of differences in D either $e = f$ and $e' = f'$ or $e = -f'$ and

$e' = -f$. In the first case $2e = 2e'$, $e = e'$, $f = f'$, and in the second case $e+f = -(e+f)$, i.e. , $e+f = 0$ and e and $-e \in D$, which is not possible. If $2d = e+f$, then $d-e = f-d$, and by the uniqueness of differences in D, either $d = f$, $e = d$ or $d = -d$, $e = -f$. In the first case there is nothing to prove, and in the second case e and $-e \in D$, which is not possible.

Hence if B is the cyclic incidence matrix of D, then B^2 has elements 0, 1, 2, and $B^2 - J$ has elements 0, 1, -1.

Now

$$\begin{aligned}\left(B^2 - J\right)\left(B^2 - J\right)^\top &= BBB^\top B^\top - BBJ + J^2 .\\ &= (qI + J)^2 - 2(q+1)^2 J + (q^2+q+1)J .\\ &= q^2 I\end{aligned}$$

So $B^2 - J$ is the required $W(q^2+q+1, q^2)$. □

Example 4.6. $\{0,1,3,9\}$ is a difference set modulo 13, whose circulant incidence matrix B has first row

$$1\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0.$$

B^2 is a circulant matrix with first row

$$1\ 2\ 1\ 2\ 2\ 1\ 1\ 0\ 0\ 2\ 2\ 0\ 2,$$

and $B^2 - J$ is the required circulant matrix with first row

$$0\ 1\ 0\ 1\ 1\ 0\ 0\ -\ -\ 1\ 1\ -\ 1.$$

Example 4.7. David Glynn [87] has further generalized this construction by observing that if A and B are the circulant incidence matrices of two projective planes of the same order and $C = AB - J$ is a $(0,1,-1)$ matrix, then C is a circulant weighing matrix.

In the above example, B, of order 13, has Hall polynomial

$$\psi(x) = x^0 + x^1 + x^3 + x^9 ,$$

and

$$\psi(x^2) = x^0 + x^2 + x^5 + x^6 .$$

We can form the two inequivalent weighing matrices of order 13 by forming

$$B^2 - J \text{ and } AB^\top - J ,$$

where A and $B^\top$ have Hall polynomials $\psi(x^2)$ and $\psi(x^{-1})$, respectively. Hence we obtain circulant weighing matrices with Hall polynomials

$$\alpha(x) = x^1 + x^3 + x^4 - x^7 - x^8 + x^9 + x^{10} - x^{11} - x^{12}$$

and

$$\beta(x) = x^2 + x^4 + x^5 + x^6 - x^7 - x^8 + x^{10} - x^{11} + x^{12}\,.$$

The first rows of the weighing matrices for $\alpha(x)$ and $\beta(x^2)$ are

$$0\ 1\ 0\ 1\ 1\ 0\ 0\ -\ -\ 1\ 1\ -\ 1$$

and

$$0\ -\ 0\ -\ 1\ 0\ 0\ 1\ 1\ -\ 1\ 1\ 1,$$

which are clearly inequivalent.

Example 4.8 (Kovacs' second method). (We refer the reader to Hughes and Piper [108] or Dembowski [40] for any unexplained terms in this and the next example.) $L_i = \{0+i, 1+i, 3+i, 9+i\}$ are the lines of a projective geometry. $L^2 = \{0,2,5,6\}$ is an oval with the property that any two of its translates $\{0+i, 2+i, 5+i, 6+i\}$ have precisely one point in common. We form a circulant matrix W with first row (a_{1j}) by choosing

$$a_{1j} = |L_j \cap L^2| - 1\,.$$

Hence the first row of W is

$$0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ -\ \ -\ \ 0\ \ 1\ \ -\ \ 1\ \ 0.$$

Example 4.9 (Kovacs' first method–for q odd). $(0,1,3,9)$ is a difference set modulo 13, so $L_i = \{0+i, 1+i, 3+i, 9+i\}$ are the lines of the projective geometry of order 3. Now $L_0^2 = \{0,2,5,6\}$ is an oval and, $L_j^2 = \{0+j, 2+j, 5+j, 6+j\}$ are also ovals, any two of which have precisely one common tangent. The tangents of L_0^2 are L_0, L_1, L_3 and L_9, so 1, 3, 4, 9, 10, 12 are exterior points, 0, 2, 5, 6 are on the oval, while 7, 8, 11 are interior to the oval.

We form our circulant weighing matrix by choosing the first row to have -1, 0, 1 in the $(0,i)$ position $(i = 0,1,\ldots,12)$ according as i is interior on or exterior to the oval, i.e.,

$$\begin{array}{cccccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & - & - & 1 & 1 & - & 1 \end{array} \tag{4.1}$$

The translates of the oval $L_0^{-1} = \{0,4,10,12\}$ also satisfy the unique common tangent condition; from this oval, we get the first row

$$0\ \ 1\ \ -\ \ 1\ \ 0\ \ -\ \ -\ \ 1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0. \tag{4.2}$$

Map $i \mapsto -2i$; then 4.2 becomes

$$0\ -\ 0\ -\ 1\ 0\ 0\ 1\ 1\ -\ 1\ 1\ 1. \tag{4.3}$$

Now 4.1 and 4.3 are inequivalent.

Remark 4.4. Choosing $r = 2$ and -1 in the example gives inequivalent $W(13,9)$. It is interesting to consider what values of r will give different solutions.

4.5 Constructions for Hadamard Matrices, $W(h,h)$, and Weighing Matrices, $W(h,h-1)$

Definition 4.5. A matrix $A = I + S$ will be called *skew-type* if $S^\top = -S$.

We recall the following:

Definition 4.6. A $(0,1,-1)$ matrix $W = W(p,k)$ of order p satisfying

$$WW^\top = kI_p$$

is called a *weighing matrix of order* p and *weight* k or simply a *weighing matrix*. A $W(p,p)$ is called an *Hadamard matrix*. A $W = W(p,k)$ for which $W^\top = -W$ is called a *skew-weighing matrix*, and an Hadamard matrix $H = I + S$ for which $S^\top = -S$ is called a *skew-Hadamard matrix*. A $W = W(p,p-1)$ satisfying $W^\top = W$, $p \equiv 2 \pmod 4$ is called a *symmetric conference matrix*.

Definition 4.7 (C-Matrix). A $(0,\pm 1)$ matrix, M, will be called a *C-matrix* if $\frac{1}{2}(M \pm M^\top)$ is also a $(0,\pm 1)$ matrix.

Remark 4.5. To help the reader compare with other literature we note conference matrices ($M = M^\top$) and skew-Hadamard matrices ($M = -M^\top$) are also called C-matrices.

Weighing matrices have long been studied in order to find optimal solutions to the problem of weighing objects whose weights are small relative to the weights of the moving parts of the balance being used. It was shown by Raghavarao [163], [164] that if the variance of the errors in the weights obtained by individual weighings is σ^2 (it is assumed the balance is not biased and the errors are mutually independent and normal), then using a $W(p,k)$ to design an experiment to weigh p objects will give a variance of $\frac{\sigma^2}{k}$. Indeed, for an Hadamard matrix the variance is $\frac{\sigma^2}{p}$, which is optimal for $p \equiv 0 \pmod 4$, and for a symmetric conference matrix the variance is $\frac{\sigma^2}{p-1}$, which is optimal for $p \equiv 2 \pmod 4$.

Sloane and Harwitt [195] survey the application of weighing matrices to improve the performance of optical instruments such as spectrometers.

Spectrometers measure the intensity of a dispersed spectrum at a finite number (n, say) of wavelengths. According to Ibbett, et al [112], either one detector scans the screen, making the n measurements sequentially, or else the n measurements are made simultaneously by a detector with spatial resolution. The first method has the disadvantage of not being able to compensate for variations in the intensity of the signal, while the second approach suffers the disadvantage of a lower signal-to-noise ratio (Ibbett, et al [112]).

A modification can be made to the second system which improves the signal-to-noise ratio. This is achieved by using a weighing matrix as square mask, where 1 is clear, 0 is opaque and -1 is a mirror (180° phase shift). Again the variance of the estimates of the wavelengths made using a mask of weight is $\frac{1}{n}$ of the estimates when measured separately.

Sloane and Harwitt [195] also indicate that weighing designs are applicable to other problems of measurements (such as lengths, voltages, resistances, concentrations of chemicals, etc.) in which the measure of several objects is the sum (or a linear combination) of the individual measurements.

The following properties of Hadamard matrices and weighing matrices are easily proved.

Lemma 4.11. *Let $U = U(p_1,k_1)$ and $V = V(p_2,k_2)$ be weighing matrices. Then $W = U \times V$ is a weighing matrix of order p_1p_2 and weight k_1k_2.*

Corollary 4.8. *Since $\left[\begin{smallmatrix} 1 & 1 \\ 1 & - \end{smallmatrix}\right]$ is a $W(2,2)$, there are Hadamard matrices of order 2^t, t a positive integer.*

Lemma 4.12 (Paley Lemma or Paley Core). *Let p be a prime power. Then there is a $W = W(p+1,p)$ for which $W^\top = (-1)^{\frac{1}{2}(p-1)}W$. If $p \equiv 3 \pmod 4$, then $W + I_p$ is a $W(p+1,p+1)$.*

Proof. Let $a_0, a_1, \ldots, a_{p-1}$ be the elements of $GF(p)$ numbered so that

$$a_0 = 0, \quad a_{p-i} = -a_i, \quad i = 1, \ldots, p-1\,.$$

Define $Q = (x_{ij})$ by

$$x_{ij} = \chi(a_j - a_i) = \begin{cases} 0 & \text{if } i = j, \\ 1 & \text{if } a_j - a_i = y^2 \text{ for some } y \in GF(p), \\ -1 & \text{otherwise.} \end{cases}$$

Now Q is a type 1 matrix with the properties that

$$\begin{aligned} QQ^\top &= pI - J, \\ QJ &= JQ = 0, \\ Q^\top &= (-1)^{\frac{1}{2}(p-1)}Q. \end{aligned}$$

This follows since exactly half of $a_1, \ldots, a_{p-1}$ are squares, -1 is a square for $p \equiv 1 \pmod 4$ but not for $p \equiv 3 \pmod 4$, and

$$\sum_y \chi(y)\chi(y+c) \;=\; \sum_y \chi\left(y^2\right)\chi\left(1+cy^{-1}\right) \;=\; \sum_{z\neq 1}\chi(x) \;=\; -1.$$

Let e be the $1 \times p$ vector of all ones. Then

$$W = \begin{bmatrix} 0 & e \\ (-1)^{\frac{1}{2}(p-1)}e^\top & Q \end{bmatrix}$$

is the required matrix. If $p \equiv 3 \pmod 4$, $W + I_p$ is a $W(p+1, p+1)$. □

Notation 4.2. Q is known as the *Paley core.*

Corollary 4.9. *There are Hadamard matrices of order $p+1$ where $p \equiv 3 \pmod 4$ is a prime power, and of order $2(p+1)$ where $p \equiv 1 \pmod 4$ is a prime power.*

Proof. For $p \equiv 3 \pmod 4$ use $W + I$; for $p \equiv 1 \pmod 4$ use $\begin{bmatrix} W+I & W-I \\ W-I & -W-I \end{bmatrix}$. □

Corollary 4.10. *There are Hadamard matrices of order $2^t \prod (p_i^{r_i} + 1)$ where $p_i^{r_i}$ are prime powers and t, an integer, is > 0 if $p_j^{r_j} \equiv 1 \pmod 4$, for some j, and ≥ 0 otherwise.*

Proof. Use Lemma 4.11 and Corollary 4.10. □

It is conjectured that:

*Conjecture 4.1 (**Hadamard Conjecture**).* There exists an Hadamard matrix of order 4t for every positive integer t.

Conjecture 4.2 (Jennifer Wallis [232]). There exists a weighing matrix $W(4t, k)$, $k = 0, 1, \ldots, 4t$, for every positive integer t.

This conjecture, of course, includes the Hadamard Conjecture.

Remark 4.6. There is now considerable literature devoted to *circulant weighing matrices.* Some of the authors are Ang, Arasu, Hain, Mac, Ma, Mullin, Seberry and Strassler [6, 7, 9–11, 153, 201] . We do not pursue this topic, though extremely interesting, here.

Definition 4.8. We say that the weighing matrix $W = W(2n, k)$ is *constructed from two circulant matrices M, N* of order n if

$$W = \begin{bmatrix} M & N \\ N^\top & -M^\top \end{bmatrix}.$$

Example 4.10.

$$M = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \qquad \text{and} \qquad N = \begin{bmatrix} - & 1 & 1 \\ 1 & - & 1 \\ 1 & 1 & - \end{bmatrix}$$

of order 3 satisfy $MM^\top + NN^\top = 5I$. Then

$$W = \begin{bmatrix} M & N \\ N^\top & -M^\top \end{bmatrix} = \left[\begin{array}{ccc|ccc} 0 & 1 & 1 & - & 1 & 1 \\ 1 & 0 & 1 & 1 & - & 1 \\ 1 & 1 & 0 & 1 & 1 & - \\ \hline - & 1 & 1 & 0 & - & - \\ 1 & - & 1 & - & 0 & - \\ 1 & 1 & - & - & - & 0 \end{array}\right]$$

is a $W(6,5)$ constructed from two circulant matrices.

Theorem 4.7 (Goethals and Seidel [88]). *Let $q \equiv 1 \pmod 4$ be a prime power; then there is a $W(q+1,q)$ of the form*

$$S = \begin{bmatrix} A & B \\ B & -A \end{bmatrix}$$

with zero diagonal and square circulant sub-matrices A and B.

Proof. Let z be any primitive element of $GF(q^2)$, the quadratic extension of $GF(q)$. We choose any basis of V the vector space of dimension 2 over $GF(q^2)$. With respect to this basis, v is defined by the matrix

$$(v) - \tfrac{1}{2} \begin{bmatrix} z^{q-1} + z^{1-q} & (z^{q-1} - z^{1-q}) z^{\frac{1}{2}(q+1)} \\ (z^{q-1} - z^{1-q}) z^{-\frac{1}{2}(q+1)} & z^{q-1} + z^{1-q} \end{bmatrix},$$

which actually has its elements in $GF(q)$. Then $\det(v) = 1$, and the eigenvalues of v are z^{q-1} and z^{1-q}, both elements of $GF(q^2)$ whose $\frac{1}{2}(q+1)$-th power, and no smaller, belongs to $GF(q)$. Hence v acts on the projective line $PG(1,q)$ as a permutation with period $\frac{1}{2}(q+1)$ without fixed points. This divides the points of $PG(1,q)$ into two sets of transitivity, each containing $\frac{1}{2}(q+1)$ points. In addition, w defined by the matrix

$$(w) = \begin{bmatrix} 0 & z^{q+1} \\ 1 & 0 \end{bmatrix}$$

has $\chi \det(w) = -\chi(-1)$. The eigenvalues of w are $\pm z^{\frac{1}{2}(q+1)}$ elements of $GF(q^2)$ whose square is in $GF(q)$. Hence w acts on $PG(1,q)$ as a permutation of period 2, which maps any point of one set of transitivity, defined above by v, into the other set. Indeed, for $i = 1, \ldots, \frac{1}{2}(q+1)$, the mapping $v^i w$ has no eigenvalue in $GF(q)$. Note $vw = wv$.

Finally, we represent the $q+1$ points of $PG(1,q)$, $x_0, x_1, \ldots, x_q$, by the following $q+1$ vectors in V:

$$x, v(x), v^2(x), \ldots, v^{\frac{1}{2}(q-1)}(x), w(x), vw(x), \ldots, v^{\frac{1}{2}(q-1)}w(x).$$

We define

$$S = \chi \det(x_i, x_j).$$

Observing that any linear mapping $u\colon V \to V$ satisfies

$$\det(u(x), u(y)) = \det u \cdot det(x, y),$$

for all $x, y \in V$, we see that

$$\det(v^i w(x), v^j w(x)) = \det(w) \cdot \det(v^i(x), v^j(x)) = \det(w) \cdot \det(x, v^{j-i}(x)),$$
$$\det(v^i(x), v^j w(x)) = -\det(v^i w(x), v^j(x)) = \det(v^j(x), v^i w(x)),$$
$$\det(v^i(x), v^j(x)) = -\det(v^{\frac{1}{2}(q+1)+i}, v^j(x)),$$

and so S has the required form. □

Example 4.11. Let $q = 5$ and z be a root of $z^2 + z + 2 = 0$ (a primitive polynomial over $GF(5^2)$). Then

$$z^4 = 3z+2, \quad z^{-4} = z^{20} = 2z+4, \quad z^3 = 4z+2, \quad z^{-3} = z^{21} = 2z+1, \quad z^6 = 2.$$

Hence

$$(v) = \tfrac{1}{2}\begin{bmatrix} z^4 + z^{-4} & (z^4 - z^{-4})z^3 \\ (z^4 - z^{-4})z^{-3} & z^4 + z^{-4} \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix}$$

and

$$(w) = \begin{bmatrix} 0 & z^6 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}.$$

We now choose some vector x, say, $x = \left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$. Then

$$x_0 = x = \left[\begin{smallmatrix}1\\0\end{smallmatrix}\right], \quad x_1 = v(x) = \left[\begin{smallmatrix}3\\2\end{smallmatrix}\right], \quad x_3 = v^2(x) = \left[\begin{smallmatrix}2\\2\end{smallmatrix}\right],$$
$$x_4 = w(x) = \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right], \quad x_5 = vw(x) = \left[\begin{smallmatrix}4\\3\end{smallmatrix}\right], \quad x_6 = v^2 w(x) = \left[\begin{smallmatrix}4\\2\end{smallmatrix}\right].$$

Since $\chi(1) = \chi(4) = 1$ and $\chi(2) = \chi(3) = -1$,

$$\det(x_i, x_j) = \left[\begin{array}{ccc|ccc} 0 & 2 & 2 & 1 & 3 & 2 \\ 3 & 0 & 2 & 3 & 1 & 3 \\ 3 & 3 & 0 & 2 & 3 & 1 \\ \hline 4 & 2 & 3 & 0 & 1 & 1 \\ 2 & 4 & 2 & 4 & 0 & 1 \\ 3 & 2 & 4 & 4 & 4 & 0 \end{array}\right] \text{ and } \chi\det(x_i x_j) = \left[\begin{array}{ccc|ccc} 0 & - & - & 1 & - & - \\ - & 0 & - & - & 1 & - \\ - & - & 0 & - & - & 1 \\ 1 & - & - & 0 & 1 & 1 \\ - & - & 1 & 1 & 1 & 0 \end{array}\right].$$

The next corollary was first explicitly stated by Turyn.

Corollary 4.11 (Turyn [218]). *Let $p \equiv 1 \pmod 4$ be a prime power. Then there exist four circulant symmetric matrices*

$$X_1 = I + A, \quad X_2 = I - A, \quad X_3 = X_4 = B$$

of order $\frac{1}{2}(p+1)$ which satisfy

$$\sum_{i=1}^{4} X_i X_i^\top = 2(p+1) I_{\frac{1}{2}(p+1)}\,.$$

These four matrices will be called *Williamson matrices* as they are circulant and symmetric.

Proof. Construct A and B as in the theorem. □

Note that the next four matrices satisfy the additive property but are not circulant but pairwise amicable, so are called *Williamson type matrices* (see Definition 4.16).

Corollary 4.12 (J. Wallis [235]). *Let $p \equiv 1 \pmod 4$ be a prime power; then there exist four symmetric $(1,-1)$ matrices X_1, X_2, X_3, X_4 of order $\frac{1}{2}p(p+1)$ which satisfy*

$$\sum_{i=1}^{4} X_i X_i^\top = 2p(p+1) I_{\frac{1}{2}p(p+1)}, \quad X_i X_j^\top = X_j X_i^\top\,.$$

Equivalently, there are Williamson type matrices of order $\frac{1}{2}p(p+1)$.

Proof. Construct A and B as in the theorem, and Q of order p as in the proof of Lemma 4.12. Then

$$\begin{aligned} X_1 &= (I \times J) + (A \times (I+Q))\,,\\ X_2 &= B \times (I+Q)\,,\\ X_3 &= (I \times J) + (A \times (I-Q))\,,\\ X_4 &= B \times (I-Q) \end{aligned}$$

are the required matrices. These type 1 matrices are symmetric. □

There are two very tough problems concerning skew Hadamard matrices. The first being the existence and construction of such matrices, the second being the number of equivalence classes. Existence results fall into two types: those constructed using four suitable complementary sequences and those constructed using linear algebra and number theory. Although the existence problem, via algebraic and number theoretic methods, has been widely studied by many researchers including Spence, Whiteman and Yamada, there many orders for which skew Hadamard matrices have not been constructed yet

(indeed there is no asymptotic existence theorem known for skew Hadamard matrices, see Chapter 9.)

Good matrices, which are four circulant ± 1 matrices of order n, constructed using four suitable complementary sequences and used in the Goethals-Seidel array to construct skew Hadamard matrices of smaller order $4n$ (orders ≤ 400), first appeared in the PhD Thesis of Jennifer (Seberry) Wallis [240]: there the matrices were given no name. Extensive computer searches have been carried out by many authors including Blatt, Đoković, Fletcher, Georgiou, Goethals, Hunt, Kotserias, Koukouvinos, Seberry, W. D. Smith, Seidel, Stylianou, Szekeres and X-M Zhang (also K. Balasubramanian in chemistry) see, for example, [24, 41, 42, 61].

In [240] good matrices were given for $n = 1, \cdots, 15, 19$ and in [229] for $n = 23$. Hunt [109] gave the matrices for $n = 1, \cdots, 25$. Later Szekeres [206] gave a list for orders $n = 1, \cdots, 31$. Đoković [42, 45] provided orders $n = 33$, 35, 43, 47, 97 and 127. Then Georgiou, Koukouvinos and Stylianou [74] provided 37, 39. Đoković [47] says that only one set of supplementary difference sets, (41;20,20,16,16;31), for 41 remains to be searched. Fletcher, Koukouvinos and Seberry [61] provided order 59.

We note that while there are no Williamson matrices of order 35 and 59 there are good matrices of order 35 and 59. [178, 236].

These results are summarised (partly) in part SV of the table of existence theorems. Suitable complementary sequences have not yet been found for orders 69 and 89 (however skew Hadamard matrices are known for orders 8×69 and 16×89 by algebraic methods).

Summary 4.1. Table 4.4 summarizes the existence of skew-Hadamard matrices.

The more recent status on known results and open problems on the existence of skew-Hadamard matrices of order $2^t n$, n odd, $n \leq 500$, are given in Table 1 of [138]. In Table 4.5, we write $n(t)$ if the skew-Hadamard matrix of order $2^t n$ exists. An $n(.)$ means that a skew-Hadamard matrix of order $2^t n$ is not yet known for any t. The values $n < 500$, missing from Table 4.5, indicate that a skew-Hadamard matrix of order $4n$ exists. Seberry Wallis [230] conjectured that skew-Hadamard matrices exist for all dimensions divisible by 4.

Table 4.5 modifies that of Koukouvinos and Stylianou [138] with more recent results.

Table 4.6 gives the current knowledge of existence for Hadamard matrices not in Geramita-Seberry [80, p.416], nor in Seberry-Yamada [188, p.543-544] which are unresolved.

Table 4.4 Skew-Hadamard existence

SI	$2^t \prod k_i$	t, r_i, all positive integers $k_i = p_i^{r_i} + 1 \equiv 0 \pmod 4$, p_i a prime.
SII	$(p-1)^u + 1$	p the order of a skew-Hadamard matrix, $u > 0$ an odd integer.
$SIII$	$2(q+1)$	$q \equiv 5 \pmod 8$ a prime power.
SIV	$2^s(q+1)$	$q = p^t$ is a prime power such that $p \equiv 5 \pmod 8$, $t \equiv 2 \pmod 4$, $s \geq 1$ an integer.
SV	$4m$	$m \in \{$odd integers between 3 and 39 inclusive$\}$
SVI	$m'(m'-1)(m-1)$	m and m' the orders of amicable Hadamard matrices, where $(m-1)\frac{m'}{m}$ is the order of a skew-Hadamard matrix.
$SVII$	$4(q+1)$	$q = 8f+1$ f odd is a prime power.
$SVIII$	$(\lvert t\rvert+1)(q+1)$	$q = s^2 + 4t^2 \equiv 5 \pmod 8$ is a prime power, and $\lvert t\rvert+1$ is the order of a skew-Hadamard matrix (Wallis [234]).
SIX	$4(1+q+q^2)$	where q is a prime power and $\begin{cases} 1+q+q^2 & \text{is a prime } \equiv 3,5, \text{ or } 7 \pmod 8; \text{ or} \\ 3+2q+2q^2 & \text{is a prime power ([197]).} \end{cases}$
SX	hm	h the order of a skew-Hadamard matrix, m the order of amicable Hadamard matrices.

4.6 The Goethals-Seidel Array and other constructions using circulant matrices – constraints on constructions using circulant matrices

In studying skew-Hadamard matrices (orthogonal designs $OD(n;1,n-1)$), Szekeres realized that none were known for quite small orders, including 36. To find this matrix Goethals and Seidel gave an array (described in this section) which uses circulant matrices. This and its generalization by Wallis and Whiteman have proved invaluable in the construction of Hadamard matrices, and we will see that they play a major role in constructing orthogonal designs. Here we have another example of a method devised to give a single case having far-reaching uses.

We now consider the use of circulant matrices in constructing orthogonal designs. All the constructions using circulants require that we find circulants $A_1, \ldots, A_s$ of order n satisfying the additive property:

Table 4.5 Existence of skew-Hadamard matrices [a]

69(3)	89(4)						
101(10)	107(10)	119(4)	149(4)				
153(3)	167(4)	177(12)	179(8)	191(.)	193(3)		
201(3)	205(3)	209(4)	213(4)	223(3)	225(4)	229(3)	233(4)
235(3)	239(4)	245(4)	249(4)	251(6)	253(4)	257(4)	259(5)
261(3)	265(4)	269(8)	275(4)	277(5)	283(11)	285(3)	287(4)
289(3)	295(5)	299(4)					
301(3)	303(3)	305(4)	309(3)	311(26)	317(6)	319(3)	325(5)
329(6)	331(3)	335(7)	337(18)	341(4)	343(6)	345(4)	347(18)
349(3)	353(4)	359(4)	361(3)	369(4)	373(7)	377(6)	385(3)
389(15)	391(4)	397(5)					
401(10)	403(5)	409(3)	413(4)	419(4)	423(4)	429(3)	433(3)
435(4)	441(3)	443(6)	445(3)	449(.)	451(3)	455(4)	457(9)
459(3)	461(17)	465(3)	469(3)	473(5)	475(4)	479(12)	481(3)
485(4)	487(5)	489(3)	491(46)	493(3)			

[a] Koukouvinos and Stylianou [138, p2728] © Elsevier

Table 4.6 Hadamard matrix orders which are unresolved

107(10)	167(3)	179(3)	191(3)			
213(4)	223(3)	239(4)	249(3)	251(3)	269(8)	283(3)
303(3)	311(26)	335(7)	347(3)	359(4)	373(7)	
419(4)	443(6)	445(3)	479(12)	487(3)	491(46)	

$$\sum_{i=1}^{s} A_i A_i^{\top} = fI, \text{ where } f = \sum_{j=1}^{r} s_j x_j^2 .$$

One question we shall explore in this section is the restrictions that must be placed on $(s_1, \ldots, s_r)$ in order that such circulant matrices exist.

This problem is analogous to the problems we discussed in Chapter 3 when we discovered algebraic limitations on orthogonal designs.

Conditions imposed on $(s_1, \ldots, s_r)$ in order to construct orthogonal designs from circulants is closer to the combinatorial spirit of the subject. Although there is no reason to believe that all the orthogonal designs we look for in orders $4n$ or $8n$, n odd, can be expected to come from circulants (or negacyclics), we will find they usually do. In cases where they do not, especially in orders divisible by 8, negacyclic matrices have proved invaluable. See [67, 68, 78, 101, 105,108,126] among others. Thus circulant matrices are important constructive tools, and we should decide what limitations there are on their use. We also note that circulant matrices are amenable to algebraic assault because of their

relationship to roots of unity. This aspect to circulants will become more apparent when we discuss Griffin' s work on Golay sequences in Section 7.2.

We first give constructions using circulants and then consider restrictions on their use.

Proposition 4.1. *Suppose there exist two circulant matrices B of order n satisfying*

$$AA^\top + BB^\top = fI_n\,.$$

Further suppose that R is the back diagonal matrix; then

$$H = \begin{bmatrix} A & B \\ -B^\top & A^\top \end{bmatrix} \text{ or } G = \begin{bmatrix} A & BR \\ -BR & A \end{bmatrix} \text{ is a } W(2n, f)\,,$$

when A, B are $(0,1,-1)$ matrices, and an orthogonal design $OD(2n; u_1, u_2, \ldots, u_s)$ on $x_1, \ldots, x_s$ when $f = \sum_{i=1}^{s} u_i x_i^2$.

Further, H and G are skew or skew-type if A is skew or skew-type.

Proof. A straightforward verification. □

Remark 4.7. We note here that these properties remain true if A and B are type 1 matrices and R is the appropriately chosen matrix (see Lemmas 4.4 to 4.7).

Definition 4.9. We say that an orthogonal design is *constructed from two circulant matrices M, N* of order n if

$$W = \begin{bmatrix} M & N \\ -N^\top & M^\top \end{bmatrix} \quad \text{or} \quad W = \begin{bmatrix} M & NR \\ -NR & M \end{bmatrix}.$$

Example 4.12.

$$A = \begin{bmatrix} x_l & x_2 & -x_2 \\ -x_2 & x_1 & x_2 \\ x_2 & -x_2 & x_1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & x_2 & x_2 \\ x_2 & 0 & x_2 \\ x_2 & x_2 & 0 \end{bmatrix}$$

of order 3 satisfy

$$AA^\top + BB^\top = (x_1^2 + 4x_2^2)I\,.$$

Thus

$$H = \begin{bmatrix} A & B \\ -B^\top & A^\top \end{bmatrix} = \left[\begin{array}{ccc|ccc} x_1 & x_2 & -x_2 & 0 & x_2 & x_2 \\ -x_2 & x_1 & x_2 & x_2 & 0 & x_2 \\ x_2 & -x_2 & x_1 & x_2 & x_2 & 0 \\ \hline 0 & -x_2 & -x_2 & x_1 & -x_2 & x_2 \\ -x_2 & 0 & -x_2 & x_2 & x_1 & -x_2 \\ -x_2 & -x_2 & 0 & -x_2 & x_2 & x_1 \end{array}\right]$$

and

$$G = \begin{bmatrix} A & BR \\ -BR & A \end{bmatrix} = \left[\begin{array}{ccc|ccc} x_1 & x_2 & -x_2 & 0 & x_2 & x_2 \\ -x_2 & x_1 & x_2 & x_2 & x_2 & 0 \\ x_2 & -x_2 & x_1 & x_2 & 0 & x_2 \\ \hline 0 & -x_2 & -x_2 & x_1 & x_2 & -x_2 \\ -x_2 & -x_2 & 0 & -x_2 & x_1 & x_2 \\ -x_2 & 0 & -x_2 & x_2 & -x_2 & x_1 \end{array}\right]$$

are orthogonal designs $OD(6;1,4)$ on x_1, x_2. H and G are constructed from two circulants.

Theorem 4.8 (Goethals-Seidel [89]). *Suppose there exist four circulant matrices A, B, C, D of order n satisfying*

$$AA^\top + BB^\top + CC^\top + DD^\top = fI_n\,.$$

Let R be the back diagonal matrix. Then GS, henceforth called the Goethals-Seidel array,

$$GS = \begin{bmatrix} A & BR & CR & DR \\ -BR & A & D^\top R & -C^\top R \\ -CR & -D^\top R & A & B^\top R \\ -DR & C^\top R & -B^\top R & A \end{bmatrix}$$

is a $W(4n,f)$ when A, B, C, D are $(0,1,-1)$ matrices, and an orthogonal design $OD(4n;u_1,u_2,\ldots,u_s)$ on the variables $(x_1,x_2,\ldots,x_s)$ when A, B, C, D have entries from $\{0,\pm x_1,\ldots,\pm x_s\}$ and

$$f = \sum_{j=1}^{s} u_j x_j^2\,.$$

Further, GS is skew or skew-type if A is skew or skew-type.

This theorem was modified by Wallis and Whiteman to allow the circulant matrices to be generalized to types 1 and 2.

Lemma 4.13 (Wallis-Whiteman [242]). *Let A, B, D be type 1 matrices and C a type 2 matrix defined on the same abelian group of order n. Then if*

$$AA^\top + BB^\top + CC^\top + DD^\top = fI_n\,,$$
$$H = \begin{bmatrix} A & B & C & D \\ -B^\top & A^\top & -D & C \\ -C & D^\top & A & -B^\top \\ -D^\top & -C & B & A^\top \end{bmatrix}$$

is a $W(4n,f)$ when A, B, C, D are $(0,1,-1)$ matrices, and an orthogonal design $OD(4n;u_1,u_2,\ldots,u_s)$ on the commuting variables $(x_1,x_2,\ldots,x_s)$ when A, B, C, D have entries from $0,\pm x_1,\ldots,\pm x_s$ and

$$f = \sum_{j=1}^{s} u_j x_j^2 .$$

Further, H is skew or skew-type if A is skew or skew-type.

Example 4.13. We construct an orthogonal design $OD(12;3,3,3,3)$ in order 12 by using the circulant matrices with first rows, respectively,

$$abc, \qquad \bar{b}ad, \qquad \bar{c}\bar{d}a, \qquad \bar{d}c\bar{b},$$

in the Goethals-Seidel array (Theorem 4.8). This is illustrated in Table 4.15. See also Example 4.21. □

To illustrate the use of Lemma 4.13 recall that in Example 4.3 we gave a type 1 matrix A and a type 2 matrix B defined on the additive group G of $GF(3^2)$ ($G = Z_3 \times Z_3$). Let R be the matrix defined on G by Lemma 4.7. Notice that by Lemma 4.7 $AR = B$ and $BR = A$. Also, R is a type 2 matrix.

Let $W = \begin{bmatrix} 0 & I_3 & 0 \\ 0 & 0 & I_3 \\ I_3 & 0 & 0 \end{bmatrix}$; then W is the type 1 $(1,0)$ incidence matrix generated by $\{2x\}$ (we are using the notation of Example 4.3).

Let $L = \begin{bmatrix} J_3 & 0 & 0 \\ 0 & J_3 & 0 \\ 0 & 0 & J_3 \end{bmatrix}$; then L is the type 1 $(1,0)$ incidence matrix generated by the subgroup $\{0,1,2\}$ of G. Since the identity matrix is always a type 1 matrix for a group G (for which the identity element of the group is the first element of G), we obtain that $U = L - I + W$ and $V = I + W^\top$ are type 1 matrices on G. (See Lemma 4.5.)

Set $X_1 = aI + bA$, $X_2 = b(U+V)$, $X_4 = b(U-V)$ and $X_3 = bB - aR$. Then X_1, X_2 and X_4 are type 1 matrices and X_3 is a type 2 matrix. By inspection, all entries are from $0, \pm a, \pm b$. Also

$$\sum_{i=1}^{4} X_i X_i^\top = (2a^2 + 26b^2) I_9 .$$

Thus these matrices may be used in place of A, B, C, D in Lemma 4.13 to give an $OD(36;2,26)$.

The most general theorem we can give on using circulant matrices in the construction of orthogonal designs is

Theorem 4.9. *Suppose there is an orthogonal design $OD(m;u_1,u_2,\ldots,u_s)$ on the variables $x_1,x_2,\ldots,x_s$. Let $X_1,X_2,\ldots,X_s$, where $s \le \rho(n)$, be circulant (type 1) matrices of order n with entries from $\{0,\pm y_1,\ldots,\pm y_r\}$ which satisfy*

$$u_1 X_1 X_1^\top + u_2 X_2 X_2^\top + \cdots + u_s X_s X_s^\top = f I_n$$

(the additive property). Further suppose

1. *all X_i are symmetric, or*

2. at most one is not symmetric, or
3. $X_1,\ldots,X_{j-1}$ are symmetric and $X_j,\ldots,X_s$ are skew-symmetric.

Then if $f = v_1y_1^2 + v_2y_2^2 + \cdots + v_ry_r^2$, there is an $OD(mn;v_1,v_2,\ldots,v_r)$ on the commuting variables $(y_l,y_2,\ldots,y_r)$.

Proof. The main difficulty arises because the variables of the orthogonal design are commutative. When we replace commuting variables by matrices y_i, $i = 1,\ldots,s$, we have to ensure that the matrices pairwise satisfy

$$Y_iY_j^\top = Y_jY_i^\top \tag{4.4}$$

We established in Section 2 that if the Y_i are circulant and symmetric, equation (4.4) is satisfied. Also if Y_iR is back circulant (type 2) and Y is circulant (type 1), then equation (4.4) is satisfied. We also note that if Y_i and Y_j are skew-symmetric, the back circulant matrices Y_iR and Y_jR satisfy equation (4.4) since

$$(Y_iR)(Y_jR)^\top = Y_iRR^\top Y_j^\top = -Y_iY_j = Y_jY_i^\top = (Y_jR)(Y_iR)^\top.$$

Thus the result can be obtained in the first case by replacing each variable x_i, $i \neq j$, in the orthogonal design of order m by the circulant symmetric matrix X_i; in the second case the variable x_i is replaced by the back circulant matrix X_jR. The third result is obtained by replacing x_i, $i \neq j$, $j+1,\ldots,s$, by X_i, and $x_j,\ldots,x_s$ by $X_jR,\ldots,X_sR$. □

Example 4.14. There is an orthogonal design $OD(16;1,1,1,1,3,3,3,3)$ (we will see this in Chapter 5, Example 6.4(c)). Consider the circulant matrices X_i, with first rows

$$\begin{array}{llll} y_1y_2y_2\bar{y}_2\bar{y}_2 & y_2\bar{y}_2y_2y_2\bar{y}_2 & \bar{y}_2y_2y_2y_2y_2 & \bar{y}_2y_2y_2y_2y_2 \\ y_3y_4\bar{y}_4\bar{y}_4y_4 & \bar{y}_4y_3\bar{y}_3\bar{y}_3y_3 & \bar{y}_3y_3y_3y_3y_3 & \bar{y}_4y_4y_4y_4y_4 \end{array}$$

and call them respectively $X_1,\ldots,X_8$. Then

$$X_1X_1^\top + X_2X_2^\top + X_3X_3^\top + X_4X_4^\top + 3X_5X_5^\top + 3X_6X_6^\top + 3X_7X_7^\top + 3X_8X_8^\top = (y_1^2 + 19y_2^2 + 30y_3^2 + 30y_4^2)I_5.$$

We use part 2 of Theorem 4.9 to assert the existence of an orthogonal design $OD(80;1,19,30,30)$; the matrix X_1R is used to replace the first variable, and the circulant symmetric matrices $X_2,\ldots,X_8$ are used to replace the other variables.

We have noted that in Theorem 4.8 the only requirement was to have circulant matrices, but in Theorem 4.9 the internal structure of the circulant matrices was restricted severely. If the matrices are circulant and symmetric, we will loosely call this *Williamson criteria*, and if merely circulant, we will

call this *Goethals-Seidel criteria*. Thus in Theorem 4.8 we only had Goethals-Seidel criteria operating, but in Theorem 4.9 we were almost entirely limited to Williamson criteria.

4.7 Constraints on construction using circulant matrices

Of course we would like to use these constructions to form orthogonal designs, but first we must consider some combinatorial limitations on these methods (algebraic limitations on the types of orthogonal designs were discussed earlier).

Lemma 4.14. *Let A_i, $i = 1, 2, 3, \ldots, m$, be circulant matrices of order n where*

$$\sum_{i=1}^{m} A_i A_i^\top = \left(\sum_{j=1}^{r} s_j x_j^2 \right) I_n \,.$$

Suppose $A_i = \sum_{j=1}^{r} x_j A_{ij}$ and that $A_{ij} J = y_{ij} J$. Then

$$s_j = \sum_{j=1}^{m} y_{ij}^2 \,.$$

Proof. By definition

$$\sum_{i=1}^{m} (x_1 A_{i1} + x_2 A_{i2} + \ldots) \left(x_1 A_{i1}^\top + x_2 A_{i2}^\top + \ldots \right) = \left(s_1 x_1^2 + s_2 x_2^2 + \ldots \right) I \,.$$

So

$$\sum_{i=1}^{m} x_1^2 \left(A_{i1} \right) A_{i1}^\top + \sum_{i=1}^{m} x_2^2 \left(A_{i2} A_{i2}^\top \right) + \cdots = \left(s_1 x_1^2 + s_2 x_2^2 + \ldots \right) I \,,$$

and setting $x_j = 1$, $x_i = 0$, for $i \neq j$ we have

$$\sum_{i=1}^{m} A_{ij} A_{ij}^\top = s_j \,.$$

Post-multiplying by J gives

$$\sum_{i=1}^{m} y_{ij}^2 J = s_j J \,,$$

and equating coefficients gives the results. □

Remark 4.8. If $m = 4$ and we have four circulants A_1, A_2, A_3, A_4 such that

$$\sum_{i=1}^{4} A_i A_i^\top = \left(x_1^2 + s x_2^2\right) I_n \,,$$

n odd, then s must be the sum of three squares. For we may assume $A_1 = x_1 I + x_2 A_{12}$, $A_2 = x_2 A_{22}$, $A_3 = x_2 A_{32}$ and $A_4 = x_2 A_{42}$. Then by the lemma we have

$$y_{12}^2 + y_{22}^2 + y_{32}^2 + y_{42}^2 = s \,.$$

But $A_{12} = -A_{l2}^\top$, and the order of A_{12} is n(odd). So $y_{12} = 0$, and consequently s is the sum of three squares. This should be compared with Proposition 3.21.

4.8 Eades' Technique for Constructing Orthogonal Designs Using Circulant Matrices

The method outlined in this section has been used successfully to compute four variable orthogonal designs of order 20 and many but not all orthogonal designs of order 28, 36 and 44. Some success has been achieved with orthogonal designs of orders 18, 22, 26, 30, 44 and 52. The results of this computation are included in the the Appendices. The method can be extended to construct orthogonal designs in orders 24, 48, 56 and 72.

The method is presented as it applies to the Goethals-Seidel construction (Theorem 4.8), but there are no difficulties in extending the results for more general circulant constructions, such as those mentioned in orders 48 and 56 (see appendices).

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

$$\sum_{i=1}^{4} X_i X_i^\top = \left(\sum_{i=1}^{u} s_i x_i^2\right) I \,. \tag{4.5}$$

The existence of an orthogonal design $OD(4v; s_1, s_2, \ldots, s_u)$ follows from the Goethals-Seidel construction (Theorem 4.8).

Remark 4.9. 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 often be constructed using other methods (see Chapter 9).

Equation (4.5) has v^2 components, but since $X_i X_i^\top$ 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.

Definition 4.10. 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).

Definition 4.11. 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 $[r_1 r_2^\top, r_1 r_3^\top, \ldots, r_1 r_w^\top]$. Note that if $(d_1, d_2, \ldots, d_v)$ is the first row of $AA^\top$, 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 equation (4.5) if and only if

$$\sum_{j=1}^{4} m_{ij} = s_i \quad \text{for } 1 \le i \le u\,, \tag{4.6}$$

and

$$\sum_{j=1}^{4} b_j = 0, \quad \text{where } b_j \text{ is the IPV of } A_j\,. \tag{4.7}$$

In other words, to find a solution of equation (4.5) we need four circulant matrices with entries from $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ whose entry matrix has i^{th} row adding to s_i for $1 \le i \le u$ and whose IPV's add to zero.

Remark 4.10. The IPV is not the most efficient way in time or space to construct Hadamard matrices, but is valuable for orthogonal designs.

Definition 4.12. The *content* of a circulant matrix A with entries from $\{0, \pm x_1, \pm x_2, \ldots, x_u\}$ is the set of pairs $(\epsilon x_i, m)$ where $\epsilon x_i (\epsilon = \pm 1)$ occurs a non-zero number m times in the first row of A. Our next task is to show how the contents of solutions of equation (4.5) may be determined from the knowledge of the parameters $v, s_1, s_2, \ldots, s_u$.

Definition 4.13. Suppose that the rowsum of A_j 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 $M - abs(P)$. The content of A_i is determined by the i-th columns of the sum and fill matrices.

The following theorem may be used to find the sum matrix of a solution of equation (4.5).

Theorem 4.10 (Eades Sum Matrix Theorem [52]). *The sum matrix P of a solution of equation* (4.5) *satisfies*

$$PP^\top = diag(s_1, s_2, \ldots, s_u). \tag{4.8}$$

Proof. Suppose that A is a $v \times v$ circulant matrix with row sum 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

$$(JA)(A^\top J^\top) = a^2 JJ^\top = a^2 vJ\,.$$

But also

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

Hence $a^2 = b+2c$. Thus if (p_{ij}) and (m_{ij}) are the sum and entry matrices of a solution of equation (4.5), then since the sum of the sums of the entries of the IPV's is zero, it follows that

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

Expanding this equation and equating coefficients of $x_i x_j$ gives equation (4.8). □

Remark 4.11. (a) Note that the Sum Matrix Theorem 4.10 implies that a necessary condition for the existence of $OD(4v; s_l, s_2, \ldots, s_u)$ constructed by using the Goethals-Seidel array is the existence of a $u \times 4$ integral matrix P satisfying equation (4.8). In fact this theorem says that the only time we can hope to construct an orthogonal design $OD(n; s_1, s_2, s_3, s_4)$ using the Goethals-Seidel array in order $n \equiv 0 \pmod 4$ is when there is a 4×4 integer matrix p such that $PP^\top = diag(s_1, s_2, s_3, s_4)$. This is analogous to Proposition 3.23 of Chapter 3, which says that in orders $n \equiv 4 \pmod 8$ a rational family of type $[s_1, s_2, s_3, s_4]$ exists in order n if and only if there is a 4×4 *rational* matrix Q with $QQ^\top = diag(s_1, s_2, s_3, s_4)$. This also shows that, for four variable designs, the Goethals-Seidel approach will be less useful in orders divisible by a large power of 2.

(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 (4.5). 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 (4.5) formed by permuting the indices of A_i and 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 (4.5).

If the algebraic necessary conditions (Proposition 3.23) for the existence of $OD(4v; s_1, s_2, \ldots, s_u)$ hold, then the existence of a solution to (4.8) is guaranteed by a result of Pall (see Eades [53]).

In most cases, if the s_i are small (for instance, $s_1 + \cdots + s_u \leq 28$), then the solution of (4.8) is essentially unique and can be found easily by hand.

It is clear that if Q is the fill matrix of a solution of (4.5), then

$$\text{the entries of } Q \text{ are even non-negative integers}, \tag{4.9}$$

and if $M = (m_{ij}) = abs(P) + Q$, then M satisfies (4.6) and

$$\text{the sum of a column of } M \text{ is at most } v. \tag{4.10}$$

There may be a large number of matrices which satisfy (4.6), (4.9) and (4.10) (see Example 4.15), but the next two lemmata may be used to reduce the number of possibilities.

Lemma 4.15 (Eades). *Suppose that A is a circulant matrix of odd order v, with entries from $\{0,1,-1\}$ and with k non-zero entries in each row.*

(i) If $k \geq v-1$, then each entry of the IPV of A is odd.
(ii) 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 ij-th entry of A is a_{ij}, and denote by B_i the set

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

for $1 \leq i \leq v$. Each B_i contains $v-k$ elements. Also, since each column of A contains k non-zero 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 $v \geq k + \sqrt{k} + 1$. □

Lemma 4.16 (Eades). *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 equation (4.5) is $\begin{bmatrix} V \\ W \end{bmatrix}$ where V is $\ell \times r$ and W is $(u-\ell) \times (4-r)$. Then*

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

and

$$\sum_{j=r+1}^{4} A_j A_j^\top = \left(\sum_{i=\ell+1}^{u} s_i x_i^2 \right) I\,.$$

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 (3.2), (3.7), (3.8) and Lemmas 4.15 and 4.16, 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.

Example 4.15. The existence of an orthogonal design $OD(20;1,5,5,9)$ is listed in Geramita and Wallis [81] 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

$$\sum_{i=1}^{4} B_i B_i^\top = (x_1^2 + 5x_2^2 + 5x_3^2 + 9x_4^2)\, I. \tag{4.11}$$

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

$$P = \begin{bmatrix} 1 & & & \\ & 1 & 2 & \\ & -2 & 1 & \\ & & & 3 \end{bmatrix}. \tag{4.12}$$

(See Remark (b) after Theorem 4.10.)

Now there are eight 4×4 integral matrices which, on the basis of equations (4.6), (4.9), and (4.10) could be fill matrices.

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

$$(d)\begin{bmatrix} 2 & & & \\ & & & 2 \\ 2\,2\,2 & & & \end{bmatrix}, \quad (e)\begin{bmatrix} & 2 & & \\ & & 2 & \\ 4 & & & 2 \end{bmatrix}, \quad (f)\begin{bmatrix} & & 2 & \\ & 2 & & \\ 4 & & & 2 \end{bmatrix}, \tag{4.13}$$

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

However, four of these matrices can be discounted as possible fill matrices by using Lemmas 4.15 and 4.16.

Suppose that (B_1, B_2, B_3, B_4) has sum matrix P above (4.12) and fill matrix (4.13) (b). Then the entry matrix is

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

which satisfies equations (4.6) and (4.10). But the $(3,2)$-th entry of this entry matrix indicates by Lemma 4.15 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 (4.13)(b) is not the fill matrix of the B_i.

Suppose that (4.13)(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 (4.12) (see Remark (b) after Theorem 4.10). It follows by Lemma 4.15 that

$$C_1C_1^\top + C_2C_2^\top = (x_1^2 + 9x_2^2)I_5\,,$$

and thus, using the two-circulant construction, there is an $OD(10;1,9)$. This is impossible, as it implies the existence of an Hadamard matrix of order 10, and so (4.13)(f) is not the fill matrix of (B_1, B_2, B_3, B_4).

Similarly it can be shown that (4.13)(h) and (4.13)(e) are not possible.

Each of the possible fill matrices (4.13)(a), (c), (d), (g) could specify the contents of a solution of (4.11). 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 (4.13)(a) we need to find four 5×5 permutation matrices M_1, M_2, M_3, M_4 such that

$$\begin{aligned}
&(x_1, x_2, -x_2, x_3, -x_3)M_1\\
&(x_2, -x_3, -x_3, x_4, -x_4)M_2\\
&(x_2, x_2, x_3, x_4, -x_4)M_3\\
&(x_4, x_4, x_4, x_4, -x_4)M_4
\end{aligned}$$

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 (4.13)(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.

Definition 4.14. 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 $(12\ldots v)$. Let R denote the $v \times v$ back diagonal matrix (see Section 4.5). The subgroup of 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, $\frac{(v-1)!}{2}$. Thus the lists L_i in Step 4 contain at most $\frac{(v-1)!}{2}$ entries. A complete set of distinct coset representatives of $\langle T, R\rangle$ in S_v is easily seen to be $E = \{M \in S_v \colon M$ represents a permutation θ on $\{1, 2, \ldots, v\}$ which satisfies $v\theta = v$ and $1\theta \leq \frac{1}{2}(v-1)\}$. Thus to compute the list L_i in Step 4, we first write out the elements of $S = \{B \colon B$ 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.

Lemma 4.17. *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,

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

Symmetrising gives

$$a_i M_1 \left(T + T^{-1}\right) M_1^{-1} a_i^\top = a_i M_2 \left(T + T^{-1}\right) M_2^{-1} a_i^\top .$$

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. Hence either $T = MTM^{-1}$ or $T^{-1} = MTM^{-1}$. In either case, since the subgroup of S_v generated by T is self-centralising, 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 $\frac{(v-1)!}{2}$. However this is rare. For instance, if the content of A_i is $\{(\epsilon x_i, n_{\epsilon i}) : 1 \leq i \leq u, \epsilon = \pm 1\}$ then the subgroup

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

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 $\frac{v!}{m}$ entries of the list L_i, and often $\frac{v!}{m} < \frac{(v-1)!}{2}$. 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, a more sophisticated search algorithm needed to be employed (see Koukouvinos et.al. [59, 66–69, 71, 73, 102, 104, 105, 135]).

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 equations (4.6), (4.8), (4.9) and (4.10). Then the sum of the sums of the entries of the IPV's of the C_i is zero (see proof of Theorem 4.10). 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

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

then

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

Hence only $\frac{1}{2}(v-3)$ of the $\frac{1}{2}(v-1)$ components of the IPV's need to add to zero for equation (4.5) 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 $0 \le i \le v$. Now if the circulant matrix A has first row a, then the i-th entry of the IPV of A is $aT^{-i}a^\top$. Hence the IPV of the circulant matrix B with first row aN has i-th entry $aNT^{-i}N^{-1}a^\top$, that is, $aT^da^\top$. 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 $\{0, 1, \ldots, v-1\}$ 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

$$\theta:\ i \rightarrowtail \begin{cases} (id)^* & \text{if } 1 \le (id)^* \le w, \\ v-(id)^* & \text{otherwise.} \end{cases} \tag{4.14}$$

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 4.16 below. First, however, we show how the facts above may be used to construct a certain four variable orthogonal design of order 28.

Example 4.16. An orthogonal design $OD(28;1,1,1,25)$ 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

$$\sum_{i=1}^{4} V_i V_i^{\top} = (x_1^2 + x_2^2 + x_3^2 + 25x_4^2) I\,. \tag{4.15}$$

The conditions (4.6), (4.8), (4.9), (4.10) 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 (4.7)); thus V_4 has IPV $(3x_4^2, 3x_4^2, 3x_4^2)$. 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 (4.14), 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 (4.6), (4.8), (4.9), (4.10), 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 (4.15).

Example 4.16 completed: The index of the normalizer of $\langle T\rangle$ in S_5 is 6, and so there are at most six 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 equation (4.11) has sum matrix P (4.12) and fill matrix (4.13)(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

$$\begin{aligned}
&(x_1, x_2, -x_3, x_3, -x_2),\\
&(x_2, x_4, -x_3, -x_3, -x_4),\\
&(x_3, x_2, x_4, -x_4, x_2),\\
&(-x_4, x_4, x_4, x_4, x_4),
\end{aligned}$$

respectively, then the B_i satisfy equation (4.11).

Using similar methods it is possible to show that it is impossible to construct a $(1,3,6,8)$, $(2,2,5,5)$, or $(3,7,8)$ in order 20 by using four circulants. It can also be shown that, while a $(4,9)$ exists in order 14, it is impossible to construct it from two circulants.

For ease of reference we summarize these results as:

Lemma 4.18 (Eades [52]). *It is not possible to find four circulant matrices A_1, A_2, A_3, A_4 of order 5 with entries the commuting variables x_1, x_2, x_3, x_4, and 0 which satisfy*

$$\sum_{i=1}^{4} A_i A_i^{\top} = \sum_{j=1}^{4} \left(s_j x_j^2\right) I_5,$$

where (s_1, s_2, s_3, s_4) is $(1,4,4,9)$, $(1,3,6,8)$, $(2,2,5,5)$ or $(3,7,8)$. Equivalently, it is not possible to use four circulant matrices in the Goethals-Seidel array to construct orthogonal designs of these types in order 20.

Lemma 4.19 (Eades). *It is not possible to construct the orthogonal design $OD(14;4,9)$ using two circulant matrices.*

Horton and Seberry [107] have undertaken a full search for $OD(n;4,9)$ for small n showing that, often, the necessary conditions for these orthogonal designs are not sufficient. The theoretical reasons for this strange result is undetermined.

Remark 4.12. It would be interesting to know if orthogonal designs of types $(1,4,4,9)$, $(1,3,6,8)$, $(2,2,5,5)$ or $(3,7,8)$ are impossible to construct by any method in order 20. If that were so, it would make the construction method by circulants assume even greater importance. We shall not even hazard a guess here, although experience should indicate that some of these designs will be impossible to construct by any method. This question is still unresolved after 30 years.

Remark 4.13. Since there is a strong relationship between circulant and negacyclic matrices with additive properties, it might appear fruitful to consider the "sum" and "fill" approach to finding desirable negacyclic matrices. However this IPV vector seems harder to constrain.

4.9 Some Arrays for Eight Circulants

Unfortunately, in trying to find designs of order $n \equiv 0 \pmod 8$ constructed using eight circulant matrices, we will not be as restricted as in Theorem 4.9 but have other problems. The difficulty of finding matrices to replace the variables has led to the following lemma using part Williamson and part Goethals-Seidel criteria. In §4.10 we will see that the Kharaghani array, which uses amicable sets and circulant and/or negacyclic matrices to greatly increase our ability to construct orthogonal designs in orders $\equiv 0 \pmod 8$.

The Kharaghani array has proved the most powerful in finding orthogonal designs of order 8. To understand why we first consider the proliferation of arrays and conditions needed to find orthogonal designs of order divisible by 8 when the Kharaghani array is not used.

Lemma 4.20. *Suppose $X_1, X_2, \ldots, X_8$ are eight circulant (type 1) matrices of order n satisfying*

(1) X_i, $1 \le i \le 8$, have entries from $\{0, \pm x_1, \ldots, \pm x_s\}$, and
(2) $\sum_{i=1}^{8} X_i X_i^\top = fI$.

Further suppose

(i) $X_1, X_2, \ldots, X_8$ are all symmetric or all skew, or
(ii) $X_1 = X_2 = \cdots = X_i$ and $X_{i+1}, \ldots, X_8$ are all symmetric or all skew, $1 \le i \le 8$, or
(iii) $X_2 = X_3 = X_4$ and X_5, X_6, X_7, X_8 are all symmetric (skew), or
(iv) $X_1 X_2^\top = X_2 X_1^\top$, $X_3 = X_4$ and X_5, X_6, X_7, X_8 are all symmetric, or
(v) $X_1, \ldots, X_i$ are all skew and $X_{i+1}, \ldots, X_8$ all symmetric, or
(vi) X_2, X_3, X_4 are all skew and X_5, X_6, X_7, X_8 all symmetric, or
(vii) $X_i X_{i+4}^\top = X_{i+4} X_i^\top$, $i = 1, 2, 3, 4$.

Then, with

$$f = \sum_{i=1}^{s} u_i x_i^2 I,$$

there exists an orthogonal design $OD(8n; u_1, u_2, \ldots, u_s)$.

Proof. As in the proof of Theorem 4.9 the main difficulty is ensuring the matrices $Y_1, \ldots, Y_8$ used to replace the commuting variables of the basic design pairwise satisfy

$$Y_i Y_j^\top = Y_j Y_i^\top.$$

The results of the lemma may be obtained, recalling the results of Section 4.5, by using the following constructions:

(i) Use the circulant matrices to replace the variables in design 1.
(ii) Use a back circulant matrix $X_1R = X_iR$ to replace the first i variables in design 1.
(iii) Use design 2 which needs A, B, E, F, G, H all circulant, B repeated three times, and E, F, G, H all symmetric.
(iv) Use design 4 for which X, A, B, C, D, E, F must all be circulant, B repeated twice, C, D, E, F symmetric, and $XA^\top = AX^\top$.
(v) Use $X_1R, \ldots$ the back circulant matrices $X_1R, \ldots, X_iR$ to replace the first i variables of design 1 and $X_{i+1}, \ldots, X_8$ to replace the last 8-i variables.
(vi) Use design 5 with $B = X_2$, $C = X_3$, $D = X_4$, $E = X_5$, $F = X_6$, $G = X_7$, $H = X_8$, there is no symmetry restriction on $A = X_1$.
(vii) Use design 6. □

Table 4.7 Design 1

$$\left[\begin{array}{cccc|cccc} A & B & C & D & E & F & G & H \\ -B & A & D & -C & F & -E & -H & G \\ -C & -D & A & B & G & H & -E & -F \\ -D & C & -B & A & H & -G & F & -E \\ \hline -E & -F & -G & -H & A & B & C & D \\ -F & E & -H & G & -B & A & -D & C \\ -G & H & E & -F & -C & D & A & -B \\ -H & -G & F & E & -D & -C & B & A \end{array}\right]$$

Table 4.8 Design 2

$$\left[\begin{array}{cccc|cccc} AR & B & B & B & E & F & G & H \\ -B & AR & B & -B & F & -E & -H & G \\ -B & -B & AR & B & G & H & -E & -F \\ -B & B & -B & AR & H & -G & F & -E \\ \hline -E & -F & -G & -H & AR & -B^\top & -B^\top & -B^\top \\ -F & E & -H & G & B^\top & AR & B^\top & -B^\top \\ -G & H & E & -F & B^\top & -B^\top & AR & B^\top \\ H & -G & F & E & B^\top & B^\top & -B^\top & AR \end{array}\right]$$

Example 4.17. The following orthogonal designs in order 24 are constructed by using this lemma. The reader may refer to the Table of the Appendix of Orthogonal Designs in order 24 to find the first rows of the circulant matrices which should be used as indicated:

Table 4.9 Design 3

$$\left[\begin{array}{cccc|cccc} AR & B & B & B & E & F & G & H \\ -B & AR & B & -B & -F & -E & -H & G \\ -B & -B & AR & B & G & H & -E & -F \\ -B & B & -B & AR & H & -G & F & -E \\ \hline -E & -F & -G & -H & AR & B^\top & B^\top & B^\top \\ -F & E & -H & G & -B^\top & AR & -B^\top & B^\top \\ -G & H & E & -F & -B^\top & B^\top & AR & -B^\top \\ -H & -G & F & E & -B^\top & -B^\top & B^\top & AR \end{array}\right]$$

Table 4.10 Design 4

$$\left[\begin{array}{cccc|cccc} XR & AR & B & B & C & D & E & F \\ -AR & XR & B & -B & D & -C & -F & E \\ -B & -B & XR & AR & E & F & -C & -D \\ -B & B & -AR & XR & F & -E & D & -C \\ \hline -C & -D & -E & -F & XR & AR & B^\top & B^\top \\ -D & C & -F & E & -AR & XR & -B^\top & B^\top \\ -E & F & C & -D & -B^\top & B^\top & XR & -AR \\ -F & -E & D & C & -B^\top & -B^\top & AR & XR \end{array}\right]$$

Table 4.11 Design 5

$$\left[\begin{array}{cccc|cccc} AR & B & C & D & E & F & G & H \\ -B & AR & D & -C & F & -E & -H & G \\ -C & -D & AR & B & G & H & -E & -F \\ -D & C & -B & AR & H & -G & F & -E \\ \hline -E & -F & -G & -H & AR & B^\top & C^\top & D^\top \\ -F & E & -H & G & -B^\top & AR & -D^\top & C^\top \\ -G & H & E & -F & -C^\top & D^\top & AR & -B^\top \\ -H & -G & F & E & -D^\top & -C^\top & B^\top & AR \end{array}\right]$$

Table 4.12 Design 6

$$\left[\begin{array}{cccc|cccc} A & BR & CR & DR & E & FR & GR & HR \\ -BR & A & D^\top R & -C^\top R & FR & -E & -H^\top R & G^\top R \\ -CR & -D^\top R & A & B^\top R & GR & H^\top R & -E & -F^\top R \\ -DR & C^\top R & -B^\top R & A & HR & -G^\top R & F^\top R & -E \\ \hline -E & -FR & -GR & -HR & A & BR & CR & DR \\ -FR & E & -H^\top R & G^\top R & -BR & A & -D^\top R & C^\top R \\ -GR & H^\top R & E & -F^\top R & -CR & D^\top R & A & -B^\top R \\ -HR & -G^\top R & F^\top R & E & -DR & -C^\top R & B^\top R & A \end{array}\right]$$

for $OD(24;1,1,1,1,6,6)$ use part (i);
for $OD(24;1,1,1,1,2,10)$ use part (ii);
for $OD(24;1,1,2,2,5,8)$ use part (iii);
for $OD(24;1,1,1,3,4,9)$ use part (iv);
for $OD(24;1,2,2,8,11)$ use part (v);
for $OD(24;1,1,4,4,5)$ use part (vi);
for $OD(24;1,2,5,5,8)$ use part (vii);
for $OD(24;1,2,2,4,13)$ use part (viii).

Remark 4.14. The conditions of Lemma 4.20 are still quite difficult to satisfy. We first consider some constraints on using circulant matrices.

4.10 Amicable Sets and Kharaghani Arrays

Kharaghani [120] has given a most useful array to be used to give orthogonal designs constructed from circulant and most excitingly nega-cyclic matrices in orders divisible by 8.

Following Kharaghani, a set $\{A_1, A_2, \ldots, A_{2n}\}$ of square real matrices is said to be *amicable* if

$$\sum_{i=1}^{n} \left(A_{\sigma(2i-1)} A_{\sigma(2i)}^{\top} - A_{\sigma(2i)} A_{\sigma(2i-1)}^{\top} \right) = 0 \tag{4.16}$$

for some permutation σ of the set $\{1, 2, \ldots, 2n\}$. For simplicity, we will always take $\sigma(i) = i$ unless otherwise specified. So

$$\sum_{i=1}^{n} \left(A_{2i-1} A_{2i}^{\top} - A_{2i} A_{2i-1}^{\top} \right) = 0\,. \tag{4.17}$$

Clearly a set of mutually amicable matrices is amicable, but the converse is not true in general. Throughout this section R_k denotes the back diagonal identity matrix of order k.

A set of matrices $\{B_1, B_2, \ldots, B_n\}$ of order m with entries in $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ is said to satisfy an additive property of type $(s_1, s_2, \ldots, s_u)$ if

$$\sum_{i=1}^{n} B_i B_i^{\top} = \sum_{i=1}^{u} \left(s_i x_i^2 \right) I_m. \tag{4.18}$$

Let $\{A_i\}_{i=1}^{8}$ be an amicable set of circulant matrices (or group developed or type 1) of type $(s_1, s_2, \ldots, s_u)$ and order t. We denote these by $8-AS(t; s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8; Z_t)$ (or $8-AS(t; s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8; G)$ for group developed or type 1). In all cases, the group G of the matrix is such that the extension by Seberry and Whiteman [187] of the group from circulant to type 1 allows the same extension to R. Then the Kharaghani array [120]

$$H = \begin{pmatrix} A_1 & A_2 & A_4R_n & A_3R_n & A_6R_n & A_5R_n & A_8R_n & A_7R_n \\ -A_2 & A_1 & A_3R_n & -A_4R_n & A_5R_n & -A_6R_n & A_7R_n & -A_8R_n \\ -A_4R_n & -A_3R_n & A_1 & A_2 & -A_8^\top R_n & A_7^\top R_n & A_6^\top R_n & -A_5^\top R_n \\ -A_3R_n & A_4R_n & -A_2 & A_1 & A_7^\top R_n & A_8^\top R_n & -A_5^\top R_n & -A_6^\top R_n \\ -A_6R_n & -A_5R_n & A_8^\top R_n & -A_7^\top R_n & A_1 & A_2 & -A_4^\top R_n & A_3^\top R_n \\ -A_5R_n & A_6R_n & -A_7^\top R_n & -A_8^\top R_n & -A_2 & A_1 & A_3^\top R_n & A_4^\top R_n \\ -A_8R_n & -A_7R_n & -A_6^\top R_n & A_5^\top R_n & A_4^\top R_n & -A_3^\top R_n & A_1 & A_2 \\ -A_7R_n & A_8R_n & A_5^\top R_n & A_6^\top R_n & -A_3^\top R_n & -A_4^\top R_n & -A_2 & A_1 \end{pmatrix}$$

is an $OD(8t; s_1, s_2, \ldots, s_u)$.

The Kharaghani array has been used in a number of papers [67, 68, 72, 100, 105, 108, 120, 126] among others to obtain infinitely many families of orthogonal designs. Research has yet to be initiated to explore the algebraic restrictions imposed an amicable set by the required constraints.

Koukouvinos and Seberry [137] have extended the construction of Holzmann and Kharaghani [101] to find infinite families of Kharaghani type orthogonal designs, and in [136] orthogonal designs $OD(8t; k, k, k, k, k, k)$ in 6 variables for odd t.

4.11 Construction using 8 Disjoint Matrices

First we give the following definition.

Definition 4.15. Define L-matrices, $L_1, L_2, \ldots, L_n$ to be n circulant (or type 1) $(0, \pm 1)$ matrices of order ℓ satisfying

(i) $L_i * L_j = 0$, $i \neq j$,

(ii) $\sum_{i=1}^{n} L_i L_i^\top = kI_\ell$,

where $*$ denotes the Hadamard product. We say k is the weight of these L-matrices.

From Definition 4.15 we observe that T-matrices of order t (see Seberry and Yamada [188] for more details) are L-matrices with $\ell = k = t$ and $n = 4$.

Then we have.

Theorem 4.11. *Suppose $L_1, L_2, \ldots, L_n$ are n circulant (or type 1) L-matrices of order s and weight k. Some of the L-matrices may be zero.*

Further suppose $A = (a_{ij})$, $B = (b_{ij})$ are amicable orthogonal designs of type $AOD(n; p_1, p_2, \ldots, p_u; q_1, q_2, \ldots, q_v)$ on the variables $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$, and $\{0, \pm y_1, \pm y_2, \ldots, \pm y_v\}$, respectively. Then there exists an amicable set of matrices $\{A_{i=1}^{2n}\}$ which satisfy

$$\sum_{i=1}^{2n} A_i A_i^\top = \left(\sum_{i=1}^{u} p_i x_i^2 + \sum_{i=1}^{v} q_i y_j^2\right) \sum_{i=1}^{n} L_i L_i^\top = \left(\sum_{i=1}^{u} p_i x_i^2 + \sum_{i=1}^{v} q_i y_j^2\right) kI_s, \tag{4.19}$$

and also (4.16).

Hence these $\{A_i\}_{i=1}^{2n}$ *of order* s *are an amicable set satisfying the additive property for* $(kp_1, kp_2, \ldots, kp_u, kq_1, kq_2, \ldots, kq_v)$.

Proof. Use

$$\begin{array}{ll}
A_1 = a_{11}L_1 + a_{12}L_2 + \cdots + a_{1n}L_n, & A_2 = b_{11}L_1 + b_{12}L_2 + \cdots + b_{1n}L_n \\
A_3 = a_{21}L_1 + a_{22}L_2 + \cdots + a_{2n}L_n, & A_4 = b_{21}L_1 + b_{22}L_2 + \cdots + b_{2n}L_n \\
A_5 = a_{31}L_1 + a_{32}L_2 + \cdots + a_{3n}L_n, & A_6 = b_{31}L_1 + b_{32}L_2 + \cdots + b_{3n}L_n \\
\vdots & \vdots \\
A_{2n-1} = a_{n1}L_1 + a_{n2}L_2 + \cdots + a_{nn}L_n, & A_{2n} = b_{n1}L_1 + b_{n2}L_2 + \cdots + b_{nn}L_n
\end{array}$$

First we note that A and B being amicable ensures that the (x, y) entry c_{xy} of $C = AB^\top$ is

$$c_{xy} = \sum_{j=1}^{n} a_{xj} b_{yj} = \sum_{j=1}^{n} a_{yj} b_{xj} = c_{yx}. \tag{4.20}$$

We also note that if A and B are amicable then $A^\top$ and $B^\top$ are also amicable so the (x, y) entry d_{xy} of $D = A^\top B$ is

$$d_{xy} = \sum_{j=1}^{n} a_{jx} b_{jy} = \sum_{j=1}^{n} a_{jy} b_{jx} = d_{yx}. \tag{4.21}$$

First let us first multiply out $A_1 A_2^\top$, where we will use $(\cdots L_\ell L_m^\top)_{\ell m}$ to denote the term in $L_\ell L_m^\top$. Then

$$A_1 A_2^\top = \sum_{j=1}^{n} a_{1j} b_{1j} L_j L_j^\top + \cdots + ((a_{1\ell} b_{1m}) L_\ell L_m^\top)_{\ell m} + \cdots. \tag{4.22}$$

Similarly

$$A_2 A_1^\top = \sum_{j=1}^{n} a_{1j} b_{1j} L_j L_j^\top + \cdots + ((b_{1\ell} a_{1m}) L_\ell L_m^\top)_{\ell m} + \cdots. \tag{4.23}$$

Hence $A_1 A_2^\top - A_2 A_1^\top$ will have no terms in $L_j L_j^\top$, $j = 1, 2, \cdots, 2n$. Thus the typical term is given by

$$A_1 A_2^\top - A_2 A_1^\top = \cdots + ((a_{1\ell} b_{1m} - b_{1\ell} a_{1m}) L_\ell L_m^\top)_{\ell m} + \cdots. \tag{4.24}$$

We now formally multiply out the expression on the left hand side of (4.16), which gives the following terms in $L_\ell L_m^\top$

$$\sum_{i=1}^{n}\left(A_{2i-1}A_{2i}^\top - A_{2i}A_{2i-1}^\top\right) =$$

$$= \cdots + \left((\sum_{j=1}^{n} a_{j\ell}b_{jm} - \sum_{i=1}^{n} b_{i\ell}a_{im})L_\ell L_m^\top\right)_{\ell m} + \cdots$$

$$= \cdots + \left((\sum_{j=1}^{n} a_{jm}b_{j\ell} - \sum_{i=1}^{n} a_{im}b_{i\ell})L_\ell L_m^\top\right)_{\ell m} + \cdots$$

$$\cdots + \cdots \text{ using (4.21)}$$

$$= 0.$$

This is formally zero and we have (4.17). These matrices also satisfy (4.18) and (4.19) by virtue of A and B being (amicable) orthogonal designs. □

Remark 4.15. Although the theorem is true for any pair of amicable orthogonal designs the arrays needed to exploit the full generality of the theorem are only known, at present, to exist for $n = 2$ or 4.

The maximum number of variables in amicable orthogonal designs of orders 2 and 4 are given in Tables 5.8 and 5.9. A detailed study of amicable orthogonal designs in order 8 is given by Deborah Street in [202, p125–134] and [203, p26–29]. Thus we have:

Corollary 4.13. *Suppose there exist* $AOD(2\ell;p_1,p_2;q_1,q_2)$. *Further suppose there exist two circulant (or type 1)* L*-matrices of order* ℓ *and weight* k. *Then there exists an* $OD(4\ell;kp_1,kp_2,kq_1,kq_2)$.

Proof. We use the L-matrices in the theorem to form an amicable set satisfying the required additive property which is then used in the Goethals-Seidel array to obtain the result. □

Corollary 4.14. *Suppose there exist* $AOD(4\ell;p_1,p_2,p_3;q_1,q_2,q_3)$. *Further suppose there exist four circulant (or type 1)* L*-matrices of order* ℓ *and weight* k. *Then there exists an* $OD(8\ell;kp_1,kp_2,kp_3,kq_1,kq_2,kq_3)$.

Proof. We use the L-matrices in the theorem to form an amicable set satisfying the additive property for $(kp_1,kp_2,kp_3,kq_1,kq_2,kq_3)$. These are then used in the Kharaghani array to obtain the result. □

Example 4.18 ($\boldsymbol{n=2}$*).* Let A and B be the $AOD(2;1,1;1,1)$ given by

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ d & -c \end{bmatrix}.$$

Let L_1 and L_2 be two circulant (or type 1) L-matrices of order ℓ and weight k. Construct

$$\begin{array}{ll} A_1 = aL_1 + bL_2\,, & A_2 = cL_1 + dL_2 \\ A_3 = -bL_1 + aL_2\,, & A_4 = dL_1 - cL_2\,. \end{array} \tag{4.25}$$

Then

$$\sum_{i=1}^{4} A_i A_i^\top = (a^2+b^2+c^2+d^2)\sum_{i=1}^{2} L_i L_i^\top = k(a^2+b^2+c^2+d^2)I_\ell \tag{4.26}$$

and

$$A_1 A_2^\top - A_2 A_1^\top + A_3 A_4^\top - A_4 A_3^\top = 0\,. \tag{4.27}$$

Hence this set of matrices $\{A_1, A_2, \ldots, A_4\}$ of order ℓ with entries in $\{0, \pm a, \pm b, \pm c, \pm d\}$ is an *amicable set* satisfying the additive property for $(1,1,1,1)$.

These can be used in a variant of the Goethals-Seidel array

$$G = \begin{pmatrix} A_1 & A_2 & A_3R & A_4R \\ -A_2 & A_1 & -A_4R & A_3R \\ -A_3R & A_4R & A_1 & -A_2 \\ -A_4R & -A_3R & A_2 & A_1 \end{pmatrix}$$

where R is the back-diagonal identity matrix, to obtain an $OD(4\ell; k, k, k, k)$. □

Example 4.19 ($\boldsymbol{n = 4}$). Let A and B be the $AOD(4; 1,1,1; 1,1,1)$ given by

$$\begin{bmatrix} a & b & c & 0 \\ -b & a & 0 & -c \\ -c & 0 & a & b \\ 0 & c & -b & a \end{bmatrix} \begin{bmatrix} d & e & f & 0 \\ e & -d & 0 & -f \\ f & 0 & -d & e \\ 0 & -f & e & d \end{bmatrix}.$$

Let $L_1,\ L_2, \cdots, L_4$ be four circulant (or type 1) L-matrices of order ℓ and weight k. Construct

$$\begin{array}{llll} A_1 = aL_1 & +bL_2 & +cL_3\,, & \\ A_3 = -bL_1 & +aL_2 & -cL_4\,, & \\ A_5 = -cL_1 & +aL_3 & +bL_4\,, & \\ A_7 = & +cL_2 & -bL_3 & +aL_4\,, \end{array} \qquad \begin{array}{llll} A_2 = dL_1 & +eL_2 & +fL_3\,, & \\ A_4 = eL_1 & -dL_2 & -fL_4\,, & \\ A_6 = fL_1 & -dL_3 & +eL_4\,, & \\ A_8 = & -fL_2 & +eL_3 & +dL_4\,. \end{array} \tag{4.28}$$

Then

$$\begin{aligned} \sum_{i=1}^{8} A_i A_i^\top &= \left(a^2+b^2+c^2+d^2+e^2+f^2\right)\sum_{i=1}^{4} L_i L_i^\top \\ &= k\left(a^2+b^2+c^2+d^2+e^2+f^2\right) I_\ell, \end{aligned} \tag{4.29}$$

and

$$A_1A_2^\top - A_2A_1^\top + A_3A_4^\top - A_4A_3^\top + A_5A_6^\top - A_6A_5^\top + A_7A_8^\top - A_8A_7^\top = 0. \tag{4.30}$$

Hence this set of matrices $\{A_1, A_2, \ldots, A_8\}$ of order ℓ with entries in $\{0, \pm a, \pm b, \pm c, \pm d, \pm e, \pm f\}$ is an *amicable set* satisfying the additive property for $(1,1,1,1,1,1)$.

They can be used in the Kharaghani array to obtain $OD(8\ell; k, k, k, k, k, k)$.

Example 4.20 ($\boldsymbol{n = 4}$). Let A and B be the $AOD(4; 1, 1, 2; 1, 1, 2)$ given by

$$\begin{bmatrix} a & b & c & c \\ -b & a & c & -c \\ c & c & -a & -b \\ c & -c & b & -a \end{bmatrix} \begin{bmatrix} d & e & f & f \\ e & -d & f & -f \\ -f & -f & e & d \\ -f & f & d & -e \end{bmatrix}.$$

Let $L_1,\ L_2, \cdots, L_4$ four circulant (or type 1) L-matrices of order ℓ and weight k. Construct

$$\begin{array}{llll} A_1 = aL_1 & +bL_2 & +cL_3 & +cL_4, \\ A_3 = -bL_1 & +aL_2 & +cL_3 & -cL_4, \\ A_5 = cL_1 & +cL_2 & -aL_3 & -bL_4, \\ A_7 = cL_1 & -cL_2 & +bL_3 & -aL_4, \end{array} \quad \begin{array}{llll} A_2 = dL_1 & +eL_2 & +fL_3 & +fL_4, \\ A_4 = eL_1 & -dL_2 & +fL_3 & -fL_4, \\ A_6 = -fL_1 & -fL_2 & +eL_3 & +dL_4, \\ A_8 = -fL_1 & +fL_2 & +dL_3 & -eL_4. \end{array} \tag{4.31}$$

Then

$$\begin{aligned} \sum_{i=1}^{8} A_iA_i^\top &= (a^2 + b^2 + 2c^2 + d^2 + e^2 + 2f^2) \sum_{i=1}^{4} L_iL_i^\top \\ &= k(a^2 + b^2 + 2c^2 + d^2 + e^2 + 2f^2) I_\ell, \end{aligned} \tag{4.32}$$

and

$$A_1A_2^\top - A_2A_1^\top + A_3A_4^\top - A_4A_3^\top + A_5A_6^\top - A_6A_5^\top + A_7A_8^\top - A_8A_7^\top = 0. \tag{4.33}$$

Hence this set of matrices $\{A_1, A_2, \ldots, A_8\}$ of order ℓ with entries in $\{0, \pm a, \pm b, \pm c, \pm d, \pm e, \pm f\}$ is an *amicable set* satisfying the additive property for $(1,1,2,1,1,2)$. These can be used in the Kharaghani array to obtain an $OD(8\ell; k, k, k, k, 2k, 2k)$.

4.11.1 Hadamard Matrices

Before going to our next result, we first note:

Lemma 4.21. *If there is $AOD(m\colon (1, m-1); (m))$ and $OD(h; 1, h-1)$, then by Wolfe's theorem (7.9) there is an $OD(mh; 1, m-1, m(h-1))$.*

Then Theorem 8.7 of Wallis [231, p.368] can be restated as:

Theorem 4.12 (Wallis). *Suppose there exists* $OD(mh; 1, m-1, m(h-1))$. *Suppose there exist "suitable" matrices of order* n *to replace the variables of this design. Then there exists an Hadamard matrix of order* mhn.

Proof. Obvious. □

Corollary 4.15. *Let* n *be the order of any Hadamard matrix* H. *Suppose there exists an orthogonal design* D *of type* $OD(n(m-1): (1, m-1, nm-n-m))$. *Then there exists an Hadamard matrix of order* $n(n-1)(m-1)$.

Proof. We write H as

$$\begin{bmatrix} 1 & e \\ -e^\top & P \end{bmatrix}$$

where e is the $1 \times (n-1)$ matrix of 1's. Then

$$PJ = J, \qquad PP^\top = nI - J.$$

The result is obtained by replacing the variables of D by P, J, P, respectively. □

Many corollaries can be made by finding "suitable" matrices, but we will not proceed further with this here.

We will show in Chapter 9 that $OD(2^t: (1, m-1, nm-n-m))$ exist in every power of 2, $2^t = (m-1)n$. Hence we have a new result.

Corollary 4.16. *With* t, s *any non-negative integers, there exists a Hadamard matrix of order* $2^s(2^s-1)(2^t-1)$.

We note the following result:

Theorem 4.13. *Let* $k > 1$ *be the order of an Hadamard matrix* H, *and* n *be the order of a symmetric conference matrix* C. *Further, suppose there exist amicable orthogonal designs* M, N *of types* $AOD(m: (1, m-1); (\frac{m}{2}, \frac{m}{2}))$. *Then there exists an* $OD(nmk: k, (m-1)k, (n-1)\frac{mk}{2}, (n-1)\frac{nk}{2})$.

Proof. let $P = \left[\begin{smallmatrix} 0 & - \\ 1 & 0 \end{smallmatrix}\right] \times I_{\frac{k}{2}}$. Then

$$R = C \times H \times N + I \times PH \times M$$

is the required orthogonal design. □

Hence we have generalized a theorem of Wallis [231, p.375, Theorem 8.24]:

Corollary 4.17. *Suppose* H, C, M, N *are as in the theorem, and suppose there are "suitable" matrices of order* p. *Then there exists an Hadamard matrix of order* $nmkp$.

Now we note that if m is of the form $\prod_i 2^t(p_i^{r_i}+1)$, where $p_i^{r_i} \equiv 3 \pmod 4$ is a prime power, then $AOD(m: (1, m-1); (\frac{m}{2}, \frac{m}{2}))$ exist. Thus we have:

Corollary 4.18. *Suppose $k>1$ is the order of an Hadamard matrix and n the order of a symmetric conference matrix. Then there exists $OD(k,(2m-1)k,(n-1)mk,(n-1)mk)$ where $m=2_i^t\prod(p_i^{r_i}+1), p_i^{r_i}\equiv 3 \pmod 4$ is a prime power, and $t>0$ is an integer.*

4.12 Baumert-Hall Arrays

In 1933 Paley wrote a most important paper on the construction of Hadamard matrices which he called 'orthogonal matrices' [160]. At the same time J.A. Todd [211] realised that these matrices gave symmetric balanced incomplete block designs–of great interest in the design and analysis of experiments for agriculture and medicine.

Thus Paley opened the way for R.C. Bose's [26] fundamental and path-finding use of Galois fields in the construction of balanced incomplete block designs–a most valuable contribution to applied statistics.

Yet it was not until Williamson's 1944 [244] and 1947 [245] papers that more Hadamard matrices were found. Williamson used what we would now call orthogonal designs $OD(n;1,n-1)$ and $OD(n;2,n-2)$.

Paley listed the orders less than 200 for which Hadamard matrices were not known, viz., 92, 116, 148, 156, 172, 184, and 188. Williamson suggested using what we will call the Williamson Array

$$\begin{bmatrix} A & B & C & D \\ -B & A & D & -C \\ -C & -D & A & B \\ -D & C & -B & A \end{bmatrix}$$

to find Hadamard matrices and in fact obtained the matrices of orders 148 and 172 by finding suitable matrices (using the theory we now call cyclotomy; see Storer [200]) to replace the variables of the array. Thus we define

Definition 4.16. Eight circulant $(1,-1)$ matrices $X_1,\ldots,X_8$ of order n which satisfy

$$\sum_{i=1}^{8} X_i X_i^\top = 8nI, \quad X_i X_j^\top = X_j X_i^\top$$

will be called *eight Williamson matrices* (cf Williamson matrices: Theorem 4.4 and proof). *Williamson matrices* are four circulant symmetric matrices $x_1,\ldots,x_u$ satisfying

$$\sum_{i=1}^{4} X_i X_i^\top = 4nI\,.$$

Baumert, Golomb and Hall [17] found Williamson matrices of order 23 giving the Hadamard matrices of orders 92 and 184. We can appreciate their excitement when on the night of September 27, 1961, after an hour of computer calculation, the output arrived. In fact, there turned out to be one and only one example of Williamson matrices of order 23.

Later, Baumert [15, 18] was to find Williamson matrices giving the Hadamard matrix of order 116. We shall give the Hadamard matrix of order 188 in Proposition 7.2.

The remainder of this section is devoted to the exciting results that have come from Baumert and Hall's search for the Hadamard matrix of order 156. But first a definition.

Definition 4.17. An orthogonal design $OD(4t;t,t,t,t)$ will be called a *Baumert-Hall array of order t*.

Now Baumert and Hall realised that since Williamson matrices of order 13 were known, if a Baumert-Hall array of order 3 could be found, then the Hadamard matrix of order 156 would be found. In fact, they realised:

Theorem 4.14. *If a Baumert-Hall array of order t and Williamson matrices of order n exist, then there exists an Hadamard matrix of order* $4nt$*; equivalently, if there exists an orthogonal design* $OD(4nt;t,t,t,t)$ *and Williamson matrices of order n, then there exists an Hadamard matrix of order* $4nt$.

Proof. Replace the variables of the Baumert-Hall array by the Williamson matrices. □

In 1965 Baumert and Hall [14] published the first Baumert-Hall array of order 3 (Table 4.13):

Table 4.13 Baumert-Hall array–order 3

$$\begin{bmatrix}
A & A & A & B & -B & C & -C & -D & B & C & -D & -D \\
A & -A & B & -A & -B & -D & D & -C & -B & -D & -C & -C \\
A & -B & -A & A & -D & D & -B & B & -C & -D & C & -C \\
B & A & -A & -A & D & D & D & C & C & -B & -B & -C \\
B & -D & D & D & A & A & A & C & -C & B & -C & B \\
B & C & -D & D & A & -A & C & -A & -D & C & B & -B \\
D & -C & B & -B & A & -C & -A & A & B & C & D & -D \\
-C & -D & -C & -D & C & A & -A & -A & -D & B & -B & -B \\
D & -C & -B & -B & -B & C & C & -D & A & A & A & D \\
-D & -B & C & C & C & B & B & -D & A & -A & D & -A \\
C & -B & -C & C & D & -B & -D & -B & A & -D & -A & A \\
-C & -D & -D & C & -C & -B & B & B & D & A & -A & -A
\end{bmatrix}$$

Many attempts were made to generalise this array, but none were successful until in 1971 L.R. Welch [243] found a Baumert-Hall array of order 5 (Table 4.14):

Table 4.14 Baumert-Hall array–order 5 constructed entirely of circulant blocks

$$
\left[\begin{array}{ccccc|ccccc|ccccc|ccccc}
-D & B & -C & -C & -B & C & A & -D & -D & -A & -B & -A & C & -C & -A & A & -B & -D & D & -B \\
-B & -D & B & -C & -C & -A & C & A & -D & -D & -A & -B & -A & C & -C & -B & A & -B & -D & D \\
-C & -B & -D & B & -C & -D & -A & C & A & -D & -C & -A & -B & -A & C & D & -B & A & -B & -D \\
-C & -C & -B & -D & B & -D & -D & -A & C & A & C & -C & -A & -B & -A & -D & D & -B & A & -B \\
B & -C & -C & -B & -D & A & -D & -D & -A & C & -A & C & -C & -A & -B & -B & -D & D & -B & A \\
\hline
-C & A & D & D & -A & -D & -B & -C & -C & B & -A & B & -D & D & B & -B & -A & -C & C & -A \\
-A & -C & A & D & D & B & -D & -B & -C & -C & B & -A & B & -D & D & -A & -B & -A & -C & C \\
D & -A & -C & A & D & -C & B & -D & -B & -C & D & B & -A & B & -D & C & -A & -B & -A & -C \\
D & D & -A & -C & A & -C & -C & B & -D & -B & -D & D & B & -A & B & -C & C & -A & -B & -A \\
A & D & D & -A & -C & -B & -C & -C & B & -D & B & -D & D & B & -A & -A & -C & C & -A & -B \\
\hline
B & -A & -C & C & -A & A & B & -D & D & B & -D & -B & C & C & B & -C & A & -D & -D & -A \\
-A & B & -A & -C & C & B & A & B & -D & D & B & -D & -B & C & C & -A & -C & A & -D & -D \\
C & -A & B & -A & -C & D & B & A & B & -D & C & B & -D & -B & C & -D & -A & -C & A & -D \\
-C & C & -A & B & -A & -D & D & B & A & B & C & C & B & -D & -B & -D & -D & -A & -C & A \\
-A & -C & C & -A & B & B & -D & D & B & A & -B & C & C & B & -D & A & -D & -D & -A & -C \\
\hline
-A & -B & -D & D & -B & B & -A & C & -C & -A & C & A & D & D & -A & -D & B & C & C & -B \\
-B & -A & -B & -D & D & -A & B & -A & C & -C & -A & C & A & D & D & -B & -D & B & C & C \\
D & -B & -A & -B & -D & -C & -A & B & -A & C & D & -A & C & A & D & C & -B & -D & B & C \\
-D & D & -B & -A & -B & C & -C & -A & B & -A & D & D & -A & C & A & C & C & -B & -D & B \\
-B & -D & D & -B & -A & -A & C & -C & -A & B & A & D & D & -A & C & B & C & C & -B & -D
\end{array}\right]
$$

For future reference we define:

Definition 4.18. *A Baumert-Hall-Welch array of order t* is a Baumert-Hall array of order t constructed from sixteen circulant or type 1 matrices.

The circulant structure of Welch's array gave the clue to generalising Baumert-Hall arrays. First we consider:

Definition 4.19. Four circulant (type 1) $(0,1,-1)$ matrices X_i, $i=1,2,3,4$, of order n which are non-zero for each of the n^2 entries for exactly one i, i.e., $X_i * X_j = 0$ for $i \neq j$, and which satisfy

$$\sum_{i=1}^{4} X_i X_i^\top = nI$$

will be called *T-matrices of order n*. These were first used by Cooper-Wallis [32].

A type 1 matrix has constant row (and column) sum; so:

Lemma 4.22. *Let X_i, $i=1,\ldots,4$, be T-matrices with row sum (and column sum) x_i, respectively. Then*

$$\sum_{i=1}^{4} x_i^2 = n\,.$$

Proof. $X_i J = x_i J$; so considering $\sum_{i=1}^{4} X_i X_i^\top J = nJ$ gives the result. □

The following result, in a slightly different form, was independently discovered by R.J. Turyn. Turyn use what are called T-sequences later in this chapter. T-sequences are the aperiodic counter part of T-matrices. The existence of T-sequences implies the existence of T-matrices.

Theorem 4.15 (Cooper-Wallis [32]). *Suppose there exist T-matrices X_i, $i=1,\ldots,4$, of order n. Let a, b, c, d be commuting variables. Then*

$$\begin{aligned}
A &= aX_1 + bX_2 + cX_3 + dX_4\\
B &= -bX_1 + aX_2 + dX_3 - cX_4\\
C &= -cX_1 - dX_2 + aX_3 + bX_4\\
D &= -dX_1 + cX - bX_3 + aX_4
\end{aligned}$$

can be used in the Goethals-Seidel (or Wallis-Whiteman [241]) array to obtain a Baumert-Hall array of order n; equivalently, if there exist T-matrices of order n, there exists an orthogonal design $OD(4n;n,n,n,n)$.

Proof. By straightforward verification. □

Example 4.21. Let

$$X_1 = \begin{bmatrix} 1&0&0\\ 0&1&0\\ 0&0&1 \end{bmatrix}, \quad X_2 = \begin{bmatrix} 0&1&0\\ 0&0&1\\ 1&0&0 \end{bmatrix}, \quad X_3 = \begin{bmatrix} 0&0&1\\ 1&0&0\\ 0&1&0 \end{bmatrix}, \quad X_4 = 0.$$

Then X_1, X_2, X_3, X_4 are T-matrices of order 3, and the Baumert-Hall array of order 3 is in Table 4.15.

Table 4.15 Baumert-Hall array–order 3

a	b	c	$-b$	a	d	$-c$	$-d$	a	$-d$	c	$-b$
c	a	b	a	d	$-b$	$-d$	a	$-c$	c	$-b$	$-d$
b	c	a	d	$-b$	a	a	$-c$	$-d$	$-b$	$-d$	c
b	$-a$	$-d$	a	b	c	$-d$	$-b$	c	c	$-a$	d
$-a$	$-d$	b	c	a	b	$-b$	c	$-d$	$-a$	d	c
$-d$	b	$-a$	b	c	a	c	$-d$	$-b$	d	c	$-a$
c	d	$-a$	d	b	$-c$	a	b	c	$-b$	d	a
d	$-a$	c	b	$-c$	d	c	a	b	d	a	$-b$
$-a$	c	d	$-c$	d	b	b	c	a	a	$-b$	d
d	$-c$	b	$-c$	a	$-d$	b	$-d$	$-a$	a	b	c
$-c$	b	d	a	$-d$	$-c$	$-d$	$-a$	b	c	a	b
b	d	$-c$	$-d$	$-c$	a	$-a$	b	$-d$	b	c	a

We will not give the proofs here which can be found in Wallis [231, p. 360] and Hunt and Wallis [110] but will just quote the results given there. More results on Baumert-Hall arrays are given in Section 7.1 after some new concepts have been introduced. In Section 7.1 we show how cyclotomy may be used in constructing these arrays, including the previously unpublished array of Hunt of order 61.

Lemma 4.23. *There exist Baumert-Hall arrays of order t, $t \in X$, $X = \{x : x$ is an odd integer, $0 \le x \le 25, 31, 37, 41, 61\}$.*

Corollary 4.19. *There exist Hadamard matrices of order $4tq$ where $t \in X$, X given in the previous lemma, and q is the order of Williamson matrices. In particular, there exist Hadamard matrices of order $4tq$, $q = \frac{1}{2}(p+1)$ or $\frac{1}{2}p(p+1)$ where $p \equiv 1 \pmod 4$ is a prime power.*

Proof. The required matrices are given in Corollaries 4.11 and 4.12. □

The long held conjecture that the Williamson method would give results for all orders of Hadamard matrices was first disproved for order 35 by Đoković in 1993 [42]. Schmidt's review [176] of Holzmann, Kharaghani and Tayfeh-Rezaie [106] points out that there are no Williamson matrices of order 47, 53

or 59. In their startling paper, Holzmann, Kharaghani and Tayfeh-Rezaie [106] indicate there are no Williamson matrices for four small orders. Table 4.16 summarizes the number of Williamson matrices of order 1–59.

Table 4.16 Number of Williamson Matrices of Order 1–59 [a]

Order:	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29
Number:	1	1	1	2	3	1	4	4	4	6	7	1	10	6	1
Order:	31	33	35	37	39	41	43	45	47	49	51	53	55	57	59
Number:	2	5	0	4	1	1	2	1	0	1	2	0	1	1	0

[a] Holzmann, Kharaghani and Tayfeh-Rezaie [106, p347] © Springer

A most important theorem which shows how Baumert-Hall-Welch arrays can be used is now given. To date, the only such arrays known are of orders 5 and 9. We note that in these BHW theorems circulant or type 1 can be replaced by negacyclic matrices.

Theorem 4.16 (Turyn [220]). *Suppose there is a Baumert-Hall-Welch array BHW of order s constructed of sixteen circulant (or type 1) $s \times s$ blocks. Further suppose there are T-matrices of order t. Then there is a Baumert-Hall array of order st.*

Proof. Since BHW is constructed of sixteen circulant (or type 1) blocks, we may write $BHW = (N_{ij})$, $i, j = 1, 2, 3, 4$, where each N_{ij} is circulant (or type 1).

Since $(BHW)(BHW)^\top = s(a^2 + b^2 + c^2 + d^2)I_{4s}$ where a, b, c, d are the commuting variables, we have

$$N_{i1}N_{j1}^\top + N_{i2}N_{j2}^\top + N_{i3}N_{j3}^\top + N_{i4}N_{j4}^\top = \begin{cases} s(a^2+b^2+c^2+d^2)I_s\,, & i = j\,, \\ & i = 1,2,3,4 \\ 0\,, & i \neq j\,. \end{cases}$$

Suppose the T-matrices are T_1, T_2, T_3, T_4. Then form the matrices

$$\begin{aligned} A &= T_1 \times N_{11} + T_2 \times N_{21} + T_3 \times N_{31} + T_4 \times N_{41} \\ B &= T_1 \times N_{12} + T_2 \times N_{22} + T_3 \times N_{32} + T_4 \times N_{42} \\ C &= T_1 \times N_{13} + T_2 \times N_{23} + T_3 \times N_{33} + T_4 \times N_{43} \\ D &= T_1 \times N_{14} + T_2 \times N_{24} + T_3 \times N_{34} + T_4 \times N_{44}\,, \end{aligned}$$

Now

$$AA^\top + BB^\top + CC^\top + DD^\top = st(a^2 + b^2 + c^2 + d^2)I_{st}\,,$$

and since A, B, C, D are type 1, they can be used in the Wallis-Whiteman generalisation of the Goethals-Seidel array to obtain the desired result. (See also Lemma 4.7) □

Since the Baumert-Hall array of order 5 given by Welch is constructed of sixteen circulant blocks, as is the Ono-Sawade-Yamamoto array of order 9 given to us by K. Yamamoto [188, p. 449].

Corollary 4.20. *Suppose there are T-matrices of order t. Then there is a Baumert-Hall array of order $5t$ and $9t$; equivalently, there is an orthogonal design $OD(20t;5t,5t,5t,5t)$ and $OD(36t;9t,9t,9t,9t)$. As we have seen, Baumert and Hall's array of order 3, discovered to obtain the Hadamard matrix of order 156, has led to one of the most powerful constructions for Hadamard matrices. In fact, to prove the Hadamard conjecture it would be sufficient to prove:*

Conjecture 4.3. There exists a Baumert-Hall array of order t for every positive integer t, or equivalently, there exists an orthogonal design $OD(4t;t,t,t,t)$ for every positive integer t.

4.13 Plotkin Arrays

Following the exciting results on Baumert-Hall arrays, which if they all exist, would answer the Hadamard conjecture in the affirmative, it became clear that similar designs in order $8n$ would give results of great import. Alas, as we shall now see, such designs of order $8n$, n odd, are very hard to find.

These classes of orthogonal designs are of great interest and worthy of further study.

Definition 4.20. An orthogonal design $OD(8t;t,t,t,t,t,t,t,t)$ will be called a *Plotkin array.*

Remark. Matrices with elements $\{1,-1\}$ which can be used in Plotkin arrays to give Hadamard matrices (eight Williamson matrices) have been found by J. Wallis [236], and of course Williamson matrices (each used twice) will also suffice. Still the problem of finding suitable matrices to replace the variables in designs to give Hadamard matrices or weighing matrices is largely untouched but displaced by the use of the Kharaghani array [120] and amicable sets.

We first see that if an Hadamard matrix exists, then Plotkin arrays exist in four times the order.

Theorem 4.17 (Plotkin [161]). *Suppose there exists an Hadamard matrix of order $2t$. Then there exists an orthogonal design $OD(8t;t,t,t,t,t,t,t,t)$.*

Proof. Let H be an Hadamard matrix of order 2t. Let

$$S=\frac{1}{2}\begin{pmatrix} I & -I \\ I & I \end{pmatrix} H, \qquad T=\frac{1}{2}\begin{pmatrix} I & I \\ -I & I \end{pmatrix} H,$$

$$U=\frac{1}{2}\begin{pmatrix} I & -I \\ -I & -I \end{pmatrix} H, \qquad V=\frac{1}{2}\begin{pmatrix} I & I \\ I & -I \end{pmatrix} H.$$

Then define

$$H_{2t}(a,b) = (S \times a) + (T \times b),$$
$$H_{4t}(a,b,c,d) = \begin{bmatrix} H_{2t}(a,b) & H_{2t}(c,d) \\ H_{2t}(-c,d) & H_{2t}(a,-b) \end{bmatrix},$$

and

$$B_{4t}(a,b,c,d) = \begin{bmatrix} S \times a + T \times b & U \times c + V \times d \\ U \times (-c) + V \times (-d) & S \times a + T \times b \end{bmatrix}.$$

Then

$$H_{8t}(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) = \begin{bmatrix} H_{4t}(x_1,x_2,x_3,x_4) & B_{4t}(x_5,x_6,x_7,x_8) \\ B_{4t}(x_5,x_6,x_7,x_8) & -H_{4t}(-x_1,x_2,x_3,x_4) \end{bmatrix}$$

is the required Plotkin array. □

The 8×8 matrix of Theorem 4.1, which is unique under the equivalence operations,

(i) multiply any row or column by -1,
(ii) interchange any pair of rows or columns,
(iii) replace any variable by its negative throughout,

is a design of type (1,1,1,1,1,1,1,1). Plotkin found that the following matrix is equivalent under (i), (ii) and (iii) to the Baumert-Hall array of the previous section.

$$A(x,y,z,w) = \begin{bmatrix} y & x & x & x & -z & z & w & y & -w & w & z & -y \\ -x & y & x & -x & w & -w & z & -y & -z & z & -w & -y \\ -x & -x & y & x & w & -y & -y & w & z & z & w & -z \\ -x & x & -x & y & -w & -w & -z & w & -z & -y & -y & -z \\ -y & -y & -z & -w & z & x & x & x & -w & -w & z & -y \\ -w & -w & -z & y & -x & z & x & -x & y & y & -z & -w \\ w & -w & w & -y & -x & -x & z & x & y & -z & -y & -z \\ -w & -z & w & -z & -x & x & -x & z & -y & y & -y & w \\ -y & y & -z & -w & -z & -z & w & y & w & x & x & x \\ z & -z & -y & -w & -y & -y & -w & -z & -x & w & x & -x \\ -z & -z & y & z & -y & -w & y & -w & -x & -x & w & x \\ z & -w & -w & z & y & -y & y & z & -x & x & -x & w \end{bmatrix} \tag{4.34}$$

Also, the next matrix is a Baumert-Hall array of order 12, but is not equivalent to (4.34).

$$B(x,y,z,w) = \begin{bmatrix} y & x & x & x & -w & w & z & y & -z & z & w & -y \\ -x & y & x & -x & -z & z & -w & -y & w & -w & z & -y \\ -x & -x & y & x & -y & -w & y & -w & -z & -z & w & z \\ -x & x & -x & y & w & w & -z & -w & -y & z & y & z \\ -w & -w & -z & -y & z & x & x & x & -y & -y & z & -w \\ y & y & -z & -w & -x & z & x & -x & -w & -w & -z & y \\ -w & w & -w & -y & -x & -x & z & x & z & y & y & z \\ z & -w & -w & z & -x & x & -x & z & y & -y & y & w \\ z & -z & y & -w & y & y & w & -z & w & x & x & x \\ y & -y & -z & -w & -z & -z & -w & -y & -x & w & x & -x \\ z & z & y & -z & w & -y & -y & w & -x & -x & w & x \\ -w & -z & w & -z & -v & v & -v & z & -x & x & -x & w \end{bmatrix} \tag{4.35}$$

Then we have

Lemma 4.24. *There is a Plotkin array of order 24, i.e. , an orthogonal design* $OD(24;3,3,3,3,3,3,3,3)$.

Proof.

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

is the required design. □

These results lead to:

Conjecture 4.4 (Plotkin [161]). There exist Plotkin arrays in every order $8n$, n a positive integer.

4.13.1 Kharaghani's Plotkin arrays

Until recently, only the original for $n = 3$ had been constructed in the ensuing twenty eight years. Holzmann and Kharaghani [101] using a new method constructed many new Plotkin ODs of order 24 and two new Plotkin ODs of order 40 and 56.

4.14 More Specific Constructions using Circulant Matrices

The constructions of this section will be used extensively later to discuss existence of orthogonal designs.

In any of the following constructions, similar results may be obtained by replacing the words circulant and back circulant by type 1 and type 2, respectively (see Section 4.2).

Construction 4.1. *Suppose there is a $W(n,k)$ constructed from two circulant matrices M, N of order $\frac{n}{2}$ with the property that $M*N=0$ ($*$ denotes Hadamard product). Then $A=x_1M+x_2N$, $B=x_1N-x_2M$ may be used in $\left[\begin{smallmatrix} A & BR \\ -BR & A \end{smallmatrix}\right]$ to obtain an $OD(n;k,k)$ on x_1, x_2.*

Proof. A straightforward verification. One need only observe that since M, N are circulant, MR, NR are back circulant, and if X is circulant and Y is back circulant, then $XY^\top = YX^\top$. □

Example 4.22. Write T for the circulant matrix of order n whose first row is nonzero only in the second column, the entry there being 1. Now

$$M=T+T^2 \quad \text{and} \quad N=T^3-T^4$$

may be used to give a $W(2n,4)$ constructed from two circulants, $(M*N=0)$. Then, using the construction $A=x_1M+x_2N$, $B=x_1N-x_2M$ gives an $OD(2n;4,4)$ constructed from circulants.

Construction 4.2. *Suppose there exist $W(n,k_i)$, $i=1,2$, constructed from circulant matrices M_i, N_i, $i=1,2$, of order $\frac{n}{2}$ where $M_1*M_2=N_1*N_2=0$ and $M_1M_2^\top+M_2M_1^\top=N_1N_2^\top+N_2N_1^\top=0$; then*

$$A=x_1M_1+x_2M_2, \qquad B=x_1N_1+x_2N_2$$

may be used as two circulants to give an $OD(n;k_1,k_2)$ on the variables x_1, x_2.

Example 4.23. With T as in the previous example and $n=2k+1$, let

$$M_1=T^{k-1}-T^{k+2} \qquad N_1=T^{k-1}+T^{k+2}$$
$$M_2=T^k+T^{k+1} \qquad N_2=T^k-T^{k+1}$$

which satisfy the conditions of the construction. Then

$$A=x_1M_1+x_2M_2 \qquad B=x_1N_1+x_2N_2$$

give an $OD(n;4,4)$.

Construction 4.3. *Suppose there exist orthogonal designs X_1, X_2 of type $OD(2n;u_{i1},u_{i2},\ldots,u_{im_i})$ on the variables $x_{i1},x_{i2},\ldots,x_{im}$, $i=1,2$, each of which is constructed using two circulants.*

Then there exists an $OD(4n;u_{11},u_{12},\ldots u_{1m_1},\ u_{21},u_{22},\ldots,u_{2m_2})$ on the variables $x_{11},x_{12},x_{1m_1},x_{21},x_{22},\ldots,x_{2m_2}$.

Proof. Let A_i, B_i be the matrices used to form the orthogonal design X_i. Then use A_1, B_1, A_2, B_2 in the Goethals-Seidel array to get the result. □

Corollary 4.21. *Suppose there exist $W(n,k_i)$, $i=1,2$, constructed from circulant matrices M_i, N_i, $i=1,2$, of order $\frac{n}{2}$. Then there exists an $OD(2n;k_1,k_2)$, and a $W(2n,k_1+k_2)$.*

Proof. Set $A=x_1M_1$, $B=x_1N_1$, $C=x_2M_2$, $D=x_2N_2$ in the Goethals-Seidel array. □

Example 4.24. The circulant matrices $A(a)$, $B(a)$,with first rows

$$a\ \ a\ \ a\ \ \bar{a}\ \ 0_{n-4}, \qquad a\ \ a\ \ \bar{a}\ \ a\ \ 0_{n-4}, \qquad \text{respectively,}$$

give a $W(2n,8)$ constructed from circulants for every $r \geq 4$, and the circulant matrices $C(c,d)$, $D(d)$ with first rows

$$d\ \ c\ \ \bar{d}\ \ 0_{m-3}, \qquad d\ \ 0\ \ d\ \ 0_{m-3}, \qquad \text{respectively,}$$

give an $OD(2m;1,4)$ in every order, $m \geq 3$, where 0_t is a sequence of t zeros.

Hence

$$\{A(a),\ B(a),\ A(b),\ B(b)\}$$
$$\{C(c,d),\ D(d),\ C(a,b),\ D(b)\}$$
$$\{A(a),\ B(a),\ C(c,d),\ D(d)\}$$

can be used as four circulant matrices in the Goethals-Seidel array to give $OD(4s;8,8)$, $OD(4s;1,1,4,4)$ and $OD(4s;1,4,8)$, $s \geq 4$ respectively.

The next theorem indicates that we may be able to prove theorems of the type, "If $(s_1,\ldots,s_r)$ satisfies all the existence criteria for an orthogonal design, then $(s_1,\ldots,s_r)$ is the type of an orthogonal design in some large enough order tn and every order un, $u \geq t$." We will give, in a later chapter, the results that Eades and others have found in this direction.

Theorem 4.18. *Suppose (s_1,s_2,s_3,s_4) satisfies Wolfe's necessary conditions for the existence of orthogonal designs in order $n=4 \pmod 8$ given by Proposition 3.23:*

(i) If $s_1+s_2+s_3+s_4 \geq 12$, there is an $OD(4t;\ s_1,s_2,s_3,s_4)$ for all $t \geq 3$.
(ii) If $s_1+s_2+s_3+s_4 \geq 16$, there is an $OD(4t;\ s_1,s_2,s_3,s_4)$ for all $t \geq 4$, with the possible exception of $(2,2,5,5)$ which exists in order $4t$, $t \geq 4$, $t \neq 5$.
(iii) If $16 < s_1+s_2+s_3+s_4 \leq 28$, the Table 4.17 gives the smallest N such that (s_1,s_2,s_3,s_4) is the type of an orthogonal design which exists for all $4t > N$.

Proof. See pages 168–170 of *Orthogonal Designs* (1st edition, 1979). □

Table 4.17 N is the order such that the indicated designs exist in every order $4t > N$

Group $12 \le 16$ [a]	N	Group $16 \le 20$ [b]	N	Group $20 \le 24$ [c]	N	Group $24 \le 28$ [d]	N
(1,1,4,9)	16	(1,1,1,16)	24	(1,1,2,18)	48	(1,1,1,25)	56
(1,2,2,9)	16	(1,1,8,8)	20	(1,1,4,16)	24	(1,1,5,20)	144
(1,2,4,8)	16	(1,1,9,9)	20	(1,1,10,10)	40	(1,1,8,18)	56
(1,4,4,4)	16	(1,2,8,9)	40	(1,2,2,16)	48	(1,1,9,16)	312
(1,4,5,5)	16	(1,3,6,8)	48	(1,2,6,12)	24	(1,1,13,13)	48
(2,2,2,8)	16	(1,4,4,9)	48	(1,4,8,8)	32	(1,2,4,18)	80
(2,2,5,5)	24	(1,5,5,9)	40	(1,4,9,9)	72	(1,3,6,18)	468
(2,3,4,6)	16	(2,2,4,9)	40	(2,2,2,18)	48	(1,4,4,16)	40
(4,4,4,4)	16	(2,2,8,8)	20	(2,2,4,16)	24	(1,4,10,10)	40
		(2,3,6,9)	40	(2,2,9,9)	24	(1,8,8,9)	80
		(2,4,4,8)	20	(2,2,10,10)	24	(1,9,9,9)	80
		(2,5,5,8)	20	(2,4,6,12)	24	(2,4,4,18)	80
		(3,3,6,6)	20	(2,4,8,9)	160	(2,8,8,8)	28
		(4,4,5,5)	20	(3,3,3,12)	48	(2,8,9,9)	80
		(5,5,5,5)	20	(3,4,6,8)	56	(3,6,8,9)	952
				(4,4,4,9)	112	(4,4,4,16)	28
				(4,4,8,8)	24	(4,4,9,9)	48
				(4,5,5,9)	168	(4,4,10,10)	28
				(6,6,6,6)	24	(5,5,8,8)	32
						(5,5,9,9)	80
						(7,7,7,7)	28

a. $12 < s_1 + s_2 + s_3 + s_4 \le 16$ *b.* $16 < s_1 + s_2 + s_3 + s_4 \le 20$ *c.* $20 < s_1 + s_2 + s_3 + s_4 \le 24$ *d.* $24 < s_1 + s_2 + s_3 + s_4 \le 28$

4.15 Generalized Goethals-Seidel Arrays

Denote by U_v the multiplicative group of generalized permutation matrices of order v; that is, the elements of U 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 $K\langle T\rangle$.

Definition 4.21. 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

$$\sum_{i=1}^{4} A_i A_i^\top = mI\,. \tag{4.36}$$

then the rows of

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

are mutually orthogonal.

Wallis and Whiteman [241] 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 (see §4.3).

Delsarte, Goethals and Seidel [39] 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.

Remarks

(a) Mullin and Stanton [155] 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,

(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 (see Section 4.17). Hence an equation of the form (4.36) 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 Goethals-Seidel array itself may be generalized as follows.

Definition 4.22. Let G denote the group

$$\langle r, x_1, x_1^\top, x_2, x_2^\top, \ldots, | x_i x_j = x_j x_i, x_i x_j^\top = x_j^\top x_i \quad \text{for } i,j \in \{1,2,\ldots\},\ r^2 = 1,\ r x_i r = x_i^\top \rangle$$

Denote by S the subset

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

of the integral group ring $\mathbb{Z}G$. The notion of transpose may be abstracted by defining an operation $(\ )^\top$ on $\mathbb{Z}G$ by $(x_i)^\top = xi^\top$, $(x_i^\top)^\top = x_i$, $r^\top = r$, 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 ij^{th} entry $a_{ji}^\top$. If A has entries from S and

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

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

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

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 $X_1, X_2, \ldots, Xu$ are $v \times v$ matrices from some GC-ring such that the entries of the X_i are from $\{0, \pm y_1, \pm y_2, \ldots, \pm y_\ell\}$ and

$$\sum_{i=1}^{u} s_i X_i X_i^\top = \left(\sum_{j=1}^{\ell} m_j y_j^2\right) I\,.$$

Then replacing the entries of A with the appropriate matrices yields an $OD(nv; m_1, m_2, \ldots, m_\ell)$. Examples of orthogonal designs constructed in this way are given later in this section.

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

Theorem 4.19 (Eades). *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*

$$\sum_{i=1}^{u} s_i A_i A_i^\top = \left(\sum_{j=1}^{\ell} m_j x_j x_j^\top\right) I\,.$$

then there is a GGS array of type $(m_1, m_2, \ldots, m_\ell)$ 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:

$$\begin{aligned} 0 &\mapsto \text{zero matrix of order } v; \\ \pm x_i &\mapsto \pm A_i\,; \\ \pm x_i^\top &\mapsto \pm A_i^\top\,; \\ \pm r x_i &\mapsto \pm r R A_i\,; \\ \pm r x_i^\top &\mapsto \pm r R A_i^\top\,. \end{aligned}$$

Then the resulting matrix B has entries from S and

$$\begin{aligned} BB^* &= \left(\sum_{i=1}^{u} s_i A_i A_i^\top\right) \times I_n \\ &= \left(\sum_{j=1}^{\ell} m_j x_j x_j^\top\right) I_{nv}\,. \end{aligned}$$ □

To illustrate this theorem, a GGS array of type $(2,2)$ and order 6 is constructed. The 2-circulant construction (see Example 4.12) gives a GGS array of type $(1,1)$ and order 2:

$$\begin{bmatrix} x_1 & rx_2^\top \\ -rx_2^\top & x_1 \end{bmatrix}.$$

The circulant matrices

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

satisfy $A_1 A_1^\top + A_2 A_2^\top = 2(x_1 x_1^\top + x_2 x_2^\top)I$. Following the replacements in the proof of Theorem 4.19, a GGS array of type (2, 2) and order 6 is obtained:

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

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 Remark 4.16). 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 $rx_2^\top$. The following proposition gives some infinite families of GGS arrays with 4-variables.

Proposition 4.2 (Eades). *Suppose that a is a positive integer and I is a product of at least a positive integers; that is, $\ell = \ell_1 \ell_2 \ldots \ell_j$ where $j \geq a$.*

(a) If $\ell_1 \geq > 2$ 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 $\ell_i \geq 4$ 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 $\ell_1 \geq 2$ consider the sequences $a_l = (x_1, x_2, 0_{\ell_1-2})$, $a_2 = (x_1, -x_2, 0_{\ell_1-2})$, $a_3 = (x_3, -x_4, 0_{\ell_1-2})$, $a_4 = (x_3, x_4, 0_{\ell_1-2})$, where 0_{ℓ_1-2} denotes a sequence of 0_{ℓ_1-2} zeros. These sequences are complementary, and, further, if A_i is the circulant matrix with first row a_i, then

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

Using Theorem 4.19 and the Goethals-Seidel array, a GGS array of type $(2,2,2,2)$ and order $4\ell_1$ may be obtained. Repeating this procedure a times gives (a), For (b) the following complementary sequences may be used in a similar fashion:

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

$$(4,4,4,4) : (x_1,-x_2,-x_3,-x_4),(x_1,x_2,-x_3,x_4),(x_1,x_2,x_3,-x_4),$$
$$(x_1,-x_2,x_3,x_4)\,.\square$$

A numerical investigation of GGS arrays of order 12 has been made, and the results are listed in Eades [52], These GGS arrays have been used to construct orthogonal designs of orders 36 and 60.

GGS arrays with 2-variables have been used successfully for constructing orthogonal designs of highly composite orders congruent to 2 modulo 4. Examples are given later.

It seems that GGS arrays are the most powerful method for constructing orthogonal designs from circulants in orders not divisible by 8.

4.15.1 Some Infinite Families of Orthogonal Designs

The Goethals-Seidel array and its generalizations have been used to construct many infinite families of orthogonal designs. The theorems below illustrate some of the techniques involved.

Theorem 4.20 (Eades). *If there is a GGS array of type $(s_1, s_2, \ldots, s_u)$ and order n, then there is an $OD(2n; s_1, s_1, s_2, s_2, \ldots, s_u, s_u)$.*

Proof. The negacyclic matrix

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

is an $OD(1,1)$. Hence

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

The combination of Theorem 4.20 and Proposition 4.2 gives a large collection of orthogonal designs. For example, for each $a > 0$ there is an $OD(8.5^a; 4^a, 4^a, 4^a, 4^a, 4^a, 4^a, 4^a, 4^a)$. □

Theorem 4.21 (Eades). *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 $\frac{4(q^2+q+1)}{3}$.*

This proof and additional theorems illustrating more of the techniques involved and their proofs appear explicitly in *Orthogonal Designs* (Ed. 1) p186-190.

4.15.2 Limitations

Remark 4.16. There are two ways in which the use of GGS arrays for constructing orthogonal designs is limited.

First, little is known about the existence of GGS arrays. A numerical investigation of GGS arrays of order 12 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 4.20 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 four variables is known.

Second, 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 Chapter 8). However, using the methods of Section 4.3, it can be shown that there is no $OD(14; 4, 9)$ constructed by using two 7×7 circulant matrices in the two-circulant construction.

4.16 Balanced Weighing Matrices

A most important concept in the design and analysis of experiments is that of a (v, k, λ) configuration. This is equivalent to a $(0,1)$ matrix A (the incidence matrix of the configuration) of order v satisfying

$$AA^\top = (k-\lambda)I + \lambda J\,, \qquad AJ = JA = kJ, \tag{4.37}$$

where

$$\lambda(v-1) = k(k-1) \tag{4.38}$$

It is natural, then, to ask when such a matrix can be signed in order to produce a weighing matrix $M = W(v,k)$. The work of this section is due to Mullin [152, 153], and Mullin and Stanton [154, 155].

Definition 4.23. A *balanced weighing matrix* M is a square $(0,1,-1)$ matrix such that squaring all its entries gives the incidence matrix of a (v,k,λ) configuration. That is,

$$MM^{\top} = kI_v$$

and $A = M * M$ satisfies Equation (4.37) with $\lambda(v-1) = k(k-1)$. We write M is a $BW(v,k)$.

Remark Although we will not study it here, balanced weighing matrices have proved most useful in providing previously unknown balanced incomplete block designs (see Mullin and Stanton [154, 155].

4.16.1 Necessary Conditions for the Existence of Balanced Weighing Matrices

Since a $BW(v,k)$ implies the existence of a (v,k,λ) configuration, the following conditions are known to be necessary:

(i) if v is even, then $(k-\lambda)$ must be a perfect square;
(ii) if v is odd, then the equation

$$x^2 = (k-\lambda)y^2 + (-1)[\frac{v-1}{2}]\lambda z^2 \tag{4.39}$$

must have a solution in integers other than $x = y = z = 0$. (See Ryser [171, p.111])

It is also trivial that for a $BW(v,k)$ to exist,

(iii) $\lambda = k\frac{(k-1)}{(v-1)}$ must be even.

Further we saw in Section 4.15 that for a $W(v,k)$ to exist,

(iv) if v is odd, then k must be a perfect square, and
(v) if v is odd, then $(v-k)^2 - (v-k) + 2 > v$;

and in Chapter 2,

(vi) if $v = 2 \pmod 4$, then k must be the sum of two squares.

In the event that $v \equiv 1 \pmod 4$, we note that (iv) is stronger than (ii) since if $k = \alpha^2$, then $x = \alpha$, $y = z = 1$, is a solution of equation (4.39), while for the parameters $v = 27$, $k = 13$, $\lambda = 6$ (4.39) has a solution, but k is not a perfect square. (Just note that $\langle 7,6\rangle = \langle 1,42\rangle$, and so (4.39) has a rational, hence integral, solution.) For $v \equiv 3 \pmod 4$, (iv) implies that (v) has a solution if and only if $k-\lambda$ is the sum of two squares.

4.16.2 Construction Method for Balanced Weighing Designs

The direct sum of two matrices $W(n_1,k)$ and $W(n_2,k)$ is a $W(n_1+n_2,k)$, and the Kronecker product of matrices $W(n_1,k_1)$ and $W(n_2,k_2)$ is a $W(n_1n_2,k_1k_2)$, but this is not true for balanced weighing designs since in general the property of balance is lost under these operations. This fact alone makes the construction of balanced designs difficult. This is further emphasized by the fact that the conditions (i), (ii), and the condition that $(v-1)|k(k-1)$ need not hold in general for an unbalanced design. Here we discuss the generation of balanced weighing designs from group difference sets.

Let G be a finite Abelian group of order v. If G admits a difference set $D=\{d_1,d_2,\ldots,d_k\}$ then choose $M(\chi)$ (or M) to be a type 1 incidence matrix of D obtained from the map χ.

Strictly speaking, $M(\chi)$ is determined only up to a permutation of rows and columns, but this is in no way relevant to the present discussion. Type 1 matrices have an interesting property, which we now discuss.

Definition 4.24. Let r_g denote the g^{th} row of a type 1 incidence matrix M defined on an Abelian group G. We say M has the *invariant scalar product property* (ISP property) if for all g, h, $\theta \in G$,

$$r_g \cdot r_h = r_{g+\theta} \cdot r_{h+\theta}\,,$$

where $\cdot$ denotes the usual scalar product of vectors.

Lemma 4.25. *Any type 1 matrix defined by χ on G has the ISP property.*

Proof. Note that

$$\begin{aligned} r_g \cdot r_h &= \sum_{k\in G} \chi^{(k-g)}\chi^{(k-h)} \\ &= \sum_{k\in G} \chi^{((k-\theta)-g)}\chi^{((k-\theta)-h)} \\ &= \sum_{k\in G} \chi^{(k-(g+\theta))}\chi^{((k-\theta)-h)} \\ &= r_{g+\theta} \cdot r_{h+\theta} \end{aligned}$$

as required. □

A similar result holds for column scalar products.

Lemma 4.26. *A type 1 $(0,1,-1)$ incidence matrix is a $W(v,k)$ matrix if and only if the following equation holds for all $g \in G$:*

$$\sum_{\theta \in G} \chi^{(\theta)} \chi^{(\theta+g)} = k\delta_{0,g}\,, \tag{4.40}$$

where $\delta_{0,g}$ is the Kronecker delta.

Proof. This is clear because of the ISP property

$$r_0 \cdot r_g = \sum_{\theta \in G} \chi^{(\theta)} \chi^{\theta - g)} = \sum_{\theta \in G} \chi^{\theta+g)} \chi^{(\theta)}\,. \qquad \square$$

The equality of these two summations is of practical importance since it saves calculation in verifying equation (4.39). In particular, if v is odd, one need only check $\frac{(v-1)}{2}$ equations since the nonzero elements of G can be partitioned into inverse pairs.

Lemma 4.27. *Let D be a difference set in G. Let $M = M(\chi)$ be a type 1 $(0,1,-1)$ incidence matrix. Then $M * M$ is the incidence matrix of a (v,k,λ) configuration if $\chi(g) = 0$ if and only if $g \in G - D$.*

Proof. This is evident. $\square$

Definition 4.25. We refer to a function χ satisfying the condition of Lemma 4.27 as a D-function. If the image of χ is $\{0,1,-1\}$, we call χ a restricted function. Putting these results together, we obtain:

Theorem 4.22 (Mullin). *There is a matrix $BW(v,k)$ if there is a D-function χ on an Abelian group of order v such that*

$$\sum_{\theta \in G} \chi^{(\theta)} \chi^{(\theta+g)} = k\delta_{0,g}\,.$$

This theorem can be used as a basis for a computer algorithm.

For notational convenience, given a restricted function χ on an Abelian group G, we denote $\sum_{\theta \in G} \chi^{(\theta)} \chi^{(\theta+g)}$ by $F(\chi, g)$. We demonstrate a limitation of the construction of Theorem 4.22 in the next theorem. (This can also be obtained from Lemma 4.28.)

Theorem 4.23 (Mullin). *If there is a D-function χ in an Abelian group G of order v such that $F(\chi,g) = k\delta_{0,g}$ for all $g \in G$ and v is even, then $\lambda = k\frac{(k-1)}{(v-1)}$ satisfies $\lambda \equiv 0 \pmod 4$.*

Proof. Since v is even, there exists an element $\bar{g} \neq 0$ in G such that $\bar{g} = -\bar{g}$. Let $(a_1,b_1)(a_2,b_2),\ldots,(a_t,b_t)$ be the pairs of elements of D whose difference is g. Here $t = \frac{\lambda}{2}$, since if $a_i - b_i = \bar{g}$, then $b_i - a_i = \bar{g}$. Now consider

$$F(\chi, \bar{g}) = \sum_{\theta \in G} \chi^{(\theta)} \chi^{(\theta+\bar{g})}\,.$$

The only nonzero terms in this expression arise when both θ and $\theta + \bar{g}$ belong to D, since χ is a D-function. Thus

$$F(\chi, \bar{g}) = \sum_{i=1}^{t} [\chi(a_i)\chi(b_i) + \chi(b_i)\chi(a_i)]$$
$$= 2\sum_{i=1}^{t} \chi(a_i)\chi(b_i) = 0\,.$$

Since each of the t terms in the latter sum is either 1 or -1, this expression must have $\frac{t}{2}$ terms of each value, and t must be even. This shows that $\lambda \equiv 0 \mod 4$ as required. □

There is a $(4,3,2)$ configuration C which is derivable from a difference set in the group of integers $\mod 4$; however, there is no D-function for any difference set which will produce a $BW(4,3)$. It is possible to sign the matrix of C to produce an orthogonal matrix nonetheless. More generally, there is a cyclic $\left(\frac{(3^{2n}-1)}{2}, 3^{2n-1}, 2.3^{2n-2}\right)$ configuration (since this is the complementary configuration of the set of hyperplanes in $PG(2n-1,3)$), but there is no way of signing these matrices cyclically to make them orthogonal in view of Theorem 4.23. The results of Mullin show that all of these can be signed to produce orthogonal matrices. Not all incidence matrices of (v,k,λ) configurations with v even can be signed to produce orthogonal matrices. It can be shown that the matrix of the self-dual $(16,6,2)$ configuration cannot be signed (Schellenberg [175]).

We introduce new concepts which provide a labour-saving device in the calculation associated with Theorem 4.22 in some applications.

Definition 4.26. Let R be a finite ring with unit. A restricted function χ on the additive group of R with the property that $\chi^{(1)} = 1$ is called a *normal function*. Let $U(R)$ denote the group of units of R. Let $N(R,\chi) = N(\chi)$ be defined by $N(\chi) = \{g :\ g \in U(R) | \chi(g,\theta) = \chi(g)\chi(\theta),\ \forall \theta \in R\}$.

Because of the importance of $N(\chi)$ in the next theorem, we demonstrate a structural property of this set.

Proposition 4.3. *$N(\chi)$ is a subgroup of $U(R)$.*

Proof. Let g and h be members of $M(\chi)$. Then for every $\theta \in R$, $\chi(g^{h\theta}) = \chi^{(g)}\chi^{(h\theta)} = \chi^{(g)}\chi^{(h)}\chi^{(\theta)}$. Since R is finite, the result follows. □

It is clear that χ is a linear representation of $N(\chi)$ under these circumstances.

Theorem 4.24 (Mullin). *Let R be a finite ring with unit and χ a normal function on R. Let $M(\chi)$ be defined as above.*

If $g \in N(\chi)$, then $F(\chi, g) = F(x, 1)$.

Proof. $F(\chi,g)=\sum_{\theta\in R}\chi(\theta)\chi(\theta+g)$.

Let $\tau=g^{-1}\theta$ or equivalently $\theta=g\tau$. Then, since this mapping is $1-1$, we have

$$\begin{aligned}F(\chi,g)&=\sum_{\tau\in R}\chi^{(g\tau)}\chi^{(g\tau+g)}\\&=\sum_{\tau\in R}\chi^{(g\tau)}\chi^{(g(\tau+1))}\\&=\sum_{\tau\in R}(\chi^{(g)})^2\chi^{(\tau)}\chi^{(\tau+1)}\end{aligned}$$

Since $\chi^{(g)}\chi^{(g-1)}=\chi^{(1)}=1$, $\chi^{(g)}\neq 0$ and $(\chi^{(g)})^2=1$. This yields

$$F(\chi,g)=\sum_{\tau\in R}\chi^{(\tau)}\chi^{(\tau+1)}=F(\chi,1)\,.\square$$

As an application of this result, let us consider $G=GF(7)$. Let $\chi^{(0)}=-1$, $\chi^{(1)}=\chi^{(2)}=\chi^{(4)}=1$ and $\chi^{(3)}=\chi^{(5)}=\chi^{(6)}=0$. Since the field marks 1, 2 and 4 are the quadratic residues and since $7=3 \pmod 4$, $N(\chi)=(1,2,4)$. Now $F(\chi,2)=F(\chi,4)=F(\chi,1)=\chi^{(0)}\chi^{(1)}+\chi^{(1)}\chi^{(2)}=0$, and since $G=\{0\}\cup N(\chi)\cup -N(\chi)$, we have

$$F(\chi,g)=4\delta_{0,g}\,,\qquad g\in G\,.$$

Thus M is a $W(7,4)$ matrix, But $\{0,1,2,4\}$ is a difference set, and therefore M is also a $BW(7,4)$ matrix. Thus the vector

$$(\,\bar{1}\;1\;1\;0\;1\;0\;0\,)$$

when developed cyclically $\mod 7$, generates a $BW(7,4)$.

4.16.3 Regular Balanced Weighing Matrices

Definition 4.27. If a $BW(v,k)$ matrix is such that the number of -1's per row is constant, we say that it is *regular*.

In a BW matrix we denote the number of -1's per row by $a(-1)$ and the number of 1's per row by $a(1)$. Since if M is regular, then $-M$ is also regular, we may assume that we are dealing with matrices for which $a(1)\geq\frac{k}{2}$. Clearly, every group-generated $BW(v,k)$ is regular, as is its transpose. Using this fact, Mullin [153] proved, using a somewhat different method, a generalization of a result of Schellenberg [175] which applies these to matrices $BW(v,k)$.

Lemma 4.28 (Mullin). *If a $W(v,k)$ matrix is a regular type 1 matrix, then $a(1)=(k\pm\sqrt{k})/2$ and $a(-1)=(k\pm\sqrt{k})/2$.*

Proof. The proof is a slight generalization of a result in Ryser [171, p.134]. Let $e = a(1) - a(-1)$, and J denote the $v \times v$ matrix all of whose entries are 1. Clearly, we have

$$HJ = eJ = H^\top J\,,$$

and hence

$$HH^\top J = e^2 J = kJ\,.$$

Thus

$$\begin{aligned} &e^2 = k\,,\\ &a(1) + a(-l) = k\,,\\ &a(1) - a(-1) = \pm\sqrt{k}\,, \end{aligned}$$

and the result follows. □

Corollary 4.22. *If a $W(v,k)$ matrix is a regular type 1 matrix, then k is a perfect square.*

Corollary 4.23. *If a $BW(v,k)$ matrix is a type 1 matrix, then $a(-1) \geq \frac{\lambda}{4}$ with equality if and only if $v = k = 4$.*

Proof. Let us first note that in any $BW(v,k)$ matrix, if $v = k$, then $k = \lambda$.

Now in any $BW(v,k)$ matrix, we observe that $4(v-k-1)+\lambda \geq 0$, with equality only for $v = k = \lambda = 4$. This is immediate from the fact that in any (v,k,λ) configuration, as defined earlier, we have $v \geq k$ with equality only for $v = k = \lambda$.

The above inequality implies that the inequality

$$4(\lambda v - \lambda + k) - 4k\lambda + \lambda^2 \geq 4k$$

is also valid, with equality only for $v = k = \lambda = 4$. But by the definition of λ, we have

$$k^2 = \lambda v - \lambda + k\,,$$

and therefore

$$(2k - \lambda)^2 \geq 4k\,,$$

with equality as above.

Now let us assume that $a(-1) < \frac{\lambda}{4}$. Since

$$k + \frac{\lambda k}{2} > \frac{k}{2} \geq \frac{\lambda}{2}\,,$$

the corollary is true unless

$$a(-1) = \frac{(k - \sqrt{k})}{2}.$$

Let us assume that $\frac{(k-\sqrt{k})}{2} < \frac{\lambda}{4}$. Then

$$(2k - \lambda)^2 \leq 4k,$$

which is impossible unless equality holds in which case $v = k = \lambda$ as required.

The design generated by

$$(-1, 1, 1, 1) \bmod 4$$

satisfies the corollary with equality. □

4.16.4 Application of the Frobenius Group Determinant Theorem to Balanced Weighing Matrices

For the theory of group characters, the reader is referred to Speiser [196]. For Abelian groups, the Frobenius group determinant theorem (Speiser [196, p.178]), in the notation employed here, becomes the following:

Theorem 4.25 (Frobenius Group Determinant Theorem). *Let M be a type 1 matrix over an Abelian group G of order v. Then*

$$\det M(\chi) = \prod_{j=1}^{v} \sum_{g \in G} \alpha^{(j)}(g)\chi(g),$$

where $\alpha^{(j)}$ denotes the j^{th} irreducible character of G.

For the cyclic group of order v (written as the residues modulo v), this becomes

$$\det M(\chi) = \prod_{j=0}^{v-1} \sum_{k=0}^{v-1} \omega^{jk}\chi(k),$$

where ω is a primitive v^{th} root of unity.

Any group G of order v admits the main character

$$a^{(1)}(g) = 1, \quad g \in G.$$

Every group determinant can be factored into forms in the indeterminates $\chi(g)$, which are irreducible over the integers, since it is clear that the expansion of the group determinant is a form with integer coefficients.

To illustrate the use of this theorem, we tackle the problem of finding a cyclic $BW(10, 9)$ matrix M. Using the integers mod 10, we can, without loss

of generality, assume that $\chi(g) = 0$ if and only if $g = 0$. Without any further theory, except for Lemma 4.28, there are $\binom{9}{3} = 84$ functions χ to consider. By the Frobenius group determinant theorem,

$$G(\chi) = \sum_{j=1}^{9} (-1)^j \chi(j),$$

corresponding to the character α defined by $\alpha(j) = (-1)^j$, is a divisor of $\det M = 3^{10}$.

Now let c denote the number of even residues j such that $\chi(j) = -1$. Then $G(\chi)$ can be determined in terms of c as follows:

c	$G(\chi)$
0	6
1	1
2	−3
3	−7.

There are 40 functions with $c = 1$ and 30 with $c = 2$; therefore, the number of functions to be investigated has been reduced. Moreover, we have some structural information. As we shall see, the structural information is extremely important. In the following, if $\chi(g) = x$, we say that x appears in position g.

We note now that the inner product of absolute values of any pair of distinct rows is 8, since $\lambda = 8$ in the associated symmetric design. Thus the number of terms with value -1 in $r_0 \cdot r_j$ must be 4 for $j = 1, 2, \ldots, 9$.

In particular, this means that in r_0 and r_j the number of times 0 opposes -1 must be even, that is, 0 or 2. Hence if translation (of row 0) by j units moves 0 to a position containing -1, then there must be a -1 in position $-j$ which is translated to column zero. Thus -1's occur in pairs of inverse positions.

Now let us consider the case of $c = 2$. There is exactly one -1 on an odd residue. But since the parity of inverse pairs is equal, this -1 must be in position 5; that is, $\chi(5) = 1$. Now it is easily verified (considering row 1) that the three -1's cannot be consecutive in any event, and thus the remaining -1's occur in inverse pairs of positions $\chi(4) = \chi(6) = 1$. Also since $c = 2$, $\chi(1) = \chi(3) = \chi(7) = \chi(9) = 1$, and $\chi(2) = \chi(8) = -1$. We have determined the only possible function χ with $c = 2$. However, for this function $r_0 \cdot r_1 = -4$, and the matrix is not orthogonal.

Let us now consider the case $c = 1$. Clearly, no solution exists in this case since there is only one self-inverse element 5, which is odd. Hence there is no cyclic $BW(10, 9)$ matrix.

4.16.5 Balanced Weighing Matrices with $v \leq 25$

Comment 4.1. In Table 4.18 we give a list of all triples v, k, λ with $k > \lambda > 0$ which satisfy $\lambda(v-1) = k(k-1)$ and $\lambda \equiv 0 \bmod 2$. We also list a function $E(v,k) = E$ where $E(v,k) = 1$ if a matrix $B(v,k)$ exists, and $E(v,k) = 0$ otherwise. In this regard it is useful to note that the matrices $BW(4n, 4n-1)$ are coexistent with skew Hadamard matrices of order $4n$ and that matrices $BW(4n+2, 4n+1)$ are coexistent with symmetric Hadamard matrices. The list of values for which such designs are known to exist are listed in Wallis [231].

Table 4.18 triples v, k, λ with $k > \lambda > 0$ satisfying $\lambda(v-1) = k(k-1)$ and $\lambda \equiv 0 \mod 2$.

	v	k	λ	E	Reason or Reference
1)	4	3	2	yes	Mullin
2)	6	5	4	yes	*, Complement $PG(1,5)$
3)	7	4	2	yes	Circulant with first row [−110100].
4)	8	7	6	yes	*, Complement $PG(1,7)$.
5)	10	9	8	yes	*, Complement $PG(1,9)$.
6)	11	5	2	no	Condition (iv).
7)	12	11	10	yes	*, Complement $PG(1,11)$.
8)	13	9	4	yes	Condition (v).
9)	14	13	12	no	*, Complement $PG(1,13)$.
10)	15	8	4	no	Condition (iv).
11)	16	6	2	no	Schellenberg
12)	16	10	6		
13)	16	15	14	yes	*
14)	18	17	16	yes	*, Complement $PG(1,17)$,
15)	19	9	4		
16)	20	19	18	yes	*, Complement $PG(1,19)$.
17)	21	16	12	yes	*, Complement $PG(2,4)$.
18)	22	7	2	no	Condition (i).
19)	22	15	10	no	Condition (i).
20)	22	21	20	no	Condition (vi).
21)	23	12	6	no	Condition (iv).
22)	24	23	22	yes	*, Complement $PG(1,23)$.
23)	25	16	10		

*see Comment 4.1

In view of our earlier remarks about the usefulness of $BW(v,k)$'s it would be of interest to establish the existence of more of these matrices. This will now be discussed.

4.16.6 There are No Circulant Balanced Weighing Matrices $BW(v,v-1)$ Based on $(v,v-1,v-2)$ Configurations

Without loss of generality we assume that in such matrices the element 0 occurs down the main diagonal.

Lemma 4.29. *In any circulant orthogonal matrix based on a (v,k,λ) configuration, the parameter k is a perfect square.*

Proof. Suppose that the first row of the orthogonal matrix contains a entries of 1 and b entries of -1. By the circulant property, every row and column has sum $a-b$. If the matrix is denoted by N, we have

$$NJ = N^\top J = (a-b)J\,.$$

But

$$NN^\top = kI\,.$$

Hence

$$NN^\top J = kIJ = kJ\,.$$

But

$$NN^\top J = N(a-b)J = (a-b)^2 J\,.$$

Thus

$$k = (a-b)^2\,. \qquad \square$$

In the following we assume without loss of generality that $a > b$; otherwise we multiply the entire matrix by -1. For convenience we set $a-b=t$.

Lemma 4.30. *If a denotes the number of 1's in the first row of an orthogonal circulant matrix, and b the number of -1's, then*

$$a = \tfrac{1}{2}\left(t^2+t\right) \text{ and } b = \tfrac{1}{2}\left(t^2-t\right)\,.$$

Proof. This is immediate since

$$\begin{aligned} a+b &= k = t^2 \\ a-b &= t\,. \end{aligned}$$

Thus in looking for circulant orthogonal matrices based on trivial designs, we need only consider (t^2+1, t^2, t^2-1) configurations where t is odd. □

Definition 4.28. An orthogonal circulant based on a (t^2+1, t^2, t^2-1) configuration will henceforth be called a *trivial circulant*.

Let $x_{\alpha\beta}$ $(\alpha, \beta = 0, 1, 2)$ represent the number of times that α in row i is in the same column as β in row j (we use 2 to represent the entry -1). We require

Lemma 4.31. *Either* $x_{01} = x_{10} = 1$, $x_{02} = x_{20} = 0$, *or vice versa.*

Proof. We actually determine all $x_{\alpha\beta}$. It is clear that

$$\text{i)} \qquad \sum x_{\alpha\beta} = t^2 + 1,$$

$$\text{ii)} \qquad \sum x_{0j} = \sum x_{i0} = 1,$$

$$\text{iii)} \qquad \sum x_{1j} = \sum x_{i1} = \frac{1}{2}(t^2 + t)$$

$$\text{iv)} \qquad \sum x_{2j} = \sum x_{i2} = \frac{1}{2}(t^2 - t)$$

Finally, orthogonality gives

$$\text{v)} \qquad x_{11} + x_{22} = x_{12} + x_{21}.$$

But $x_{11} + x_{22} + x_{12} + x_{21} = \lambda$, and thus each expression in v) equals $\frac{1}{2}(t^2-1)$. From iii) and iv), addition gives

$$x_{10} + x_{20} = 1 = x_{01} + x_{02}\,; x_{00} = 0\,.$$

Also

$$x_{10} - x_{01} = x_{02} - x_{20} = x_{21} - x_{12} = \text{ an even number.}$$

This proves that $x_{10} = x_{01}$, $x_{02} = x_{20}$, as required. It is useful to record the table of values following. □

	Case A	Case B
x_{00}	0	0
$x_{01} = X_{10}$	1	0
$x_{02} = X_{20}$	0	1
$x_{12} = X_{21}$	$\frac{1}{4}t^2 - 1$	$\frac{1}{4}t^2 - 1$
x_{11}	$\frac{1}{4}(t+3)(t-1)$	$\frac{1}{4}(t-1)^2$
x_{22}	$\frac{1}{4}(t+1)^2$	$\frac{1}{4}(t-3)(t+1)$

In the light of Lemma 4.31, we note that we can write $v = 4m+2$, $k = 4m+1 = t$, $\lambda = 4m$, and the typical circulant has the following form (illustration for $m = 6$).

$$\text{Row 1:} \quad 0a_1a_2 \ldots a_{11}a_{12}\theta a_{12}a_{11} \ldots a_3a_2a_1$$

(The symmetry of the sequence is guaranteed by the fact that $0x_{0i} = x_{i0}$ for $i = 1, 2$.)

Row j is obtained by a cyclic shift through $j-1$ places to the right.

We now prove:

Lemma 4.32. $\theta = 1$ *if* $t \equiv 1 \pmod 4$; $\theta = -1$ *if* $t \equiv 3 \pmod 4$. *Also*

$$\sum_{j=1}^{m} a_{2j} = 0, \qquad \sum_{i=0}^{m-1} a_{2i+1} = \frac{t-\theta}{2}$$

Proof. Take the scalar products of row 1 with rows $2, 4, 6, \ldots 2m+2$; add, and re-arrange. We have

$$2(a_1 + a_3 + \cdots + a_{2m-1})(a_2 + a_4 + \cdots + a_{2m}) + \theta(a_2 + a_4 + \cdots + a_{2m}) = 0.$$

Thus

$$(2a_1 + \cdots + 2a_{2m-1} + \theta)(a_2 + a_4 + \cdots + a_{2m}) = 0;$$

Thus since only the second integer is even, we get $\sum a_{2j} = 0$. Also, since $2\sum a_{2n} + 2\sum a_{2j} + \theta = t$, we find that $\sum a_{2i} = \frac{t-\theta}{2}$.

Finally, note that the sum $\sum a_{2i}$ is an even integer (m terms); thus $t - \theta$ is divisible by 4, and $\theta = 1$ for $t \equiv 1 \pmod 4$, $\theta = -1$ for $t \equiv 3 \pmod 4$. This completes the proof. □

Actually, if one takes scalar products of row 1 with rows $3, 5, \ldots, 2m+1$, and adds, one gets the identity

$$\left(\sum a_{2i}\right)\left(\sum a_{2i} + \theta\right) + \left(\sum a_{2j}\right)^2 = m,$$

which also produces the desired results.

Example 4.25. At this stage, it is most instructive to look at the example for $m = 6$, The scalar products for rows $2, 4, 6, 8, 10, 12$ are written down as follows.

1) $\displaystyle\sum_{i=1}^{12} a_i a_{i+1} = 0 \, (a_{13} = \theta)$.

In the sequence $a_l, a_2, a_3, \ldots, a_{13}$ there must be exactly six sign changes to produce a zero sum in 1). Hence a_1 has the same sign as a_{13}; that is,

2) $a_1a_2 + \sum_1^{10} a_i a_{i+3} + a_{11}a_{12} = 0\,.$

Write the sequence

$$a_3, a_6, a_9, a_{12}, a_{11}, a_8, a_5, a_2, a_1, a_4, a_7, a_{10}, a_{13}\,.$$

By the same argument, $a_3 = 0$.

3) $a_1a_4 + a_2a_3 + \sum_1^{8} a_i a_{i+5} + a_9a_{12} + a_{10}a_{11} = 0\,.$

Consider the sequence

$$a_5, a_{10}, a_{11}, a_6, a_1, a_4, a_9, a_{12}, a_7, a_2, a_3, a_8, \theta\,,$$

and we get $a_5 = 0$.

4) $a_1a_6 + a_2a_5 + a_3a_5 + \sum_1^{6} a_i a_{i+7} + a_7a_{12} + a_9a_{10} = 0\,.$

The relevant sequence is

$$a_7, a_{12}, a_5, a_2, a_9, a_{10}, a_3, a_4, a_{11}, a_8, a_1, a_6, \theta\,,$$

and the result is $a_7 = 0$.

5) $a_1a_8 + a_2a_7 + a_3a_6 + a_4a_5 + \sum_1^{4} a_i a_{i+9} + a_5a_{12} + a_6a_{11} + a_7a_{10} + a_8a_9 = 0\,.$

Hence, the sequence

$$a_9, a_8, a_1, a_{10}, a_7, a_2, a_{11}, a_6, a_3, a_{12}, a_5, a_4, \theta \quad \text{proves } a_9 = 0\,.$$

Similarly, $a_{11} = \theta$, and $\sum a_{2i+1} = 6\theta = 6$ (a contradiction of Lemma 4.32).

The method outlined is completely general and gives:

Lemma 4.33. *In an orthogonal circulant of the type we have been considering, with one zero per row, we have*

$$a_1 = a_3 = \cdots = a_{2m-1} = \theta\,.$$

Thus

$$\sum a_{2i+1} = m\theta = \tfrac{1}{2}\,(t - \theta)\,.$$

It is easy to deduce, from Lemma 4.33, that

$$t = \theta(2m+1)\,.$$

But $t^2 = 4m+1$, and so $4m+1 = (2m+1)^2$.

We conclude that $m = 0$ and state:

Theorem 4.26. *An orthogonal circulant with one zero per row only exists for $m = 0$; in this case, it is the identity matrix of order 2 or, equivalently, the transposition matrix of order 2.*

4.17 Negacyclic Matrices

A type of weighing matrix, of weight n and weight $n-1$, called a C-matrix or conference matrix, was previously studied by Delsarte-Goethals-Seidel [39]. These can be based on circulant or on negacyclic matrices. We consider these negacyclic based matrices with weight $k \leq n$.

Definition 4.29. Let P, called the "negacyclic shift matrix" be the square matrix of order n, whose elements p_{ij} are defined as follows:

$$\begin{aligned} p_{i,i+1} &= 1, \quad i = 0,1,\ldots,n-2, \\ p_{n-1,0} &= -1, \\ p_{ij} &= 0, \quad \text{otherwise.} \end{aligned}$$

Any matrix of the form $\sum a_i P^i$, with a_i commuting coefficients, will be called *negacyclic*.

We see there are similarities but not necessarily sameness between the properties of circulant/cyclic matrices and negacyclic matrices.

Lemma 4.34. *Let $P = (p_{ij})$ of order n be a negacyclic matrix. Then*

(i) The inner product of the first row of P with the i^{th} row of P equals the negative of the inner product of the first row of P with the $(-i+2)^{nd}$ row. That is

$$\sum_{j=1}^{n} p_{1j}p_{ij} = -\sum_{j=1}^{n} p_{1j}p_{n-i+2,j} \tag{4.41}$$

(This is the negative of the result for circulant/cyclic matrices).

(ii) The inner product of the first row of P with the i^{th} row of P equals the inner product of the k^{th} row of P with the $(i+k-1)^{st}$ row of P. That is

$$\sum_{j=1}^{n} p_{1j}p_{ij} = \sum_{j=1}^{n} p_{jk}p_{i+k-1,j} \tag{4.42}$$

(This is the same result as for circulant/cyclic matrices).

(iii) Then P of order n satisfies

$$P^n = -1, \quad P^\top = -P^{n-1}, \quad PP^\top = I.$$

If $A = \sum a_i P^i$, $B = \sum b_j P^j$ and R is the back diagonal matrix, then

$$AB = BA \ \text{ and } \ A(BR)^\top = BRA^\top.$$

A and BR are amicable matrices.

We now note some other properties of negacyclic matrices which were shown by L.G. Kovacs and Peter Eades [52]. The second result appears in Geramita and Seberry [80, p.206–207]. We give the proof here to emphasize a result which appears to have been forgotten.

Lemma 4.35. *If $A = \sum a_i P^i$ is a negacyclic matrix of odd order n, then XAX, where $X = diag(1,-1,1,-1,\ldots,1)$, is a circulant matrix.*

Lemma 4.36. *Suppose $n \equiv 0 \pmod 2$. The existence of a negacyclic $C = W(n,n-1)$ is equivalent to the existence of a $W(n,n-1)$ of the form*

$$\begin{bmatrix} A & B \\ B^\top & -A^\top \end{bmatrix} \tag{4.43}$$

where A and B are negacyclic, $A^\top = (-1)A^{n/2}A$. That is the 2-block suitable matrix gives a weighing matrix which is equivalent to a 1-block matrix.

Proof. First we suppose there is a negacyclic matrix $N = W(2n,2n-1)$ of order 2 which is used to form two negacyclic matrices A and B of order n which satisfy

$$AA^\top + BB^\top = (2n-1)I. \tag{4.44}$$

Let the first row of the negacyclic matrix N be

$$0x_1y_1x_2y_2\ldots y_{n-1}x_n$$

We choose A and B to be negacyclic matrices with first rows

$$0y_1y_2\ldots y_{n-1}, \text{ and } x_1x_2\ldots x_n,$$

respectively. If the order $n = 2t+1$ is odd and the first rows of A and B are

$$0a_1\ldots a_t\,(\epsilon_t a_t)\ldots(\epsilon_1 a_1) \text{ and } 1b_1b_2\ldots b_t\,(\delta_t b_t)\ldots(\delta_1 b_1),$$

with $\epsilon_i = \pm 1$, $\delta_j = \pm 1$, then taking the dot product of the first and $(i+1)^{\text{th}}$ rows, $i \le t$ (reducing using $xy \equiv x+y-1 \pmod 4$), we obtain

$$2t-2i+\epsilon_i \pmod 4 \text{ and } 2t-2i+1 \pmod 4,$$

respectively. Hence using equation (4.44),

$$\epsilon_i + 1 \equiv 0 \pmod 4,$$

we have $\epsilon_i = -1$.

If the order n is even and the first rows of A and B are

$$0a_1 \dots a_{t-1} a_t (\epsilon_{t-1} a_{t-1}) \dots (\epsilon_1 a_1)$$

and

$$1b_1 b_2 \dots b_t (\delta_{t-1} b_{t-1}) \dots (\delta_1 b_1),$$

with $\epsilon_i = \pm 1$, $\delta_j = \pm 1$, then taking the dot product of the first and $(\mathrm{i}+1)^{\mathrm{th}}$ rows, $i \le t-1$ (reducing modulo 4), we obtain

$$2t - 2t - 1 + \epsilon_i \pmod 4 \text{ and } 2t - 2i + 2b_i - 2 \pmod 4,$$

respectively. Hence, using equation (4.44),

$$\epsilon_i + 2b_i - 3 \equiv 0 \pmod 4,$$

and since $b_i \neq 0$, we have $\epsilon_i = 1$.

This means the first row of the original negacyclic matrix of order $2n$ can be written as

$$0x_1 a_1 x_2 a_2 \dots x_t a_t 1 \bar{a}_t (\delta_t x_t) \bar{a}_{t-1} \dots \bar{a}_2 (\delta_2 x_2) \bar{a}_1 (\delta_1 x_1) \text{ for } n \text{ odd}$$

and

$$0x_1 a_1 x_2 a_2 \dots a_{t-1} x_t a_t (\delta_t x_t) a_{t-1} \dots a_2 (\delta_2 x_2) a_1 (\delta_1 x_1) \text{ for } n \text{ even}$$

with $\delta_j \neq \pm 1$ and $\bar{a}_i = -a_i$.

The inner product of the first and $(2i-1)^{\mathrm{th}}$ rows, $i \le t$ and $t-1$ respectively, is

$$-\delta_i + 1 \equiv 0 \pmod 4 \text{ and } \delta_i + 1 \equiv 0 \pmod 4.$$

So we have the first rows of A and B

$$0a_1 \dots a_t \bar{a}_t \dots \bar{a}_1 \text{ and } b_1 b_2, \dots b_t 1 b_t \dots b_2 b_1 \text{ for } n \text{ odd} \tag{4.45}$$

and

$$0a_1 \dots a_{t-1} a_t a_{t-1} \dots a_1 \text{ and } b_1 b_2 \dots b_t \bar{b}_t \dots \bar{b}_2 \bar{b}_1 \text{ for } n \text{ even} \tag{4.46}$$

as required.

It is straightforward to check that negacyclic matrices A and B, which satisfy $AA^\top + BB^\top = (2n-1)I_n$ and are of the form (4.45) and (4.46), give a negacyclic matrix $W(2n, 2n-1)$ when formed into first rows

$$0b_1 a_1 b_2 \dots b_t a_t 1 \bar{a}_t b_t \dots \bar{a}_l b_1, \text{ for } n \text{ odd},$$

or

$$0b_1a_1b_2\ldots b_ta_t\bar{b}_t\ldots a_1\bar{b}_1 \text{ for } n \text{ even.}\square$$

Example 4.26. The first rows of negacyclic matrices $(n, n-1)$ of orders 4, 6, 8, and 10, respectively;

$$\begin{array}{l} 0\,1\,1\,-, \\ 0\,1\,-\,1\,1\,1 \\ 0\,1\,1\,-\,1\,1\,1\,- \\ 0\,1\,1\,-\,1\,-\,-\,-\,-\,1. \end{array}$$

are equivalent to the existence of

$$\begin{bmatrix} 0 & 1 \\ - & 0 \end{bmatrix}, \begin{bmatrix} 1 & - \\ 1 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & - & 1 \\ - & 0 & - \\ 1 & - & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ - & 1 & 1 \\ - & - & 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ - & 0 & 1 & 1 \\ - & - & 0 & 1 \\ - & - & - & 0 \end{bmatrix}, \begin{bmatrix} 1 & - & 1 & - \\ 1 & 1 & - & 1 \\ - & 1 & 1 & - \\ 1 & - & 1 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 1 & 1 & - & - \\ 1 & 0 & 1 & 1 & - \\ 1 & 1 & 0 & 1 & 1 \\ - & 1 & 1 & 0 & 1 \\ - & - & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & - & - & - & 1 \\ - & 1 & - & - & - \\ 1 & - & 1 & - & - \\ 1 & 1 & - & 1 & - \\ 1 & 1 & 1 & - & 1 \end{bmatrix}$$

Comment. Peter Eades [52] and Delsarte-Goethals-Seidel [39] have determined that the only negacyclic $W(v, v-1)$ of order $v < 1000$ have $v = p^r + 1$ where p^r is an odd prime power. On the positive side we know (we omit the proof):

Theorem 4.27 (Delsarte-Goethals-Seidel [39]). *There is a negacyclic $W(p^r+1, p^r)$ whenever p^r is an odd prime power.*

G. Berman [21] has led us to believe that many results of a similar type to those found for circulant matrices can be obtained using negacyclic matrices. Negacyclic matrices are curiosities because of their properties and potential exhibited in Lemma 4.36 and Example 4.27.

Example 4.27. The four negacyclic matrices

$$A_1 = \begin{bmatrix} 1 & - & 0 & 0 & 0 \\ 0 & 1 & - & 0 & 0 \\ 0 & 0 & 1 & - & 0 \\ 0 & 0 & 0 & 1 & - \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix} \quad A_2 = \begin{bmatrix} 1 & 1 & - & - & 0 \\ 0 & 1 & 1 & - & - \\ 1 & 0 & 1 & 1 & - \\ 1 & 1 & 0 & 1 & 1 \\ - & 1 & 1 & 0 & 1 \end{bmatrix}$$

$$A_3 = \begin{bmatrix} 0 & - & 0 & 0 & 1 \\ - & 0 & - & 0 & 0 \\ 0 & - & 0 & - & 0 \\ 0 & 0 & - & 0 & - \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad A_4 = \begin{bmatrix} 0 & - & 0 & 0 & 0 \\ 0 & 0 & - & 0 & 0 \\ 0 & 0 & 0 & - & 0 \\ 0 & 0 & 0 & 0 & - \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

satisfy

$$A_1A_1^\top + A_2A_2^\top + A_3A_3^\top + A_4A_4^\top = 9I\,.$$

They can be merged to form two negacyclic matrices

$$B_1 = \begin{bmatrix} 1\ 0\ -\ -\ 0\ 0\ 0\ 0\ 0\ 1 \\ -\ 1\ 0\ -\ -\ 0\ 0\ 0\ 0\ 0 \\ \text{etc.} \end{bmatrix}$$

$$B_2 = \begin{bmatrix} 1\ 0\ 1\ -\ -\ 0\ -\ 0\ 0\ 0 \\ 0\ 1\ 0\ 1\ -\ -\ 0\ -\ 0\ 0 \\ \text{etc.} \end{bmatrix}$$

which satisfy

$$B_1B_1^\top + B_2B_2^\top = 9I\,.$$

These can be further merged to obtain the first row of a negacyclic $W(20,9)$:

$$1\ \ 1\ \ 0\ \ 0\ \ -\ \ 1\ \ -\ \ -\ \ 0\ \ -\ \ 0\ \ 0\ \ 0\ \ -\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0.$$

Negacyclic matrices are worthy of further existence searches. The question of when negacyclic matrices can be decomposed as in Example 4.27 is open for further research.

4.17.1 Constructions

We recall suitable (plug-in) matrices $X_1, X_2, X_3, X_4, \cdots X_t$ are t matrices of order n, with elements ± 1 which satisfy the additive property, $\sum_{i=1}^{t} X_i X_i^\top =$ constant times the identity matrix. They are suitable if they satisfy other equations which enable them to be substituted into a plug-into array to make an orthogonal matrix (see Definition 4.4). Xia, Xia and Seberry [251] show 4-suitable plug-in negacyclic matrices of odd order exist if and only if 4-suitable plug-in circulant matrices exist for the same odd order. 4-suitable negacyclic matrices of order n, may be used instead of 4-suitable circulant matrices, in the Goethals-Seidel plug-into array [88], to construct Hadamard matrices and orthogonal designs of order $4n$. Other useful plug-into arrays are due to Kharaghani, Ito, Spence, Seberry-Balonin and Wallis-Whiteman [114, 115, 120, 182, 198, 241].

In computer searches, for some even orders, 2-suitable or 4-suitable negacyclic matrices have proved easier to find. This experimental fact has been used extensively by Holzmann, Kharaghani and Tayfeh-Rezaie [66, 67, 104, 105, 122] to complete searches for OD's in orders 24, 46, 48, 56, and 80. We note that if there are 2-suitable negacyclic matrices of order n and Golay sequences of order m, there are 2-suitable matrices of order mn.

This means a negacyclic matrix may give 2-suitable and 4-suitable plug-in matrices to use in plug-into arrays to make larger orthogonal matrices.

From Table 4.19 there exist $W(12,k)$ constructed using two negacyclic matrices of order 6 for $k = 1,2,\ldots,12$. From Delsarte-Goethals-Seidel [39], there exists $0,\pm 1$ negacyclic $W(12,11)$. Results for 7, 9, and 11 are due to Gene Awyzio [13] and Tianbing Xia [250].

Table 4.19 First rows of $W(12,k)$ constructed from two negacyclic matrices of order 6 [a]

k	First Rows	k	First Rows
1	$1\,0\,0\,0\,0\,0\,;\,0_6$	7	$0\,1\,1\,1\,-\,1\,;\,1\,0\,0\,1\,0\,0$
2	$1\,0_5\,;\,1\,0_5$	8	$1\,1\,-\,1\,0_2\,;\,1\,1\,1\,-\,0_2$
3	$1\,0\,0\,1\,0\,;\,1\,0_5$	9	$0\,1\,1\,-\,1\,1\,;\,1\,0\,1\,-\,0\,-$
4	$1\,1\,0_4\,;\,1\,-\,0_4$	10	$0\,1\,1\,1\,-\,1\,;\,0\,1\,1\,1\,-\,1$
5	$1\,1\,-\,0_3\,;\,1\,0\,1\,0_3$	11	$0\,1\,1\,-\,1\,1\,;\,1\,-\,1\,1\,1\,1$
6	$0\,1\,1\,1\,-\,1\,;\,1\,0_5$	12	$1\,1\,1\,1\,-\,1\,;\,-\,1\,1\,1\,-\,1$

[a] G. Awyzio [13] and T. Xia [250]

Remark 4.17. The question of which $W(4n,k)$ can be constructed using two negacyclic $0,\pm 1$ matrices of order $2n$ has yet to be resolved.

It is easy to see that there exist $W(2n,k)$ constructed from 2 negacyclic matrices of order n whenever there exist two 0, ± 1 sequences of length n and weight k with NPAF zero.

Using results obtained by Awyzio (private communication) and Tianbing Xia (private communication) we conjecture:

Conjecture 4.5. Suppose n, $n \equiv 2 \pmod 4$ and k, the sum of two squares, are integers. Then there exists a $W(2n,k)$ constructed via two negacyclic $(0,1,-1)$ matrices.

4.17.2 Applications

In Ang et al [8], 4-suitable negacyclic matrices are used to construct new orthogonal bipolar spreading sequences for any length 4 (mod 8) where the resultant sets of sequences possess very good autocorrelation properties that make them amenable to synchronization requirements. In particular, their aperiodic autocorrelation characteristics are very good.

It is well known, e.g. [222, 249], that if the sequences have good aperiodic cross-correlation properties, the transmission performance can be improved for those CDMA systems where different propagation delays exist.

Orthogonal bipolar sequences are of a great practical interest for the current and future direct sequence (DS) code-division multiple-access (CDMA) systems where the orthogonality principle can be used for channels separation, e.g. [8]. The most commonly used sets of bipolar sequences are Walsh-Hadamard sequences [222], as they are easy to generate and simple to implement. However, they exist only for sequence lengths which are an integer power of 2, which can be a limiting factor in some applications. The overall autocorrelation properties of the modified sequence sets are still significantly better than those of Walsh-Hadamard sequences of comparable lengths.

4.17.3 Combinatorial Applications

For combinatorial applications see [21, 22, 89, 117, 121].

We also see from papers [100, 102, 104, 105] that OD's in orders 24, 40, 48, 56, 80, that had proved difficult to constructed using circulant matrices were found using negacyclic matrices.

Chapter 5
Amicable Orthogonal Designs

In this chapter we consider the theory of amicable orthogonal designs and some of their usage.

Interest in amicable orthogonal designs was renewed by the paper of Tarokh, Jafarkhani and Calderbank [209] which showed how they could be used in mobile communications. A delightful introduction to the use of orthogonal designs for CDMA codes for communications has been given by Adams [1]. We notice that for communications the matrices need not be square and may have combinations of complex or quaternion elements. Amicability increases the number of messages which can be transmitted simultaneously but suitable designs have been difficult to find.

In Chapter 6 we will consider families and systems which further generalize the concept of amicability.

5.1 Introduction

In the paper, Geramita-Geramita-Wallis [77], the following remarkable pairs of orthogonal designs are given:

$$X = \begin{bmatrix} x_1 & x_2 \\ x_2 & -x_1 \end{bmatrix}; \qquad Y = \begin{bmatrix} y_1 & y_2 \\ -y_2 & y_1 \end{bmatrix}. \tag{5.1}$$

$$X = \begin{bmatrix} x_1 & x_2 & x_3 & x_3 \\ -x_2 & x_1 & x_3 & -x_3 \\ x_3 & x_3 & -x_1 & -x_2 \\ x_3 & -x_3 & x_2 & -x_1 \end{bmatrix}; \qquad Y = \begin{bmatrix} y_1 & y_2 & y_3 & y_3 \\ y_2 & -y_1 & y_3 & -y_3 \\ -y_3 & -y_3 & y_2 & -y_1 \\ -y_3 & y_3 & -y_1 & y_2 \end{bmatrix}. \tag{5.2}$$

They have the property that $XY^\top = YX^\top$.

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5_5

The existence of just these two pairs of orthogonal designs has the following useful consequences.

Proposition 5.1. *If there is an orthogonal design* $OD(n;a,b)$*, then*

(i) there is an orthogonal design $OD(2n;a,a,b,b)$*;*
(ii) there is an orthogonal design $OD(4n;a,a,2a,b,b,2b)$*.*

Proof. (i) Let the $OD(n)$ be on the variables $z_1,\ z_2$. Using X and Y as in (5.1) above and setting $z_1 = X$ and $z_2 = Y$ gives the result.
(ii) is proved analogously using the X and Y from (5.2) above. □

The following replication result was obtained.

Corollary 5.1. *If all* $OD(n;1,k)$*,* $1 \le k \le n-1$*, exist in order* n*, then all* $OD(n;1,\ell)$*,* $1 \le \ell \le 2n-1$*, exist in order* $2n$*.*

Corollary 5.2. *If all* $OD(n;a,b,n-a-b)$ *exist then all* $OD(2n;x,y,2n-x-y)$ *exist.*

Example 5.1. There is an $OD(4;1,1;2)$ and so if $n = 2^s$, there are $OD(2^s;1,k)$, $1 \le k \le 2^s - 1$. In particular, there are weighing matrices $W(k,k)$, for all $k \le n$, when $n = 2^s$.

This very simple application of the existence of pairs of orthogonal designs like (5.1) and (5.2) and other replications that come from them proved that such pairs would be extremely important in constructing OD themselves. Consequently, it was suggested [77] that these examples be studied in greater detail.

This suggestion was taken up by Warren Wolfe in his Queen's University dissertation [247] and was a major breakthrough not only in the study of such pairs of orthogonal designs but in the study of OD themselves. A major portion of this chapter is devoted to an exposition of this aspect of Wolfe's contributions.

Subsequent to Wolfe's work on this problem, he and D. Shapiro had an opportunity to meet and discuss Wolfe's work. Shapiro was greatly interested in Wolfe's handling of the problem and saw that what had begun as two interesting examples could in fact be the basis for the study of an interesting aspect of the theory of quadratic forms. Using a different approach, Shapiro has brilliantly analysed this problem about quadratic forms in (Shapiro [194]). His work has had deep implications back into the combinatorial problems that originally motivated the entire discussion. This happy state of affairs will be briefly discussed in this chapter.

5.2 Definitions and Elementary Observations

Definition 5.1. Let X be an $OD(n;u_1,\dots,u_s)$ on variables $\{x_1,\dots,x_s\}$ and Y an $OD(n;v_1,\dots,v_t)$ on the variables $\{y_1,\dots,y_t\}$. It is said that X and Y are *amicable orthogonal designs* if $XY^\top = YX^\top$.

It was observed that writing $Z = XY^\top$, forces $ZZ^\top = (u_1x_1^2 + \cdots + u_sx_s^2)(v_1y_1^2, + \cdots + v_ty_t^2)I_n$. So amicable OD are related to symmetric Z which have inner product factorization into quadratic forms.

Notation 5.1. With X, Y as above it will be said that there are $AOD(n : (u_1,\dots,u_s); (v_1,\dots,v_t))$.

With this notation, examples (5.1) and (5.2) are amicable $AOD(2:(1,1);(1,1))$ and $AOD(4:(1,1,2);(1,1,2))$, respectively.

Example 5.2. Before christening these pairs, and after finding a few it was realized that such things had already been anticipated in the study of Hadamard matrices. Namely, in [228] the study of pairs of Hadamard matrices $W = I+S$ and M, where W, M have order $= n$, $S = -S^\top$, $M = M^\top$ and $WM^\top = MW^\top$, was extensively pursued and many examples discovered. These *amicable Hadamard matrices* are an important special case of amicable orthogonal designs. They have type $AOD(n:(1,n-1);(n))$ in order n.

Let X and Y be amicable orthogonal designs $AOD(n:(u_1,\dots,u_s);(v_1,\dots,v_t))$. Write

$$X = \sum_{i=1}^{s} A_i x_i,\ Y = \sum_{j=1}^{t} B_j y_j\,. \tag{5.3}$$

The fact that x's and y's are assumed to commute and that $\mathbb{Z}$ is an infinite integral domain easily yields:

(0) The A_i and B_j are all $0,1,-1$ matrices, and $A_i * A_\ell = 0,\ 1 \le i \ne \ell \le s$, $b_j * B_k = 0,\ 1 \le j \ne k \le t$.
(i) $A_iA_i^\top = u_iI_n,\ 1 \le i \le s$; $B_jB_j^\top = v_jI_n,\ 1 \le j \le t$.
(ii) $A_iA_\ell^\top + A_\ell A_i^\top = 0,\ 1 \le i \ne \ell \le s$; $B_jB_k^\top + B_kB_j^\top = 0,\ 1 \le j \ne k \le t$.
(iii) $A_iB_j^\top = B_jA_i^\top,\ 1 \le i \le s,\ l \le j \le t$.

Conditions (0), (i) and (ii) are not new. They are just the assertions that X and Y exist (ie, OD of that order and type exist). Condition (iii) is the new one. It is seen, again, the dichotomy between algebraic and combinatorial properties: (i), (ii) and (iii) can, and will, be treated separately from (0). This was, in fact, Wolfe's approach to the problem, ie, to just consider (at first) conditions (i), (ii) and (iii). (Oddly enough, it was first in the study of amicable OD that the algebraic and combinatorial distinctions became clear. The treatment given in this text, especially in Chapter 3, is a classic story of hindsight! It is to Wolfe's credit that he forced this distinction.)

It is clear that conditions (0) to (iii) are necessary and sufficient for the existence of $AOD(n:(u_1,\ldots,u_s);(v_1,\ldots,v_t))$. For reference here it is stated precisely.

Proposition 5.2. *A necessary and sufficient condition that there exist amicable OD, X and Y $AOD(n:(u_1,\ldots,u_s);(v_1,\ldots,v_t))$ is that there exists a family of matrices $\{A_1,\ldots,A_s;B_1,\ldots,B_t\}$ of order n satisfying (0) to (iii) above.*

Following the route in Chapter 3, the following definition is made.

Definition 5.2. An *amicable family of type* $[[u_1,\ldots,u_s];[v_1,\ldots,v_t]]$ in order n is a collection of rational matrices of order $n, \{A_1,\ldots,A_x;B_1,\ldots,B_t\}$ satisfying (i), (ii), (iii) above, where the u_i and v_j are positive rational numbers.

Proposition 5.3. *Let $\{A_1,\ldots,A_s;B_1,\ldots,B_t\}$ be an amicable family of type $[u_1,\ldots,u_s]$; $[v_1,\ldots,v_t]$ in order n, and let P and Q be rational matrices of order n satisfying $PP^\top = aI_n, Q^\top = bI_n$. Then $\{PA_1Q,\ldots,PA_sQ;$ $PB_1Q,\ldots,PB_tQ\}$ is an amicable family of order n and type $[[u_1ab,\ldots,u_sab];$ $[v_1ab,\ldots,v_tab]]$.*

Proof. Direct verification. □

The existence problem for amicable families and amicable OD in some special cases will now be investigated. Observe that if $\{A_1,\ldots,A_s;B_1,\ldots,B_t\}$ is an amicable family in order n, then $\{A_1,\ldots,A_s\}$ and $\{B_1,\ldots,B_t\}$ are each rational families in order n, and so $s,\ t \le \rho(n)$.

5.2.1 n Odd

In this case $\rho(n) = 1$, and so an amicable family of type $[[u];[v]]$ is $\{A;B\}$, A,B rational matrices, where $AA^\top = uI_n, BB^\top = vI_n$ and $AB^\top = BA^\top$. It is known from proposition 2.2 that u and v are each squares in $\mathbb{Q}$. With that observation it can proved, though somewhat disappointing, the following proposition.

Proposition 5.4. *Let n be odd. A necessary and sufficient condition that there be an amicable family of type $[[u];[v]]$ in order n is that there exist rational families of type $[u]$ and $[v]$ in order n.*

Proof. The necessity is obvious since an amicable family is made up of two rational families (plus more). To show the sufficiency, let $u = a^2, v = b^2$, $a,b \in \mathbb{Q}^+$; then $\{aI_n;bI_n\}$ is an amicable family of the desired order and type.

Thus, there are no new algebraic restrictions which prohibit amicable OD from existing in order n, n odd. □

Problem 5.1. Let n be odd, and suppose there is a $W(n,k)$. Is there a symmetric $W(n,k)$?

A small contribution can be made to the question of existence for symmetric $W(n,k)$ by considering the following lemma.

Lemma 5.1. *Let $\{M_1,\ldots,M_s;N_1,\ldots,N_r\}$ be a family of weighing matrices of order n and lengths $(s,\ r)$ which satisfy*

(a) $M_i^\top = -M_i,\ i=1,\ldots,s;\ N_j = N_j^\top,\ j=1,\ldots,r$
(b) $M_iM_i^\top = iI_n,\ N_jN_j^\top = jI_n,\ 1\le i\le s,\ 1\le j\le r$
(c) $M_iN_j^\top = M_jN_i^\top,\ 1\le i\le s, 1\ \le j\le r.$

Then

(i) if there is a family of order n and length $(s,1)$, then there is a family of order $2n$ and length $(2s+1,1)$;
(ii) there is a family of order 2^s and length $(2^s-1,1)$;
(iii) there exist skew-symmetric $W(2^s,i)$ for all $i=0,\ 1,\ldots,2^s-1$ where s is a positive integer;
(iv) if there is a family of order n and length $(s,1)$, there is a family of order $2n$ and length $(0,2s+2)$;
(v) there is a family of order 2^s and length $(0,2^s)$;
(vi) there exist symmetric $W(2^s,i)$ for all $i=0,1,\ldots,2^s$.

Proof. (i) Let $\{M_1,\ldots,M_s;N_1\}$ be the family of length $(s,1)$. Then with

$$A=\begin{bmatrix} 0 & 1\\ -1 & 0\end{bmatrix};\qquad H=\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix};\qquad M=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}. \tag{5.4}$$

$\{I_2\otimes M_1,\ldots,\ I_2\otimes M_s,\ A\otimes N_1,\ A\otimes N_1+I_2\otimes M_1,\ldots,\ A\otimes N_1+I_2\otimes M_s;\ H\otimes M_s\}$ is the family of length $(2n+1,1)$.

(ii) Clearly $\{A;H\}$ is a family in order 2 and with length $(1;1)$, and so by repeated application of (i) gives the result.

(iii) The skew-symmetric matrices of the family of (ii) give the result.

(iv) Consider
$\{A\otimes M_1,\ldots,A\otimes M_s,M\otimes N_1,I\otimes N_1+A\otimes M_1,\ldots,I\otimes N_1+A\otimes M_s,H\otimes N_1\}$.

(v) The symmetric matrices of the family of (iv) give the result. □

The lemma shows that only symmetric weighing matrices are needed of odd order to ensure the existence of symmetric weighing matrices for most large orders and most weights. Clearly, by taking the back circulant matrix one obtains from Theorem 4.6 (see Lemma 4.7 also), we obtain a symmetric $W(q^2+q+1,q^2)$ whenever q is a prime power. Also it was noted that the $W(p+1,p)$ constructed for prime powers p in Lemma 4.12 is symmetric for $p\equiv 1 \pmod 4$. Further observe that using circulant matrices $M,\ N$ of order $2n+1$ with first rows 0_n110_{n-1} and 0_n1-10_{n-1} in

$$\begin{bmatrix} M & N \\ -N^\top & M^\top \end{bmatrix} \tag{5.5}$$

where 0_k is the zero vector of length k, gives a symmetric $W(4n+2,\ 4)$ for every integer $n \leq 1$.

The following is a summary of this.

Proposition 5.5. *(i) There is a symmetric $W(n,\ 4)$ for all $n \geq 10$.*
(ii) There is a symmetric $W(n,\ 9)$ for all $n \geq 68$.
(iii) Let k be a square integer; then there exists an integer $N(k)$ such that here is a symmetric $W(n,\ k)$ for every $n \geq N(k)$.

Since fewer symmetric weighing matrices than weighing matrices are known and since they always give amicable OD, this area merits further study, as does the entire question of amicable OD in odd orders.

5.2.2 $n = 2b$, b Odd

In this case $\rho(n) = 2$, and so the largest possible size for an amicable family is $\{A_1, A_2; B_1, B_2\}$.

Proposition 5.6. *Let $n = 2b$, b odd. A necessary and sufficient condition that here be an amicable family in order n of type $[[u_1, v_1]; [u_2, v_2]]$ is that there be rational families of type $[u_1, v_1]$ and $[u_2, v_2]$ in order n.*

Proof. The necessity is obvious. To prove sufficiency it should be noted that a glance at the proof of Theorem 2.3 should convince the reader that it is enough to consider the case where $u_1 = v_1 = u$ and $u_2 = v_2 = v$, with u and v each a sum of two squares in $\mathbb{Q}$, and $n = 2$. In this case, suppose $u = \alpha^2 + \beta^2,\ v = \gamma^2 + \delta^2$; then

$$A_1 = \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix};\ A_2 = \begin{bmatrix} -\beta & \alpha \\ -\alpha & -\beta \end{bmatrix};\ B_1 = \begin{bmatrix} \gamma & \delta \\ \delta & -\gamma \end{bmatrix};\ B_2 = \begin{bmatrix} \delta & -\gamma \\ -\gamma & -\delta \end{bmatrix}. \tag{5.6}$$

give the required amicable family. □

Thus, the only algebraic restrictions on the existence of amicable families in orders $n = 2b$, b odd, come from the restrictions on rational families that are already known.

That there are new combinatorial restrictions on amicable orthogonal designs in orders $n = 2b$, b odd, is evident from the following example.

Example 5.3. (W. Wolfe) There is no $AOD(6 : (1); (2, 2))$. (Wolfe's result is more general; [247].)

It is known that there are $OD(6; 1)$ and $OD(6; 2, 2)$ (Geramita, Geramita, Wallis: [77]), so this example will show the inadequacy of Proposition 5.6.

There is no loss in assuming the first orthogonal design in the (presumed) pair of type $((1);(2,2))$ is zI_6 and the second is $X = Ax + By$. The A and B are symmetric weighing matrices of weight 2 and order 6.

Lemma 5.2. *If a symmetric $W(n,2)$ exists with zero diagonal, then $n \equiv 0 \pmod 4$.*

Proof. It is easy to check that a symmetric $W(n,2)$ with zero diagonal is (up to simultaneous row and column permutation and simultaneous multiplication of row i and column i by "-1") the direct sum of blocks

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

Now, it is possible to show that there is no symmetric $OD(6;2,2)$.

By the lemma, each variable must appear on the diagonal. Thus, we may assume that X looks like

$$\begin{bmatrix} x & x & y & y & 0 & 0 \\ x & -x & a & b & & \\ y & & & & & \\ y & & & & & \\ 0 & & & & & \\ 0 & & & & & \end{bmatrix}.$$

Case 1. $a \neq 0$ Then it may be assumed $a = y$, $b = -y$, and so

$$X = \begin{bmatrix} x & x & y & y & 0 & 0 \\ x & -x & y & -y & 0 & 0 \\ y & y & u & v & & \\ y & -y & w & s & & \\ 0 & 0 & & & & \\ 0 & 0 & & & & \end{bmatrix}.$$

Checking columns 1 and 3, it is seen that u, w are $\neq 0$, and hence the rest of column 3 consists of zeros, and that gives too many zeros in the last two rows.

Case 2. $a = 0$. Then $b = 0$, also, and therefore

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

Now there must be exactly two y's in the third column, but putting the second y in either the third or fourth rows gives the wrong inner product with columns one and three, while putting the second y in either the fifth or sixth rows gives trouble with the inner product of columns two and three.

Thus, such an X cannot exist. □

Remark 5.1. Wolfe's result is that there is no symmetric $OD(6;2,2)$ in any order $n \equiv 2 \pmod 4$. This example has not been able to be placed in any general framework but is can be seen later that the symmetry conditions come into play in many places.

5.3 More on the Number of Variables in an Amicable Orthogonal Design

Given a positive integer n, it may be asked it may be asked the maximum number of variables that may appear in an amicable $OD(n)$. Clearly, the number of variables in both designs cannot exceed $2\rho(n)$. Indeed, when n is odd or if $n = 2b$, b odd, then the examples of Section 5.2 show that $2\rho(n)$ is possible. A bit of reflection shows that there are two separate questions that can, and should, be considered.

Problem 5.2. Given an orthogonal design X involving s variables, let

$$A(X) = \{\text{orthogonal designs } Y | X \text{ and } Y \text{ are amicable}\}.$$

($A(X) = \emptyset$ is entirely possible!)

$$\text{Define } m(X) = \max_{Y \in A(X)} \{\text{number of variables in } Y\}.$$

What is $m(X)$?

Problem 5.3. Fix an integer $s \leq \rho(n)$, and let

$${}_n0_s = \{\text{orthogonal designs of order } n \text{ involving } s \text{ variables}\}$$

$$\text{Define } m(s) = \max_{X \in {}_n0_s} \{s + m(X)\};$$

then what is $m(s)$?

Problem 5.2 seems extremely difficult, in general. In fact, deciding whether or not $A(X) = \emptyset$ seems, in general, intractable. Directly a little will be said about this problem.

Problem 5.3, on the other hand, can be given a complete solution. The presentation of the solution to this problem follows, for the most part, that of W. Wolfe [247]. A different, and more general, solution is given by D. Shapiro [194].

Imitating some of the notions of Chapter 1, suppose X and Y form an $AOD(n : (u_o, u_1, \ldots, u_s); (v_1, \ldots, v_t))$. [Note the numbering of the variables in the first design.] The coefficient matrices of the two orthogonal designs will be denoted

$$\{A_i,\ 0 \le i \le s;\ B_j,\ 1 \le j \le t\}$$

Now, consider the *real* matrices

$$\alpha_i = \frac{1}{\sqrt{u_0 u_i}} A_i A_0^\top,\ 0 \le i \le s, \qquad \beta_j = \frac{1}{\sqrt{u_0 v_j}} B_j A_0^\top,\ 1 \le j \le t$$

form a collection of real matrices of order n satisfying

(0) $\alpha_i = -\alpha_i^\top,\ 1 \le i \le s; \quad \beta_j = \beta_j^\top,\ 1 \le j \le t;$
(i) $\alpha_i^2 = -I_n,\ 1 \le i \le s; \quad \beta_j^2 = I_n,\ 1 \le j \le t;$
(ii) $\alpha_i\alpha_j + \alpha_j\alpha_i = 0,\ 1 \le i \ne j \le s; \quad \beta_k\beta_\ell + \beta_\ell + \beta_\ell\beta_k = 0,\ 1 \le k \ne \ell \le t;$
(iii) $\alpha_i\beta_j + \beta_j\alpha_i = 0$, for all $1 \le i \le s,\ 1 \le j \le t.$

By analogy with Definition 1.1, the following definition can be made.

Definition 5.3. A family of real matrices $\{\alpha_j,\ 1 \le i \le s;\ \beta_j,\ 1 \le j \le t\}$ of order n satisfying (0), (i), (ii), (iii) above will be called a *Hurwitz-Radon family of type* (s,t) *in order* n (or simply an H-R(s,t) family in order n).

A H-R$(s,0)$ family was discussed in Chapter 1. It can be shown, for a given s and t, that there cannot be an H-R(s,t) family in order n, then there cannot be amicable $OD(n)$ formed by X and Y, where X involves $s+1$ variables and Y involves t variables.

If condition (0) is neglected, it can be seen that (i), (ii), (iii) amount to saying that there is a representation of the Clifford algebra of the real quadratic form $s\langle -1\rangle \perp t\langle 1\rangle$ on the vector space $\mathbb{R}^n$; i.e., $\mathbb{R}^n$ is a module for this Clifford algebra. Now, the irreducible modules for a Clifford algebra always have dimension a power of 2, and if $n = 2^a b$, b odd, the maximum dimension of an irreducible module is $\le 2^a$; i.e., we get a representation of the Clifford algebra of $s\langle -1\rangle \perp t\langle 1\rangle$ on $\mathbb{R}^{2^a}$.

Let $C^{s,t}$ denote the Clifford algebra of $s\langle -1\rangle \perp t\langle 1\rangle$. If $n = 2^a$, can $C^{s,t}$ be non-trivially represented on $\mathbb{R}^{2^a}$. If it cannot, then there is no H-R(s,t) family in any order $2^a b$, b odd. This will, at least, provide upper bounds for Problem 5.3 (and, consequently Problem 5.2). Then the sharpness of these bounds will have to be dealt with.

Fortunately, the representation theory of the algebras $C^{s,t}$ is very well known. The earliest complete discussion to be found is in the 1950 paper of Kawada and Iwahori [119]. A more modern treatment can be found in Lam [142, pp.126–139].

If d is given the degree of an irreducible real matrix representation of $C^{s,t}$ of minimal degree > 1, then the following are restatements of Kawada-Iwahori theorems [119].

Theorem 5.1. *If $s+t=2k$, then $C^{s,t}$ is a central simple $\mathbb{R}$-algebra, and d (as defined above) is given by:*

(a) if $t-k \equiv 0, 1 \pmod 4$, then $d=2^k$;
(b) if $t-k \equiv 2, 3 \pmod 4$, then $d=2^{k+1}$.

Theorem 5.2. *If $s+t=2k+1$, then $C^{s,t}$ is a semi-simple algebra over $\mathbb{R}$, and d is given by:*

(a) if $t-k \equiv 0, 2$ or $3 \pmod 4$, then $d=2^{k+1}$;
(b) if $t-k \equiv 1 \pmod 4$, then $d=2^k$.

Definition 5.4. Let $n=2^a$, t be integers, $t>0$. Define $\rho_t(n) = \max\{s | C^{s-1,t}$ has an irreducible real matrix representation of degree $\leq n\}$.

The relevance of ρ_t to our discussion is obvious, for if $m=2^a b$, b odd, we could never find an amicable orthogonal design formed by X and Y in order m, where X involves s variables and Y involves t variables if $s > \rho_t(2^a)$.

The exact values of $\rho_t(n)$ are given by Kawada and Iwahori [119].

Theorem 5.3. *Let $n=s^{4a+b}$, $0 \leq b \leq 4$. Then $\rho_t(n)-1=8a-t+\delta$, where the values of δ are given in the table below:*

Table 5.1 Values of δ for $\rho_t(n)-1=8a-t+\delta$

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

5.4 The Number of Variables

Some easy (but tedious) consequences of this theorem are:

Corollary 5.3. *(i) $\rho_0(n)=\rho(n)$,*
(ii) $\rho_t(2n)=\rho_{t-1}(n)+1$,
(iii) $\rho_t(n)=\rho_{t+8}(2^4 n)$.

The next example will illustrate how to use these theorems in some low orders.

Example 5.4. Let $n = 4x,\ x$ odd; then $\rho(n) = 4$, and so an orthogonal design in order n cannot involve more than 4 variables. Let X and Y be amicable orthogonal designs in order n, and suppose Y involves t variables ($t \leq 4$). Then, the discussion before Theorem 5.3 assets that X cannot involve more than $\rho_t(4)$ variables.

We enumerate the possibilities in Table 5.2.

Table 5.2 $n = 4x$, x odd

$t =$ number of variables in Y	Number of variables in X is $\leq$
4	$\rho_4(4) = 0$
3	$\rho_3(4) = 3$
2	$\rho_2(4) = 3$
1	$\rho_1(4) = 3$
0	$\rho_0(4) = 4$

It can be seen already that there is a marked change from n odd and $n = 2x,\ x\ odd$, which we investigated in the previous section.. There is **no** orthogonal design which is "amicable" with a 4-variable design in such an order. Furthermore, the maximum total number of variables that may ever be hoped to involve between X and Y is $6 < 2\rho(4) = 8$.

For future reference, there is included a similar table for $n = 8x$ and $n = 16x,\ x$ odd.

Table 5.3 $n = 8x$, x odd

$t =$ number of variables in Y	Number of variables in X is $\leq$
8	$\rho_8(8) = 0$
7	$\rho_7(8) = 0$
6	$\rho_6(8) = 0$
5	$\rho_5(8) = 1$
4	$\rho_4(8) = 4$
3	$\rho_3(8) = 4$
2	$\rho_2(8) = 4$
1	$\rho_1(8) = 5$
0	$\rho_0(8) = 8$

It can be seen, at least for these three special cases, that these bounds are achieved by an H-R(s,t) family (condition 0) is now considered; and

Table 5.4 $n = 16x$, x odd

$t =$ number of variables in Y	Number of variables in X is $\leq$
9	$\rho_9(16) = 1$
8	$\rho_8(16) = 1$
7	$\rho_7(16) = 1$
6	$\rho_6(16) = 2$
5	$\rho_5(16) = 5$
4	$\rho_4(16) = 5$
3	$\rho_3(16) = 5$
2	$\rho_2(16) = 6$
1	$\rho_1(16) = 9$
0	$\rho_0(16) = 9$

moreover, have the α_i (respectively the β_j) be disjoint $(0,1,-1)$ matrices. As in the discussion which preceded Theorem 1.3 of Chapter 1, that will follow immediately if it is known that all matrices have integer entries.

Now, we saw in Proposition 1.2 that there is an H-R(3,0) family of integer matrices in order 4 (and by tensoring with I_x, in order $4x$ for any odd x), and so, in Table 5.2, we have taken care of the possibility that $t = 4 =$ number of variables in Y, $0 =$ number of variables in X. To show that all other possibilities in Table 5.2 are actually achieved, it suffices just to construct an H-R(2,3) integer family in order 4. The rest of the table comes from omitting some members of this family.

$$\text{Let } A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \qquad P = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad \mathbb{Q} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Proposition 5.7 (Wolfe's Slide Lemma). *If* $\{M_i,\ 1 \leq i \leq s;\ N_j,\ 1 \leq j \leq t\}$ *is an H-R*(s,t) *family in order* n *(of integer matrices), then*

$$\{P \otimes M_i,\ 1 \leq i \leq s, \quad A \otimes I_n; \quad P \otimes N_j,\ 1 \leq j \leq t, \quad Q \otimes I_n\}$$

is an H-R$(s+1, t+1)$ *family in order* n *(of integer matrices).*

Proof. The verifications are routine.

It is an easy matter to check that $\{A; Q, P\}$ is an integer H-R(1,2) family in order 2, and so, by the Slide Lemma, an H-R(2,3) family of integer matrices in order 4 can be obtained.

In considering orders $8x$, x odd, first note that Table 5.5 gives an H-R(7,0) family of integer matrices in order 8 (and hence in order $8x$, x odd). Now there is a symmetric $(1,1,1,1,1)$ design in order 8 (proof of Theorem 4.2) and hence an H-R(0,5) family of integer matrices in order 8. Finally to obtain an

Table 5.5 H-R(7,0), order $8x$, x odd

0	a	b	c	d	e	f	g
$-a$	0	c	$-b$	e	$-d$	$-g$	f
$-b$	$-c$	0	a	f	g	$-d$	$-e$
$-c$	b	$-a$	0	g	$-f$	e	$-d$
$-d$	$-e$	$-f$	$-g$	0	a	b	c
$-e$	d	$-g$	f	$-a$	0	$-c$	b
$-f$	g	d	$-e$	$-b$	c	0	$-a$
$-g$	$-f$	e	d	$-c$	$-b$	a	0

H-R(3,4) integer family in order 8, use the Slide Lemma with the H-R(2,3) and H-R(3,0) families in order 4. These give all possibilities in Table 5.2.

To complete the special cases observe that there is an H-R(0,9) integer family in order 16 (given by the symmetric $(1,1,1,1,1,1,1,1,1)$ design in order 16 which appears in the proof of Theorem 4.2). Use the Slide Lemma with the integer matrices of the H-R(0,5), H-R(3,4), H-R(4,1) and H-R(7,0) families in order 8 to obtain the integer H-R(1,6), H-R(4,5), H-R(5,2) and H-R(8,1) families in order 16. These give all the possibilities for Table 5.3.

Wolfe has given the general result in [247], and so the proofs shall not be pursued here. We are content to just state Wolfe's theorem and the three lemmata that were used to obtain it (in addition to the Slide Lemma and the explicit computations in orders 4, 8 and 16). The lemmata are of independent interest and provide some construction methods. They shall be generalised later. □

Theorem 5.4. *For any integer n and any $t \leq \rho(n)$, there is an H-R$(\rho_t(n)-1,t)$ family of integer matrices of order n.*

Corollary 5.4. *For any integer n there are amicable orthogonal designs X and Y involving s and t variables, respectively, X of type $\underbrace{(1,\ldots,1)}_{s-tuple}$, Y of type $\underbrace{(1,\ldots,1)}_{t-tuple}$ for any $s \leq \rho_t(n)$.*

Lemma 5.3. *Conversely it can be noted that the existence of AOD$(n:(u_0,u_1,\ldots,u_s);(v_1,v_2,\ldots,v_t))$, X,Y on variables x_i and y_j, respectively, implies the existence of an H-R(s,t) family.*

A summary of all the relevant facts can be seen in the proof of theorem 5.4.

Proposition 5.8 (Wolfe). *Let A, P, Q be as above.*

(1) If $\{M_i,\ 1 \leq i \leq s\}$ is an H-R$(s,0)$ (integer) family in order n, then $\{A \otimes M_i,\ 1 \leq i \leq s,\ P \otimes I_n,\ Q \otimes I_n\}$ is an H-R$(0,s+2)$ (integer) family in order $2n$.

(2) If $\{N_j,\ 1 \le j \le t\}$ *is an H-R*$(0,t)$ *(integer) family in order* n*, then*

$$\{A\otimes Q\otimes I_2\otimes N_j,\ 1\le j\le t,\ I_2\otimes A\otimes I_{2n},\ A\otimes P\otimes Q\otimes I_n,\ Q\otimes Q\otimes A\otimes I_n,$$
$$P\otimes Q\otimes A\otimes I_n,\ \ I_2\otimes P\otimes A\otimes I_n,\ \ A\otimes P\otimes P\otimes I_n\}$$

is an H-R$(t+6,0)$ *(integer) family in order* $8n$*.*

(3) (Jump) If $\{M_i,\ 1\le i\le s;\ \ N_j,\ 1\le j\le t\}$ *is an H-R*(s,t) *(integer) family in order* n*, then*

$$\{A\otimes P\otimes A\otimes Q\otimes M_i,\ 1\le i\le s;\ \ A\otimes P\otimes A\otimes Q\otimes N_j,\ 1\le j\le t,$$
$$Q\otimes Q\otimes Q\otimes Q\otimes I_n,\ \ P\otimes I_4\otimes Q\otimes I_n,\ \ Q\otimes P\otimes I_2\otimes Q\otimes I_n,$$
$$Q\otimes Q\otimes P\otimes Q\otimes I_n,\ \ I_8\otimes P\otimes I_n,\ \ P\otimes Q\otimes A\otimes A\otimes I_n,$$
$$I_2\otimes P\otimes A\otimes A\otimes I_n\}$$

is an H-R$(s,\ t+8)$ *(integer) family in order* $2^4\cdot n$*.*

Wolfe proves one more fact which will be of interest.

Theorem 5.5. *If* $n = 2^a n_0,\ \ n_0$ *odd. If* $t \le \rho(n)$*, then* $t+\rho_t(n) \le 2a+2$*. Furthermore, there is a* $t_0 \le \rho(n)$ *with* $t_0+\rho_{t_0}(n) = 2a+2$*.*

Corollary 5.5. *If* X *and* Y *are amicable orthogonal designs in order* $n = 2^a n_0$*,* n_0 *odd, then the total number of variables in* X *and* Y *is* $\le 2a+2$*, and that bound is achieved.*

5.5 The Algebraic Theory of Amicable Orthogonal Designs

The pursuit of the analogy already seen between the study of orthogonal designs and the study of amicable orthogonal designs is continuing. The algebraic theory, naturally, well rest on the study of amicable families.

Proposition 5.9 (Wolfe). *Let* $\{A_1,\dots,A_s;\ B_1,\dots,B_t\}$ *be an amicable family of type* $\big[[u_1,\dots,u_s];\ [v_1,\dots,v_t]\big]$ *in order* n*.*

Then $\{A_1A_2^{\top}B_i,\ 1\le i\le t,\ A_3,\dots,A_s\}$ *is a rational family of type* $[u_1u_2v_1,\ u_1u_2v_2,\dots,u_1u_2v_5,u_3,\dots,u_s]$ *in order* n*.*

Proof. A routine check. □

Corollary 5.6. *Let* $n \equiv 4 \pmod 8$*. In order that there be amicable families of type* $\big[[a_1,a_2,a_3];[b_1,b_2,b_3]\big]$ *in order* n*, one must have*

(i) rational families of type $[a_1,a_2,a_3]$ *and* $[b_1,b_2,b_3]$ *in order* n*, and*
(ii) $a_1a_2a_3b_1b_2b_3$ *a square in* $\mathbb{Z}$*.*

Proof. Use proposition 5.9 and the results of Chapter 3. □

In the same vein:

Corollary 5.7. *Let $n \equiv 4 \pmod 8$. Necessary conditions that there be amicable families in order n of type*

(1) $\left[[a_1,a_2,a_3];[b_1,b_2]\right]$ *are that*

(i) there be rational families of type $[a_1,a_2,a_3]$ and $[b_1,b_2]$ in order n, and
(ii) at every prime $p, (-1,a_1,a_2,a_3b_1b_2)_p = (b_1,b_2)_p(a_1a_2a_3,b_1b_2)_p$;

(2) $\left[[a_1,a_2,a_3];[b_1]\right]$ *are that*

(i) there be rational families of type $[a_1,a_2,a_3]$ and $[b_1]$ in order n, and
(ii) $a_1a_2a_3b_1$ be a sum of fewer than four squares in $\mathbb{Z}$.

Shapiro has given a different formulation of these two corollaries and generalised this to other n. His results shall be given later in this section.

Example 5.5. (i) There are no amicable orthogonal designs $AOD(4n_0 : (1,1,1);(1,1,2))$ in any order $4n_0, n_0$ odd, although designs of both types exist in every order $4n$.
(ii) There are no amicable orthogonal designs $AOD(4n_0 : (1,1,1);(1,3))$ in any order $4n_0$ by 5.7. This also eliminates amicable orthogonal designs $AOD(12 : (1,11);(4,4,4))$ and, in fact, in any order $4n_0$, n_0 odd, $n_0 \geq 3$.
(iii) There is no amicable family of type $[[1,1,1];[7]]$ in any order $4n_0$, n_0 odd, $n_0 > 1$. So, in particular, there are no amicable orthogonal designs $AOD(12 : (4,4,4);(7))$ in order 12.

Daniel Shapiro has solved the entire algebraic problem of amicable orthogonal designs. This is in [194]. He has continued his study of the space of similarities and extended his earlier work to handle amicable families. These techniques are too complicated to attempt to analyze here. Suffice it to say that his work requires a deep understanding of the modern theory of quadratic forms and applies to a much more general setting than has been considered here. A source of great pleasure has been the realisation that the combinatorial problem that was considered inspired, an interesting new investigation in quadratic forms. Not only has this problem borrowed heavily from the theory of quadratic forms for answers, but it has suggested new problems in that theory.

Quoted here are a few of Shapiro's theorems (in a form suitable to this discussion).

The first theorem, though not surprising, is surprisingly complicated to prove and is the analogue of Theorem 3.11.

Theorem 5.6. *Let $n = 2^m n_0$, n_0 odd. There is an amicable family of type $\big[[a_1,\ldots,a_s];[b_1,\ldots,b_t]\big]$ in order $n \Leftrightarrow$ there is an amicable family of the same type in order 2^m.*

The next theorem also has its counterpart in 3.17, part A.

Theorem 5.7. *Let $n = 2^m$ $(m \geq 3)$, and choose $t \leq \rho(n)$ and $s \leq \rho_t(n)$. If $s+t \leq 2m-1$, then for any positive rationals $a_1,\ldots,a_s, b_1,\ldots,b_t$ there is an amicable family of type $\big[[a_1,\ldots,a_s];[b_1,\ldots,b_t]\big]$.*

Thus, for s,t as above $(m \geq 3)$, the only time there are algebraic restrictions are when $2m \leq s+t \leq 2m+2$. In the next proposition a portion of Shapiro's theorem dealing with the interval $[2m, 2m+2]$ for the special cases of $n = 2^2$ and $n = 2^3$ is abstracted.

Theorem 5.8. *Let $n \equiv 4 \pmod 8$. Necessary and sufficient conditions that there be an amicable family in order n of type*

(1) $\big[[a_1,a_2,a_3];[b_1,b_2,b_3]\big]$ *are that*

(i) $\langle a_1,a_2,a_3\rangle$ *and* $\langle b_1,b_2,b_3\rangle$ *be isometric to subforms of* $4\langle 1\rangle$, *and*
(ii) $\langle a_1,a_2,a_3\rangle \simeq \langle b_1,b_2,b_3\rangle$;

(2) $\big[[a_1,a_2,a_3];[b_1,b_2]\big]$ *is that* $\langle b_1,b_2\rangle < \langle a_1,a_2,a_3\rangle < 4\langle 1\rangle$;
(3) $\big[[a_1,a_2,a_3];[b_1]\big]$ *is that* $\langle b_1\rangle < \langle a_1,a_2,a_3\rangle < 4\langle 1\rangle$.

If $n \equiv 8 \pmod{16}$, necessary and sufficient conditions that there be an amicable family in order n of type

(4) $\big[[a_1,a_2,a_3,a_4];[b_1,b_2,b_3,b_4]\big]$ *is that* $\langle a_1,a_2,a_3,a_4\rangle \simeq \langle b_1,b_2,b_3,b_4\rangle$;
(5) $\big[[a_1,a_2,a_3,a_4];[b_1,b_2,b_3]\big]$ *is that* $\langle b_1,b_2,b_3\rangle < \langle a_1,a_2,a_3,a_4\rangle$;
(6) $\big[[a_1,a_2,a_3,a_4,a_5];[b_1]\big]$ *is that* $b_1\prod_{i=1}^5 a_i$ *is a square in* $\mathbb{Q}$;
(7) $\big[[a_1,a_2,a_3,a_4];[b_1,b_2]\big]$ *is that* $\langle b_1,b_2\rangle < \langle a_1,a_2,a_3,a_4\rangle$.

Example 5.6. We have already been seen that are eliminated by this theorem in orders $\equiv 4 \pmod 8$. To see some possibilities eliminated in orders $n \equiv 8 \pmod{16}$, observe:

(1) There is no amicable family of $\big[[1,1,1,2];[1,1,1,1]\big]$ in order $8n_0$, n_0 odd. Thus, since $\langle 1,1\rangle \simeq \langle 2,2\rangle$, we have no $AOD(8:(2,2,2,2);(1,2,2,2))$.
(2) There is no amicable family of $\big[[1,1,3];[1,1,1,1]\big]$ in any order $n \equiv 8 \pmod{16}$ since $\langle 1,1,3\rangle \not< \langle 1,1,1,1\rangle$. This is clear, for if $\langle 1,1,3\rangle < \langle 1,1,1,1\rangle$, we would have, by Witt Cancellation, that $\langle 3\rangle < \langle 1,1\rangle$, but 3 is not the sum of two squares in $\mathbb{Q}$.
In particular, there are no $AOD(8:(2,2,2,2);(2,2,3))$.
(3) There is no amicable family of type $\big[[1,1,1,1,2];[1]\big]$ in any order $n \equiv 8 \pmod{16}$, so, in particular, there are no $AOD(8:(1,1,2,2,2);(1))$.
(4) There is no amicable family of type $\big[[1,1,1,1];[1,k]\big]$ when k is not the sum of three squares in $\mathbb{Q}$ for any order $n \equiv 8 \pmod{16}$. So, in particular, there are no $AOD(8:(2,2,2,2);(1,7))$.

5.6 The Combinatorial Theory of Amicable Orthogonal Designs

It has already be seen that there is more at stake in deciding if there are amicable orthogonal designs of a certain order and type than just the existence of amicable families of the same order and type: first, because there may not be orthogonal designs of a certain type, much less amicable ones, and second, because even when orthogonal designs of the appropriate types exist, none may be amicable.

Unfortunately, in this area there are only a few theorems and a few examples. There has not yet been discovered anything analogous to Corollary 2.3 for amicable orthogonal designs.

Warren Wolfe has given two useful combinatorial theorems which exclude possibilities not eliminated by the algebraic theory. The second of these has been extended by Peter J Robinson [166].

Theorem 5.9 (Wolfe). *Suppose X and Y are amicable orthogonal designs in order $n \equiv 0 \pmod 4$, where X is of type $(1,1,1,a_1,\ldots,a_s)$ and Y is of type $(b_1,\ldots,b_t)$. Then, there exists an orthogonal design in order n of type $(1,b_1,\ldots,b_t)$.*

Proof. Let $X = A_1x_1 + A_2x_2 + A_3x_3 + \sum_{j=1}^{s} B_j x_{j+3}$. By applying row and column operations to X and Y simultaneously, it can be assumed

$$A_1 = \otimes_{\frac{n}{4}} \begin{bmatrix} 0 & 1 & & \\ -1 & 0 & & \\ & & 0 & 1 \\ & & -1 & 0 \end{bmatrix}, A_2 = \otimes_{\frac{n}{4}} \begin{bmatrix} & & 1 & 0 \\ & & 0 & -1 \\ -1 & 0 & & \\ 0 & 1 & & \end{bmatrix}, A_3 = \otimes_{\frac{n}{4}} \begin{bmatrix} & & 0 & 1 \\ & & 1 & 0 \\ 0 & -1 & & \\ -1 & 0 & & \end{bmatrix}.$$

The patient reader will then discover that the relations $A_iYA_i^\top$, $i = 1,2,3$, force Y to be skew-symmetric. Then $zI_n + Y$ is the required orthogonal design. □

Remark 5.2. This theorem is, in some sense, only "$\frac{1}{2}$" combinatorial. An examination of the proof shows that all we really need to get Y skew-symmetric is that A_1, A_2, A_3 have integer entries (and hence $\{0,1,-1\}$ entries). This indicates that there may be some merit in defining and studying integer families and integer amicable families (by analogy with rational families and amicable families).

Example 5.7. We may use Theorem 5.9 to observe that there are no $AOD(20:(1,1,1);(1,1,16))$ since there is no $OD(20;1,1,1,16)$. This type is not eliminated by any other theorems. This also eliminates anything of type $AOD(n:(1,1,1,\ldots);(b_1,\ldots,b_t))$ where $\sum_{i=1}^{t} b_i = n$, e.g., $AOD(8:(1,1,1,5);(8))$.

Before proceeding onto the next theorem, a lemma is given:

Lemma 5.4. *Suppose X and Y are amicable orthogonal designs of order n where X is of type $(1,u_1,\ldots,u_s)$ on the variables $x_0,\ldots,x_s$ and Y is of order n and type $(v_1,\ldots,v_t)$ on the variables $y_1,\ldots,y_t$; then there exist monomial matrices P and Q (ie, with elements $0,\pm1$ and only one non-zero element per row and column) so that*

$$PXQ = x_0 I + \sum x_i M_i, \quad PYQ = \sum y_i N_i\,,$$

where

(0) $M_i * M_j = 0$ *for* $i \neq j$; $N_\ell * N_k = 0$ *for* $\ell \neq k$;
(i) $M_i^\top = -M_i$, $\forall i$; $N_j^\top = N_j$, $\forall j$;
(ii) $M_i M_i^\top = u_i I_n$, $\forall i$; $N_j N_j^\top = v_j I_n$, $\forall j$;
(iii) $M_i N_j^\top = N_j M_i^\top$;
(iv) $M_i M_j^\top + M_j M_i^\top = 0$, $i \neq j$; $N_\ell N_k^\top + N_k N_\ell^\top = 0$, $k \neq \ell$.

Proof. Choose P and Q so that the variable x_0 occurs on the diagonal of PXQ, and the rest follows immediately. □

Lemma 5.5 (Robinson). *If A and $C = xB + yD$ are amicable orthogonal designs of order $n \equiv 0 \pmod 4$ and types $AOD(n:(1,n-1);(1,m))$, $m \in \{0,1,\ldots,n-1\}$, then it may be assumed*

$$B = \oplus_{\frac{n}{2}-1} Y \oplus X,$$

where

$$X = \begin{bmatrix} - & 0 \\ 0 & 1 \end{bmatrix} \qquad \text{and} \qquad Y = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Proof. From Lemma 5.4 it may be assumed B is symmetric and $A = I x_1 + W x_2$, where W is a skew weighing matrix of weight $n-1$. It is obvious that there can be found a monomial matrix P such that

$$PBP^\top = \oplus_{1 \leq i \leq \frac{n}{2}} X_i,$$

where $X_i = X$ or Y or $\pm I_2$.

If, however, $X_i = \pm I_2$, for any i, then positions $(2i, 2i-1)$ and $(2i-1, 2i)$ of AB cannot be equal. Therefore, none of the X_i's are $\pm I_2$. This also means that, at most, one of the X_i's is $\pm X$, for if two X_i's are $\pm X$, there can be found another monomial matrix which produces $\pm I_2$ somewhere on the diagonal of B.

We now assume $X_i = Y$, $1 \leq i \leq \frac{n}{2}$, and

$$A = \begin{bmatrix} \begin{smallmatrix} 01 \\ -0 \end{smallmatrix} & A_1 & A_2 & \dots \\ \overline{A}_1^\top & & & \\ \overline{A}_2^\top & & Z & \\ \vdots & & & \end{bmatrix};$$

where A_i are (2×2) matrices with entries ± 1.

Since A and B are amicable, and that W and B are amicable, and therefore WB is symmetric. Let

$$A_1 = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \; x_i = \pm 1, \quad A_1 Y = \begin{bmatrix} x_2 & x_1 \\ x_4 & x_3 \end{bmatrix} \quad \text{and} \quad \overline{A}_1^\top Y = \begin{bmatrix} \overline{x}_3 & \overline{x}_1 \\ \overline{x}_4 & \overline{x}_2 \end{bmatrix}.$$

Because AB is symmetric, it must have $x_2 = -x_3$ and $x_1 = -x_4$;ie,

$$A_1 = \pm \begin{bmatrix} 1 & 1 \\ - & - \end{bmatrix} \quad \text{or} \quad \pm = \begin{bmatrix} 1 & - \\ 1 & - \end{bmatrix}.$$

This reasoning is also true for the other A_i's.

Now $\sum_{i=1}^{\frac{n}{2}-1} A_i A_i^\top = (n-2) I_2$, by the orthogonality of A, and

$$A_i A_i^\top = \begin{bmatrix} 2 & -2 \\ -2 & 2 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix}.$$

But since there is an odd number of A_i's,

$$\sum A_i A_i^\top \neq (n-2) I_2.$$

Therefore, at least one of the X_i's is X.

It can now be assumed $X_1 = \pm X_2 = X$. Then it can be seen that the product AB is not symmetric. Therefore,

$$X_1 = X \text{ and } X_i = Y, \; 2 \leq i \leq \frac{n}{2}. \qquad \square$$

Theorem 5.10 (Wolfe-Robinson). *Let X and Y be $AOD(n : (1, a, n-a-1); (u_1, \dots, u_s))$; let $n \equiv 0 \pmod 4$, $n \neq 4$, $a = 1$ or $n \equiv 0 \pmod 8$, $a = 2, 3, 4, 5$. Then $u_i \neq 1$ for any $1 \leq i \leq s$.*

Proof. The case for $a = 1$. Write $X = A_1 x_1 + A_2 x_2 + A_3 x_3$, $Y = \sum_{j=1}^{s} B_j y_j$. With no loss of generality it may be assumed

$$A_1 = \oplus_{\frac{n}{2}} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad A_2 = \oplus_{\frac{n}{2}} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

The conditions $A_1 A_3^\top + A_3 A_1^\top = 0$ and $A_i B_j^\top = B_j A_i^\top$, $i = 1, 2$, $1 \leq j \leq s$, will show that A_3 and the B_j are all block matrices with every 2×2 block

of the form $\left[\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right]$. Such a block may be thought as the complex number $a+bi$, where $a,b \in \{0,1,-1\}$. Let $\overline{A}_3$, $\overline{B}_j$ be the $\frac{n}{2} \times \frac{n}{2}$ complex matrices so obtained.

If "$*$" denotes conjugate transpose, then

(i) $\overline{A}_3 = \overline{A}_3^{\top}$, $\overline{B}_j = \overline{B}_j^{\top}$, $1 \le j \le s$;
(ii) $\overline{A}_3\overline{A}_3^* = (n-2)I_{\frac{n}{2}}$, $\overline{B}_j\overline{B}_j^* = u_j I_{\frac{n}{2}}$, $1 \le j \le s$;
(iii) $\overline{A}_3\overline{B}_j^* = \overline{B}_j\overline{A}_3^*$, $1 \le j \le s$.

The fact that A_3 had weight $n-2$ implies that the off-diagonal elements of $\overline{A}_3$ are neither pure real nor pure imaginary.

Now, let it be assumed that one of the u's $= 1$; with no loss it can assume $u_1 = 1$. Then, the entries in $\bar{B}_1$ are from $\{0, \pm 1, \pm i\}$. It can be claimed that $\bar{B}_1$ is a diagonal matrix, for suppose there is a non-zero entry in the (i,j)-position of $\bar{B}_1$ for $i \ne j$ (there is no loss in assuming it's in the $(1,2)$ position); then let z be the $(1,2)$ entry in $\overline{A}_3$, it can be obtained from (i) and (iii)

$$\begin{bmatrix} 0 & z \\ -z & 0 \end{bmatrix} \begin{bmatrix} 0 & \overline{x} \\ \overline{x} & 0 \end{bmatrix} = \begin{bmatrix} 0 & x \\ x & 0 \end{bmatrix} \begin{bmatrix} 0 & -z \\ \overline{z} & 0 \end{bmatrix}$$

("-" denotes complex conjugation); ie, $z\overline{x} = x\overline{z}$.

Since x is pure real or pure imaginary, this gives that z is pure real or pure imaginary. This, however, contradicts the fact that all non-diagonal entries in $\overline{A}_3$ were *not* pure real or pure imaginary.

Thus, the assumption is that $\overline{B}_1$ is a diagonal matrix. It may be as well assumed the first diagonal entry in $\overline{B}_1$ is $+1$ (if not, multiply $\overline{A}_3$ and $\overline{B}_1$ by one of $\pm iI_{\frac{n}{2}}$ or $-I_{\frac{n}{2}}$; the resulting matrices still satisfy (i), (ii), (iii). The next diagonal entry is ± 1 or $\pm i$. Considering just the top 2×2 block of $\overline{A}_3$ and $\overline{B}_1$, we have (by (iii))

$$\begin{bmatrix} 0 & z \\ -z & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \overline{x} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & x \end{bmatrix} \begin{bmatrix} 0 & -\overline{z} \\ \overline{z} & 0 \end{bmatrix},$$

and so $\overline{z} = \overline{x}z$. If x were real, it would have $\overline{z} = \pm z$, which implies z is pure real or pure imaginary (a contradiction). Thus $x = \pm i$, and so the $(1,2)$ entry of $\overline{A}_3$ is $\overline{z}$, where $\overline{z} = \pm iz$. Now by assumption $n \ne 4$, so there is a third diagonal entry in $\overline{B}_1$. Call it y. If z_{ij} is allowed to denote the (i,j)-th entry of $\overline{A}_3$, we find (by (iii)) that

(a) $z_{13}\overline{y} = -\overline{z}_{13}$ and
(b) $z_{23}\overline{y} = \pm iz_{23}$.

Hence, if y is real, (a) implies that z_{13} is pure real or pure imaginary, while if y is pure imaginary, then (b) implies that z_{23} is pure real or pure imaginary; in either case, a contradiction. This completes the proof for $a = 1$. □

5.6.1 Cases $a = 2, 3$ or 4

Assume that A and B are $AOD(n : (1, a, n-a-1); (1))$, respectively.

It may be assumed B is of the form given in Lemma 5.4, and this implies that the first two rows of A have the following form:

$$x_1 a_2 a_3 a_4 a_5 a_6 \dots a_{\frac{n}{2}-3} a_{\frac{n}{2}-2} a_{\frac{n}{2}-1} a_{\frac{n}{2}},$$

$$\overline{a}_2 x_1 \overline{a}_4 \overline{a}_3 \overline{a}_6 \overline{a}_5 \dots \overline{a}_{\frac{n}{2}-2} \overline{a}_{\frac{n}{2}-3} \overline{a}_{\frac{n}{2}-1} \overline{a}_{\frac{n}{2}}$$

for some a_i's. The inner product of these two rows gives

$$-2\left(a_3 a_4 + \dots + a_{\frac{n}{2}-3} a_{\frac{n}{2}-2}\right) - a_{\frac{n}{2}-1}^2 + a_{\frac{n}{2}}^2 = 0. \tag{5.7}$$

Let x_2 be the variable which appears a times per row and column, and x_3 the remaining variable.

From equation (5.7) it is found

(i) $a_{\frac{n}{2}-1} = \pm a_{\frac{n}{2}}$,
(ii) $a_i = \pm x_2$ for an even number of i's, $z \le i \le \frac{n}{2} - 1$,
(iii) $a_{2i-1} = a_{2i} = \pm x_2$ for an even number of i's, $2 \le i \le \frac{n}{4} - 1$.

It is noted that similar properties exist for the other rows of A, except the last two.

Now consider the matrix A_1 obtained from A by putting $x_1 = x_3 = 0$ and $x_2 = 1$ and show that no such matrix can exist if $a = 2$, 3 or 4.

5.6.1.1 Case 1: $a = 2$ or 3

A monomial P can be found such that $PBP^\top = B$, and if $n \ge 16$, $PA_1P^\top$ is given in Table 5.6.

By deleting rows and columns 3, 4, 5, 6, $n-2$, $n-3$, $n-4$ and $n-5$, a matrix similar in structure to A_1 but in order $n-8$ is obtained. Hence the existence of A_1 in order n implies the existence of a similar matrix in order 8. It is easy to see, however, that no such design exists in order 8.

Therefore, there is no A_1 in order n. Thus there are no $AOD(n : (1), (1, a, n-a-1))$, $a = 2$ or 3, in order $n \equiv 0 \pmod 8$.

5.6.1.2 Case 2: $a = 4$

A monomial Q such that $QBQ^\top = B$ and, if $n \ge 24$ can be found,

Table 5.6 $a_i = \pm 1$ if $a = 3$, or 0 if $a = 2$

$$\left[\begin{array}{cc|cccc|c|cccc|cc}
0 & a_1 & 0 & & & & 0 & 0 & & & & 1 & 1 \\
\overline{a}_1 & 0 & & & & & & & & & & - & 1 \\
\hline
 & 0 & a_2 & & & & & 1 & 0 & 1 & 0 & & \\
0 & & \overline{a}_2 & 0 & & & 0 & 0 & - & 0 & - & 0 & \\
 & & & & 0 & a_2 & & 1 & 0 & - & 0 & & \\
 & & & & \overline{a}_2 & 0 & & 0 & - & 0 & 1 & & \\
\hline
0 & & 0 & & & & A_2 & 0 & & & & 0 & \\
\hline
 & & - & 0 & - & 0 & & 0 & a_2 & & & & \\
0 & & 0 & 1 & 0 & 1 & 0 & \overline{a}_2 & 0 & & & 0 & \\
 & & - & 0 & 1 & 0 & & & & 0 & a_2 & & \\
 & & 0 & 1 & 0 & - & & & & \overline{a}_2 & 0 & & \\
\hline
- & + & & & & & & & & & & 0 & a_1 \\
- & - & 0 & & & & 0 & 0 & & & & \overline{a}_1 & 0
\end{array}\right]$$

$$QA_1Q^\top = \left[\begin{array}{ccc}
 & 0 & 0 \quad Z_1 \; L \\
 & & Z_1 \; Z_2 \\
\hline
 & 0 & A_2 \quad 0 \\
\hline
 & \overline{Z}_1^\top & \\
\overline{Z}_1^\top & \overline{Z}_2^\top & 0 \quad 0 \\
\overline{L}^\top & &
\end{array}\right].$$

where

$$L = \begin{bmatrix} 1 & 1 \\ - & 1 \\ 1 & 1 \\ - & 1 \end{bmatrix}, \qquad Z_1 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & - & 0 & - \\ - & 0 & - & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \qquad Z_2 = \begin{bmatrix} 1 & 0 & - & 0 \\ 0 & - & 0 & 1 \\ 1 & 0 & - & 0 \\ 0 & - & 0 & 1 \end{bmatrix}.$$

By deleting rows and columns 1, 2, 3, 4, n, $n-1$, $n-2$ and $n-3$ of $QA_1Q^\top$ and replacing the first two columns (rows) of the $Z_2(\overline{Z}_2^\top)$ in the corners by $L(\overline{L}^\top)$, a matrix is obtained with similar structure to A_1 but in order $n-8$. Hence, the existence of A_1 in order n implies the existence of a similar matrix in order 16. It is easy to see that no such designs can exist in order 8 or 16, and so there can be no amicable designs $AOD(n:(1);(1,4,n-5))$ in order $n \equiv 0 \pmod 8$.

5.6.1.3 Case 3 $a = 5$.

Proceeding in a similar fashion to that of 5.6.1.2-Case 2 but with diagonal 2×2 blocks of the form $\begin{bmatrix} 0 & a_1 \\ \overline{a}_1 & 0 \end{bmatrix}$ inserted. Note that this makes no difference to the proof.

Corollary 5.8. *There are no amicable orthogonal designs* $AOD(n : (1); (1, a, b, c))$ *of order* $n \equiv 0 \pmod 4$ *for* $a+b+c = n-1$, $a, b, c \neq 0$, *and* abc *odd.*

Proof. By considering Equation (5.7) in the proof of Lemma 5.4 it can be seen that each variable appears an even number of times off the diagonal 2×2 block, and therefore only one of a, b and c is odd. □

Remark 5.3. This theorem uses, at every stage, the full force of the fact that the matrices that are being considered have $\{0, 1, -1\}$ entries and very strongly the fact that X had no zeros. Wolfe was led to prove the case $a = 1$ of this theorem after a frustrating attempt to construct pairs of amicable orthogonal designs in orders $n = 2^a$ of type $((1, 1, 2, \ldots, 2^{a-1}); (1, 1, 2, \ldots, 2^{a-1}))$. If they had existed, they would have involved the greatest number of variables $(2a+2)$ and would have no zeros. In orders $n = 2$ and $n = 4$ they exist, but those are the only times.

This theorem eliminates many types not previously eliminated; eg, there are no $AOD(8 : (1, 1, 6); (1, 7))$.

The only other general combinatorial theorems known which shed some light on the existence problem for amicable orthogonal designs come out of work of Robinson [165] which now will be discussed briefly.

Theorem 5.11 (Robinson [165]). *There are no amicable orthogonal designs* $AOD(n : (1, 1, k); (n))$ *of order* $n \equiv 0 \pmod 4$, $n \geq 8$, *for* k *odd.*

Proof. Assume that such an amicable pair, A and B, exists.

By multiplying by suitable monomial matrices if necessary, it may be assumed

$$A = x_1 I + x_2 X + x_3 Y,$$

with

$$X = \oplus_{\frac{n}{2}} \begin{bmatrix} 0 & 1 \\ - & 0 \end{bmatrix}.$$

By considering $XY^\top = -YX^\top$, $Y^\top = -Y$, $XB^\top = BX^\top$, and $B^\top = B$, it can be seen that Y and B are made up of 2×2 blocks of the form

$$\begin{bmatrix} a & b \\ b & \overline{a} \end{bmatrix}; \quad a, b \in 0, 1, -1.$$

Now $(AB)^\top = B^\top A^\top = BA^\top = AB^\top = AB$, and therefore A and B are amicable only if AB is symmetric and hence only if the top left hand 2×2 block of AB, and therefore YB, is symmetric.

The top left hand 2×2 block of YB, however, is made up of the sum of 2×2 blocks of the form

$$\begin{bmatrix} x & y \\ y & \overline{x} \end{bmatrix} \begin{bmatrix} a & b \\ b & \overline{a} \end{bmatrix} \quad = \quad \begin{bmatrix} xa+yb & xb-ya \\ -xb+ya & xa+yb \end{bmatrix},$$

with $a,b=\pm 1$ and $x,y\oplus 0,1,-1$.

This sum cannot produce a symmetric block unless the sum of the $(ya-xb)$'s is zero, which is clearly impossible with an odd number of non-zero x and y's.

Therefore, there can be no designs A and B of the required types.

An indication of the gap between the algebraic theory of amicable families and the actual existence of amicable orthogonal designs has been highlighted by work of P. J. Robinson and of Robinson in collaboration with Seberry Wallis.

Robinson [165] has shown that the following are *not* the types of amicable orthogonal designs in order 8, although these types are not eliminated by the theorems of Wolfe and Robinson or by the algebraic theory:

$$AOD(8:(1),(2,2,2,2)),\ AOD(8:(1,2,2,3),(4,4)),\ AOD(8:(1,7),(5)).$$

Robinson and Seberry [170] have also shown that there is no $AOD(16:(1,15);(1))$. This is a most surprising result, since the number of variables is so much less than the number allowed by Theorem 5.4. □

5.7 Construction of Amicable Orthogonal Designs

In the first section of this chapter two examples were given of amicable orthogonal designs and gave a small indication in Proposition 5.1 of the strength of this notion. This section will turn away from the limitations on existence to the actual construction of amicable orthogonal designs. As will soon be apparent, the construction problem is an exceedingly difficult one and, as with so many aspects of this area, deserves further study.

Particular attention will be paid to amicable orthogonal designs which are full (ie, neither matrix has any zeros) because of their special relevance to the Hadamard Matrix Problem.

One class of important full amicable orthogonal designs is the amicable Hadamard matrices (Example 5.2). There is a substantial literature on these objects, and in view of their importance to the Hadamard Matrix Problem, their construction shall be dealt with in the next section.

Lemma 5.6 (Wolfe). *Suppose there are amicable orthogonal designs*

$$X = x_1X_1 + x_2X_2 + \cdots + x_rX_r \text{ and } Y = y_1Y_1 + y_2Y_2 + \cdots + y_sY_s$$

$AOD(n : (u_1, u_2, \ldots, u_r); (v_1, v_2, \ldots, v_s))$. Further suppose there are amicable orthogonal designs $W = w_1W_1 + w_2W_2 + \cdots + w_tW_t$ and Z in order $AOD(m : (p_1, p_2, \ldots, p_t); (z))$. Then there exist

$$AOD(mn : (zu_1, zu_2, \ldots, zu_{i-1}, p_1u_i, p_2u_i, \ldots, p_tu_i, zu_{i+1}, \ldots, zu_r); (zv_1, zv_2, \ldots, zv_s)).$$

Proof. The required matrices in the variables

$$a_1, a_2, \ldots, a_{i-1},\ c_1, \ldots, c_t,\ a_{i+1}, \ldots, a_r \text{ and } b_1, \ldots, b_s$$

are

$$a_1X_1 \times Z + \cdots + a_{i-1}X_{i-l} \times Z + \sum_{j=1}^{t} c_jX_i \times W_j + a_{i+1}X_{i+l} \times Z + \cdots + a_rX_r \times \mathbb{Z},$$

and

$$\sum_{j=1}^{s} b_jY_j \times Z. \qquad \square$$

Corollary 5.9. *Suppose there is $AOD(n : (u_1, u_2, \ldots, u_t); (v_1, v_2, \ldots, v_s))$. Further suppose there exist amicable Hadamard matrices of order m. Then there exist $AOD(mn : (u_1, (m-1)u_1, mu_2, \ldots, mu_t); (mv_1, mv_2, \ldots, mv_s))$.*

Corollary 5.10. *There exist $AOD(2^{t+1} : (1, 1, 2, 4, \ldots, 2^t); (2^t, 2^t))$ and $AOD(2^{t+1} : (1, 2^{t+1} - 1); (2^t, 2^t))$.*

Proof. In proposition 5.1 $AOD(2 : (1, 1); (1, 1))$ were given. Setting the variables in the second design equal to each other, amicable Hadamard matrices of order 2 are obtained. This corollary then follows by repeated application of corollary 5.9. $\square$

As one special case of 5.10, the well-known fact that amicable Hadamard matrices exist in orders which are a power of 2 were obtained. Consequently, it has:

Corollary 5.11. *Suppose there is $AOD(n : (u_1, u_2, \ldots, u_r); (v_1, v_2, \ldots, v_s))$. Then $AOD(2^t n : (u_1, u_1, 2u_1, \ldots, 2^{t-1}u_1, 2^tu_2, \ldots, 2^tu_r); (2^tv_1, 2^tv_s))$ exist.*

Now to a different construction for amicable orthogonal designs. A similar construction based on the constructions of R.E.A.C. Paley [160] was first used to construct amicable Hadamard matrices.

Theorem 5.12. *Let $p \equiv 3 \pmod 4$ be a prime power; then there exist $AOD(p + 1 : (1, p); (1, p))$.*

Proof. Let Q be the matrix constructed in Lemma 4.12. Recall that Q is a type 1 matrix with the properties:

$$\begin{aligned} QQ^\top &= pI - J\,, \\ QJ &= JQ = 0\,, \\ Q^\top &= (-1)^{\frac{1}{2}(p-1)}Q\,. \end{aligned}$$

Now let $U = cI + dQ$, where c, d are commuting variables. Define $R = (r_{ij})$ by

$$r_{ij} = \begin{cases} 1 & a_i + a_j = 0\,, \\ 0 & \text{otherwise}\,. \end{cases}$$

Then UR is a (symmetric) type 2 matrix.

Let a, b be commuting variables. Then for $p \equiv 3 \pmod 4$

$$A = \begin{bmatrix} a & b \dots b \\ -b & \\ \vdots & aI + bQ \\ -b & \end{bmatrix} \qquad \text{and} \qquad B = \begin{bmatrix} -c & d \ \dots \ d \\ d & \\ \vdots & (cI + dQ)R \\ d & \end{bmatrix}$$

are the required $AOD(p+1 : (1,p);(1,p))$.

Table 5.7 shows $AOD(8 : (1,7);(1,7))$. □

Table 5.7 $AOD(8 : (1,7);(1,7))$

$$A = \begin{bmatrix} a & b & b & b & b & b & b & b \\ -b & a & b & b & -b & b & -b & -b \\ -b & -b & a & b & b & -b & b & -b \\ -b & -b & -b & a & b & b & -b & b \\ -b & b & -b & -b & a & b & b & -b \\ -b & -b & b & -b & -b & a & b & b \\ -b & b & -b & b & -b & -b & a & b \\ -b & b & b & -b & b & -b & -b & a \end{bmatrix} \text{ and } B = \begin{bmatrix} -c & d & d & d & d & d & d & d \\ d & -d & -d & d & -d & d & d & c \\ d & -d & d & -d & d & d & c & -d \\ d & d & -d & d & d & c & -d & -d \\ d & -d & d & d & c & -d & -d & d \\ d & d & d & c & -d & -d & d & -d \\ d & d & c & -d & -d & d & -d & d \\ d & c & -d & -d & d & -d & d & d \end{bmatrix}$$

Corollary 5.12. *Let $p \equiv 3 \pmod 4$ be a prime power. Then there exist $AOD(2^s(p+1) : (1,1,2,\dots,2^{s-1},2^s p);\ (2^s, 2^s p))$.*

Proof. Construct the amicable orthogonal designs $x_1 I + x_2 S$ and $y_1 R + y_2 P$ of types $((1,p);(1,p))$ in order $(p+1)$. Now repeatedly replace the variable x_1 by $\begin{bmatrix} x_1 & x_{s+2} \\ -x_{s+2} & x_1 \end{bmatrix}$; and any other variables x_i or y_j by $\begin{bmatrix} x_i & x_i \\ x_i & -x_i \end{bmatrix}$ or $\begin{bmatrix} y_j & y_j \\ y_j & -y_j \end{bmatrix}$. □

In a similar vein:

Lemma 5.7. *Let $n+1 \equiv 2 \pmod 4$ be the order of a symmetric conference matrix N (ie, $N^\top = N$, $NN^\top = nI_{n+1}$, and N has entries $0,1,-1$). Then there exist*

(i) $AOD(2(n+1) : (2,2n);(2,2n))$,
(ii) $AOD(2(n+1) : (1,n),(1,n))$.

Proof. Let a, b, c, d be commuting variables. Then for (i) the required designs are

$$\begin{bmatrix} aI+bN & aI-bN \\ aI-bN & -aI-bN \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} cI+dN & cI-dN \\ -cI+dN & cI+dN \end{bmatrix},$$

while for (ii) they are

$$\begin{bmatrix} aI & bN \\ bN & -aI \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} cI & dN \\ -dN & cI \end{bmatrix}.$$

The fact that N can be chosen to have zero diagonal is guaranteed by theorem 2.5. □

With $N = \begin{bmatrix} 0 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & Q & \\ 1 & & & \end{bmatrix}$ where Q is formed as above, we have

Corollary 5.13. *Let $q \equiv 1 \pmod 4$ be a prime power. Then there exist (i) $AOD(2(q+1) : (2,2q);\ (2,2q))$, (ii) $AOD(2(q+1) : (1,q);\ (1,q))$ and thus*

(i) $AOD(2^{s+1}(q+1) : (2,2,4,\dots,2^s,2^{s+1}q);\ (2^{s+1}(q+1))$,
(ii) $AOD(2^{s+1}(q+1) : (1,1,2,\dots,2^{s-1},2^sq);\ (2^s,2^sq))$.

Part (i) of the next theorem is a corollary to 5.6, while part (ii) is not. The theorem is motivated by 5.12.

Theorem 5.13. *Suppose there are $AOD(n : (1,s);(r,p))$. Suppose further that there are $AOD(m : (1,a);(b))$. Then there are*

(i) $AOD(mn : (1,a,sb);\ (rb,pb))$,
(ii) $AOD(mn : (1,ra,p);\ (b,sa))$.

Proof. From 5.4 it may be chosen that $OD(1,s)$ to be $x_1I + x_2S$, where $S^\top = -S$, and $OD(r,p)$ to be $x_3R + x_4P$, where $R^\top = R$ and $P^\top = P$. Further, the design of type $(1,a)$ can be chosen as $v_1I + v_2A$, where $A^\top = -A$, and the design of type (b) as v_3B, where $B^\top = B$. Then

(i) $y_1I \times I + y_2I \times A + y_3S \times B$ and $y_4R \times B + y_5P \times B$,
(ii) $y_1I \times I + y_2R \times A + y_3P \times A$ and $y_4I \times B + y_5S \times A$,

may be used to give the required amicable orthogonal designs. □

5.8 Construction Methods

Corollary 5.14. *Let $q \equiv 3 \pmod 4$ be a prime power. Suppose there are $AOD(m:(1,a);(b))$. Then there are*

(i) $AOD(m(q+1):(1,a,bq);(b,bq))$,
(ii) $AOD(m(q+1):(1,a,qa);(b,qa))$.

Consider

$$\begin{aligned} X_1 &= \begin{bmatrix} x_1 & x_2 & x_3 & x_3 \\ -x_2 & x_1 & x_3 & -x_3 \\ x_3 & x_3 & -x_1 & -x_2 \\ x_3 & -x_3 & x_2 & -x_1 \end{bmatrix}, Y_1 = \begin{bmatrix} y_1 & y_2 & y_3 & y_3 \\ y_2 & -y_1 & y_3 & -y_3 \\ -y_3 & -y_3 & y_2 & y_1 \\ -y_3 & y_3 & y_1 & -y_2 \end{bmatrix} \\ &= x_1X_1 + x_2X_2 + x_3X_3 \qquad = y_1Y_1 + y_2Y_2 + y_3Y_3 \\ X_2 &= \begin{bmatrix} x_1 & x_2 & x_3 & x_3 \\ -x_2 & x_1 & x_3 & -x_3 \\ -x_3 & -x_3 & x_1 & -x_2 \\ -x_3 & x_3 & -x_2 & x_1 \end{bmatrix}, Y_2 = \begin{bmatrix} y_1 & y_2 & y_3 & y_3 \\ y_2 & -y_1 & y_3 & -y_3 \\ y_3 & y_3 & -y_2 & -y_1 \\ y_3 & -y_3 & -y_1 & y_2 \end{bmatrix} \\ &= x_1U_1 + x_2U_2 + x_3U_3 \qquad = y_1V_1 + y_2V_2 + y_3V_3 \end{aligned} \tag{5.8}$$

Then there is:

Lemma 5.8. *Suppose there is a set of pairwise amicable weighing matrices (or orthogonal designs) $\{M_1,\ldots,M_s,N_1,\ldots,N_t\}$ of order m and weights $(m_1,\ldots,m_s,n_1,\ldots,n_s)$ where $M_i^\top = -M_i$, $\forall j$ and $N_j^\top = N_j$, $\forall j$. Then there are*

(i) $AOD(4m:(1,m_a,m_b,2m_c);(n_d,m_e,2m_f))$,
(ii) $AOD(4m:(1,m_a,n_b,2n_c);(n_d,n_e,2n_f))$,
(iii) $AOD(4m:(1,m_a,n_b2m_c);(n_d,n_e,2m_f))$,
(iv) $AOD(4m:(1,m_a,n_b,2m_c);(n_d,m_e,2n_f))$,

where $m_i \in \{m_1,\ldots,m_s\}$, $\in \{1,\ldots,s\}$ and $n_j \in \{n_1,\ldots,n_t\}$, $j \in \{l,\ldots,t\}$.

Proof. Use the matrices defined by (5.8) above. The required designs are:

(i) $u_1I\times I + u_2V_1\times M_a + u_3V_2\times M_b + u_4V_3\times M_c$ and
$v_1U_1\times N_d + v_2U_2\times M_e + v_3U_3\times M_f$,
(ii) $u_1I\times I + u_2U_1\times M_a + u_3U_2\times N_b + u_4U_3\times N_c$ and
$v_1V_1\times N_d + v_2V_2\times N_e + v_3\times N_f$,
(iii) $u_1I\times I + u_2U_1\times M_a + u_3U_2\times N_b + u_4U_3\times M_c$ and
$v_1V_1\times N_d + v_2V_2\times N_e + v_3V_3\times M_f$,
(iv) $u_1I\times I + u_2V_1\times M_a + u_3V_2\times M_b + u_4V_3\times N_c$ and
$v_1U_1\times N_d + v_2U_2\times M_e + v_3U_3\times N_f$.

Now look specifically at what happens for orders which are a power of 2. □

5.9 Specific Orders 2^n

Corollary 5.10 gives a powerful result for AOD in order 2^n. Now we will consider $n = 2, 3$, and 4.

5.9.1 Amicable OD of order 2

Table 5.8 amicable orthogonal designs X Y of order 2 exist

X	Y
(1)	$* * *$
(2)	$* *$
(1,1)	$*$

Lemma 5.9. *There are amicable orthogonal designs X, Y of order 2 for the types indicated in Table 5.8 (by symmetry consider only the upper triangular block):*

Proof. All these can be obtained by equating and killing variables in

$$X = \begin{bmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{bmatrix} \qquad \text{and} \qquad \begin{bmatrix} y_1 & y_2 \\ y_2 & -y_1 \end{bmatrix}. \square$$

Lemma 5.10. *There are amicable orthogonal designs X, Y of order 4 for the types indicated in Table 5.9 (those entries left blank correspond to designs which do not exist by Theorem 5.9.*

Proof. Let a, b, c, x, y, z be commuting variables. Then

$$\begin{bmatrix} a & b & c & 0 \\ -b & a & 0 & -c \\ -c & 0 & a & b \\ 0 & c & -c & a \end{bmatrix} \qquad \text{and} \qquad \begin{bmatrix} x & y & z & 0 \\ y & -x & 0 & -z \\ z & 0 & -x & y \\ 0 & -z & y & x \end{bmatrix},$$

or

$$\begin{bmatrix} 0 & a & b & c \\ -a & 0 & c & -b \\ -b & -c & 0 & a \\ -c & b & -a & 0 \end{bmatrix} \qquad \text{and} \qquad \begin{bmatrix} 0 & x & y & z \\ -x & 0 & -z & y \\ -y & z & 0 & -x \\ -z & -y & x & 0 \end{bmatrix},$$

are $AOD((1,1,1);(1,1,1))$; $AOD((1,1,2);(1,1,2))$ are given in section 5.1; now, equating and killing variables in these designs gives the result. $\square$

Table 5.9 X, Y of order 4 exist

X \ Y	(1)	(2)	(3)	(4)	(1,1)	(1,2)	(1,3)	(2,2)	(1,1,1)	(1,1,2)
(1)	*	*	*	*	*	*	*	*	*	*
(2)		*	*	*	*	*	*	*	*	*
(3)			*	*	*	*	*	*	*	*
(4)				*	*	*	*	*		*
(1,1)					*	*	*	*	*	*
(1,2)						*	*	*	*	*
(1,3)							*	*		*
(2,2)								*		*
(1,1,1)									*	
(1,1,2)										*

5.9.2 Amicable Orthogonal Designs of Order 8

Remark 5.4. With quite some surprise, it was noticed that only "full" (ie, no zeros) $AOD(8:(1,1,2,4);(2,2,4))$, $AOD(8:(1,1,2,2,2);(8))$, $AOD(8:(1,2,2,3);(2,6))$ and $AOD(8:(1,7);(1,7))$ could be found. Robinson [166] has established that there are no other "full" $AOD(8:(1,a,b,c,d);(e,f,g))$. There are other amicable orthogonal designs, eg, $AOD(8:(1,1,2);(1,1,2))$ and $AOD(8:(1,1,1,1,1),(1))$. These results indicate that the algebraic theory comes nowhere near explaining the existence or non-existence of amicable orthogonal designs.

The precise situation for amicable orthogonal designs in order 8 of type $(8:(1,u_1,\ldots,u_t);(v_1,\ldots,v_s))$ with $\sum_{i=1}^{t} u_i = 7$ and $\sum_{i=1}^{s} v_i = 8$ is given by:

Theorem 5.14 (Robinson-Wolfe [80, p.248]). *The following amicable orthogonal designs (and those which can be derived from them) exist in order* 8*:*

$$AOD(8:(1,1,2,2,2);(8)), \quad AOD(8:(1,2,2,3);(2,6)),$$
$$AOD(8:(1,1,2,4);(2,2,4)), \quad AOD(8:(1,7);(1,7)).$$

All others, of the type $AOD(8:(1,a,b,c,d);(e,f,g))$*, where* $a+b+c+d=7$ *and* $a+b+c+d=7$ *and* $e+f+g=8$*, do not exist.*

Proof. Corollary 5.10 gives the $(8:(1,1,2,4);(2,2,4))$; Theorem 5.12, the $AOD(8:(1,7);(1,7))$. $AOD(8:(1,1,2,2,2);(8))$ and $AOD(8:(1,2,2,3);(2,6))$ are given in Robinson [165].

Theorems 5.10, 5.9 and 5.7 eliminate many possibilities.

As can be shown below, there are no $AOD(8:(1,7);(5))$; this eliminates several remaining possibilities.

Example 5.6 part (4) eliminates the $(8:(1,7);(2,2,2,2))$. Theorem 5.8 part (5) eliminates $(8:(1,1,3,3);(2,2,4))$.

The remaining possibilities are not excluded by the algebraic theory, but Robinson [166] has shown (combinatorially) that the $(8:(1,1,3,3);(8))$ and the $(8:(1,2,2,3);(4,4))$ are impossible, and that takes care of all the rest. □

To finish the proof of Theorem 5.14, we need to show non-existence of $AOD(8:(1,7);(5))$, $(8:(1,1,3,3);(8))$ and $(8:(1,2,2,3);(4,4))$ in order 8. Only the argument for $AOD(8:(1,7);5)$ shall be shown here. The other two require longer but similar arguments.

Note that by Lemma 5.4 it is enough to prove:

Theorem 5.15. *There are no amicable orthogonal designs A, B of type $((7);(5))$ in order 8 where $A^\top = -A$ and $B^\top = B$. (Hence there are no $AOD(8:(1,7);(5))$.*

The proof is given in full in Geramita and Seberry [80, p.249-252].

A detailed study of amicable orthogonal designs in order 8 is given by Deborah Street in [202, p125–134] and [203, p26–29]. This was checked and extended by Elaine Zhao, Yejing Wang and Jennifer Seberry [258].

We now include the tables from [203] which summarize the known results about the existence and non-existence of amicable designs of order 8. In Tables 5.10 to 5.18, all references in square brackets are to Geramita and Seberry (1979) [80] and

No_A means that such a pair cannot exist by virtue of [Theorem 5.39],
No_B means that such a pair cannot exist by virtue of [Theorem 5.41],
No_C means that such a pair cannot exist by virtue of [Theorem 5.45],
No_D means that such a pair cannot exist by virtue of [Theorem 5.47],
No_F means that such a pair cannot exist by virtue of [p.240],
No_G means that such a pair cannot exist by virtue of [Theorem 5.64],
No_H means that such a pair cannot exist from Zhao, Wang and Seberry [258],
y_1 means that such a pair can be constructed using Theorem 7.1.7 [247],
y_2 means that such a pair can be constructed using [Theorem 5.52],
y_3 means that such a pair can be constructed using [Theorem 5.58],
y_4 means that such a pair can be constructed using [Theorem 5.64],
y_5 means that such a pair can be constructed using [Theorem 5.95],
y_6 means that such a pair can be constructed using [Table 5.6],
y_7 means that such a pair can be found in Zhao, Wang and Seberry [258],
R-S means that such a pair is given in Robinson and Seberry (1978) [170], and
* means that such a pair can be constructed using Example 7.1.10 [202].

The number of variables in each member of a pair is shown in the caption of the table.

Table 5.10 Both designs with 4 variables [a]

	1111	1114	1122	2222
1111	27			No_B
1114		*		No_B
1122			y_1	No_F
2222				

	1112	1124	1222
1112	y_1	No_B	y_7
1124		No_C	No_C
1222			

	1113	1223
1113		No_B
1223		No_C

1115	1123	1133
No_B		No_C

[a] D. Street [203, p.26-29] ©Cambridge University Press

Table 5.11 Designs with 4 and 3 variables [a]

	1,1,1,1	1,1,1,4	1,1,2,2	2,2,2,2	1,1,1,2	1,1,2,4	1,2,2,2	1,1,1,3	1,2,2,3	1,1,2,3	1,1,1,5	1,1,3,3
1,1,1	y_1	*		No_B	y_5	No_B			No_B	No_A	No_B	No_A
1,1,4		*		No_F	No_H	No_C			No_C	No_A	No_C	No_A
1,2,2			y_5	No_F	y_5	No_C			No_C	No_A	No_C	No_A
2,2,4	No_B	No_B		y_1	No_B	y_1		No_B	No_F	No_A	No_B	No_A
1,1,2	y_5		y_1	No_F	y_1	No_C		No_A	No_A		No_A	No_A
1,2,4		*		No_F	y_7	No_C		No_A	No_A		No_A	No_A
2,2,2			y_1		y_7			No_A	No_A		No_A	No_A
1,1,3	No_A	No_A	No_A	No_A	y_6	No_C			No_C		No_A	No_C
1,3,4	No_A	No_A	No_A	No_A	No_B	No_C	No_C	No_B	No_C	No_C	No_A	No_C
2,2,3	No_A	No_A	No_A	No_A	No_B	No_F		No_B	No_F		No_A	No_F
1,2,3			y_1	No_F	No_A	No_A	No_A		No_C		No_A	No_A
1,1,5		*		No_D	No_A	No_A	No_A	No_A	No_A		No_C	No_A
1,3,3	No_A	No_A	No_A	No_A	No_A	No_A	No_A	No_A	No_A	y_6	No_A	No_C
1,1,y_6	No_A	No_A	No_A	No_A	No_B	No_C	No_C	No_A	No_A	No_A	No_B	No_C
1,2,5	No_A	No_A	No_A	No_A	No_B	No_C	No_C	No_B	No_C	No_A	No_B	No_A
2,3,3	No_A	No_A	No_A	No_A	No_A	No_A	No_A	No_B	No_F	No_A	No_A	No_D

[a] D. Street [203, p.26-29] ©Cambridge University Press

Table 5.12 Designs with 4 and 2 variables [a]

	1,1,1,1	1,1,1,4	1,1,2,2	2,2,2,2	1,1,1,2	1,1,2,4	1,2,2,2	1,1,1,3	1,2,2,3	1,1,2,3	1,1,1,5	1,1,3,3
1,1	y_1	*	y_1	No_F	y_1	No_C			No_C		No_C	No_C
1,4		*	y_5	No_F	y_6	No_C			No_C		No_C	No_C
2,2	y_6		y_1	y_1	y_1	y_1						
4,4	No_B	No_B		y_1	No_B	y_1		No_B	No_F	No_D	No_B	No_D
1,2	y_1	*	y_1	No_F	y_1	No_C			No_C		No_C	No_A
2,4		*	y_1	y_1	y_7	y_1						No_A
1,3	y_5		y_1	No_F	y_1	No_C			No_C	y_6	No_A	No_C
3,4		*			y_7					y_6	No_A	
1,5		*	y_1	No_F	No_H	No_C			No_C		No_C	No_A
1,6		*		No_F	y_7	No_C		No_A	No_A	y_6	No_C	No_C
1,7	No_A	No_A	No_A	No_A	No_B	No_C	No_F	No_B	No_C	No_D	No_B	No_C
2,3			y_5		y_6	No_F			No_F		No_F	No_F
2,5		*			y_7	No_F			No_F		No_F	No_F
2,6	No_B	No_B		y_1	No_B	y_1		No_B	y_4	No_A	No_B	No_D
3,3			y_1		No_A	No_A	No_A	y_1		y_1	No_A	
3,5	No_B	No_B			No_B	No_F		No_B	No_F	No_D	No_B	No_D

[a] D. Street [203, p.26-29]

Table 5.13 Designs with 4 and 1 variables [a]

	1,1,1,1	1,1,1,4	1,1,2,2	2,2,2,2	1,1,1,2	1,1,2,4	1,2,2,2	1,1,1,3	1,2,2,3	1,1,2,3	1,1,1,5	1,1,3,3
1	y_1	*	y_1	No_F	y_1	No_C			No_C	No_C	y_6	No_C
2	y_1	*	y_1	y_1	y_1	y_1			y_4			
3	y_1	*	y_1		y_1			y_1			y_1	
4	y_6	*	y_1	y_1	y_1	y_1						
5		*	y_5		y_6	No_F			No_F	No_F		No_F
6		*	y_1	y_1	y_7	y_1		y_1	y_4		y_1	
7		*			y_7						y_6	
8	No_B	No_B		y_1	No_B	y_1		No_B	y_4	No_B	No_D	No_D

[a] D. Street [203, p.26-29] ©Cambridge University Press

Table 5.14 Both designs with 3 variables [a]

	1,1,1	1,1,4	1,2,2	2,2,4	1,1,2	1,2,4	2,2,2	1,1,3	2,2,3	1,3,4	1,2,3	1,1,5	1,3,3	1,1,6	1,2,5	2,3,3
1,1,1	48	*	48	48	*		6		B		*		B	B	B	
1,1,4		*		48	*	48			C	48	*		C	C		
1,2,2			95	48		48	6		C	95			C	C		
2,2,4				48	48	48	D		48		D		48	48	48	
1,1,2				48		48	48		C	48		48	C	C		
1,2,4					48				C		*	6	C	C		
2,2,2						48				48						
1,1,3							6		C			6	C	C	D	
2,2,3									F			6	F	F		
1,3,4									C	C	C	C	C	C	F	
1,2,3										48		6	C	C		
1,1,5											*	6	C	C	D	
1,3,3												6	C	C	F	
1,1,6													C	C	G	
1,2,5														C	F	
2,3,3																

[a] D. Street [203, p.26-29] ©Cambridge University Press

Table 5.15 Designs with 3 and 2 variables [a]

	1,1,1	1,1,4	1,2,2	2,2,4	1,1,2	1,2,4	2,2,2	1,1,3	2,2,3	1,3,4	1,2,3	1,1,5	1,3,3	1,1,6	1,2,5	2,3,3
1,1	y_1	*	y_1	y_1	y_1	*	y_1	y_1		No_C	y_1	*	y_1	No_C	No_C	
1,4	y_2	*	y_5	y_1	y_1	*	y_1	y_6		No_C	y_5	*	y_6	No_C	No_C	
2,2	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1		y_1	y_1		y_1	y_1	y_1	y_1
4,4	No_B	y_1		y_1	y_1	y_1	y_1	No_D		y_1		No_D		y_1	y_1	y_1
1,2	y_1	*	y_1	y_1	y_1	*	y_1	y_1		No_C	y_1	*	y_1	No_C	No_C	
2,4	*	y_1	y_1	y_1	y_1	y_1	y_1			y_1	y_1	*	y_6	y_1	y_1	y_1
1,3	y_1	y_1	y_1	y_1	y_1	y_6	y_1	y_1	y_6	No_C	y_1	y_6	y_1	No_C	No_C	
3,4	*	*		y_1	y_6	y_6		y_6	y_6		y_6	y_6	y_2			
1,5	*	*	y_5	y_1	y_1	*	y_1			No_C	y_1	*	y_6	No_C	No_C	
1,6	*	*		y_1	y_6	y_6		y_6	y_6	No_C	y_6	y_6	y_6	No_C	No_C	
1,7	No_B	No_F	No_F	y_1		No_F		No_D	No_F	No_C	No_F	No_D		No_C	No_C	No_F
2,3	y_2	y_1	y_2		y_1		y_1	y_2		No_F	y_5		y_2	No_F	No_F	
2,5	*	*		y_1		*				No_F		*	y_6	No_F	No_F	
2,6	No_B	y_1	y_4	y_1	y_1	y_1	y_1	No_D	y_4	y_1	y_4	No_D		y_1	y_1	y_1
3,3	y_1		y_5	y_1	y_1	y_6	y_1	y_1	y_1		y_1	y_6	y_1			
3,5	No_B			y_1				No_D		No_F		No_D		No_F	No_F	

[a] D. Street [203, p.26-29] ©Cambridge University Press

Table 5.16 Designs with 3 and 1 variables [a]

	1,1,1	1,1,4	1,2,2	2,2,4	1,1,2	1,2,4	2,2,2	1,1,3	2,2,3	1,3,4	1,2,3	1,1,5	1,3,3	1,1,6	1,2,5	2,3,3
1	y_1	*	y_1	y_1	y_1	y_6	y_1	y_1	y_6	$\mathrm{No_C}$	y_1	y_6	y_1	$\mathrm{No_C}$	$\mathrm{No_C}$	
2	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_4	y_1	y_1	*	y_1	y_1	y_1	y_1
3	y_1	*	y_1	y_1	y_1	y_6	y_1	y_1	y_1		y_1	y_6	y_1			
4	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_5	y_1	y_1	*	y_1	y_1	y_1	y_1
5	y_3	*	y_3	y_1	y_1	*	y_1	y_6		$\mathrm{No_F}$	y_5	*	y_3	$\mathrm{No_F}$	$\mathrm{No_F}$	
6	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_6	y_1	y_1	y_1	y_1
7	*	*		y_1	y_6	y_6		y_6	y_6		y_6	y_6	y_3			
8	$\mathrm{No_B}$	y_1	y_4	y_1	y_1	y_1	y_1	$\mathrm{No_D}$	y_4	y_1	y_4	$\mathrm{No_D}$		y_1	y_1	y_1

[a] D. Street [203, p.26-29] ©Cambridge University Press

Table 5.17 Both designs with 2 variables [a]

	1,1	1,2	1,3	1,4	1,5	1,6	1,7	2,2	2,3	2,4	2,5	2,6	3,3	3,4	3,5	4,4
1,1	y_1	y_1	y_1	y_1	y_1	y_1		y_1	y_1	y_1	*	y_1	y_1	y_1		y_1
1,2		y_1	y_1	y_1	y_1	y_1		y_1	y_1	y_1	*	y_1	y_1	y_1		y_1
1,3			y_1	y_1	y_1	y_1		y_1	y_1	y_1	y_6	y_1	y_1	y_1		y_1
1,4				y_6	y_5	y_6	No_F	y_1	y_3	y_1	*	y_1	y_1	y_6		y_1
1,5					*	y_6	No_F	y_1	y_5	y_1	*	y_1	y_1	y_6		y_1
1,6						y_6		y_1	y_3	y_1	y_6	y_1	y_1	y_3		y_1
1,7							y_2	y_1	No_F	y_1	No_F	y_1			No_F	y_1
2,2								y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1
2,3									y_3	y_1		y_1	y_1	y_3		y_1
2,4										y_1	y_1	y_1	y_1	y_1	y_1	y_1
2,5											*	y_1	y_1	y_6		y_1
2,6												y_1	y_1	y_1	y_1	y_1
3,3													y_1	y_1		y_1
3.4														y_3		y_1
3,5																y_1
4,4																

[a] D. Street [203, p.26-29] ©Cambridge University Press

Table 5.18 Both designs with 2 and 1 variables [a]

	1,1	1,2	1,3	1,4	1,5	1,6	1,7	2,2	2,3	2,4	2,5	2,6	3,3	3,4	3,5	4,4
1	y_1	y_1	y_1	y_1	y_1	y_1	y_2	y_1	y_1	y_1	y_6	y_1	y_1	y_1		y_1
2	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1
3	y_1	y_1	y_1	y_1	y_1	y_1	R-S	y_1	y_1	y_1	y_6	y_1	y_1	y_1		y_1
4	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1
5	y_1	y_1	y_1	y_3	y_5	y_3	No_F	y_1	y_3	y_1	*	y_1	y_1	y_3		y_1
6	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1
7	y_1	y_1	y_1	y_6	y_6	y_3	y_2	y_1	y_3	y_1	y_6	y_1	y_1	y_3		y_1
8	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1	y_1

[a] D. Street [203, p.26-29] ©Cambridge University Press

A complete determination of exactly which (non-full) amicable orthogonal designs may exist in order 16 has not yet been made. In fact, full amicable orthogonal designs, when neither design is of type $(1, \ldots)$, have hardly been looked at in order 16.

5.10 Amicable Hadamard Matrices

Skew-Hadamard matrices have played a significant part in the search for Hadamard matrices (see Williamson [245]) Spence [197] and Wallis [224–226]). Szekeres [205] realized that skew-Hadamard matrices were of interest in themselves and, in fact, equivalent to doubly regular tournaments.

Once attention was focused on skew-Hadamard matrices, (Seberry)Wallis [227] realised that in order to form skew-Hadamard matrices of order mn from ones of orders m and n, a notion of "amicability" could be decisive. This was the origin of the idea of amicable Hadamard matrices.

Although this section is embedded in the chapter on amicable orthogonal designs, it will be clear that the ideas here, which historically precede the rest of the ideas of this chapter, have exerted a strong influence on the development of "amicability" for orthogonal designs.

We restate a theorem of J. Wallis [231, p.337, Theorem 4.20] in terms of our new notation:

Theorem 5.16 (J. Wallis). *Suppose there exist amicable orthogonal designs* $AOD(m\colon (1,m-1);(m))$ *and* $AOD(n\colon (1,n-1);(n))$. *Further suppose there exists* $OD((m-1)n\colon (1,(m-1)n-1))$. *Then there exists an* $OD(1,mn(mn-1)(m-1)-1)$ *in order* $mn(mn-1)(m-1)$.

Proof. We use Lemma 5.6 with the designs of types $((1,m-1);(m))$ and $(1,(m-l)n-1)$ to see that there is $OD(1,m-1,mn(m-1)-m)$ in order $mn(m-1)$. We use the designs of types $((1,m-1);(m))$ and $((1,n-1);(n))$ to see that there are $AOD(mn\colon (1,mn-1);(mn))$.

We now write $AOD((1,mn-1);(mn)$ (after suitable pre- and post-multiplication by monomial matrices) as

$$M=\begin{bmatrix} x & ye \\ -ye^\top & P \end{bmatrix} \qquad \text{and} \qquad N=\begin{bmatrix} 1 & e \\ e^\top & D \end{bmatrix},$$

where $e=(1,\dots,1)$ is of order $1\times(mn-1)$, and x, y are commuting variables. Then

$$\begin{aligned} &JP^\top = xJ, \quad (P-xI)^\top = -(P-xI), \quad D^\top = D, \quad JD^\top = -J, \\ &PP^\top = (x^2+(mn-1)y^2)I - y^2J, \end{aligned}$$

Since

$$\begin{aligned} MN^\top &= \begin{bmatrix} x & ye \\ -ye^\top & P \end{bmatrix}\begin{bmatrix} 1 & e \\ e^\top & D^\top \end{bmatrix} = \begin{bmatrix} x+(mn-1)y & (x-y)e \\ (x-y)e^\top & -yJ+PD^\top \end{bmatrix} \\ &= \begin{bmatrix} x+(mn-1)y & (-y+x)e \\ (x-y)e^\top & -yJ+DP^\top \end{bmatrix} = \begin{bmatrix} 1 & e \\ e^\top & D \end{bmatrix}\begin{bmatrix} x & -ye \\ ye^\top & P^\top \end{bmatrix} = NM^\top \\ PD^\top &= DP^\top \end{aligned}$$

We now replace the variables of the $(1, m-1, mn(m-1)-m)$ design A by the matrices P, yJ, yD to obtain a matrix B. Now

$$\begin{aligned} BB^\top &= (PP^\top + (m-1)y^2J^2 + (m^2n - mn - m)y^2DD^\top) \times I \\ &= [(x^2 + (mn-1)y^2)I - y^2J + (m-1)(mn-1)y^2J \\ &\qquad + mn(m^2n - m - mn)y^2I - (m^2n - mn - m)y^2J] \times I \\ &= (x^2 + (mn(mn-1)(m-1) - 1)y^2)I_{mn(mn-1)(m-1)}. \end{aligned}$$

Hence B is the required orthogonal design. □

Corollary 5.15. *Suppose there exist* $AOD(n\colon (1, n-1); (n))$. *Then, since there exist* $AOD(2\colon (1,1);(2))$, *there is* $OD(1, 2n(2n-1)-1)$ *in order* $2n(2n-l)$.

Definition 5.5. The $s \times s$ matrices W and M are *amicable Hadamard matrices* if

(i) $W = I + S$,where $S^\top = -S$ and $M = M^\top$ are both Hadamard matrices, ie, weighing matrices of weight s, and
(ii) $WM^\top = MW^\top$.

These pairs of matrices exist for many orders, some of which are discussed below.

Conjecture 5.1. There exist amicable Hadamard matrices in all orders $n \equiv 0 \pmod 4$.

Amicable Hadamard matrices and amicable orthogonal designs of type $AOD(n : (1, n-1); (n))$ are equivalent notions (Lemma 5.4). Hence they may be used to construct other orthogonal designs as follows (Lemma 5.6):

Lemma 5.11. *Let* $y_1A_1 + y_2A_2 + \cdots + y_pA_p$ *be* $OD(n; a_1, a_2 \ldots, a_p)$ *on the* p *variables* $y_1, y_2, \ldots, y_p$.
Let $W = I_s + S$ *and* M *be amicable Hadamard matrices of order* s.
Then

$$x_0A_1 \times I_s + x_1A_1 \times S + x_2A_2 \times M + \cdots + a_pA_p \times M$$

is $OD(sn; a_1, a_1(s-1), sa_2, \ldots, sa_p)$ *on the variables* $x_0, x_1, \ldots, x_p$.

Corollary 5.16. *Let* W *and* M *(as above) be amicable Hadamard matrices of order* s, *and let* n *be any integer. Then there is* $OD(ns; 1, s-1, s, s, \ldots, s)$ *on the variables* $x_0, x_1, x_2, \ldots, x_{\rho(n)}$.

Proof. Use the $(1,1,1,\ldots,1)$ design on $\rho(n)$ variables that exist in every order n. The first variable is replaced by $x_0I + x_1W_1$; the i-th variable $i > 1$ is replaced by x_iM. □

Example 5.8. The most interesting consequence of this corollary is to note that there is an $OD(2n; (1, 1, 2, \ldots, 2))$ on $\rho(n) + 1$ variables. This follows because

there is an $OD(n;(1,1,1,\ldots,1))$ on $\rho(n)$ variables and amicable Hadamard matrices of order 2. In particular, there is an $OD(16;(1,1,2,2,2,2,2,2,2))$.

Corollary 5.17. *If there is a Baumert-Hall array of order n and amicable Hadamard matrices of order s, then there is an $OD(4n;n,n(s-1),ns,ns,ns)$.*

Example 5.9. As was seen in Chapter 4, Section 4.12 there is a Baumert-Hall array of order 3. Hence there exists an $OD(24;3,3,6,6,6)$ by using amicable Hadamard matrices of order 2.

Corollary 5.18. *Let W, M be amicable Hadamard matrices of order s. If there is a Plotkin array of order $8n$, then there is an $OD(8ns;(n,n(s-1),ns,\ldots,ns))$ on the variables $x_1,x_2,x_3,\ldots,x_9$.*

Example 5.10. Plotkin found an array of order 24, $OD(24;(3,3,3,3,3,3,3,3))$. Hence, using the amicable Hadamard matrices of order 2, an orthogonal design $OD(48;(3,3,6,6,6,6,6,6))$ is obtained. Similar results follow from Plotkin arrays $OD(8t;t,\ldots,t)$, see Section 4.13.

From Seberry and Yamada [188, p535], Geramita, Pullman and Seberry Wallis [79] and this chapter, amicable Hadamard matrices exist for the following orders:

Key	Order	Method
AI	2^t	t a non-negative integer. See [80, p224].
AII	p^r+1	$p^r \equiv 3 \pmod 4$ is a prime power. See [188, p110].
AIII	$2(q+1)$	$2q+1$ is a prime power, $q \equiv 1 \pmod 4$ is a prime. See [188, p114].
AIV	$(\lvert t\rvert+1)(q+1)$	q(prime power) $\equiv 5 \pmod 8 = s^2+4t^2$, $s \equiv 1 \pmod 4$, and $\lvert t\rvert+1$ is the order of amicable orthogonal designs of type $((1,\lvert t\rvert);(\frac{1}{2}(\lvert t\rvert+1))$.
	$2^r(q+1)$	q(prime power) $\equiv 5 \pmod 8 = s^2+4(2^r-1)^2$, $s \equiv 1 \pmod 4$, r some integer.
AV	$(4t-1)^r+1$	when circulant (or type 1) Hadamard cores of order $4t-1$ exist.
AVI	nh	n,h, are orders of amicable Hadamard matrices. See [80, p255].

AVI is proved first and then $AOD(2;(1,1),1,1)$ give AI.

Theorem 5.17 (Wallis [227]). *Suppose there are amicable Hadamard matrices of orders m and n. Then there are amicable Hadamard matrices of order mn. In particular, there exist amicable Hadamard matrices of order 2^t, t a non-negative integer.*

Proof. This is a special case of Corollary 5.9. For the last part, see Corollary 5.10. □

Proposition 5.10. *There are amicable Hadamard matrices of order* p^n+1, $p^n \equiv 3 \pmod 4$, p *a prime.*

Proof. This is a special of Theorem 5.12 (the structure is ensured by Lemma 5.4).

This justifies Case AII. □

To prove Case AIII a new concept is introduced due to Szekeres [205] which arose while he was considering tournaments. Szekeres used supplementary difference sets with one symmetry condition ($a \in M \Rightarrow -a \notin M$) to construct skew-Hadamard matrices. He pointed out to Seidel that there was no skew-Hadamard matrix of order 36 known (at that time). This, in turn, led to Goethals and Seidel publishing their array, which was to prove so significant and useful.

Definition 5.6. Let G be an additive abelian group of order $2m+1$. Then two subsets, M and N, of G, which satisfy

(i) M and N are m-sets,
(ii) $a \in M \Rightarrow -a \notin M$,
(iii) for each $d \in G$, $d \neq 0$, the equations $d = a_1 - a_2$, $d = b_1 - b_2$ have together $m-1$ distinct solution vectors for $a_1, a_2 \in M$, $b_1, b_2 \in N$,

will be called *Szekeres difference sets.* Alternatively, $2-\{2m+1; m; m-1\}$ supplementary difference sets, M and $N \subset G$, are called *Szekeres difference sets*, if $a \in M \Rightarrow -a \notin M$.

The following shows such sets exist.

Theorem 5.18 (Szekeres). *If* $q = 4m+3$ *is a prime power and* G *is the cyclic group of order* $2m+1$*, then there exist Szekeres difference sets* M *and* N *in* G *with* $b \in N \Rightarrow -b \in N$.

Proof. Let x be a primitive root of $GF(q)$ and $Q = \{x^{2b} : b = 1, \ldots, 2m+1\}$ the set of quadratic residues in $GF(q)$. Define M and N by the rules

$$a \in M \qquad \Longleftrightarrow \qquad x^{2a} - 1 \in Q\,, \tag{5.9}$$

$$b \in N \qquad \Longleftrightarrow \qquad x^{2b} + 1 \in Q\,. \tag{5.10}$$

Since

$$\begin{aligned} -1 = x^{2m+1} &\notin Q\,, \\ x^{2a} - 1 \in Q \Rightarrow x^{-2a} - 1 = -x^{-2a}(x^{2a} - 1) &\notin Q\,, \\ x^{2b} + 1 \in Q \Rightarrow x^{-2b} + 1 = x^{-2b}(x^{2b} + 1) &\in Q\,, \end{aligned}$$

so that $a \in M \Rightarrow -a \notin M$, $b \in N \Rightarrow > -b \in N$, and conditions i) and ii) of Definition 5.6 are satisfied. Also, writing N' for the complement of N, gives

$$b' \in N' \qquad \text{if} \qquad -(x^{2b'}+1) \in Q\,. \tag{5.11}$$

Suppose

$$d = \alpha - a \neq 0, \qquad a, \alpha \in M\,, \tag{5.12}$$

where

$$x^{2a} = 1 + x^{2(i-d)}\,, \tag{5.13}$$

$$x^{2\alpha} = 1 + x^{2j}\,, \tag{5.14}$$

by (5.9) for suitable $i, j \in G$. Then

$$x^{2\alpha} = x^{2(a+d)} = x^{2d} + x^{2i}\,,$$

by (5.12) and (5.13); hence by (5.14)

$$x^{2d} - 1 = x^{2j} - x^{2i}\,, \tag{5.15}$$

where $x^{2j}+1 \in Q$ by (5.14). Similarly, if

$$d = b' - \beta' \neq 0, \qquad b', \beta' \in N'\,, \tag{5.16}$$

where by (5.16)

$$-x^{2\beta'} = 1 + x^{2(i-d)}\,, \tag{5.17}$$

$$-x^{2b'} = 1 + x^{2j}\,, \tag{5.18}$$

for some $i, j \in G$, producing

$$-x^{2b'} = -x^{2(d+\beta')} = x^{2d} + x^{2i}\,;$$

hence again

$$x^{2d} - 1 = x^{2j} - x^{2i}\,,$$

with $-(x^{2j}+1) \in Q$ by (5.18).

Conversely to every solution, $i, j \in G$, of equation (5.15), we can determine uniquely $\alpha \in M'$ or $b \in N'$ from (5.14) or (5.18) depending on whether $1 + x^{2j} = x^{2d} + x^{2i}$ is in Q or not; hence a or β from (5.12) (5.16) so that also (5.13) or (5.17) is satisfied, implying $a \in M$, $\beta \in N'$. Thus the total number of solutions of (5.12) and (5.16) is equal to the number of solutions of (5.15) which is m. □

Example 5.11. Consider $q = 23$ which has primitive root 5 and quadratic residues $Q = \{1,2,3,4,6,8,9,12,13,16,18\}$. Hence

$$M = \{1,2,5,7,8\} \text{ and } N = \{2,4,5,6,7,9\}$$

are Szekeres difference sets.

Szekeres and Whiteman (see Wallis [236, p.32]) have independently shown that there exist Szekeres difference sets of size $\frac{(p^t-1)}{2}$ when $p \equiv 5 \pmod 8$ is a prime power and $t \equiv 2 \pmod 4$. But in this case both sets M, N satisfy the condition, $x \in M, N \longrightarrow -x \notin M, N$, and as yet these sets have not been used to construct amicable Hadamard matrices. Nevertheless, the next theorem and corollary indicate the way these Szekeres difference sets may, in some cases, be used:

Theorem 5.19. *Suppose there exist* $(1,-1)$ *matrices* A, B, C, D *of order* n *satisfying:*

$$C = I + U, \quad U^\top = -U, \quad A^\top = A, \quad B^\top = B, \quad D^\top = D,$$

$$AA^\top + BB^\top = CC^\top + DD^\top = 2(n+1)I - 2J,$$

and with $e = [1, \ldots, 1]$ *a* $1 \times n$ *matrix*

$$eA^\top = eB^\top = eC^\top = eD^\top = e, \quad AB^\top = BA^\top, \quad \textit{and} \quad CD^\top = DC^\top.$$

Then if

$$X = \begin{bmatrix} 1 & 1 & e & e \\ 1 & -1 & -e & e \\ e^\top & -e^\top & A & -B \\ e^\top & e^\top & -B & -A \end{bmatrix}, \qquad Y = \begin{bmatrix} 1 & 1 & e & e \\ -1 & 1 & e & -e \\ -e^\top & -e^\top & C & D \\ -e^\top & -e^\top & -D & C \end{bmatrix},$$

X is a symmetric Hadamard matrix and Y is a skew-Hadamard matrix both of order $2(n+1)$. *Further, if*

$$AC^\top - BD^\top \quad \textit{and} \quad BC^\top + AD^\top$$

are symmetric, X and Y are amicable Hadamard matrices of order $2(n+1)$.

The next result illustrates how the conditions of the theorem can be satisfied;

Corollary 5.19. *Let G be an additive abelian group of order* $2m+1$. *Suppose there exist Szekeres difference sets, M and N, in G.*

Further suppose there exist $2 - \{2m+1; m+1; m+1\}$ *supplementary difference sets P and S in G such that $x \in X \Rightarrow -x \in X$ for $X \in \{N, P, S\}$. Then there exist amicable Hadamard matrices of order* $4(m+1)$.

Proof. Form the type 1 $(1,-1)$ incidence matrix C of M. Form the type 2 $(1,-1)$ incidence matrices, D, A, B of N, P, S, respectively. Now use the properties of type 1 and type 2 matrices in the theorem.

In these theorems, circulant and back circulant can be used to replace type 1 and type 2 incidence matrices, respectively, when the orders are prime.

We now wish to show that sets satisfying the conditions of Corollary 5.19 exist for some orders $n \equiv 1 \pmod 4$.

Let $n = 4t+1$ be a prime power, and choose $Q = \{x^{2b} : b = 1, 2, \ldots, 2t\}$ and $R = xQ$, where x is a primitive element of $GF(n)$. Then Q and R are $2 - \{4t+1; 2t; 2t-1\}$ supplementary difference sets. Further, $y \in Q \Rightarrow -y \in Q$, and $y \in R \Rightarrow -y \in R$ since $-1 = x^{2t}$. So Q and R satisfying the conditions of the corollary exist. □

To find M and N, we use the result of Szekeres in Theorem 5.18. Then we have:

Corollary 5.20. *There exist amicable Hadamard matrices of order* $2(t+1)$ *whenever* $t \equiv 1 \pmod 4$ *is a prime and* $2t+1$ *is a prime power.*

Proof. With $q = 4m+3 = 2t+1$, we form Szekeres difference sets M and N of order $2m+1 = t+1$. Using the notation of Theorem 5.18,

$$b \in N \Rightarrow x^{2b}+1 \in Q \Rightarrow x^{-2b}+1 = x^{-2b}(l+x^{2b}) \in \Rightarrow -b \in N\,,$$

and so M and N are as required by Corollary 5.19.

Choose $P = Q$ and $S = xQ$; then, as observed above, they too satisfy the conditions of the theorem, and we have the result. □

This justifies Case AIII.

Theorem 5.20. *Let* $q \equiv 5 \pmod 8$ *be a prime power and* $q = s^2 + 4t^2$ *be its proper representation with* $s \equiv 1 \pmod 4$. *Suppose there are* $AOD(2r : (1, 2r-1); (r, r))$, $2r = |t|+1$. *Then there exist amicable Hadamard matrices of order* $(|t|+1)(q+1)$.

Proof. Using the theory of cyclotomy (see Chapter 7 for more details), we can show that for the q of the enunciation,

$$C_0 \;\&\; C_1 \text{ and } |t| \text{ copies of } C_0 \;\&\; C_2$$

are $(|t|+1) - \{q; \frac{(q-1)}{2}; (|t|+1)\frac{(q-3)}{4}\}$*s.d.s.* , with the property that

$$x \in C_0 \;\&\; C_1 \Rightarrow -x \notin C_0 \;\&\; C_1$$

and

$$y \in C_0 \;\&\; C_2 \Rightarrow -y \in C_0 \;\&\; C_2\,.$$

Also $\frac{(|t|+1)}{2}$ copies of each of C_0 & C_2 and C_1 & C_3 are

$$(|t|+1) \;-\; \{q; \frac{(q-1)}{2}; (|t|+1)\frac{(q-3)}{4}\} \text{ s.d.s.}$$

with the property that

$$y \in C_0 \ \& \ C_2 \Rightarrow -y \in C_0 \ \& \ C_2\,,$$
$$z \in C_1 \ \& \ C_3 \Rightarrow -z \in C_1 \ \& \ C_3\,.$$

let A be the type $1(1,-1)$ incidence matrix of C_0 & C_1, and B and C be the type $2(1,-1)$ incidence matrices of C_0 & C_2 and C_1 & C_3, respectively.

Then

$$AJ = BJ = CJ = -J\,, \quad (A+I)^\top = -(A+I)\,, \quad B^\top = B\,, \quad C^\top = C\,,$$

$$\begin{aligned} AA^\top + |t|BB^\top &= \frac{(|t|+1)}{2}(BB^\top + CC^\top) \\ &= (|t|+1)(q+1)I - (|t|+1)J\,. \end{aligned}$$

Let $P = x_0U + x_1V$ and $Q = x_3X + x_4Y$ be $AOD(2r : (1, 2r-1); (r,r))$. Further, let e be the $1 \times q$ matrix of all ones. Clearly, we may assume that $U = I$, $V^\top = -V$, $X^\top = X$, $Y^\top = Y$, for if not, we pre-multiply P and Q by the same matrix W until U, V, X, Y do have the required properties. Now

$$E = \left[\begin{array}{c|c} U+V & (U+V)\times e \\ \hline (-U+V)\times e^\top & U\times -A + V \times B \end{array}\right]$$

and

$$F = \left[\begin{array}{c|c} X+Y & (X+Y)\times e \\ \hline (X+Y)\times e^\top & X\times C + Y \times D \end{array}\right]$$

are the required amicable Hadamard matrices. □

We note that $AOD(2r : (1, 2r-1); (r,r))$ certainly exist where $2r$ is a power of two (this is proved in Corollary 5.10). Hence we have:

Corollary 5.21. *Let $q \equiv 5 \pmod 8$ be a prime power and $q = s^2 + 4t^2$ be its proper representation with $s \equiv 1 \pmod 4$. Further, suppose $|t| = 2^r - 1$ for some r. Then there exist amicable Hadamard matrices of order $2^r(q+1)$.*

In particular, this leads to two results published elsewhere (Wallis [228], [233]) which now become corollaries:

Corollary 5.22. *Let $q \equiv 5 \pmod 8$ be a prime power, and suppose $q = s^2 + 4$ or $q = s^2 + 36$ with $s \equiv 1 \pmod 4$. Then there exist amicable Hadamard matrices of orders $2(s^2+5)$ or $4(s^2+37)$, respectively.*

Corollaries 5.20 and 5.21 justify Case AIV.

5.11 Amicable Hadamard Matrices and Cores

To make Case AV clear we first define what we mean by different types of cores.

Definition 5.7 (Amicable Hadamard Cores). Let $A = I + S$ and B be amicable Hadamard matrices of order n, so $AB^\top = BA^\top$, which can be written in the form

$$A = \begin{bmatrix} 1 & e \\ -e^\top & I+W \end{bmatrix}$$

and

$$B = \begin{bmatrix} -1 & e \\ e^\top & R+V \end{bmatrix}$$

where e is a $1 \times n-1$ vector of all $+1$s. Let R be the back-diagonal matrix, W and V have row sum $+1$ and

$$V^\top = V, \quad VW^\top = WV, \quad \text{and} \quad RW^\top = WR. \tag{5.19}$$

Then $I+W$ and $R+V$ will be said to be *amicable cores* of amicable Hadamard matrices. We call W and V *amicable Hadamard cores* when the properties of Equation 5.19 are satisfied. We call W the skew-symmetric core and V the symmetric (partner) core.

Now $C_1 = I + W$ or $C_2 = R + V$ are said to be *amicable cores* of the Hadamard matrix, and

$$C_i C_i^\top = nI_{n-1} - J_{n-1}, \quad C_i J = JC_i = J, \quad i = 1,2.$$

*Example 5.12 (**Amicable Hadamard Matrices and Their Cores**).* The following two Hadamard matrices are amicable Hadamard matrices.

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \end{bmatrix}$$

with the following two matrices

$$I+W = \begin{bmatrix} 1 & 1 & -1 \\ -1 & 1 & 1 \\ 1 & -1 & 1 \end{bmatrix} \quad \text{and} \quad R+V = \begin{bmatrix} -1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & -1 & 1 \end{bmatrix}$$

as amicable cores of the amicable Hadamard matrices. Note they satisfy all the properties of Equation 5.19.

In early papers Belevitch [19, 20] and Goldberg [91] showed that the core of a skew-Hadamard matrix, of order $n+1$, could be used to generate a core of a skew-Hadamard matrix of order n^3+1. Seberry Wallis [240] realized that this construction could be extended to orders n^5+1 and n^7+1. These were further generalized by Turyn [217] to orders n^r+1, where $r>0$ is an odd integer. We now give the results in considerable detail to try to make the constructions as clear as possible.

Theorem 5.21 (Belevitch-Goldberg Theorem). *Suppose W is a skew-symmetric core of size $n \equiv 3 \pmod 4$ then*

$$I \times J \times W + W \times I \times J + J \times W \times I + W \times W \times W$$

is a core of order n^3.

Remark 5.5. If $I+W$ and $R+V$ are amicable Hadamard cores then the symmetric companion of the above skew-symmetric core is

$$R \times J \times V + V \times R \times J + J \times V \times R + V \times V \times V$$

We now use part of Corollary 3.12 of [231] which shows that is W is a skew-symmetric (symmetric) core of size $n \equiv 3 \pmod 4$ then there exists a skew-symmetric (symmetric) of size n^r for all odd $r>1$.

Example 5.13. The skew-symmetric core of order n^5 from a skew-symmetric core of order n is the sum of

$$I \times J \times I \times J \times W; \text{ and } I \times J \times W \times W \times W;$$

plus

$$W \times W \times W \times W \times W,$$

plus their circulants

$$\begin{array}{ll} W \times I \times J \times I \times J; & W \times I \times J \times W \times W; \\ J \times W \times I \times J \times I; & W \times W \times I \times J \times W; \\ I \times J \times W \times I \times J; & W \times W \times W \times I \times J; \\ J \times I \times J \times W \times I; & J \times W \times W \times W \times I. \end{array}$$

The symmetric core will have the same form with I replaced by R and W replaced by V. So it becomes the sum of

$$R \times J \times R \times J \times V; \text{ and } R \times J \times V \times V \times V; V \times V \times V \times V \times V,$$

plus their circulants

$$V\times R\times J\times R\times J;\quad V\times R\times J\times V\times V;\quad J\times V\times R\times J\times R;$$
$$V\times V\times R\times J\times V;\quad R\times J\times V\times R\times J;\quad V\times V\times V\times R\times J;$$
$$J\times R\times J\times V\times R;\quad J\times V\times V\times V\times R.$$

These amicable cores, that is the skew-symmetric and the symmetric cores, are amicable term by term. □

We now use this to construct amicable Hadamard matrices of order n^r+1 from amicable Hadamard matrix cores of order $n+1$. This is illustrated by the Belevitch-Goldberg construction Theorem 5.21 for $n=3$ and by Example 5.13 for $n=5$.

Theorem 5.22 (Construction). *Suppose W is a skew-symmetric core of size $n\equiv 3 \pmod 4$ and V ($V^\top = V$) is an amicable symmetric core. Let $\mathcal{M}$ and $\mathcal{N}$ given by*

$$I\times I\times I\cdots\times I+B_r$$

and

$$R\times R\times R\cdots\times R+D_r$$

where each single term is comprised of the sum of the Kronecker product of n terms as described below. Then $\mathcal{M}$ and $\mathcal{N}$ are cores of amicable Hadamard matrices of order n^r for any odd $r>0$.

Proof. Let I, J, W of order n be as above. The proof consists of taking the sum of the Kronecker product of all the possible basic terms A of the form $I\times J\times W\times\cdots\times W$, $I\times J\times I\times J\times W\times\cdots\times W$, $I\times J\times W\times I\times J\times\cdots\times W$ and so on and all their circulants. That is, if a new term is introduced to make a larger power, the newly introduced terms will have $I\times J$ or $W\times W$ inserted at the beginning of each term of the smaller order A_{r-2}. Call this matrix $B=B_r$. Then B will satisfy $BB^T=n^rI_{n^r}-J_{n^r}$, $BJ=JB=0$.

Because $WJ=JW=0$, it becomes easy to see that the terms of $BB^\top$ are actually each individual term of A each multiplied by its transpose.

It is a little more difficult to see that B will be a skew-symmetric core, that is that all the off diagonal elements are ±1. However this can be shown from the careful placements of the elements and that J and W (and J and V) occur in the same position in each distinct pair of terms for the higher power construction (note $JW=WJ=0$) and each pair of terms is disjoint.

Carrying out the same procedure but with A_r and B_r, with elements I, J and W replaced by C_r and D_r which have elements R, J and V gives the symmetric partner. □

Corollary 5.23. *Suppose there exist amicable Hadamard matrices of order n with amicable cores of order $n-1$. Then there exist amicable Hadamard matrices of order $(n-1)^r+1$, for all odd $r\geq 1$.*

Problem 5.4 (Research Problem). Further research is needed to extend our knowledge of amicable Hadamard matrices.

5.12 Strong Amicable Designs

As an introduction to our search for generalizations of amicable Hadamard matrices, we now consider the concept of *strong amicable Hadamard matrices.*

Definition 5.8 (Strong Amicable Hadamard Matrices). Two Hadamard matrices, M and N, of order n which are amicable, so $MN^\top = NM^\top$, and can be written as $M = I + S$, where I is the identity matrix and $S^\top = -S$ is a skew-symmetric weighing matrix ($W(n, n-1)$) and N, which can be written in the form $N = U + V$, U a symmetric monomial matrix and V is a symmetric weighing matrix ($W(n, n-1)$) will be said to be *strongly amicable Hadamard matrices.* (In fact M and N are also $AOD(n : 1, n-1; 1, n-1)$).

Seberry [180] showed:

Theorem 5.23 (Multiplication Theorem for Strong Amicable Orthogonal Designs). *If there are strong amicable orthogonal designs of orders n_1 and n_2 there are strong amicable orthogonal designs of order $n_1 n_2$. (The theorem also holds if "orthogonal designs" is replaced by "Hadamard matrices".)*

A more direct proof of the following corollary appears in [179].

Corollary 5.24. *Let t be a positive integer. Then there exist $SAOD(2^t : 1, 2^t - 1; 2^t - 1)$ and strongly amicable Hadamard matrices for every 2^t.*

The following theorem, due to Paley [160], is quoted from Geramita and Seberry [80, Theorem 5.52]

Theorem 5.24. *Let $q \equiv 3 \pmod 4$ be a prime power. Then there exist strong $AOD(p+1; (1, p), (1, p))$.*

These are the required cores for the main result of Seberry [179].

Proposition 5.11 (Powers of Cores). *If there exist a strong $AOD(n : 1, n-1; 1, n-1)$ and a suitable amicabilizer then there exists a strong $AOD((n-1)^r + 1)$ for every odd integer $r > 0$.*

Proposition 5.12. *Using the circulant difference set $SBIBD(2^t - 1, 2^{t-1} - 1, 2^{t-2} - 1)$ to form the core of a strong $AOD(2^t : 1, 2^t - 1; 1, 2^t - 1)$ allows a more efficient construction for practical purposes.*

From Seberry and Yamada [188, p535], Geramita, Pullman and Seberry Wallis [79] and Seberry [180], strong amicable Hadamard matrices and strong amicable orthogonal designs $SAOD$ exist for the following orders:

Summary 5.1. $AOD(n:1,n-1;1,n-1)$, $SAOD$, (or $SAOD$) exist for orders:

Key	Order	Method
x_1	2^t	t a non-negative integer; Corollary 5.24.
x_2	p^r+1	$p^r \equiv 3 \pmod 4$ is a prime power; Theorem 5.24.
x_3	$(n-1)^r+1$	n is the order of $SAOD$ with suitable cores $r>0$ is any odd integer; Proposition 5.11.
x_4	nh	n,h, are the orders of $SAOD$s; Theorem 5.23.

The constraints on finding amicable orthogonal designs, even using the most promising candidates, that is those from skew-Hadamard matrices, makes the further construction of strong AOD most challenging.

5.13 Structure of Amicable Weighing Matrices

Lemmas 5.4 and 5.5 have already indicated that the amicability condition might force strong constraints on the structure of the component weighing matrices. In this section we study this idea a bit more.

A combinatorial argument lets us obtain the following result:

Theorem 5.25. *Let R be a monomial matrix of order $n=0 \pmod 4$. Let A be a symmetric weighing matrix of order n. Suppose $RA^\top = -AR^\top$. Then $A*R=0$ (and the Hadamard product). Further, if A has weight $n-1$, then R is symmetric if A has any diagonal element zero, and R is skew-symmetric otherwise.*

Theorem 5.26. *The existence of strong amicable orthogonal designs of order $n=0 \pmod 4$ and types $((1,n-1);(1,n-1))$ is equivalent to the existence of a symmetric weighing matrix of order n and weight $n-1$ with at least one zero on the diagonal.*

Proof. Let A be the symmetric weighing matrix. We use the theorem of Delsarte-Goethals-Seidel – Theorem 2.4 to see that we can find monomial matrices P and Q so that $B=PAQ$ is skew-symmetric. Let $R=P^{-1}Q^{-1}$. Then R is a monomial matrix, and $B^\top=(PAQ)^\top=-Q^\top AP^\top=Q^{-1}AP^{-1}=-PAQ$, so $RA^\top=-AR^\top$. Hence by the previous theorem, $A*R=0$, and R is symmetric. So $uR+vA$ and $xI+yAR$ are the required amicable orthogonal designs.

Now if $xU+yV$ and $uN+vM$ are $AOD(n:(1,n-1);(1,n-1))$, we pre- and post-multiply both matrices by monomial matrices P and Q, where $I=PUQ$. Then the amicable matrices can be written in the form $xI+yPVQ=xI+yS$ and $uPNQ+vPMQ=uR+vA$. Now the amicability and orthogonality gives us R and A are symmetric and $AR^\top=-RA^\top$. We now assume A has weight $n-1$ and no zero on the diagonal. Then considering the orthogonality

conditions on the rows of $A+R$ leads to a contradiction, and we have the result. □

Remark 5.6. We note that this proof also shows that the existence of a symmetric weighing matrix C of order n and weight $n-1$ with a zero on the diagonal is equivalent to the existence of a best pair of weights $(n-1,1)$ in order n. (See Definition 5.9)

We recall (Theorem 5.12) that $AOD(p+1:(1,p);(1,p))$ do exist when $p=3 \pmod 4$ is a prime power. Hence we have:

Corollary 5.25. *There is a symmetric weighing matrix with a zero on the diagonal of order $p+1$ and weight p where $p \equiv 3 \pmod 4$ is a prime power.*

We use Lemma 5.5 to show that symmetric weighing matrices of order n and weight $n-1$ with a zero on the diagonal do not always exist since:

5.14 A Generalization of Amicability – Families

In the algebraic theory for both orthogonal designs and amicable orthogonal designs, we were concerned with families whose members satisfied given conditions. In Lemma 5.1 we saw a useful family of weighing matrices. Product designs and repeat designs are further kinds of families. Furthermore, constructions such as 6.1 and 6.2 only become powerful if matrices such as the $\{M_1, M_2, N\}$ and $\{P_1, P_2, P_3, H\}$, respectively, mentioned there exist. We shall show later how the results of this section can be used in these constructions.

Let

$$K = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, L = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, M = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

We use $+$ for $+1$ and $-$ for -1. Also we use I for the identity matrix.

Definition 5.9. Matrices A, B which satisfy $AB^\top = BA^\top$ will be said to be *amicable*. A *best pair* is a pair of amicable weighing matrices (A,B) of weights i, j, respectively, satisfying

$$A^\top = -A, \quad B^\top = B, \quad AB^\top = BA^\top.$$

A *best pair family of order* n is a set of best pairs (A_i, B_j) of order n and weights i and j where

$$i = 1,2,3,\ldots,n-1, \quad j = 1,2,3,\ldots,n \quad \text{and}$$

$$A_i^\top = -A_i, \quad B_j^\top = B_j, \quad A_i B_j^\top = B_j A_i.$$

Theorem 5.27. *There is no best pair of weights* $(15,1)$ *in order* 16*. Equivalently, there is no symmetric weighing matrix of order* 16 *and weight* 15 *with a zero on the diagonal.*

Proof. The proof is long and combinatorial. It is given in detail in Robinson [166]. □

Definition 5.10. For convenience we will call a repeat design $(P;(R;S);H)$ of type $(1;(r;s);h)$ in order n a triplet when $P = I$. Alternatively, a triplet is three weighing matrices (R,S,H) of order n and weights (r,s,h), respectively, which are pairwise amicable; R,S are skew-symmetric, and H is symmetric.

We note that:

Lemma 5.12. *There are triplets in orders* $n = 2$ *and* 4 *for weights* (i,j,k) *where* $i,j = 1,2,\ldots,n-1$ *and* $k = 1,2,\ldots,n$*. Hence, there is a best pair family of orders* 2 *and* 4*.*

Proof. For order 2 consider the pairs (K,M) and (K,H). The required matrices for order 4 are (the weights are given in brackets):

1. $(1,2,1)$ $\{K\times I,\ K\times H;\ L\times I\}$,
2. $(1,2,2)$ $\{K\times I, K\times H;\ L\times H\}$,
3. $(1,2,3)$ $K\times I, K\times H;\ L\times H + M\times I$,
4. $(1,2,4)$ $\{K\times I, K\times H;\ H\times H\}$,
5. $(1,3,1)$ $\{K\times L, K\times I + H\times K;\ M\oplus -L\}$,
6. $(1,3,2)$ $\{K\times L, L\times I + H\times K;\ H\times L\}$,
7. $(1,3,3)$ $\{K\times L, K\times I + H\times K;\ M\oplus K + I\times M + K\times K\}$,
8. $(1,3,4)$ $\{K\times L, L\times I + H\times K;\ L\times I + M\times L + I\times M + K\times K\}$,
9. $(2,3,1)$ $\{I\times L + L\times M, L\times I + H\times L;\ L\oplus -M\}$,
10. $(2,3,2)$ $\{K\times H, L\times K + M\times K + K\times I;\ M\times I - L\times I\}$,
11. $(2,3,3)$ $\{I\times L + L\times M, L\times I + H\times L;\ M\oplus L + I\times M + L\times L\}$,
12. $(2,3,4)$ $\{I\times K + K\times M, K\times I + H\times K;$ $L\times I + M\times L + I\times M + K\times K\}$. □

Because of the extremely powerful constructions that arise from repeat designs, we wished to extend this lemma to higher powers of two. This effort led to the results that follow:

Construction 5.1. *If* A,B,C *is a triplet of weights* $(a,b,1)$ *in order* n*, then* (A,B,AC) *and* $(A,B,AC+C)$ *are triplets of weights* (a,b,a) *and* $(a,b,a+1)$*.*

Since by Theorem 5.15 there is no best pair of weights $(7,5)$ in order 8, we have, regarding a best pair (A,B) as a triplet (X,A,B):

Corollary 5.26. *There are no triplets of weight* $(x,7,5)$*,* $(4,7,1)$ *or* $(5,7,1)$ *in order* 8*.*

We are grateful to Amnon Neeman for the proof of another result using Lemma 5.5.

Theorem 5.28. *Let $n \equiv 0 \pmod 8$. Then it is not possible to have triplets of weights $(a, n-1, 1)$ in order n, where $a = n-4$, $n-3$, $n-2$, or of weights $(3,7,1)$ in order 8.*

Proof. Lemma 5.5 allows us to consider the triplet (X,Y,Z) where $Z = \frac{\oplus}{\frac{1}{2}n-1}\left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right] \oplus \left[\begin{smallmatrix}-1&0\\0&1\end{smallmatrix}\right]$. The result follows by a careful combinatorial argument. □

In fact, in order 8 we can say:

Lemma 5.13. *In order 8 all triplets (R,S,H) of weights (r,s,h), $0 \le r$, $s \le 7$, $0 \le k \le 8$, exist except*

(i) $(3,7,1)$, $(4,7,1)$, $(5,7,1)$, $(6,7,1)$ *and* $(r,7,5)$, $1 \le r \le 6$, *which do not exist, and possibly,*

(ii) $(5,7,2)$, $(6,7,2)$, $(6,7,4)$, $(3,7,3)$, $(4,7,3)$, $(5,6,3)$, $(5,7,3)$, $(6,7,3)$, $(1,5,7)$, $(3,5,7)$, $(3,7,7)$, $(4,7,7)$, $(5,7,7)$, $(6,7,7)$, *which are undecided.*

Proof. Part i) follows from the previous corollary and Theorem 5.28 which shows that $(3,7,1)$ and $(6,7,1)$ do not exist.

Lemma 6.9 parts i), iii), iv), v) and the above construction give all those that exist except $(3,5,1)$, $(3,5,5)$, $(1,5,1)$, $(1,7,1)$, $(2,7,1)$ and $(1,7,3)$. □

Now we note that a repeat design of type $(r;(p_1,\dots;q);w_1,\dots)$ in order n gives a repeat design of type $(r;(q;p_1,\dots,q);w_1,\dots)$ in order $2n$ by Lemma 6.9.

Hence the repeat design of type $(1;(2;3);1)$ in order 4 gives the $(1;(3;5);1)$ in order 8 and hence the triplet $(3,5,1)$ and by Construction 5.1 the $(3,5,5)$ in 8. We now give specific constructions for $(1,5,1)$, $(1,7,1)$, $(2,7,1)$ and $(1,7,3)$.

Let

$$S = \begin{bmatrix} 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1\\ -&0&0&0 \end{bmatrix}, R = \begin{bmatrix} 0&0&0&1\\ 0&0&1&0\\ 0&1&0&0\\ 1&0&0&0 \end{bmatrix}, R^2 = I$$

and K, L, M be as defined above. Write $E = -S + S^2 + S^3$ and $G = S + S^2 + S^3$. Then

$$(L \times S^2,\ I_2 \times (S + S^3) + K \times ER,\ L \times S^2)$$

and

$$(L \times S^2,\ L \times G + K \times (E+I)^\top R(S^3 + S - I)^\top R \oplus (-S^2 - S + I)^\top R)$$

are $(1,5,1)$ and $(1,7,3)$, respectively. Amnon Neeman found the following $(1,7,1)$:

$$\left[\begin{array}{cccc|cccc} 0 & 1 & & & & & & \\ - & 0 & & & & & & \\ & & 0 & 1 & & & & \\ & & - & 0 & & & & \\ \hline & & & & 0 & 1 & & \\ & & & & - & 0 & & \\ & & & & & & 0 & 1 \\ & & & & & & - & 0 \end{array}\right], \quad \left[\begin{array}{cccc|cccc} 0 & 1 & 1 & - & - & 1 & 1 & 1 \\ - & 0 & 1 & 1 & - & - & - & 1 \\ - & - & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & - & - & 0 & - & 1 & - & 1 \\ \hline 1 & 1 & - & 1 & 0 & - & 1 & 1 \\ - & 1 & - & - & 1 & 0 & - & 1 \\ - & 1 & - & 1 & - & 1 & 0 & - \\ - & - & - & - & - & - & 1 & 0 \end{array}\right],$$

$$\left[\begin{array}{cccc|cccc} 0 & 0 & 0 & 1 & & & & \\ 0 & 0 & 1 & 0 & & & & \\ 0 & 1 & 0 & 0 & & & & \\ 1 & 0 & 0 & 0 & & & & \\ \hline & & & & 0 & 1 & 0 & 0 \\ & & & & 1 & 0 & 0 & 0 \\ & & & & 0 & 0 & 1 & 0 \\ & & & & 0 & 0 & 0 & 0 \end{array}\right].$$

The following three matrices give a $(2,7,1)$:

$$\left[\begin{array}{cccc|cccc} 0 & 1 & 1 & 0 & & & & \\ - & 0 & 0 & - & & & & \\ - & 0 & 0 & 1 & & & & \\ 0 & 1 & - & 0 & & & & \\ \hline & & & & 0 & 0 & 1 & 1 \\ & & & & 0 & 0 & 1 & - \\ & & & & - & - & 0 & 0 \\ & & & & - & 1 & 0 & 0 \end{array}\right], \quad \left[\begin{array}{cccc|cccc} 0 & 1 & 1 & - & 1 & - & - & 1 \\ - & 0 & 1 & - & - & 1 & 1 & 1 \\ - & - & 0 & 1 & 1 & 1 & - & 1 \\ 1 & 1 & - & 0 & 1 & 1 & 1 & 1 \\ \hline - & 1 & - & - & 0 & 1 & - & - \\ 1 & - & - & - & - & 0 & - & 1 \\ 1 & - & 1 & - & 1 & 1 & 0 & - \\ - & - & - & - & 1 & - & 1 & 0 \end{array}\right], v$$

$$\left[\begin{array}{cccc|cccc} 0 & 1 & 0 & 0 & & & & \\ 1 & 0 & 0 & 0 & & & & \\ 0 & 0 & 0 & 1 & & & & \\ 0 & 0 & 1 & 0 & & & & \\ \hline & & & & 0 & - & 0 & 0 \\ & & & & - & 0 & 0 & 0 \\ & & & & 0 & 0 & 1 & 0 \\ & & & & 0 & 0 & 0 & - \end{array}\right].$$

This gives the results of the enunciation after using Construction 5.1 to obtain $(1,5,5)$, $(1,7,7)$ and $(2,7,7)$.

Remark 5.7. This lemma indicates that the existence problem for triplets (R,S,H) which are repeat designs $(I;(R;S);H)$ is very difficult and far from resolved.

But this lemma does allow us to say:

Corollary 5.27. *There are best pairs for all* (a,b), $0 \le a \le 7$, $0 \le b \le 8$, *in order* 8 *except* $(7,5)$. *There are amicable weighing matrices for all* (a,b), $0 \le a$, $b \le 8$, *in order* 8.

The results on repeat designs §5.10 allow us to say:

Theorem 5.29. *There are amicable weighing matrices for all* (a,b), $0 \le a$, $b \le 2^t$, *in order* 2^t. *Now Lemma 5.8, together with the results quoted above, let us say:*

Lemma 5.14. *In order* 16 *there exist best pairs* (a,b) *(= repeat designs* $(1;(a);b)$*) for all* $a = 1,2,\ldots,15$ *and* $b = 1,2,\ldots,16$ *except possibly the pairs* (a,b)*:* $(13,1)$, $(13,5)$, $(13,9)$, $(15,7)$, $(15,9)$, $(15,15)$, *which are undecided, and* $(15,1)$, *which does not exist.*

Now, as promised, we apply these results to Constructions 6.1 and 6.2 to obtain:

Construction 5.2. *Suppose there is a triplet of weights* (a,b,c) *in order* n. *Then there is an orthogonal design of type*

(i) $OD(2n;(1,1,a,b))$

and when $c = 1$, *of types,*

(ii) $OD(4n;(1,1,1,a,a,a,c))$, $\quad OD(4n\colon (1,1,1,a,a,b,c))$.

Construction 5.3. *Suppose there is a best pair of weights* (a,b) *in order* n. *Further suppose there is a product design of type* $(a_1,\ldots,a_p;\ b_1,\ldots,b_q;\ c_1,\ldots,c_r)$ *in order* m. *Then there is an* $OD(mn;(a_1,\ldots,a_p,\ ab_1,\ldots,ab_q,\ bc_1,\ldots,bc_r))$. *See Chapter 6 for more details.*

Example 5.14. There is a product design of type $(1,1,1,1,2,4,\ldots,2^{t-4};\ 2,2^{t-3};\ 2,4,\ldots,2^{t-4},2^{t-3},2^{t-3})$ in order 2^t. So using a best pair of weights (a,b) in order n gives an $OD(2^tn;(1,1,1,1,2,4,\ldots,2^{t-4},\ 2a,2^{t-3}a,\ 2b,4b,\ldots,\ 2^{t-4}b,\ 2^{t-3}b,2^{t-3}b))$.

5.15 Repeat and Product Design Families

Just as the delightful discovery of amicable orthogonal designs led to both beautiful constructions and algebraic depth associated with quadratic forms, we will see in Chapter 6 that powerful repeat and product designs lead to wonderful results building on the basis of amicable orthogonal designs.

We see

$$\{OD,\ AOD,\ POD\} \subset \{\text{Repeat Design Families}\}.$$

Chapter 6
Gastineau-Hills Schemes: Product Designs and Repeat Designs

6.1 Generalizing Amicable Orthogonal Designs

We started our study of orthogonal designs by constructing some and then analyzing their structure using well known theorems on Clifford algebras and far-reaching theorems of Hurwitz and Radon.

We noted the use of amicable Hadamard matrices in the construction of Hadamard matrices and saw that amicable orthogonal designs arose in a natural way in the construction of orthogonal designs hinting that they are simple cases of a far deeper concept. So in Chapter 4 we turned to study the structure and existence theory of amicable orthogonal designs. In Chapter 5 we explored the construction of amicable orthogonal designs.

Chapter 3 showed us that a knowledge of existence of orthogonal designs in orders which are powers of two was necessary for the solution for the algebraic problem. Then in Chapter 5 we saw that knowledge of existence of amicable designs in powers of two was crucial to the algebraic theory.

Some results in the original paper [83] of Geramita and Seberry then hinted that the existence of new kinds of designs and algebras would prove invaluable in the construction of powers of two greater than five. Powers of two up to four were amenable to extremely clever computer searches but higher power were computationally infeasible.

This chapter further studies higher powers re-affirming the powerful contributions of Peter J. Robinson in his PhD thesis which exploited the unnamed construction of Geramita and Seberry which came to be called product designs and repeat designs.

This work of Robinson hinted that there might be deeper designs and structures which used product designs and repeat designs as examples of their algebraic fundamentals.

Thus we have the work of Humphrey Gastineau-Hills [63] whose brilliant construction and insights have led to a new algebra, the Clifford-Gastineau-Hills algebra completely resolving the algebraic existence for product designs,

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5_6

which are a special case of repeat designs. Sections 6.4 and later are devoted to this beautiful theory.

6.1.1 Product Designs

Geramita and Seberry Wallis [83] gave a number of interesting matrices in their journey to construct orthogonal designs. We repeat here some of these constructions in order to try to elicit the underlying structure. We have changed variable names and the wording of theorems to further the journey.

In an early construction they give:

Theorem 6.1 (Geramita-Seberry [83]). *Suppose S, R, P are $\{0, 1, -1\}$ matrices where*

(i) $R * P = 0$;
(ii) $R + P$ is an orthogonal design $OD(n; p_1, p_2)$;
(iii) S and $x_1R + x_2P$ are amicable $AOD(n; (s_1, \ldots, s_t), (p_1, p_2))$.

Then the matrix Q is an $OD(4n; s_1, \ldots, s_t, p_1, p_1, p_1, p_z, p_2, p_2)$.

$$Q = \begin{bmatrix} y_1R + z_1P & y_2R + z_2P & xS & y_3R + z_3P \\ -y_2R + z_2P & y_1R - z_1P & -y_3R - z_3P & xS \\ -xS & y_3R - z_3P & y_1R + z_1P & -y_2R + z_2P \\ -y_3R + z_3P & -xS & y_2R + z_2P & y_1R - z_1P \end{bmatrix} \tag{6.1}$$

We note that the above matrix can be written in the form

$$M_1 \times R + M_2 \times P + N \times S,$$

where M_1, M_2 and N are the 4×4 matrices of the coefficients of R, P and S, respectively. In the next subsection we use X for R, Y for P and Z for S.

$[M_1, M_2, N]$ are sometimes written , to save space, in superimposed notation

$$\begin{bmatrix} y_1z_1 & y_2z_2 & x & y_3z_3 \\ \bar{y}_2z_2 & y_1\bar{z}_1 & \bar{y}_3\bar{z}_3 & x \\ \bar{x} & y_3\bar{z}_3 & y_1z_1 & \bar{y}_2z_2 \\ \bar{y}_3z_3 & \bar{x} & y_2z_2 & y_1\bar{z}_1 \end{bmatrix}$$

In [83] a variation of the matrix in equation 6.1 was introduced:

Theorem 6.2 (Geramita-Seberry [83]). *Suppose R is the identity matrix and P_1, P_2, P_3 are skew-symmetric $\{0, 1, -1\}$ matrices of order n where*

(i) $R * P_i = 0$, $i = 1,2,3$;
(ii) $R + P_i$ *are orthogonal designs* $OD(n;1,p_{i1},p_{i2},\ldots)$, $i = 1,2,3$;
(iii) H *is an* $OD(n;h_1,h_2,\ldots)$;
(iv) $P_iP_j^\top = P_jP_i^\top$, P_i,P_j *are amicable* $OD(n;(p_{i1},p_{i2},p_{i3},\ldots);(p_{j1},p_{j2},\ldots))$, $i = 1,2,3$;
(v) $P_kH^\top = HP_k^\top$ *are amicable* $AOD(n;(p_{k1},\ldots);(h_1,h_2,\ldots))$

Then the matrix Q *is an* $OD(4n;r_1,r_2,\ldots,p_{11},p_{12},\ldots,r_1,r_2,\ldots,p_{21},p_{22},\ldots,r_1,r_2,\ldots,p_{31},p_{32},\ldots,h_1,h_2$.

Then

$$\begin{bmatrix} x_1R+P_1 & x_3R+P_2 & x_5R+P_3 & H \\ -x_3R+P_2 & x_1R-P_1 & H & -x_5R-P_3 \\ -x_5R+P_3 & -H & x_1R-P_1 & x_3R+P_2 \\ -H & x_5R-P_3 & -x_3R+P_2 & x_1R+P_1 \end{bmatrix}$$

is an $OD(4n;(1,p_{11},p_{12},\ldots,1,\ p_{21},p_{22},\ldots,1,\ p_{31},p_{32},\ldots,h_1,h_2,\ldots))$.

These conditions seem to be inconceivably onerous but Geramita and Seberry [80] and Peter Robinson [166] showed that they can be satisfied many times. We are interested in generalizing this idea. With this in mind, we give the following definition.

Definition 6.1. Let M_1, M_2 and N be $OD(n;a_1,\ldots,a_r)$, $OD(n;b_1,\ldots,b_s)$ and $OD(n;c_1,\ldots,c_t)$, respectively. Then $(M_1\,;M_2\,;N)$ are *product designs* of order n and types $(a_1,\ldots,a_r;\ b_1,\ldots,b_s;\ c_1,\ldots,c_t)$ if

(i) $M_1 * N = M_2 * N = 0$ (Hadamard product),
(ii) $M_1 + N$ and $M_2 + N$ are orthogonal designs, and
(iii) $M_1M_2^\top = M_2M_1^\top$ (i.e., M_1 and M_2 are amicable orthogonal designs).

Example 6.1. Theorem 6.1 produces product designs of order 4 and types $POD(4:1,1,1;1,1,1;1)$.

We also note:

Example 6.2. Table 6.1 gives product designs $POD(8;1,1,1;1,1,1;5)$.

Example 6.3. Table 6.2 gives product designs $POD(12;1,1,1;1,1,1;9)$.

6.1.2 Constructing Product Designs

The next theorem gives us a way of obtaining product designs from product designs of smaller orders.

Theorem 6.3 (P. J. Robinson). *Let* $(M_1;y_1M_3+y_2M_4;N)$ *be product designs* $POD(n;a_1,\ldots,a_r;b_1,b_2;c_1,\ldots,c_t)$, *and let* S *and* x_1R+x_2P *be* $AOD(m;(u),(v,w))$. *Then*

Table 6.1 Product Design: $POD(8;1,1,1;1,1,1;5)$

$$\left[\begin{array}{cccccccc}
x_1 & x_2 & z & x_3 & z & z & z & \bar{z} \\
\bar{x}_2 & x_1 & \bar{x}_3 & z & z & \bar{z} & z & z \\
\bar{z} & x_3 & x_1 & \bar{x}_2 & z & \bar{z} & \bar{z} & \bar{z} \\
\bar{x}_3 & \bar{z} & x_2 & x_1 & z & z & \bar{z} & z \\
\bar{z} & \bar{z} & \bar{z} & \bar{z} & x_1 & x_2 & z & \bar{x}_3 \\
\bar{z} & z & z & \bar{z} & x_2 & x_2 & x_3 & z \\
\bar{z} & \bar{z} & z & z & \bar{z} & \bar{x}_3 & x_1 & \bar{x}_2 \\
z & \bar{z} & z & \bar{z} & x_3 & \bar{z} & x_2 & x_1
\end{array}\right]
\left[\begin{array}{cccccccc}
y_1 & y_2 & 0 & y_3 & & & & \\
y_2 & \bar{y}_1 & \bar{y}_3 & 0 & & 0 & & \\
0 & \bar{y}_3 & y_1 & y_2 & & & & \\
y_3 & 0 & y_2 & \bar{y}_1 & & & & \\
& & & & y_2 & y_3 & 0 & \bar{y}_1 \\
& & & & y_3 & \bar{y}_2 & y_1 & 0 \\
& 0 & & & 0 & y_1 & y_2 & y_3 \\
& & & & \bar{y}_1 & 0 & y_3 & \bar{y}_2
\end{array}\right]$$

(where $\bar{x} = -x$)

Table 6.2 Product Design: $POD(12;1,1,1;1,1,1;9)$

$$\left[\begin{array}{cccccccccccc}
x_1 & x_2 & x_3 & \bar{z} & z & z & z & \bar{z} & z & \bar{z} & z & \bar{z} \\
\bar{x}_2 & x_1 & \bar{z} & \bar{x}_3 & z & \bar{z} & \bar{z} & \bar{z} & \bar{z} & \bar{z} & \bar{z} & \bar{z} \\
\bar{x}_3 & z & x_1 & x_2 & z & z & \bar{z} & z & z & z & \bar{z} & \bar{z} \\
z & x_3 & \bar{x}_2 & x_1 & z & \bar{z} & z & z & z & \bar{z} & \bar{z} & z \\
\bar{z} & \bar{z} & \bar{z} & \bar{z} & x_1 & x_2 & x_3 & \bar{z} & z & z & \bar{z} & z \\
\bar{z} & z & \bar{z} & z & \bar{x}_2 & x_1 & \bar{z} & \bar{x}_3 & z & \bar{z} & z & z \\
\bar{z} & z & z & \bar{z} & \bar{x}_3 & z & x_1 & x_2 & \bar{z} & \bar{z} & \bar{z} & z \\
z & z & \bar{z} & \bar{z} & z & x_3 & \bar{x}_2 & x_1 & \bar{z} & z & z & z \\
\bar{z} & z & \bar{z} & \bar{z} & \bar{z} & \bar{z} & z & z & x_1 & x_2 & x_3 & \bar{z} \\
z & z & \bar{z} & z & \bar{z} & z & z & \bar{z} & \bar{x}_2 & x_1 & \bar{z} & \bar{x}_3 \\
\bar{z} & z & z & z & z & \bar{z} & z & \bar{z} & \bar{x}_3 & z & x_1 & x_2 \\
z & z & z & \bar{z} & \bar{z} & \bar{z} & \bar{z} & \bar{z} & z & x_3 & \bar{x}_2 & x_1
\end{array}\right]$$

$$\left[\begin{array}{cccccccccccc}
y_1 & y_2 & y_3 & 0 & & & & & & & & \\
y_2 & \bar{y}_1 & 0 & \bar{y}_3 & & 0 & & & & 0 & & \\
y_3 & 0 & \bar{y}_1 & y_2 & & & & & & & & \\
0 & \bar{y}_3 & y_2 & y_1 & & & & & & & & \\
& & & & y_2 & y_3 & y_1 & 0 & & & & \\
& & 0 & & y_3 & \bar{y}_2 & 0 & \bar{y}_1 & & & 0 & \\
& & & & y_1 & 0 & \bar{y}_2 & y_3 & & & & \\
& & & & 0 & \bar{y}_1 & y_3 & y_2 & & & & \\
& & & & & & & & y_3 & \bar{y}_1 & \bar{y}_2 & 0 \\
& & 0 & & & & 0 & & \bar{y}_1 & \bar{y}_3 & 0 & y_2 \\
& & & & & & & & \bar{y}_2 & 0 & \bar{y}_3 & \bar{y}_1 \\
& & & & & & & & 0 & y_2 & \bar{y}_1 & y_3
\end{array}\right]$$

$$(x_1P \times M_3 + R \times M_1; y_1S \times M_3 + y_2R \times M_4; z_1P \times M_4 + S \times N)$$

are product designs of order mn and types

$$(wb_1, va_1, \ldots, va_r; ub_1, vb_2; wb_2, uc_1, \ldots, uc_t).$$

Proof. By straightforward verification. □

A very useful form of this theorem is using $AOD(2;(1,1),(2))$ (see Section 5.1). We state this particular case in the following corollary.

Corollary 6.1. *Let* $(M_1; y_1M_3 + y_2M_4; N)$ *be product designs* $POD(n : a_1, \ldots, a_r; b_1, b_2; c_1, \ldots, c_t)$. *Then there are product designs* $POD(2n: b_1, a_1, \ldots, a_r; 2b_1, b_2; b_2, 2c_1, \ldots, 2c_t)$.

In Theorem 6.3 and Corollary 6.1 we may have M_3 or M_4 equal to zero. In this case, however, the next theorem gives a better result.

Theorem 6.4 (P.J. Robinson). *If* $(M_1; M_2; N)$ *are product designs* $POD(n; a_1, \ldots, a_r; b; c_1, \ldots, c_t)$ *and if* S *and* $y_1R + x_2P$ *are amicable orthogonal designs* $AOD(m; (u_1, \ldots, u_j), (v, w_1, \ldots, w_k))$, *then there are product designs of order mn and the following types:*

(i) $(va_1, \ldots, va_r; vb; cu_1, \ldots, cu_j, bw_1, \ldots, bw_k)$ *and*
(ii) $(va_1, \ldots, va_r; vb; uc_1, \ldots, uc_t, bw_1, \ldots, bw_k)$,

where u and c are the sums of the u_i*'s and* c_i*'s, respectively.*

Proof. We consider

$$(R \times M_1; R \times M_2; S \times N + P \times M_2),$$

with the appropriate variables equated. □

The next result gives us a way of obtaining product designs from amicable orthogonal designs.

Theorem 6.5. *If* S *and* $y_1R + y_2P$ *are* $AOD(n; (u_1, \ldots, u_j), (v, w))$ *then*

$$\left(\begin{bmatrix} zS & x_1R \\ x_{1R} & S \end{bmatrix}; \quad \begin{bmatrix} y_1R + y_3P & y_2R \\ y_2R & -y_1R + y_3P \end{bmatrix}; \quad \begin{bmatrix} 0 & P \\ -P & 0 \end{bmatrix} \right)$$

are product designs of order $2n$ *and types*

$$(v, u_1, \ldots, u_j; v, v, w; w).$$

Proof. By straightforward verification. □

In the following Lemma we give examples of product designs which will be used later to produce a very useful orthogonal design.

Lemma 6.1 (P.J. Robinson). *There are product designs of order* $2^t, t \geq 4$, *and types*

$$(1,1,1,1,2,4,\ldots,2^{t-3};2,2^{t-3};2,4,\ldots,2^{t-3},2^{t-2},2^{t-2}).$$

Proof. The product designs $POD(4\colon 1,1,1;\ 1,2;\ 1)$ produce product designs $POD(8\colon 1,1,1,1;\ 2,2;\ 2,2)$ (Corollary 6.1). This design in turn produces product designs $POD(16\colon 1,1,1,1,2;\ 2,4;\ 2,4,4)$.

By repeated use of Corollary 6.1 we obtain the required result. □

Table 6.3 lists product designs of orders 4 and 8 which are obtained by using the results given here.

Table 6.3 Product designs of order 4 and 8

Product Designs	**Construction**	
Order 4		
$(1,1,1;1,1,1;1)$	Example 6.1	
Order 8		
$(1,1,1,2;1,1,3;3)$	$((1,1,2);(1,3))$	$((1,1);(1,1))$
$(1,1,2,3;1,3,3;1)$	$((1,1,2);(3,1))$	$((1,1);(1,1))$
$(1,1,2,2;2,2,2;2)$	$((1,1,2);(2,2))$	$((1,1);(1,1))$
$(1,1,1,1;2,2;2,2)$	$(1,1,1;1,2;1)$	
$(1,1,1,2;1,4;1,2)$	$(1,1,1;2,1,1)$	
$(1,1,1;1,1,1;5)$	Example 6.3	

6.2 Constructing Orthogonal Designs from Product Designs

We now produce a generalization of Theorem 6.1.

Theorem 6.6 (P.J. Robinson). *Let* S *and* y_1R+P *be* $AOD(m;(u_1,\ldots,u_j),(v,w_1,\ldots,w_k))$, *and let* $(M_1;M_2;N)$ *be product designs* $POD(n\colon a_1,\ldots,a_r;\ b_1\ldots,b_s;\ c_1\ldots,c_t)$. *Then there exist orthogonal designs*

(i) $OD(mn;(va_1,\ldots,va_r,wb_1,\ldots,wb_s,uc_1,\ldots,uc_t))$,
(ii) $OD(mn;(va_1,\ldots,va_r,wb_1,\ldots,wb_s,u_1c,\ldots,u_jc))$,
(iii) $OD(mn;(va_1,\ldots,va_r,w_1b,\ldots,w_kb,uc_1,\ldots,uc_t))$,
(iv) $OD(mn;(va_1,\ldots,va_r,w_1b,\ldots,w_kb,u_1c,\ldots,u_jc)$.

where b, c, u *and* w *are the sums of the* b_i*'s,* c_i*'s,* u_i*'s and* w_i*'s, respectively.*

Proof. We consider

$$M_1 \times R + M_2 \times P + N \times S,$$

with the appropriate variables equated. □

As an example of the use of this theorem, we give the following lemma.

Lemma 6.2 (P.J. Robinson). *There is an* $OD(2t;(1,1,1,1,2,2,4,4,\ldots,2^{t-2},2^{t-2}))$, $t \geq 2$.

Proof. If $t \geq 5$, we apply the above theorem with the product designs of order 2^{t-1} and types $(1,1,1,1,2,4,\ldots,2^{t-4};\ 2,2^{t-3};\ 2,4,...,2^{t-4},2^{t-3},2^{t-3})$ (Lemma 6.1) and $AOD(2;(1,1),(2))$. □

The $OD(16;(1,1,1,1,2,2,4,4))$ may be obtained in a similar manner by using the product designs $POD(8\colon 1,1,1,1;\ 2,2;\ 2,2)$ (see proof of Lemma 6.1).

The design of order 4 and type $(1,1,1,1)$ is given in Section 4.1, and the design of type $(1,1,1,1,2,2)$ is obtained from $OD(8;(1,1,1,1,1,1,1,1))$ (see §4.1).

We note that the above orthogonal designs have $2t$ variables. If $t = 4k+1$, $\rho(2^t) = 8k+2 = 2t$, and if $t = 4k+2$, $\rho(2^t) = 8k+4 = 2t$. Therefore, if $t = 4k+1$ or $4k+2$, the above design has the maximum number of variables allowed. We also note that the above design is full. That is, the design contains no zeros.

By equating variables in the above design, we obtain:

Corollary 6.2 (P.J. Robinson). *All orthogonal designs of type* $(1,1,a,b,c)$, $a+b+c = 2^t-2$, *exist in order* 2^t, $t \geq 3$.

Proof. Noting that any number $< 2^{t-1}-1$ can be formed from $1,2,4,\ldots,2^{t-2}$, we have the result. □

In Appendix F we give the types of some orthogonal designs in order 32 obtained from product designs and by doubling orthogonal designs in order 16. We further illustrate Theorem 6.6 by obtaining designs in order 16.

Corollary 6.3 (Geramita-Wallis). *Suppose there exist* $AOD(n:(u_1,\ldots,u_p);(v_1,\ldots,v_q))$. *Then, since there are product designs of type* $(1,1,1;1,1,1;1)$ *in order* 4, *there exist orthogonal designs of type*

(i) $OD(4n;(u_1,u_1,u_1,3u_2,\ldots,3u_p,v_1,\ldots,v_q))$ *and*
(ii) $OD(4n;(u_1,u_1,u_1,w,w,w,v_1,\ldots,v_q))$.

where $w = u_2+u_3+\cdots+u_p$.

Example 6.4. There exist orthogonal designs of types

(a) $OD(16;(1,1,1,1,1,1,1,1,2))$,
(b) $OD(16;(1,1,1,1,1,2,2,2,2))$,

(c) $OD(16;(1,1,1,1,1,2,3,3,3))$,
(d) $OD(16;(1,1,2,2,2,2,2,2,2))$,
(e) $OD(16;(1,1,2,2,2,2,3,3))$

Proof. Use $AOD(4;(1,1),(1,1,2))$, $AOD(4;(1,2),(1,1,2))$, $AOD(4;(1,1,2),(1,1,2))$ and $AOD(4;(2,2),(1,1,2))$ in Corollary 6.3 part (ii) to obtain a), b), c) and d). For e) we use $AOD(4;(2,1,1),(1,1,2))$ in 6.3 part (i). □

Remark 6.1. More recent notation of Kharaghani [120] would write these designs

$$OD(16;1_8,2)\ OD(16;1_5,2_4)\ \ OD(16;1_5,2,3_3)$$
$$OD(16;1_2,2_7)\ OD(16;1_2,2_4,3_2)$$

We now give two results to show how product designs may be used to obtain orthogonal designs in orders other than powers of 2.

Lemma 6.3 (P.J. Robinson). *There are product designs of order* 12 *and types*

$$POD(12;1,1,1;1,1,4;4),\ POD(12;1,1,4;1,1,1;1),$$
$$POD(12;1,1,4;1,4,4;1),\ POD(12;1,1,4;1,1,4;4),$$
$$POD(12;1,4,4;1,4,4;1),\ POD(12;1,1,1;1,1,1;9).$$

Proof. Wolfe [247] gives $AOD(6;(1,1),(1,4))$ and $AOD(6;(1,4),(1,4))$. By using these designs in Theorem 6.5, we obtain the first five designs. The last is given in Example 6.3. □

By using Theorem 6.6 with the above designs, we obtain:

Corollary 6.4 (P.J. Robinson). *There are orthogonal designs*

$$OD(24;(1,1,1,1,1,1,9,9)),\qquad OD(24;(1,1,1,1,4,4,4,4)),$$
$$OD(24;(1,1,1,1,1,4,4,4)),\qquad OD(24;(1,1,1,1,1,1,1,4)).$$

(That is $OD(24;1_6,9_2)$, $OD(24;1_5,4_3)$, $OD(24;1_4,4_4)$, $OD(24;1_7,4)$.)

By using Lemma 6.3 and Corollary 6.4 we obtain:

Lemma 6.4 (P.J. Robinson). *There are product designs*

$$POD(12;1,1,1;1,1,4;4),\ POD(12;1,1,4;1,4,4;1),$$
$$POD(12;1,1,4;1,1,4;4),\ POD(12;1,4,4;1,4,4;1),$$
$$POD(12;1,1,4;1,1,1;1),\ POD(12;1,1,1;1,1,1;9).$$

Lemma 6.5. *There are orthogonal designs of order 24 and types:*

$$OD(24;1,1,1,1,1,1,9,9),\ OD(24;1,1,1,1,4,4,4,4),$$
$$OD(24;1,1,1,1,1,4,4,4),\ OD(24;1,1,1,1,1,1,1,4).$$

We note

Lemma 6.6 (Ghaderpour [84]). *There is no* $POD(n;1,1,1;1,1,1;n-3)$ *for* $n \neq 4,8,12$.

6.2.1 Applications

By equating variables in the orthogonal designs given in Appendix D, we obtain the following lemmas.

Lemma 6.7 (P.J. Robinson). *All 6-tuples of the form* $(a,b,c,d,e,32-a-b-c-d-e)$, $0 < a+b+c+d+e < 32$, *are the types of orthogonal designs in order 32.*

Corollary 6.5. *All n-tuples,* $n = 1,2,3,4$, *are the types of orthogonal designs in order 32.*

6.3 Using Families of Matrices – Repeat Designs

Repeat designs introduced by Geramita and Seberry [80] were first named repeat designs in Robinson's PhD Thesis [166]. The motivation for the constructions of this chapter arises from the following observations:

Construction 6.1. *Suppose* $(M_1;M_2;N)$ *is a product design of type* $(u_1,u_2,\ldots;v_1,v_2;\ldots;w)$ *and order n. Then, with* x_1, x_2 *commuting variables.*

$$\begin{bmatrix} M_1+x_1N & M_2+x_2N \\ M_2-x_2N & -M_1+x_1N \end{bmatrix}$$

is $OD(2n;(w,w,u_1,u_2,\ldots,v_1,v_2,\ldots))$.

(This construction will be discussed further in Section 6.4)

Construction 6.2 (Geramita-Wallis [83]). *Let* Y_1, Y_2, Y_3 *be skew-symmetric orthogonal designs of types* $(p_{i1},p_{i2},\ldots)$, $i = 1,2,3$ *in order n, and Z a symmetric* $OD(n: h_1,h_2,\ldots)$. *Further, suppose* $Y_iY_j^\top = Y_jY_i^\top$ *and* $Y_kZ^\top = ZY_k^\top$. *Then*

$$\begin{bmatrix} x_1I_n+Y_1 & x_3I_n+Y_2 & x_5I_n+Y_3 & Z \\ -x_3I_n+Y_2 & x_1I_n-Y_1 & Z & -x_5I_n-Y_3 \\ -x_5I_n+Y_3 & -Z & x_1I_n-Y_1 & x_3I_n+Y_2 \\ -Z & x_5I_n-Y_3 & -x_3I_n+Y_2 & x_1I_n+Y_1 \end{bmatrix}$$

is an $OD(4n;(1,p_{11},p_{12},\ldots,1,\ p_{21},p_{22},\ldots,1,\ p_{31},p_{32},\ldots,h_1,h_2,\ldots))$.

Proof. By straightforward verification. □

To generalize this design, we introduce the following definition:

Definition 6.2. Let $X,Y_1,Y_2,\ldots,Z$ be orthogonal designs $OD(n;(r_1,r_2,\ldots),\ (p_{i1},p_{i2},\ldots))$, $i = 1,2,\ldots,(h_1,h_2,\ldots)$, respectively.
Then $(X: (Y_1;Y_2;\ldots);Z)$ are *repeat orthogonal designs*, *ROD*, of order n and types $(r_1,r_2,\ldots)$; $(p_{11},p_{12},\ldots;\ p_{21},p_{22},\ldots;\ \ldots)$; $(h_1,h_2,\ldots)$ if

(i) $X * Y_i = 0,\ i = 1,2,\ldots,$
(ii) $X + Y_i,\ i = 1,2,\ldots,$ are orthogonal designs,
(iii) $X + Y_i$ and $Z,\ i = 1,2,\ldots,$ are amicable orthogonal designs,
(iv) $Y_i Y_j^\top = Y_j Y_i^\top,\ i \neq j.$

Then we have

Construction 6.3. *Let* $(L; M_1 + M_2 + \cdots + M_s; N)$ *be product designs* $POD(n : a_1,\ldots,a_p;\ b_{11},\ldots,b_{1_{q_1}},\ b_{21},\ldots,\ b_{2_{q_2}},\ldots,\ b_{s1},\ldots,\ b_{sq_s};\ c_1,\ldots,c_t)$, *where* M_i *is of type* $(b_{i1},\ldots,b_{iqi})$.

Further, let $(X; (Y_1; Y_2; \ldots; Y_u); Z)$ *be repeat orthogonal designs,* $ROD(m : (r_1,\ldots,r_w);\ (p_{11},\ldots,p_{1_{v_1}};\ p_{21},\ldots,p_{2_{v_2}};\ p_{u1},\ldots,p_{uv_u});\ h_1,\ldots,h_x)$. *Then*

$$L \times X + M_1 \times Y_{j1} + \cdots + M_k \times P_{jk} + N \times Z$$

is an orthogonal design of order mn *and type* 1 *of*

(i) $(a_1 r,\ldots,a_p r,\ b_1 p_{11},\ldots,\ b_1 p_{1_{v_1}},\ldots,\ b_s p_{s1},\ldots,\ b_s p_{sq_s},\ ch_1,\ldots,ch_x)$,
(ii) $(a_1 r,\ldots,a_p r,\ b_1 p_{11},\ldots,\ b_1 p_{1_{v_1}},\ldots,\ b_s p_{s1},\ldots,\ b_s p_{sq_s},\ c_1 h,\ldots,c_t h)$,
(iii) $(ar_1,\ldots,ar_w,\ b_1 p_{11},\ldots,\ b_1 p_{1_{v_1}},\ldots,\ b_s p_{s1},\ldots,\ b_s p_{sq_s},\ ch_1,\ldots,ch_x)$,
(iv) $(ar_1,\ldots,ar_w,\ b_1 p_{11},\ldots,\ b_1 p_{1_{v_1}},\ldots,\ b_s p_{s1},\ldots,\ b_s p_{sq_s},\ c_1 h,\ldots,c_t h)$.

where a, c, r, h *are the sum of some or all of the* a_i, c_i, r_i, h_i, *respectively, and* $b_i = b_{i1} + \cdots + b_{iq_i}$.

This construction is at first sight quite formidable, but as we shall see, it does lead to new orthogonal designs.

We have previously mentioned product designs, so we need to find some repeat designs to see if any new orthogonal designs can be obtained. First we see that they do lead to new designs:

Example 6.5. There are repeat designs $ROD(4 : (1; (1;3); 1,3))$, $ROD(4 : (1; (2;3); 1,3))$, $ROD(4 : (1; (1;2); 1,1,2))$, and $ROD(4 : (1; (2;1,2); 1,2))$. They are $(I; (T_1; T_4); T_0)$, $(I; (T_3; T_4); T_0)$, $(I; (T_1; T_3); T_3)$, and $(I; (T_2; T_6); T_7)$, where

$$T_0 = \begin{bmatrix} x & y & y & y \\ y & -x & y & y \\ y & -y & y & -x \\ y & y & -x & -y \end{bmatrix}, \quad T_1 = \begin{bmatrix} 0 & + & 0 & 0 \\ - & 0 & 0 & 0 \\ 0 & 0 & 0 & - \\ 0 & 0 & + & 0 \end{bmatrix},$$

$$T_2 = \begin{bmatrix} 0 & 0 & + & + \\ 0 & 0 & + & - \\ - & - & 0 & 0 \\ - & + & 0 & 0 \end{bmatrix}, \qquad T_3 = \begin{bmatrix} 0 & 0 & + & + \\ 0 & 0 & - & + \\ - & + & 0 & 0 \\ - & - & 0 & 0 \end{bmatrix},$$

$$T_4 = \begin{bmatrix} 0 & + & + & + \\ - & 0 & + & - \\ - & - & 0 & + \\ - & + & - & 0 \end{bmatrix}, \qquad T_5 = \begin{bmatrix} u & v & w & w \\ v & -u & -w & w \\ w & -w & v & -u \\ w & w & -u & -v \end{bmatrix},$$

$$T_6 = \begin{bmatrix} 0 & a & b & b \\ -a & 0 & -b & b \\ -b & b & 0 & -a \\ -b & -b & a & 0 \end{bmatrix}, T_7 = \begin{bmatrix} u & 0 & w & w \\ 0 & -u & -w & w \\ w & -w & 0 & -u \\ w & w & -u & 0 \end{bmatrix}.$$

Repeat designs $ROD(4:(1;(1,1;1,1);1))$, $ROD(4:(1;(1,1;1,2);2))$, $ROD(4:(1;(1,1;2);1,2))$, $ROD(4:(1;(1;1,2);2,2))$ and $ROD(4:(1;(1,2;1,2);4))$ can be constructed using Lemma 6.9 .

Example 6.6. There are product designs $POD(8:1,1,2,3;1,3,3;1)$, $POD(8:2,2;1,1,1,1;4)$ and $POD(8:1,1,1;1,1,1;5)$. Then using the repeat design $ROD(4:1;(2;3);1,3)$ with the matrix of weight 2 used once only, we have $OD(32;(1,1,2,3,2,9,9,1,3))$, $OD(32;(2,2,2,3,3,3,4,12))$ and $OD(32;(1,1,1,2,3,3,5,15))$.

Since all of these have weight 31, we use the Geramita-Verner theorem to obtain the following orthogonal designs: $OD(32;1,1,1,1,2,2,3,3,9,9)$, $OD(32;1,2,2,2,3,3,3,4,12)$ and $OD(32;1,1,1,1,2,3,3,5,15)$. These last two designs are new.

The product designs $POD(4:1,1,1;1,1,1;1)$ can be used with the repeat designs of types $(1;(p;3);1,3)$, $p=1,2$, to obtain $OD(16;1,1,1,1,p,p,3,3)$, $p=1,2$. These were first given in Geramita and Seberry [80].

Remark 6.2. In the preceding example we have concentrated on constructing orthogonal designs with no zero. There is considerable scope to exploit these constructions to look, for other orthogonal designs in order 32 and higher powers of 2.

We can collect the results from Example 6.5 in the following statement:

Statement 6.1. In order 4 there exist repeat designs of types $(1;(r;s);h)$ for $0 \le r,\ s \le 3,\ 0 \le h \le 4$.

Noting that the repeat designs $(R;(P);H)$ are just amicable orthogonal designs $R+P$ and H, we see that:

Corollary 6.6. *There exist* $AOD(4;(1,r),(h))$ *for* $0 \le r \le 3$, $0 \le h \le 4$.

Remark 6.3. The non-existence of $AOD(8;(1,7),(5))$ and $AOD(16;(1,15),(1))$ means there are no repeat designs of types $(1;(r;7);5)$ in order 8 and $(1;(r;15);1)$ in order 16 (see Robinson [167]).

The construction and replication lemmas given later allow us to say:

Comment 6.1. In order 8 there, in fact, exist repeat designs $(1;(r);h)$ for all $0 \le r \le 7$ and $0 \le h \le 8$, except $r=7$, $h=5$ (which cannot exist).

In order 16 there exist repeat designs $(1;(r);h)$ for all $r = 1,2,3,\ldots,15$, $h = 1,2,\ldots,16$, except possibly the following pairs (r,h): $(13,1)$, $(13,5)$, $(13,9)$, $(15,7)$, $(15,9)$, $(15,15)$ which are undecided and $(15,1)$ which does not exist.

6.3.1 Construction and Replication of Repeat Designs

We now show that many repeat designs can be constructed.

Lemma 6.8. *Suppose* $((a);(b_1,b_2))$ *and* $((c);(d_1,d_2))$ *are the types of amicable orthogonal designs in orders* n_1 *and* n_2. *Then there is a repeat design in order* n_1n_2 *of type* $(b_1d_1;\ (ad_2,b_2d_1;b_2c,b_1d_2);ac)$.

Proof. Let $A, x_1B_1+x_2B_2$ and $C, y_1D_1+y_2D_2$ be the amicable orthogonal designs. Then $(B_1\times D_1;(xA\times D_2+yB_2\times D_1;uB_2\times C+wB_1\times D_2);A\times C)$ are the required repeat designs. □

Example 6.7. Let $A=C=\left[\begin{smallmatrix}1&1\\1&-\end{smallmatrix}\right]$, $B_1=D_1=\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]$, and $B_2=D_2=\left[\begin{smallmatrix}0&1\\-&0\end{smallmatrix}\right]$. Then the repeat design in order 4 and type $(1;(1,2;1,2);4)$ is

$$\left(I_4;\ \left(\left[\begin{array}{cc|cc} 0 & y & x & x \\ \bar{y} & 0 & x & \bar{x} \\ \hline \bar{x} & \bar{x} & 0 & y \\ \bar{x} & x & \bar{y} & 0 \end{array}\right];\ \left[\begin{array}{cc|cc} 0 & u & w & u \\ \bar{u} & 0 & \bar{u} & w \\ \hline \bar{w} & u & 0 & \bar{u} \\ \bar{u} & \bar{w} & u & 0 \end{array}\right] \right);\quad z\ \left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ \hline 1 & 1 & - & - \\ 1 & - & - & 1 \end{array}\right] \right).$$

Before we proceed to our uses of repeat designs, we first note some replication results.

Lemma 6.9. *Suppose there are repeat designs* $ROD(n:(r;(p_1,\ldots,p_i;q_1,\ldots,q_j);h_1,\ldots,h_k))$ *called* X,Y,Z *where* $h_1+h_2+\cdots+h_k=h$ *and* $p_1+\cdots+p_i=p$. *Further suppose* $A+B$ *and* $C+D$ *are* $AOD(m;(a,b),(c,d))$. *Then there are repeat designs of order* mn *and types*

(i) $(ar;(cp_1,cp_2,\ldots,b_r;aq_1,aq_2,\ldots,bh);ch)$,

(ii) $(ar;(ap_1,ap_2,\ldots;cq_1,cq_2,\ldots);ah_1,ah_2,\ldots,ch_i,\ldots)$,
(iii) $(ar;(ap_1,ap_2,\ldots,bh_1;cq_1,cq_2,\ldots);ch_1,ah_2,ah_3,\ldots)$,
(iv) $(ar;(bh_1,bh_2,\ldots;rb+pd,cq_1,cq_2,\ldots);rd+bp)$, *where* $d=b$,
(v) $(ar;(cq_1,cq_2,\ldots;cp);ah_1,ah_2,\ldots,bp)$,
(vi) $(ar;(br,dp_1,dp_2,\ldots;aq_1,aq_2,\ldots,bh);dh)$,
(vii) $(ar;(cp_1,\ldots;cq_1,\ldots);ch_1,ch_2,\ldots,dr)$,
(viii) $(ar;(cp_1,\ldots,dq_1,\ldots);ah_1,ah_2,\ldots,bp_1,bp_2,\ldots)$,
(ix) $(ar;(ap_1,\ldots;aq_1,\ldots);ch,dh)$,
(x) $(cr;(br;bh_1,bh_2,\ldots);ar)$,
(xi) $(cr;(br;bh);ar,abrh)$.

Proof. Use the following constructions:

(i) $(A\times X;(C\times Y+xB\times X;yA\times Q+zB\times Z);C\times Z)$,
(ii) $(A\times X;(A\times Y;C\times Q);xA\times V+C\times W)$,
(iii) $(A\times X;(A\times Y+xB\times V;C\times Q);C\times V+yA\times W)$,
(iv) $(A\times X;(B\times Z;xB\times X+yC\times Q-xD\times Y);D\times Z+B\times Y)$,
(v) $(A\times X;(C\times Q;C\times Y);xA\times Z+yB\times Y)$,
(vi) $(A\times X;(B\times X+wD\times Y;xA\times Q+yB\times Z);D\times Z)$,
(vii) $(A\times X;(C\times Y;C\times Q);C\times Z+yD\times X)$,
(viii) $(A\times X;(C\times Y+xD\times Q);A\times Z+yB\times Y)$,
(ix) $(A\times X;(A\times Y;A\times Q);C\times Z+yD\times Z)$,
(x) $(C\times X;(B\times X;B\times Z);A\times X)$,
(xi) use Lemma on the result (x). □

Corollary 6.7. *There are repeat designs of type* $ROD(2^t:1;(1,2,\ldots,2^{t-1};1,2,\ldots,2^{t-1});2^t)$.

Proof. Use part (i) of Lemma 6.9 repeatedly with repeat designs $ROD(4:1;(1,2;1,2);4)$ and type $AOD(2;(1,1),(2))$. □

6.3.2 Construction of Orthogonal Designs

The use of repeat designs with product designs is so powerful a source of orthogonal designs that it is quite impossible to indicate all the designs constructed. Hence we give only those that are used to give Corollary 5.131. We use Robinson's Ph.D. thesis and Appendix I as a source for product designs.

Corollary 6.8. *The following types of orthogonal designs exist in order* 2^t*:*

(i) $(1,1,1,1,2,2,4,4,\ldots,2^{t-2},2^{t-2})$,
(ii) $(1,1,2,1,2,4,8,\ldots,2^{t-3},3,6,12,\ldots,3.2^{t-3})$,
(iii) $(1,1,2,4,8,\ldots,2^{t-3},2^{t-3},2^{t-2},3,3,6,\ldots,3.2^{t-4})$,
(iv) $(1,1,2,4,8,\ldots,2^{t-3},3,6,9,18,\ldots,9.2^{t-5},3.2^{t-4})$,
(v) $(1,2,3,2^{t-4},3.26[t-4],3.26[t-3],3,3,6,6,12,12,\ldots,3.2^{t-5},3.2^{t-5})$,

(vi) $(2,1,2,\ldots,2^{t-s-4},\ (2^{t-s-3}-1)(bin(2^{s+1}-1))2^{t-s-2}(bin(2^{s+1}-1)),$ $2^{s+1},\ 2^{t-2}2^{t-s-3}-1, 2^{t-s-3}-1)$.

where $xbin(2^y-1)$ *means* x *times the binary expansion of* 2^y-1, *i.e.,* $x,x,2x,4x,\ldots,2^{y-1}x$.

Proof. (i) Proved by Robinson [166, Lemma 5.36,p.46].

(ii) Use the product design $POD(2^t: 1,1,2,3,6,12,\ldots,3.2^{t-4};\ 1,3.2^{t-3};\ 1,2,$ $\ldots,2^{t-4})$ with $AOD((1,1);(1,1))$. For the remainder we use product designs with repeat designs as indicated.

(iii) Use $(1,1,1,2,\ldots,2^{t-4};\ 1,2^{t-3};\ 1,2,\ldots,2^{t-4})$ with $(1;(1,2;3);4)$.

(iv) Use $(1,1,2,3,6,\ldots,3.2^{t-5};\ 1,3.2^{t-4};\ 1,2,\ldots,2^{t-5})$ with $(1;(1,2;3);4)$.

(v) Use $(1,1,2,1,2,\ldots,2^{t-5};\ 3,2^{t-4};\ 3,6,\ldots,3.2^{t-3})$ with $(1;(1,2;3);4)$.

(vi) $(1,1,1,1,2,\ldots,2^s;\ 2,2^{s+1};\ 2,\ldots,2^{s+1},2^{s+1})$ with $(1;(bin(2^{t-s-3}-1);$ $2^{t-s-3}-1);\ 2^{t-s-3})$. □

Remark 6.4. This corollary allows us to find all four variable designs of type $(a,b,c,2^t-a-b-c)$ for $t=5,6,7$ (see Appendix F), all but the design of type $(13,13,15,215)$ for $t=8$, and all but the designs of types $(13,13,15,471)$, $(27,29,29,427)$, $(29,29,29,425)$, $(29,29,31,423)$, $(31,45,45,391)$ for $t=9$.

To eliminate those remaining, we observe:

Corollary 6.9. *All orthogonal designs of order* 2^{t+k} *exist of types*

(i) $a,b,ma,2^{t+k}-a-ma-b)$, *where* $a=2^t-1$, $m<2^{k-1}$, $0\le b\le 2^{t+k-1}$;

(ii) $(a,b,ma,2^{t+k}-a-ma-b)$, *where* $a=2^t-2^s-1$, $m<2^{k-1}$, $0\le b\le 2^{t+k-1}+1$;

(iii) $(a,a,a,2^{t+k}-3a)$, *where* $0\le a\le 2^{t+k-2}$;

(iv) $(a,a,b,2^{t+k}-2a-b)$, *where* $2^{t-1}\le a\le 2^t$, $0\le b\le 2^{k-1}-1$;

(v) $(a,a,2^t-a$, *(bin* a*)*, $2^{t+k}-2^t-2a)$, *where* $2^{t-1}\le a\le 2^t$ *(note:* 2^t-a, *(bin* a*) can always be used to give* 2^t-1 *or* $2^{t-1}-1$*).*

Proof. Call the product designs $(1,\text{bin}x,2^j-x,2^j,\ldots,2^{k-2};\ 1,2^{k-1};\ 1,2,\ldots,$ $2^{k-2})$ the product designs A. We now use product designs with repeat designs as indicated:

(i) Use A with $(1;(1,2,,2^{t-1};2^t-1);2^t)$.

(ii) Use A with $(1,2^s;(1,2,\ldots,2^{s-1},2^{s+1},\ldots,2^{t-1};2^t-2^s-1);2^t)$.

(iii) Use $AOD((a,2^{t+k-2}-a);\ (2^{t+k}))$ in order 2^{t+k} with product designs $POD(4\colon 1,1,1;1,1,1;1)$.

(iv & v) Use A with $(2^t-a;\ ((\text{bin}\ (a));a);2^t)$ to get the orthogonal design $(a,a,a$ $\text{bin}(2^{k-l}-b-1)$, $b(\text{bin}\ (a))$, 2^t-a, $2^{k-1}(2^t-a)$, $2^t,2^{t+1},\ldots,2^{t+k-2})$. □

So we have:

Corollary 6.10. *All orthogonal designs of type* $(a,b,c,2^t-a-b-c)$ *and of type* (a,b,c), $0\le a+b+c\le 2^t$, *exist for* $t=2,3,4,5,6,7,8,9$.

Remark 6.5. We believe these results do, in fact, allow the construction of all full orthogonal designs (that is, with no zero) with four variables in every power of 2, but we have not been able to prove this result.

6.4 Gastineau-Hills on Product Designs and Repeat Designs

We recall Theorem 6.1 and equation (6.1). Observe that this matrix may be expressed in the form:

$$M_1 \otimes R + M_2 \otimes P + N \otimes S \tag{6.2}$$

where C, Y, Z are the 4×4 matrices of the coefficients of M_1, M_2, N respectively.

Using the notation X for xR, Y for P and Z for S in Equation (6.1), then it may be verified that

$$(X,Y,Z) = \begin{bmatrix} y_1 z_1 & y_2 z_2 & x & y_3 z_3 \\ \bar{y}_2 z_2 & y_1 \bar{z}_1 & \bar{y}_3 \bar{z}_3 & x \\ \bar{x} & y_3 \bar{z}_3 & y_1 z_1 & \bar{y}_2 z_2 \\ \bar{y}_3 z_3 & \bar{x} & y_2 z_2 & y_1 \bar{z}_1 \end{bmatrix}$$

is a triple of orthogonal designs on $(x; y_1, y_2; z_1, z_2)$ (we have "superimposed" X, Y, Z as in Definition (3.1) in Gastineau-Hills [63, p.11]), which satisfies the following conditions:

$$\begin{array}{l} \text{(i) } X * Y = X * Z = 0 \\ \text{(ii) } X + Y, X + Z \text{ are orthogonal designs} \\ \text{(iii) } Y Z^\top = Z Y^\top \end{array} \tag{6.3}$$

It may also be shown that if $(X = xR, Y, Z)$ is any triple satisfying (6.3), and if M_1, M_2, N are as in Equation (6.1), then $M_1 \otimes R + M_2 \otimes P + N \otimes S$ is an orthogonal design. (This fact will appear later to be a particular case of a more general theorem).

This generalization of Equation (6.1) has proved very useful for constructing new orthogonal designs, and has led Robinson [168] to the study of general triples (X, Y, Z) which satisfy (6.3) (here we may remove the restriction that X is on only one variable). Such triples are called *product designs*.

We wish to present an alternative definition of a product design. In the following we suppose that X, Y, Z are designs of types $(u_1, \ldots, u_p), (v_1, \ldots, v_q)$, $(w_1, \ldots, w_r)$ on variables $x_1, \ldots, x_p; y_1, \ldots, y_q; z_1, \ldots, z_r$ respectively.

Note first that the conditions (6.3) imply:

$$X Y^\top = -Y X^\top, \quad X Z^\top = -Z X^\top \tag{6.4}$$

Proof. For suppose X, Y, Z satisfy (6.3). Then on the one hand since $X + Y, X + Z$ are orthogonal designs clearly of types $(u_1, \ldots, u_p, v_1, \ldots, v_q)$, $(u_1, \ldots, u_p, w_1, \ldots, w_r)$ on $(x_1, \ldots, x_p, y_1, \ldots, y_q), (x_1, \ldots, x_p, z_1, \ldots, z_r)$ respectively, we have

$$(X+Y)(X+Y)^\top = (u_1x_1^2+\cdots+u_px_p^2+v_1y_1^2+\cdots+v_qy_q^2)I$$

and

$$(X+Z)(X+Z)^\top = (u_1x_1^2+\cdots+u_px_p^2+w_1z_1^2+\cdots+w_rz_r^2)I.$$

On the other hand

$$\begin{aligned}(X+Y)(X+Y)^\top &= XX^\top+YY^\top+XY^\top+YX^\top\\ &= (u_1x_1^2+\cdots+u_px_p^2)I+(v_1y_1^2+\cdots+v_qy_q^2)I+XY^\top+YX^\top\end{aligned}$$

and similarly

$$(X+Z)(X+Z)^\top = (u_1x_1^2+\cdots+u_px_p^2)I+(w_1z_1^2+\cdots+w_rz_r^2)I+XZ^\top+ZX^\top.$$

Hence

$$XY^\top+YX^\top=0,\quad XZ^\top+ZX^\top=0 \text{ and (6.4) follows.}\square$$

Note secondly that the conditions (6.4) and (6.3) (i) together imply the condition (6.3) (ii).

Proof. For suppose X,Y,Z are orthogonal designs satisfying (6.4) and (6.3) (i). Then $X+Y, X+Z$ are clearly defined as $\{0,\pm x_i,\pm y_j\},\{0,\pm x_i,\pm z_k\}$ matrices respectively, and are orthogonal since

$$\begin{aligned}(X+Y)(X+Y)^\top &= XX^\top+YY^\top+XY^\top+YX^\top\\ &= (\sum u_ix_i^2)I+(\sum v_iy_i^2)I\\ &= (\sum u_ix_i^2+v_jy_j^2)I\,,\end{aligned}$$

and similarly

$$(X+Z)(X+Z)^\top = (\sum u_ix_i^2+w_kz_k^2)I\,.$$

Hence (6.3)(ii) holds. $\square$

It follows that the following definition of a product design is essentially equivalent to our previous definition.

Definition 6.3. Suppose X,Y,Z are orthogonal designs of order n, types $(u_1,\ldots,u_p),(v_1,\ldots,v_q),(w_1,\ldots,w_r)$ on variables $(x_1,\ldots,x_p),(y_1,\ldots,y_q)$, $(z_1,\ldots,z_r)$ respectively, and that

$$\begin{aligned}&\text{(i) } XY^\top=-YX^\top,\quad XZ^\top=-ZX^\top,\quad YZ^\top=ZY^\top\\ &\text{(ii) } X*Y=0,\quad X*Z=0.\end{aligned}$$

Then we call the triple (X,Y,Z), a *product design* of order n, type $(u_1,\ldots,u_p),(v_1,\ldots,v_q),(w_1,\ldots,w_r)$ on the variables $(x_1,\ldots,x_p;y_1,\ldots,y_q;$ $z_1,\ldots,z_r)$.

The condition $YZ^\top = ZY^\top$ of Definition 6.3 (i) is the condition of amicability. We introduce a new expression to apply to the other two conditions of 6.3:

Definition 6.4. Orthogonal designs X, Y are called *anti-amicable* if they satisfy the condition $XY^\top = -YX^\top$

$$(\text{equivalently: } X^\top Y = -Y^\top X).$$

Thus a product design is a triple of orthogonal designs, one pair of which is amicable, and the other two pairs anti-amicable, and such that the anti-amicable pairs have zero Hadamard products.

As with amicable k-tuples, we might expect that it would be very useful to have information on the connections between possible orders of product designs and numbers of variables involved. Before pursuing this matter however, let us consider yet another method which has been used to construct new orthogonal designs, and which leads naturally to what can be regarded as generalization of the product designs. This is a slight variation of Theorem 6.2.

Lemma 6.10 (Geramita, Seberry-Wallis [83]). *If P_1, P_2, P_3, H are pairwise amicable orthogonal designs, with P_1, P_2, P_3 skew symmetric and H symmetric, then*

$$\begin{bmatrix} z_1I+P_1 & z_2I+P_2 & z_3I+P_3 & H \\ -z_2I+P_2 & z_1I-P_1 & H & -z_3I-P_3 \\ -z_3I+P_3 & -H & z_1I-P_1 & z_2I+P_2 \\ -H & z_3I-P_3 & -z_2I+P_2 & z_1I+P_1 \end{bmatrix}$$

is an orthogonal design. (I is the identity matrix of appropriate size).

Observe that this matrix may be expressed in the form:

$$I \otimes A + P_1 \otimes B_1 + P_2 \otimes B_2 + P_3 \otimes B_3 + H \otimes C$$

where A, B_1, B_2, B_3, C are 4×4 matrices of the coefficients of I, P_1, P_2, P_3, H respectively.

A, B_1, B_2, B_3, C are $\{0, \pm 1\}$ matrices, but if we set $Y_i = y_i B_i$ $(i = 1, 2, 3)$, $Y = Y_1 + Y_2 + Y_3$, $X = xC$ then it may be verified that $(X, Y = Y_1 + Y_2 + Y_3, Z)$ is a product design on the variables $(x; y_1, y_2, y_3; z_1, z_2, z_3)$.

Also if we set $R = rI$, then R, P_1, P_2, P_3, H are orthogonal designs which satisfy:

$$\begin{aligned} &\text{(i) } R * P_i = 0 \text{ for each } i, \\ &\text{(ii) } R + P_i \text{ is an orthogonal design for each } i, \\ &\text{(iii) All pairs } (R, H), (P_i, H), (P_i, P_j) \text{ are amicable.} \end{aligned} \tag{6.5}$$

Proof. (i) since $R = rI$ and the P_i are antisymmetric; (ii) since $(R + P_i)(R + P_i)^\top = RR^\top + RP_i^\top + P_iR^\top + P_iP_i^\top = r^2I + r(P_i^\top + P_i) + P_iP_i^\top = r^2I + P_iP_i^\top$ etc.; (iii) is trivial. □

It may also be shown that if $Z, Y_1 = y_1 B_1, \ldots, Y_k = y_k B_k$, $X = xC$, ($B_i, C, \{0, \pm 1\}$ matrices) are orthogonal designs such that $Y_i * Y_j = 0$ (all $i \neq j$) and $(X, Y = Y_1 + \cdots + Y_k, Z)$ is a product design, and if $R = rA$ (A a $\{0, \pm 1\}$ matrix), $P_1, \ldots, P_k, H$ are orthogonal designs satisfying (6.5), then

$$A \otimes Z + P_1 \otimes B_1 + \cdots + P_k \otimes B_k + H \otimes C \tag{6.6}$$

is an orthogonal design (this fact will appear later as a particular case of a general theorem).

This generalization of Lemma 6.10 has proved useful for constructing new orthogonal designs. So it seems that a study of sets of designs satisfying (6.5) could be profitable. Following Robinson and Seberry [169] we call such a set a *repeat design*, but as we did with product designs we prefer to give the formal definition in an alternative form:

Definition 6.5. Suppose $X, Y_1, \ldots, Y_k, Z$ are orthogonal designs of order n, types $(u_1, \ldots, u_p), (v_{11}, \ldots, v_{1q_1}), \ldots, (v_{k1}, \ldots, v_{kq_k}), (w_1, \ldots, w_r)$ on the variables $(x_1, \ldots, x_p), (y_{11}, \ldots, y_{1q_1}), \ldots, (y_{k1}, \ldots, v_{kp_k}), (z_1, \ldots, z_r)$ respectively, and that

$$\begin{aligned} &\text{(i) } Y_i X^\top = -X Y_i^\top, \\ &\text{(ii) } Y_j Y_i^\top = Y_i Y_j^\top, \quad Z X^\top = X Z^\top,\ Z Y_i^\top = Y_i Z^\top \text{ (all } i, j) \\ &\text{(iii) } X * Y_i = 0 \text{ (all } i) \end{aligned}$$

Then we call the $(k+2)$-tuple $(X, Y_1, \ldots, Y_k, Z)$ a *repeat design* of order n, type $(u_1, \ldots, u_p; v_{11}, \ldots, v_{1q_1}; \ldots; v_{k1}, \ldots, v_{kq_k}; w_1, \ldots, w_r)$ on the variables $(x_1, \ldots, x_p; y_{11}, \ldots, y_{1q_1}; \ldots; y_{k1}, \ldots, v_{kp_k}; z_1, \ldots, z_r)$.

Of course $X, Y_1, \ldots, Y_k, Z$ in 6.5 correspond to $R, P_1, \ldots, H$ respectively in (6.5). Otherwise, apart from the fact that we have allowed X in 6.5 to be on more than one variable, the conditions (6.5), 6.5 are equivalent, by the same kind of argument as given in our previous discussion of product designs.

Product designs may be regarded as particular cases of repeat designs, given by $k = 2$, $Z = 0$ (zero matrix, which may be regarded as an orthogonal design on no variables) .

Similarly a theory of repeat designs should yield a theory of amicable k-tuples, if we can allow $X = Z = 0$. In the immediate following we assume that X has at least one variable (while allowing $Y_1, \ldots, Y_k, Z$ to have as few as no variables each), but later it will be found that this restriction may be removed painlessly.

Let $(X, Y_1, \ldots, Y_k, Z)$ be a repeat design of order n, type $(u_0, u_1, \ldots, u_p; v_{11}, \ldots, v_{1q_1}; \ldots; v_{k1}, \ldots, v_{kq_k}; w_1, \ldots, w_r)$ on the $p+1, q_1, \ldots, q_k, r$ variables $(x_0, x_1, \ldots, x_p; y_{11}, \ldots, y_{1q_1}; \ldots; y_{k1}, \ldots, y_{kq_k}; z_1, \ldots, z_r)$, $(p, q_1, \ldots, q_k, r\ r \geq 0)$

We have

$$
\begin{aligned}
&XX^\top = \left(\sum_0^p u_j x_j^2\right) I\,,\ Y_i Y_i^\top = \left(\sum_1^{q_i} v_{ij} y_{ij}^2\right) I\,,\ ZZ^\top = \left(\sum_1^r w_j z_j^2\right) I \\
&Y_1 X^\top = -XY_1^\top\,, \\
&Y_j Y_i^\top = Y_i Y_j^\top\ \ (i \neq j)\,,\ Y_i Z^\top = ZY_i^\top\,,\ XZ^\top = ZX^\top\,,
\end{aligned}
\tag{6.7}
$$

and similar equations with $X^\top X$, etc., in place of $XX^\top$, etc.

Write

$$
X = \sum_0^p x_j A_j\,, \qquad Y_i = \sum_1^{q_i} y_{ij} B_{ij}\,, \qquad Z = \sum_1^r z_j C_j
$$

$$
(A_j, B_{ij}, C_j\ \{0 \pm 1\} \text{ matrices})
$$

Substituting into (6.7) and comparing like terms gives:

$$
\begin{cases}
A_j A_j^\top = u_j I, \qquad B_{ij} B_{ij}^\top = v_{ij} I, \qquad C_j C_j^\top = w_j I, \\
A_i A_j^\top + A_j A_i^\top = 0\ \ (i \neq j), \qquad B_{ij} B_{ik}^\top + B_{ik} B_{ij}^\top = 0\ \ (j \neq k), \\
C_i C_j^\top + C_j C_i^\top = 0\ \ (i \neq j), \\
B_{jk} A_i^\top = -A_i B_{jk}^\top\,, \qquad C_j A_i^\top = A_i C_j^\top\,, \\
B_{k\ell} B_{ij}^\top = B_{ij} B_{k\ell}^\top\ \ (i \neq k)\,, \qquad C_k B_{ij}^\top = B_{ij} C_k^\top\,,
\end{cases}
$$

and similar equations with products reversed.

Set

$$
E_i = \frac{1}{\sqrt{u_i u_0}} A_i A_0^\top\,, \quad F_{ij} = \frac{1}{\sqrt{v_{ij} u_0}} B_{ij} A_0^\top\,, \quad G_i = \frac{1}{\sqrt{w_i u_0}} C_i A_0^\top\,. \tag{6.8}
$$

It is easily verified that $E_0 = I$ and $E_1, \ldots, E_p$, $F_{11}, \ldots, F_{1p_1}$, $F_{k1}, \ldots, F_{kp_k}$, $G_1, \ldots, G_r$ satisfy

$$
\begin{cases}
E_i^2 = -I\,, \qquad F_{ij}^2 = -I\,, \qquad G_i^2 = I \\
E_j E_i = -E_i E_j\ \ (i \neq j) \qquad F_{ik} F_{ij} = -F_{ik} F_{ij}\ \ (j \neq k)\,, \\
G_j G_i = -G_j G_i\ \ (i \neq j) \\
F_{jk} E_i = -E_i F_{jk}\,, \qquad G_j E_i = -E_i G_j\,, \\
F_{k\ell} F_{ij} = F_{ij} F_{k\ell}\ \ (i \neq k)\,, \qquad G_k F_{ij} = -F_{ij} G_k
\end{cases}
$$

Again we have arrived at an order n representation of a real algebra which is "Clifford-like", with the one "non-Clifford" property that some pairs of distinct generators commute.

This algebra may be defined as the real algebra on $p + q_1 + \cdots q_k + r$ generators $\alpha_1, \ldots, \alpha_p$, $\beta_{11}, \ldots, \beta_{lq_1}, \ldots, \beta_{k1}, \ldots, \beta_{kq_k}$, $\gamma_1, \ldots, \gamma_r$, with defining equations:

$$\begin{cases} \alpha_i^2 = -1, \quad \beta_{ij}^2 = -1, \quad \gamma_i^2 = 1 \\ \alpha_j\alpha_i = -\alpha_i\alpha_j \ \ (i \neq j), \quad \beta_{ik}\beta_{ij} = -\beta_{ij}\beta_{ik} \ \ (j \neq k) \\ \gamma_j\gamma_i = -\gamma_i\gamma_j \ \ (i \neq j) \\ \beta_{jk}\alpha_i = -\alpha_i\beta_{jk}, \quad \gamma_j\alpha_i = -\alpha_i\gamma_j, \\ \beta_{k\ell}\beta_{ij} = \beta_{ij}\beta_{k\ell} \ \ (i \neq k), \quad \gamma_k\beta_{ij} = -\beta_{ij}\gamma_k. \end{cases} \tag{6.9}$$

For a repeat design of order n on $p+1, q_1, \ldots, q_k, r$ variables to exist it is *necessary* for a real order n representation of this algebra to exist.

We shall return later to the questions of just what are the possible orders of representations of (6.9), and whether the existence of an order n representation of (6.9) is sufficient for the existence of repeat design (6.7).

Observe that the case of product designs is included in what we have just done — we simply take $k = 2$ and $r = 0$.

If we also rewrite $q_1, q_2, \beta_{1j}, \beta_{2j}$ as q, r, β_j, γ_j respectively we find that the existence of an order n product design on $(p+1, q, r)$ variables implies the existence of an order n representation of the real algebra on $p+q+r$ generators $\alpha_1, \ldots, \alpha_p$, $\beta_1, \ldots, \beta_q, \gamma_1, \ldots, \gamma_r$ with defining equations.

$$\begin{cases} \alpha_i^2 = \beta_j^2 = \gamma_k^2 = -1 \\ \alpha_j\alpha_i = -\alpha_i\alpha_j, \quad \beta_j\beta_i = -\beta_i\beta_j, \quad \gamma_j\gamma_i = -\gamma_i\gamma_j \ \ (i \neq j) \\ \beta_j\alpha_i = -\alpha_i\beta_j, \quad \gamma_j\alpha_i = -\alpha_i\gamma_j, \quad \gamma_j\beta_i = \beta_i\gamma_j, \end{cases} \tag{6.10}$$

again a "not-quite-Clifford" algebra.

Note that (6.10) is not quite the same as equation (3.10) in [63, p.20], so that a theory of amicable triples need not necessarily by itself yield a theory of product designs.

In fact not even equation (3.8) in [63, p.18] (the algebra corresponding to more general amicable k-tuples), seems to contain (6.10) as a particular case.

6.5 Gastineau-Hills Systems of Orthogonal Designs

So far we have encountered several instances of sets of orthogonal designs (amicable sets [63, p.11], product designs (Definition 6.3), and repeat designs (Definition 6.5)), each such set having the property that each pair of members is either *amicable* or *anti-amicable*. Each such set happened also to have the property that each pair of anti-amicable members has zero Hadamard product.

We have examined some of the more fruitful techniques that have been developed to help find new orthogonal designs, and have found that each such technique could be described as taking certain such sets of amicable/ anti-amicable designs, and forming sums of *Kronecker products* (Equations [63, (3.6),p.15], (6.2), (6.6)).

We have found that an attempt to find a relationship between the possible *orders* of the designs in such sets and the *numbers of variables* involved leads in each case to the consideration of an algebra which in general generalizes the Clifford algebras and which, apparently, has not yet been studied ([63, (3.8)p.18], (6.9)).

It seems reasonable to introduce the following more general concept in the hope that the theory discussed so far may be unified in a natural way, and in the hope that through this unification and generalization more powerful ways of tackling "the orthogonal design problem" may emerge.

Definition 6.6. A *k-Gastineau-Hills system* of order n, *genus* (δ_{ij}) $1 \le i \le j \le k$ (where each $\delta_{ij} = 0$ or 1), type $(u_{11},\dots,u_{1p_1};\dots;u_{k1},\dots,u_{kp_k})$, on $p_1,\dots,p_k$ *distinct* commuting variables $x_{11},\dots,x_{1p_1};\dots;x_{k1},\dots,x_{kp_k}$ is an (*ordered*) k-tuple of $n \times n$ matrices $(X_1,\dots,X_k)$ where, for each i, X_i has entries from $\{0, \pm x_{i1},\dots,\pm x_{ip_i}\}$, and

$$\text{(i)} \qquad X_i X_i^\top = \left(\sum_{k=1}^{p_i} u_{ik} x_{ik}^2\right) I \quad (1 \le i \le k)$$

$$\text{(ii)} \qquad X_j X_i^\top = (-1)^{\delta_{ij}} X_i X_j^\top \quad (1 \le i < j \le k)$$

We will write k-GH-system as shorthand for k-Gastineau-Hills system. The system is called *regular* if in addition the *Hadamard product* $X_i * X_j$ is zero whenever $\delta_{ij} = 1$.

Thus each X_i is an *orthogonal design*, and each pair X_i, X_j is either *amicable* $(\delta_{ij} = 0)$ or *anti-amicable* $(\delta_{ij} = 1)$. Regular systems have the additional property that anti-amicable pairs are element-wise *disjoint*.

Example 6.8. (i) A *single orthogonal design* $X = x_1A_1 + \cdots + x_pA_p$ (the A_i $\{0, \pm 1\}$ matrices) on p variables where $XX^\top = \left(\sum_1^p u_i x_i^2\right) I$. Its genus is vacuous (there being no i, j satisfying $1 \le i < j \le 1$!), and it is vacuously regular. On the other hand note that $(x_1A_1,\dots,x_pA_p)$ is a regular p-system of genus (δ_{ij}), $1 \le i < j \le p$, where each $\delta_{ij} = 1$, and type $(u_1;\dots;u_p)$. Naturally it could be suggested that these two systems (X) and $(x_1A_1,\dots,x_pA_p)$ should be regarded as "equivalent" – we pursue this matter shortly.

(ii) An *amicable k-tuple* is a regular k-GH-system with genus (δ_{ij}) where each $(\delta_{ij}) = 0$.

(iii) A *product design* (X, Y, Z) (as defined in Definition 6.3) is a regular 3-GH-system of genus (δ_{ij}) where $\delta_{12} = \delta_{13} = 1$ $\delta_{23} = 0$.

(iv) A *repeat design* $(X, Y_1,\dots,Y_k, Z)$ (as defined in Definition 6.5) is a regular $(k+2)$-GH-system of genus (δ_{ij}) where $\delta_{12} = \delta_{13} = \cdots = \delta_{1k+1} = 1$, and all other $\delta_{ij} = 0$.

(v) $\begin{bmatrix} xy & x\bar{y} \\ \bar{x}y & xy \end{bmatrix}$, as a pair of order 2 designs on the variables $(x; y)$ (written "superimposed" –see [63, Example (3.3),p.12]), is a 2-GH-system of type $(2;2)$ and genus $(\delta_{12} = 1)$. This system is not regular.

From 6.8 (v) we see that in general the property of being regular is non trivial. However:

Lemma 6.11. *A system of type* $(1,1,\ldots,1;1,1,\ldots,1;\ldots)$ *is regular.*

Proof. In systems of this type each X_i has each of its variables occurring just once in each row. Suppose X_i, X_j $(i \neq j)$ are anti-amicable. Then $X_j X_i^\top (= -X_i X_j^\top)$ is skew-symmetric, with zero diagonal elements. Suppose $X_i = (a_{k\ell})$, $X_j = (b_{k\ell})$ where each $a_{k\ell}$ is from $\{0, \pm x_{i1}, \ldots, \pm x_{ip_i}\}$ and each $b_{k\ell}$ is from $\{0, \pm x_{j1}, \ldots, \pm x_{jp_j}\}$. Then for fixed k the *non zero* $|a_{k\ell}|$, $|b_{km}|$ are distinct independent variables, and $\sum_\ell a_{k\ell} b_{k\ell}, = 0$. Clearly then each term in this sum must be zero and the result follows. □

The importance of being regular is that if $X_i, X_j, X_k, \ldots$ are pairwise anti-amicable members of a regular system, they may be added to make a design $X_i + X_j + X_k + \cdots$. This design is orthogonal.

Remark 6.6. Indeed $(X_i + X_j + \cdots)(X_i + X_j + \cdots)^\top = (\sum_a u_{ia} x_{ia}^2 + \sum_b u_{jb} x_{jb}^2 + \cdots) I$, where $(x_{ia}), (u_{ia})$ are respectively the variables, types of X_i etc., - since sums like $X_i X_j^\top + X_j X_i^\top$ are zero.

In particular:

Corollary 6.11. *If, in a regular* k*-GH-system* $(X_1, \ldots, X_k)$ *of genus* (δ_{ij})*, all* $\delta_{ij} = 1$*, then* $X_1 + \cdots + X_k$ *is an orthogonal design.*

In Corollary 6.11 we have in a sense reduced a k-GH-system to an "equivalent" ℓ-system, by adding pairwise anti-amicable designs. More generally we have the following:

Lemma 6.12. *Suppose, possibly after reordering the* X_i *of a* k*-GH-system* $(X_1, \ldots, X_k)$ *and correspondingly reordering the genus, type and variable components* (δ_{ij}), (u_{ij}), (x_{ij}), *that for some* r $(1 \leq r \leq k)$ *the designs* $X_r, \ldots, X_k$ *are pairwise anti-amicable, with pairwise Hadamard products zero. Suppose further that, for each* $i < r$, $\delta_{ir} = \delta_{ir+1} = \cdots = \delta_{ik}$.

Then $(X_1, \ldots, X_{r-1}, X_r + \cdots + X_k)$ *is an* r*-system of genus* (δ'_{ij})*, where* $\delta'_{ij} = \delta_{ij}$ $(1 \leq i < j \leq r)$*, type* $(u_{11}, \ldots; u_{21}, \ldots; \ldots; u_{r1}, \ldots, u_{r+1\,1}, \ldots, u_{k1}, \ldots)$ *on the variables* $x_{11} \ldots; x_{21}, \ldots; x_{r1}, \ldots, x_{r+1\,1}, \ldots, x_{k1}, \ldots)$.

The new system is regular if and only if the original system is regular.

Proof. As in Corollary 6.11 $X_r + \cdots + X_k$ is an orthogonal design. Its type is $(u_{r1}, \ldots, u_{r+1\,1}, \ldots, u_{k1})$ and its variables are $(x_{r1}, \ldots, x_{r+1\,1}, \ldots, x_{k1}, \ldots)$.

We need only check $(X_r + \cdots + X_k) X_i^\top$ $(i < r)$

$$
\begin{aligned}
&= X_r X_i^\top + \cdots + X_k X_i^\top \\
&= (-1)^{\delta_{ir}} X_i X_r^\top + (-1)^{\delta_{ik}} X_i X_k^\top \\
&= (-1)^{\delta_{ij'}} X_i (X_r + \cdots + X_k)^\top
\end{aligned}
$$

and the first part follows.

The statement about regularity follows easily from

$$X_i * (X_r + \cdots + X_k) = X_i * X_r + \cdots + X_i * X_k \,.\square$$

We now formalize the concept of "equivalence" of systems. The following definition incorporates trivial equivalences as well as those suggested by Lemma 6.12:

Definition 6.7. A k-GH-system S and an ℓ-GH-system T are called *equivalent* if there is a sequence $S = S_0, S_1, \ldots, S_m = T$ of systems where for each i either:

(i) each of S_{i-1}, S_i may be obtained from the other by one of the steps:

- (a) renaming variables,
- (b) changing signs of a variable throughout,
- (c) changing signs of all elements of the same row (or column) of all the designs,
- (d) applying the same permutation to the rows (or columns) of each design,
- (e) transposing all the designs,
- (f) reordering the designs within the system, or

(ii) one of S_{i-1}, S_i may be obtained from the other using Lemma 6.12.

Clearly each step of types (a) to (e) has no effect on genus or type, while a step of type (f) merely reorders genus, type and variable components.

Also, if a system is regular, so is any equivalent system.

Hence we may speak of an "equivalence class" of systems, and may identify any equivalence class as being regular or not, according as all or none of its member systems are regular.

Thus the two systems (X), $(x_1 A_1, \ldots, x_p A_p)$ mentioned in Example 6.8 (i) are equivalent in the sense of Definition 6.7 – the first being obtainable from the second using Lemma 6.12.

As this example suggests, there are, in a sense, within each *regular* "equivalence class" of systems two extremes.

On the one hand we could find an ℓ-GH-system in the equivalence class which minimises ℓ. This can be done by taking a system $(X_1, \ldots, X_p)$ in the class, and defining a relation - on the set of X_i by:

$$X_i \sim X_j \text{ means either: } \begin{cases} i = j, \text{ or} \\ \delta_{ij} (\text{or } \delta_{ji}) = 1, \text{ or} \\ \delta_{ik} (\text{or } \delta_{ki}) = \delta_{jk} (\text{or } \delta_{kj}), \text{ for all } k \neq i, j. \end{cases}$$

It is easy to show that this is an equivalence relation. As in Lemma 6.12 we may add together equivalent designs (remember that we are assuming regularity!) producing an equivalent ℓ-GH-system which clearly minimises ℓ.

On the other hand we may write each X_i as $\sum_j x_{ij}A_{ij}$ (each A_{ij} a $\{0,\pm 1\}$ matrix), and form the system $(x_{11}A_{11},\ldots,x_{21}A_{21},\ldots,x_{k1}A_{k1},\ldots)$. This is an equivalent ℓ-GH-system where ℓ is maximal (for the purposes of this argument we must exclude from consideration systems which contain zero — i.e. no variable designs).

Note that the A_{ij} are here weighing matrices which satisfy $A_{k\ell}A_{ij}^{\top} = \pm A_{ij}A_{k\ell}^{\top}$ (all i,j,k,ℓ).

It turns out that as far as the algebraic theory developed later is concerned, we could well consider only those ℓ-GH-systems for which ℓ is maximal in an equivalence class of systems. In other words we shall essentially be considering sets of weighing matrices A_{ij} which satisfy $A_{k\ell}A_{ij}^{\top} = \pm A_{ij}A_{k\ell}^{\top}$ (all i,j,k,ℓ).

But for the Gastineau-Hills [63, p.44] theory of Kronecker products it will be more convenient to work as far as possible with systems in more or less "reduced" form.

6.6 The Structure and Representations of Clifford-Gastineau-Hills Algebras

Definition 6.8. Let F be a commutative field of characteristic not 2, m an integer ≥ 0, $(k_i)_{1\leq i\leq m}$ a family of non-zero elements of F, and $(\delta_{ij})_{1\leq i<j\leq m}$ a family of elements from $\{0,1\}$.

The *Quasi Clifford* or QC, algebra $C = C_F[m,(k_i),(\delta_{ij})]$ is the algebra (associative, with a 1) over F or m generators $\alpha_1,\ldots,\alpha_m$ say with defining equations:

$$(i)\begin{cases}\alpha_i^2 = k_i, & (1\leq i\leq m)\\ \alpha_j\alpha_i = (-1)^{\delta_{ij}}\alpha_i\alpha_j, & (1\leq i<j\leq m)\end{cases} \tag{6.11}$$

where $k_i \in F$ is identified with $k_i 1$ of C.

If all $\delta_{ij} = 1$ we have the Clifford algebra corresponding to some non singular quadratic form on F^m. If in addition each $k_i = \pm 1$, we have those special Clifford algebras studied by Kawada and Iwahori [119]. Later we shall be considering *QC* algebras for which the (α_i) of Definition 6.8 are given, or may be chosen, such that each $k_i = \pm 1$. We call such algebras *Clifford-Gastineau-Hills* or *CGH*, algebras.

The QC algebra C of Definition 6.8 is defined to within isomorphism by the properties:

Definition 6.9. (a) It has m elements,$\alpha_1,\ldots,\alpha_m$ say, which generate C (that is, each element of C is an F-linear combination of words in the α_i – the "null word" 1 being one possible word), and which satisfy Definition 6.8;

(b) If D is any F-algebra containing elements $\beta_1,\ldots,\beta_m$, which satisfy $\beta_i^2 = k_i$, $\beta_j\beta_i = (-1)^{\delta_{ij}}$, $(i<j)$, there is an F-algebra homomorphism $C\mapsto D$ which maps α_i to β_i, for each i.

The algebra described by equation (6.11) may be constructed as the free F-algebra or m generators $\alpha_1,\ldots,\alpha_m$, factored out by the ideal generated by the elements $\alpha_i^2 - k_i 1$, $\alpha_j\alpha_i - (-1)^{\delta_{ij}}\alpha_i\alpha_j$. $(i<j)$.

Because of Definition 6.8 (i), any product of the α_i reduces to an F-multiple of one of the 2^m elements $\alpha_1^{\epsilon_1}\ldots\alpha_m^{\epsilon_m}$ (each $\epsilon_i = 0$ or 1). So as a vector space over F, C is spanned by these 2^m elements and $\dim C \le 2^m$.

To show that $\dim C$ actually is 2^m, let us define D to be the vector space of all formal F-linear combinations of the 2^m formal expression $\beta_1^{\epsilon_1}\ldots\beta_m^{\epsilon_m}$ $(\epsilon_i = 0,1)$. [These expressions may be identified as the 2^m subsets of an m-set in an obvious way]. Make D into an algebra by defining products:

$$(\beta_1^{\epsilon_1}\ldots\beta_m^{\epsilon_m})\left(\beta_1^{\eta_1}\ldots\beta_m^{\eta_m}\right) = h\beta_1^{\xi_1}\ldots\beta_m^{\xi_m}$$

where for each i, ξ_i is $\epsilon_i+\eta_i$ reduced modulo 2, and

$$h = h(\underset{\sim}{\epsilon},\underset{\sim}{\eta}) = \prod_{i=1}^{m}\left(k_i^{\epsilon_i}\prod_{j=i+1}^{m}(-1)^{\epsilon_j\delta_{ij}}\right)^{\eta_i}$$

We must check that this product is associative:

$$\begin{aligned}
&(\beta_1^{\epsilon_1}\ldots\beta_m^{\epsilon_m})\left(\left(\beta_1^{\eta_1}\ldots\beta_m^{\eta_m}\right)\left(\beta_1^{\xi_1}\ldots\beta_m^{\xi_m}\right)\right)\\
=&(\beta_1^{\epsilon_1}\ldots\beta_m^{\epsilon_m})\,h\left(\underset{\sim}{\eta},\underset{\sim}{\xi}\right)\left(\beta_1^{\eta_1\dot{+}\xi_1}\ldots\beta_m^{\eta_m\dot{+}\xi_m}\right)\\
=&h\left(\underset{\sim}{\eta},\underset{\sim}{\xi}\right)h\left(\underset{\sim}{\epsilon},\underset{\sim}{\eta}\dot{+}\underset{\sim}{\xi}\right)\beta_1^{\epsilon_1\dot{+}(\eta_1\dot{+}\xi_1)}\ldots\beta_m^{\epsilon_m\dot{+}(\eta_m\dot{+}\xi_m)}
\end{aligned}$$

where $\dot{+}$ is addition modulo 2.

Similarly

$$\begin{aligned}
&\left((\beta_1^{\epsilon_1}\ldots\beta_m^{\epsilon_m})\left(\beta_1^{\eta_1}\ldots\beta_m^{\eta_m}\right)\right)\left(\beta_1^{\xi_1}\ldots\beta_m^{\xi_m}\right)\\
=&h\left(\underset{\sim}{\epsilon},\underset{\sim}{\eta}\right)h\left(\underset{\sim}{\epsilon}\dot{+}\underset{\sim}{\eta},\underset{\sim}{\xi}\right)\beta_1^{(\epsilon_1\dot{+}\eta_1)\dot{+}\xi_1}\ldots\beta_m^{(\epsilon_m\dot{+}\eta_m)\dot{+}\xi_m}.
\end{aligned}$$

Since addition mod 2 is associative it remains only to verify that

$$h(\underset{\sim}{\eta},\underset{\sim}{\xi})h(\underset{\sim}{\epsilon},\underset{\sim}{\eta}\dot{+}\underset{\sim}{\xi}) = h(\underset{\sim}{\epsilon},\underset{\sim}{\eta})h(\underset{\sim}{\epsilon}\dot{+}\underset{\sim}{\eta},\underset{\sim}{\xi}).$$

[The former gives each k_i raised to the power $\eta_i\xi_i+\epsilon_i(\eta_i\dot{+}\xi_i) = k_1$ say, and -1 raised to the power $\sum_{i=1}^m\sum_{j=i+1}^m\eta_j\delta_{ij}\xi_i + \sum_{i=1}^m\sum_{j=i+1}^m\epsilon_i\delta_{ij}(\eta_i\dot{+}\xi_i) = \lambda_1$ say.

The latter gives each k_i raised to the power $\epsilon_i\eta_i + (\epsilon_i\dot{+}\eta_i)\xi_i = k_2$ say, and -1 raised to the power $\sum_{i=1}^m\sum_{j=i+1}^m\epsilon_j\delta_{ij}\eta_i + \sum_{i=1}^m\sum_{j=i+1}^m(\epsilon_j\dot{+}\eta_j)\delta_{ij}\xi_i = \lambda_2$

say. Clearly $k_1 = k_2$ since each of $\epsilon_i, \eta_i, \xi_i$ is 0 or 1, and also clearly $\lambda_1 \equiv \lambda_2 \pmod 2$ as required].

$\beta_1^0 \beta_2^0 \dots \beta_m^0$ is clearly a 1 for D, and identifying β_i with

$$\beta_1^0 \dots \beta_{i-1}^0 \beta_i^1 \beta_{i+1}^0 \dots \beta_m^0 \ (i = 1, \dots, m)$$

it is also easy to verify that

$$\beta_i^2 = k_i 1, \quad \beta_j \beta_i = (-1)^{\delta_{ij}} (\beta_i \beta_j) \quad (i < j)$$

So by Definition 6.9 (b) there is a homomorphism $C \mapsto D$ which takes α_i to β_i (each i). Clearly the β_i generate D, so that in fact this homomorphism is subjective and $\dim C \geq \dim D = 2^m$ [indeed we can now deduce $C \cong D$]

We have proved:

Theorem 6.7. *The algebra C of Equation* (6.11) *has dimension 2^m as a vector space over F, and a basis is*

$$\{\alpha_1^{\eta_1} \dots \alpha_m^{\eta_m} : \epsilon_i = 0 \text{ or } 1\}.$$

We use $[\dots]$ for algebra generators, $\langle \dots \rangle$ for vector space generators. So

$$\begin{aligned} C &= [\alpha_1 \dots \alpha_m] \\ &= \langle 1, \alpha_1, \dots, \alpha_m, \alpha_1\alpha_2, \dots, \alpha_1\alpha_2 \dots \alpha_m \rangle \end{aligned}$$

Remark 6.7. The 2^m basis elements in Theorem 6.7 have the properties

(a) each squares to a non zero F-multiple of 1, that multiple being $\pm$ a product of the members of a subset of the (k_1).
(b) each pair commutes or anti-commutes

Gastineau-Hills [63, p.67] then proceeds to show QC algebras are semi-simple and develops the theory of QC algebras and Clifford-Gastineau-Hills (CGH) algebras. We do not consider this here but proceed to their application to product and repeat designs.

6.7 Decomposition

We now consider the following QC algebra:

Notation 6.1. For $b \in \boldsymbol{F}$, let $\mathbb{C}_b = \mathbb{C}_b(F)$ denote the QC algebra over F on one generator, β say, satisfying $\beta^2 = b$.

For $c, d \in \boldsymbol{F}$, let $\mathbb{Q}_{c,d} = \mathbb{Q}_{c,d}(F)$ denote the QC algebra over F on two generators, γ, δ say, where $\gamma^2 = c$, $\delta^2 = d$, $\delta\gamma = -\gamma\delta$.

These algebras are in fact Clifford algebras and their structures are known.

The importance of the algebras $\mathcal{C}_b, \mathbb{Q}_{c,d}$ lies in the fact that any QC algebra decomposes into tensor product of such algebras. To show this we assume all the elementary properties of tensor products, including the following:

Lemma 6.13. *Let A be a finite dimensional algebra over F, and H, K sub-algebras each containing the 1 of A. Suppose*

(i) each element of H commutes with each element of K;
(ii) $HK = A$ (where HK is the set of all finite sums $\sum h_i k_i : h_i \in H,\ k_i \in K$), and
(iii) $\dim A = \dim H \dim K$.

Then there is an isomorphism $A \cong H \otimes_F K$ (the tensor product of algebras over F), given by $hk \mapsto h \otimes k$. (in this case we shall identify h with $h \otimes 1$, k with $1 \otimes k$) [4, Ch.1 §5].

Clearly there is an extension of this lemma to the case of any finite number of sub-algebras $H_1, \ldots, H_r$ of A each containing the 1 of A and satisfying

(i) each element of H_i commutes with each element of H_j, $(i \neq j)$,
(ii) $H_1 \ldots H_r = A$,
(iii) $\dim A = \dim H_1 \ldots \dim H_r$;

in which case $A \cong H_1 \otimes_F \ldots \otimes_F H_r$.

The decomposition of $C = C[m, (k_i), (\delta_{ij})] = [\alpha_1, \ldots, \alpha_m]$ (see definition 6.8) proceeds as follows:

Suppose that all $\delta_{ij} = 0$, so that C is commutative. If $m > 1$, $[\alpha_1, \ldots, \alpha_m] = [\alpha_1][\alpha_2, \ldots, \alpha_m]$ since each basis element $\alpha_1^{\epsilon_1}\alpha_2^{\epsilon_2}\ldots\alpha_m^{\epsilon_m}$ of C is the product of elements of $[\alpha_1], [\alpha_2, \ldots, \alpha_m]$ respectively.

Also $\dim C = 2^m = 2 \times 2^{m-1} = \dim[\alpha_1] \dim[\alpha_2, \ldots, \alpha_m]$ So by Lemma 6.13

$$C \cong [\alpha_1] \otimes [\alpha_2, \ldots, \alpha_m] = \mathcal{C}_{k_1} \otimes C[m-1, (k_i'), (\delta_{ij}')]$$

where $k_{i-1}' = k_i$ $(2 \leq i \leq m)$, $\delta_{i-1,j-1}' = \delta_{ij}$ $(2 \leq i < j \leq m)$.

Suppose on the other hand that some $\delta_{ij} = 1$. We may suppose (possibly after reordering the α_i and correspondingly the k_i, δ_{ij}) that $\delta_{12} = 1$, so that α_1, α_2 anti-commute.

If $m > 2$, $[\alpha_1, \ldots, \alpha_m] = [\alpha_1, \alpha_2][\alpha_1^{\delta_{23}}\alpha_2^{\delta_{13}}\alpha_3, \ldots, \alpha_1^{\delta_{2m}}\alpha_2^{\delta_{1m}}\alpha_m]$ since each basis element $\alpha_1^{\epsilon_1}\ldots\alpha_m^{\epsilon_m}$ of C is the product

$$\left(\alpha_1^{\eta_1}\alpha_2^{\eta_2}\right)\left(\left(\alpha_1^{\delta_{23}}\alpha_2^{\delta_{13}}\alpha_3\right)^{\epsilon_3}\ldots\left(\alpha_1^{\delta_{2m}}\alpha_2^{\delta_{1m}}\alpha_m\right)^{\epsilon_m}\right)$$

(divided possibly by $\pm$ a product of some of the k_i), where $\eta_1 = \epsilon_1 + \sum_{j=3}^m \delta_{2j}\epsilon_j$ reduced modulo 2, and $\eta_2 = \epsilon_2 + \sum_{j=3}^m \delta_{1j}\epsilon_j$ reduced modulo 2.

Now $[\alpha_1^{\delta_{23}}\alpha_2^{\delta_{13}}\alpha_3, \ldots, \alpha_1^{\delta_{2m}}\alpha_2^{\delta_{1m}}\alpha_m] = 2^{m-2}$, as products of the $\alpha_1^{\delta_{2i}}\alpha_2^{\delta_{1i}}\alpha_i$ $(3 \leq i \leq m)$ yield $\boldsymbol{F}$-multiples of precisely 2^{m-2} of the basis elements $\alpha_1^{\epsilon_1}, \ldots, \alpha_m^{\epsilon_m}$ of C.

So $\dim C = 2^2 \times 2^{m-2} = \dim[\alpha_1, \alpha_2][\alpha_1^{\delta_{23}}\alpha_2^{\delta_{13}}\alpha_3, \ldots, \alpha_1^{\delta_{2m}}\alpha_2^{\delta_{1m}}\alpha_m]$. Also, as is easily verified, α_1 and α_2 commute with each $\alpha_1^{\delta_{2i}}\alpha_2^{\delta_{1i}}\alpha_i$ (which is why the latter elements were chosen!). So by Lemma 6.13:

$$\begin{aligned} C &\cong [\alpha_1, \alpha_2] \otimes \left[\alpha_1^{\delta_{23}}\alpha_2^{\delta_{13}}\alpha_3, \ldots, \alpha_1^{\delta_{2m}}\alpha_2^{\delta_{1m}}\alpha_m\right] \\ &= Q_{k_1,k_2} \otimes C\left[m-2, (k_i'), (\delta_{ij}')\right] \quad \text{for some } k_i' \in F,\ \delta_{ij}' \in \{0,1\}. \end{aligned}$$

Let us find the k_i', δ_{ij}'.

k_{i-2}' is found by squaring $\alpha_1^{\delta_{2i}}\alpha_2^{\delta_{1i}}\alpha_i$ $(3 \le i \le m)$, thus

$$\begin{aligned} k_{i-2}' = &\left(\alpha_1^{\delta_{2i}}\alpha_2^{\delta_{1i}}\alpha_i\right)\left(\alpha_1^{\delta_{2i}}\alpha_2^{\delta_{1i}}\alpha_i\right) \\ = &\ \alpha_1^{\delta_{2i}}\alpha_2^{\delta_{1i}}\left(\alpha_1^{\delta_{2i}}\alpha_2^{\delta_{1i}}\alpha_i\right)\alpha_i \\ &\quad \text{(since } \alpha_1^{\delta_{2i}}\alpha_2^{\delta_{1i}}\alpha_i \text{ commutes with both } \alpha_1 \text{ and } \alpha_2) \\ = &\ (-1)^{\delta_{1i}\delta_{2i}}\alpha_1^{\delta_{2i}}\alpha_1^{\delta_{2i}}\alpha_2^{\delta_{1i}}\alpha_2^{\delta_{1i}}\alpha_i^2 \\ = &\ (-1)^{\delta_{1i}\delta_{2i}}\left(\alpha_1^2\right)^{\delta_{2i}}\left(\alpha_2^2\right)^{\delta_{1i}}\alpha_i^2 \\ = &\ (-1)^{\delta_{1i}\delta_{2i}}k_1^{\delta_{2i}}k_2^{\delta_{1i}}k_i \end{aligned}$$

which is $\pm$ a product of some of the original $k_1, \ldots, k_m$.

$\delta_{i-2,j-2}'$ is found by considering:

$$\begin{aligned} &\left(\alpha_1^{\delta_{2j}}\alpha_2^{\delta_{1j}}\alpha_j\right)\left(\alpha_1^{\delta_{2i}}\alpha_2^{\delta_{1i}}\alpha_i\right) \qquad (3 \le i < j \le m) \\ = &\ \alpha_1^{\delta_{2i}}\alpha_2^{\delta_{1i}}\left(\alpha_1^{\delta_{2j}}\alpha_2^{\delta_{1j}}\alpha_j\right)\alpha_i \\ = &\ (-1)^{\delta_{ij}}(-1)^{\delta_{2i}\delta_{1j}}(-1)^{\delta_{1i}\delta_{2j}}\alpha_1^{\delta_{2i}}\alpha_2^{\delta_{1i}}\alpha_i\alpha_1^{\delta_{2j}}\alpha_2^{\delta_{1j}}\alpha_j \\ = &\ (-1)^{\delta_{1i}\delta_{2j}+\delta_{1j}\delta_{2i}+\delta_{ij}}\left(\alpha_1^{\delta_{2i}}\alpha_2^{\delta_{1i}}\alpha_i\right)\left(\alpha_1^{\delta_{2j}}\alpha_2^{\delta_{1j}}\alpha_j\right) \end{aligned}$$

So $\delta_{i-2,j-2}' = \delta_{1i}\delta_{2j} + \delta_{1j}\delta_{2i} + \delta_{ij}$ (reduced modulo 2)

Remark 6.8. From this last result it is clear that if C is a Clifford algebra with all $\delta_{ij} = 1$, then all $\delta_{ij}' = 1$ and so the second factor in the tensor product is again a Clifford algebra.

In general however C decomposes into an algebra $\not{C}_{b_1}$, or $\mathbb{Q}_{c_1,d_1}$ tensored by a QC algebra $C[m-1$ or $m-2, (k_i'), (\delta_{ij}')]$ of dimension less than 2^m. Note that the new parameters k_i', as well as the b_1 or c_1, d_1 are each one of the original k_i, or $\pm$ a product of some of them.

Also the factors of the tensor product are given in terms of generators, m in all, which can be identified as being an "alternative" generating set taken from the basis $\{\alpha_1^{\epsilon_1}\ldots\alpha_m^{\epsilon_m}\}$. Induction on m gives the following theorem:

Theorem 6.8. *A QC algebra $C_F[m,(k_i),(\delta_{ij})] = [\alpha_1,\ldots,\alpha_m]$ (see Definition 6.8) is expressible as a tensor product over F:*

$$\begin{aligned} C \cong\ & \not{C}_{b_1} \otimes \ldots \otimes \not{C}_{b_r} \otimes \mathbb{Q}_{c_1,d_1} \otimes \ldots \otimes \mathbb{Q}_{c_s,d_s} \\ =\ & [\beta_1] \otimes \ldots \otimes [\beta_r] \otimes [\gamma_1,\delta_1] \otimes \ldots \otimes [\gamma_s,\delta_s] \text{ say} \end{aligned} \tag{6.12}$$

where $r,s \geq 0$, $r+2s=m$, and each b_i,c_j,d_k is $\pm$ a product of some of the k_i.

Each $\beta_i,\gamma_j,\delta_k$ (where $\beta_i^2=b_i$, $\gamma_j^2=c_j$, $\delta_k^2=d_k$, and all pairs commute except $\delta_i\gamma_i=-\gamma_i\delta_i$, $1\leq i\leq s$) may be taken as being, to within multiplication by $\pm$ a product of some of the k_i, one of the basis elements $\{\alpha_1^{\epsilon_1}\ldots\alpha_m^{\epsilon_m}\}$ is (to within division by $\pm$ a product of k_i's) one of $\beta_1^{\theta_1}\ldots\beta_r^{\theta_r}\gamma_1^{\phi_1}\delta_1^{\psi_1}\ldots\gamma_s^{\phi_s}\delta_s^{\psi_s}$ (each θ_i, ϕ_j, $\psi_k=0$ or 1). Thus the latter $2^{r+2s}=2^m$ elements form a new basis of C, and $(\beta_1,\ldots,\beta_r,\gamma_1,\delta_1,\ldots,\gamma_s,\delta_s)$ is a new set of generators.

The numbers r,s are invariants of C as can be deduced from the following:

Lemma 6.14. *The centre of $C=[\beta_1]\otimes\ldots\otimes[\beta_r]\otimes[\gamma_1,\delta_1]\otimes\ldots\otimes[\gamma_s,\delta_s]$ ($\beta_i,\gamma_j,\delta_k$ as in Theorem 6.8) is the 2^r dimensional sub-algebra $[\beta_1]\otimes\ldots\otimes[\beta_r]$.*

Proof. Clearly this subalgebra is contained in the centre. Conversely, let ξ be in the centre. Expressing ξ as a linear combination of the basis $\{\beta_1^{\theta_1}\ldots\beta_r^{\theta_r}\gamma_1^{\phi_1}\delta_1^{\psi_1}\ldots\gamma_s^{\phi_s}\delta_s^{\phi_s}\}$ we have

$$\xi = \sum h\beta_1^{\theta_1}\ldots\beta_r^{\theta_r}\gamma_1^{\phi_1}\delta_1^{\psi_1}\ldots\gamma_s^{\phi_s}\delta_s^{\phi_s}$$

where $h=h(\theta_1,\ldots,\theta_r,\phi_1,\psi_1,\ldots,\phi_s,\psi_s)$ is in F

For each $i=1,...,s$,

$$\xi = \gamma_i^{-1}\xi\gamma_i = \sum \pm h\beta_1^{\theta_1}\ldots\beta_r^{\theta_r}\gamma_1^{\phi_1}\delta_1^{\psi_1}\ldots\gamma_s^{\phi_s}\delta_s^{\phi_s}$$

where the sign is negative when $\psi=1$ (since γ_i commutes with all $\beta_j,\gamma_j,\delta_j$ except δ_i).

Comparison of the two expressions for ξ shows that $h=0$ for any basis element with $\psi_i=1$.

A similar argument using $\xi=\delta_i^{-1}\xi\delta_i$ shows that for each i, $h=0$ for any basis element with $\phi_i=1$.

Hence ξ is a linear combination of the $\beta_1^{\theta_1}\ldots\beta_r^{\theta_r}$ only, so that $\xi\in[\beta_1,\ldots,\beta_r]=[\beta_1]\otimes\ldots\otimes[\beta_r]$ as required. □

Remark 6.9. The converse of Theorem 6.8 is obviously also true – that is, any algebra of the form (6.12) is a QC algebra. Indeed, regarded as an algebra on the generators $\{\beta_i,\gamma_j,\delta_k\}$, C of the form (6.12) is the QC algebra $C[r+2s,(k_i'),(\delta_{ij}')]$ where $k_i',\ldots,k_{r+2s}'=b_1,\ldots,b_r,c_1,d_1,\ldots,c_s,d_s$ respectively, and all $\delta_{ij}'=0$ except $\delta_{r+2i-1,r+2i}'=1$ for $1\leq i\leq s$.

From these facts it is clear that a tensor product of a finite number of QC algebras is itself a QC algebra.

If C is a Clifford algebra, it follows from the remark 6.8 that the decomposition process splits off only $\mathbb{Q}_{c_i,d_i}$ type algebras, except for a possible final commutative algebra on one generator. In other words, r of theorem 6.8 must be 0 or 1 if C is a Clifford algebra.

Conversely, any algebra of the form (6.12) with $r = 0$ or 1 is a Clifford algebra. This can be proved by induction on s. For suppose C is a Clifford algebra on $2s$ generators $[\alpha_1, \ldots, \alpha_{2s}]$. Then

$$\begin{aligned} C \otimes \mathbb{Q}_{c,d} &= [\alpha_1, \ldots, \alpha_{2s}] \otimes [\gamma, \delta] \\ &\cong [\alpha_1, \ldots, \alpha_{2s}, \alpha_1, \ldots, \alpha_{2s}\gamma, \alpha_1, \ldots, \alpha_{2s}\delta] \end{aligned}$$

using Lemma 6.13

This is a Clifford algebra on $2s+2$ generators since, as is easily verified, $\alpha_1, \ldots, \alpha_{2s}, \alpha_1, \ldots, \alpha_{2s}\gamma, \alpha_1, \ldots, \alpha_{2s}\delta$ all anti-commute.

Similarly, again supposing C is a Clifford algebra on $2s$ generators,

$$\begin{aligned} C \otimes \mathcal{C}_b &= [\alpha_1, \ldots, \alpha_{2s}] \otimes [\beta] \\ &\cong [\alpha_1, \ldots, \alpha_{2s}, \alpha_1 \ldots \alpha_{2s}\beta] \quad \text{(using Lemma 6.13)} \end{aligned}$$

is a Clifford algebra.

Collecting these facts we have the following relationship between the classes of QC algebras and Clifford algebras over a field F of characteristic not 2.

Theorem 6.9. *The class of QC algebras over F is the smallest class which is closed under tensor products and contains the Clifford algebras corresponding to non singular quadratic forms over F.*

It is the smallest class which is closed under tensor products over F and contains the algebras $\mathcal{C}_b, Q_{c,d}$ $(b, c, d \in \boldsymbol{F})$.

The Clifford algebras are the QC algebras with 1 or 2 dimensional centres (general QC algebras having 2^r dimensional centres, r any non negative integer).

6.8 Clifford-Gastineau-Hills (CGH) Quasi Clifford Algebras

The structures of Clifford-Gastineau-Hills (CGH) algebras ($C_F[m, (k_i), (\delta_{ij})]$ with each $k_i = \pm 1$) can be deduced fairly quickly from the results of the previous sections. However, since we shall be particularly interested in explicit matrix representations of certain CGH algebras, it will be more convenient to work from the prior results – in particular Theorem 6.8.

As in [119] it is convenient to classify the possible fields F into three types:

(I) *F contains p such that $-1 = p^2$.*

(II) *F is not of type* I, *but contains p,q such that* $-1=p^2+q^2$.
(III) *F is not of type* I *or* II.

Summary 6.1. The following summary of structures and representations of $\mathcal{C}_b, \mathbb{Q}_{c,d}$ for $b,c,d=\pm 1$ is readily deduced [64, p.10]:

Table 6.4 Summary of structures and representations [64] [a]

Algebra	**FT**[b]	**S**[c]	**IR**[d]	**O**[e]
$\mathcal{C}_1=[\beta]$	any	$2F$	$\beta\mapsto(1)$ or $\beta\mapsto(-1)$	1
$\mathcal{C}_{-1}=[\beta]$ {	I	$2F$	$\beta\mapsto(p)$ or $\beta\mapsto(-p)$	1
	II or III	$\mathcal{C}$	$\beta\mapsto\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$	2
$\mathbb{Q}_{\pm1,1}=[\gamma,\delta]$	any	F_2	$\gamma\mapsto\left(\begin{smallmatrix}0&\pm1\\1&0\end{smallmatrix}\right)$, $\delta\mapsto\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)$	2
$\mathbb{Q}_{1,-1}=[\gamma,\delta]$	any	F_2	$\gamma\mapsto\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$, $\delta\mapsto\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$	2
$\mathbb{Q}_{-1,-1}=[\gamma,\delta]$ {	I	F_2	$\gamma\mapsto\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$, $\delta\mapsto\left(\begin{smallmatrix}p&0\\0&-p\end{smallmatrix}\right)$	2
	II	F_2	$\gamma\mapsto\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$, $\delta\mapsto\left(\begin{smallmatrix}p&-q\\-q&-p\end{smallmatrix}\right)$	2
	III	$\mathbb{Q}$	$\gamma\mapsto\left[\begin{smallmatrix}0&-1&0&0\\1&0&0&0\\0&0&0&-1\\0&0&1&0\end{smallmatrix}\right]$, $\delta\mapsto\left[\begin{smallmatrix}0&0&-1&0\\0&0&0&1\\1&0&0&0\\0&-1&0&0\end{smallmatrix}\right]$	4

[a] H. Gastineau-Hills [64, p.10] ©Cambridge University Press [b] field type [c] structure [d] irreducible representation [e] order

where $\mathcal{C}$ denotes the field $F[\sqrt{-1}]$ (F type II or III), and $\mathbb{Q}$ denotes the quaternion division algebra $[\gamma,\delta](\gamma^2=\delta^2=-1,\delta\gamma=-\gamma\delta)$ over F (F type III).

Remark 6.10. For fields of-type III there are irreducible representations of $\mathcal{C}_b, \mathbb{Q}_{c,d}$ $(b,c,d=\pm1)$ in which are each represented by $\{0,\pm1\}$ matrices with just one non zero entry in each row and column.

Now in the decomposition of an CGH algebra, each of the b_i,c_j,d_k of equation (6.12) is ±1. From Summary 6.1 it follows that the decomposition of an CGH algebra takes (possibly after reordering the factors) the form:

$$\begin{aligned} C=\ & [\alpha_1,\ldots,\alpha_m] \\ \cong\ & 2F\otimes\ldots\otimes 2F\otimes F_2\otimes\ldots\otimes F_2 \quad (F \text{ type I}) \\ & \text{or } 2F\otimes\ldots\otimes 2F\otimes \mathcal{C}\otimes\ldots\otimes \mathcal{C}\otimes F_2\otimes\ldots\otimes F_2 \quad (\text{type II}) \\ & \text{or } 2F\otimes\ldots\otimes 2F\otimes \mathcal{C}\otimes\ldots\otimes \mathcal{C}\otimes\mathbb{Q}\otimes\ldots\otimes\mathbb{Q}\otimes F_2\otimes\ldots\otimes F_2 \quad (\text{type III}) \\ \cong\ & [\beta_1]\otimes\ldots[\beta_r]\otimes[\gamma_1,\delta_1]\otimes\ldots\otimes[\gamma_s,\delta_s] \quad \text{say} \end{aligned} \tag{6.13}$$

where each $\beta_i,\gamma_j,\delta_k$ is $\pm$ a product of the α_i, and conversely each α_i is $\pm$ a product of the $\beta_i,\gamma_j,\delta_k$.

The following lemma contains particular cases of more general results: we draw attention to an important detail common to the proof of each part.

Lemma 6.15. *(i)* $\mathcal{C}\otimes\mathcal{C} \cong 2F\otimes\mathcal{C}$ *(F a field of type II or III),*

(ii) $\mathcal{C}\otimes\mathbb{Q} \cong \mathcal{C}\otimes F_2$ *(F type III),*

(iii) $\mathbb{Q}\otimes\mathbb{Q} \cong F_2\otimes F_2$ *(F type III).*

Proof.
(i) $\mathcal{C}\otimes\mathcal{C}$
$= \mathcal{C}_{-1}\otimes\mathcal{C}_{-1}$
$= [\beta_1]\otimes[\beta_2]$ say $(\beta_i^2=-1)$
$\cong [\beta_1,\beta_2]$
$\cong [\beta_1\beta_2]\otimes[\beta_1]$ by Lemma 6.13, since $\beta_1\beta_2,\beta_1$ commute and generate $[\beta_1,\beta_2]$
$\cong 2F\otimes\mathcal{C}$ since $(\beta_1\beta_2)^2=1$.

(ii) $\mathcal{C}\otimes\mathbb{Q}$
$= \mathcal{C}_{-1}\otimes\mathcal{C}_{-1,-1}$
$= [\beta]\otimes[\gamma,\delta]$ say $(\beta^2=-1,\ \gamma^2=\delta^2=-1,\ \delta\gamma=-\gamma\delta)$
$= [\beta,\gamma,\delta]$
$\cong [\beta]\otimes[\beta\gamma,\delta]$ by Lemma 6.13
$\cong \mathcal{C}\otimes\mathbb{Q}_{1,-1}$ since $(\beta\gamma)^2=1$
$\cong \mathcal{C}\otimes F_2$ by Summary 6.1.

(iii) $\mathbb{Q}\otimes\mathbb{Q}$
$= \mathbb{Q}_{-1,-1}\otimes\mathbb{Q}_{-1,-1}$
$= [\gamma_1,\delta_1]\otimes[\gamma_2,\delta_2]$ say $(\gamma_i^2=\delta_i^2=-1,\ \delta_i\gamma_i=-\gamma_i\delta_i)$
$= [\gamma_1,\delta_1,\gamma_2,\delta_2]$
$\cong [\gamma_1\delta_2,\delta_1]\otimes[\delta_1\gamma_2,\delta_2]$ by Lemma 6.13
$\cong \mathbb{Q}_{1,-1}\otimes\mathbb{Q}_{1,-1}$ since $(\gamma_1\delta_2)^2=(\delta_1\gamma_2)^2)=1$
$\cong F_2\otimes F_2\square$

Note that in the proof of each part of Lemma 6.15 tensor products of algebras in terms of certain generators are converted to tensor products of algebras in terms of new generators. In each case the new generators are certain products of the old, and each old generator is $\pm$ a product of the new. Hence

Corollary 6.12. *If Lemma 6.15 is applied to pairs of factors in equation* (6.13)*, the new generators are still* $\pm$ *products of the original* α_i*, and each* α_i *is* $\pm$ *a product of the new generators.*

Application of Lemma 6.15 sufficiently often to equation (6.13) yields:

$$C \cong \begin{cases} \text{(i)} \;\; 2F \otimes \ldots \otimes 2F \otimes F_2 \otimes \ldots \otimes F_2 & \text{any type of field} \\ \text{(ii)} \;\; 2F \otimes \ldots \otimes 2F \otimes \not{C} \otimes F_2 \otimes \ldots \otimes F_2 & \text{type II or III} \\ \text{(iii)} \;\; 2F \otimes \ldots \otimes 2F \otimes \mathbb{Q} \otimes F_2 \otimes \ldots \otimes F_2 & \text{type III} \end{cases} \tag{6.14}$$

If we use the fact that $\otimes$ distributes over $\oplus$, and $F_m \otimes F_n = F_{mn}$ we immediately obtain the possible Wedderburn structures of CGH algebras:

Theorem 6.10. *The Wedderburn structure of an CGH algebra $C = C[m,(k_i),(\delta_{ij})]$ $(k_i = \pm 1)$ as a direct sum of full matrix algebras over division algebras is (depending on $m,(k_i),(\delta_{ij})$) one of*

$$\begin{cases} \textit{(i)} \;\; 2^r F_{2^s} & \textit{any type of field} \\ \textit{(ii)} \;\; 2^{r-1} \not{C} \otimes F_{2^s} & \textit{type II or III} \\ \textit{(iii)} \;\; 2^r \mathbb{Q} \otimes F_{2^{s-1}} & \textit{type III,} \end{cases}$$

where in each case $r+2s = m$, and 2^r is the dimension of centre.

Conversely (as in remark 6.9) any such algebra (I), (II) or (III) is an CGH algebra $C[r+2s,(k_i),(\delta_{ij})]$ $(k_i = \pm 1)$ with respect to certain generators. Also (as in theorem 6.9) the subclass of algebras with structures (i), (ii) or (iii) for which $r \leq 1$ is precisely the class of algebras isomorphic to Clifford-Gastineau-Hills algebras on $r+2s$ generators (the generators anticommuting and squaring to ± 1).

Corollary 6.13. *In case (i) of theorem 6.10 there are 2^r inequivalent irreducible representations, of order 2^s; in case (ii) 2^{r-1} of order 2^{s+1}, and in case (iii) 2^r of order 2^{s+1}. Any representation must be of order a multiple of (i) 2^s, (ii)2^{s+1}, (iii) 2^{s+1} respectively, and any such multiple is the order of some representation.*

Explicit matrix representations may be constructed using Summary 6.1 and equation (6.14) as follows.

Consider the case when C takes the form (6.14) (i), that is.:

$$\begin{aligned} C \cong \;& 2F \otimes \ldots \otimes 2F \otimes F_2 \otimes \ldots \otimes F_2 \\ =\; & [\beta_1] \otimes \ldots \otimes [\beta_r] \otimes [\gamma_1, \delta_1] \otimes \ldots \otimes [\gamma_s, \delta_s] \;\; \text{say.} \end{aligned}$$

By Summary 6.1 we have irreducible matrix representations for each $[\beta_i]$, $[\gamma_j, \delta_j]$, of orders 1,2 respectively. Suppose $\beta_i \mapsto B_i$, $\gamma_j \mapsto C_j$ and $\delta_k \mapsto D_k$. Then a representation λ say of C is defined by setting

$$\begin{aligned} \lambda \left(\beta_1^{\theta_1} \ldots \beta_r^{\theta_r} \gamma_1^{\phi_1} \delta_1^{\psi_1} \ldots \gamma_s^{\phi_s} \delta_s^{\psi_s} \right) \\ = B_1^{\theta_1} \otimes \ldots \otimes B_r^{\theta_r} \otimes C_1^{\phi_1} D_1^{\psi_1} \otimes \ldots \otimes C_s^{\phi_s} D_s^{\psi_s} \end{aligned} \tag{6.15}$$

(each $\theta_i, \phi_j, \psi_k = 0$ or 1) where here $\otimes$ denotes the Kronecker product.

Clearly λ is of order $1 \times \cdots \times 1 \times 2 \times \cdots \times 2 = 2^s$ so by Corollary 6.13 (i) it is irreducible. The two inequivalent choices for each $[\beta_i]$ give rise to all

2^r inequivalent irreducible representations of C. Now since C is semi-simple, to within equivalence any representation μ of C may be formed from some family $\{\lambda_1, \ldots, \lambda_t\}$ of irreducible representations by defining:

$$\mu(\gamma) = \left[\begin{array}{c|c} \lambda_1(\gamma) & \bigcirc \\ \hline & \lambda_2(\gamma) \\ \bigcirc & \ddots \end{array}\right] \quad \text{for all } \gamma \text{ in } C.$$

Any matrix representation μ' equivalent to μ is of course given by $\mu'(\gamma) = T^{-1}\mu(\gamma)T$ for some non singular matrix T over F.

Representations of C in the cases (6.14)(ii), (iii) are formed similarly.

Now the class of $\{0, \pm 1\}$ matrices with just one non zero entry per row and column is closed under the operations

(a) taking $\pm$ ordinary products,
(b) taking Kronecker products,
(c) forming $\left[\begin{array}{c|c} X_1 & \bigcirc \\ \hline & X_2 \\ \bigcirc & \ddots \end{array}\right]$ from matrices $X_1, X_2, \ldots$.

So using Remark 6.10 and Corollary 6.12 the following can be deduced:

Theorem 6.11. *If F is a field of type III (-1 is not the sum of two squares) each representation of an CGH algebra $C[m, (k_i), (\delta_{ij})]$ ($k = \pm 1$) on generators (α_i) is equivalent to a matrix representation in which each α_i corresponds to a $\{0, \pm 1\}$ matrix with just one non zero entry in each row and column (an orthogonal $\{0, \pm 1\}$ matrix).*

6.9 The Order Number Theorem

We now apply the theory of Clifford-Gastineau-Hills algebras to the problem of determining the possible orders of systems of orthogonal designs of a given genus and on given numbers of variables.

Gastineau-Hills has shown that the existence of a k-system W of order n, genus $(\delta'_{ij})_{1 \le i \le j \le k}$ say ($\delta'_{ij} \in \{0, 1\}$), on $p_1 + 1, p_2, \ldots, p_k$ variables (each $p_i \ge 0$), implies the existence of an order n representation of a certain real algebra, C say, on $p_1 + p_2 + \cdots + p_k$ generators (see [63, Ch.7]). In fact C is the algebra on generators $\alpha_{11}, \ldots, \alpha_{1p_1}, \alpha_{21}, \ldots, \alpha_{2p_2}, \ldots, \alpha_{k_1}, \ldots, \alpha_{kp_k}$ say with defining equations:

$$\begin{cases} \alpha_{ij}^2 = (-1)^{\delta'_{1i}} & \\ \alpha_{ik}\alpha_{ij} = -\alpha_{ij}\alpha_{ik} & (j \ne k) \\ \alpha_{j\ell}\alpha_{ik} = (-1)^{\delta'_{1i} + \delta'_{1j} + \delta'_{ij}} \alpha_{ik}\alpha_{j\ell} & (i < j) \text{ (where } \delta'_{11} \text{ is taken as 1)} \end{cases} \tag{6.16}$$

We have used δ'_{ij} here to avoid confusion with the parameters δ_{ij} of theorem 6.10 which is to be used immediately].

Thus C is an CGH algebra with respect to the generators α_{ij} and the results of Section 6.8 apply.

From Theorem 6.10 and Corollary 6.13 we deduce that the possible orders of the system W are restricted to multiples of a certain integer, ρ say, where $\rho = 2^s, 2^{s+1}, 2^{s+1}$ according to whether the C of 6.16 has structure 6.10(i),(ii),(iii) respectively. Here the F of 6.10 is the reals (a field of type III), the m of 6.10 is $p_1 + \cdots + p_k$, and each k_i of 6.10 may be expressed easily in terms of the δ'_{ij}.

We have in effect described an algorithm whereby, given $p_1 + 1, p_2, \ldots, p_k$ and (δ'_{ij}), a corresponding number ρ , a power of 2, may be computed. We may regard ρ as being determined by the family $(p_1 + 1, p_2, \ldots, p_k; (\delta'_{ij}\ 1 \le i \le j \le k)$ and we make the following definition.

Definition 6.10. The *order number* of the family $(p_1 + 1, p_2, \ldots, p_k; (\delta'_{ij})_{1 \le i \le j \le k})$ $(p_i \ge 0, \delta'_{ij} \in \{0, 1\})$ is the order of the irreducible representations of the algebra (6.16) (all irreducible representations of (6.16) having the same order – a power of 2).

Thus a k-system W of genus $(\delta'_{ij})_{1 \le i \le j \le k}$ on $p_1 + 1, p_2, \ldots, p_k$ variables must have order a multiple of the order number of the family $\left(p_1 + 1, p_2, \ldots, p_k; (\delta'_{ij})\right)$.

We wish to show that conversely any multiple of the order number of $(p_1 + 1, p_2, \ldots, p_k; (\delta'_{ij}))$ is the order of some k-system W of genus (δ'_{ij}) on $p_1 + 1, p_2, \ldots, p_k$ variables. We wish to show further that the system W may be chosen to be *regular*, and of type $(1, 1, \ldots; 1, 1, \ldots; \ldots)$.

Let n be any multiple of the order number of $\left(p_1 + 1, p_2, \ldots, p_k; (\delta'_{ij})\right)$. By Corollary 6.13 there is an order n representation of the algebra (6.16), and by theorem 6.11 we may take the α_{ij} as each being represented by an order n, $\{0, \pm 1\}$ matrix, E_{ij} say, with just one non zero entry per row and column. §6.8 contains a description of how such a matrix representation may be constructed].

The matrices E_{ij} satisfy:

$$\begin{cases} E_{ij}^2 = (-1)^{\delta'_{1i}} I \\ E_{ik} E_{ij} = -E_{ij} E_{ik}\,, & (j \ne k) \\ E_{j\ell} E_{ik} = (-1)^{\delta'_{1i} + \delta'_{1j} + \delta'_{ij}} E_{ik} E_{j\ell} & (i < j)\ (\text{where } \delta'_{11} = 1) \end{cases}$$

Also the matrices E_{ij} are orthogonal.

It follows that $E_{ij}^\top = (-1)^{\delta'_{1i}} E_{ij}$ for all i, j. Since $\delta'_{11} = 1$, all E_{1j} are anti-symmetric, so $I * E_{1j} = 0$. Also if $1 \le j < k \le p_i$, then:

$$E_{ik} E_{ij}^\top = (-1)^{\delta'_{1i}} \quad E_{ik} E_{ij} = -(-1)^{\delta'_{1i}} \quad E_{ij} E_{ik} = -E_{ij} E_{ik}^\top$$

Since E_{ij}, E_{ik} each have only one non-zero entry per row it follows that $E_{ij} * E_{ik} = 0$ [This is essentially a particular case of lemma 6.11, since ($X_1 = x_1 E_{ij}$, $X_2 = x_2 E_{ik}$) is a 2-system of type (1;1) on the variables $(x_1; x_2)$, with $X_2 X_1^\top = -X_1 X_2^\top$].

Hence we may form designs:

$$\begin{aligned} X_1 &= x_{10} I + x_{11} E_{11} + \cdots + x_{1p_1} E_{1p_1}\,, \\ X_2 &= x_{21} E_{21} + \cdots + x_{2p_2} E_{2p_2}\,, \\ &\vdots \\ X_k &= x_{k1} E_{k1} + \cdots + x_{kp_k} E_{kp_k}\,. \end{aligned}$$

Now

$$E_{1j} I^\top = -I E_{1j}^\top\,,\ \ E_{ik} E_{ij}^\top = -E_{ij} E_{ik}^\top;\ (j \neq k)\,,\ \ E_{ij} E_{ij}^\top = (-1)^{\delta'_{1i}} E_{ij}^2 = I\,.$$

It follows that:

$$X_i X_i^\top = \sum_j x_{ij}^2 I$$

so that each design X_i is an orthogonal design, of type $(1,1,\ldots)$.

Since for $i < j$

$$\begin{aligned} E_{j\ell} E_{ik}^\top &= (-1)^{\delta'_{1i}} E_{j\ell} E_{ik} \\ &= (-1)^{\delta'_{1i} + \delta'_{1i} + \delta'_{1j} + \delta'_{ij}} E_{ik} E_{j\ell} \\ &= (-1)^{\delta'_{ij}} E_{ik} E_{j\ell}^\top \end{aligned}$$

it follows that

$$X_j X_i^\top = (-1)^{\delta'_{ij}} X_i X_j^\top\,.$$

So $(X_1, \ldots, X_k)$ is a k-system of order n, genus $(\delta'_{ij})_{1 \leq i < j \leq k}$. Its type is $(1,1,\ldots;1,1,\ldots;\ldots)$ so by lemma 6.11 it is regular.

We have shown:

Theorem 6.12. *Suppose p is the order number of the family $(p_1+1, p_2, \ldots, p_k; (\delta_{ij})_{1 \leq i < j \leq k})$ (p_i integers ≥ 0, $\delta_{ij} \in \{0,1\}$). Then any k-system of any type, genus (δ_{ij}), on $p_1+1, p_2, \ldots, p_k$ variables, has order a multiple of ρ. If n is a multiple of ρ there is a regular k-system of order n, type $(1,1,\ldots;1,1,\ldots;\ldots)$, genus (δ_{ij}) on $p_1+1, p_2, \ldots, p_k$ variables.*

[We have renamed δ'_{ij} as δ_{ij} in the statement of this theorem.]

Note that this theorem does not give information on which multiples of the order p are the possible orders of k-systems (of genus (δ_{ij} on $p_1+1, p_2, \ldots, p_k$ variables) for types other than $(1,1,\ldots;1,1,\ldots;\ldots)$.

Note also that while the second part of this theorem merely asserts the existence of systems with certain properties, we have in fact developed a

technique whereby such systems may easily be constructed. The following example illustrates the method:

Example 6.9. We find the possible orders of *product designs* (as defined in definition 6.3) on $(2,2,4)$ variables, and construct such a product design for each of these orders.

The algebras corresponding to product designs (see 6.3) have been explicitly determined earlier. In the case of $(2,2,4)$ variables we have an algebra C on $1+2+4=7$ generators (see equation (6.16)) $\alpha,\beta_1,\beta_2,\gamma_1,\gamma_2,\gamma_3,\gamma_4$ say, with defining equations

$$\begin{cases} \alpha^2=\beta_j^2=\gamma_k^2=-1 \\ \beta_2\beta_1=-\beta_1\beta_2\,, \quad \gamma_j\gamma_i=-\gamma_i\gamma_j \quad (i\neq j) \\ \beta_j\alpha=-\alpha\beta_j\,, \quad \gamma_j\alpha=-\alpha\gamma_j\,, \quad \gamma_j\beta_i=\beta_i\gamma_j\,. \end{cases}$$

Now

$$\begin{aligned} C &= [\alpha,\beta_1,\beta_2,\gamma_1,\gamma_2,\gamma_3,\gamma_4] \\ &\cong [\beta_1,\beta_2]\otimes[\gamma_1,\gamma_2]\otimes[\gamma_1\gamma_2\gamma_3,\gamma_1\gamma_2\gamma_4]\otimes[\alpha\beta_1\beta_2\gamma_1\gamma_2\gamma_3\gamma_4] \end{aligned}$$

(by lemma 6.13 – an algorithm which yields this or an alternative such decomposition is described in Section 6.7)

$$\begin{aligned} &\cong \mathbb{Q}_{-1,-1}\otimes\mathbb{Q}_{-1,-1}\otimes\mathbb{Q}_{-1,-1}\otimes \not{C}_1 \\ &\cong \mathbb{Q}\otimes\mathbb{Q}\otimes F_2\otimes 2F \qquad \text{(by (16.1))} \\ &\cong [\beta_1\gamma_2,\beta_2]\otimes[\beta_2\gamma_1,\gamma_2]\otimes[\gamma_1\gamma_2\gamma_3,\gamma_1\gamma_2\gamma_4]\otimes[\alpha\beta_1\beta_2\gamma_1\gamma_2\gamma_3\gamma_4] \end{aligned}$$

(using the technique in the proof of Lemma 6.15 part (iii))

$$\begin{aligned} &\cong Q_{1,-1}\otimes Q_{1,-1}\otimes F_2\otimes 2F \\ &\cong F_2\otimes F_2\otimes F_2\otimes 2F \quad \text{(Summary 6.1)} \\ &\cong 2F_{2^3} \end{aligned}$$

So by theorem 6.10(i) and corollary 6.13(i) the order number is $2^3=8$, and the possible orders of product designs on $(2,2,4)$ variables are the multiples of 8.

Such a product design of minimal order 8 may be constructed as follows:

We first find a suitable order 8 matrix representations for $\alpha,\beta_1,\beta_2,\gamma_1,\ldots,\gamma_4$ using the technique described in §6.8. To do this we express each of the $\alpha,\beta_1,\beta_2,\gamma_1,\ldots,\gamma_4$ in the form

$$\pm(\beta_1\gamma_2)^{\phi_1}\,\beta_2^{\psi_1}\,(\beta_2\gamma_1)^{\phi_2}\,\gamma_2^{\psi_2}\,(\gamma_1\gamma_2\gamma_3)^{\phi_3}\,(\gamma_1\gamma_2\gamma_4)^{\psi_3}\,(\alpha\beta_1\beta_2\gamma_1\gamma_2\gamma_3\gamma_4)^{\theta}$$

(each $\theta,\phi_j,\psi_k=0$ or 1)

For example

$$\alpha = \pm(\beta_1\gamma_2)^1\,\beta_2^0\,(\beta_2\gamma_1)^1\,\gamma_2^0\,(\gamma_1\gamma_2\gamma_3)^1\,(\gamma_1\gamma_2\gamma_4)^1\,(\alpha\beta_1\beta_2\gamma_1\gamma_2\gamma_3\gamma_4)^1$$

is found by solving

$$\left.\begin{aligned}
\theta &\equiv 1\\
\phi_1+\theta &\equiv 0\\
\psi_1+\phi_2+\theta &\equiv 0\\
\phi_2+\phi_3+\psi_3+\theta &\equiv 0\\
\phi_1+\psi_2+\phi_3+\psi_3+\theta &\equiv 0\\
\phi_3+\theta &\equiv 0\\
\psi_3+\theta &\equiv 0
\end{aligned}\right\} \text{ modulo 2.}$$

(in fact the sign is $-$, but this is unimportant). So

$$\alpha = \pm(\beta_1\gamma_2)\times(\beta_2\gamma_1)\times(\gamma_1\gamma_2\gamma_3)\,(\gamma_1\gamma_2\gamma_4)\times(\alpha\beta_1\beta_2\gamma_1\gamma_2\gamma_3\gamma_4)$$

$$\to \begin{bmatrix}0&1\\1&0\end{bmatrix}\otimes\begin{bmatrix}0&1\\1&0\end{bmatrix}\otimes\begin{bmatrix}0&-1\\1&0\end{bmatrix}\otimes(1) \quad \text{(using [63, 16.1–cf. 16.9])}$$

$$= \begin{bmatrix} & & & & 0 & 0 & 0 & -1\\ & & & & 0 & 0 & -1 & 0\\ & \bigcirc & & & 0 & -1 & 0 & 0\\ & & & & -1 & 0 & 0 & 0\\ 0&0&0&1 & & & & \\ 0&0&1&0 & & \bigcirc & & \\ 0&1&0&0 & & & & \\ 1&0&0&0 & & & & \end{bmatrix} = E \text{ say.}$$

Similarly,

$$\beta_1 = \pm(\beta_1\gamma_2)\times\gamma_2\times 1\times 1$$

$$\to \begin{bmatrix}0&1\\1&0\end{bmatrix}\otimes\begin{bmatrix}0&-1\\1&0\end{bmatrix}\otimes\begin{bmatrix}1&0\\0&1\end{bmatrix}\otimes(1)$$

$$= \begin{bmatrix} 0&0&0&-1 & & & & \\ 0&0&-1&0 & & \bigcirc & & \\ 0&1&0&0 & & & & \\ 1&0&0&0 & & & & \\ & & & & 0&0&0&-1\\ & \bigcirc & & & 0&0&-1&0\\ & & & & 0&1&0&0\\ & & & & 1&0&0&0 \end{bmatrix} = F_1 \text{ say.}$$

$$\beta_2 = \pm\beta_2 \times 1 \times 1 \times 1$$

$$\to \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes (1)$$

$$= \begin{bmatrix} 0 & -1 & 0 & 0 & & & & \\ 1 & 0 & 0 & 0 & & & & \\ 0 & 0 & 0 & -1 & & & & \\ 0 & 0 & 1 & 0 & & & & \\ & & & & 0 & -1 & 0 & 0 \\ & & & & 1 & 0 & 0 & 0 \\ & & & & 0 & 0 & 0 & -1 \\ & & & & 0 & 0 & 1 & 0 \end{bmatrix} = F_2 \text{ say.}$$

$$\gamma_1 = \pm\beta_2 \times (\beta_2\gamma_1) \times 1 \times 1$$

$$\to \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes (1)$$

$$= \begin{bmatrix} 0 & 0 & 0 & -1 & & & & \\ 0 & 0 & 1 & 0 & & & & \\ 0 & -1 & 0 & 0 & & & & \\ 1 & 0 & 0 & 0 & & & & \\ & & & & 0 & 0 & 0 & -1 \\ & & & & 0 & 0 & 1 & 0 \\ & & & & 0 & -1 & 0 & 0 \\ & & & & 1 & 0 & 0 & 0 \end{bmatrix} = G_1 \text{ say.}$$

$$\gamma_2 = \pm 1 \times \gamma_2 \times 1 \times 1$$

$$\to \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes (1)$$

$$= \begin{bmatrix} 0 & 0 & -1 & 0 & & & & \\ 0 & 0 & 0 & -1 & & & & \\ 1 & 0 & 0 & 0 & & & & \\ 0 & 1 & 0 & 0 & & & & \\ & & & & 0 & 0 & -1 & 0 \\ & & & & 0 & 0 & 0 & -1 \\ & & & & 1 & 0 & 0 & 0 \\ & & & & 0 & 1 & 0 & 0 \end{bmatrix} = G_2 \text{ say.}$$

$$\gamma_3 = \pm\beta_2 \times (\beta_2\gamma_1)\gamma_2 \times (\gamma_1\gamma_2\gamma_3) \times 1$$

$$\to \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \otimes \left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right) \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes 1$$

$$= \begin{bmatrix} & & & \\ & \bigcirc & & \\ & & & \\ & & & \end{bmatrix} \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix} = G_3 \text{ say.}$$

$$\begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} & & & \\ & \bigcirc & & \\ & & & \\ & & & \end{bmatrix}$$

And $\gamma_4 = \pm\beta_2 \times (\beta_2\gamma_1)\gamma_2 \times (\gamma_1\gamma_2\gamma_4) \times 1$

$$\to \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \otimes \left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right) \otimes \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \otimes (1)$$

$$= \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} & & & \\ & \bigcirc & & \\ & & & \\ & & & \end{bmatrix} \begin{bmatrix} & & & \\ & & & \\ & \bigcirc & & \\ & & & \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = G_4 \text{ say.}$$

Set $X = x_0 I + x_1 E$

$Y = y_1 F_1 + y_2 F_2$

$Z = z_1 G_1 + z_2 G_2 + z_3 G_3 + z_4 G_4$.

Then (X, Y, Z) is the following product design $POD(8:1,1;1,1;1,1,1,1)$ on $2, 2, 4$ variables):

$$\begin{bmatrix}
x_0 & \bar{y}_2\bar{z}_4 & \bar{z}_2 & \bar{y}_1\bar{z}_1 & 0 & \bar{z}_3 & 0 & \bar{x}_1 \\
y_2z_4 & x_0 & \bar{y}_1z_1 & \bar{z}_2 & z_3 & 0 & \bar{x}_1 & 0 \\
z_2 & y_1\bar{z}_1 & x_0 & \bar{y}_2z_4 & 0 & \bar{x}_1 & 0 & z_3 \\
y_1z_1 & z_2 & y_2\bar{z}_4 & x_0 & \bar{x}_1 & 0 & \bar{z}_3 & 0 \\
0 & \bar{z}_3 & 0 & x_1 & x_0 & \bar{y}_2z_4 & \bar{z}_2 & \bar{y}_1\bar{z}_1 \\
z_3 & 0 & x_1 & 0 & y_2\bar{z}_4 & x_0 & \bar{y}_1z_1 & \bar{z}_2 \\
0 & x_1 & 0 & z_3 & z_2 & y_1\bar{z}_1 & x_0 & \bar{y}_2\bar{z}_4 \\
x_1 & 0 & \bar{z}_3 & 0 & y_1z_1 & z_2 & y_2z_4 & x_0
\end{bmatrix}$$

[we have superimposed X, Y, Z as in §6.4].

Finally we note that

$$(X \otimes I_t, Y \otimes I_t, Z \otimes I_t) = \left[\begin{bmatrix} X & & \bigcirc \\ & X & \\ \bigcirc & & \ddots \end{bmatrix}, \begin{bmatrix} Y & & \bigcirc \\ & Y & \\ \bigcirc & & \ddots \end{bmatrix}, \begin{bmatrix} Z & & \bigcirc \\ & Z & \\ \bigcirc & & \ddots \end{bmatrix} \right]$$

is a product design of order 8, type $(1,1;1,1;1,1,1,1)$ on $2,2,4$ variables.

6.10 Periodicity

By considering a suitable *CGH* algebra we are now able, given $(p_1+1, p_2, \ldots, p_k; (\delta_{ij}))$, to calculate the order number ρ, and to construct regular k-systems of order any multiple of ρ, genus (δ_{ij}), type $(1,1,\ldots;1,1,\ldots;\ldots)$, on $(p_1+1, p_2, \ldots, p_k$ variables.

In practice we may wish to produce tables of order number of families $(p_1+1, p_2, \ldots, p_k; (\delta_{ij}))$ for fixed k and (δ_{ij}) but varying p_i. The following result is useful in this context:

Theorem 6.13 (Periodicity 8 Lam [142, Prop.4.2 p.127]). *If ρ is the order number (see 6.10) of $(p_1+1, p_2, \ldots, p_k; (\delta_{ij}))$ $(p_i \geq 0,\ \delta_{ij} \in \{0,1\})$, then the order number of each of $(p_1+9, p_2, \ldots, p_k; (\delta_{ij}))$, $(p_1+1, p_2+8, \ldots, p_k; (\delta_{ij}))$, $\ldots, (p_1+1, p_2, \ldots, p_{k-1}, p_k+8; (\delta_{ij}))$ is $2^4\rho$.*

[That is, increasing any p_i by 8 multiplies the order number by 16. This means that from a table giving order numbers for the 8^k cases $0 \leq p_i \leq 7$, the order number for any other values of (p_i) is readily calculated.]

Proof. Let $C = [\alpha_1, \ldots, \alpha_m]$ be the *CGH* algebra (6.16) corresponding to $(p_1+1, p_2, \ldots, p_k; (\delta_{ij}))$ [where $m = p_1, p_2, \ldots, p_k$, and $\alpha_1, \ldots, \alpha_m$ are $\alpha_{11}, \ldots, \alpha_{1p_1}$, $\alpha_{21}, \ldots, \alpha_{2p_2}, \ldots, \alpha_{k1}, \ldots, \alpha_{kp_k}$ respectively]. Let C' be the corresponding *CGH* algebra when p_j say is increased by 8. It is clear that C' will have $m+8$ generators, m of which may be identified with the generators of C, so that we may write

$$C' = [\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_8 .]$$

It is also clear that the $\beta_1,\ldots,\beta_8$ (may be chosen to) anti-commute with each other, and all square to 1 or all square to -1; also that each α_i either commutes with all of $\beta_1,\ldots,\beta_8$ or anti-commutes with all of them (in the notation of (6.16), $\beta_1,\ldots,\beta_8$ would be a $\alpha_{jp_{j+1}},\ldots,\alpha_{jp_j+8}$ respectively).

$$\text{Set } \epsilon_i = \begin{cases} 0 & \text{if } \alpha_i \text{ commutes with the } \beta_1,\ldots,\beta_8, \\ 1 & \text{otherwise,} \quad (i=1,\ldots,m). \end{cases}$$

Then clearly $\alpha_i(\beta_1,\ldots,\beta_8)^{\epsilon_i}$ commutes with each of $\beta_1,\ldots,\beta_8$. From lemma 6.13 it follows that

$$\begin{aligned} C' &\cong \left[\alpha_1(\beta_1,\ldots,\beta_8)^{\epsilon_1},\ldots,\alpha_m(\beta_1,\ldots,\beta_8)^{\epsilon_m}\right] \otimes [\beta_1,\ldots,\beta_8] \\ &= C" \otimes [\beta_1,\ldots,\beta_8] \text{ say.} \end{aligned}$$

Now it is easy to verify $(\alpha_i(\beta_1,\ldots,\beta_8)^{\epsilon_i})^2 = \alpha_i^2$, and that $\alpha_i(\beta_1,\ldots,\beta_8)^{\epsilon_i}$ commutes or anti-commutes with $\alpha_j(\beta_1,\ldots,\beta_8)^{\epsilon_j}$ according as α_i commutes or anti-commutes with α_j So $C'' \cong C$, and $C' \cong C \otimes [\beta_1,\ldots,\beta_8]$.

Let us now decompose $[\beta_1,\ldots,\beta_8]$:

$$\begin{aligned} [\beta_1,\ldots,\beta_8] &\cong [\beta_1,\beta_2] \otimes [\beta_1\beta_2\beta_3, \beta_1\beta_2\beta_4] \otimes [\beta_1\beta_2\beta_3\beta_4\beta_5, \beta_1\beta_2\beta_3\beta_4\beta_6] \\ &\qquad \otimes [\beta_1\beta_2\beta_3\beta_4\beta_5\beta_6\beta_7, \beta_1\beta_2\beta_3\beta_4\beta_5\beta_6\beta_8] \\ &\cong \begin{cases} F_2 \otimes Q \otimes F_2 \otimes Q & \text{if all } \beta_i^2 = 1, \\ Q \otimes F_2 \otimes Q \otimes F_2 & \text{if all } \beta_i^2 = -1, \text{ using Summary 6.1} \end{cases} \\ &\cong F_2 \otimes F_2 \otimes F_2 \otimes F_2 \quad \text{using Lemma 6.15 part (iii)} \\ &\cong F_{2^4}. \end{aligned}$$

Hence $C' \cong C \otimes F_{2^4}$. So if the structure of C is $2^k D \otimes F_n$ (D a division algebra) then the structure of C' is $2^k D \otimes F_{2^4 n}$. The result follows, using theorem 6.10 and corollary 6.13. □

It may be remarked that the process of constructing a CGH algebra from a k-system $(X_1,\ldots,X_k)$ on $(p_1+1,p_2,\ldots,p_k)$ variables, (as described in §6.6) seems to involve a certain lack of symmetry, in that while any of $p_2,\ldots,p_k$ could be zero, it would appear that p_1+1 cannot. For in the derivation of the algebra (6.16), the substitutions which use u_{10}, A_{10} depend on X_1 having at least the variable x_{10}.

However this restriction (on the number of variables in X_1) may be removed - provided at least *one* of $X_1,\ldots,X_k$ is non zero - since in (6.16) instead of u_{10}, A_{10} we could just as well use $u_{i_0 j_0}, A_{i_0 j_0}$ for any other i_0, j_0 ($x_{i_0 j_0}$ being one of the variables). Different CGH algebras may arise in this way (according to the choice of i_0, j_0), but they would have the same order irreducible representations (since as in Definition 6.10 each such order is the minimal order of the same class of k-systems). So the possible orders of k-systems of genus $(\delta_{ij})_{1\le i<j\le k}$ on $0, p_2,\ldots,p_k$ variables ($p_2,\ldots,p_k$ not all zero) may

be computed by looking at a *CGH* algebra constructed using a suitable alternative to Equation 6.8. Furthermore, as in theorem 6.13, the minimal order would be $\frac{1}{16}^{\text{th}}$ of the minimal order of k-systems of genus (δ_{ij}) on $8, p_2, \ldots, p_k$.

Thus we make the following extension to definition 6.10:

Definition 6.11. The order number of the family $(0, p_2, \ldots, p_k; (\delta_{ij})_{1 \le i < j \le k}$ is $\frac{1}{16}^{\text{th}}$ of the order number (as defined in 6.10) of $(8, p_2, \ldots, p_k; (\delta_{ij}))$.

Now theorem 6.12 remains valid even for $p_1 + 1 = 0$ (provided some of $p_2, \ldots, p_k$ are non zero). Actually in definition 6.11 we have not excluded the possibility that all of $p_2, \ldots, p_k$ are zero. In this case the order number is the rather strange value 2^{-1}, since the order number of $(8, 0, \ldots, 0; (\delta_{ij}))$ is 2^3.

[To see this, note that the algebra (6.9) corresponding to $(8, 0, \ldots, 0; (\delta_{ij}))$ is on 7 generators, $\alpha_1, \ldots, \alpha_7$ say, with defining equations $\alpha_i^2 = -1$, $\alpha_j \alpha_i = -\alpha_i \alpha_j$ $(i < j)$, and that:

$$
\begin{aligned}
[\alpha_1, \ldots, \alpha_7] &\cong [\alpha_1, \alpha_2] \otimes [\alpha_1\alpha_2\alpha_3, \alpha_1\alpha_2\alpha_4] \otimes [\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5, \alpha_1\alpha_2\alpha_3\alpha_4\alpha_6] \\
&\qquad \otimes [\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5\alpha_6\alpha_7] \qquad \text{decomposition} \\
&\cong Q_{-1,-1} \otimes Q_{1,1} \otimes Q_{-1,-1} \otimes \not{C}_1 \\
&\cong Q \otimes F_2 \otimes Q \otimes 2F \qquad \text{(by Summary 6.1)} \\
&\cong F_2 \otimes F_2 \otimes F_2 \otimes 2F \\
&\cong 2F_{2^3}
\end{aligned}
$$

giving order number 2^3.

We have just proved algebraically the well known fact that the minimal order of single orthogonal designs on eight variables is 8 - see [80, Ch.4]].

Theorem 6.12 may not be enhanced by allowing *all* of $p_1 + 1, p_2, \ldots, p_k$ to be 0, with order number 2^{-1}, but theorem 6.13 remains valid in all cases. For it is easy to show that not only $(8, p_2, \ldots, p_k; (\delta_{ij}))$, but each of $(0, p_2 + 8, p_3, \ldots, p_k; (\delta_{ij}))$,$\ldots$,$(0, p_2, \ldots, p_{k-1}, p_k + 8; (\delta_{ij}))$ has order number 16 times that of $(0, p_2, \ldots, p_k; (\delta_{ij}))$.

For example the order number of $(0, p_2 + 8, p_3, \ldots, p_k; (\delta_{ij})) = \frac{1}{16}$ that of $(8, p_2 + 8, \ldots, p_k; (\delta_{ij})) = 16 \times \frac{1}{16}$ that of $(8, p_2, \ldots, p_k; (\delta_{ij}))$ (by 6.13) $= 16\times$ that of $(8, p_2, \ldots, p_k; (\delta_{ij}))$.

Incorporating the extension 6.11 of the definition 6.10 and the subsequent observations into both 6.12 and 6.13 gives the following, which "improves" 6.12, 6.13 by restoring symmetry (we replace $p_1 + 1$ by p_1):

Theorem 6.14 (Gastineau-Hills). *Let $p_i \ge 0$ $(1 \le i \le k)$, $\delta_{ij} \in \{0, 1\}$ $(1 \le i < j \le k)$. The order number ρ of the family $(p_1, \ldots, p_k; (\delta_{ij})_{1 \le i < j \le k}$, as defined in 6.10, 6.11, is the minimal order of k-systems of genus (δ_{ij}) on $p_1, \ldots, p_k$ variables if some p_i is non zero – and in this case each multiple of ρ is the order of some regular k-system of genus (δ_{ij}), type $(1, 1, \ldots; 1, 1, \ldots; \ldots)$, on $p_1, \ldots, p_k$ variables – and is 2^{-1} if all $p_i = 0$. The order number of each of*

$(p_1+1,p_2,\dots,p_k;(\delta_{ij}))$,…,$(p_1,\dots,p_{k-1},p_k+8;(\delta_{ij}))$ is $2^4\rho$, for all cases of $p_i \geq 0$.

So given k and $(\delta_{ij})_{1\leq i<j\leq k}$ we may form tables of order numbers of the families $(p_1,\dots,p_k;(\delta_{ij}))$ for the 8^k cases $0 \leq p_i \leq 7$, and the order numbers in cases where some $p_i \geq 8$ are immediately deducible.

As we shall soon see it is convenient to allow for k-systems $(X_1,\dots,X_k)$ in which some designs (in particular X_1) may have no variables (such a k-system may be identified in an obvious way with an ℓ-system for some $\ell < k$).

Theorem 6.14 effectively gives a complete generalization of the well known "Radon bounds" for single orthogonal designs to the case of arbitrary k-systems of orthogonal designs.

6.11 Orders of Repeat Designs

As an illustration of the techniques that we have developed, we shall now obtain a complete answer to the question of what are the possible orders of repeat designs on given numbers of variables. Now those other systems which have been explicitly used in the previous literature (single orthogonal designs, amicable sets, and product designs) may be identified as special cases of repeat designs (see §6.4). So we shall get as immediate corollaries complete answers to the questions of what are the possible orders for given numbers of variables of those other systems.

We have already found explicitly the CGH algebra corresponding to a repeat design $(X,Y_1,\dots,Y_k,Z)$ (defined in 6.5) in $p+1,q_1,\dots,q_k,r$ variables $(p,q_i,r,\geq 0)$. It is the algebra C say on $p+q_1+\dots+q_k+r$ generators $\alpha_i(1 \leq i \leq p)$, $\beta_{ij}(1 \leq j \leq p_i, 1 \leq i \leq k)$, $\gamma_i(1 \leq i \leq r)$ satisfying the equations (6.7).

$$\text{Let } \ell = [p/2], \qquad m_i = [q_i/2]\ (1 \leq i \leq k), \qquad n = [r/2]$$
$$([\ ] \text{ here meaning "the integral part of"})$$

so that $p = 2\ell(+1)$, $q_i = 2m_i(+1)$ $(1 \leq i \leq k)$, $r = 2n(+1)$ (in each case the "+1" being present when the left hand side is odd).

Let j be how many of $q_1,\dots,q_k$ are odd – so $0 \leq j \leq k$. By reordering the $Y_1,\dots,Y_k$ if necessary, we may assume that $q_1,\dots,q_j$ are odd, and $q_{j+1},\dots,q_k$ are even.

It is convenient to rename the generators of C as follows:
Write $\alpha_1,\bar{\alpha}_1,\dots,\alpha_\ell,\bar{\alpha}_\ell,(\bar{\bar{\alpha}})$ for $\alpha_1,\alpha_2,\dots,\alpha_{2\ell-1},\alpha_{2\ell}(,\alpha_{2\ell+1})$ respectively.
$\beta_{i1},\bar{\beta}_{i1},\dots,\beta_{im_i},\bar{\beta}_{im_i},(\bar{\bar{\beta}}_i)$ for $\beta_{i1},\beta_{i2},\dots,\beta_{2m_i-1},\beta_{2m_i}(,\beta_{2m_i+1})$ respectively $(1 \leq i \leq k)$, and $\gamma_1,\bar{\gamma}_1,\dots,\gamma_n,\bar{\gamma}_n,(\bar{\bar{\gamma}})$ for $\gamma_1,\gamma_2,\dots,\gamma_{2n-1},\gamma_{2n}(,\gamma_{2n+1})$ respectively.

So

$$C = [\alpha_1, \bar{\alpha}_1, \ldots, \alpha_\ell, \bar{\alpha}_\ell, \beta_{11}, \bar{\beta}_{11}, \ldots, \beta_{1m_1}, \bar{\beta}_{1m_1}, \ldots,$$
$$\beta_{k1}, \bar{\beta}_{k1}, \ldots, \beta_{km_k}, \bar{\beta}_{km_k}, \gamma_1, \bar{\gamma}_1, \ldots,$$
$$\gamma_n, \bar{\gamma}_n, (\bar{\bar{\alpha}}), \bar{\bar{\beta}}_1, \ldots, \bar{\bar{\beta}}_j, (\bar{\bar{\gamma}})]$$

(Where $\bar{\bar{\alpha}}, \bar{\bar{\gamma}}$ respectively are present when p, r respectively are odd, and some $\bar{\bar{\beta}}_i$ are present when $j > 0$).

From equation (6.7) all the "α" generators and all the "β" generators square to -1, while all the "γ" generators are square to 1. Also all pairs of distinct generators anti-commute except that for $i \neq j$ each of $\beta_{i1}, \bar{\beta}_{i1}, \ldots, \beta_{im_i}, \bar{\beta}_{im_i}, (\bar{\bar{\beta}}_i)$ commutes with each of $\beta_{j1}, \bar{\beta}_{j1}, \ldots, \beta_{jm_j}, \bar{\beta}_{jm_j}, (\bar{\bar{\beta}}_j)$.

Let
$$\alpha = \alpha_1 \bar{\alpha}_1 \ldots \bar{\alpha}_\ell \alpha_\ell$$
$$\beta_i = \beta_{i1} \bar{\beta}_{i1} \ldots \beta_{im_i} \bar{\beta}_{im_i} \qquad (1 \leq i \leq k)$$
$$\beta = \beta_1 \beta_2 \ldots, \beta_k,$$
$$\gamma = \gamma_1 \bar{\gamma}_1 \ldots \gamma_n \bar{\gamma}_n$$

Then it is easy to verify that the following is a decomposition of C into a tensor product of elementary CGH algebras:

$$C \cong [\alpha_1, \bar{\alpha}_1] \otimes [\alpha_1 \bar{\alpha}_1 \alpha_2, \alpha_1 \bar{\alpha}_1 \bar{\alpha}_2] \otimes \ldots$$
$$\otimes [\alpha_1 \bar{\alpha}_1 \ldots \alpha_{\ell-1}, \bar{\alpha}_{\ell-1} \alpha_\ell, \alpha_1 \bar{\alpha}_1 \ldots \alpha_{\ell-1} \bar{\alpha}_{\ell-1} \bar{\alpha}_\ell]$$
$$\otimes [\alpha\beta_{11}, \alpha\bar{\beta}_{11}] \otimes \ldots \otimes [\alpha\beta_{11}\bar{\beta}_{11} \ldots \beta_{1m_1-1}\bar{\beta}_{1m_1-1}\beta_{1m_1},$$
$$\alpha\beta_{11}\bar{\beta}_{11} \ldots \beta_{1m_1-1}\bar{\beta}_{1m_1-1}\bar{\beta}_{1m_1}] \otimes \ldots \otimes [\alpha\beta_{k1}, \alpha\bar{\beta}_{k1}]$$
$$\otimes \ldots \otimes [\alpha\beta_{k1}\bar{\beta}_{k1} \ldots \beta_{km_k-1}\bar{\beta}_{km_k-1}\beta_{km_k},$$
$$\alpha\beta_{k1}\bar{\beta}_{k1} \ldots \beta_{km_k-1}\bar{\beta}_{km_k-1}\bar{\beta}_{km_k}]$$
$$\otimes [\alpha\beta\gamma_1, \alpha\beta\bar{\gamma}_1] \otimes \ldots \otimes [\alpha\beta\gamma_1\bar{\gamma}_1 \ldots \gamma_{n-1}\bar{\gamma}_{n-1}\gamma_n, \alpha\beta\gamma_1\bar{\gamma}_1 \ldots \gamma_{n-1}\bar{\gamma}_{n-1}\bar{\gamma}_n]$$
$$\otimes \begin{cases} \text{(i) nothing more} & \text{if } p \text{ even, } r \text{ even, } j = 0, \text{ or} \\ \text{(ii) } [\alpha\beta\gamma\bar{\bar{\alpha}}] & p \text{ odd, } r \text{ even, } j = 0, \text{ or} \\ \text{(iii) } [\alpha\beta\gamma\bar{\bar{\gamma}}] & p \text{ even, } r \text{ odd, } j = 0, \text{ or} \\ \text{(iv) } [\alpha\beta\gamma\bar{\bar{\alpha}}, \alpha\beta\gamma\bar{\bar{\gamma}}] & p \text{ odd, } r \text{ odd, } j = 0, \text{ or} \\ \text{(v) } [\alpha\beta_1\gamma\bar{\bar{\beta}}_1] \otimes \ldots \otimes [\alpha\beta_J\gamma\bar{\bar{\beta}}_J] & p \text{ even, } r \text{ even, } j > 0, \text{ or} \\ \text{(vi) } [\alpha\beta\gamma\bar{\bar{\alpha}}, \alpha\beta_1\gamma\bar{\bar{\beta}}_1] \otimes [\beta_1\beta_2\bar{\bar{\beta}}_1\bar{\bar{\beta}}_2] \otimes \ldots \otimes [\beta_1\beta_J\bar{\bar{\beta}}_1\bar{\bar{\beta}}_J] & p \text{ odd, } r \text{ even, } j > 0, \text{ or} \\ \text{(vii) } [\alpha\beta\gamma\bar{\bar{\gamma}}, \alpha\beta_1\gamma\bar{\bar{\beta}}_1] \otimes [\beta_1\beta_2\bar{\bar{\beta}}_1\bar{\bar{\beta}}_2] \otimes \ldots \otimes [\beta_1\beta_J\bar{\bar{\beta}}_1\bar{\bar{\beta}}_J] & p \text{ even, } r \text{ odd, } j > 0, \text{ or} \\ \text{(viii) } [\alpha\beta\gamma\bar{\bar{\alpha}}, \alpha\beta\gamma\bar{\bar{\gamma}}] \otimes [\alpha\beta_1\gamma\bar{\bar{\alpha}}\bar{\bar{\gamma}}\bar{\bar{\beta}}_1] \otimes \ldots \otimes [\alpha\beta_J\gamma\bar{\bar{\alpha}}\bar{\bar{\gamma}}\bar{\bar{\beta}}_J] & p \text{ odd, } r \text{ odd, } j > 0. \end{cases}$$

Now let $m = m_1 + \cdots + m_k$. Then from Summary 6.1 it is easy to verify that:

$$C \cong Q \otimes F_2 \otimes Q \otimes F_2 \otimes \ldots \otimes \begin{Bmatrix} F_2 & (\ell \text{ even}) \\ Q & (\ell \text{ odd}) \end{Bmatrix} \ (\ell \text{ factors, alternating } Q, F_2)$$
$$\otimes \begin{Bmatrix} Q & (\ell \text{ even}) \\ F_2 & (\ell \text{ odd}) \end{Bmatrix} \otimes \ldots \otimes \begin{Bmatrix} F_2 & (\ell + m_1 \text{ even}) \\ Q & (\ell + m_1 \text{ odd}) \end{Bmatrix} \ m_1 \text{ factors, similarly alternating}$$

$$\otimes \ldots \tag{6.17}$$

$$\otimes \left\{ \begin{matrix} Q \ (\ell \text{ even}) \\ F_2 \ (\ell \text{ odd}) \end{matrix} \right\} \otimes \ldots \otimes \left\{ \begin{matrix} F_2 \ (\ell+m_k \text{ even}) \\ Q \ (\ell+m_k \text{ odd}) \end{matrix} \right\} \ m_k \text{ factors, similarly alternating}$$

$$\otimes \left\{ \begin{matrix} F_2 \ (\ell+m \text{ even}) \\ Q \ (\ell+m \text{ odd}) \end{matrix} \right\} \otimes \ldots \otimes \left\{ \begin{matrix} Q \ (\ell+m+n \text{ even}) \\ F_2 \ (\ell+m+n \text{ odd}) \end{matrix} \right\} \ n \text{ factors, similarly alternating}$$

$$\otimes \begin{cases} \text{(i) nothing more} \\ \text{(ii)} \ \left\{ \begin{matrix} \mathcal{C} \ (\ell+m+n \text{ even}) \\ 2F \ (\ell+m+n \text{ odd}) \end{matrix} \right\} \\ \text{(iii)} \ \left\{ \begin{matrix} 2F \ (\ell+m+n \text{ even}) \\ \mathcal{C} \ (\ell+m+n \text{ odd}) \end{matrix} \right\} \\ \text{(iv)} \ F_2 \\ \text{(v)} \ \begin{cases} 2^j F & (\text{all } \ell+m_1+n,\ldots,\ell+m_j+n \text{ odd}) \\ 2^{j-1}\ \mathcal{C} & (\text{some } \ell+m_1+n,\ldots,\ell+m_j+n \text{ even}) \end{cases} \\ \text{(vi)} \ \begin{cases} 2^{j-1}F_2 & (\ell+m+n, \ell+m_1+n \text{ not both even, but } m_1+m_2,\ldots,m_1+m_j \text{ all even}) \\ 2^{j-1}Q & (\ell+m+n, \ell+m_1+n \text{ both even, and } m_1+m_2,\ldots,m_1+m_j \text{ all even}) \\ 2^{j-2}\ \mathcal{C}\otimes F_2 & (\text{some } m_1+m_2,\ldots,m_1+m_j \text{ odd}) \end{cases} \\ \text{(vii)} \ \begin{cases} 2^{j-1}F_2 & (\ell+m+n \text{ even or } \ell+m_1+n \text{ odd, and } m_1+m_2,\ldots,m_1+m_j \text{ all even}) \\ 2^{j-1}Q & (\ell+m+n \text{ odd and } \ell+m_1+n \text{ even, and } m_1+m_2,\ldots,m_1+m_j \text{ all even}) \\ 2^{j-2}\ \mathcal{C}\otimes F_2 & (\text{some } m_1+m_2,\ldots,m_1+m_j \text{ odd}) \end{cases} \\ \text{(viii)} \ \begin{cases} 2^j F_2 & (\text{all } \ell+m_1+n,\ldots,\ell+m_j+n \text{ odd}) \\ 2^{j-1}\ \mathcal{C}\otimes F_2 & (\text{some } \ell+m_1+n,\ldots,\ell+m_j+n \text{ even}) \end{cases} \end{cases}$$

with (i),...,(viii) as above.

The problem now is to simplify this tensor product.

Let

$$N = \ell + m_1 + \cdots + m_k + n = \ell + m + n\,.$$

Let us first simplify the tensor product of the first N factors – that is, those factors not involving (i) or... or (viii).

Clearly by lemma 6.15(iii) this product simplifies to either F_{2^N} or $Q \otimes F_{2^{N-1}}$ according to whether there is an even or odd number of Q factors.

We seek convenient conditions to distinguish these two possibilities.

One particularly simple situation occurs when ℓ is even and $\ell+m$ is odd. In this case we get F_{2^N} if an even number of $\ell, m_1, \ldots, m_k, n$ is congruent to 1 or to 2 modulo 4, and we get $Q \otimes F_{2^{N-1}}$ otherwise, This is because if $\ell \equiv 1$ or $\ell \equiv 2 \pmod 4$, we get an *odd* number of Q factors from the first ℓ factors, and similar statements hold for each of $m_1, \ldots, m_k, n$.

That is, we get F_{2^N} when an *even* number of $p, q_1, \ldots, q_k, r$ is congruent to one of 2,3,4,5 modulo 8.

Suppose however $\ell+m$ is even. In this case we are concerned with whether n is congruent to 2 or to 3 modulo 4 (since the last n factors would be $F_2 \otimes Q \otimes \ldots$ instead of $Q \otimes F_2 \otimes \ldots$) - that is we could be concerned with whether r is congruent to one of 4,5,6,7 modulo 8.

Similarly if ℓ is odd we would be concerned with how many of $q_1, \ldots, q_k$ are congruent to one of 4,5,6,7 modulo 8.

These observations suggest the following device:

Define

$$q_i' = \left\{ \begin{array}{c} q_i \quad (\ell \text{ even}) \\ q_i - 2 \ (\ell \text{ odd}) \end{array} \right\} \quad 1 \le i \le k$$

$$r' = \left\{ \begin{array}{c} r-2 \ (\ell+m \text{ even}) \\ r \quad (\ell+m) \text{ odd} \end{array} \right\}$$

Now let $S =$ how many of $p, q_1', \ldots, q_k', r'$ are congruent to one of 2,3,4,5 modulo 8.

Then in all cases the first N factors of (6.17) give F_{2^N} if S is even, and $Q \otimes F_{2^{N-1}}$ if S is odd.

It is now easy to incorporate the remaining factor(s) ((i) or ... or (viii)) using lemma 6.15, giving the following complete description of the structure of C:

$$C \cong \text{(i)} \begin{cases} F_{2^N} & (S \text{ even}) \\ Q \otimes F_{2^{N-1}} & (S \text{ odd}) \end{cases}$$

$$\text{(ii)} \begin{cases} \mathcal{C} \otimes F_{2^N} & (\ell+m+n \text{ even}) \\ 2F_{2^N} & (S \text{ even}, \ \ell+m+n \text{ odd}) \\ 2Q \otimes F_{2^{N-1}} & (S \text{ odd}, \ \ell+m+n \text{ odd}) \end{cases}$$

$$\text{(iii)} \begin{cases} 2F_{2^N} & (S \text{ even}, \ \ell+m+n \text{ even}) \\ 2Q \otimes F_{2^{N-1}} & (S \text{ odd}, \ \ell+m+n \text{ even}) \\ \mathcal{C} \otimes F_{2^N} & (\ell+m+n \text{ odd}) \end{cases}$$

$$\text{(iv)} \begin{cases} F_{2^{N-1}} & (\text{S even}) \\ Q \otimes F_{2^N} & (S \text{ odd}) \end{cases}$$

$$\text{(v)} \begin{cases} 2^J F_{2^N} & (S \text{ even and all } \ell+m_1+n, \ldots, \ell+m_J+n \text{ odd}) \\ 2^J Q \otimes F_{2^{N-1}} & (S \text{ odd and all } \ell+m_1+n, \ldots, \ell+m_J+n \text{ odd}) \\ 2^{J-1} \ \mathcal{C} \otimes F_{2^N} & (\text{some } \ell+m_1+n, \ldots, \ell+m_J+n \text{ even}) \end{cases}$$

$$\text{(vi)} \begin{cases} 2^{J-1} F_{2^{N+1}} & (S \text{ even}, \ \ell+m+n \text{ or } \ell+m_1+n \text{ odd}, \ m_1, \ldots, m_J \text{ all congruent mod 2; or } S \text{ odd}, \ \ell+m+n \text{ or } \ell+m_1+n \text{ even}, \ m_1, \ldots, m_J \text{ all congruent mod 2}) \\ 2^{J-1} Q \otimes F_{2^N} & (S \text{ odd}, \ \ell+m+n \text{ or } \ell+m_1+n \text{ odd}, \ m_1, \ldots, m_J \text{ all congruent mod 2; or } S \text{ even}, \ \ell+m+n \text{ or } \ell+m_1+n \text{ even}, \ m_1, \ldots, m_J \text{ all congruent mod 2}) \\ 2^{J-1} \ \mathcal{C} \otimes F_{2^{N+1}} & (m_1, \ldots, m_J \text{ not all congruent mod 2}) \end{cases}$$

$$\text{(vii)}\quad \begin{cases} 2^{J-1}F_{2^{N+1}} & (S \text{ even, } \ell+m+n \text{ even or } \ell+m_1+n \text{ odd, } m_1,\dots,m_J \text{ all congruent mod 2; or } S \text{ odd, } \ell+m+n \text{ odd, and } \ell+m_1+n \text{ even, } m_1,\dots,m_J \text{ all congruent mod 2}) \\ 2^{J-1}Q\otimes F_{2^N} & (S \text{ odd, } \ell+m+n \text{ even or } \ell+m_1+n \text{ odd, } m_1,\dots,m_J \text{ all congruent mod 2; or } S \text{ even, } \ell+m+n \text{ odd and } \ell+m_1+n \text{ even, } m_1,\dots,m_J \text{ all congruent mod 2}) \\ 2^{J-2}\not{C}\otimes F_{2^{N+1}} & (m_1,\dots,m_J \text{ not all congruent mod 2}) \end{cases}$$

$$\text{(viii)}\quad \begin{cases} 2^{J}F_{2^{N+1}} & (S \text{ even and all } \ell+m_1+n,\dots,\ell+m_J+n \text{ odd}) \\ 2^{J}F_{2^{N}} & (S \text{ odd and all } \ell+m_1+n,\dots,\ell+m_J+n \text{ odd}) \\ 2^{J-2}\not{C}\otimes F_{2^{N+1}} & (\text{some } \ell+m_1+n,\dots,\ell+m_J+n \text{ even}) \end{cases}$$

with (i),...,(viii) as above.

Actually (i) can be absorbed into (v), if in (v) we assume the conditions "all $\ell+m_1+n,\dots,\ell+m_J+n$ odd", "some $\ell+m_1+n,\dots,\ell+m_J+n$ even" are respectively true, false when $J=0$. Similarly (iv) may be absorbed into (viii).

If we also combine (ii) with (vi) and (iii) with (vii), and apply corollary 6.13, then from Theorem 6.14 we derive the following complete description of the possible orders of repeat designs:

Theorem 6.15 (Gastineau-Hills). *Let $p+1,q_1,\dots,q_k,r$ be non negative integers, not all zero, with $q_1,\dots,q_J$ odd and $q_{J+1},\dots,q_k$ even (some J such that $0\le J\le k$). Suppose $\ell=[p/2]$, $m_i=[q_i/2]$ $(1\le i\le k)$, $n=[r/2]$, $m=m_1+\cdots+m_k$, $N=\ell+m+n$,*

$$q_i'=\begin{Bmatrix} q_i & (\text{if } \ell \text{ even}) \\ q_i-2 & (\text{if } \ell \text{ odd}) \end{Bmatrix}, \quad r'=\begin{Bmatrix} r-2 & (\text{if } \ell+m \text{ even}) \\ r & (\text{if } \ell+m \text{ odd}) \end{Bmatrix}, \text{ and}$$

S = how many of $p,q_i',\dots,q_k',r'$ are congruent to one of 2,3,4,5 modulo 8.

Then the possible orders of repeat designs $(X,Y_1,\dots,Y_k,Z)$ on $p+1$, $q_1,\dots,q_k,r$ variables are all the multiples of ρ where ρ is given below.

(i) p even, r even

$$\rho=\begin{cases} 2^N & (S \text{ even and } \ell+m_1+n,\dots,\ell+m_J+n \text{ all odd}) \\ 2^{N+1} & (\text{otherwise}) \end{cases}$$

(ii) p odd, r even

$$\rho=\begin{cases} 2^N & (J=0,\ S \text{ even},\ \ell+m+n \text{ odd}) \\ 2^{N+1} & (J=0, \text{ and either } S \text{ odd or } \ell+m+n \text{ even; or } J>0, \\ & S \text{ even},\ \ell+m+n,\ \ell+m_1+n \text{ not both even, and} \\ & m_1,\dots,m_J \text{ all congruent mod 2; or } J>0,\ S \text{ odd}, \\ & \ell+m+n,\ \ell+m_1+n \text{ both even, and } m_1,\dots,m_J \text{ all congruent mod 2}) \\ 2^{N+2} & (\text{otherwise}) \end{cases}$$

(iii) p even, r odd

$$\rho = \begin{cases} 2^N & (J=0,\ S \text{ even},\ \ell+m+n \text{ even}) \\ 2^{N+1} & (J=0, \text{ and } S,\ \ell+m+n \text{ not both even; or } J>0,\ S \\ & \text{even},\ \ell+m+n \text{ even or } \ell+m_1+n \text{ odd, and } m_1,\ldots,m_J \\ & \text{all congruent} \mod 2; \text{ or } J>0,\ S \text{ odd},\ \ell+m+n \text{ odd} \\ & \text{and } \ell+m_1+n \text{ even, and } m_1,\ldots,m_J \text{ all congruent} \\ & \mod 2) \\ 2^{N+2} & (\text{otherwise}) \end{cases}$$

(iv) p odd, r odd

$$\rho = \begin{cases} 2^{N+1} & (S \text{ even and } \ell+m_1+n,\ldots,\ell+m_J+n \text{ all odd}) \\ 2^{N+2} & (\text{otherwise}) \end{cases}$$

Note that "periodicity-8" can be verified for repeat designs from this theorem. For if any of $p, q_1, \ldots, q_k, r$ is increased by 8, clearly N is increased by 4 and the oddness/evenness and congruency modulo 8 conditions on the p, q_i, r, ℓ, m_i, n etc. are unaltered.

In particular the theorem conforms to "periodicity-8" for the cases $p+1=0$, so by the results of Section 6.10 we are justified in the way we stated the Theorem 6.15, removing the original restriction that $p+1$ be non zero. In other words 6.15 remains valid for repeat designs $(X, Y_1, \ldots, Y_k, Z)$ with $X=0$, provided $Y_1, \ldots, Y_k, Z$ are not all zero.

Example 6.10. The possible orders of repeat designs (X, Y_1, Y_2, Y_3, Z) on $3, 5, 2, 12, 1$ variables are all the multiples of 2^{12}.

Proof. Here $p=2$ (even), $r=1$ (odd) so case (iii) of 6.17 applies. Now $\ell=1$, $m_1=2$, $m_2=1$, $m_3=6$, $n=0$, $m=9$, $N=10$. Also ℓ is odd, $\ell+m$ even, so $p=2$, $q_1'=3$, $q_2'=0$, $q_3'=10\equiv 2 \pmod 8$, $r'=-1\equiv 7 \pmod 8$.

So $S=3$ is odd. But $J=1>0$ and $\ell+m+n=10$ is even, so the "otherwise" of 6.15(iii) applies: $\rho = 2^{N+2} = 2^{12}$.

By symmetry the possible orders of repeat designs on, say, $3, 2, 5, 12, 1$ variables would also be all the multiples of 2^{12}. □

6.12 Orders of Product Designs and Amicable Sets

We conclude by finding the possible orders of product designs and of amicable sets of orthogonal designs, on given numbers of variables. We could do this by taking the algebras of equation 6.7 (the algebras corresponding to product designs) and the algebras corresponding to amicable k-tuples and proceeding in each case as in Section 6.11. However, as we have remarked before, both product designs and amicable sets can be taken as particular cases of repeat designs $(X, Y_1, \ldots, Y_k, Z)$ by setting some of $X, Y_1, \ldots, Y_k, Z$ to zero.

So since in theorem 6.15 we allowed for some of $p+1, q_1, \ldots, q_k, r$ (the numbers of variables in $X, Y_1, \ldots, Y_k, Z$ respectively) to be zero – even $p+1$ – we can obtain the required results very quickly as corollaries of Theorem 6.15.

Let us first consider product designs. These are given by those repeat designs $(X, Y_1, \ldots, Y_k, Z)$ for which $Z = 0$ and $k = 2$. That is, we use Theorem 6.15 where $r = 0$, $k = 2$.

Note that in this case neither r nor $r-2$ is congruent to any of $2,3,4,5$ modulo 8, so that the S of Theorem 6.15 is always just how many of p, q_1', q_2' are congruent to $2,3,4,5$ modulo 8. From this we easily deduce the following corollary to Gastineau-Hills Theorem 6.15:

Corollary 6.14. *Let $p+1, q_1, q_2$ be non-negative integers, not all zero. Let $\ell = [p/2]$, $m_1 = [q_1/2]$, $m_2 = [q_2/2]$, $N = \ell + m_1 + m_2$,*

$$q_1' = \left\{ \begin{matrix} q_i & (\ell \text{ even}) \\ q_i - 2 & (\ell \text{ odd}) \end{matrix} \right\} \qquad (i = 1,2)\,, \text{ and}$$

$$S = \text{how many of } p, q_1', q_2' \text{ are congruent to one of } 2,3,4,5 \text{ modulo } 8$$

Then the possibility of orders of product designs (X, Y_1, Y_2) (as defined in Definition 6.3) on $p+1, q_1, q_2$ variables are all the multiples of ρ where ρ is given by the following:

(i) p even, q_1 even, q_2 even

$$\rho = \begin{cases} 2^N & (S \text{ even}) \\ 2^{N+1} & (S \text{ odd}) \end{cases}$$

(ii) p odd, q_1 even, q_2 even

$$\rho = \begin{cases} 2^N & (S \text{ even}, \ \ell + m_1 + m_2 \text{ odd}) \\ 2^{N+1} & (\text{otherwise}) \end{cases}$$

(iii) p even, q_1 odd, q_2 even

$$\rho = \begin{cases} 2^N & (S \text{ even}, \ \ell + m_1 \text{ odd}) \\ 2^{N+1} & (\text{otherwise}) \end{cases}$$

(iv) p even, q_2 even, q_1 odd
as for *(iii)* with m_1, m_2 interchanged

(v) p odd, q_1 even, q_2 even

$$\rho = \begin{cases} 2^{N+1} & (S \text{ even}, \ \ell + m_1, m_2 \text{ not both even; or } S \text{ odd}, \ \ell + m_1, m_2 \text{ both even}) \\ 2^{N+2} & (\text{otherwise}) \end{cases}$$

(vi) p *odd,* q_1 *even,* q_2 *odd*
as for (v) with m_1, m_2 *interchanged*

(vii) p *even,* q_1 *odd,* q_2 *odd*

$$\rho = \begin{cases} 2^N & (S \text{ even, } \ell+m_1, \ell+m_2 \text{ both odd}) \\ 2^{N+1} & (\text{otherwise}) \end{cases}$$

(viii) p *odd,* q_1 *odd,* q_2 *odd*

$$\rho = \begin{cases} 2^{N+1} & (S \text{ even, } \ell, m_1 \text{ not both even; and } m_1+m_2 \text{ even; or} \\ & S \text{ odd, } \ell, m_1, m_2 \text{ all even}) \\ 2^{N+2} & (\text{otherwise}) \end{cases}$$

From this corollary the arrays in Table 6.5 are easily constructed. They give the minimal orders (expressed for convenience as indices base 2, so that an entry n means minimal order 2^n) of product designs on $p+1, q, r$ variables for all 8^3 cases $0 \le p+1, q, r \le 7$. (the entry for $p+1, q, r = 0, 0, 0$ is justified in Section 6.10)

So for example we can verify from the Table 6.5 the result of the calculation in example 6.9 – that the minimal order of product designs on $2, 2, 4$ variables is 2^3.

By "periodicity-8" the minimal orders for larger values of $p+1, q, r$ are easily deduced. Thus for example the minimal order for each of $(10, 2, 4)$, $(2, 10, 4)$, $(2, 2, 12)$ is $2^{3+4} = 2^7$.

The table for $p+1 = 0$ is effectively a table giving the minimal orders of amicable pairs on (q, r) variables.

The cases $p+1 = q = 0$ give the well known minimal orders of single orthogonal designs on r variables.

Now let us consider amicable k-tuples. These are given by those repeat designs $(X, Y_1, \ldots, Y_k, Z)$ for which $X = Z = 0$. That is, we use theorem 6.15 where $p = -1$, $r = 0$. Note that in this case $\ell = [p/2] = -1$ is odd, so $q_i' = q_i - 2$ $(1 \le i \le k)$ and $r' = r = 0$, so the S of 6.15 is here how many of $q_1 - 2, \ldots, q_k - 2$ is congruent to one of $2, 3, 4, 5$ modulo 8. This means that S is how many of $q_1, \ldots, q_k$ is congruent to one of $4, 5, 6, 7$ modulo 8. Also, although the N of 6.15 would here be $-1 + m_1 + \cdots + m_k$, let us redefine N to be simply $\sum_1^k m_i$.

This gives:

Corollary 6.15. *Let* $q_1, \ldots, q_k$ *be non negative integers, not all zero, with* $q_1, \ldots, q_J$ *odd,* $q_{J+1}, \ldots, q_k$ *even (some* J *such that* $0 \le J \le k$*).*

Let $m_i = [q_i/2]$ *(*$1 \le i \le k$*) and* $N = m_1 + \cdots + m_k$*, and let* S *= how many of* $q_1, \ldots, q_k$ *is congruent to one of* $4, 5, 6, 7$ *modulo 8.*

Then the possible orders of amicable k*-tuples on* $q_1, \ldots, q_k$ *variables are all the multiples of* p *where:*

Table 6.5 Minimal orders of product designs on $p+1, q, r$ variables (indices base 2)[a]

$p+1=0$

q \ r	0	1	2	3	4	5	6	7
0	-1	0	1	2	2	3	3	3
1	0	0	1	2	3	3	4	4
2	1	1	1	2	3	4	4	5
3	2	2	2	2	3	4	5	5
4	2	3	3	3	3	4	5	6
5	3	3	4	4	4	4	5	6
6	3	4	4	5	5	5	5	6
7	3	4	5	5	6	6	6	6

$p+1=1$

q \ r	0	1	2	3	4	5	6	7
0	0	1	2	2	3	3	3	3
1	1	1	2	2	3	3	4	4
2	2	2	2	2	3	4	5	5
3	2	2	2	2	3	4	5	5
4	3	3	3	3	4	5	6	6
5	3	3	4	4	5	5	6	6
6	3	4	5	5	6	6	6	6
7	3	4	5	5	6	6	6	6

$p+1=2$

q \ r	0	1	2	3	4	5	6	7
0	1	2	2	3	3	3	3	4
1	2	2	3	3	3	3	4	5
2	2	3	3	3	3	4	5	6
3	3	3	3	3	4	5	6	6
4	3	3	3	4	5	6	6	7
5	3	3	4	5	6	6	7	7
6	3	4	5	6	6	7	7	7
7	4	5	6	6	7	7	7	7

$p+1=3$

q \ r	0	1	2	3	4	5	6	7
0	2	2	3	3	3	3	4	5
1	2	2	3	3	3	3	4	5
2	3	3	4	4	4	4	5	6
3	3	3	4	4	5	5	6	6
4	3	3	4	5	6	6	7	7
5	3	3	4	5	6	6	7	7
6	4	4	5	6	7	7	8	8
7	5	5	6	6	7	7	8	8

$p+1=4$

q \ r	0	1	2	3	4	5	6	7
0	2	3	3	3	3	4	5	6
1	3	3	4	4	4	4	5	6
2	3	4	4	5	5	5	5	6
3	3	4	5	5	6	6	6	6
4	3	4	5	6	6	7	7	7
5	4	4	5	6	7	7	8	8
6	5	5	5	6	7	8	8	9
7	6	6	6	6	7	8	9	9

$p+1=5$

q \ r	0	1	2	3	4	5	6	7
0	3	3	3	3	4	5	6	6
1	3	3	4	4	5	5	6	6
2	3	4	5	5	6	6	6	6
3	3	4	5	5	6	6	6	6
4	4	5	6	6	7	7	7	7
5	5	5	6	6	7	7	8	8
6	6	6	6	6	7	8	9	9
7	6	6	6	6	7	8	9	9

[a] Gastineau-Hills [63, p155–156] © H. Gastineau-Hills

Table 6.5 Minimal orders of product designs on $p+1, q, r$ variables (indices base 2) [63] [a] *(continued)*

$p+1=6$

q \ r	0	1	2	3	4	5	6	7
0	3	3	3	4	5	6	6	7
1	3	3	4	5	6	6	7	7
2	3	4	5	6	6	7	7	7
3	4	5	6	6	7	7	7	7
4	5	6	6	7	7	7	7	8
5	6	6	7	7	7	7	8	9
6	6	7	7	7	7	8	9	10
7	7	7	7	7	8	9	10	10

$p+1=7$

q \ r	0	1	2	3	4	5	6	7
0	3	3	4	5	6	6	7	7
1	3	3	4	5	6	6	7	7
2	4	4	5	6	7	7	8	8
3	5	5	6	6	7	7	8	8
4	6	6	7	7	7	7	8	9
5	6	6	7	7	7	7	8	9
6	7	7	8	8	8	8	9	10
7	7	7	8	8	9	9	10	10

[a] Gastineau-Hills [63, p155–156] © H. Gastineau-Hills

$$\rho = \begin{cases} 2^{N-1} & (J=0,\ S \text{ and } N \text{ both even}) \\ 2^{N} & (J=0,\ S \text{ and } N \text{ not both even; or } J>0,\ S \text{ even}, \\ & N, m_1 \text{ not both odd, and } m_1, \ldots, m_J \text{ all congruent } \mod 2; \\ & \text{or } J>0,\ S \text{ odd}, N, m_1 \text{ both odd, and } \\ & m_1, \ldots, m_J \text{ all congruent } \mod 2) \\ 2^{N+1} & (\text{otherwise}). \end{cases}$$

The conditions determining ρ in 6.15 may be more neatly expressed. Let us for any integer j define n_j to be how many of $q_1, \ldots, q_k$ are congruent to j modulo 8.

Then in 6.15 the condition S even is equivalent to $n_4+n_5+n_6+n_7 \equiv 0 \pmod 2$. The condition N even is equivalent to $n_2+n_3+n_6+n_7 \equiv 0 \pmod 2$. The condition $J=0$ is equivalent to $n_1=n_3=n_5=n_7=0$.

So if $J=0$, then S, N both even is equivalent to $n_2 \equiv n_4 \equiv n_6 \pmod 2$.

Now suppose $J>0$. The condition $m_1, \ldots, m_J$ all even is equivalent to $n_3=n_7=0$, and all odd is equivalent to $n_1=n_5=0$. So S even, N, m_1 not both odd and $m_1, \ldots, m_J$ congruent $\mod 2$ implies that either:

$$n_3=n_7=0,\ n_4+n_5+n_6+n_7 \equiv 0 \pmod 2;\ \text{or}$$
$$n_1=n_5=0,\ n_4+n_5+n_6+n_7=n_2+n_3+n_6+n_7 \equiv 0 \pmod 2;$$

which implies that either

$$n_3=n_7=0,\ n_4+n_5+n_6 \equiv 0 \pmod 2,\ \text{or}$$
$$n_1=n_5=0,\ n_2+n_3+n_4 \equiv 0 \pmod 2.$$

Also S odd, N, m_1 both odd and $m_1, \ldots, m_J$ congruent $\mod 2$ implies that

$$n_1 = n_5 = 0,\ n_4 + n_5 + n_6 + n_7 \equiv n_2 + n_3 + n_6 + n_7 \equiv 1 \pmod 2;$$

which implies that

$$n_1 = n_5 = 0 \text{ and } n_2 + n_3 + n_4 \equiv 0 \pmod 2.$$

Conversely $n_3 = n_7 = 0$ and $n_4 + n_5 + n_6 \equiv 0 \pmod 2$, or $n_1 = n_5 = 0$, $n_2 + n_3 + n_4 = 0 \pmod 2$ implies that: either S even, N, m_1 not both odd, $m_1, \ldots, m_J$ congruent mod 2, or S odd, N, m_1 both odd, $m_1, \ldots, m_J$ congruent mod 2. A11 these facts mean that we can give the following equivalent formulation of 6.15 (we need no longer assume the q_i are ordered with the odds first):

Corollary 6.16. *Let $q_1, \ldots, q_k$ be non negative integers, not all zero. Let $N = [q_1/2] + \cdots + [q_k/2]$, and for any integer j let n_j be how many of $q_1, \ldots, q_k$ are congruent to j modulo 8.*

Then the possible orders of amicable k-tuples on $q1, \ldots, q_k$ variables are all the multiple of ρ where:

$$\text{If all } q_i \text{ are even } \rho = \begin{cases} 2^{N-1} & \text{if } n_2 \equiv n_4 \equiv n_6 \pmod 2 \\ 2^N & \text{otherwise.} \end{cases}$$

$$\text{If some } q_i \text{ is odd } \rho = \begin{cases} & n_3 = n_7 = 0,\ n_4 + n_5 + n_6 \equiv 0 \pmod 2, \\ 2^N & \text{or} \\ & n_1 = n_5 = 0,\ n_2 + n_3 + n_4 \equiv 0 \pmod 2. \\ 2^{N+1} & \text{otherwise.} \end{cases}$$

The case $k = 2$ will give the bounds for Wolfe's amicable pairs (cf. [247]).

The case $k = 1$ gives the familiar "Radon bounds" for single orthogonal designs; thus

Corollary 6.17. *The single orthogonal designs on q variables have orders all multiples of ρ, where*

$$\rho = \begin{cases} 2^{[q/2]-1} & \text{if } q \equiv 0 \pmod 8 \\ 2^{[q/2]} & \text{if } q \equiv 1, 2, 4, 6 \text{ or } 7 \pmod 8 \\ 2^{[q/2]+1} & \text{if } q \equiv 3 \text{ or } 5 \pmod 8 \end{cases}$$

The entries in Table 6.5 for $p + 1 = r = 0$ agree with this result.

Chapter 7
Techniques

7.1 Using Cyclotomy

We remarked in Section 4.12 that Williamson [244] used (implicitly) the theory of cyclotomy to construct Hadamard matrices of order 148 and 172.

Subsequently, many authors have used this theory to construct Hadamard and skew-Hadamard matrices. Some of these are mentioned in Section 5.10. R. M. Wilson [246] and others have used the theory to make major advances in studying balanced incomplete block designs. In this section we will give the constructions for Baumert-Hall arrays promised in §4.12 and indicate some other constructions for orthogonal designs. We remark that the possibilities for using cyclotomy in the theory of orthogonal designs has by no means been exhausted here.

Definition 7.1. [Storer [200]] Let x be a primitive root of $F = GF(q)$, where $q = p^\alpha = ef+1$ is a prime power. Write $G = \langle x \rangle$. The *cyclotomic classes* C_i in F are:

$$C_i = \{x^{es+i} :\ s = 0, 1, \ldots, f-1\}, i = 0, 1 \ldots, e-1\,.$$

We note that the C_i are pairwise disjoint and their union is G.

For fixed i and j, the *cyclotomic number* (i, j) is defined to be the number of solutions of the equation

$$z_i + 1 = z_j \quad (z_i \in C_i\,, \quad z_j \in C_j)\,,$$

where $1 = x^0$ is the multiplicative unit of F. That is, (i, j) is the number of ordered pairs s, t such that

$$x^{se+i} + 1 = x^{et+j} \quad (0 \le s, t \le f-1)\,.$$

Note that the number of times

$$x^{es+i} - x^{et+k} \in C_j$$

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5_7

is the cyclotomic number $(k-j, i-j)$.

Notation 7.1. Let $A = a_1, a_2, \ldots, a_k$ be a k-set; then we will use ΔA for the collection of differences between distinct elements of A, i.e.,

$$\Delta A = [a_i - a_j : \ i \neq j, \ 1 \leq i, \ j \leq k] \, .$$

Now

$$\Delta C_i = (0,0)C_i + (1,0)C_{i+1} + (2,0,)C_{i+2} + \cdots$$

and

$$\begin{aligned} \Delta(C_i - C_j) = &(0,0)C_j + (1,0)C_{j+1} + \cdots \\ &\cdots + (0,0)C_i + (1,0)C_{i+1} + \cdots \\ &\cdots + (0,i-j)C_j + (1,i-j)C_{j+1} + \cdots \\ &\cdots + (0,j-i)C_i + (1,j-i)C_{i+1} + \cdots \end{aligned}$$

Notation 7.2. We use $C_a \& C_b$ to denote the adjunction of two sets with repetitions remaining. If $A = \{a,b,c,d\}$ and $B = \{b,c,e\}$, then $A \& B = [a,b,b,c,c,d,e]$. $C_a \sim C_b$ is used to denote adjunction, but with the elements of the second set becoming signed. So $A \sim B = [a,b,-b,c,-c,d,-e]$. We note many authors now (in 2016) use *multiset* instead of the adjunction of sets. □

The transpose of a cyclotomic class $C_i^{\top}$ will be defined as $-C_i$, where

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

with $k = \frac{e}{2}$ for f odd and $k = 0$ for f even.

We define $[C_i]$ the incidence matrix of the cyclotomic class C_i by

$$c_{jk} = \begin{cases} 1, & \text{if } z_j - z_k \in C_i \\ 0, & \text{otherwise.} \end{cases}$$

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

Now if $[C_i]$ is the incidence matrix of a cyclotomic class, then $[C_i^{\top}] = [C_i]^{\top}$, and

$$\begin{aligned} [C_i]^{\top} &= [C_i] \text{ if } f \text{ is even;} \\ [C_i]^{\top} &= [C_{i+\frac{e}{2}}] \text{ if } f \text{ is odd.} \end{aligned}$$

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

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

where the a_s are integers giving the coefficients of the matrices.

The incidence matrices of $C_a \,\&\, C_b$ and $C_a \sim C_b$ will be given by

$$[C_a \,\&\, C_b] = [C_a] + [C_b] \text{ and } [C_a \sim C_b] = [C_a] - [C_b].$$

In order to illustrate the method and use of cyclotomy, we will now prove the result quoted in Theorem 5.20, viz. ,

Lemma 7.1. *Let $q \equiv 5 \pmod 8$ be a prime power and $q = s^2 + 4t^2$ be its proper representation with $s \in 1 \pmod 4$. Then with C_i the cyclotomic class defined above,*

$$C_0 \,\&\, C_1 \text{ and } |t| \text{ copies of } C_0 \,\&\, C_2$$

are $(|t|+1) - \{q; \frac{(q-1)}{2}; (|t|+1)\frac{(q-3)}{4}\}$ supplementary difference sets with

$$x \in C_0 \,\&\, C_1 \Rightarrow -x \notin C_0 \,\&\, C_1$$

and

$$y \in C_0 \,\&\, C_1 \Rightarrow -y \in C_0 \,\&\, C_2 .$$

Proof. We see from Storer that the cyclotomic numbers for $q = ef + 1 = 4f + 1$ (f odd) are given by

	0	**1**	**2**	**3**
0	A	B	C	D
1	E	E	D	B
2	A	E	A	E
3	E	D	B	E

$$\begin{aligned} 2A + 2E &= f - 1, \\ B + D + 2E &= f, \\ A + B + C + D &= f, \end{aligned}$$

where for f odd we have

$$\begin{aligned} 16A &= q - 7 + 2s, & 16D &= q + 1 + 2s + 8t, \\ 16B &= q + 1 + 2s - 8t, & 16E &= q - 3 - 2s. \\ 16C &= q + 1 - 6s, \end{aligned}$$

Now $-1 \in C_2$, so

$$x \in C_0 \,\&\, C_1 \Rightarrow -x \in C_2 \,\&\, C_3 \Rightarrow -x \notin C_0 \,\&\, C_1\,,$$

and

$$y \in C_0 \,\&\, C_2 \Rightarrow -y \in C_0 \,\&\, C_2\,.$$

Clearly, $|C_0 \,\&\, C_1| = |C_0 \,\&\, C_2| = \frac{(q-1)}{2}$. So it remains to show that

$$\Delta(C_0 \,\&\, C_1) \& |t| \Delta(C_0 \,\&\, C_2) = [(|t|+1)\frac{(q-3)}{4}]G.$$

Now

$$\begin{aligned}
\Delta(C_0 \,\&\, C_1) &= (A+E)G \,\&\, BC_0 \,\&\, EC_1 \,\&\, EC_2 \,\&\, DC_3 \,\& \\
&\qquad EC_0 \,\&\, DC_1 \,\&\, BC_2 \,\&\, EC_3 \\
&= \left[\frac{(q-5)}{8}\right] C \,\&\, \frac{(q-1-4t)}{8}\,(C_0 \,\&\, C_2) \,\& \\
&\qquad \frac{(q-1+4t)}{8}\,(C_1 \,\&\, C_2)\,; \\
\Delta(C_0 \,\&\, C_2) &= 2AC_0 \,\&\, 2EC_1 \,\&\, 2AC_2 \,\&\, 2EC_3 \,\& \\
&\qquad (C+A)(C_0 \,\&\, C_2) \,\&\, (D+B)(C_1 \,\&\, C_3) \\
&= \frac{(q-5)}{4}(C_0 \,\&\, C_2) \,\&\, \frac{(q-1)}{4}(C_1 \,\&\, C_3).
\end{aligned}$$

Since the sign of t is ambiguously determined, we choose a generator of F which gives $|t| = -t$. Then

$$\begin{aligned}
\Delta(C_0 \,\&\, C_1) \,\&\, |t| \Delta(C_0 \,\&\, C_2) &= \frac{(q-5+q-1-4t-2qt+10t)}{8}(C_0 \,\&\, C_2) \,\& \\
&\qquad \frac{(q-5+q-1+4t-2qt+2t1)}{8}(C_1 \,\&\, C_3) \\
&= \left[\frac{(q-3-qt+3t1)}{4}\right] G \\
&= \left[\frac{(q-3)(1+t)}{4}\right] G
\end{aligned}$$

as required. □

We can adapt the cyclotomic arrays of Storer [200] in order to consider the matrices

$$P = \sum_{i=1}^{s} a_i [C_i]$$

where the a_i, are commuting variables (see Hunt and Wallis [110]). For the following results the arrays are often hard to use, and an individual calculation of the arrays was made. The result for 61 was due to David C. Hunt.

Lemma 7.2. *There exist T-matrices of order $t \in 13, 19, 25, 31, 41, 61$.*

Proof. Use the matrices X_1, X_2, X_3, X_4 given below:

t		X_1, X_2, X_3, X_4
$13 = 4.3+1$	$3^2+2^2+0^2+0^2$	$[C_0]$, $[C_1 \sim \{0\}]$, $[C_2 \sim C_3]$, $[\phi]$
$19 = 6.3+1$	$3^2+3^2+1^2+0^2$	$[C_O]$, $[C_2]$, $[\{0\} \,\&\, C_3 \sim C_4]$, $[C_1 \sim C_5]$
$25 = 8.3+1$	$5^2+0^2+0^2+0^2$	$[C_0 \,\&\, C_5 \sim \{0\}]$, $[C_1 \sim C_7]$, $[C_2 \sim C_3]$, $[C_4 \sim C_6]$
$31 = 10.3+1$	$3^2+3^2+3^2+2^2$	$[C_0 \,\&\, C_3 \sim C_2]$, $[C_4 \,\&\, C_5 \sim C_9]$, $[C_7 \,\&\, C_8 \sim C6]$, $[C_1 \sim \{0\}]$
$37 = 12.3+1$	$6^2+1^2+0^2+0^2$	$[C_0 \,\&\, C_1 \sim C_2 \sim C_3 \,\&\, C_4 \,\&\, C_5]$, $[\{0\}]$, $[C_6 \sim C_7 \,\&\, C_8 \sim C_9 \,\&\, C_{10} \sim C_{11}]$, $[\phi]$
$41 = 8.5+1$	$5^2+4^2+0^2+0^2$	$[C_0 \sim C_2 \sim C_3]$, $[C_4 \,\&\, C6 \sim C1 \sim \{0\}]$, $[C_5 \sim C_7]$, $[\phi]$
$61 = 20.3+1$	$6^2+5^2+0^2+0^2$	$[\{0\} \,\&\, C_1 \,\&\, C_{11} \sim C_5]$, $[C_7 \,\&\, C_{10} \sim C_0 \sim C_9]$, $[C_2 \,\&\, C_4 \,\&\, C_6 \sim C_3 \sim C_8]$, $[\phi]$

□

In the remainder of this section we shall consider various matrices obtained by taking linear combinations of the incidence matrices of cyclotomic classes. Part of this work appeared in the Ph.D. thesis of Joan Cooper [30].

We always consider p to be a prime power.

Case 1. $p = 2f+1$, f *odd*

Consider

$$P = aI + b[C_0] + c[C_1] \tag{7.1}$$

where a, b, c are commuting variables. Now

$$PP^\top = a^2 I + a\left(b[C_0] + c[C_1] + b[C_0]^\top + c[C_1]^\top\right) + b[C_0][C_0]^\top + c^2[C_1][C_1]^\top + bc\left([C_0][C_1]^\top + [C_0]^\top[C_1]\right).$$

Using the adapted cyclotomic array of Hunt and Wallis [110] for $e = 2$ given in Table 7.1 we can calculate the coefficients of the incidence matrices in $PP^\top$.

The coefficient of $[C_0]$ and $[C_1]$ is $\left(b^2+c^2+bc\right)A + bcB + ab + ac$. Hence, in this case we have

Table 7.1 Coefficients of the incidence matrices in $PP^\top$

	$\mathbf{C_0}, \mathbf{C_1}$	$\{\mathbf{0}\}$	
00	$A = \frac{(f-1)}{2}$	f	where ii is short for $[C_i][C_i]^\top$
11	$A = \frac{(f-1)}{2}$	f	and ij is short for
01	$A+B=f$	0	$\big([C_i][C_j]^\top + [C_i]^\top[C_j]\big)$.

$$PP^\top = \left(a^2 - ab - ac + \frac{(b^2+c^2)}{2} + \frac{(b-c)^2}{2f}\right) I + \left(ab + ac - \frac{(b^2+c^2)}{2} + \frac{(b+c)^2}{2f}\right) J. \quad (7.2)$$

Summarizing:

Theorem 7.1. *Suppose $p = 2f+1$ (f odd) is a prime power and G is the associated cyclic group $GF(p)/\{0\}$ of order $p-1$ with cyclotomic classes C_0 and C_1 of order f. Then*

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

a, b, c commuting variables, is a square matrix satisfying equation (7.2).

Corollary 7.1. *Suppose $p = 2f+1$ (f odd) is a prime power. Then there exists a nontrivial orthogonal integer matrix of order p.*

Proof. Set $a = \frac{-(f-1)c}{2}$, $b = 0$, and c any integer in Theorem 7.1.

We now use P to obtain orthogonal designs. Let X, Y, Z and W be derived from P given in Table 7.1 by setting

$$\begin{array}{ll} \text{i) } a = c = 0, & \text{iii) } a = b, c = 0, \\ \text{ii) } a = -b, c = 0, & \text{iv) } c = -b, \end{array}$$

respectively; then

$$\begin{aligned} XX^\top &= \left[\tfrac{1}{2}b^2(f+1)\right] I + \left[\tfrac{1}{2}b^2(f-1)\right] J, \\ YY^\top &= \left[\tfrac{1}{2}b^2(5+f)\right] I + \left[\tfrac{1}{2}b^2(f-3)\right] J, \\ ZZ^\top &= \left[\tfrac{1}{2}b^2(f+1)\right] I + \left[\tfrac{1}{2}b^2(f+1)\right] J, \\ WW^\top &= \left(a^2 + b^2 + 2b^2 f\right) I - b^2 J. \square \end{aligned}$$

Then we have:

Theorem 7.2. *Let $1+S$ be a skew-Hadamard matrix of order*

$$\textit{(i)}\ \tfrac{1}{2}(f+1), \quad \textit{(ii)}\ \tfrac{1}{2}(f-1), \quad \textit{(iii)}\ \tfrac{1}{2}(f+3),$$

Table 7.2 Cyclotomic numbers

	$\mathbf{C_0}$	$\mathbf{C_1}$	$\{\mathbf{0}\}$
00	B	A	f
11	A	B	f
01	A	A	0

(writing ii for $[C_i]^2$ and ij for $[C_i][C_j]$).

respectively, where $p = 2f+1$ (f odd) is a prime power. Then with X, Y, Z, W as above,

$$\textit{(i)}\ I\times XR+S\times W\,,\ \textit{(ii)}\ I\times YR+S\times W\,,\ \textit{(iii)}\ I\times ZR+S\times X\,,$$

respectively (R is the back circulant unit), are orthogonal designs of order

$$\begin{aligned}
&\textit{(i)}\ OD\left(\tfrac{1}{2}(f+1)(2f+1);\ \tfrac{1}{2}(f-1), f^2\right),\\
&\textit{(ii)}\ OD\left(\tfrac{1}{2}(f-1)(2f+1);\ \tfrac{1}{2}(f-3), (f-1)^2\right),\\
&\textit{(iii)}\ OD\left(\tfrac{1}{2}(f+3)(2f+1);\ \tfrac{1}{2}(f+1), (f+1)^2\right),
\end{aligned}$$

respectively.

Proof. Straightforward verification. □

Example 7.1. With $f = 5$ we see that an $OD(22;1,16)$ exists.

Case 2. $p = 2f+1$, $e = 2$, f *even*

Again we use

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

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

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

From Storer [200] the cyclotomic matrix for $e = 2$, f even, is

	0	**1**
0	B	A
1	A	A

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

Using Hunt and Wallis [110] we see that the expression $[C_i][C_j]$ is easily determined (see Table 7.2) and, since for f even $C_i^\top = C_i$, the cyclotomic arrays can be used immediately to evaluate $PP^\top$.

Hence

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

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

(i) $b=c$, or
(ii) $2a=b+c$.

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

$$PP^\top = \left(\frac{1}{4}(b-c)+(b-c)^2\frac{f}{2}\right)I + \left((b+c)^2\frac{f}{2}+bc\right)J.$$

Thus we have:

Theorem 7.3. *Let $p=2f+1$ (f even) be a prime power and G the associated cyclic group of $GF(p)$ of order $p-1$ with cyclotomic classes C_0 and C_1 of order f. Then*

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

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

$$PP^\top = \left(\frac{1}{4}(b-c)+(b-c)^2\frac{f}{2}\right)I + \left((b+c)^2\frac{f}{2}+bc\right)J.$$

To obtain orthogonal designs we will consider

$$\begin{aligned} P &= aI + b[C_0] + c[C_1] \\ Q &= aI + c[C_0] + b[C_1] \end{aligned} \tag{7.3}$$

Now

$$PP^\top + QQ^\top = \left((a-b-c)^2+a^2-2bc+(b-c)^2f\right)I + \left(2a(b+c)-(b^2+c^2)+(b+c)^2f\right)J.$$

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

$$MM^\top + NN^\top = 2\left(a^2+b^2+2b^2f\right)I - 2b^2J.$$

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

$$XX^\top + YY^\top = 2\left(d^2+b^2\right)I + 2b^2(2f-I)J,$$

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

Theorem 7.4. *Let $p = 4f + 1$ (f even or odd) be a prime power. Suppose there exists a skew-Hadamard matrix $I + S$ of order $4f$. Then*

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

is an $OD\left(8f(4f+I);\, 2, 2(4f-1), 32f^2\right)$.

Clearly, we have by no means exploited all the possibilities for constructing orthogonal designs by these methods, in particular, they could easily be used to obtain similar results for other e.

7.2 Sequences with Zero-autocorrelation Function

Sequences with zero or small auto-correlation function have long been of interest to engineers working on signal processing–for example, in radar and sonar.

R.J. Turyn [219] was the first to apply an idea common in the fields of radar pulse compression and work in surface wave encodings in constructing Baumert-Hall arrays.

The early work of Golay was concerned with two $(1, -1)$ sequences, but Welti approached the subject from the point of view of two orthonormal vectors, each corresponding to one of two orthogonal waveforms. Later work, including Turyn's [221], used four or more sequences. Kharaghani and Tayfeh-Rezaie [123] used 6 Turyn-type sequences of lengths $36, 36, 36, 36, 35, 35$ to find the most recently discovered Hadamard matrix of order 428 (See Section 7.7).

Other authors who have worked in this area are Jaurequi [118], Kruskal [139], Squire, Whitehouse and Aleup [199], Taki, Miyakawa, Hatori and Namba, [207] and Tseng [215].

Since we are concerned with orthogonal designs, we shall consider sequences of commuting variables.

Let $X = \{\{a_{11}, \ldots, a_{1n}\}, \{a_{21} \ldots\} \ldots \{a_{2n}, \ldots\} \ldots \{a_{m1}, \ldots, a_{mn}\}\}$ be m sequences of commuting variables of length n.

Definition 7.2. (1) The *non-periodic auto-correlation function of the family of sequences X* (denoted N_X) is a function defined by

$$N_x = \sum_{i=1}^{n-j} \left(a_{1,i}a_{1,i+j} + a_{2,i}a_{2,i+j} + \cdots + a_{m,i}a_{m,i+j}\right).$$

Note that if the following collection of m matrices of order it is formed,

$$\begin{bmatrix} a_{11}a_{12}\dots a_{1n} \\ a_{11} \quad a_{1,n-1} \\ \ddots \\ \bigcirc \quad a_{11} \end{bmatrix}, \begin{bmatrix} a_{21}a_{22}\dots a_{2n} \\ a_{21} \quad a_{2,n-1} \\ \ddots \\ \bigcirc \quad a_{11} \end{bmatrix} \dots \begin{bmatrix} a_{m1}a_{m2}\dots a_{mn} \\ \ddots \quad a_{m,n-1} \\ \ddots \\ \bigcirc \quad a_{11} \end{bmatrix}$$

then N_x is simply the sum of the inner products of rows 1 and $j+1$ of these matrices.

(2) The *periodic auto-correlation function of the family of sequences* X (denoted P_X) is a function defined by

$$P_X(j) = \sum_{i=1}^{n} (a_{1,i}a_{1,i+j} + a_{2,i}a_{2,i+j} + \dots + a_{m,i}a_{m,i+j}),$$

where we assume the second subscript is actually chosen from the complete set of residues modulo n.

We can interpret the function P_x, in the following way: form the m circulant matrices which have first rows, respectively,

$$[a_{11}a_{12}\dots a_{1n}], [a_{21}a_{22}\dots a_{2n}], \dots, [a_{m1}a_{m2}\dots a_{mn}];$$

then $P_X(j)$ is the sum of the inner products of rows 1 and $j+1$ of these matrices.

If X is as above with $N_X(j) = 0$, $j = 1, 2, \dots, n-1$, then we will call X *m–complementary sequences* of length n (they are also called *suitable sequences* because they work).

Our most useful construction uses m-complementary sequences with zero periodic autocorrelation function or zero non-periodic autocorrelation function, of length n, which are used to form first rows of circulant matrices which are plugged into some array. For us, the most useful case is to form four, $m = 4$, matrices of order n which are plugged into the Goethals-Seidel array to obtain matrices of order $4n$. In the case of sequences with zero non-periodic autocorrelation function, the sequences are first padded with sufficient zeros added to the beginning and/or the end to make their length n. We say the *weight* of a set of sequences X is the number of nonzero entries in X.

If $X = \{A_1, A_2, \dots, A_m\}$ are m-complementary sequences of length n and weight 2k such that

$$Y = \left\{ \frac{(A_1 + A_2)}{2}, \dots, \frac{(A_{2i-1} + A_{2i})}{2}, \frac{(A_{2i-1} - A_{2i})}{2}, \dots \right\}$$

are also m-complementary sequences (of weight k), then X will be said to be *m-complementary disjointable sequences* of length n. X will be said to be *m-complementary disjoint sequences* of length n if all $\binom{m}{2}$ pairs of sequences are disjoint, i.e. ,$A_i * A_j = 0$ for all i, j, where $*$ is the Hadamard product.

Example 7.2. For example {1 1 0 1}, {0 0 1 0 −}, {0 0 0 0 0 1 0 0 −}, {0 0 0 0 0 0 1 −} are disjoint as they have zero non-periodic auto-correlation function and precisely one $a_{ij} \neq 0$ for each j. (Here − means "minus 1".) With padding these sequences become

$$[11010000000], [0010-000000], [00000100-00], [0000000001-].$$

Notation 7.3. We sometimes use − for −1, and $\bar{x}$ for $-x$, and A^* to mean the order of the entries in the sequence A are reversed. We use the notation A/B to denote the interleaving of two sequences $A = \{a_1, \ldots, a_m\}$ and $B = \{b_1, \ldots, b_{m-1}\}$.

$$A/B = \{a_1, b_1, a_2, b_2, \ldots, b_{m-1}, a_m\}$$

and (A, B) to denote the adjoining

$$(A, B) = \{a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_{m-1}, b_m\}.$$

One more piece of notation is in order. If g_r denotes a sequence of integers of length r, then by xg_r we mean the sequence of integers of length r obtained from g_r by multiplying each member of g_r by x.

Proposition 7.1. *Let X be a family of sequences as above; then*

$$P_X(j) = N_X(j) + N_X(n-j), \quad j = 1, \ldots, n-1.$$

Corollary 7.2. *If $N_X(j) = 0$ for all $j = 1, \ldots, n-1$, then $P_X(j) = 0$ for all $j = 1, \ldots, n-1$.*

Note. $P_X(j)$ may equal 0 for all $j = 1, \ldots, n-1$, even though the $N_X(j)$ are not.

Definition 7.3. If $X = \{\{a_1, \ldots, a_n\}, \{b_1, \ldots, b_n\}\}$ are two sequences where $a_i, b_j \in \{1, -1\}$ and $N_X(j) = 0$ for $j = 1, \ldots, n-1$, then the sequences in X are called *Golay complementary sequences of length n* or a Golay pair. E.g.,

$n = 2$	11 and 1−
$n = 10$	1−−1−1−−−1 and 1−−−−−−11−
$n = 26$	111−−111−1−−−−−1−11−−1−−−− and
	−−−11−−−1−11−1−1−11−−1−−−−.

We note that if X is as above and A is the circulant matrix with first row $\{a_1, \ldots, a_n\}$ and B the circulant matrix with first row $\{b_1, \ldots, b_n\}$, then

$$AA^\top + BB^\top = \sum \left(a_i^2 + b_i^2\right) I_n.$$

Consequently, such matrices may be used to obtain Hadamard matrices constructed from two circulants.

We would like to use Golay sequences to construct other orthogonal designs, but first we consider some of their properties.

Lemma 7.3. *Let $X = \{\{a_1,\ldots,a_n\},\{b_1,\ldots,b_n\}\}$ be Golay complementary sequences of length n. Suppose k_1 of the a_i are positive and k_2 of the b_i are positive; then*

$$n = (k_1 + k_2 - n)^2 + (k_1 - k_2)^2\,,$$

and n is even.

Proof. Since $P_X(j) = 0$ for all j, we may consider the two sequences as $2 - \{n; k_1, k_2; \lambda\}$ supplementary difference sets with $\lambda = k_1 + k_2 - \frac{1}{2}n$. But the parameters (counting differences two ways) satisfy $\lambda(n-1) = k_1(k_1-1) + k_2(k_2-1)$. On substituting λ in this equation we obtain the result of the enunciation. □

The smaller values of n, k_1, k_2 of the lemma are considered in Table 7.3. We note that the lemma says there is "no solution" when the length n is not the sum of two squares. "OK" in the table indicates an order for which Golay sequences exist (see later in this section). Malcolm Griffin has shown (see Theorem 7.5) no Golay sequences can exist for lengths $n = 2.9^t$. The value $n = 18$ had previously been excluded by a complete search but is now theoretically excluded by Griffin's theorem and independently by a result of Kruskal [139] and C. H. Yang [253]. The powerful results of Eliahou-Kervaire-Saffari [56,57] show that there are no Golay sequences of length n when any factor of the prime decomposition of n is $\equiv 3 \pmod 4$.

Lemma 7.4. *For Golay sequences $X = \{\{x_i\},\{y_i\}\}$ of length n*

$$x_{n-i+1} = e_i x_i \Leftrightarrow y_{n-i+1} = -e_i y_i,\ \textit{where } e_i = \pm 1\,.$$

That is,

$$x_{n-i+1}x_i = -y_{n-i+1}y_i\,,$$

Example 7.3. The sequences of length 10 are

$$1--1-1---1$$
$$1------11-$$

Clearly, $e_l = 1$, $e_2 = 1$, $e_3 = 1$, $e_4 = -1$, and $e_5 = -1$.

Proof. We use the fact that if x, y, z are ± 1, $(x+y)z \equiv x+y \pmod 4$ and $x + y \equiv xy + 1 \pmod 4$.

Let $i = 1$. Clearly the result holds. We proceed by induction. Suppose the result is true for every $i \le k-1$. Now consider $N(j) = N(n-k) = 0$, and we have

Table 7.3 Smaller values of n

n and **Status**					
2	OK	34	do not exist	68	?
4	OK	36	do not exist	70	no solution
6	no solution	38	no solution	72	no solution
8	OK	40	OK	74	?
10	OK	42	no solution	76	no solution
12	no solution	44	no solution	78	no solution
14	no solution	46	no solution	80	OK
16	OK	48	no solution	82	?
18	do not exist	50	do not exist	84	no solution
20	OK	52	OK	86	no solution
22	no solution	54	no solution	88	no solution
24	no solution	56	no solution	90	no solution
26	OK	58	do not exist	92	no solution
28	no solution	60	no solution	94	no solution
30	no solution	62	no solution	96	no solution
32	OK	64	OK	98	no solution
		66	no solution	100	OK

$$
\begin{aligned}
0 &= x_1x_{n+1-k} + x_2x_{n+2-k} + \cdots + x_kx_n + y_1y_{n+1-k} + y_2y_{n+2-k} + \cdots + y_ky_n \\
&= x_ie_kx_k + x_2e_{k-1}x_{k-1} + \cdots + x_ke_1x_1 + y_1y_{n+l-k} \\
&\qquad\qquad - y_2e_{k-1}y_{k-1} - \cdots - y_ke_1y_1 \\
&\equiv e_1 + e_2 + \cdots + e_k + y_1y_{n+1-k} - e_{k-1} - \cdots - e_2 - y_ke_1y_1 \pmod 4 \\
&\equiv e_1 + e_k + y_1y_{n+1-k} - y_ke_1y_1 \pmod 4 \\
&\equiv e_k + y_ky_{n+1-k} \pmod 4 \\
&\equiv 0 \pmod 4 .
\end{aligned}
$$

So

$$y_{n+1-k} = -e_ky_k \square$$

Lemma 7.5 (Griffin [93]). *Let $a_0, a_1, \ldots, a_m$ and $b_0, b_1, \ldots, b_m$ be Golay sequences of length $2n = m+1$. We recall that $a_{2n-1-i} = e_ia_i \Leftrightarrow b_{2n-1-i} = -e_ib_i$ and write $S = \{0 \le i \le n \colon e_i = 1\}$ and $D = \{0 \le i \le n \colon e_i = -1\}$. Let η be a $2n$-th root of unity and ζ be a $4n$-th root of unity. Then*

$$\left|\sum_{i=0}^{m} a_i\eta^i\right|^2 + \left|\sum_{i=0}^{m} b_i\eta^i\right|^2 = 4n . \tag{7.4}$$

and

$$\left|\sum_{i\in S} a_i Re\left(\zeta^{2i+1}\right)\right|^2 + \left|\sum_{i\in D} a_i Im\left(\zeta^{2i+1}\right)\right|^2 + \left|\sum_{i\in S} b_i Im\left(\zeta^{2i+1}\right)\right|^2 + \left|\sum_{i\in S} a_i Re\left(\zeta^{2i+1}\right)\right|^2 = n \tag{7.5}$$

Remark 7.1. Equation (7.5) is not equivalent to being a Golay sequence, as can be seen from the sequences

$$X = \{\{1,1,1,1,-1,-1,1,1\},\ \{1,-1,-1,1,1,-1,1,-1\}\}$$

which satisfy (7.5) but for which $N_X \neq 0$.

Proof. We recall that for Golay sequences X, $N_X = 0 \Rightarrow P_X = 0$. Thus if $T = (t_{ij})$ is defined by $t_{12} = t_{i,i+1} = 1$ and all other elements zero, we have, writing

$$A = \sum_{i=0}^{m} a_i T^i \text{ and } B = \sum_{i=0}^{m} b_i T^i,$$
$$AA^\top + BB^\top = 4nI.\square$$

Since $TT^\top = T^{2n} = I$ and T has characteristic polynomial $\lambda^{2n} - 1$, there exists a unitary matrix U such that $USU^* = \Delta = diag(1,\xi,\xi,\ldots,\xi^m)$, where ξ is a primitive $2n$-th root of unity. Consequently

$$\left(\sum_{i=0}^{m} a_i \Delta^i\right)\left(\sum_{i=0}^{m} a_i \Delta^i\right)^* + \left(\sum_{i=0}^{m} b_i \Delta^i\right)\left(\sum_{i=0}^{m} b_i \Delta^i\right)^* = 4nI.$$

Let $\eta = \xi^{j-1}$; then the j-th term on the main diagonal gives

$$4n = \left(\sum_{i=0}^{m} a_i \eta^i\right)\left(\sum_{i=0}^{m} a_i \eta^{-i}\right) + \left(\sum_{i=0}^{m} b_i \eta^i\right)\left(\sum_{i=0}^{m} b_i \eta^{-i}\right)$$
$$= \left|\sum_{i=0}^{m} a_i \eta^i\right|^2 + \left|\sum_{i=0}^{m} b_i \eta^i\right|^2. \qquad \text{(Condition (1))}$$

We now substitute $a_{2n-i-1} = e_i a_i$ and $b_{2n-i-1} = e_i b_i$, $0 \leq i < n$, in Condition (1) with $\eta = \zeta^2$. Thus

$$
\begin{aligned}
4n &= \left|\sum_{i=0}^{n-1}\left(a_i\eta^i + e_i a_i \eta^{-(i+1)}\right)\right|^2 + \left|\sum_{i=0}^{n-1}\left(b_i\eta^i - e_i b_i \eta^{-(i+1)}\right)\right|^2 \\
&= \left|\sum_{i\in S} a_i\left(\zeta^{2i}+\zeta^{-(2i+2)}\right) + \sum_{i\in D} a_i\left(\zeta^{2i}-\zeta^{-(2i+2)}\right)\right|^2 \\
&\qquad + \left|\sum_{i\in S} b_i\left(\zeta^{2i}-\zeta^{-(2i+2)}\right) + \sum_{i\in D} b_i\left(\zeta^{2i}+\zeta^{-(2i+2)}\right)\right|^2 \\
&= \left|\sum_{i\in S} a_i\left(\zeta^{2i+1}+\zeta^{-(2i+1)}\right) + \sum_{i\in D} a_i\left(\zeta^{2i+1}-\zeta^{-(2i+1)}\right)\right|^2 \\
&\qquad + \left|\sum_{i\in S} b_i\left(\zeta^{2i+1}-\zeta^{-(2i+1)}\right) + \sum_{i\in D} b_i\left(\zeta^{2i+1}+\zeta^{-(2i+1)}\right)\right| \\
&= 4\left|\sum_{i\in S} a_i Re\left(\zeta^{2i+1}\right)\right|^2 + 4\left|\sum_{i\in D} a_i Im\left(\zeta^{2i+1}\right)\right|^2 \\
&\qquad + 4\left|\sum_{i\in S} b_i Im\left(\zeta^{2i+1}\right)\right|^2 + 4\left|\sum_{i\in D} b_i Re\left(\zeta^{2i+1}\right)\right|^2 \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(Condition (2))}
\end{aligned}
$$

We now use Condition (2) to prove:

Theorem 7.5 (Griffin [93]). *There are no Golay sequences of length* 2.9^t.

Proof. We show that Condition (2) cannot be satisfied for all 12^{th} roots when n is a power of 3. Setting $S = -I$ in Condition (2), we get

$$
\left(\sum_S a_i\right)^2 + \left(\sum_D b_i\right)^2 = n\,. \qquad \text{(Condition (3))}
$$

If n is a product of primes, each $\equiv 3 \pmod 4$, then by elementary number theory, n must be a square, $n = q^2$, and solutions to this equation must be unique (up to order and sign), yielding

$$
\sum_S a_i + \sum_D b_i = \alpha q\,, \quad \alpha = \pm 1\,. \qquad \text{(Condition (4))}
$$

If $3|q$, we use $\xi = \frac{1}{2} + \frac{1}{2}\sqrt{-3}\left(\xi^3 = -1,\ \xi^5 = \xi^{-1}\right)$ in Condition (2) to give a Diophantine equation of the form

$$
3\left(c^2 + d^2\right) + e^2 + f^2 = 4q^2\,, \qquad \text{(Condition (5))}
$$

and since the summation in forming c involves only $i \in D$ with $i \not\equiv 1 \pmod 3$ and the summation for d involves $i \in S$ with $i \not\equiv 1 \pmod 3$, c and d involve $\frac{2}{3}$

of the q^2 elements, and consequently $c \equiv d \pmod 3$. Taking residues $\bmod 8$ shows that c, d, e, f are all even, giving

$$3\left(c_0^2 + d_0^2\right) + e_0^2 + f_0^2 = q^2 .$$

When q is a power of 3, this equation has a unique solution (up to order and sign), so $c = d = 0$ and $e + f = 2\beta q$, $\beta = \pm 1$. From now on assume that q is a power of 3. Let $S(0) = \{i \in S | i \equiv 0, 5 \pmod 6\}$, $S(1) = \{i \in S \equiv 1, 4 \pmod 6\}$ and $S(2) = \{i \in S | i \equiv 2, 3 \pmod 6\}$ with a similar notation for D. Then $e + f = 2\beta q$ gives

$$\sum_S a_i - 3\sum_{S(1)} a_i + \sum_D b_i - 3\sum_{d(1)} b_i = 2\beta q . \qquad \text{(Condition (6))}$$

The same argument with $\xi = \frac{1}{2}\left(\sqrt{3} + \sqrt{-1}\right)$ a primitive 12-th root again yields an equation of type Condition (5), and $c = d = 0$ gives $c + d = 0$; so

$$\sum_{S(0)} a_i - \sum_{S(2)} a_i + \sum_{D(0)} b_1 - \sum_{D(2)} b_i = 0 . \qquad \text{(Condition (7))}$$

Adding Condition (6), twice Condition (4), and thrice Condition (7), we get

$$6\left(\sum_{S(0)} a_i + \sum_{D(0)} b_i\right) = 2q(\alpha + \beta) \equiv 0 \pmod 4 .$$

But this is a contradiction since $S(0) \cup D(0$ has an odd number of elements, $\frac{q^2}{3}$. □

7.2.1 Other sequences with zero auto-correlation function

We now discuss other sequences with zero auto-correlation function.

Lemma 7.6. *Suppose $X = \{X_1, X_2, \ldots, X_m\}$ is a set of $(0, 1, -1)$ sequences of length n for which $N_X = 0$ or $P_X = 0$. Further suppose the weight of X_i is x_i and the sum of the elements of X_i is a_i. Then*

$$\sum_{i=1}^{m} a_i^2 = \sum_{i=1}^{m} x_i$$

Proof. Form circulant matrices Y_i for each X_i. Then

$$Y_i J = a_i J \quad \text{and} \quad \sum_{i=1}^{m} Y_i Y_i^{\top} = \sum_{i=1}^{m} x_i$$

Now considering

$$\sum_{i=1}^{m} Y_i Y_i^{\top} J = \sum_{i=1}^{m} a_i^2 J = \sum_{i=1}^{m} x_i J\,,$$

we have the result. □

Now a few simple observations are in order, and for convenience we put them together as a lemma. We use X^* to denote the elements of a sequence X written in the reverse order.

Lemma 7.7. *Let $X = \{A_1 A_2, \ldots, A_m\}$ are m-complementary sequences of length n. Then*

(i) $Y = \{A_1^*, A_2^*, \ldots, A_i^*, A_{i+1}, \ldots, A_m\}$ *are m-complementary sequences of length n;*

(ii) $W = \{A_1, A_2, \ldots, A_i, -A_{i+1}, \ldots, -A_m\}$ *are m-complementary sequences of length n;*

(iii) $Z = \{\{A_1, A_2\}, \{A_1, -A_2\}, \ldots, \{A_{2i-1}, A_{2i}\}, \{A_{2i-1}, -A_{2i}\}, \ldots\}$ *are $m-$ (or $m+1$ if m was odd when we let A_{m+1} be n zeros) complementary sequences of length $2n$;*

(iv) $U = \{\{A_1/A_2\}, \{A_1/-A_2\}, \ldots, \{A_{2i-1}/A_{2i}\}, \{A_{2i-1}/-A_{2i}\}, \ldots\}$, *where A_j/A_k means $a_{j1}a_{k1}a_{j2}a_{k2}\ldots a_{jn}a_{kn}$, are m- (or $m+1$ if m was odd when we let A_{m+1} be n zeros) complementary sequences of length $2n$.*

By a lengthy but straightforward calculation, it can be shown that:

Theorem 7.6. *Suppose $X = \{A_1, \ldots, A_{2m}\}$ are $2m$-complementary sequences of length n and weight ℓ and $Y = \{B_1, B_2\}$ are 2-complementary disjointable sequences of length t and weight $2k$. Then there are $2m$-complementary sequences of length nt and weight $k\ell$.*

The same result is true if X are $2m$-complementary disjointable sequences of length n and weight 2ℓ and Y are 2-complementary sequences of weight k.

Proof. Using an idea of R.J. Turyn [221], we consider

$$A_{2i-1} \times \frac{(B_1 + B_2)}{2} + A_{2i} \times \frac{(B_1^* - B_2^*)}{2} \quad \text{and}$$
$$A_{2i-1} \times \frac{(B_1 - B_2)}{2} - A_{2i} \times \frac{(B_1^* + B_2^*)}{2}$$

for $i = 1, \ldots, m$, which are the required sequences in the first case, and

$$\frac{(A_{2i-1} + A_{2i})}{2} \times B_1 + \frac{(A_{2i-1} - A_{2i})}{2} \times B_2^* \quad \text{and}$$
$$\frac{(A_{2i-1} + A_{2i})}{2} \times B_2 - \frac{(A_{2i-1} - A_{2i})}{2} \times B_1^*\,,$$

for $i = 1, \ldots, m$, which are the required sequences for the second case. □

The proof now follows by an exceptionally tedious but straightforward verification.

Corollary 7.3. *Since there are Golay sequences of lengths 2, 10, and 26, there are Golay sequences of length* $2^a 10^b 26^c$ *for a, b, c non-negative integers.*

Corollary 7.4. *There are 2-complementary sequences of lengths* $2^a 6^b 10^c 14^d 26^e$ *of weights* $2^a 5^b 10^c 13^d 26^e 2$*, where a, b, c, d, e are non-negative integers.*

Proof. Use the sequences of Tables G.8 and G.9 of Appendix G. □

7.3 Current Results for Non-Periodic Golay Pairs

Through extended calculations made by hand, Golay demonstrated the existence of two inequivalent pairs at length 10 and a pair at length 26. He also gave rules of composition for forming pairs of lengths $2n$ and $2mn$ from existing pairs of length m and n. His constructions for lengths 2^k give all existing pairs for $0 \leq k \leq 6$.

The first exhaustive search for Golay pairs was conducted at length 26 (Jauregui [118]), taking 75 hours to confirm the single example of inequivalent pairs. In his 1977 master's thesis, Andres [5] showed that a further reduction modulo 2 enables an initial search involving $2^{\frac{n}{2}}$ cases. A further reduction modulo 4 was applied for examples surviving this test. He used one of the equivalences, bringing this to a $2^{\frac{n}{2}-1}$ search, reducing the time taken at $n = 26$ to 1 minute. His work showed nonexistence of pairs at lengths 34, 50 and 58 and produced complete lists of representatives at lengths 8, 10, 16, 20 and 32. Later work by James [116] (1987) established the nonexistence of pairs at length 68. Đoković [43] (1998) demonstrated how to choose a canonical pair from each class of equivalent pairs. He conducted exhaustive searches at lengths 32 and 40, producing complete lists of canonical pairs.

The work of Borwein and Ferguson [25] outlines improvements which may be made to Andres' algorithm, enabling a $2^{\frac{n}{2}-5}$ search at length 82 with a running time of two weeks. Exhaustive searches have been conducted at all allowable lengths under 100, confirming earlier work and showing the nonexistence of pairs at lengths 74 and 82.

Recent search results by Borwein and Ferguson [25] are summarized in Table G.1. For all lengths other than 1, 2, 4, and 80, complete lists of canonical pairs were compiled by the search program. The total numbers of pairs agree exactly with those obtained by compositions from the primitive pairs. At length 80, the search was restricted to canonical pairs for which no conjugate is H-regular. The total number of pairs is that determined by composition from the two primitive pairs at length 10 and the single primitive pair of

length 20. (The superscript σ in Table G.1 indicates work done at Simon Frazer University.)

A Golay pair is said to be *primitive* if it cannot be derived through composition from pairs of shorter lengths. A theory for producing pairs of length 2^n from a primitive pair of length n is developed in [25].

Golay complementary sequences contain no zeros but considerable effort has also been devoted to ternary complementary sequences which still have zero non-periodic autocorrelation function but contain elements $\{0, \pm 1\}$. Craigen and Koukouvinos [37] have made a theory for these ternary sequences and given a table for their existence for some smaller lengths and weights.

7.4 Recent Results for Periodic Golay Pairs

Đoković and Kotsireas [51] show that if $v > 1$ is a periodic Golay number then v is even, it is a sum of two squares and satisfies the Arasu-Xiang condition [51, Theorem 2, p.525]. They cite new lengths 34,50,58,74,82,122,136,202,226 as those for which periodic sequences exist. Periodic sequences can be used in the construction of T-matrices. The following list is all numbers in the range $1, 2, \ldots, 300$ which satisfy the three necessary conditions and for which the question whether they are periodic Golay numbers remains open:

$$90, 106, 130, 146, 170, 178, 180, 194, 212, 218, 234, 250, 274, 290, 292, 298\,.$$

This list may be useful to readers interested in constructing new periodic Golay pairs or finding new periodic Golay numbers.

7.5 Using complementary sequences to form Baumert-Hall arrays

We now discuss other sequences with zero autocorrelation function.

Lemma 7.8. *Suppose that $X = \{X_1, X_2, \ldots, X_m\}$ is a set of 0, ± 1 sequences of length n for which $N_X = 0$ or $P_X = 0$. Further suppose that the weight of X_i is x_i and the sum of the elements of X_i is a_i. Then*

$$\sum_{i=1}^{n} a_i^2 = \sum_{i=1}^{m} x_i.$$

Proof. Form the circulant matrices Y_i for each X_i. Then

$$Y_i J = a_i J \quad \text{and} \quad \sum_{i=1}^{m} Y_i Y_i^{\top} = \sum_{i=1}^{m} x_i I.$$

Now considering

$$\sum_{i=1}^{m} Y_i Y_i^{\top} J = \sum_{i=1}^{m} a_i^2 J = \sum_{i=1}^{m} x_i J$$

we have the result. □

We now propose to use R.J. Turyn's [216] idea of using m-complementary sequences to construct orthogonal designs.

Lemma 7.9. *Consider four* $(1,-1)$ *sequences* $A = \{X,U,Y,W\}$*, where*

$$\begin{aligned}
X &= \{x_1 = 1, x_2, x_3, \ldots, x_m, h_m x_m, \ldots, h_3 x_3, h_2 x_2, h_1 x_1 = -1\},\\
U &= \{u_1, u_2, u_3, \ldots, u_m, f_m u_m, \ldots, f_3 u_3, f_2 u_2, f_1 u_1 = 1\},\\
Y &= \{y_1, y_2, \ldots, y_{m-1}, y_m, g_{m-1} y_{m-1}, \ldots, g_3 y_3, g_2 y_2, g_1 y_1\},\\
V &= \{v_1, v_2, \ldots, v_{m-1}, v_m, e_{m-1} v_{m-1}, \ldots, e_3 v_3, e_2 v_2, e_1 v_1\}.
\end{aligned}$$

Then $N_A = 0$ *implies that* $h_i = f_i$ *for* $i \geq 2$ *and* $g_j = e_j$ *for* $j \geq 2$*. Here*

$$\begin{aligned}
8m-2 = &\left(\sum_{i=1}^{m}(x_i + x_i h_i)\right)^2 + \left(\sum_{i=1}^{m}(u_i + u_i f_i)\right)^2\\
&+ \left(y_m + \sum_{i=1}^{m-1}(y_i + y_i g_i)\right)^2 + \left(v_m + \sum_{i=1}^{m-1}(v_i + v_i e_i)\right)^2.
\end{aligned}$$

Proof. We note that if a, b, x, y, z are all ± 1, $a+b \equiv ab+1 \pmod 4$, and so $x+xyz \equiv y+z \pmod 4$. Clearly, $N_A(2m-1) = 0$ gives $-h_1 = f_1 = 1$, and

$$\begin{aligned}
N_A(2m-2) &= x_1 x_2 h_2 + x_2 h_1 x_1 + f_2 u_1 u_2 + u_2 f_1 u_1 + g_1 y_1^2 + e_1 v_1^2\\
&\equiv h_1 + h_2 + f_1 + f_2 + g_1 + e_1 \pmod 4\\
&\equiv h_2 f_2 + g_1 e_1 + 2 \pmod 4\\
&\equiv 0 \pmod 4.
\end{aligned}$$

This gives $h_2 f_2 = g_1 e_1$. We proceed by induction to show that $h_i f_i = g_{i-1} e_{i-1}$ for all $i \leq m$.

Assume $h_i f_i = g_{i-1} e_{i-1}$, i.e. $h_i + f_i + g_{i-1} + e_{i-1} \equiv 0 \pmod 4$ for all $i < k \leq m$. Now consider

$$\begin{aligned}
N_A(2m-k) &= (x_1x_kh_k + x_2x_{k-1}h_{k-1} + \cdots + x_{k-1}x_2h_2 + x_kx_1h_1)\\
&\quad + (u_1u_kf_k + u_2u_{k-1}f_{k-1} + \cdots + u_{k-1}u_2f_2 + u_ku_1f_1)\\
&\quad + (y_1y_{k-1}g_{k-1} + y_2y_{k-2}g_{k-2} + \cdots + y_{k-2}y_2g_2 + y_{k-1}y_1g_1)\\
&\quad + (v_1v_{k-1}e_{k-1} + v_2v_{k-2}e_{k-2} + \cdots + v_{k-2}v_2e_2 + v_{k-1}v_1e_1)\\
&\equiv h_1 + \cdots + h_k + f_1 + \cdots + f_k + g_1 + \cdots + g_{k-1}\\
&\qquad\qquad + e_1 + \cdots + e_{k-1} \pmod 4\\
&\equiv h_kf_k + g_{k-1}e_{k-1} + 2 \pmod 4\\
&\equiv 0 \pmod 4.
\end{aligned}$$

This gives the result for all $i \le m$.

Suppose $k = m + j > m$. Then

$$\begin{aligned}
N_A(2m-k) &= (x_1x_{m-j+1} + \cdots + x_jx_m) + (x_{j+1}h_mx_m + \ldots\\
&\quad + x_mh_{j+1}x_{j+1}) + (h_mx_mh_jx_j + \cdots + h_{m-j+1}x_{m-j+1}h_1x_1)\\
&\quad + (u_1u_{m-j+1} + \cdots + u_ju_m) + (u_{j+1}f_mu_m + \cdots + u_mf_{j+1}u_{j+1})\\
&\qquad + (f_mu_mf_ju_j + \cdots + f_{m-j+1}u_{m-j+1}f_1u_1)\\
&\qquad\quad + (y_1y_{m-j+1} + \cdots + y_jy_m)\\
&\qquad\qquad + (y_{j+1}g_{m-1}y_{m-1} + \cdots + y_{m-1}g_{j+1}y_{j+1})\\
&\qquad\qquad\quad + (y_mg_jy_j + \cdots + g_{m-j+1}y_{m-j+1}g_1y_1)\\
&\qquad\qquad\qquad + (v_1v_{m-j+1} + \cdots + v_jm_j)\\
&\qquad\qquad\qquad\quad + (v_{j+1}e_{m-1}v_{m-1} + \cdots + v_{m-1}e_{j+1}v_{j+1})\\
&\qquad\qquad\qquad\qquad + (v_me_jv_j + \cdots + e_{m-j+1}v_{m-j+1}e_1v_1)\\
&\equiv h_1f_1 + h_{m-j+1}f_{m-j+1} \pmod 4\\
&\equiv h_{m-j+1}f_{m-j+1} - 1 \pmod 4
\end{aligned}$$

Hence $h_{m-j+1}f_{m-j+1} = 1$. So in general $h_if_i = 1$, $i \ge 2$ and $e_ig_i = 1$.

The last result follows by Lemma 7.7. □

Corollary 7.5. *Consider four* $(1,-1)$ *sequences* $A = \{X,U,Y,V\}$, *where*

$$\begin{aligned}
X &= \{x_1 = 1, x_2, x_3, \ldots, x_m, -x_m, \ldots, -x_3, -x_2, -x_1 = -1\},\\
U &= \{u_1 = 1, u_2, u_3, \ldots, u_m, f_mu_m, \ldots, f_3u_3, f_2u_2, f_1u_1 = 1\},\\
Y &= \{y_1, y_2, \ldots, y_{m-1}, y_m, y_{m-1}, \ldots, y_3, y_2, y_1\},\\
V &= \{v_1, v_2, \ldots, v_{m-1}, v_m, e_{m-1}v_{m-1}, \ldots, e_3v_3, e_2v_2, e_1v_1\}.
\end{aligned}$$

Then $N_A = 0$ *implies that all* e_i *are* $+1$ *and all* f_i *are* -1. *Here* $8m-6$ *is the sum of two squares.*

Similarly we can prove

Corollary 7.6. *Consider four* $(1,-1)$ *sequences* $A = \{X,U,Y,V\}$, *where*

$$X = \{x_1 = 1, x_2, x_3, \ldots, x_m, x_{m+1}, x_m, \ldots, x_3, x_2, x_1 = 1\},$$
$$U = \{u_1 = 1, u_2, u_3, \ldots, u_m, u_{m+1}, f_m u_m \ldots, f_3 u_3, f_2 u_2, -1\},$$
$$Y = \{y_1, y_2, \ldots, y_m, -y_m, \ldots, -y_2, -y_1\},$$
$$V = \{v_1, v_2, \ldots, v_m, e_m v_m, \ldots, e_2 v_2, e_1 v_1\}.$$

which have $N_A = 0$. *Have* $e_i = -1$ *for all* i *and* $f_i = +1$ *for all* i. *Here* $8m+2$ *is the sum of two squares.*

Definition 7.4. Sequences such as those described in Lemma 7.9 will be called *Turyn sequences* of length ℓ: (the four sequences are of weights ℓ, ℓ, $\ell-1$ and $\ell-1$). A sequence $X = \{x_1, \ldots, x_n\}$ will be called *skew* if n is even and $x_i = -x_{n-i+1}$ and *symmetric* if n is odd and $x_i = x_{n-i+1}$.

Lemma 7.10. *There exist Turyn sequences of lengths* $2, 4, 6, 8, 3, 5, 7, 13$ *and* 15.

Proof. Consider

$$\ell = 2 : X = \{\{1-\}, \{11\}, \{1\}, \{1\}\}$$
$$\ell = 4 : X = \{\{11--\}, \{11-1\}, \{111\}, \{1-1\}\}$$
$$\ell = 6 : X = \{\{111---\}, \{11-1-1\}, \{11-11\}, \{11-11\}\}$$
$$\ell = 8 : X = \{\{11-1-1--\}, \{1111---1\}, \{111-111\}, \{1--1--1\}\}$$
$$\ell = 3 : X = \{\{111\}, \{11-\}, \{1-\}, \{1-\}\}$$
$$\ell = 5 : X = \{\{11-11\}, \{1111-\}, \{11--\}, \{11--\}\}$$
$$\ell = 7 : X = \{\{111-111\}, \{11---1-\}, \{11-1--\}, \{11-1--\}\}$$
$$\ell = 13 : X = \{\{1111-1-1-1111\}, \{111--1-1--11-\}, \{111-11--1---\}, \{111--1-11---\}\},$$

or

$$X = \{\{111-11-11-111\}, \{111-1-1-11-\}, \{11-1-111\}, \{1111-1-1-----\}\}$$
$$\ell = 15 : X = \{\{11-111-1-111-11\}, \{111-11---11-11-\}, \{111--1-11-----\}, \{1----1-1-1111-\}\}.\square$$

Remark 7.2. These sequences were constructed using the Research School of Physical Sciences, Australian National University, DEC-10 System in 1972-73.

A complete computer search in the case of $2 = 9$, 10, 14 and 16 gave no solution for any decomposition into squares. The results are listed in Table 7.4.

Edmondson, Seberry and Anderson [55] using a combination of mathematics and computer search show there are no further Turyn sequences of length

Table 7.4 Turyn sequences for $4\ell-6=x^2+y^2$

ℓ	$4\ell-6=x^2+y^2$	Result
6	$18=3^2+3^2$	yes
8	$26=1^2+5^2$	yes
10	$34=3^2+5^2$	none
12	$42\neq x^2+y^2$	no
14	$50=1^2+7^2$	none
	$=5^2+5^2$	none
16	$58=3^2+7^2$	none
18	$66\neq x^2+y^2$	no

$n\leq 43$. We note that at this time, year 2016, about length 43 is the upper limit for these types of computer searches.

Conjecture 7.1. The lengths $2,4,6,8,3,5,7,13,15$ are the only lengths for Turyn sequences.

In order to satisfy the conditions of Theorem 4.15, we are led to study sequences of a more restricted type.

Definition 7.5. Four complementary disjoint $(0,1,-1)$ sequences of length t and total weight t will be called *T-sequences.*

Example 7.4. Consider

$$T=\{\{10000\},\{01100\},\{0001-\},\{00000\}\}.$$

The sequences are disjoint, as the i-th entry is non-zero in one and only one of the four sequences. The total weight is 5, and $N_T=0$.

Another example is obtained by using the Golay sequences

$$X=1--1-1---1 \quad \text{and} \quad Y=1-------11-.$$

Let $\underline{0}$ be the vector of 10 zeros; then

$$T=\big\{\{1,\underline{0}\},\{0,\tfrac{1}{2}(X+Y)\},\{0,\tfrac{1}{2}(X-Y)\},\{0,\underline{0}\}\big\}$$

are T sequences of length 11.

Theorem 7.7 (Turyn). *Suppose $A=\{X,U,Y,V\}$ are Turyn sequences of length ℓ, where X is skew and Y is symmetric for ℓ even and X is symmetric and Y is skew for ℓ odd. Then there are T-sequences of length $2\ell-1$ and $4\ell-1$.*

Proof. We use the notation A/B as before to denote the interleaving of two sequences $A=\{a_1,\ldots,a_m\}$ and $B=\{b_1,\ldots,b_{m-1}\}$.

$$A/B=\{a_1,b_1,a_2,b_2,\ldots,b_{m-1},a_m\}.$$

Let 0_t be a sequence of zeros of length t. Then

$$T_1=\left\{\{\tfrac{1}{2}(X+Y),0_{\ell-1}\},\{\tfrac{1}{2}(X-Y),0_{\ell-1}\},\{0_\ell,\tfrac{1}{2}(Y+V)\},\{0_\ell,\tfrac{1}{2}\{(Y-V)\}\}\right\}$$

and

$$T_2=\{\{1,0_{4\ell-2}\},\{0,X/Y,0_{2\ell-1}\},\{0,0_{2\ell-1},U/0_{\ell-1}\},\{0,0_{2\ell-1},0_\ell/V\}\}$$

are the T-sequences of lengths $2\ell-1$ and $4\ell-1$, respectively. □

Corollary 7.7. *There are T-sequences constructed from Turyn sequences of lengths* $3,5,7,9,11,13,15,19,23,25,27,29,31,51,59$.

Theorem 7.8. *If X and Y are Golay sequences of length r, then writing 0_r for the vector of r zeros, $T=\{\{1,0_r\},\{0,\frac{1}{2}(X+Y)\},\{0,\frac{1}{2}(X-Y)\},\{O_r+1\}\}$ are T-sequences of length $r+1$.*

Corollary 7.8 (Turyn [221]). *There exist T-sequences of lengths $1+2^a10^b26^c$, where a,b,c are non-negative integers.*

Combining these last two corollaries, we have

Corollary 7.9. *There exist T-sequences of lengths* 3, 5, 7,…,33, 41, 51, 53, 59, 65, 81, *and* 101.

A desire to fill the gaps in the list in Corollary 7.9 leads to the following idea.

Lemma 7.11. *Suppose $X=\{A,B,C,D\}$ are 4-complementary sequences of length $\ell,\ell,\ell-1,\ell-1$, respectively, and weight k. Then*

$$Y=\{\{A,C\},\{A,-C\},\{B,D\},\{B,-D\}\}$$

are 4-complementary sequences of length $2\ell-1$ and weight $2k$. Further, if $\frac{1}{2}(A+B)$ and $\frac{1}{2}(C+D)$ are also $(0,1,-1)$ sequences, then, with 0_t the sequence of t zeros,

$$Z=\left\{\{\tfrac{1}{2}(A+B),0_{\ell-1}\},\{\tfrac{1}{2}(A-B),0_{\ell-1}\},\{0_\ell,\tfrac{1}{2}(C+D)\},\{0_\ell,\tfrac{1}{2}(C-D)\}\right\}$$

are 4-complementary sequences of length $2\ell-1$ and weight k. If A,B,C,D are $(1,-1)$ sequences, then Z consists of T-sequences of length $2\ell-1$.

In fact, Turyn has found sequences satisfying these conditions.

Corollary 7.10. *The following four* $(1,-1)$ *sequences are of lengths* 24, 24, 23, 23*:*

$$
\begin{array}{cccccccccccccccccccccccc}
1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 \\
1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 \\
1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 & 1
\end{array}
$$

Hence there are T*-sequences of length* 47*.*

These sequences may be used in the Goethals-Seidel array to construct the Hadamard matrix of order 188 which was unknown for over 40 years. This method is far more insightful than the construction given in Hedayat and Wallis [98].

We may summarise these results in one theorem.

Theorem 7.9. *If there exist* T*-sequences of length* t*, then*

(i) there exist T*-matrices of order* t*;*
(ii) there exists a Baumert-Hall array of order t*;*
(iii) there exists an orthogonal design $OD(4t;t,t,t,t)$*.*

Proof. (i) follows by using the T-sequences as first rows of circulant matrices. The rest follows from Theorem 4.15. □

Hence we have:

Proposition 7.2. *Combining the results of Section 4.12 and this section, we have Baumert-Hall arrays of order*

(i) $A = \{1+2^a 10^b 26^c,\ a,b,c$ *non-negative integers}* ,
(ii) $B = \{1,3,\ldots,33,37,41,47,51,53,59,61,65,81,101\}$,
(iii) $5b$ *and* $9b$ *where* $b \in A \cup B$ *.*

We note there is a Baumert-Hall array of order 47, and hence, as noted before, there is an Hadamard matrix of order 188.

7.6 Construction using complementary sequences

We now give some results which are useful in constructing new sequences from old. In particular, we want to use both periodic and aperiodic complementary sequences to construct orthogonal designs.

Remark 7.3. Since our interest is in orthogonal designs, we shall not be restricted to sequences with entries only ± 1, but shall allow 0's and variables too. One very simple remark is in order. If we have a collection of sequences X (each having length n) such that $N_X(j) = 0$, $j = 1,\ldots,n-1$, then we may

augment each sequence at the beginning with k zeros and at the end with ℓ zeros so that the resulting collection (say $\bar{X}$) of sequences having length $k+n+\ell$ still has $N_{\bar{X}}(j)=0$, $j=1,\ldots,k+n+\ell-1$.

Lemma 7.12. *Suppose there exist complementary sequences X_i, Y_i of length n_i, which give an $OD(u_{1i},u_{2i})$ constructed from two circulants, $i=1,2$.*

Then there exist 4-complementary sequences of length n which can be used in the Goethals-Seidel array to give $OD(4n;u_{11},u_{12},u_{21},u_{22})$ where $n \geq \max(n_1,n_2)$.

If in addition X_2, Y_2 are disjointable, then there exists an orthogonal design $OD(4n;u_{11},u_{21},\frac{1}{2}u_{12},\frac{1}{2}u_{22})$ where $n \geq \max(n_1,n_2)$.

Proof. Very straightforward. □

Corollary 7.11. *Let r be any number of the form $2^a10^b26^c5^d13^e$, and let n be any integer $\geq 2^a10^b26^c6^d14^e$, a,b,c,d,e non-negative integers. Then there exist orthogonal designs*

(i) $OD(4n;1,1,r,r)$,
(ii) $OD(4n;1,4,r,r)$,
(iii) $OD(2n;r,r)$.

Proof. Sequences of the weights r are by Corollary 7.3 and Theorem 7.6 disjointable, and the $(1,4)$ sequences are $\{ab\bar{a},a0a\}$. □

Another construction based on the existence of 2-complementary sequences which is extremely useful is:

Lemma 7.13. *Let $X=\{U,V\}$ be 2-complementary sequences of length n giving a design constructed of two circulants of type (a,b) such that $N_X(j)=0$. Then, with $U*$ and $V*$ their reverse sequences and w,x,y,z variables,*

(i) $Y=\{x,y,zU,zV\}$,
(ii) $Y=\{yx\bar{y},y0y,zU,zV\}$,
(iii) $Y=\{\{zU,0,zU*\},\{zU,x,-zU*\},\{zV,0,zV*\},\{zV,y,-zV*\}\}$

have $N_Y(j)=0$. Furthermore, they may be used in the Goethals-Seidel array to give orthogonal designs

(i) $OD(4m:(1,1,a,b),(1,4,a,b))$, $\quad m \geq n$, *and*
(ii) $OD(4m;1,1,4a,4b)$, $\quad m \geq 2n+1$.

Proof. Use $\{101,\ 11-\}$, $\{10111-,\ 101--1\}$, $\{aab\bar{b},\ a\bar{a}bb\}$, $\{ab,\bar{a}b\}$, $\{aaab\bar{a}aab\bar{a}a\bar{a}b0b,\ bbb\bar{a}\bar{b}bba\bar{b}b\bar{b}\bar{a}0\bar{a}\}$. □

We give one other method for constructing orthogonal designs using complementary sequences.

Lemma 7.14. *Let $X = \{A, B, Z, Z\}$ be 4-complementary sequences of length n and weight k. Then writing Z^* for the reverse of Z and with x, y, z variables,*

$$Y = \{\{yA, 0, yB\}, \{yA, 0, -yB\}, \{yZ, 0, yZ^*\}, \{yZ, x, -yZ*\}\}$$

are 4-complementary sequences of length $2n+1$ which may be used to give $OD(4m; 1, 2k)$, $m \geq 2n+1$.

Proof. Use the four sequences of Y to generate matrices which can be used in the Goethals-Seidel array. □

Summary 7.1. Two sequences $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ are called Golay complementary sequences of length n if all their entries are ± 1 and

$$\sum_{i=1}^{n-j} (x_i x_{i+j} + y_i y_{i+j}) = 0 \text{ for every } j \neq 0, \quad j = 1, \ldots, n-1,$$

$$\text{i.e., } N_X = 0.$$

These sequences have the following properties:

1. $\sum_{i=1}^{n-j} (x_i x_{i+j} + y_i y_{i+j}) = 0$ for every $j \neq 0, \quad j = 1, \ldots, n-1$, (where the subscripts are reduced modulo n), i.e., $P_X = 0$.
2. n is even and the sum of two squares.
3. $x_{n-i+1} = e_i x_i \Leftrightarrow y_{n-i+1} = -e_i y_i$ where $e_i = \pm 1$.
4. $\left[\sum_{i \in S} x_i Re\left(\zeta^{2i+1}\right)\right]^2 + \left[\sum_{i \in D} x_i Im\left(\zeta^{2i+1}\right)\right]^2 + \left[\sum_{i \in S} y_i Im\left(\zeta^{2i+1}\right)\right]^2 + \left[\sum_{i \in D} y_i Re\left(\zeta^{2i+1}\right)\right]^2 = \frac{1}{2}n$, where $S = \{i : 0 \leq i < n, e_i = 1\}, \quad D = \{i : 0 \leq i < n, e_i = -1\}$ and ζ is a $2n^{\text{th}}$ root of unity.
5. Exist for orders $2^a 10^b 26^c$, a, b, c non-negative integers.
6. Do not exist for orders $2.n$ (n a positive integer), when any factor of the prime decomposition of n is $\equiv 3 \pmod 4$ or $34, 50$ or 58.

Kharaghani, et al [35,36] has made fundamental advances in studying Golay type sequences in other contexts such as with complex entries or matrix entries. The following theorem is needed in one proof of the asymptotic existence results for Hadamard matrices:

Theorem 7.10 (Kharaghani). *For any positive integer n, there is a pair of Golay sequences of length 2^n in type 1 matrices each appearing 2^{n-1} times in each of the sequences.*

Proof. Let A_{n-1} and B_{n-1} be a pair of Golay sequences of length 2^{n-1} in type 1 matrices each appearing 2^{n-2} times in each of the sequences. Then $A_n = (A_{n-1}, B_{n-1})$ and $B_n = (A_{n-1}, -B_{n-1})$ form a Golay pair of length 2^n in type 1 matrices, as desired, where (A, B) means sequence A followed by sequences B. □

7.7 6-Turyn-type Sequences

Definition 7.6. 6-complementary sequences A, B, C, C, D and D of lengths m, m, m, m, n, and n with elements $0, \pm 1$ and $NPAF = 0$ will be called *6-Turyn-type sequences.*

Kharaghani and Tayfeh-Rezaie [122] in 2004 found six compatible ± 1 complementary sequences with zero NPAF of lengths $36, 36, 36, 36, 35, 35$ which can be used in the following theorem to construct Hadamard matrices of order $428 = 4 \times 107$ and $BH(428; 107, 107, 107, 107)$. We quote from Kharaghani and Tayfeh-Rezaie [123, p. 5]:

The following solution was implemented on a cluster of sixteen 2.6 GHz PC's for

$$214 = x^2 + y^2 + z^2 + 2w^2$$

with $x = 0$, $y = 6$, $z = 8$ and $w = 5$ and found the following solution after about 12 hours of computation.

$$A = (+++----++-+-+------++++-++-++++----+-),$$
$$B = (+-++++++--+-+--+--++--++++-++++----++-),$$
$$C = (+-++++++-+--++++-+++-++--++++-+--+---+),$$
$$D = (+++-+-----++--+-+++--+-+-+++-++++++-+).$$

Hence:

Theorem 7.11. *Suppose these exist 6-Turyn-type sequences of lengths m, m, m, m, m, m, n, n, that is 6 suitable compatible ± 1 complementary sequences with zero NPAF and lengths m, m, m, m, m, m, n, n called A, B, C, C, D, D. Then there exist $BH(4(2m+n); 2m+n, 2m+n, 2m+n, 2m+n)$ and an Hadamard matrix of order $4(2m+n)$.*

Proof. Let 0_t be the sequences of t zeros. Write $\{X, Y\}$, where X is the sequence $\{x_1, \ldots, x_p\}$ and Y is the sequence $\{y_1, \ldots, y_q\}$ for the sequence $\{x_1, x_2, \ldots, x_p, y_1, y_2, \ldots, y_q\}$ of length $p+q$. Then the required T-sequence for the constructions are

$$\{\tfrac{1}{2}(A+B), 0_{m+n}\}, \quad \{\tfrac{1}{2}(A-B), 0_{m+n}\}, \quad \{0_{2m}, D\}, \quad \{0_m, C, 0_n\}. \square$$

Corollary 7.12. *There are base sequences of lengths 71, 71, 36, 36 and therefore T-sequences of length 107.*

Corollary 7.13. *There is a Hadamard matrix of order 428 and Baumert-Hall array $BH(428; 107, 107, 107, 107)$.*

Chapter 8
Robinson's Theorem

In trying to decide which orthogonal designs to look for, it would be useful to formulate, and hopefully prove valid, some general principles of the sort, "All orthogonal designs of a certain type exist in certain orders." The Hadamard conjecture, the skew-Hadamard conjecture, the weighing matrix conjecture, and other conjectures that have been made, and extensively verified, provide some solid information which must be dealt with in order to state such principles. We have seen singularly unsuccessful in formulating correct principles of a general nature; some conjectures that we have made in the light of those principles have proved to be false.

One principle we had bandied about for awhile was: "In order n, if k is much smaller than $\rho(n)$, then all orthogonal designs on k variables exist in order n." Of course, the key to focusing on this principle is to decide what "much smaller" should mean.

In orders n where n is odd or $n = 2t$, t odd, algebraic conditions appear immediately in deciding if orthogonal designs exist, and so, in terms of deciding what "much smaller" should mean, we put those cases aside. When $n = 4t$, t odd, the situation is different. The algebraic theory says nothing about one-variable designs, i.e., weighing matrices. This fact, coupled with a fair bit of evidence for the weighing matrix conjecture in orders $4t$, t odd, led us to formulate a "sub-principle" for the phase "much smaller": to wit, we proposed the following: "If, in order n, the algebraic theory imposes *no* restrictions on any possible k-variable design in order n, than all k-variable designs exist in order n."

If this principle was a sound one, it would say, for example, that whenever $n = 16t$, $t \geq 1$, any orthogonal design on ≤ 7 variables exists. (See Proposition 3.34 and what follows it.) The principle, unfortunately (depending on your point of view), is far from correct. Peter J. Robinson decisively settled that issue and many other alternative ones with the following remarkable theorem.

Using the orthogonal designs $AOD(24;1,1,1,1,1,2,17)$ from Lemma A.7, $OD(32;1,1,1,1,1,12,15)$, $OD(32;1,1,1,1,1,9,9,9)$ and $OD(40;1,1,1,1,1,35)$

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5_8

found by Kharaghani and Tayfeh-Rezaie [122] given in Tables 8.1, 8.2 and 8.3 respectively we have using theorem 8.2

Theorem 8.1 (Robinson). *An $OD(n;1,1,1,1,1,n-5)$ exists if and only if $n = 8$, 16, 24, 32, 40.*

Theorem 8.2 (Robinson). *If $n > 40$, there is no orthogonal design of type $(1,1,1,1,1,n-5)$ in order n.*

We first note that:

$OD(8;1,1,1,1,1,3)$	See: Section 4.2
$OD(16;1,1,1,1,1,11)$	Appendix F.2
$OD(24;1,1,1,1,1,19)$	Table 8.1
$OD(32;1,1,1,1,1,27)$	Table 8.2
$OD(40;1,1,1,1,1,35)$	Table 8.3

do exist.

Proof. The proof is a very careful analysis of what such a design would have to look like, and we have expanded Robinson's proof so as to make the verification a bit easier for the reader. □

With no loss of generality we may assume the first 4×4 diagonal block of the orthogonal design is

$$\begin{bmatrix} x_1 & x_2 & x_3 & a_1 \\ -x_2 & x_1 & a_1 & -x_3 \\ -x_3 & -a_1 & x_1 & x_2 \\ -a_1 & x_3 & -x_2 & x_1 \end{bmatrix}$$

Either $a_1 = \pm x_4$, or not.

If $a_1 = \pm x_4$, we proceed to obtain the following 8×8 diagonal block:

$$\begin{bmatrix} x_1 & x_2 & x_3 & a_1 & x_5 & & & \\ -x_2 & x_1 & a_1 & -x_3 & & -x_5 & & * \\ -x_3 & -a_1 & x_1 & x_2 & & & -x_5 & \\ -a_1 & x_3 & -x_2 & x_1 & & * & & x_5 \\ -x_5 & & & & x_1 & x_2 & x_3 & b_1 \\ & x_5 & * & & -x_2 & x_1 & b_1 & -x_3 \\ * & & x_5 & & -x_3 & -b_1 & x_1 & x_2 \\ & & & -x_5 & -b_1 & x_3 & -x_2 & x_1 \end{bmatrix}, \tag{8.1}$$

and $b_1 = -a_1$.

In case $a_1 \neq \pm x_4$, we may proceed to make the following 8×8 diagonal block.

$$\begin{bmatrix} x_1 & x_2 & x_3 & a_1 & x_4 & & & \\ -x_2 & x_1 & a_1 & & & -x_4 & * & \\ -x_3 & -a_1 & x_1 & x_2 & * & & -x_4 & \\ -a_1 & x_3 & -x_2 & x_1 & & & & x_4 \\ -x_4 & & & & x_1 & x_2 & x_3 & b_1 \\ & x_4 & * & & -x_2 & x_1 & b_1 & -x_3 \\ & * & x_4 & & -x_3 & -b_1 & x_1 & x_2 \\ & & & -x_4 & -b_1 & x_3 & -x_2 & x_1 \end{bmatrix}, \tag{8.2}$$

and $b_1 = -a_1$.

We continue the process and end up with 8×8 blocks of type (8.1) or (8.2) on the diagonal.

Claim. There is at most one diagonal block of type (8.1).

Proof of Claim. Let X denote the orthogonal design of type $(1,1,1,1,1,n-5)$ in order n, and write $X = A_1x_1 + A_2x_2 + A_3x_3 + \cdots + A_6x_6$. As we have already seen, we may assume

$$A_1 = I_n, A_2 = \underset{n/2}{\oplus} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

and

$$A_3 = \underset{\frac{n}{4}}{\oplus} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Since X is an orthogonal design, we must have $A_iA_j^\top + A_jA_i^\top = 0$, $1 \le i \ne j \le 6$. The patient reader will then discover than these conditions force A_4, A_5, A_6 to each be skew-symmetric and partitioned into 4×4 blocks, where if $(p\,q\,r\,s)$ is the first row of a block, then the block looks like:

$$\begin{bmatrix} p & q & r & s \\ q & -p & s & -r \\ r & -s & -p & q \\ -s & -r & q & p \end{bmatrix}.$$

Now, assume that there are two 8×8 diagonal blocks like (8.1), with $a_1 = \pm x_4, b_1 = -a_1, a_2 = \pm x_4, b_2 = -a_2$; we shall obtain a contradiction (we shall first consider the case $a_1 = a_2 = x_4$ and leave the remaining three possibilities for the reader to check). The contradiction shall be obtained by looking at the 8×8 off-diagonal blocks which are at the juncture of the two diagonal positions. See Figure 8.1.

If we number the rows of figure 8.1 from 1 to 16, then we obtain (by taking the inner product of rows 1 and 9) a summand $2sx_4$ which we cannot eliminate since x_4 appears only once in each column and row.

(Note: We have used here the fact that $s \ne 0$, but we would get the same result if *any* of p, q, r, or s were $\ne 0$ or if any of k, l, m, v were $\ne 0$. Thus, so far,

Fig. 8.1 Contradiction of off-diagonal blocks at juncture of two diagonal positions

$$
\begin{bmatrix}
x_1 & x_2 & x_3 & x_4 & & & & \\
-x_2 & x_1 & x_4 & -x_3 & & & & \\
-x_3 & -x_4 & x_1 & x_2 & & * & & \\
-x_4 & x_3 & -x_2 & x_1 & & & & \\
 & & & & x_1 & x_2 & x_3 & -x_4 \\
 & & & & -x_2 & x_1 & -x_4 & -x_3 \\
 & & * & & -x_3 & x_4 & x_1 & x_2 \\
 & & & & x_4 & x_3 & -x_3 & x_1
\end{bmatrix}
\leftrightsquigarrow
\begin{bmatrix}
p & q & r & s & b & c & d & e \\
q & -p & s & -r & c & -b & e & d \\
r & -s & -p & q & d & -e & -b & c \\
-s & -r & q & p & -e & -d & c & b \\
f & g & h & j & k & \ell & m & v \\
g & -f & j & -h & \ell & -k & v & -m \\
h & -j & -f & g & m & -v & -k & \ell \\
-j & -h & g & f & -v & -m & \ell & k
\end{bmatrix}
$$

$$
\updownarrow
$$

$$
\begin{bmatrix}
-p & -q & -r & s & -f & -g & -h & j \\
-q & p & s & r & -g & f & j & h \\
-r & -s & p & -q & -h & -j & f & -g \\
-s & r & -q & p & -j & h & -g & -f \\
-b & -c & -d & e & -k & -\ell & -m & v \\
-c & b & e & d & -\ell & k & v & m \\
-d & -e & b & -c & -m & -v & k & -\ell \\
-e & d & -c & -b & -v & m & -\ell & -k
\end{bmatrix}
\leftrightsquigarrow
\begin{bmatrix}
x_1 & x_2 & x_3 & x_4 & & & & \\
-x_2 & x_1 & x_4 & -x_3 & & & & \\
-x_3 & -x_4 & x_1 & x_2 & & & * & \\
-x_4 & x_3 & -x_2 & x_1 & & & & \\
 & & & & x_1 & x_2 & x_3 & -x_4 \\
 & & & & -x_2 & x_1 & -x_4 & -x_3 \\
 & & * & & -x_3 & x_4 & x_1 & x_2 \\
 & & & & x_4 & x_3 & -x_3 & x_1
\end{bmatrix}
$$

we could be discussing orthogonal designs of type $(1,1,1,1,1,n-k)$, $5 \le k \le 8$, and the conclusions that are drawn would still hold; i.e., no two diagonal blocks of type (8.1).)

We have now seen that there can only be one diagonal block of type (8.1) and that all other diagonal blocks are of type (8.2).

We now seek to discover where in the orthogonal design the x_5's are located. If there is a diagonal block of type (8.1), then we know where the x_5's in the rows and columns controlled by that diagonal block are, namely, in the diagonal block.

Claim. The x_5's are always in the diagonal blocks.

Proof. To prove this, it would be enough to show that there is no x_5 in an off-diagonal block which is above **and** across from a diagonal block of type Equation (8.2). Thus, we have the following in Figure 8.2.

Now, by checking inner products (just using x_4's), we find that

$$
\begin{aligned}
bx_4 - fx_4 = 0\,, &\quad \text{i.e., } b = f;\\
-cx_4 - gx_4 = 0\,, &\quad \text{i.e., } c = -g;\\
-dx_4 - hx_4 = 0\,, &\quad \text{i.e., } d = -h;\\
ex_4 - jx_4 = 0\,, &\quad \text{i.e., } e = j.
\end{aligned}
$$

Similarly,

Fig. 8.2 No x_5 in off-diagonal block above and across from a diagonal block of type Equation (8.2)

$$\begin{bmatrix} x_1 & x_2 & x_3 & \alpha & x_4 & & & \\ -x_2 & x_1 & \alpha & -x_3 & & -x_4 & & \\ -x_3 & -\alpha & x_1 & x_2 & & & -x_4 & \\ -\alpha & x_3 & -x_2 & x_1 & & & & x_4 \\ -x_4 & & & & x_1 & x_2 & x_3 & -\alpha \\ & x_4 & & & -x_2 & x_1 & -\alpha & -x_3 \\ & & x_4 & & -x_3 & \alpha & x_1 & x_2 \\ & & & x_4 & \alpha & x_3 & -x_2 & x_1 \end{bmatrix} \leftrightsquigarrow \begin{bmatrix} p & q & r & s & b & c & d & e \\ q & -p & s & -r & c & -b & e & -d \\ r & -s & -p & q & d & -e & -b & c \\ -s & -r & q & p & -e & -d & c & b \\ f & g & h & j & k & \ell & m & v \\ g & -f & j & -h & \ell & -k & v & -m \\ h & -j & -f & g & m & -v & -k & \ell \\ -j & -h & g & f & -v & -m & \ell & k \end{bmatrix} = Y$$

$$\updownarrow \qquad\qquad \updownarrow \qquad\qquad \updownarrow$$

$$-Y^{\top} = \begin{bmatrix} -p & -q & -r & s & -f & -g & -h & j \\ -q & p & s & r & -g & f & j & h \\ -r & -s & p & -q & -h & -j & f & -g \\ -s & r & -q & p & -j & h & -g & -f \\ -b & -c & -d & e & -k & -\ell & -m & v \\ -c & b & e & d & -\ell & k & v & m \\ -d & -e & b & -c & -m & -v & k & -\ell \\ -e & d & -c & -b & -v & m & -\ell & -k \end{bmatrix} \leftrightsquigarrow \begin{bmatrix} x_1 & x_2 & x_3 & \beta & x_4 & & & \\ -x_2 & x_1 & \beta & -x_3 & & x_4 & & \\ -x_3 & -\beta & x_1 & x_2 & & & x_4 & \\ -\beta & x_3 & -x_2 & x_1 & & & & x_4 \\ -x_4 & & & & x_1 & x_2 & x_3 & -\beta \\ & x_4 & & & -x_2 & x_1 & \beta & -x_3 \\ & & x_4 & & -x_3 & \beta & x_1 & x_2 \\ & & & -x_4 & \beta & x_3 & -x_2 & x_1 \end{bmatrix}$$

$$\begin{aligned} k &= -p, \\ \ell &= q, \\ m &= r, \\ v &= -s; \end{aligned}$$

i.e., we have

$$Y = \left[\begin{array}{cccc|cccc} p & q & r & s & b & c & d & e \\ \multicolumn{4}{c|}{\text{etc.}} & \multicolumn{4}{c}{\text{etc.}} \\ \hline \multicolumn{4}{c|}{\text{etc.}} & \multicolumn{4}{c}{\text{etc.}} \\ -e & d & -c & b & s & -r & q & -p \end{array}\right]$$

If we consider the inner product between the two rows and recall that none of p, q, r, s, b, c, d, or $e = 0$, we find that $\pm x_5 \notin \{p, q, r, s, b, c, d, e\}$.

Now, the i^{th} diagonal block of type (8.2) has four (as yet) undetermined entries, and we have seen that one of them must be $\pm x_5$. If there are four (or more) blocks of type (8.2), then in two of them x_5 (up to sign) must occupy the same position. We shall assume that occurs in the i^{th} and j^{th} diagonal blocks and write them (along with the $(i,j)^{\text{th}}$ and $(j,i)^{\text{th}}$ off-diagonal blocks) in Figure 8.3.

Now, suppose β_1 and β_2 are each $\pm x_5$. Considering rows 1 and 9 of Figure 8.3 we find $\beta_1 c + \beta_2 c = 0$, i.e., $\beta_1 = -\beta_2$, but considering rows 1 and 11 we find $-\beta_1 e + \beta_2 e = 0$, i.e., $\beta_1 = \beta_2$. This contradiction establishes that β_1, β_2 cannot

Fig. 8.3 Four (or more) blocks of type (8.2), x_5 must occupy the same position in two of them

$$\begin{bmatrix} x_1 & x_2 & x_3 & \alpha_1 & x_4 & \beta_1 & \gamma_1 & \delta_1 \\ -x_2 & x_1 & \alpha_1 & -x_3 & \beta_1 & -x_4 & \delta_1 & -\gamma_1 \\ -x_3 & -\alpha_1 & x_1 & x_2 & \gamma_1 & -\delta_1 & -x_4 & \beta_1 \\ -\alpha_1 & x_3 & -x_2 & x_1 & -\delta_1 & -\gamma_1 & \beta_1 & x_4 \\ -x_4 & -\beta_1 & -\gamma_1 & \delta_1 & x_1 & x_2 & x_3 & -\alpha_1 \\ -\beta_1 & x_4 & \delta_1 & \gamma_1 & -x_2 & x_1 & -\alpha_1 & -x_3 \\ -\gamma_1 & -\delta_1 & x_4 & -\beta_1 & -x_3 & \alpha_1 & x_1 & x_2 \\ -\delta_1 & \gamma_1 & -\beta_1 & -x_4 & \alpha_1 & x_3 & -x_2 & x_1 \end{bmatrix} \leftrightsquigarrow \begin{bmatrix} p & q & r & s & b & c & d & e \\ q & -p & s & -r & c & -b & e & -d \\ r & -s & -p & q & d & -e & -b & c \\ -s & -r & q & p & -e & -d & c & b \\ b & -c & -d & e & -p & q & r & -s \\ -c & -b & e & d & q & p & -s & -r \\ -d & -e & -b & -c & r & s & p & q \\ -e & d & -c & b & s & -r & q & -p \end{bmatrix}$$

$$\updownarrow \qquad\qquad \updownarrow \qquad\qquad \updownarrow$$

$$\begin{bmatrix} -p & -q & -r & s & -b & c & d & e \\ -q & p & s & r & c & b & e & -d \\ -r & -s & p & -q & d & -e & b & c \\ -s & r & -q & p & -e & -d & c & -b \\ -b & -c & -d & e & p & -q & -r & -s \\ -c & b & e & d & -q & -p & -s & r \\ -d & -e & b & -c & -r & s & -p & -q \\ -e & d & -c & -b & s & r & -q & p \end{bmatrix} \leftrightsquigarrow \begin{bmatrix} x_1 & x_2 & x_3 & \alpha_2 & x_4 & \beta_2 & \gamma_2 & \delta_2 \\ -x_2 & x_1 & \alpha_2 & -x_3 & \beta_2 & -x_4 & \delta_2 & -\gamma_2 \\ -x_3 & -\alpha_2 & x_1 & x_2 & \gamma_2 & -\delta_2 & -x_4 & \beta_2 \\ -\alpha_2 & x_3 & -x_2 & x_1 & -\delta_2 & -\gamma_2 & \beta_2 & x_4 \\ -x_4 & -\beta_2 & -\gamma_2 & \delta_2 & x_1 & x_2 & x_3 & -\alpha_2 \\ -\beta_2 & x_4 & \delta_2 & \gamma_2 & -x_2 & x_1 & -\alpha_2 & -x_3 \\ -\gamma_2 & -\delta_2 & x_4 & -\beta_2 & -x_3 & \alpha_2 & x_1 & x_2 \\ -\delta_2 & \gamma_2 & -\beta_2 & -x_4 & \alpha_2 & x_3 & -x_2 & x_1 \end{bmatrix}$$

both have absolute value x_5. A similar argument gives the same conclusion for Y_1 and Y_2, Δ_1 and Δ_2, and α_1 and α_2. This then completes the proof. □

It is possible to use Robinson's Theorem to obtain many other non-existence results. We give just two illustrations.

Corollary 8.1. *There do not exist amicable orthogonal designs of type* $AOD((1,1,m-2);(1,m-1))$ *in any order* $m > 10$.

Proof. If there did, we could use Theorem 6.1 (i.e., a product design of type $PD(4:1,1,1,;1,1,1;1))$ to obtain an orthogonal design in order $4m > 40$ of type $(1,1,m-2,1,1,1,m-1,m-1,m-1)$, contradicting Theorem 8.2. □

Note. This shows how difficult it is to obtain "full" amicable orthogonal designs which have several 1's in their types.

Corollary 8.2. *There is no product design of type* $PD(n;1,1,n-3;1,n-2;1)$ *in any order* $n > 20$.

Proof. If there were, Construction 6.1 would contradict Robinson's Theorem. □

Remark 8.1. This corollary shows how special the product designs constructed in Examples 6.2, 6.3 and Theorem 6.1 really are.

Table 8.1 An $OD(32;1,1,1,1,1,12,15)$ [a]

$$\left[\begin{array}{cccc}
abcsdts\bar{e} & \bar{s}st\bar{t}\bar{s}stt & ssss\bar{t}\bar{t}\bar{t}t & t\bar{s}\bar{t}\bar{t}\bar{t}st\bar{t} \\
\bar{b}a\bar{s}ct\bar{d}es & sst\bar{t}ss\bar{t}t & s\bar{s}\bar{s}st\bar{t}\bar{t}\bar{t} & \bar{s}t\bar{t}\bar{t}sttt \\
\bar{c}sa\bar{b}s\bar{e}\bar{d}\bar{t} & \bar{t}\bar{t}s\bar{s}\bar{t}ts\bar{s} & ss\bar{s}\bar{s}\bar{t}\bar{t}t\bar{t} & \bar{t}\bar{t}\bar{t}st\bar{t}\bar{t}s\bar{s} \\
\bar{s}\bar{c}baes\bar{t}d & t\bar{t}\bar{s}\bar{s}\bar{t}t\bar{s}\bar{s} & \bar{s}s\bar{s}s\bar{t}\bar{t}\bar{t}\bar{t} & t\bar{t}s\bar{t}\bar{t}t\bar{s}\bar{t} \\
\bar{d}\bar{t}\bar{s}\bar{e}abc\bar{s} & \bar{s}\bar{s}\bar{t}tss\bar{t}t & \bar{t}\bar{t}\bar{t}t\bar{s}sss\bar{s} & t\bar{t}s\bar{t}\bar{t}\bar{t}st \\
\bar{t}de\bar{s}\bar{b}asc & \bar{s}s\bar{t}\bar{t}s\bar{s}\bar{t}\bar{t} & \bar{t}\bar{t}\bar{t}ssss & \bar{t}\bar{t}\bar{t}s\bar{t}\bar{t}\bar{t}s \\
\bar{s}\bar{e}dt\bar{c}\bar{s}a\bar{b} & \bar{t}tss\bar{t}t\bar{s}\bar{s} & ttttss\bar{s}s\bar{s} & s\bar{t}\bar{t}\bar{t}sttt \\
e\bar{s}t\bar{d}s\bar{c}ba & \bar{t}\bar{t}s\bar{s}\bar{t}\bar{t}\bar{s}s & \bar{t}\bar{t}\bar{t}t\bar{s}ss\bar{s}\bar{s} & tstt\bar{t}st\bar{t} \\
\\
s\bar{s}t\bar{t}sstt & abc\bar{s}d\bar{s}e\bar{t} & \bar{t}\bar{t}\bar{t}\bar{t}\bar{s}s\bar{t} & \bar{t}\bar{s}\bar{t}\bar{s}stst \\
\bar{s}\bar{s}ttss\bar{t}\bar{t}t & \bar{b}asc\bar{s}\bar{d}te & \bar{t}ttt\bar{s}tts & \bar{s}ts\bar{t}t\bar{s}\bar{t}s \\
tt\bar{s}stt\bar{s}\bar{s} & \bar{c}\bar{s}a\bar{b}e\bar{t}\bar{d}s & t\bar{t}\bar{t}ts\bar{t}ts & \bar{t}\bar{s}tsst\bar{s}\bar{t} \\
ttss\bar{t}t\bar{s}s & s\bar{c}batesd & ttt\bar{t}tss\bar{t} & s\bar{t}s\bar{t}\bar{t}s\bar{t}s \\
s\bar{s}\bar{t}t\bar{s}\bar{s}tt & \bar{d}s\bar{e}\bar{t}abcs & \bar{t}s\bar{s}\bar{t}\bar{t}ttt & s\bar{t}s\bar{t}t\bar{s}t\bar{s} \\
\bar{s}\bar{s}\bar{t}\bar{t}\bar{s}s\bar{t}t & sdt\bar{e}\bar{b}a\bar{s}c & sttt\bar{s}\bar{t}\bar{t}\bar{t}t & \bar{t}\bar{s}ts\bar{s}\bar{t}st \\
\bar{t}t\bar{s}sttss & \bar{e}\bar{t}d\bar{s}\bar{c}sa\bar{b} & \bar{s}\bar{t}t\bar{s}\bar{t}\bar{t}\bar{t}t & s\bar{t}\bar{s}tt\bar{s}\bar{t}s \\
\bar{t}\bar{t}ss\bar{t}ts\bar{s} & t\bar{e}\bar{s}\bar{d}\bar{s}\bar{c}ba & t\bar{s}\bar{s}\bar{t}\bar{t}ttt & tstsstst \\
\\
\bar{s}\bar{s}\bar{s}st\bar{t}\bar{t}t & tt\bar{t}\bar{t}t\bar{s}s\bar{t} & abcsdes\bar{t} & ts\bar{s}t\bar{s}\bar{t}t\bar{s} \\
\bar{s}ss\bar{s}\bar{s}t\bar{t}\bar{t}\bar{t} & t\bar{t}\bar{t}t\bar{s}\bar{t}ts & \bar{b}a\bar{s}ced\bar{t}s & s\bar{t}\bar{t}\bar{s}\bar{t}sst \\
\bar{s}ssst\bar{t}\bar{t}\bar{t} & \bar{t}\bar{t}\bar{t}ts\bar{t}ts & \bar{c}sa\bar{b}s\bar{t}\bar{d}\bar{e} & \bar{s}t\bar{t}\bar{s}t\bar{s}st \\
\bar{s}\bar{s}s\bar{s}\bar{t}\bar{t}\bar{t}\bar{t} & t\bar{t}\bar{t}\bar{t}tsst & \bar{s}\bar{c}batse\bar{d} & \bar{t}\bar{s}\bar{s}tstt\bar{s} \\
t\bar{t}\bar{t}ts\bar{s}\bar{s}\bar{s} & ts\bar{s}\bar{t}\bar{t}\bar{t}\bar{t}t & \bar{d}\bar{e}\bar{s}\bar{t}abc\bar{s} & \bar{t}\bar{s}\bar{s}t\bar{s}\bar{t}ts \\
\bar{t}\bar{t}\bar{t}t\bar{s}\bar{s}s\bar{s} & s\bar{t}t\bar{s}ttt\bar{t} & \bar{e}dts\bar{b}asc & \bar{s}tt\bar{s}\bar{t}s\bar{s}\bar{t} \\
tt\bar{t}ts\bar{s}\bar{s}\bar{s} & \bar{s}\bar{t}\bar{t}\bar{s}\bar{t}ttt & \bar{s}\bar{t}de\bar{c}\bar{s}a\bar{b} & \bar{s}ttst\bar{s}st \\
\bar{t}ttts\bar{s}ss & t\bar{s}\bar{s}t\bar{t}\bar{t}\bar{t}\bar{t} & t\bar{s}e\bar{d}s\bar{c}ba & \bar{t}\bar{s}st\bar{s}\bar{t}t\bar{s} \\
\\
tst\bar{t}\bar{t}t\bar{s}\bar{t} & tst\bar{s}\bar{s}t\bar{s}\bar{t} & \bar{t}\bar{s}sttsst & abc\bar{d}e\bar{s}t\bar{s} \\
s\bar{t}ttttt\bar{s} & s\bar{t}sttst\bar{s} & \bar{s}t\bar{t}ss\bar{t}\bar{t}s & \bar{b}adc\bar{s}\bar{e}st \\
t\bar{t}t\bar{s}\bar{s}\bar{t}t\bar{t} & ts\bar{t}\bar{s}\bar{s}\bar{t}st\bar{t} & sttsst\bar{t}\bar{s} & \bar{c}\bar{d}a\bar{b}t\bar{s}\bar{e}s \\
tt\bar{s}tt\bar{s}\bar{t}\bar{t} & st\bar{s}tt\bar{s}\bar{t}\bar{s} & \bar{t}ss\bar{t}\bar{t}s\bar{s}t & d\bar{c}bastse \\
t\bar{s}\bar{t}ttt\bar{s}t & \bar{s}t\bar{s}\bar{t}ts\bar{t}\bar{s} & st\bar{t}\bar{s}stts & \bar{e}st\bar{s}abcd \\
\bar{s}\bar{t}\bar{t}t\bar{t}\bar{t}t\bar{s} & \bar{t}st\bar{s}stst\bar{t} & t\bar{s}s\bar{t}\bar{t}s\bar{s}t & ses\bar{t}\bar{b}ad\bar{c} \\
\bar{t}\bar{t}\bar{t}s\bar{s}\bar{t}\bar{t}\bar{t} & \bar{s}st\bar{t}\bar{s}t\bar{s} & \bar{t}\bar{s}\bar{s}\bar{t}ts\bar{s}\bar{t} & \bar{t}\bar{s}e\bar{s}\bar{c}da\bar{b} \\
t\bar{t}st\bar{t}\bar{s}\bar{t}t & \bar{t}\bar{s}t\bar{s}s\bar{t}\bar{s}\bar{t} & st\bar{t}ss\bar{s}t\bar{t}s & s\bar{t}\bar{s}\bar{e}\bar{d}\bar{c}ba
\end{array}\right]$$

[a] Kharaghani and Tayfeh-Rezaie [122, p317-324]

Table 8.2 An $OD(32;1,1,1,1,1,9,9,9)$ [a]

$$\left[\begin{array}{cccc}
abcsdut\bar{e} & \bar{s}s\bar{s}\bar{s}\bar{t}ttt & utut\bar{t}u\bar{t}u & \bar{s}\bar{u}\bar{u}\bar{s}\bar{s}uu\bar{s} \\
\bar{b}a\bar{s}cu\bar{d}et & sss\bar{s}tt\bar{t}t & t\bar{u}\bar{t}uut\bar{u}\bar{t} & \bar{u}ss\bar{u}ussu \\
\bar{c}sa\bar{b}t\bar{e}\bar{d}\bar{u} & \bar{s}\bar{s}s\bar{s}ttt\bar{t} & ut\bar{u}\overline{tt}ut\bar{u} & \bar{u}\bar{s}suu\bar{s}s\bar{u} \\
\bar{s}\bar{c}baetu\bar{d} & s\bar{s}\bar{s}\bar{s}t\overline{tt}\bar{t} & \bar{t}ut\bar{u}u\bar{t}\bar{u}\bar{t} & s\bar{u}u\bar{s}suu\bar{s} \\
\bar{d}\bar{u}t\bar{e}abc\bar{s} & \overline{ttt}ss\bar{s}s & \bar{t}\bar{u}tuu\bar{u}tu\bar{t} & s\bar{u}us\bar{s}\bar{u}us \\
\bar{u}de\bar{t}\bar{b}asc & \bar{t}t\bar{t}ts\bar{s}\bar{s}\bar{s} & \bar{u}t\bar{u}ttutu & \bar{u}\bar{s}suu\bar{s}su \\
\bar{t}\bar{e}du\bar{c}\bar{s}a\bar{b} & \bar{t}ttt\bar{s}ss\bar{s} & tutuu\bar{t}u\bar{t} & u\bar{s}\bar{s}uussu \\
e\bar{t}u\bar{d}s\bar{c}ba & \overline{ttt}\bar{s}\bar{s}\bar{s}s & \bar{u}tu\bar{t}tut\bar{u} & suus\bar{s}uu\bar{s} \\
\\
s\bar{s}s\bar{s}tttt & abc\bar{s}d\bar{t}e\bar{u} & \bar{u}\bar{s}s\bar{u}\bar{s}\bar{u}u\bar{s} & \bar{u}\bar{u}\overline{tt}uutt \\
\bar{s}\bar{s}sstt\overline{tt} & \bar{b}asc\bar{t}\bar{d}ue & \bar{s}uusu\bar{s}ssu & \bar{u}ut\bar{t}u\bar{u}\bar{t}t \\
s\bar{s}\bar{s}stt\overline{tt} & \bar{c}s\bar{a}be\bar{u}\bar{d}t & s\bar{u}usu\bar{s}su & \overline{tt}uutt\bar{u}\bar{u} \\
ssss\bar{t}t\bar{t}t & s\bar{c}bauetd & ussu\bar{s}uu\bar{s} & tt\bar{u}u\bar{t}t\bar{u}u \\
tt\overline{tt}\bar{s}\bar{s}ss & \bar{d}t\bar{e}\bar{u}abcs & \bar{s}u\bar{u}\bar{s}u\bar{s}su & tt\bar{u}u\bar{t}t\bar{u}\bar{u} \\
\overline{tttt}\bar{s}s\bar{s}s & tdu\bar{e}\bar{b}a\bar{s}c & ussu\bar{s}\bar{u}\bar{u}s & \overline{tt}uutt\bar{u}u \\
\bar{t}tt\bar{t}ssss & \bar{e}\bar{u}d\bar{t}\bar{c}sa\bar{b} & \bar{u}\bar{s}s\bar{u}su\bar{u}s & u\bar{u}\bar{t}tu\bar{u}\bar{t}t \\
\overline{tttt}\bar{s}ss\bar{s} & u\bar{e}\bar{t}d\bar{s}\bar{c}ba & s\bar{u}\bar{u}\bar{s}\bar{u}ssu & uuttuutt \\
\\
\bar{u}t\bar{u}\bar{u}ttut\bar{u} & uss\bar{u}\bar{u}s\bar{u}u\bar{s} & abctdes\bar{u} & st\bar{t}s\bar{t}\bar{s}s\bar{t} \\
\bar{t}ut\bar{u}\bar{u}ut\bar{u}\bar{t} & s\bar{u}u\bar{s}\bar{u}\bar{s}su & \bar{b}at\bar{c}ed\bar{u}s & t\bar{s}\bar{s}\bar{t}\bar{s}tts \\
\bar{u}tut\bar{t}ut\bar{u} & \bar{s}\bar{u}\bar{u}\bar{s}u\bar{s}\bar{s}u & \bar{c}tab\bar{s}\bar{u}d\bar{e} & \bar{t}s\bar{s}\bar{t}st\bar{t}s \\
\bar{t}\bar{u}t\bar{u}\bar{u}t\bar{u}t & u\bar{s}\bar{s}usuus & \bar{t}\bar{c}bau\bar{s}\bar{e}d & \bar{s}t\overline{tt}stsst\bar{t} \\
tu\bar{u}uut\bar{u}\bar{t} & su\bar{u}\bar{s}\bar{u}s\bar{s}u & \bar{d}\bar{e}\bar{s}\bar{u}abc\bar{t} & \bar{s}t\overline{tt}s\bar{t}\bar{s}\bar{s}t \\
\bar{u}t\bar{u}t\bar{t}\bar{u}tu & u\bar{s}\bar{s}u\bar{s}u\bar{u}\bar{s} & \bar{e}du\bar{s}\bar{b}atc & \bar{t}s\bar{s}\bar{t}\bar{s}tt\bar{s} \\
tut\bar{u}u\bar{t}\bar{u}t & \bar{u}\bar{s}\bar{s}\bar{u}\bar{s}uu\bar{s} & \bar{s}\bar{u}de\bar{c}\bar{t}a\bar{b} & \bar{t}sst\bar{s}tts \\
\bar{u}tutt\bar{u}tu & su\bar{u}\bar{s}u\bar{s}\bar{s}\bar{u} & u\bar{s}e\bar{d}t\bar{c}ba & \bar{s}\bar{t}t\bar{s}\bar{t}\bar{s}s\bar{t} \\
\\
suu\bar{s}\bar{s}u\bar{u}\bar{s} & uutt\overline{tt}\bar{u}\bar{u} & \bar{s}\bar{t}tsstts & abc\bar{d}e\bar{u}t\bar{s} \\
u\bar{s}suussu\bar{u} & u\bar{u}tttt\bar{u}\bar{u} & \bar{t}s\bar{s}tt\bar{s}\bar{s}t & \bar{b}adc\bar{u}\bar{e}st \\
u\bar{s}\bar{s}\bar{u}\bar{u}\bar{s}s\bar{u} & tt\bar{t}\bar{u}\bar{u}\bar{u}\bar{u}t\bar{t} & tsstts\bar{s}\bar{t} & \bar{c}\bar{d}a\bar{b}t\bar{s}\bar{e}u \\
su\bar{u}ss\bar{u}\bar{u}\bar{s} & tt\bar{u}uu\bar{u}\overline{tt} & \bar{s}tt\bar{s}\bar{s}tts & d\bar{c}bastue \\
s\bar{u}\bar{u}\bar{s}su\bar{u}s & \bar{u}\bar{u}t\overline{tt}t\bar{u}\bar{u} & ts\bar{s}\bar{t}tsst & \bar{e}ut\bar{s}abcd \\
\bar{u}\bar{s}s\bar{u}u\bar{s}\bar{s}\bar{u} & \bar{u}ut\overline{tt}ttu\bar{u} & st\bar{t}s\bar{s}t\bar{t}s & uest\bar{b}a\bar{d}c \\
\bar{u}\bar{s}\bar{s}u\bar{u}s\bar{s}\bar{u} & \bar{t}tuu\bar{u}\bar{u}t\bar{t} & \bar{s}t\overline{tt}\bar{s}st\bar{t}\bar{s} & \bar{t}\bar{s}e\bar{u}\bar{c}da\bar{b} \\
s\bar{u}us\bar{s}\bar{u}\bar{u}s & \overline{tt}tu\bar{u}u\bar{u}\overline{tt} & t\bar{s}\bar{s}t\bar{t}ss\bar{t} & st\bar{u}\bar{e}\bar{d}\bar{c}ba
\end{array}\right]$$

[a] Kharaghani and Tayfeh-Rezaie [122, p317-324] ©Elsevier

Table 8.3 An $OD(40;1,1,1,1,1,35)$ [a]

$$\begin{bmatrix}
abcsdss\bar{e} & \bar{s}ssss\bar{s}\bar{s}\bar{s} & s\bar{s}s\bar{s}ssss & \bar{s}ss\bar{s}\bar{s}\bar{s}\bar{s} & \bar{s}\bar{s}\bar{s}\bar{s}\bar{s}\bar{s}\bar{s} \\
\bar{b}a\bar{s}cs\bar{d}es & ss\bar{s}ssss\bar{s} & \bar{s}\bar{s}ssss\bar{s}\bar{s} & ssss\bar{s}ss\bar{s} & \bar{s}ss\bar{s}\bar{s}\bar{s}\bar{s} \\
\bar{c}sa\bar{b}s\bar{e}\bar{d}\bar{s} & sss\bar{s}\bar{s}\bar{s}s\bar{s} & s\bar{s}\bar{s}ssss\bar{s} & s\bar{s}s\bar{s}\bar{s}ss & \bar{s}\bar{s}ss\bar{s}\bar{s}s \\
\bar{s}\bar{c}baes\bar{s}d & \bar{s}s\bar{s}\bar{s}s\bar{s}\bar{s} & ssss\bar{s}s\bar{s}s & ss\bar{s}\bar{s}s\bar{s}\bar{s} & s\bar{s}s\bar{s}\bar{s}ss \\
\bar{d}\bar{s}\bar{s}\bar{e}abc\bar{s} & \bar{s}\bar{s}s\bar{s}ssss\bar{s} & s\bar{s}ss\bar{s}\bar{s}ss & ss\bar{s}\bar{s}s\bar{s}s & ssssss\bar{s}\bar{s}s \\
\bar{s}de\bar{s}\bar{b}asc & \bar{s}ssssss\bar{s}s & \bar{s}\bar{s}\bar{s}\bar{s}s\bar{s}\bar{s} & s\bar{s}s\bar{s}ss\bar{s}\bar{s} & s\bar{s}s\bar{s}\bar{s}\bar{s}\bar{s} \\
\bar{s}\bar{e}dsc\bar{s}a\bar{b} & s\bar{s}ssss\bar{s}\bar{s}\bar{s} & \bar{s}ss\bar{s}ssss & \bar{s}\bar{s}\bar{s}\bar{s}ss\bar{s} & ss\bar{s}\bar{s}\bar{s}s\bar{s} \\
es\bar{s}d\bar{s}\bar{c}ba & sss\bar{s}ss\bar{s}s & \bar{s}\bar{s}ss\bar{s}ss\bar{s} & s\bar{s}\bar{s}\bar{s}\bar{s}\bar{s}\bar{s} & \bar{s}s\bar{s}\bar{s}\bar{s}ss \\
s\bar{s}\bar{s}ssss\bar{s}\bar{s} & abc\bar{s}d\bar{s}e\bar{s} & \bar{s}\bar{s}s\bar{s}\bar{s}\bar{s}s\bar{s} & \bar{s}\bar{s}\bar{s}\bar{s}ssss & \bar{s}\bar{s}\bar{s}\bar{s}\bar{s}\bar{s}\bar{s} \\
\bar{s}\bar{s}\bar{s}s\bar{s}s\bar{s}s & \bar{b}asc\bar{s}\bar{d}se & \bar{s}ssss\bar{s}ss & \bar{s}ss\bar{s}s\bar{s}\bar{s} & \bar{s}ss\bar{s}\bar{s}ss\bar{s} \\
\bar{s}ss\bar{s}\bar{s}\bar{s}\bar{s}\bar{s} & \bar{c}\bar{s}ab\bar{e}\bar{s}\bar{d}s & s\bar{s}ssss\bar{s}ss & \bar{s}\bar{s}ssss\bar{s}\bar{s} & \bar{s}\bar{s}ss\bar{s}\bar{s}ss \\
\bar{s}\bar{s}ssss\bar{s}\bar{s}s & sc\bar{b}asesd & sss\bar{s}ssss\bar{s} & s\bar{s}s\bar{s}\bar{s}s\bar{s} & s\bar{s}s\bar{s}s\bar{s}\bar{s} \\
s\bar{s}s\bar{s}\bar{s}\bar{s}\bar{s}\bar{s} & \bar{d}s\bar{e}\bar{s}abcs & \bar{s}s\bar{s}\bar{s}s\bar{s}ss & s\bar{s}s\bar{s}s\bar{s}s\bar{s} & \bar{s}ss\bar{s}s\bar{s}\bar{s}s \\
\bar{s}\bar{s}sss\bar{s}ss\bar{s} & sds\bar{e}\bar{b}a\bar{s}c & ssss\bar{s}\bar{s}\bar{s}\bar{s}s & \bar{s}\bar{s}ssss\bar{s}ss & ssssss\bar{s}\bar{s}\bar{s} \\
s\bar{s}\bar{s}ss\bar{s}\bar{s}ss & \bar{e}\bar{s}d\bar{s}\bar{c}sa\bar{b} & \bar{s}\bar{s}s\bar{s}ssss & s\bar{s}\bar{s}sss\bar{s}\bar{s}s & s\bar{s}s\bar{s}\bar{s}s\bar{s}s \\
ssssss\bar{s}s\bar{s} & s\bar{e}\bar{s}\bar{d}\bar{s}\bar{c}ba & s\bar{s}\bar{s}\bar{s}\bar{s}ssss & ssssssss & ss\bar{s}\bar{s}\bar{s}\bar{s}ss \\
\bar{s}s\bar{s}\bar{s}\bar{s}ssss & ss\bar{s}\bar{s}s\bar{s}\bar{s}\bar{s} & abcsdes\bar{s} & \bar{s}\bar{s}ssss\bar{s}\bar{s}s & ss\bar{s}\bar{s}s\bar{s}\bar{s}s \\
ssss\bar{s}ss\bar{s}s & s\bar{s}s\bar{s}\bar{s}\bar{s}ss & \bar{b}a\bar{s}ce\bar{d}ss & \bar{s}s\bar{s}s\bar{s}\bar{s}\bar{s}\bar{s} & s\bar{s}s\bar{s}\bar{s}\bar{s}\bar{s} \\
\bar{s}\bar{s}s\bar{s}ssss\bar{s} & \bar{s}\bar{s}\bar{s}\bar{s}s\bar{s}\bar{s}s & \bar{c}sa\bar{b}s\bar{s}\bar{d}\bar{e} & ssss\bar{s}s\bar{s}s & \bar{s}\bar{s}\bar{s}\bar{s}\bar{s}s\bar{s}s \\
s\bar{s}\bar{s}\bar{s}s\bar{s}s\bar{s}\bar{s} & s\bar{s}\bar{s}ssss\bar{s}s & \bar{s}\bar{c}bassed & \bar{s}ss\bar{s}\bar{s}s\bar{s}s & s\bar{s}\bar{s}s\bar{s}\bar{s}ss \\
\bar{s}\bar{s}\bar{s}ssss\bar{s}s & ss\bar{s}\bar{s}\bar{s}s\bar{s}s & \bar{d}\bar{e}\bar{s}\bar{s}abc\bar{s} & \bar{s}ss\bar{s}ss\bar{s}\bar{s} & ssss\bar{s}s\bar{s}s \\
\bar{s}ss\bar{s}\bar{s}s\bar{s}\bar{s} & s\bar{s}s\bar{s}ss\bar{s}\bar{s} & \bar{e}ds\bar{s}\bar{b}asc & ssssss\bar{s}s\bar{s} & s\bar{s}\bar{s}ssss\bar{s}\bar{s} \\
\bar{s}ssss\bar{s}s\bar{s}\bar{s} & \bar{s}\bar{s}\bar{s}\bar{s}s\bar{s}s\bar{s} & \bar{s}\bar{s}de\bar{c}\bar{s}a\bar{b} & s\bar{s}s\bar{s}\bar{s}s\bar{s}\bar{s} & ss\bar{s}\bar{s}\bar{s}ss\bar{s} \\
\bar{s}\bar{s}s\bar{s}\bar{s}\bar{s}\bar{s}\bar{s}s & s\bar{s}\bar{s}s\bar{s}\bar{s}\bar{s}\bar{s} & s\bar{s}e\bar{d}s\bar{c}ba & ss\bar{s}\bar{s}s\bar{s}\bar{s}s & \bar{s}s\bar{s}\bar{s}s\bar{s}\bar{s}\bar{s} \\
s\bar{s}\bar{s}\bar{s}\bar{s}\bar{s}\bar{s}s\bar{s} & ssss\bar{s}\bar{s}ss\bar{s} & ss\bar{s}ss\bar{s}\bar{s}\bar{s} & abc\bar{d}es\bar{s}\bar{s} & s\bar{s}\bar{s}\bar{s}\bar{s}\bar{s}s\bar{s} \\
\bar{s}\bar{s}s\bar{s}\bar{s}ssss & s\bar{s}ssssss\bar{s} & s\bar{s}\bar{s}\bar{s}\bar{s}\bar{s}s\bar{s} & \bar{b}adcs\bar{e}s\bar{s} & \bar{s}\bar{s}s\bar{s}\bar{s}ssss \\
\bar{s}\bar{s}\bar{s}ssss\bar{s}ss & s\bar{s}\bar{s}\bar{s}\bar{s}\bar{s}ss\bar{s} & \bar{s}ss\bar{s}\bar{s}\bar{s}\bar{s}s & \bar{c}\bar{d}ab\bar{s}\bar{s}\bar{e}\bar{s} & \bar{s}\bar{s}\bar{s}ssss\bar{s}ss \\
s\bar{s}ssssss\bar{s} & ss\bar{s}ssss\bar{s}\bar{s} & \bar{s}\bar{s}\bar{s}ssss\bar{s}ss & d\bar{c}bas\bar{s}\bar{s}e & s\bar{s}ssssss\bar{s} \\
ssss\bar{s}s\bar{s}ss & \bar{s}\bar{s}\bar{s}s\bar{s}s\bar{s}\bar{s} & \bar{s}ssss\bar{s}\bar{s}s\bar{s} & \bar{e}\bar{s}s\bar{s}abcd & s\bar{s}ssss\bar{s}\bar{s}\bar{s}s \\
s\bar{s}ssss\bar{s}\bar{s}\bar{s}s & \bar{s}s\bar{s}\bar{s}ssss\bar{s} & ss\bar{s}s\bar{s}ssss & \bar{s}es\bar{b}a\bar{d}c & \bar{s}\bar{s}\bar{s}s\bar{s}s\bar{s}\bar{s} \\
s\bar{s}\bar{s}\bar{s}ssss\bar{s}s & \bar{s}ssss\bar{s}\bar{s}s\bar{s} & ssss\bar{s}s\bar{s}ss & s\bar{s}es\bar{c}da\bar{b} & ss\bar{s}s\bar{s}ssss \\
ss\bar{s}s\bar{s}ssss & \bar{s}\bar{s}s\bar{s}\bar{s}s\bar{s}\bar{s} & \bar{s}s\bar{s}\bar{s}ssss\bar{s} & ssse\bar{d}\bar{c}ba & \bar{s}ssss\bar{s}s\bar{s} \\
ssss\bar{s}\bar{s}\bar{s}\bar{s}s & ssss\bar{s}s\bar{s}\bar{s} & \bar{s}\bar{s}s\bar{s}\bar{s}\bar{s}\bar{s}s & \bar{s}ss\bar{s}s\bar{s}s & abc\bar{e}dsss \\
s\bar{s}ssss\bar{s}\bar{s}\bar{s} & s\bar{s}ssss\bar{s}s\bar{s} & \bar{s}ssss\bar{s}s\bar{s}\bar{s} & ssssssss\bar{s} & \bar{b}aecs\bar{d}\bar{s}s \\
s\bar{s}\bar{s}\bar{s}\bar{s}ssss & s\bar{s}\bar{s}\bar{s}\bar{s}\bar{s}s & s\bar{s}ss\bar{s}ssss & s\bar{s}s\bar{s}\bar{s}ss\bar{s} & \bar{c}\bar{e}a\bar{b}ss\bar{d}\bar{s} \\
ss\bar{s}s\bar{s}\bar{s}s\bar{s} & ss\bar{s}ssss\bar{s}s & ssss\bar{s}\bar{s}s\bar{s} & ss\bar{s}\bar{s}\bar{s}\bar{s}\bar{s} & e\bar{c}ba\bar{s}s\bar{s}d \\
\bar{s}ssss\bar{s}ssss & ssss\bar{s}\bar{s}sss & \bar{s}ssssss\bar{s}ss & ss\bar{s}\bar{s}ssss & \bar{d}\bar{s}\bar{s}sabce \\
ss\bar{s}ssss\bar{s}s & s\bar{s}ssssss\bar{s} & ss\bar{s}s\bar{s}\bar{s}\bar{s}\bar{s}s & s\bar{s}s\bar{s}s\bar{s}\bar{s}s & \bar{s}d\bar{s}\bar{s}\bar{b}a\bar{e}c \\
ssss\bar{s}ssss & s\bar{s}\bar{s}\bar{s}ssss\bar{s} & ssss\bar{s}ss\bar{s}s & \bar{s}\bar{s}\bar{s}\bar{s}s\bar{s}\bar{s}\bar{s} & \bar{s}sdsc\bar{e}a\bar{b} \\
\bar{s}s\bar{s}\bar{s}\bar{s}s\bar{s}\bar{s} & ss\bar{s}\bar{s}s\bar{s}\bar{s}\bar{s} & \bar{s}s\bar{s}\bar{s}\bar{s}ssss & s\bar{s}\bar{s}\bar{s}s\bar{s}s & \bar{s}\bar{s}sd\bar{e}\bar{c}ba
\end{bmatrix}$$

[a] Kharaghani and Tayfeh-Rezaie [122, p317-324] ©Elsevier

Chapter 9
Existence of Hadamard Matrices and Asymptotic Existence results for Orthogonal Designs

Heretofore we have studied extensively the Hadamard conjecture,

> "There exists an Hadamard matrix of order 1, 2 and $4t$ for every positive integer t."

Many infinite families and ad-hoc constructions have been given. However, the density of known orders has continued to be zero.

The first portion of this chapter is devoted to proving the first powerful asymptotic theorem Seberry(=Wallis) [237] on the existence of Hadamard matrices. We then explore how the use of more "twos" leads us to considerably improved results for Hadamard matrices by Craigen [34] (but not using orthogonal designs), and then the wonderful results by Craigen, Holzmann and Kharaghani [36] for asymptotic existence of complex Hadamard matrices, orthogonal designs and amicable Hadamard matrices. Asymptotic results for repeat designs remain a major research problem.

9.1 Existence of Hadamard Matrices

As in many other combinatorial design problems, recursive construction are of very great use in constructing orthogonal designs and Hadamard matrices. In fact, in Theorem 9.3 this method gives us a most powerful method for constructing Hadamard matrices now known.

Lemma 9.1. *Suppose all orthogonal designs of type* $(a,b,n-a-b)$, $0 \le a+b \le n$, *exist in order* n. *Then all orthogonal designs of type* $(x,y,2n-x-y)$, $0 \le x+y \le 2n$, *exist in order* $2n$. *This also means that all* $OD(n;x,y)$ *exist.*

Proof. Recall that from Lemma 4.11 (ii) we have that the existence of the design of type $(a,b,n-a-b)$ in order n implies the existence of the design of type $(a,a,2b,2(n-a-b))$ in order $2n$.

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5_9

Let (u,v,w) be a full orthogonal design of order $2n$ (we may assume $0 \le u \le v \le w$). It follows that $v < n$. We distinguish four cases, depending on weather u or v are even or odd.

Case 1: u even, v even.
Then $u = 2a$, $v = 2b$, and $a+b \le n$. Then $(a,b,n-a-b)$ exists in order n, and we may apply Lemma 4.11(ii).

Case 2: u even, v odd.
Write $u = 2a$, $v = 2a+\ell$. Then $a+v = 3a+\ell \le n$, for in this case $w = 2n-4a-\ell$, and $v \le w \Rightarrow 3a+\ell \le n$.
Thus, $(v,a,n-a-v)$ exists in order n, and we may apply Lemma 4.11(ii) to it.

Case 3: u odd, v even.
Write $u = 2a+1$, $v = 2b$. Then $w = 2t+1$ and $u+v+w = 2n$, and so $a+b+t+1 = n$. Notice that $u+b \le n$, for if not, $u+b > n$, which implies $a > t$.
Thus, there is an orthogonal design of type $(u,b,n-u-b)$ in order n, and we may proceed as before.

Case 4: u odd, v odd.
In this case, write $v = u+2b$, $b \ge 0$. Clearly, $u+b \le n$, and so there is an orthogonal design of type $(u,b,n-u-b)$ in order n, and we're done. □

Corollary 9.1. *Since all the orthogonal designs of type $(a,b,4-a-b)$ exist in order 4 for $0 \le a+b \le 4$, we have all orthogonal designs of type $(x,y,n-x-y)$ for $0 \le x+y \le n$ whenever n is a power of 2.*

Corollary 9.2. *Since all orthogonal designs of type $(x,y,n-x-y)$, $0 \le x+y \le n$, exist in all orders for which n is a power of 2, all designs of type (z,w), $0 \le z+w \le n$, exist in all orders n which are powers of 2.*

It is presently known that

Corollary 9.3. *There exist Hadamard matrices of orders 2, 4, $2^t.2$, $2^t.3$, $2^t.5$, and $2^t.7$ for all positive integers $t \ge 2$.*

Proof. From Corollary 4.9. □

Conjecture 9.1 (Seberry). All orthogonal designs of type $(x,y,m-x-y)$, $0 \le x+y \le m$, exist in orders $m = 2^t q$ for any natural q and sufficiently large t.

9.2 The Existence of Hadamard Matrices

The following theorem of Sylvester, which he studied because of a problem posed by Frobenius, is well known.

Theorem 9.1. *Given any two relatively prime integers x and y, every integer $N > (x-1)(y-1)$ can be written in the form $ax+by$ for some non-negative integers a and b.*

Corollary 9.4. *Given $x = (v+1)$ and $y = (v-3)$, where v is odd and $v \geq 9$, there exist non-negative integers a and b such that $a(v+1)+b(v-3) = n = 2^t$ for some t.*

Proof. Let g be the greatest common divisor of $v+1$ and $v-3$. Then $g = 1, 2$ or 4. If $g \neq 1$, let m be the smallest power of 2 greater than $N = [((v+1)/g)-1][((v-3)/g)-1]$. Then by the theorem, there exist integers a and b such that $a(v+1)/g + b(v-3)/g = m$, and hence we have the corollary, since g is a power of 2. □

Lemma 9.2. *Let $v \equiv 3 \pmod 4$ be a prime ≥ 9. Then there exist a t such that an Hadamard matrix exists in every order $2^s.v$ for $s \geq t$.*

Proof. Let $x = v+1$ and $y = v-3$; then by the previous corollary there exists an a and b such that $ax+by = n = 2^t$ for some t. Now we know the orthogonal design D of type $(a, b, n-a-b)$ exists with order 2^t on the variables x_1, x_2, x_3.

Then replace each variable x_1 by the matrix J, each variable x_2 by $J-2I$ and each variable x_3 by the back-circulant $(1,-1)$ matrix $B = (Q+I)R$, where Q is defined in the proof of Lemma 4.12 and R is the back-diagonal matrix, to form a matrix E. Now

$$B^\top = B,\ BJ = J,\ B(J-21) = (J-21)B,\ BB^\top = (v+1)I - J,$$

$$DD^\top = \left(ax_1^2 + bx_2^2 + (n-a-b)x_3^2\right) I_n,$$

and

$$\begin{aligned} EE^\top &= \left(aJ^2 + b(J-21)^2 + (n-a-b)BB^\top\right) \times I_n, \\ &= [avJ + 4bI + b(v-4)J + (n-a-b)(v+1)I - (n-a-b)J] \times I_n, \\ &= ([n(v+1) - a(v+1) - b(v-3)]I + [a(v+1) + b(v-3) - n]J) \times I_n, \\ &= nvI_{nv}. \square \end{aligned}$$

Lemma 9.3. *Let $v \equiv 1 \pmod 4$ be a prime ≥ 9. Then there exists a t such that an Hadamard matrix exists in every order $2^s.v$ for $s \geq t+1$.*

Proof. Choose x, y, n, t, a, b, and D as in the previous lemma. Now note there exists an orthogonal design F of type $(2a, 2b, n-a-b, n-a-b)$ in order $2n = 2^{t+1}$ on the variables x_1, x_2, x_3, x_4.

Form the matrix E by replacing the variable x_1 of F by J, each variable X_2 of F by $J-2I$, and the variables x_3 and x_4 by the two circulant $(1,-1)$ incidence matrices $X = I+Q$ and $Y = I-Q$, where Q is defined in the proof of Lemma 4.12. Now

$$X^\top = X,\ Y^\top = Y,\ XY^\top = YX^\top,\ XX^\top + YY^\top = 2(v+1)I - 2J,$$
$$XJ = YJ = J,\ X(J-2I) = (J-2I)X,\ Y(J-2I) = (J-2I)Y,$$
$$FF^\top = \left(2ax_1^2 + 2bx_2^2 + (n-a-b)x_3^2 + (n-a-b)x_4^2\right) I_{2n},$$

and

$$\begin{aligned} EE^\top &= ((2aJ^2 + 2b(J-2I)^2 + (n-a-b)(XX^\top + YY^\top) \times I_{2n} \\ &= [2avJ + 8bI + 2b(v-4)J + (n-a-b)(2(v+1)I - 2J)] \times I_{2n}, \\ &= [2n(v+1) - 2a(v+1) - 2b(v-3)I_{2nv} \\ &\qquad + [2a(v+1) + 2b(v-3) - 2n]J_v \times I_{2n}, \\ &= 2nvI_{2nv}. \square \end{aligned}$$

Theorem 9.2. *Given any integer q, there exists t dependent on q such that an Hadamard matrix exists of every order $2^s q$ for $s \geq t$.*

Proof. Decompose q into its prime factors, and apply the previous lemma to each factor. The result follows because the Kronecker product of any two Hadamard matrices is an Hadamard matrix. □

In Corollary 9.4 we chose t so that

$$2^t \geq \left(\frac{v+1}{g} - 1\right)\left(\frac{v-3}{g} - 1\right)$$

Hence, if $v \equiv 1 \pmod 4$, $g = 2$, and we need $2^t \geq \frac{1}{4}(v-1)(v-5)$. Thus, we may choose $t = [2\log_2(v-3)] - 1$ in Lemma 9.3.

For $v \equiv 3 \pmod 4$, $g = 4$, and choosing $t = [2\log_2(v-5)] - 3$ ensures the existence of an Hadamard matrix of order $2^t v$ in Lemma 9.2.

We observe that if $v = p.q$ where p and q are primes $\equiv 1 \pmod 4$, we can ensure the existence of an Hadamard matrix of order $2^r.pq$ where $r = [2\log_2(p-3)] + [2\log_2(q-3)] < [2\log_2(pq-3)]$. Since a v comprising a product of primes $\equiv 1 \pmod 4$ would give the highest theoretical t for which an Hadamard matrix of order $2^t v$ exists, we can say:

Theorem 9.3. *(i) Given any natural number q, there exists an Hadamard matrix of order $2^s q$ for every $s \geq [2\log_2(q-3)] + 1$.*

(ii) Given any natural number q, there exists a regular (i.e., constant row sum) symmetric Hadamard matrix with constant diagonal of order $2^{2s}q^2$ for s as before.

Proof. Part (ii) of the theorem follows from a theorem of Goethals and Seidel (see Wallis [231], p. 341) that if there is an Hadamard matrix of order n, there is a regular symmetric Hadamard matrix with constant diagonal of order n^2.

The result that orthogonal designs $(a, b, n-a-b)$ exist in all orders $n = 2^t.3$, $t \geq 3$, may be used in a similar fashion to that employed in Lemma 9.2 to construct Hadamard matrices of order $2^s.3q$ for sufficiently large s. It may

happen that proceeding via this result for appropriate natural numbers $3q$ gives a smaller s than if Theorem 9.3 were used.

This last remark indicates that a knowledge of orthogonal designs $(a,b,n-a-b)$ in orders $n=2^tp$, p odd, could lead to Hadamard matrices of order 2^spq for smaller s than that given by Theorem 9.3.

Clearly, in general, there will be Hadamard matrices, given by the construction, of order 2^tq where $t<[\log_2(q-3)]$. □

9.3 Asymptotic Existence Results for Orthogonal Designs

Necessary conditions for the existence of orthogonal designs have been derived from a study of rational matrices. The theorems below show that many of these conditions are also sufficient if the order of the orthogonal design is much larger than the number of non-zero entries in each row.

If n is odd, then $\rho(n)=1$, so the only orthogonal designs of order n are weighing matrices. We have shown that the weight k of a weighing matrix of odd order n must be a square. If n is much larger than k, this is sufficient for existence; in fact,

Theorem 9.4 (Geramita-Wallis). *Suppose k is a square. Then there is an integer $N=N(k)$ such that for any $n>N$ there is a $W(n,k)$.*

This theorem follows from Lemma 9.4 below.

Suppose $n\equiv 2 \pmod 4$; then an orthogonal design of order n has at most two variables. For these orders we derived the following necessary conditions:

(i) If there is an orthogonal design of type (a,b), then there is a 2×2 rational matrix P such that $PP^\top = diag(a,b)$.
(ii) If there is a weighing matrix $W(n,k)$ then k is a sum of at most two squares.
(iii) If there is a skew-symmetric weighing matrix $W(n,k)$ then k is a square.

We can prove an asymptotic converse to (i), (ii) and (iii):

Theorem 9.5 (Eades).

(i) Suppose there is a 2×2 rational matrix P such that $PP^\top = \mathrm{diag}(a,b)$ where a and b are positive integers. Then there is an integer $N=N(a,b)$ such that for all $t\geq N$ there is an $OD(2t;a,b)$.
(ii) Suppose k is a sum of two integer squares. Suppose $k\neq 2t-1$, t odd, then there is an integer $N=N(k)$ such that for all $t\geq N$ there is a $W(2t,k)$.
(iii) Suppose k is a square. Then there is an integer $N=N(k)$ such that for all $t\geq N$ there is a skew-symmetric $W(2t,k)$.

The proof of Theorem 9.5 comes later. We merely note here that (ii) and (iii) follow immediately from (i).

Suppose $n \equiv 4 \pmod 8$; then an orthogonal design of order n has at most four variables. The results of Chapter 3 show that for these orders the following necessary conditions apply:

(i) If there is an orthogonal design of type (a,b,c,d) and order $n \equiv 4 \pmod 8$, then there is a 4×4 rational matrix P such that $PP^\top = diag(a,b,c,d)$.
(ii) If there is a skew-symmetric $W(n,k)$ where $n \equiv 4 \pmod 8$, then k is a sum of three integer squares.

In 1971 Seberry(Wallis) [232] conjectured:

Conjecture 9.2 (Seberry). For every positive integer $k \leq n \equiv 0 \pmod 4$ there is a $W(n,k)$.

We can prove an asymptotic result on this conjecture, an asymptotic converse for (ii) and a partial asymptotic converse for (i).

Theorem 9.6 (Eades).

(i) Suppose m, z_1, z_2, z_3 and z_4 are positive integers. Then there is an integer $N = N(m, z_1, z_2, z_3, z_4)$ such that for all $t \geq N$ there is an $OD(4t; mz_1^2, mz_2^2, mz_3^2, mz_4^2)$.
(ii) Suppose $m_1, m_2, z_1, z_2, z_3, z_4$ are positive integers and m_1 and m_2 are each sums of two integer squares. Then there is an integer N depending on $m_1, m_2, z_1, z_2, z_3, z_4$ such that for all $t \geq N$ there is an $OD(4t; m_1z_1^2, m_1z_2^2, m_2z_3^2, m_2z_4^2)$.
(iii) For any integer k there is an integer $N = N(k)$ such that for all $t \geq N$ there is a $W(4t,k)$.
(iv) If k is a sum of three integer squares, then there is an integer $N = N(k)$ such that for all $t \geq N$ a skew-symmetric $W(4t,k)$ exists.

Again we will leave the proof of this theorem for later and merely note that (iii) and (iv) follow from (i).

For $n \equiv 0 \pmod 8$ it is conjectured that for every $k < n$ there is a skew-symmetric $W(n,k)$. We can prove:

Theorem 9.7. *(i) Suppose $u_1, u_2, \ldots, u_8$ are integers. Then there is an integer $N = N(u_1, u_2, \ldots, u_8)$ such that for all $t \geq N$ an orthogonal design of type $u_1^2, u_2^2, \ldots, u_8^2$ and order $8t$ exists.*
(ii) For any pair (a,b) of integers there is an integer $N = N(a,b)$ such that for all $t \geq N$ there is an orthogonal design of type (a,b) and order $8t$.
(iii) For any integer k there is an integer $N = N(k)$ such that for all $t \geq N$ there is a skew-symmetric $W(8t,k)$.

Since any integer is a sum of four squares of integers, (ii) and (iii) follow from (i).

From Theorem 9.4, Theorem 9.5(ii) and (iii), Theorem 9.6 (iii) and (iv), and Theorem 9.7 (iii), we can deduce:

Corollary 9.5. *(i) For any integer k there is only a finite number, $M_1(k)$, of orders for which the existence of a weighing matrix of weight k is undecided.*

(ii) For any integer k there is only a finite number, $M_2(k)$ of orders for which the existence of a skew-symmetric weighing matrix of weight k is undecided.

From Theorem 9.5 (i) we can deduce:

Corollary 9.6. *For any pair (a,b) of integers there are only a finite number, $M_3(a,b)$ of orders $n \equiv 2 \pmod 4$ for which the existence of an orthogonal design of order n and type (a,b) is undecided.*

Lemma 9.4. *Suppose $k \neq 0$ is a square, and let $k = \prod_{i=1}^{m} q_i^2$ where each q_i is either 1 or a prime power, for $i = 1,2,\ldots,m$. Suppose $a_1, a_2, \ldots, a_m$ are any positive integers, and let $n = \prod_{i=1}^{m} a_i(q_i^2 + q_i + 1)$. Then there is a type-1 $W(n,k)$ and type-2 $W(n,k)$ on the group $\prod_{i=1}^{m} Z_{v_i}$, $v_i = a_i(q_i^2 + q_i + 1)$.*

Proof. If q is either 1 or a prime power, then there is a circulant $W(q^2+q+1, q^2)$. Suppose the first row of the matrix is (w_i), $1 \le i \le q^2+q+1$. If a is a positive integer and $1 \le i \le a(q^2+q+1)$, then define

$$W'_t = \begin{cases} w_i, & \text{if } i \equiv 0 \pmod a, \\ 0, & \text{otherwise.} \end{cases}$$

Then $(W'_i), 1 \le i \le a(q^2+q+1)$, is the first row of a circulant $W(a(q^2+q+1), q^2)$.

Proceed now by induction. If there is a type-1 $W(n_i,k_i)$ on G_i, for $i = 1,2$, then the tensor product of $W(n_1,k_1)$ with $W(n_2,k_2)$ is a type-1 $W(n_1,n_2,k_1,k_2)$ on $G_1 \times G_2$.

We recall that the existence of a type-1 $W(n,k)$ on G implies the existence of a type-2 $W(n,k)$. (See Corollary 4.7.) □

The next lemma is a consequence of Sylvester's theorem (Theorem 9.1).

Lemma 9.5. *Suppose orthogonal designs of type $(u_1,u_2,\ldots,u_m)$ exist in orders n_1 and n_2. Let $h = g.c.d.(n_1,n_2)$. Then there is an integer N such that for all $t > N$ there is an orthogonal design of type $OD(ht;u_1,u_2,\ldots,u_m)$.*

Proof. Proof of Theorem 9.4. By Lemma 9.4, for every square k there is an odd number n such that $W(n,k)$ exists, By Corollary 9.2 there is a $W(2^t,k)$ for some t. Now since n is odd, $g.c.d.(n,2^t) = 1$, so Lemma 9.5 gives Theorem 9.4. □

Lemma 9.6. *Suppose there is an orthogonal design of type* $OD(n;u_1,u_2,\ldots,u_k)$*; suppose* $z_1,z_2,\ldots,z_k$ *are integers. Then there is an odd number,* y*, such that an orthogonal design of type* $OD(yn;z_1^2u_1,z_2^2u_2,\ldots,z_k^2u_k)$ *exists.*

Proof. Let $z=\prod_{i=1}^{b}q_i$ be a decomposition of z into prime powers. Let $y_1=\prod_{i=1}^{b}(q_i^2+q_i+1)$, and let W be the type-2 $W(y_1z_1^2)$ assured by Lemma 9.4. Type-2 matrices are always symmetric, so the k-tuple $(W,I,I,\ldots,I)$ comprises pairwise amicable matrices. Hence, using Lemma 4.20, there is an orthogonal design of type $OD(y_1n;z_1^2u_1,u_2,\ldots,u_k)$. Note that y_1 is odd.

We can clearly continue this process to prove the lemma. □

In fact, all the weighing matrix results in Theorems 9.6, 9.7 and Corollary 9.5 (9.5 (ii) and (iii), 9.6(iii) and (iv), 9.7(iii)) follow from Corollary 9.2, Lemmas 9.4, 9.5 and 9.6. However, we will prove the more general results first.

Lemma 9.7. *Suppose* m *is a sum of two integer squares. Then there is an odd number* t *such that an orthogonal design of type* $OD(2t;m,m)$ *exist.*

Proof. Let $m=m_1^2+m_2^2$. If $m_j\neq 0$, let $m_j^2=\prod_{i=1}^{k}q_{ij}^2$ where q_{ij} is either 1 or a prime power. For each $i=1,2,\ldots,k$ let $b_i=LCM\{q_{ij}^2+q_{ij}+1;m_j\neq 0\}$. If $m_j\neq 0$, let W_j be the type-1

$$W\left(\prod_{i=1}^{k-1}b_i,\prod_{i=1}^{k-1}q_{ij}^2\right)$$

and on the group $\prod_{i=1}^{k-1}Z_{b_j}$ from Lemma 9.4. Note that C_j is circulant. Suppose the first row of C_j is $(c_{rj},\ 1\leq r\leq b_k$.

Define (d_{rj}), $1\leq r\leq 3b_k$.

$$d_{rj}=\begin{cases}c_{rj}, & \text{if } r\equiv j \pmod 3\\ 0, & \text{otherwise.}\end{cases}$$

Then the circulant D_j with the first row (d_{rj}) is a type-1 $W(3b_k,q_{kj}^2)$ on Z_{3b_k}. Moreover, if $m_1\neq 0$ and $m_2\neq 0$, then D_1 and D_2 are mutually disjoint. If $m_j\neq 0$, let $F_j=D_j\times W_j$. If $m_j=0$, let F_j be the zero matrix of order $3\prod_{i=1}^{k}b_i$. Then F_1 and F_2 are disjoint type-1 weighing matrices of weights m_1^2 and m_2^2, respectively, on the group $\prod_{i=1}^{k-1}Z_{b_i}\times Z_{3b_k}$. Each b_i is odd, so the order of F_1 is an odd number, $t=3\prod_{i=1}^{k}b_i$. Hence, we can use the matrices $x_1F_1+x_2F_2$ and $x_2F_1-x_1F_2$ in the Wallis-Whiteman generalization of the two circulant construction, obtained by using the remarks before Lemma 4.4 with Proposition 4.1 to produce an orthogonal design of type $OD(2t;m,m)$ on the variables x_1 and x_2. □

To prove Theorem 9.5 we need a simple fact about 2×2 rational matrices.

Lemma 9.8. *Suppose a and b are integers such that there exists a rational 2×2 matrix P satisfying $PP^\top = \mathrm{diag}(a,b)$. Then there are integers x,y,z,w such that $a = \left(z^2+w^2\right)x^2$ and $b = \left(z^2+w^2\right)y^2$.*

Proof. Let $a = x^2 z_1$ and $b = y^2 z_2$, where z_1 and z_2 are square-free integers. Now $ab = (\det P)(\det P^\top)$ is a rational square. Hence $z_1 = z_2$. Now a is a sum of two rational squares; hence z_1 is a sum of two rational squares. The Cassells-Davenport theorem the implies that z_1 is a sum of two integer squares, say, $z_1 = z^2+w^2$. So $a = x^2\left(z^2+w^2\right)$, $b = y^2\left(z^2+w^2\right)$. □

Proof. Proof of Theorem 9.5. Suppose a and b are integers such that there exists a rational 2×2 matrix P satisfying $PP^\top = \mathrm{diag}(a,b)$. Then by Lemma 9.8 there are integers x, y and m such that $a = x^2 m$, $b = y^2 m$, and m is a sum of at most two integer squares. Lemma 9.7 gives an orthogonal design of type $OD(2t;m,m)$ for some odd t. Lemma 9.6 gives an orthogonal design of type $OD(2ty;x^2m,y^2m) = (a,b)$, for some odd y. Corollary 9.2 gives an orthogonal design of type $OD(2^d;a,b)$, for some integer d. Now $g.c.d.(2^d,2ty) = 2$, so we can use Lemma 9.5 to obtain Theorem 9.5. □

The proof of the next lemma is very similar to the proof of Lemma 9.7 and so is omitted.

Lemma 9.9. *For any positive integer m there exists an odd number t such that an orthogonal design of type $OD(4t;m,m,m,m)$ exists.*

We have exhibited an orthogonal design of type $(1,1,\ldots,1)$ and order n on $\rho(n)$ variables. Since $\rho(2^d)$ is a strictly increasing function of d, equating variables in the Geramita-Pullman orthogonal design gives the following lemma.

Lemma 9.10. *Let $(u_1,u_2,\ldots,u_k)$ be a sequence of positive integers. Then there is an integer d such that an orthogonal design of type $OD(2^d;u_1,u_2,\ldots,u_k)$ exists.*

Proof. Proof of Theorem 9.6. By Lemma 9.9 there is an orthogonal design of type $OD(4t;m,m,m,m)$ for some odd t for any integer m. If z_1, z_2, z_3 and z_4 are integers, then Lemma 9.6 implies the existence of an orthogonal design of type $OD(4ty;z_1^2m,z_2^2m,z_3^2m,z_4^2m)$ for some odd y. Lemma 9.10 gives an orthogonal design of type $OD(2^d;z_1^2m,z_2^2m,z_3^2m,z_4^2m)$ for some d. Since $g.c.d.(4ty,2^d) = 4$, we have Theorem 9.6 (i) and (iv) following immediately. Theorem 9.6 (ii) follows from Theorem 9.5 (i). □

Proof. Proof of Theorem 9.7. There is an orthogonal design of type $OD(8;1,1,1,1,1,1,1,1)$. Hence by Lemma 9.6 there is an orthogonal design of type $OD(8y;z_1^2,z_2^2,\ldots,z_8^2)$ for some odd y. Lemma 9.10 ensures the existence of an orthogonal design $OD(2^d;z_1^2,z_2^2,\ldots,z_8^2)$, $d>3$. Hence Lemma 9.5 gives Theorem 9.7 (i); Theorem 9.7 (ii) and (iii) follow immediately. □

9.4 n-Tuples of the Form $(2^p b_1, 2^p b_2, \ldots, 2^p b_n)$

The above discussion led us to believe that while we might not yet know all about orthogonal designs in "small" orders, we might be able to say far more about their existence in "large" orders. The remainder of this section is another case of hindsight: Eades, Robinson, Wallis and Williams first saw the results in powers of 2, and then Eades showed that the same argument could always be used.

This section also shows a distinction in approach between an algebraist and a combinatorialist. The algebraist can ensure the existence of any n-tuple as the type of an orthogonal design in some order $2^t q$ by allowing most of the entries of the design to be zero. The combinatorialist is interested in establishing existence with as few zeros as possible, as this case is more useful in applications.

In the remainder of this section the figures and diagrams are taken directly from the printed form in [80].

Definition 9.1. A *binary expansion* of a positive integer s is a non-decreasing sequence $B = b_1, b_2, \ldots, b_k)$ of powers of 2 such that $b_1 + b_2 + \cdots + b_k = s$. If B is strictly increasing, we say B is the binary decomposition of s. The binary expansion of $A = (s_1, \ldots, s_n)$, an n-tuple of positive integers, is $(B_1, \ldots, B_n)$, where B_i is the binary expansion of s_i.

From a binary expansion $B = (b_1, b_2, \ldots, b_k)$ of s, we can obtain new binary expansions by *combining*:

$$\left(b_1, b_2, \ldots, 2^j, 2^j, \ldots, b_k\right) \to \left(b_1, b_2, \ldots, 2^{j+1}, \ldots, b_k\right)$$

or by *splitting*

$$\left(b_1, b_2, \ldots, 2^{j+1}, \ldots, b_k\right) \to \left(b_1, b_2, \ldots, 2^j, 2^j, \ldots, b_k\right)$$

with suitable reordering. If a binary expansion C is obtained from a binary expansion B by repeating these operations, we say C is *equivalent* to B. Clearly, this relation is transitive.

Lemma 9.11. *Any two binary expansions of s are equivalent.*

Proof. All binary expansions of s are equivalent to the binary decomposition of s by combining. □

Lemma 9.12. *Suppose there is an orthogonal design of type B and order t, where B is a binary expansion of s, Then for every binary expansion C of s, there is an orthogonal design of type $OD(2^p t; 2^p C)$ for some integer p.*

Proof. If there is an orthogonal design of type

$$OD\left(t; b_1, b_2, \ldots, 2^j, 2^j, \ldots, b_k\right)$$

then there is an orthogonal design of type

$$OD\left(t;b_1,b_2,\ldots,2^{j+1},\ldots,b_k\right)$$

If there is an orthogonal design of type

$$OD\left(t;b_1,b_2,\ldots,2^{j+1},\ldots,b_k\right)$$

then there is an orthogonal design of type

$$OD\left(2t;b_1,b_2,\ldots,2^j,2^j,\ldots,b_k\right) \text{ (Theorem 4.3).}\square$$

Clearly, the integer p in the lemma above is the number of splittings to get C from B.

We can now deduce:

Theorem 9.8. *Let B be a binary expansion of s, and suppose there is an orthogonal design $OD(t;B)$.*

Let $(a_1,a_2,\ldots,a_u)$ be a u-tuple of positive integers such that $a_1+a_2+\cdots+a_u=2^k s$ for some k.

Then there is an integer p such that an orthogonal design of type $OD(2^{p+k}t;2^p a_1,2^p a_2,\ldots,2^p a_u)$ exist.

Proof. We can split B to obtain an orthogonal design of type C and order $2^k t$, for some binary expansion C of $2^k s$. Let D be the binary expansion of $2^k s$ which is obtained from the binary decompositions of the a_i. Then the theorem follows by Lemma 9.12. □

This theorem is most interesting when $s=t$. The case $s=t=1$ can be proved using the orthogonal design of order 1 for B.

The integer p depends on the sum of the lengths of the binary decompositions of the a_i. Since there are only a finite number of u-tuples which add to $2^k s$, we can state:

Theorem 9.9. *Suppose B is a binary expansion of s, and suppose there is an orthogonal design $OD(t;B)$. Let u and k be integers. Then there is an integer q such that every orthogonal design of type $OD(2^{q+k}t;2^q a_1,2^q a_2,\ldots,2^q a_u)$ exist for all $(a_1,a_2,\ldots,a_u)$ such that $a_1+a_2+\cdots+a_u=2^k s$.*

Example 9.1. There is an orthogonal design of type $OD(12;1,1,2,8)$. This gives an $OD(24;1,1,2,4,16)$. Hence, for every $(a_1,a_2,\ldots,a_u)$ such that $a_1+a_2+\cdots+a_u=2^k.12$, there is an integer p such that there is an orthogonal design of type $OD(2^{p+k}.12;2^p a_1,2^p a_2,\ldots,2^p a_u)$.

We can use the same algorithm described in Figure 9.1 to obtain p. If $(a_1,a_2,\ldots,a_u)=(1,1,2,6,14)$, the algorithm is as follows;

1	1	2	2	2	4	4	8	1	1	2		4					16		
2	2	4	4	4	8	8	16	2	2	4		8			16			16	
4	4	8	8	8	16	16	32	4	4	8		16		16		16			32
8	8	16	16	16	32	32	64	8	8	16	16		16	32		32		64	

and so $p = 3$, and a design of type $8 \times (1, 1, 2, 6, 14)$ exists in order $2^4 \times 12$.

9.4.1 Description of the Construction Algorithm

Let A be an n-tuple of positive integers, and let B be the binary union of A described above. We write $B = (b_1, b_2, \ldots, b_j)$. Then algorithm proceeds as shown in Figure 9.1:

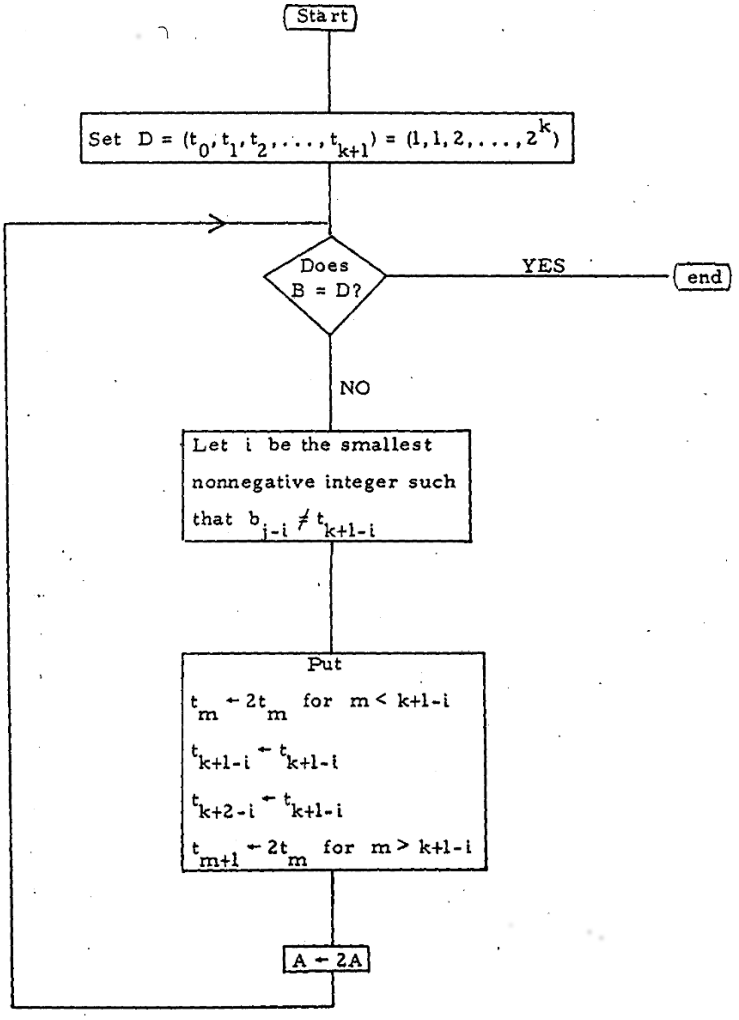
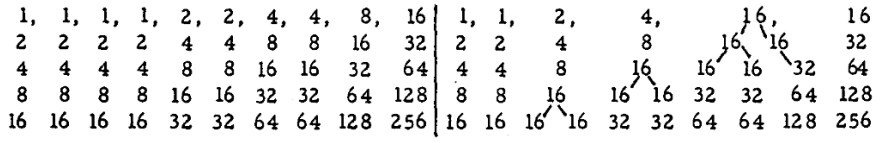


Fig. 9.1 n-tuple construction algorithm

Example 9.2. There is an orthogonal design of type $OD(20;4,8,8)$. Let $(a_1,a_2,\ldots,a_u)=(1,1,5,15,18)$. Now from the $(4,8,8)$ of order 20, we can find a $4(1,1,2,4,16,16)$ of order 160. We can use the algorithm as in Figure 9.1:

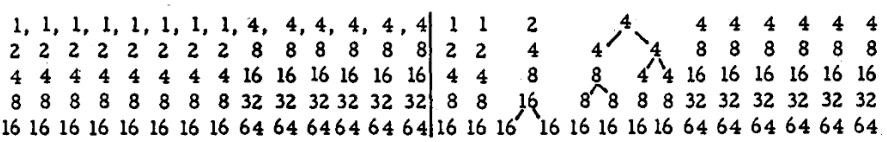


Hence, there is an orthogonal design of type

$$4\times 16\times(1,1,5,15,18)$$

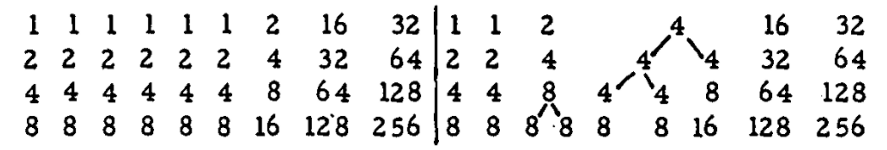
and order $8\times 16\times 20$, Thus, in this case $p=6$.

Example 9.3. For a third example, consider $(a_1,a_2,\ldots,a_u)=(1,1,5,5,5,5,5,5)$. This 8-tuple expands to $(1,1,1,1,1,1,1,1,4,4,4,4,4,4)$, and so the methods of Figure 9.1 give an orthogonal design of type $(1,1,5,5,5,5,5,5)\times 2^8$. But if we use the orthogonal design of type $OD(8;1,1,1,1,1,1,1,1)$ for B in Theorem 9.8, we obtain an orthogonal design of type $(1,1,5,5,5,5,5,5)\times 2^4$ and order 32×2^4. The algorithm proceeds as follows:



and so $p=4$.

Example 9.4. There is an orthogonal design of type $OD(28;4,4,4,16)$. The 8-tuple $(1,1,1,1,1,2,17,32)$ illustrates the use of combining as well as splitting. From the $(4,4,4,16)$ we obtain a design of type $4(1,1,2,4,8,8,32)$ and order 4×56. We use the combining operation to form a design of type $4(1,1,2,4,16,32)$ and order 4×56 and then proceed with splitting in the usual way:



So in this case $p=5$.

9.4.2 Implementing the Algorithm

We consider the n-tuple $A = (s_1, \ldots, s_n)$, $\sum s_i = s$, in order $2^k q$.

Suppose $n \leq 3$. Then if s is a power of 2, by Corollary 9.1, A corresponds to the type of an orthogonal design.

Suppose $n > 3$, and 2^j is the highest power of 2 which divides each s_i. Then we can use Lemma 7.30 9.12 with the n-tuple $(s_1/2^j, \ldots, s_n/2^j) = (t_1, \ldots, t_n)$ in order 2^{k-j}.

In fact, for any n and only two odd entries in A, we can usually use the following process to obtain a starting point for the algorithm in a lower power of 2.

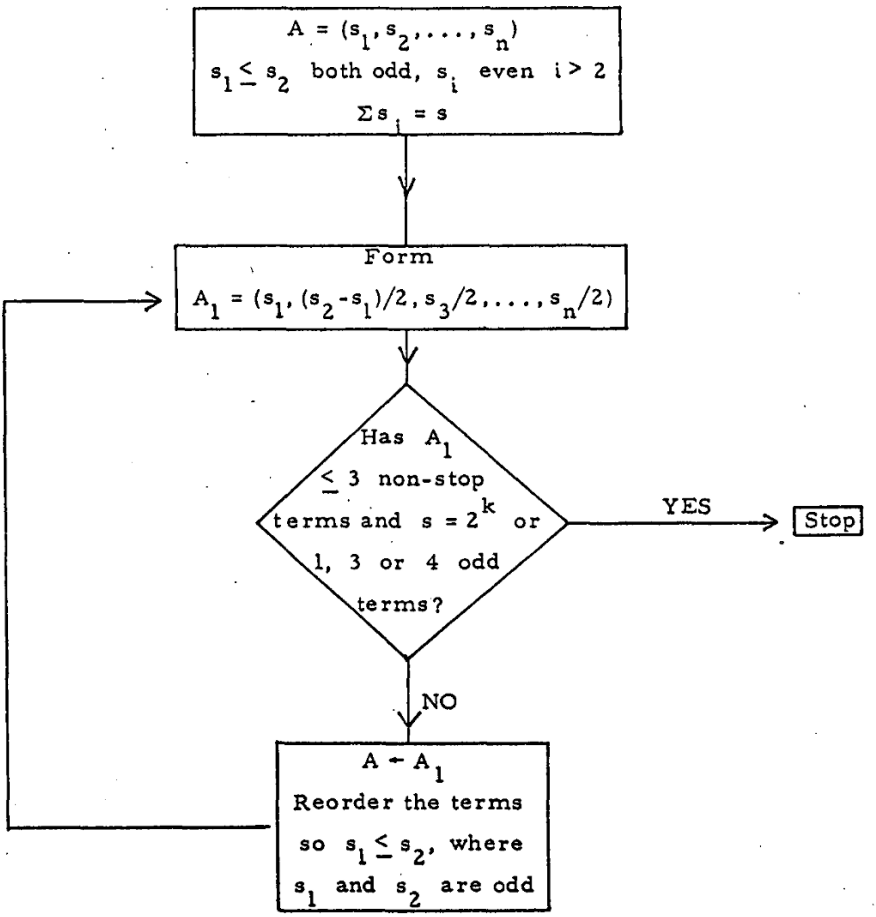


Fig. 9.2 Implementing the algorithm

Example 9.5. Consider the binary 5-tuple $A = (3,3,6,20,96)$ in order 128. Now the binary expansion of A is $(1,2,1,2,2,4,4,16,32,64)$, which is a 10-tuple. So Theorem 9.9 guarantees the existence of a 5-tuple $(2^3.3, 2^3.3, 2^3.6, 2^3.20, 2^3.96)$ in order 2^{10}. But if we use the method of Figure 9.2, we form

$$(3,(3-3)/2,6/2,20/2,96/2) = (3,3,10,48) \text{ in order } 64,$$

and then

$$(3,(3-3)/2,10/2,48/2) = (3,5,24) \text{ in order } 32.$$

But all 3-tuples $(a,b,32-a-b)$ exist in order 32, so $(3,3,6,20,96)$ is the type of an orthogonal design in order 128.

9.4.3 n-Tuples in Powers of 2 With No Zeros

In the case where the sum of the entries of A is a power of 2 and A has no zero entries, i.e., the sum of the entries of A is the order of A, it is possible to determine the maximum value of p.

Definition 9.2. Let $A = (s_1, s_2, \ldots, s_n)$ be an n-tuple of positive integers with $s_1 + s_2 + \cdots + s_n = s = 2^t$. We write the binary expansion of each s_i, $i = 1, \ldots, n$, and rearrange the order to obtain $B = (b_1, b_2, \ldots, b_k)$, the *binary expansion* of A, where each b_i is a power of 2 and $b_j \le b_{j+1}$. We say the *binary length* of A is $k = R_A(n,t)$, the number of entries of B, and use $R(n,t)$ for $\max_A R_A(n,t)$.

Theorem 9.10. *Let $A = \{s_i\}$ be an n-tuple of positive integers such that at least two entries of A are odd and the sum of the entries of A is 2^k. Then there is an orthogonal design of type $OD(2^{p+k}; 2^p A)$, where p is the binary length of A minus $k+1$.*

Example 9.6. Robinson's Theorem 8.1 shows that there is no orthogonal design of type $(1,1,1,1,1,2^t-5)$ in any order $2^t > 40$. Now $2^t - 5$ has a binary expansion $1 + 2 + 2^3 + 2^4 + \cdots + 2^{t-1}$, so $B = (1,1,1,1,1,1,2,8,16,\ldots,2^{t-1})$ and $p = t + 4 - (t+1) = 3$. Hence there is an orthogonal design of type $OD(2^{t+3}; 2^3.1, 2^3.1, 2^3.1, 2^3.1, 2^3.1, 2^3.(2^t-5))$.

Proof. Let $A = (a_1, a_2, \ldots, a_n)$ be a sequence such that $\sum_{i=1}^n a_i = 2^t$. Let $a_i = b_{i0} + b_{i1}.2 + \cdots + b_{ik_i} 2^{k_i}$ be the binary expansion of a_i.

Now

$$R_A(n,t) = \sum_{i-1}^{n} \sum_{j=0}^{k} b_{ij}, \quad k = \max_i k_i\,.$$

and hence any sequence A such that $R_A(n,t) = R(n,t)$ has the property that the sequences $(b_{1j}, b_{2j}, \ldots, b_{nj})$ $j = 0, \ldots, k-1$, contain as many one's as possible. That is, $(b_{ij}, \ldots, b_{nj})$, $j = 0, \ldots, k-1$, contains at most one zero.

Now, we let the binary expansion of $n-1$ be $c_0 + c_1.2 + \cdots + c_m 2^m$ and consider the following $n \times (m+2)$ matrix:

$$X = \begin{bmatrix} 1 & 1 & \dots & 1 & 1 & c_0 \\ 2 & 2 & \dots & 2 & 2 & c_1.2 \\ \vdots & & & & & \vdots \\ 2^m & 2^m & \dots & 2^m & 2^m & c_m.2^m \\ 2^{m+1} & \dots & 2^{m+1} & 0 & \dots & 0 \end{bmatrix}$$

Let the number of 2^{m+1}'s in the last row be a. The sum S of all the entries in this matrix is:

$$\begin{aligned} S &= (n-1-a)\left(2^{m+1}-1\right) + a\left(2^{m+2}-1\right) + n - 1 \\ &= (n-1-a)\,2^{m+1} + a.2^{m+2} \\ &= 2^{m+1}\,(n-1+a)\,. \end{aligned}$$

Now $m = [\log_2(n-1)]$, and so when $n \neq 2^j + 1$ for some j, $n-1 \leq 2^{m+1} < 2(n-1)$. However, since $0 \leq a \leq n-1$, we can find an a such that $n-1+a = 2^{m+1}$; that is, $a = 2^{m+1} - n + 1$, and so

$$S = 2^{2m+2}\,.$$

We now consider the matrix Y, which is obtained from X by replacing all non-zero terms by 1, and define a sequence $A = \{a_i\}$ by letting row j of Y be $(b_{1j}, b_{2j}, \dots, b_{nj})$ and choosing

$$a_i = \sum_{j=0}^{m+1} b_{ij} 2^j\,.$$

It is obvious that the sequences $(b_{1j} \dots, b_{nj})$, $j = 0, \dots, m$, are as full as possible, and since

$$S = 2^{2m+2}$$

$$R_A(n, 2m+2) = R(n, 2m+2)\,. \tag{9.1}$$

But

$$R_A(n, 2m+2) = a + (n-1)(m+1) + B(n-1),$$

where $B(n-1)$ is the number of non-zero terms in the binary expansion of $n-1$.

Therefore,

$$R(n, 2m+2) = 2^{m+1} + (n-1)m + B(n-1)\,.$$

We now consider

$$R(n, 2m+3)\,.$$

From our choice of a, it can be seen that

$$(n-1-a)2^{m+2}+a.2^{m+3}=2^{2m+3}.$$

Therefore, to obtain an A such that $R_A(n,2m+3)=R(n,2m+3)$, we use the A of (9.1) and put $b_{a+1,m}=b_{a+2,m}=\ldots=b_{n-1,m}=1$, $b_{nm}=0$ and $b_{1,m+1}=b_{2,m+1}=b_{a,m+1}=1$. This produces sequences as full as possible, and therefore, $R(n,2m+3)=R(n,2m+2)+(n-1)$. We continue in this way to obtain the following:

$$R(n,2m+i)=2^{m+1}+B(n-1)+(n-1)(m+i-2),\text{ where } i=2,3,\ldots\ .$$

We note that if $n=2^m+1$, then

$$2^{2m}=(n-1)\,(2^m-1)+n-1\,.$$

So

$$R\,(2^m+1,2m)=2^m m+1\,.$$

The maximum number of steps in the algorithm of Figure 9.1 is $R(n,t)-(t+1)$. The actual number of steps for an n-tuple A is $p=R_A(n,t)-(t+1)\leq R(n,t)-(t+1)$. We have shown that $R(n,t)$ is finite and may be evaluated easily. □

9.5 Enough Powers of Two: Asymptotic Existence

Craigen [34], almost two decades later, using groups containing a distinguished central involution was able to greatly improve Seberry's results of Theorem 9.3. He was able to show that s could be upper bounded by $4\lceil\frac{1}{16}log_2(q-1)/2)\rceil+2$. The present bound is also due to Craigen. We do not give Craigen's proof as Craigen, Ghaderpour, Holzmann and Kharaghani [34,36,85,86] have proved results, given in the next section which include these results.

Theorem 9.11. *[34, 36]For any positive integer m there exists an Hadamard matrix*

(1) of order $2^{2b}q$, where b is the number of nonzero digits in the binary expansion of q, and
(2) of order $2^t q$ for $t=6\lfloor\frac{1}{16}log_2((m-1)/2)\rfloor+2$.

Craigen's theorem implies that there is an Hadamard matrix of order 2^s whenever $2^s\geq ct^a$, where we may take $a=\frac{3}{8}$ and $c=2^{\frac{26}{16}}$.

de Launey [143] looks at this issue from the perspective of the density of the existence of Hadamard matrices in the set of integers $4t$ and amazingly shows that this is greater than or equal to a half. This is further discussed in Section 9.7.

Seberry's and Craigen's asymptotic formulae for t in terms of q, versus the Hadamard conjecture is given in Figure 9.3.

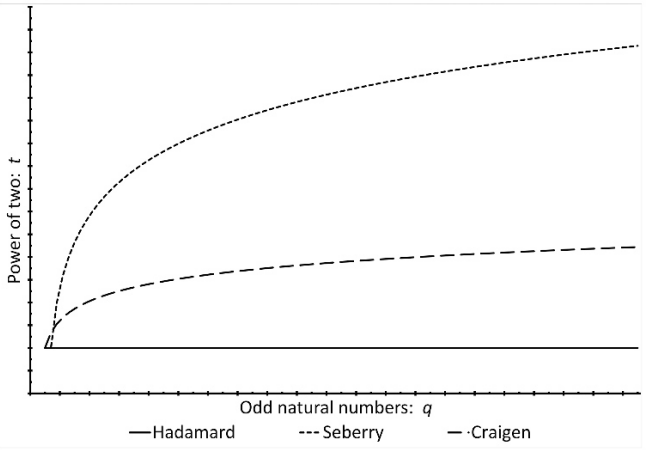


Fig. 10.3 Asymptotic support for the Hadamard Conjecture

The present situation can be summarized as

Theorem 9.12 (Asymptotic Hadamard matrix Theorem). *Let p be any integer then there exists a t_0 such that for all $t > t_0$ an Hadamard matrix of order $2^t p$ exists (Craigen-Seberry [183]).*

Theorem 9.13 (Craigen-Holzmann-Kharaghani [36]). *Let p be any integer then there exists a t_0 such that for all $t > t_0$ a complex Hadamard matrix of order $2^t p$ exists.*

Theorem 9.14. *Given any s-tuple $(p_1, p_2, \ldots, p_s)$ then there exists a t_0 such that for all $t > t_0$ an orthogonal design $OD(2^t p_1, 2^t p_2, \ldots, 2^t p_s)$ exists (Ghaderpour and Kharaghani [86], Craigen-Holzmann-Kharaghani [36], Eades [52]).*

Theorem 9.15 (Ghaderpour-Kharaghani [86]). *For any two sequences $(u_1, \ldots, u_p)$ and $(v_1, \ldots, v_q)$ of positive integers, there are integers h, h_1, h_2 and t_0 such that there exists an*

$$AOD\left(2^t h; 2^{t+h_1} u_1, \ldots, 2^{t+h_1} u_p; 2^{t+h_1} v_1, \ldots, 2^{t+h_1} v_q\right),$$

for each $t \geq t_0$.

Conjecture 9.3. Let p be any integer then there exists a t_0 such that for all $t > t_0$ a skew-Hadamard matrix of order $2^t p$ exists.

Conjecture 9.4. Let p be any integer then there exists a t_0 such that for all $t > t_0$ a symmetric Hadamard matrix of order $2^t p$ exists.

Conjecture 9.5. Let p be any integer then there exists a t_0 such that for all $t > t_0$ a pair of amicable Hadamard matrix of order $2^t p$ exists.

9.5.1 The Asymptotic Hadamard Existence Theorem

The following presentation is due to Ghaderpour and Kharaghani [86] and shows that with sufficient twos the asymptotic results are very accessible. The real question is how many two's are needed. Of course, for the Hadamard conjecture to hold, the number of twos must be 2 so we want matrices of order 2^2q to exist for odd q.

9.5.2 Ghaderpour and Kharaghani's Uber Asymptotic Results

We start with the following well-known result first used by Holzmann and Kharaghani [103].

Lemma 9.13. *For any positive integer n, there is a Golay pair of length 2^n in two type 1 matrices each appearing 2^{n-1} times in each of the sequences.*

Proof. Let A_{n-1} and B_{n-1} be a Golay pair of length 2^{n-1} in two type 1 matrices each appearing 2^{n-2} times in both A_{n-1} and B_{n-1}. Then $A_n = (A_{n-1}, B_{n-1})$ and $B_n = (A_{n-1}, -B_{n-1})$ form a Golay pair of length 2^n in two type 1 matrices as desired, where (A, B) means sequence A followed by sequence B. □

Theorem 9.16. *For any given sequence of positive integers $(b, a_1, a_2, \ldots, a_k)$, there exists a full COD of type $\left(2^{N(m)} \cdot 1_{(b)}, 2^{N(m)} \cdot 2^{a_1}_{(4)}, \ldots, 2^{N(m)} \cdot 2^{a_k}_{(4)}\right)$, where $m = 4k+b+2$ if b is even, $m = 4k+b+1$ if b is odd, and $N(m)$ is the smallest positive integer such that $m \le \rho\left(2^{N(m)-1}\right)$.*

Proof. Let $(b, a_1, a_2, \ldots, a_k)$ be a sequence of positive integers . We distinguish two cases:

Case 1. b is even. Consider the type 1 matrices x_i, $0 \le i \le \frac{b}{2}$, y_j and z_j. $1 \le j \le k$ of order 2. For each j, $1 \le j \le k$, let G_{j1} and G_{j2} be a Golay pair of length 2^{a_j} in two type 1 matrices y_j and z_j. Let

$$s_1 = 0 \text{ and } s_j = 2\sum_{r=1}^{j-1} 2^{a_r}, \quad 2 \le j \le k+1\,. \tag{9.2}$$

Let $d = \frac{b}{2} + s_{k+1}$ and define

$$\begin{aligned} M_0 &:= \operatorname{circ}\left(0_{(d)}, x_0, 0_{(d-1)}\right), \qquad M_1 := \operatorname{circ}\left(x_1, 0_{(2d-1)}\right), \\ M_h &:= \operatorname{circ}\left(0_{(h-1)}, x_h, 0_{(2d-h)}\right), \qquad 2 \le h \le \tfrac{b}{2}. \end{aligned} \tag{9.3}$$

For each j, $1 \le j \le k$, define

$$N_{2j-1} := \mathrm{circ}\left(0_{(\frac{b}{2}+s_j)}, G_{j1}, 0_{(2d-\frac{b}{2}-s_j-2^{a_j})}\right),$$

$$N_{2j} := \mathrm{circ}\left(0_{(\frac{b}{2}+s_j+2^{a_j})}, G_{j2}, 0_{(2d-\frac{b}{2}-s_j+1)}\right).$$

Considering that all the variables in these matrices are assumed to be type 1 matrices of order 2, these matrices are in fact commuting block-circulant matrices, and the 0 entries denote the zero matrix of order 2. Let $m = 4k+b+2$ and let $N(m)$ be the smallest positive integer such that $m \leq \rho\left(2^{N(m)-1}\right)$. So there is a set

$$A' = \{A_1, \ldots, A_m\} \tag{9.4}$$

of mutually disjoint anti-amicable signed permutation matrices of order $2^{N(m)-1}$. These matrices are known as Hurwitz-Radon matrices (see [80, chapter 1]). Suppose H is a Hadamard matrix of order $2^{N(m)-1}$. Let

$$\begin{aligned} C = {} & \tfrac{1}{2}\left(M_0 + M_0^\top\right) \otimes A_1 H + \tfrac{i}{2}\left(M_0 - M_0^\top\right) \otimes A_2 H \\ & + \tfrac{1}{2}\left(M_1 + M_1^\top\right) \otimes A_3 H + \tfrac{i}{2}\left(M_1 - M_1^\top\right) \otimes A_4 H \\ & + \sum_{h=2}^{\frac{b}{2}} \Big(\left(M_h + M_h^\top\right) \otimes \tfrac{1}{2}\left(A_{2h+1} + A_{2h+2}\right) H \\ & + i\left(M_h - M_h^\top\right) \otimes \tfrac{1}{2}\left(A_{2h+1} - A_{2h+2}\right) H \Big) \\ & + \sum_{j=1}^{2k} \Big(\left(N_j + N_j^\top\right) \otimes \tfrac{1}{2}\left(A_{2j+b+1} + A_{2j+b+2}\right) H \\ & + i\left(N_j - N_j^\top\right) \otimes \tfrac{1}{2}\left(A_{2j+b+1} - A_{2j+b+2}\right) H \Big). \end{aligned} \tag{9.5}$$

We show that

$$CC^* = 2^{N(m)} \omega I_{2^{n(m)}d}, \tag{9.6}$$

where $\omega = \frac{1}{2}x_0x_0^\top + \frac{1}{2}x_1x_1^\top + x_2x_2^\top + \cdots + x_{\frac{b}{2}}x_{\frac{b}{2}}^\top + 2^{a_1}y_1y_1^\top + 2^{a_1}z_1z_1^\top + \cdots + 2^{a_k}y_ky_k^\top + 2^{a_k}z_kz_k^\top$. To this end, we first note that each of the sets

$$\left\{\tfrac{1}{2}\left(M_0 + M_0^\top\right), \tfrac{i}{2}\left(M_0 - M_0^\top\right), \tfrac{1}{2}\left(M_1 + M_1^\top\right), \tfrac{i}{2}\left(M_1 - M_1^\top\right)\right\}$$

$$\left\{\left(M_h + M_h^\top\right), \left(N_j + N_j^\top\right), \quad 2 \leq h \leq \tfrac{b}{2}, \quad 1 \leq j \leq 2k\right\}$$

and

$$\left\{ i\left(M_h - M_h^\top\right), i\left(N_j - N_j^\top\right);\quad 2 \le h \le \tfrac{b}{2},\quad 1 \le j \le 2k \right\}$$

consist of mutually disjoint Hermitian circulant matrices. Moreover, for $u = 0, 1$, we have

$$\tfrac{1}{4}\left(M_u + M_u^\top\right)\left(M_u + M_u^\top\right)^\top + \tfrac{1}{4}\left(M_u - M_u^\top\right)\left(M_u - M_u^\top\right)^\top = x_u x_u^\top I_{2d}$$

and for each h, $2 <\le h \le \frac{b}{2}$,

$$\left(M_h + M_h^\top\right)\left(M_h + M_h^\top\right)^\top + \left(M_h - M_h^\top\right)\left(M_h - M_h^\top\right)^\top = 4x_h x_h^\top I_{2d}$$

Also, for each j, $1 \le j \le k$, we have

$$\begin{aligned}
&\sum_{r=2j-1}^{2j}\left(\left(N_r + N_r^\top\right)\left(N_r + N_r^\top\right)^\top + \left(N_r - N_r^\top\right)\left(N_r - N_r^\top\right)^\top\right) \\
&\qquad = 2\sum_{r=2j-1}^{2j}\left(N_r N_r^\top + N_r^\top N_r\right) \\
&\qquad = 2^{a_j+2}\left(y_j y_j^\top + z_j z_j^\top\right) I_{2d}\,.
\end{aligned}$$

Note that for each j, $3 \le j \le \frac{b}{2} + 2k + 1$, the matrices $\frac{1}{2}\left(A_{2j-1} + A_{2j}\right)H$ and $\frac{1}{2}\left(A_{2j-1} - A_{2j}\right)H$ are disjoint with $0, \pm 1$ entries. Furthermore, since the set A' consists of mutually anti-amicable matrices, the set

$$\left\{ A_1 H, A_2 H, A_3 H, A_4 H, \tfrac{1}{2}\left(A_{2j-1} \pm A_{2j}\right)H\,,\quad \text{for } \left(3 \le j \le \tfrac{b}{2} + 2k + 1\right) \right\}$$

consists of mutually anti-amicable matrices. Since for each j, $3 \le j \le \frac{b}{2} + 2k + 1$,

$$\begin{aligned}
&\left(\tfrac{1}{2}\left(A_{2j-1} \pm A_{2j}\right)H\right)\left(\tfrac{1}{2}\left(A_{2j-1} \pm A_{2j}\right)H\right)^\top \\
&\qquad = \tfrac{1}{4}\left(2^{N(m)-1}\right)\left(A_{2j-1} \pm A_{2j}\right)\left(A_{2j-1} \pm A_{2j}\right)^\top I_{2N(m)-1} \\
&\qquad = 2^{N(m)-2} I_{2N(m)-1}\,,
\end{aligned}$$

the validity of equation (9.6) follows.

In the equation (9.6), we now replace x_o by $\left[\begin{smallmatrix} \alpha & \alpha \\ -\alpha & \alpha \end{smallmatrix}\right]$, x_1 by $\left[\begin{smallmatrix} \beta & \beta \\ -\beta & \beta \end{smallmatrix}\right]$, x_h by $\left[\begin{smallmatrix} \alpha_h & \beta_h \\ -\beta_h & \alpha_h \end{smallmatrix}\right]$, $2 \le h \le \frac{b}{2}$, y_j by $\left[\begin{smallmatrix} \alpha'_j & \beta'_j \\ -\beta'_j & \alpha'_j \end{smallmatrix}\right]$, and z_j by $\left[\begin{smallmatrix} \alpha''_j & \beta''_j \\ -\beta''_j & \alpha''_j \end{smallmatrix}\right]$, $1 \le j \le k$.

The resultant matrix will be a full COD of type

$$\left(2^{N(m)} \cdot 1_{(b)}, 2^{N(m)} \cdot 2_4^{a_1}, \ldots, 2^{N(m)} \cdot 2_{(4)}^{a_k}\right),$$

where the α, β, α_h's, β_h's, α'_j's, β'_j's, α''_j's and β''_j's are commuting variables.

Case 2. b is odd. Consider the following circulant matrices of order $2d+1$, where $d = \frac{b-1}{2} + s_k + 1$ with the same s_j's as in equation (9.2),

$$M_1 = \mathrm{circ}\,(x_1, 0_{2d})\,,$$
$$M_h = \mathrm{circ}\,(0_{h-1}, x_h, 0_{2d-h+1})\,, \quad \text{for } 2 \le h \le \tfrac{b+1}{2}\,.$$

For each j, $1 \le j \le k$, assume

$$N_{2j-1} = \mathrm{circ}\left(0_{\left(\frac{b+1}{2}+s_j\right)}, G_{j1}, 0_{\left(2d-\frac{b+1}{2}-s_j-2^{a_j}\right)}\right),$$
$$N_{2j} = \mathrm{circ}\left(0_{\left(\frac{b+1}{2}+s_j+2^{a_j}\right)}, G_{j2}, 0_{\left(2d-\frac{b-1}{2}-s_j+1\right)}\right)$$

The rest of proof is similar to Case 1, and so $m = 4k+b+1$. □

Remark 9.1. The choice of $N(m)$ in Theorem 9.16 and the next few asymptotic results is crucial; the smaller $N(m)$, the better asymptotic result. All $N(m)$'s we use are either equal to or 1 less than the ceiling of $(m+2)/2$, depending on the value of m.

Let $(u_1, \ldots, u_\ell)$ be an ℓ-tuple of positive integers and suppose 2^t is the largest power of 2 appearing in the binary expansions of u_i, $i = 1, 2, \ldots \ell$. Using the binary expansion of each u, we write

$$\begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_\ell \end{bmatrix} = E \begin{bmatrix} 1 \\ 2 \\ \vdots \\ 2^t \end{bmatrix} \tag{9.7}$$

where $E = [e_{ij}]$ is the unique $\ell \times (t+1)$ matrix with 0 and 1 entries. We call E the *binary matrix* corresponding to the ℓ-tuple $(u_1, \ldots, u_\ell)$.

For convenience and in order to make the first column of the binary matrix E non-zero, in the following lemma, we assume that the ℓ-tuples of positive integers have at least one odd element.

Lemma 9.14. *Suppose that $(u_1, \ldots, u_\ell)$ is an ℓ-tuple of positive integers such that at least one of the u_i's is odd. Then there exists an integer $m = m(u_1, \ldots, u_\ell)$ such that there is a*

$$COD\,(2^m(u_1, \ldots, u_\ell); 2^m u_1, \ldots, 2^m u_\ell)\,.$$

Proof. Let $(u_1, \ldots, u_\ell)$ be an ℓ-tuple of positive integers such that at least one of u_i's is odd, and let $s = (u_1 + \cdots + u_\ell)$. By applying Theorem 9.16 all we need is to equate variables appropriately. We do this by applying the following procedure. We form the $\ell \times (t+1)$ binary matrix $E = [e_{ij}]$ corresponding to the ℓ-tuple $(u_1, \ldots, u_\ell)$, where t is the largest exponent appearing in the binary expansions of u_i, $i = 1, 2, \ldots, \ell$. Let

$$\gamma_{j-1} := \sum_{i=1}^{\ell} e_{ij}\,, \quad 1 \le j \le t+1\,. \tag{9.8}$$

$$k := t;\ \gamma'_t := \left\lfloor \frac{\gamma_t}{4} \right\rfloor\,; \quad (\lfloor x \rfloor \text{ is floor of } x) \tag{9.9}$$

$$\begin{aligned}
\text{while } k > 0 \quad & \beta_k := \gamma_k \pmod 4;\\
& k := k-1;\\
& \gamma_k := \gamma_k + 2\beta_{k+1};\\
\text{if } k \neq 0 \text{ then } \quad & \gamma'_k := \left\lfloor \frac{\gamma_t}{4} \right\rfloor;\\
\text{else} \quad & \gamma'_k := \gamma_k;
\end{aligned}$$

Now we apply Theorem 9.16 to the sequence $\left(\gamma'_0, 1_{(\gamma'_1)}, 2_{(\gamma'_2)}, \ldots, t_{(\gamma'_t)}\right)$. Thus, there is an integer m such that there is a

$$COD\left(2^m s; 2^m \cdot 1_{(\gamma'_0)}, 2^m \cdot 2_{(4\gamma'_1)}, 2^m \cdot 2^2_{(4\gamma'_2)}, \ldots, 2^m \cdot 2^t_{(4\gamma'_t)}\right), \tag{9.10}$$

where

$$m = N\left(4\sum_{j=1}^{t}\gamma'_j + \gamma'_0 + 2\right) \text{ if } \gamma'_0 \text{ is even, and}$$

$$m = N\left(4\sum_{j=1}^{t}\gamma'_j + \gamma'_0 + 1\right) \text{ if } \gamma'_0 \text{ is odd.}$$

Equating variables in (9.10) in an appropriate way, we obtain a

$$COD\,(2^m d; 2^m u_1, \ldots, 2^m u_\ell)\,.\square$$

Lemma 9.15. *For any ℓ-tuple $(s_1, \ldots, s_\ell)$ of positive integers, there is an integer $r = r(s_1, \ldots, s_\ell)$ such that there is a*

$$COD\,(2^r\,(s_1 + \cdots + s_\ell); 2^r s_1, \ldots, 2^r s_\ell)\,.$$

Proof. Suppose that $(s_1, \ldots, s_\ell)$ is an ℓ-tuple of positive integers and let

$$(s_1, \ldots, s_\ell) = 2^q (u_1, \ldots, u_\ell)\,,$$

where q is the unique integer such that one of u_i's is odd. By Lemma 9.14, there exists an integer $m = m(u_1, \ldots, u_\ell)$ such that there is a

$$COD\,(2^m(u_1 + \cdots + u_\ell); 2^m u_1, \ldots, 2^m u_\ell)\,;$$

Choose $r = m - q$, if $m \ge q$, and if $m < q$, then $A \otimes H$ is a

$$COD\left(2^q(u_1+\cdots+u_\ell);2^q u_1,\ldots,2^q u_\ell\right)=COD\left(s_1+\cdots+s_\ell;s_1\ldots,s_\ell\right),$$

where H is a Hadamard matrix of order 2^{q-m}, and therefore we may choose $r=0$ to complete the proof. □

Theorem 9.17. *For any ℓ-tuple $(s_1,\ldots,s_\ell)$ of positive integers, there is an integer $N=N(s_1,\ldots,s_\ell)$ such that for each $n\geq N$ there is an*

$$OD\left(2^n(s_1+\cdots+s_\ell);2^n s_1,\ldots,2^n s_\ell\right).$$

Proof. Let $(s_1,\ldots,s_\ell)$ be a ℓ-tuple of positive integers. From Lemma 9.14, there is an integer $r=r(s_1,\ldots,s_\ell)$ such that there is a

$$COD\left(2^r(s_1+\cdots+s_\ell);2^r s_1,\ldots,2^r s_\ell\right),$$

call it A. We may write $A=X+iY$, where X and Y are disjoint and amicable matrices such that $XX^\top+YY^\top=AA^*$. It can be seen that the matrix B,

$$B=\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\otimes X+\begin{bmatrix}-1 & 1\\ 1 & 1\end{bmatrix}\otimes Y$$

is an

$$OD\left(2^{r+1}(s_1+\cdots+s_\ell);2^{r+1}s_1,2^{r+1}s_2,\ldots,2^{r+1}s_\ell\right).$$

Let $N=r+1$, and H is a Hadamard matrix of order 2^{n-N}. Then $B\otimes H$ is an

$$OD\left(2^n(s_1+\cdots+s_\ell);2^n s_1,\ldots,2^n s_\ell\right).\square$$

Example 9.7. Consider the 5-tuple $(8,12,20,68,136)$. We may write this as $2^2(2,3,5,17,34)$. We apply the equation 9.7 to $(2,3,5,17,34)$ as follows:

$$\begin{bmatrix}2\\3\\5\\17\\34\end{bmatrix}=\begin{bmatrix}0&1&0&0&0&0\\1&1&0&0&0&0\\1&0&1&0&0&0\\1&0&0&0&1&0\\0&1&0&0&0&1\end{bmatrix}\begin{bmatrix}1\\2\\2^2\\2^3\\2^4\\2^5\end{bmatrix}$$

From the equation (9.8), we have $\gamma_0=3$, $\gamma_1=3$, $\gamma_2=1$, $\gamma_3=0$, $\gamma_4=1$, and $\gamma_5=1$. By applying the procedure (9.9), we find $\gamma'_0=5$, $\gamma'_1=1$, $\gamma'_2=1$, $\gamma'_3=1$, $\gamma'_4=0$ and $\gamma'_5=0$. So, we apply Theorem 9.16 to the sequence $(b,a_1,a_2,a_3)=(5,1,2,3)$. Since b is odd, we use Case 2 of the theorem, and so $m=4\times 3+5+1=18$. $N(18)=10$ as 10 is the smallest positive integer such that $18\leq\rho(2^{10-1})$. Thus there is a

$$COD\left(2^{10}\cdot 61;2^{10}\cdot 1_{(5)},2^{10}\cdot 2_{(4)},2^{10}\cdot 2^2_{(4)},2^{10}\cdot 2^3_{(4)}\right).$$

By equating variables, we obtain a

$$COD\left(2^8\cdot 244;\ 2^8\cdot 8, 2^8\cdot 12, 2^8\cdot 20, 2^8\cdot 68, 2^8\cdot 136\right).$$

Example 9.8. We apply the equation (9.7) to the 4-tuple $(1,5,7,17)$. Thus

$$\begin{bmatrix} 1 \\ 5 \\ 7 \\ 17 \end{bmatrix} = \begin{bmatrix} 1&0&0&0&0 \\ 1&0&1&0&0 \\ 1&1&1&0&0 \\ 1&0&0&0&1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 2^2 \\ 2^3 \\ 2^4 \end{bmatrix}$$

From (9.8) we have $\gamma_0 = 4$, $\gamma_1 = 1$, $\gamma_2 = 2$, $\gamma_3 = 0$, $\gamma_4 = 1$. By applying the procedure (9.9), we find $\gamma_0' = 6$, $\gamma_1' = 1$, $\gamma_2' = 1$, $\gamma_3' = 0$, $\gamma_4' = 0$. Now we apply Theorem 9.16 to the sequence $(b, a_1, a_2) = (6,1,2)$. Since b is even, we use Case 1 of Theorem 9.16, and so $m = 4\times 2+6+2 = 16$. $N(16) = 8$ as 8 is the smallest positive integer such that $16 \le \rho(2^{8-1})$. Thus there is a

$$COD\left(2^8\cdot 30; 2^8\cdot 1_{(6)}, 2^8\cdot 2_{(4)}, 2^8\cdot 2_{(4)}^2\right).$$

By equating variables, we obtain a

$$COD\left(2^8\cdot 30;\ 2^8\cdot 8, 2^8\cdot 1, 2^8\cdot 5, 2^8\cdot 7, 2^8\cdot 17\right).$$

9.6 The Asymptotic Existence of Amicable Orthogonal Designs

We now include an asymptotic result related to the amicable orthogonal designs due to Ghaderpour and Kharaghani [86, p.333-346].

Lemma 9.16. *If there exists an* $ACOD(n; u_1,\ldots,u_s; v_1,\ldots,v_t)$*, then there exists an*

$$AOD(2n; 2u_1,\ldots,2u_s; 2v_1,\ldots,2v_t).$$

Proof. Suppose that $(X;Y)$ is a complex amicable orthogonal design. We write $X = A+iB$ and $Y = C+iD$, where A and B (C and D) are disjoint and amicable matrices such that $AA^\top + BB^\top = XX^*$ and $CC^\top + DD^\top = YY^*$. Let $R = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ and $H = \left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right]$. Since $(X;Y)$ is a complex amicable orthogonal design,

$$AC^\top + BD^\top = CA^\top + DB^\top, \qquad AD^\top - BC^\top = CB^\top - DA^\top.$$

Let $X' = A\otimes RH + B\otimes H$ and $Y' = C\otimes RH + D\otimes H$. Then

$$X'Y'^\top = 2\left(AC^\top + BD^\top\right)\otimes I + 2\left(AD^\top - BC^\top\right)\otimes R$$
$$Y'^\top X' = 2\left(CA^\top + DB^\top\right)\otimes I + 2\left(CB^\top - DA^\top\right)\otimes R.$$

Therefore $(X';Y')$ is an amicable orthogonal design as desired. □

We are now ready for the main result of this section.

Theorem 9.18. *For any two sequences $(u_1,\dots,u_s)$ and $(v_1,\dots,v_t)$ of positive integers, there are integers h, h_1, h_2 and N such that there exists an*

$$AOD\left(2^n h; 2^{n+h_1}u_1,\dots,2^{n+h_1}u_s; 2^{n+h_2}v_1,\dots,2^{n+h_2}v_t\right),$$

for each $n \geq N$.

Proof. Suppose that $(u_1,\dots,u_s)$ and $(v_1,\dots,v_t)$ are two sequences of positive integers. Let $(u_1,\dots,u_s) = 2^{q_1}(u'_1,\dots,u'_s)$ and $(v_1,\dots,v_t) = 2^{q_2}(v'_1,\dots,v'_t)$, where q_1 and q_2 are the unique integers such that at least one of u_i's and one of v_j's is odd.

Let $u'_1+\cdots+u'_s = c_1$ and $v'_1+\cdots+v'_t = c_2$. We may use the procedure (9.9) in the proof of Lemma 9.14 for sequences $(u'_1,\dots,u'_s)$ and $(v'_1,\dots,v'_t)$ to get sequences $(b,a_1,a_2,\dots,a_k)$ and $(\beta,\alpha_l,\alpha_2,\dots,\alpha_\ell)$ of positive integers, respectively.

We have $c_1 = b+4\sum_{i=1}^{k}2^{a_i}$ and $c_2 = \beta+4\sum_{i=1}^{\ell}2^{\alpha_i}$. Without loss of generality we may assume that $c_1 \geq c_2$, and b and β are both even. Let $m = \max\{4k+b+2, 4\ell+\beta+2\}$.

Wolfe [247], continuing Shapiro's work [190], studied amicable and anti-amicable orthogonal designs in detail. The following construction will be needed later.

Theorem 9.19. *Given an integer $n = 2^s d$, where d is odd and $s \geq 1$, there exists two sets $A = \{A_1,\dots,A_{s+1}\}$ and $B = \{B_1,\dots,B_{s+1}\}$ of signed permutation matrices of order n such that*

(i) A consists of pairwise disjoint anti-amicable matrices,
(ii) B consists of pairwise disjoint anti-amicable matrices,
(iii) for each i and j, $A_iB_j^t = B_jA_1^\top$.

Proof. For each $2 \leq k \leq s+1$ let

$$A_1 = \left(\bigotimes_{i=1}^{s} P\right)\bigotimes I_d, \qquad A_k = \left(\bigotimes_{i=1}^{k-2} I\right)\bigotimes R\bigotimes\left(\bigotimes_{i=1}^{s} P\right)\bigotimes I_d$$

and

$$B_1 = \left(\bigotimes_{i=1}^{s} P\right)\bigotimes I_d, \qquad B_k = \left(\bigotimes_{i=1}^{k-2} I\right)\bigotimes Q\bigotimes\left(\bigotimes_{i=1}^{s} P\right)\bigotimes I_d$$

where $P = \left[\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right]$, $Q = \left[\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right]$, $R = \left[\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right]$, and I and I_d are the identity matrices of order 2 and d, respectively. Then the matrices A_i and B_i $(1 \leq i \leq s+1)$ satisfy the three properties *(i)*, *(ii)* and *(iii)*. □

Suppose that $A = \{A_1, \ldots, A_m\}$ and $B = \{B_1, \ldots, B_m\}$ are the same set of matrices of order 2^{m-1} as in Theorem 9.19.

Apply Theorem 9.16 to the sequence $(b, a_1, a_2, \ldots, a_k)$ by using the set A which contains matrices of order 2^{m-1} instead of the set A' in (9.4) which contains matrices of order $2^{N(m)-1}$. It can be seen that there is a COD, say C, of order $2^m c_1$ and type $\left(2^m \cdot 1_{(b)}, 2^m \cdot 2^{a_k}_{(4)}, \ldots, 2^m \cdot 2^{\alpha_\ell}_{(4)}\right)$.

Again apply Theorem 9.16 to the sequence $(\beta + c_1 - c_2, \alpha_1, \alpha_2, \ldots, \alpha_\ell)$ by using the set B instead of the set A' in (9.4). It can be seen that there is a COD, say D, of order $2^m c_1$ and type $\left(2^m \cdot 1_{(\beta)}, 2^m \cdot 2^{\alpha_1}_{(4)}, \ldots, 2^m \cdot 2^{\alpha_\ell}_{(4)}\right)$. Note that there is no need to use circulant matrices M_i's corresponding to the $c_1 - c_2$ variables to construct matrix D, and we do not necessarily need to use all matrices in sets A and B.

Since the circulant matrices used to construct C and D in (9.5) are Hermitian of order c_1 and $A_i B_j^\top = B_i A_i^\top$ for $1 \le i, j \le m$, $(C; D)$ is an

$$ACOD\left(2^m c_1; 2^m \cdot 1_{(b)}, 2^m \cdot 2^{a_k}_{(4)}; 2^m \cdot 1_{(\beta)}, 2^m \cdot 2^{\alpha_1}_{(4)}, \ldots, 2^m \cdot 2^{\alpha_\ell}_{(4)}\right).$$

Equating variables in C and D in an appropriate way, we obtain an

$$ACOD\left(2^m c_1; 2^m u'_1, \ldots, 2^m u'_s; 2^m v'_1, \ldots, 2^m v'_t\right),$$

and so by Lemma 9.16, there exists an

$$AOD\left(2^{m'} c_1; 2^{m'} u'_1, \ldots, 2^{m'} u'_s; 2^{m'} v'_1, \ldots, 2^{m'} v'_t\right), \tag{9.11}$$

where $m' = m + 1$.

Now if $q_1 = q_2 = 0$, then we choose $h = c_1$, $h_1 = h_2 = 0$ and $N = m'$. If $q_1 \le q_2 \le m'$, then we choose $h = c_1$, $h_1 = -q_1$, $h_2 = -q_2$ and $N = m'$. For cases $q_1 \le m' \le q_2$ and $m' \le q_1 \le q_2$, the Kronecker product of a Hadamard matrix of order $2^{q_2 - m'}$ with the amicable orthogonal design (9.11) implies $h = 2^{q_2} c_1$, $h_1 = q_2 - q_1$ and $h_2 = N = 0$. Therefore, there exists an

$$AOD\left(2^n h; 2^{n+h_1} u_1, \ldots, 2^{n+h_1} u_s; 2^{n+h_2} v_1, \ldots, 2^{n+h_2} v_t\right)$$

for each $n \ge N$.

If β and b are not both even, then we may use Case 2 in Theorem 9.16 with a similar argument. □

Example 9.9. Let $(u_1, u_2, u_3, u_4, u_5) = (8, 12, 20, 68, 136)$ and $(v_1, v_2, v_3, v_4) = (1, 5, 7, 17)$. We use the same notation as in the proof of Theorem 9.18. Thus, we have

$$\left(u_1', u_2', u_3', u_4', u_5'\right) = (2,3,5,17,34), \quad \left(v_1', v_2', v_3', v_4'\right) = (1,5,7,17),$$
$$q_1 = 2, \quad q_2 = 0, \quad c_1 = \sum_{i=1}^{5} u_i' = 61, \quad c_2 = \sum_{i=1}^{4} v_i' = 30 \text{ and } c_1 \geq c_2.$$

In Examples 9.7 and 9.8, we applied the procedure (9.9) to the sequences

$$\left(u_1', u_2', u_3', u_4', u_5'\right) = (2,3,5,17,34) \text{ and } \left(v_1', v_2', v_3', v_4'\right) = (1,5,7,17),$$

and we obtained the two sequences

$$(b, a_1, a_2, a_3) = (5,1,2,3) \text{ and } (\beta, \alpha_1, \alpha_2) = (6,1,2),$$

respectively. We may choose $m = \max\{4\cdot 3+b+1, 4\cdot 2+\beta+2\} = \max\{18,16\} = 18$. Note that b is odd, and β is even. From the proof of Theorem 9.18, there is an

$$ACOD\left(2^{18}\cdot 61; \right.$$
$$\left. 2^{18}\cdot 1_{(5)}, 2^{18}\cdot 2_{(4)}, 2^{18}\cdot 2_{(4)}^2, 2^{18}\cdot 2_{(4)}^3; 2^{18}\cdot 1_{(6)}, 2^{18}\cdot 2_{(4)}, 2^{18}\cdot 2_{(4)}^2\right),$$

and so there is an

$$AOD\left(2^{19}\cdot 61; \right.$$
$$\left. 2^{19}\cdot 1_{(5)}, 2^{19}\cdot 2_{(4)}, 2^{19}\cdot 2_{(4)}^2, 2^{19}\cdot 2_{(4)}^3; 2^{19}\cdot 1_{(6)}, 2^{19}\cdot 2_{(4)}, 2^{19}\cdot 2_{(4)}^2\right).$$

Equating variables, we obtain an

$$AOD\left(2^{19}\cdot 61; \right.$$
$$\left. 2^{19}\cdot 2, 2^{19}\cdot 3, 2^{19}\cdot 5, 2^{19}\cdot 17, 2^{19}\cdot 34; 2^{19}\cdot 1, 2^{19}\cdot 5, 2^{19}\cdot 7, 2^{19}\cdot 17\right).$$

Since $q_2 \leq q_1 \leq 19$, we choose $N = 19$, $h = 61$, $h_1 = -2$, $h_2 = 0$, and therefore for each $n \geq 19$, there exists an

$$AOD\left(2^n\cdot 61; \right.$$
$$\left. 2^{n-2}\cdot 8, 2^{n-2}\cdot 12, 2^{n-2}\cdot 20, 2^{n-2}\cdot 68, 2^{n-2}\cdot 136; 2^n\cdot 1, 2^n\cdot 5, 2^n\cdot 7, 2^n\cdot 17\right).$$

9.7 de Launey's Theorem

While it is conjectured that Hadamard matrices exist for all orders $4t$ $t > 0$, sustained effort over five decades only yielded a theorem of the type "that for all odd natural numbers q, there exists an Hadamard matrix of order $q^{2(a+blog_2 q)}$ where a and b are non-negative constants. To prove the Hadamard conjecture

it is necessary to show we may take $a = 2$ and $b = 0$. Seberry [237] showed that we may take $a = 0$ and $b = 2$. This was improved by Craigen [34], who showed that we may take $a = 0$ and $b = \frac{3}{8}$. Then astonishingly, de Launey [143, 145] showed, using a number theoretic argument of Erdos and Odlyzko [58], that there are enough Paley Hadamard matrices to ensure that for all $\epsilon > 0$, the set of odd numbers q for which there is an Hadamard matrix of order $q^{22+[\epsilon log_2 k]}$ has positive density in the natural numbers. It is beyond the scope of this book to prove this result but it is so important we have chosen to report it.

We give three important research questions posed by Warwick de Launey shortly before he died;

Problem 9.1 (Research Problem of de Launey). Improve the known results on the density of Hadamard matrices in the set of natural numbers. See Warwick de Launey and Daniel M.Gordon [144]

Problem 9.2 (Research Problem of de Launey). Improve the known bounds on the existence of partial Hadamard matrices See Warwick de Launey and David A. Levin [146].

Problem 9.3 (Research Problem). Improve the de Launey bound on the order of the power of two for the existence of an Hadamard matrix of order $2^t q$, q an odd natural number. See Warwick de Launey [143].

Problem 9.4 (Research Problem). Find asymptotic results for the existence of repeat designs.

Chapter 10
Complex, Quaternion and Non Square Orthogonal Designs

10.1 Introduction

A detailed study of complex, quaternion and non-square orthogonal designs is beyond the scope of this book. We give just a small taste to highlight the deep and practical nature of these almost unstudied algebraic structures.

A multiple antenna system has been used to solve bandwidth limitation and channel fading problems in a wireless communication system. Space-time block codes from real and complex orthogonal designs, have attracted considerable attention lately, since they can approach the potential huge capacity of multiple antenna systems and have a simple decoupled maximum-likelihood (ML) decoding scheme [208]. Space-time block codes have been adopted in the newly proposed standard for wireless LANs IEEE 802.11n [147]. Multi-path fading in a wireless channel can cause severe degradation of transmission performance. In order to overcome the fading problem, some diversity techniques are used, e.g. space-time coding scheme combines space diversity and time diversity. We expect that additional forms of diversity, i.e. polarization diversity and frequency diversity, should be considered with space and time diversity to improve capacity.

It has been shown that polarization diversity, together with other forms of diversity, can add to the performance improvements offered by other diversity techniques. Isaeva and Sarytchev [113] showed that the utilization of polarization diversity with other forms of diversity can be modelled by means of quaternions since two orthogonal complex constellations form a quaternion. This motivated the study of orthogonal designs over the quaternion domain for future applications in signal processing as space-time-polarization block codes [28, 60, 184, 257].

We give general construction techniques to build amicable orthogonal designs of quaternions, which we believe can be used for constructing quaternion orthogonal designs, just like the applications of amicable orthogonal de-

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5_10

signs(AODs) for complex space-time codes, e.g. our previous work in [186,212].

10.2 Complex orthogonal designs

Complex orthogonal design is a complex analog of orthogonal designs and was first studied by A.V. Geramita and J.M. Geramita in [76]. The coefficient matrices of complex orthogonal designs are over the complex domain and can be used in the study of complex weighing matrices.

Seberry and Adams [181] noted that quaternion orthogonal designs (QODs) were introduced as a mathematical construct with the potential for applications in wireless communications. The potential applications require new methods for constructing QODs, as most of the known methods of construction do not produce QODs with the exact properties required for implementation in wireless systems. Real amicable orthogonal designs and the Kronecker product may be used to construct new families of QODs. Their Amicable-Kronecker Construction can be applied to build quaternion orthogonal designs of a variety of sizes and types. Although it has not yet been simulated whether the resulting designs are useful for applications, their properties look promising for the desired implementations. Furthermore, the construction itself is interesting because it uses a simple family of real amicable orthogonal designs and the Kronecker product as building blocks, opening the door for future construction algorithms using other families of amicable designs and other matrix products.

The exposition of the bulk of this chapter is due to Zhao, Seberry, Xia, Wysocki, Wysocki [257], Chun Le Tran [186, 212], and Sarah Spence Adams [2, 181, 184, 185].

There are many possible definitions for COD. Signal processing encourages us to consider matrices with complex entries $a+\boldsymbol{i}b$, rather than a and/or $\boldsymbol{i}b$, a, b real.

Definition 10.1. A *complex orthogonal design*, *COD*, of order n and type $(s_1, s_2, \ldots, s_u)$, denoted $COD(n; s_1,\ s_2, \ldots, s_u)$, is an $n \times n$ matrix A with entries in the set of complex variables $y_i + \boldsymbol{i}z_i$ where y_i, z_i are in the set of real commuting variables $x_1, x_2, \ldots, x_u$ satisfying

$$A^H A = AA^H = \left(\sum_{h=1}^{u} s_h x_h^2 \right) I_n,$$

where $(.)^H$ denotes the Hermitian transpose. We note this is a different definition of *COD* from that which we have previously used.

Example 10.1. The matrix $\begin{bmatrix} \boldsymbol{i}x_1 & x_2 \\ x_2 & \boldsymbol{i}x_1 \end{bmatrix}$, where x_1 and x_2 are real commuting variables, is a $COD(2; 1, 1)$.

In [254], Yuen, Guan and Tjhung defined an amicable complex orthogonal design which is a complex extension of amicable orthogonal design.

Definition 10.2. Two complex orthogonal designs, A and B, with complex coefficient matrices, are said to be *amicable* if $AB^H = BA^H$ or $A^HB = B^HA$. We write $ACOD(n; w_1, w_2, \ldots, w_u; z_1, z_2, \ldots, z_v)$ to denote that two designs $COD(n; w_1, w_2, \ldots, w_u)$ and $COD(n; z_1, z_2, \ldots, z_v)$ are *complex amicable*.

Example 10.2. Let $A = \left[\begin{smallmatrix} a & b \\ -\boldsymbol{i}b & \boldsymbol{i}a \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} c & d \\ \boldsymbol{i}d & -\boldsymbol{i}c \end{smallmatrix}\right]$, where $a, b, c, d \in \mathbb{R}$. A and B are amicable complex orthogonal designs $ACOD(2; 1, 1; 1, 1)$.

Yuen et al [254] also concluded that the maximum total number of variables of an ACOD is equal to the maximum total number of variables in an AOD of same order.

10.3 Amicable orthogonal designs of quaternions

Definition 10.3. A *quaternion variable* $\mathbf{a}$ is defined in the form $\boldsymbol{a} = a_1 + a_2\boldsymbol{i} + a_3\boldsymbol{j} + a_4\boldsymbol{k}$, where a_p, $p = 1, \ldots, 4$ are real numbers and the elements $\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$ satisfy $\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = \boldsymbol{ijk} = -1$.

A quaternion variable is a non-commutative extension of the complex variables since we can also write $\boldsymbol{a} = (a_1 + a_2\boldsymbol{i}) + (a_3 + a_4\boldsymbol{i})\boldsymbol{j}$.

The *quaternion conjugate* is given by $\boldsymbol{a}^Q = a_1 - a_2\boldsymbol{i} - a_3\boldsymbol{j} - a_4\boldsymbol{k}$.

The *quaternion norm* is therefore defined by

$$\sqrt{\boldsymbol{a}\boldsymbol{a}^Q} = \sqrt{a_1^2 + a_2^2 + a_3^2 + a_4^2}.$$

Given a matrix $A = (\boldsymbol{a}_{\ell,m})$, where $\boldsymbol{a}_u$ are quaternion variables or numbers, we define its *quaternion transform* by $A^Q = (\boldsymbol{a}^Q_{m,\ell})$.

The following definitions of orthogonal design of quaternions and restricted quaternion orthogonal design were originally given in [184].

Definition 10.4. An *orthogonal design of quaternions*, ODQ, of order n and type $(s_1, s_2, \ldots, s_u)$ denoted $ODQ(n; s_1, s_2, \ldots, s_u)$, on the commuting real variables $x_1, x_2, \ldots, x_u$ is a square matrix A of order n with entries from $\{0, \boldsymbol{q}_1x_1, \boldsymbol{q}_2x_2, \ldots, \boldsymbol{q}_ux_u\}$, where each $\boldsymbol{q}_j \in \{\pm\mathbf{1}, \pm\boldsymbol{i}, \pm\boldsymbol{j}, \pm\boldsymbol{k}\}$ such that

$$A^QA = AA^Q = \left(\sum_{h=1}^{u} s_hx_h^2\right) I_n\,,$$

where $(.)^Q$ denotes quaternion transform. We can extend this definition to include *rectangular* designs that satisfy

$$A^Q A = \left(\sum_{h=1}^{u} s_h x_h^2 \right) I_n .$$

Example 10.3. Consider $A = \begin{bmatrix} -x_1 & x_2\boldsymbol{i} \\ -x_2\boldsymbol{j} & x_1\boldsymbol{k} \end{bmatrix}$, where x_1, x_2 are real, commuting variables. Then,

$$\begin{aligned} A^Q A &= \begin{bmatrix} -x_1 & x_2\boldsymbol{j} \\ -x_2\boldsymbol{i} & -x_1\boldsymbol{k} \end{bmatrix} \quad \begin{bmatrix} -x_1 & x_2\boldsymbol{i} \\ -x_2\boldsymbol{j} & x_1\boldsymbol{k} \end{bmatrix} \\ &= \begin{bmatrix} x_1^2 + x_2^2 & 0 \\ 0 & x_1^2 + x_2^2 \end{bmatrix} \end{aligned}$$

so A is an $ODQ(2;1,1)$.

Definition 10.5. A *restricted quaternion orthogonal design* of order n and type $(s_1, s_2, \ldots, s_u)$, denoted $RQOD(n; s_1, s_2, \ldots, s_u)$, on the complex variables z_1, z_2, …, z_u is an $n \times n$ matrix A with entries from $\{0, \boldsymbol{q}_1 z_1, \boldsymbol{q}_1 z_1^*, \boldsymbol{q}_2 z_2, \boldsymbol{q}_2 z_2^*, \ldots, \boldsymbol{q}_u z_u, \boldsymbol{q}_u z_u^*\}$, where each $\boldsymbol{q}_p$ is a linear combination of $\{\pm\mathbf{1}, \pm\boldsymbol{i}, \pm\boldsymbol{j}, \pm\boldsymbol{k}\}$ such that

$$A^Q A = A A^Q = \left(\sum_{h=1}^{u} s_h |z_h|^2 \right) I_n .$$

This definition can be extended to include *rectangular* designs that satisfy $A^Q A = (\sum_{h=1}^{u} s_h |z_h|^2) I_n$.

Example 10.4. Consider $A = \begin{bmatrix} \boldsymbol{i}z_1 & \boldsymbol{i}z_2 \\ -\boldsymbol{j}z_2^* & \boldsymbol{j}z_1^* \end{bmatrix}$, where z_1, z_2 are complex commuting variables. Then,

$$\begin{aligned} A^Q A &= \begin{bmatrix} -z_1^*\boldsymbol{i} & z_2\boldsymbol{j} \\ -z_2^*\boldsymbol{i} & -z_1\boldsymbol{j} \end{bmatrix} \quad \begin{bmatrix} \boldsymbol{i}z_1 & \boldsymbol{i}z_2 \\ -\boldsymbol{j}z_2^* & \boldsymbol{j}z_1^* \end{bmatrix} \\ &= \begin{bmatrix} |z_1|^2 + |z_2|^2 & 0 \\ 0 & |z_1|^2 + |z_2|^2 \end{bmatrix} \end{aligned}$$

so A is an $RQOD(2;1,1)$. To illustrate why this is called a *restricted* QOD, we replace complex variables in A using $z_i = x_i + y_i\boldsymbol{i}$, where the x_i, y_i are real variables. This gives

$$A = \begin{bmatrix} -y_1 + \boldsymbol{i}x_1 & -y_2 + \boldsymbol{i}x_2 \\ -\boldsymbol{j}x_2 - \boldsymbol{k}y_2 & \boldsymbol{j}x_1 + \boldsymbol{k}y_1 \end{bmatrix} .$$

We now can see that the entries of A are quaternion variables such that certain components of the variables are *restricted* to zero.

Definition 10.6. Two orthogonal designs of quaternions, A and B, are said to be *amicable* if $AB^Q = BA^Q$ or $A^Q B = B^Q A$. We write

$$AODQ(n;w_1,w_2,\ldots,w_u;z_1,z_2,\ldots,z_v)$$

to denote that two designs $ODQ(n;w_1,w_2,\ldots,w_u)$ and $ODQ(n;z_1,z_2,\ldots,z_v)$ are amicable.

Example 10.5. Let

$$A=\begin{bmatrix} -x_1 & x_2\boldsymbol{i} \\ -x_2\boldsymbol{j} & x_1\boldsymbol{k}\end{bmatrix} \text{ and } B=\begin{bmatrix} y_1 & y_2\boldsymbol{i} \\ y_2\boldsymbol{j} & y_1\boldsymbol{k}\end{bmatrix}$$

where $x_1,x_2,x_3,x_4\in\mathbb{R}$. A and B are amicable orthogonal designs of quaternions of type $AODQ(2;1,1;1,1)$.

Proof. The proof that A and B are orthogonal designs of quaternions is straight-forward. We show A and B are amicable.

$$\begin{aligned} AB^Q &= \begin{bmatrix} -x_1 & x_2\boldsymbol{i} \\ -x_2\boldsymbol{j} & x_1\boldsymbol{k}\end{bmatrix}\quad\begin{bmatrix} y_1 & -y_2\boldsymbol{j} \\ -y_2\boldsymbol{i} & -y_1\boldsymbol{k}\end{bmatrix} \\ &= \begin{bmatrix} -x_1y_1+x_2y_2 & x_1y_2\boldsymbol{j}+x_2y_1\boldsymbol{j} \\ -x_2y_1\boldsymbol{j}-x_1y_2\boldsymbol{j} & -x_2y_2+x_1y_1\end{bmatrix} \\ BA^Q &= \begin{bmatrix} y_1 & y_2\boldsymbol{i} \\ y_2\boldsymbol{j} & y_1\boldsymbol{k}\end{bmatrix}\quad\begin{bmatrix} -x_1 & x_2\boldsymbol{j} \\ -x_2\boldsymbol{i} & -x_1\boldsymbol{k}\end{bmatrix} \\ &= \begin{bmatrix} -x_1y_1+x_2y_2 & x_1y_2\boldsymbol{j}+x_2y_1\boldsymbol{j} \\ -x_2y_1\boldsymbol{j}-x_1y_2\boldsymbol{j} & -x_2y_2+x_1y_1\end{bmatrix} \\ &= AB^Q \end{aligned}$$

Hence A and B are amicable orthogonal designs of quaternions. □

Let X and Y be amicable orthogonal designs of quaternions of type $AODQ(n;u_1,\ldots,u_s;v_1,\ldots,v_t)$. Write

$$X=\sum_{i=1}^{s}A_ix_i\,,\quad Y=\sum_{j=1}^{t}B_jy_j\,,$$

we then have:

(i) $A_i*A_\ell=0,\quad 1\le i\ne\ell\le s;$
$B_j*B_k=0,\quad 1\le j\ne k\le t;$
(ii) $A_iA_i^Q=u_iI_n,\quad 1\le i\le s;$
$B_jB_j^Q=v_jI_n,\ 1\le j\le t;$
(iii) $A_iA_\ell^Q+A_\ell A_i^Q=0,\quad 1\le i\ne\ell\le s;$
$B_jB_k^Q+B_kB_j^Q=0,\quad 1\le j\ne k\le t;$
(iv) $A_iB_j^Q=B_jA_i^Q,\quad 1\le i\le s,\ 1\le j\le t,$

where A_i, B_j are all $\{0, \pm 1, \pm i, \pm j, \pm k\}$ quaternion matrices. It is clear that conditions (i)–(iv) are necessary and sufficient for the existence of amicable orthogonal designs of quaternions $AODQ(n; u_1, \ldots, u_s; v_1, \ldots, v_t)$.

Problem 10.1 (Research Problem 4). Investigate the algebra which corresponds to the properties (i), (ii), (iii) and (iv) of the proof of Example 10.5.

Proposition 10.1. *A necessary and sufficient condition that there exist amicable orthogonal designs of quaternions X and Y of type $AODQ(n; u_1, \ldots, u_s; v_1, \ldots, v_t)$ is that there exists a family of matrices of $\{A_1, \ldots, A_s; B_1, \ldots, B_t\}$ of order n satisfying (i)–(iv) above.*

Proof. Let X and Y be such an amicable pair and write $X = A_1x_1 + \cdots + A_sx_s$ and $Y = B_1y_1 + \cdots + B_ty_t$ as linear monomials in the $x_i, y_i \in \mathbb{R}$. By definition, the proof of (i) and (ii) is straight-forward. Since we have

$$\begin{aligned} XX^Q &= (A_1x_1 + \cdots + A_sx_s)(A_1^Qx_1 + \cdots + A_s^Qx_s) \\ &= \sum_{j=1}^{s} \left(A_jA_j^Qx_j^2 \right) + \sum_{j \neq k} \left(A_jA_k^Q + A_kA_j^Q \right) x_jx_k \\ &= \left(\sum_{j=1}^{s} u_jx_j^2 \right) I_n, \end{aligned}$$

hence, conditions in (iii) are satisfied. Condition (iv) can be proved by comparing coefficient matrices of $XY^Q = YX^Q$ on both sides. Conversely, if we have $\{A_1, \ldots, A_s; B_1, \ldots, B_t\}$ of order n satisfying (i)–(iv), then it is obvious that $X = A_1x_1 + \cdots + A_sx_s$ and $Y = B_1y_1 + \cdots + B_ty_t$ are an AODQ with required type. □

Definition 10.7. An *amicable family of quaternions*(AFQ) of type $(u_1, \ldots, u_s; v_1, \ldots, v_t)$ in order n is a collection of quaternion matrices $\{A_1, \ldots A_s; B_1, \ldots, B_t\}$ satisfying (ii), (iii), (iv) above.

The definition of amicable family of quaternions(AFQ) is analogous to the definition of amicable family of orthogonal designs given in [80]. However, the upper bound on the total number of variables of an AODQ, i.e. $s+t$, is an unsolved problem.

10.4 Construction techniques

In this section, we present several construction techniques for building amicable orthogonal designs over the real and quaternion domain. There are some existing methods for generating real amicable orthogonal designs. We can

extend these techniques to build designs over the quaternion domain. However, due to the non-commutativity of the quaternions, we need to modify existing techniques to make them suitable for designs over the quaternion domain.

10.4.1 Amicable orthogonal designs

We recall from Chapter 5:

Definition 10.8. A symmetric conference matrix N of order n is a square $(0,1,-1)$ matrix satisfying $N = N^T$ and $NN^T = (n-1)I_n$. It is shown in [39] that if such a matrix exists, one may assume it has zero diagonal.

A symmetric conference matrix is a special type of weighing matrix which has been long studied in order to design experiments to weight n objects whose weights are small compared with the weights of the moving parts of the balance being used [80]. In Chapter 5 we have studied the application of symmetric conference matrices for constructing amicable orthogonal designs.

Lemma 10.1. *Let N be a symmetric conference matrix in order n and x, y real commuting variables. Then there is a complex orthogonal design $COD(n;1,n-1)$.*

Proof. Let $Y = xI_n\boldsymbol{i} + yN$; then Y is easily proved to be the required COD. □

Lemma 10.2 below improves results of Theorem 2 given in [177].

Lemma 10.2. *Let N be a symmetric conference matrix in order n. Then there exist pairs of amicable orthogonal designs:*

a) $AOD(2n;n,n;n,n)$,
b) $AOD(2n;n,n;2,2(n-1))$,
c) $AOD(2n;n,n;1,n-1)$,
d) $AOD(2n;2,2(n-1);1,n-1)$.

Proof. Let a, b, c and d be real commuting variables. Then the required designs are:

$$\text{for a)} \begin{bmatrix} aI_n+bN & bI_n-aN \\ bI_n-aN & -aI_n-bN \end{bmatrix} \text{ and } \begin{bmatrix} cI_n+dN & dI_n-cN \\ -dI_n+cN & cI_n+dN \end{bmatrix},$$

$$\text{for b)} \begin{bmatrix} aI_n+bN & bI_n-aN \\ bI_n-aN & -aI_n-bN \end{bmatrix} \text{ and } \begin{bmatrix} cI_n+dN & cI_n-dN \\ -cI_n+dN & cI_n+dN \end{bmatrix},$$

$$\text{for c)} \begin{bmatrix} aI_n+bN & bI_n-aN \\ bI_n-aN & -aI_n-bN \end{bmatrix} \text{ and } \begin{bmatrix} cI_n & dN \\ -dN & cI_n \end{bmatrix},$$

$$\text{for d)} \begin{bmatrix} aI_n+bN & aI_n-bN \\ aI_n-bN & -aI_n-bN \end{bmatrix} \text{ and } \begin{bmatrix} cI_n & dN \\ -dN & cI_n \end{bmatrix}. \square$$

Corollary 10.1. *Let n be the order of the symmetric conference matrices, we then have a number of amicable orthogonal designs of order $2n$ of different types. For example, for $n-1 \equiv 1 \pmod 4$, where $n-1$ is a prime power, there exist*

a) $AOD(2n;n,n;n,n)$,
b) $AOD(2n;n,n;2,2(n-1))$,
c) $AOD(2n;n,n;1,n-1)$,
d) $AOD(2n;2,2(n-1);1,n-1)$.

Example 10.6. For $n=6$ and $n=10$, there exist

a) $AOD(12;6,6;6,6)$, a') $AOD(20;10,10;10,10)$,
b) $AOD(12;6,6;2,10)$, b') $AOD(20;10,10;2,18)$,
c) $AOD(12;6,6;1,5)$, c') $AOD(20;10,10;1,9)$,
d) $AOD(12;2,10;1,5)$, d') $AOD(20;2,18;1,9)$,

separately.

We recall the oft quoted:

Lemma 10.3. *For $p \equiv 3 \pmod 4$ be a prime power. Then there exists a pair of amicable orthogonal designs $AOD(p+1;1,p;1,p)$.*

Proof. Almost straightforward verification since $aI+bS$ is type 1 and $(cI+dS)R$ is type 2 matrix. □

Example 10.7. For $p=3$, we define type 1 matrix $S = \left[\begin{smallmatrix} 0 & 1 & - \\ - & 0 & 1 \\ 1 & - & 0 \end{smallmatrix}\right]$ and the back diagonal matrix $R = \left[\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{smallmatrix}\right]$. Then, we construct

$$A = \begin{bmatrix} a & b & b & b \\ -b & a & b & -b \\ -b & -b & a & b \\ -b & b & -b & a \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} -c & d & d & d \\ d & -d & d & c \\ d & d & c & -d \\ d & c & -d & d \end{bmatrix}.$$

A and B is a pair of amicable orthogonal design $AOD(4;1,3;1,3)$.

10.5 Amicable orthogonal design of quaternions

Theorem 10.1. *If there exists a pair of amicable orthogonal designs of quaternions, $AODQ(n;a_1,\cdots,a_s;b_1,\cdots,b_t)$ and a pair of amicable orthogonal designs $AOD(m;c_1,\cdots,c_u;d_1,\cdots,d_v)$, then there exists a pair of amicable orthogonal designs of quaternions*
$AODQ(nm;b_1c_1,\ldots,b_1c_{u-1},a_1c_u,\ldots,a_sc_u;b_1d_1,\ldots,b_1d_v,b_2c_u,\ldots,b_tc_u)$.

Proof. Let $X = \sum_{i=1}^{s} A_i x_i$ and $Y = \sum_{j=1}^{t} B_j y_j$ be the amicable orthogonal designs of quaternions in order n and let $Z = \sum_{k=1}^{u} C_k z_k$ and $W = \sum_{l=1}^{v} D_l w_l$ be the amicable orthogonal designs in order m.
Construct the matrices

$$P = \sum_{i=1}^{u-1} (B_1 \otimes C_i)\, p_i + \sum_{j=1}^{s} (A_j \otimes C_u)\, p_{j+u-1}$$
$$Q = \sum_{i=1}^{v} (B_1 \otimes D_i)\, q_i + \sum_{j=2}^{t} (B_j \otimes C_u)\, q_{j+v-1}$$

where the p_i's and q_i's are real commuting variables and $\otimes$ denotes Kronecker product. □

The above theorem is similar to Wolfe's theorem [247] which gave a general construction method for amicable orthogonal designs. The only change in Theorem 10.1 is that X and Y are amicable orthogonal designs of quaternions (AODQ). It is important to note that Z and W must be amicable orthogonal designs over the **real** domain, otherwise the non-commutative property of quaternions can not guarantee the amicability of the results.

Example 10.8. Let $A = \begin{bmatrix} -x_1 & x_2\boldsymbol{i} \\ -x_2\boldsymbol{j} & x_1\boldsymbol{k} \end{bmatrix}$ and $B = \begin{bmatrix} y_1 & y_2\boldsymbol{i} \\ y_2\boldsymbol{j} & y_1\boldsymbol{k} \end{bmatrix}$, where $x_1, x_2, y_1, y_2 \in \mathbb{R}$. A and B are amicable orthogonal designs of quaternions $AODQ(2;1,1;1,1)$. Another pair of amicable orthogonal designs is given as $Z = \begin{bmatrix} z_1 & z_2 \\ -z_2 & z_1 \end{bmatrix}$ and $W = \begin{bmatrix} w_1 & w_2 \\ w_2 & -w_1 \end{bmatrix}$, where $z_1, z_2, w_1, w_2 \in \mathbb{R}$. Theorem 10.1 gives

$$P = (B_1 \otimes C_1)p_1 + (A_1 \otimes C_2)p_2 + (A_2 \otimes C_2)p_3\,,$$
$$Q = (B_1 \otimes D_1)q_1 + (B_1 \otimes D_2)q_2 + (B_2 \otimes C_2)q_3\,.$$

The quaternion coefficient matrices for P and Q are:

$$P_1 = B_1 \otimes C_1 = \begin{bmatrix} 1 & 0 \\ 0 & \boldsymbol{k} \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \boldsymbol{k} & 0 \\ 0 & 0 & 0 & \boldsymbol{k} \end{bmatrix},$$

$$P_2 = A_1 \otimes C_2 = \begin{bmatrix} -1 & 0 \\ 0 & \boldsymbol{k} \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$
$$= \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \boldsymbol{k} \\ 0 & 0 & -\boldsymbol{k} & 0 \end{bmatrix},$$

$$P_3 = A_2 \otimes C_2 = \begin{bmatrix} 0 & \boldsymbol{i} \\ -\boldsymbol{j} & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 0 & \boldsymbol{i} \\ 0 & 0 & -\boldsymbol{i} & 0 \\ 0 & -\boldsymbol{j} & 0 & 0 \\ \boldsymbol{j} & 0 & 0 & 0 \end{bmatrix},$$

$$Q_1 = B_1 \otimes D_1 = \begin{bmatrix} 1 & 0 \\ 0 & \boldsymbol{k} \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & \boldsymbol{k} & 0 \\ 0 & 0 & 0 & -\boldsymbol{k} \end{bmatrix},$$

$$Q_2 = B_1 \otimes D_2 = \begin{bmatrix} 1 & 0 \\ 0 & \boldsymbol{k} \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \boldsymbol{k} \\ 0 & 0 & \boldsymbol{k} & 0 \end{bmatrix},$$

$$Q_3 = B_2 \otimes C_2 = \begin{bmatrix} 0 & \boldsymbol{i} \\ \boldsymbol{j} & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 0 & \boldsymbol{i} \\ 0 & 0 & -\boldsymbol{i} & 0 \\ 0 & \boldsymbol{j} & 0 & 0 \\ -\boldsymbol{j} & 0 & 0 & 0 \end{bmatrix}.$$

Then

$$P = \begin{bmatrix} p_1 & -p_2 & 0 & p_3\boldsymbol{i} \\ p_2 & p_1 & -p_3\boldsymbol{i} & 0 \\ 0 & -p_3\boldsymbol{j} & p_1\boldsymbol{k} & p_2\boldsymbol{k} \\ p_3\boldsymbol{j} & 0 & -p_2\boldsymbol{k} & p_1\boldsymbol{k} \end{bmatrix} \quad \text{and} \quad Q = \begin{bmatrix} q_1 & q_2 & 0 & q_3\boldsymbol{i} \\ q_2 & -q_1 & -q_3\boldsymbol{i} & 0 \\ 0 & q_3\boldsymbol{j} & q_1\boldsymbol{k} & q_2\boldsymbol{k} \\ -q_3\boldsymbol{j} & 0 & q_2\boldsymbol{k} & -q_1\boldsymbol{k} \end{bmatrix}$$

are are amicable orthogonal designs of quaternions $AODQ(4;1,1,1;1,1,1)$ since they both are ODQs and satisfy $PQ^Q = QP^Q$.

Corollary 10.2. *If there exists a pair of amicable orthogonal designs of quaternions $AODQ(n;a_1,...,a_s;b_1,...,b_t)$, then there exists a pair of amicable orthogonal designs of quaternions of type*

a) $AODQ(2n;a_1,a_1,2a_2...,2a_s;2b_1,...,2b_t)$,
b) $AODQ(2n;a_1,a_1,a_2...,a_s;b_1,...,b_t)$.

Proof. Let $X = \sum_{i=1}^{s} A_i x_i$ and $Y = \sum_{j=1}^{t} B_j y_j$ be amicable designs of quaternions in order n.
a) Let $M = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$, $N = \left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right]$ be **real** weighing matrices and construct the matrices

$$P = (A_1 \otimes I_2)\, p_1 + (A_1 \otimes M)\, p_2 + \sum_{i=2}^{s} (A_i \otimes N)\, p_{i+1}$$

and

$$Q = \sum_{j=1}^{t} (B_j \otimes N)\, q_j$$

b) Same as a), only set $N = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

It's obvious that all the quaternion matrices P_i's and Q_i's satisfy the conditions (i)-(iv) because the weighing matrices M, N have the following properties: $M = -M^\top$, $N = N^\top$, and $MN^\top = NM^\top$, where $(.)^\top$ denotes matrix transpose. □

Example 10.9. Consider a pair of $AODQ(2;1,1;1,1)$ given in Example 10.5, we construct a new $AODQ(4;1,1,2;2,2)$ using Corollary 10.2(a):

$$P = \begin{bmatrix} -p_1 & -p_2 & p_3\boldsymbol{i} & p_3\boldsymbol{i} \\ p_2 & -p_1 & p_3\boldsymbol{i} & -p_3\boldsymbol{i} \\ -p_3\boldsymbol{j} & -p_3\boldsymbol{j} & p_1\boldsymbol{k} & p_2\boldsymbol{k} \\ -p_3\boldsymbol{j} & p_3\boldsymbol{j} & -p_2\boldsymbol{k} & p_1\boldsymbol{k} \end{bmatrix} \quad Q = \begin{bmatrix} q_1 & q_1 & q_2\boldsymbol{i} & q_2\boldsymbol{i} \\ q_1 & -q_1 & q_2\boldsymbol{i} & -q_2\boldsymbol{i} \\ q_2\boldsymbol{j} & q_2\boldsymbol{j} & q_1\boldsymbol{k} & q_1\boldsymbol{k} \\ q_2\boldsymbol{j} & -q_2\boldsymbol{j} & q_1\boldsymbol{k} & -q_1\boldsymbol{k} \end{bmatrix}$$

In Theorem 10.1, we can also replace the amicable orthogonal designs $AOD(m;c_1,\ldots,c_u;d_1,\ldots,d_v)$ by an amicable family to get more amicable orthogonal designs of quaternions.

Example 10.10. Consider a pair of $AODQ(2;1,1;1,1)$ given in Example 10.5, let

$$C_1 = \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}, \quad C_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad D_1 = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}, \quad \text{and } D_2 = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$$

be an amicable family $\{C_1, C_2; D_1, D_2\}$. We construct

$$P = (B_1 \otimes C_1)p_1 + (A_1 \otimes C_2)p_2 + (A_2 \otimes C_2)p_3\,,$$
$$Q = (B_1 \otimes D_1)q_1 + (B_1 \otimes D_2)q_2 + (B_2 \otimes C_2)q_3\,.$$

The new amicable orthogonal designs of quaternions are:

$$P = \begin{bmatrix} -p_1 - p_2 & p_1 - p_2 & p_3\boldsymbol{i} & p_3\boldsymbol{i} \\ p_1 - p_2 & p_1 + p_2 & p_3\boldsymbol{i} & -p_3\boldsymbol{i} \\ -p_3\boldsymbol{j} & -p_3\boldsymbol{j} & -p_1\boldsymbol{k} + p_2\boldsymbol{k} & p_1\boldsymbol{k} + p_2\boldsymbol{k} \\ -p_3\boldsymbol{j} & p_3\boldsymbol{j} & p_1\boldsymbol{k} + p_2\boldsymbol{k} & p_1\boldsymbol{k} - p_2\boldsymbol{k} \end{bmatrix}$$

and

$$Q = \begin{bmatrix} q_1 + q_2 & -q_1 + q_2 & q_3\boldsymbol{i} & q_3\boldsymbol{i} \\ q_1 - q_2 & q_1 + q_2 & q_3\boldsymbol{i} & -q_3\boldsymbol{i} \\ q_3\boldsymbol{j} & q_3\boldsymbol{j} & q_1\boldsymbol{k} + q_2\boldsymbol{k} & -q_1\boldsymbol{k} + q_2\boldsymbol{k} \\ q_3\boldsymbol{j} & -q_3\boldsymbol{j} & q_1\boldsymbol{k} - q_2\boldsymbol{k} & q_1\boldsymbol{k} + q_2\boldsymbol{k} \end{bmatrix}.$$

In this design, some entries are linear combinations of two variables which may make it unsuitable for real applications in communications. To normalize the above design, we set new variables $a_1 = p_1 + p_2$, $a_2 = p_1 - p_2$, $a_3 = p_3$, and $b_1 = q_1 + q_2$, $b_2 = q_1 - q_2$, $b_3 = q_3$, then we get

$$P = \begin{bmatrix} -a_1 & a_2 & a_3\boldsymbol{i} & a_3\boldsymbol{i} \\ a_2 & a_1 & a_3\boldsymbol{i} & -a_3\boldsymbol{i} \\ -a_3\boldsymbol{j} & -a_3\boldsymbol{j} & -a_2\boldsymbol{k} & a_1\boldsymbol{k} \\ -a_3\boldsymbol{j} & a_3\boldsymbol{j} & a_1\boldsymbol{k} & a_2\boldsymbol{k} \end{bmatrix} \quad Q = \begin{bmatrix} b_1 & -b_2 & b_3\boldsymbol{i} & b_3\boldsymbol{i} \\ b_2 & b_1 & b_3\boldsymbol{i} & -b_3\boldsymbol{i} \\ b_3\boldsymbol{j} & b_3\boldsymbol{j} & b_1\boldsymbol{k} & -b_2\boldsymbol{k} \\ b_3\boldsymbol{j} & -b_3\boldsymbol{j} & b_2\boldsymbol{k} & b_1\boldsymbol{k} \end{bmatrix}.$$

This is an $AODQ(4;1,1,2;1,1,2)$ design without zero entries and no linear processing.

In [255], Yuen et al gave a construction method for amicable complex orthogonal designs. We can also apply it in constructing amicable orthogonal designs of quaternions.

Lemma 10.4. *If there exists a pair of amicable orthogonal designs of quaternions $AODQ(n;a_1,\ldots,a_s;b_1,\ldots,b_t)$, then there exists a pair of amicable orthogonal designs of quaternions of type $AODQ(4n;a_1,a_1,a_1,b_2,\ldots,b_t;b_1,b_1,b_1,a_2,\ldots,a_s)$.*

Proof. Let $X = \sum_{i=1}^{s} A_i x_i$ and $Y = \sum_{j=1}^{t} B_j y_j$ be the amicable orthogonal designs of quaternions in order n and define following **real** weighing matrices:

$$M_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix} \qquad M_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$M_3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix} \qquad N_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$N_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix} \qquad N_3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}$$

Construct the matrices

$$P = \sum_{i=1}^{3} (A_1 \otimes N_i)\, p_i + \sum_{j=2}^{t} (B_j \otimes I_4)\, p_{2+j}$$
$$Q = \sum_{i=1}^{3} (B_1 \otimes M_i)\, q_i + \sum_{j=2}^{s} (A_j \otimes I_4)\, q_{2+j}\,.$$

All the quaternion matrices P_i's and Q_i's satisfy the conditions (i)-(iv) because the weighing matrices $\{M_i\}$ and $\{N_i\}$ are skew-symmetric and they also form an amicable family. □

Example 10.11. Consider a pair of $AODQ(2;1,1;1,1)$ given in Example 10.5, we apply Lemma 10.4 to construct the following $AODQ(8;1,1,1,1;1,1,1,1)$:

$$P = \begin{bmatrix} 0 & -p_1 & -p_2 & -p_3 & p_4\boldsymbol{i} & 0 & 0 & 0 \\ p_1 & 0 & p_3 & -p_2 & 0 & p_4\boldsymbol{i} & 0 & 0 \\ p_2 & -p_3 & 0 & p_1 & 0 & 0 & p_4\boldsymbol{i} & 0 \\ p_3 & p_2 & -p_1 & 0 & 0 & 0 & 0 & p_4\boldsymbol{i} \\ p_4\boldsymbol{j} & 0 & 0 & 0 & 0 & p_1\boldsymbol{k} & p_2\boldsymbol{k} & p_3\boldsymbol{k} \\ 0 & p_4\boldsymbol{j} & 0 & 0 & -p_1\boldsymbol{k} & 0 & -p_3\boldsymbol{k} & p_2\boldsymbol{k} \\ 0 & 0 & p_4\boldsymbol{j} & 0 & -p_2\boldsymbol{k} & p_3\boldsymbol{k} & 0 & -p_1\boldsymbol{k} \\ 0 & 0 & 0 & p_4\boldsymbol{j} & -p_3\boldsymbol{k} & -p_2\boldsymbol{k} & p_1\boldsymbol{k} & 0 \end{bmatrix},$$

$$Q = \begin{bmatrix} 0 & q_1 & q_2 & q_3 & q_4\boldsymbol{i} & 0 & 0 & 0 \\ -q_1 & 0 & q_3 & -q_2 & 0 & q_4\boldsymbol{i} & 0 & 0 \\ -q_2 & -q_3 & 0 & q_1 & 0 & 0 & q_4\boldsymbol{i} & 0 \\ -q_3 & q_2 & -q_1 & 0 & 0 & 0 & 0 & q_4\boldsymbol{i} \\ -q_4\boldsymbol{j} & 0 & 0 & 0 & 0 & q_1\boldsymbol{k} & q_2\boldsymbol{k} & q_3\boldsymbol{k} \\ 0 & -q_4\boldsymbol{j} & 0 & 0 & -q_1\boldsymbol{k} & 0 & q_3\boldsymbol{k} & -q_2\boldsymbol{k} \\ 0 & 0 & -q_4\boldsymbol{j} & 0 & -q_2\boldsymbol{k} & -q_3\boldsymbol{k} & 0 & q_1\boldsymbol{k} \\ 0 & 0 & 0 & -q_4\boldsymbol{j} & -q_3\boldsymbol{k} & q_2\boldsymbol{k} & -q_1\boldsymbol{k} & 0 \end{bmatrix}.$$

Although we only give examples of $AODQ$ of orders 2, 4 and 8 in this chapter, there actually exist many designs of order other than powers of 2. We know that symmetric conference matrices exist for orders $n = q+1$, $q \equiv 1 \pmod 4$ a prime power, e.g., $n = 6$. Applying Theorem 10.1 on AODQ(2;1,1;1,1) and AODs from Corollary 10.1 gives us the following corollary.

Corollary 10.3. *Let $n \equiv 2 \pmod 4$ be the order of the symmetric conference matrices, then there exist*

a) $AODQ(4n;n,n,n;n,n,n)$,
b) $AODQ(4n;n,n,n;2,2(n-1),n)$,
c) $AODQ(4n;n,n,n;1,n-1,n)$,
d) $AODQ(4n;2,2(n-1),2(n-1);1,n-1,2(n-1))$,

An example is that for $n=6$, we have $AODQ(24;6,6,6;6,6,6)$, $AODQ(24;6,6,6;2,10,6)$, etc.

Corollary 10.4. *For* $q \equiv 3 \pmod 4$ *a prime power, there exist* $AODQ(2(q+1);1,q,q;1,q,q)$.

Proof. This corollary follows by applying Theorem 10.1 on $AODQ(2;1,1;1,1)$ and AODs from Lemma 10.3. □

The above corollary also gives an example of $AODQ(24;1,11,11;1,11,11)$ when $q=11$.

10.6 Combined Quaternion Orthogonal Designs from Amicable Designs

In [184], Seberry et al gave a technique named *combined quaternion orthogonal designs* from real and complex orthogonal designs. This combined design uses the property that if AB^H is a symmetric matrix, where A and B are matrices with complex entries, so that $AB^H\boldsymbol{q} = \boldsymbol{q}BA^H$ for $\boldsymbol{q} \in \{\pm\boldsymbol{j}, \pm\boldsymbol{k}\}$, to construct new $RQOD$. There is a connection between the combined design and amicable designs, in that the form of AB^H are examined. For amicable orthogonal designs of quaternions, the condition that AB^Q is a symmetric matrix can be relaxed since we have $AB^Q = BA^Q$ for A and B. In the case of combined design from amicable orthogonal design of quaternions, we also need to be careful about what quaternion appears as entries of AB^Q. We illustrate this with the following example:

Example 10.12. Consider the $AODQ(2;1,1;1,1)$ designs A and B from Example 10.5. We have

$$\begin{aligned} A^QB &= \begin{bmatrix} -x_1 & x_2\boldsymbol{j} \\ -x_2\boldsymbol{i} & -x_1\boldsymbol{k} \end{bmatrix} \quad \begin{bmatrix} y_1 & y_2\boldsymbol{i} \\ y_2\boldsymbol{j} & y_1\boldsymbol{k} \end{bmatrix} \\ &= \begin{bmatrix} -x_1y_1 - x_2y_2 & (-x_1y_2 + x_2y_1)\boldsymbol{i} \\ (x_1y_2 - x_2y_1)\boldsymbol{i} & x_1y_1 + x_2y_2 \end{bmatrix} \\ &= B^QA. \end{aligned}$$

Let $D = A + B\boldsymbol{q}$, $\boldsymbol{q} \in \{\pm\boldsymbol{i}, \pm\boldsymbol{j}, \pm\boldsymbol{k}\}$ be a new design for which we have

$$\begin{aligned} D^Q D &= (A^Q - \boldsymbol{q}B^Q)(A + B\boldsymbol{q}) \\ &= A^Q A + A^Q B\boldsymbol{q} - \boldsymbol{q}B^Q A - \boldsymbol{q}B^Q B\boldsymbol{q} \\ &= (A^Q A + B^Q B) + (A^Q B)\boldsymbol{q} - \boldsymbol{q}(B^Q A), \end{aligned}$$

where $A^Q B = B^Q A$ for the amicability of A and B, we also notice that all entries in $A^Q B$ are either real or products with quaternion $\boldsymbol{i}$. Thus $A^Q B\boldsymbol{i} = \boldsymbol{i}B^Q A$, and we have $D^Q D = A^Q A + B^Q B = (x_1^2 + x_2^2 + y_1^2 + y_2^2)I_2$. The new design $D = A + B\boldsymbol{i}$ is of the form:

$$D = \begin{bmatrix} -x_1 + y_1\boldsymbol{i} & x_2\boldsymbol{i} - y_2 \\ -x_2\boldsymbol{j} - y_2\boldsymbol{k} & x_1\boldsymbol{k} + y_1\boldsymbol{j} \end{bmatrix}.$$

Let complex symbols $z_i = x_i + \boldsymbol{i}y_i$, for $1 \le i \le 2$, then we can write above D as

$$D = \begin{bmatrix} -z_1^* & \boldsymbol{i}z_2 \\ -\boldsymbol{j}z_2^* & \boldsymbol{k}z_1 \end{bmatrix}.$$

The above design satisfies $D^Q D = (|z_1|^2 + |z_2|^2)I_2$ and hence is an $RQOD(2;1,1)$ on complex variables z_1 and z_2. The new RQOD in Example 10.12 has no zero entries, which may have practical advantages when used in wireless communication since there is no need to switch antennas off and back on during transmission.

We now provide an example constructing an $RQOD$ with order 4, which has no zero entries but with linear processing.

Example 10.13. Consider the $AODQ(4;1,1,2;1,1,2)$ designs A and B in Example 10.10 with variables a_1, a_2, a_3 and $b_1, b_2, b_3 \in \mathbb{R}$. We have $X = A^Q B$

$$\begin{aligned} &= \begin{bmatrix} -a_1 & a_2 & a_3\boldsymbol{j} & a_3\boldsymbol{j} \\ a_2 & a_1 & a_3\boldsymbol{j} & -a_3\boldsymbol{j} \\ -a_3\boldsymbol{i} & -a_3\boldsymbol{i} & a_2\boldsymbol{k} & -a_1\boldsymbol{k} \\ -a_3\boldsymbol{i} & a_3\boldsymbol{i} & -a_1\boldsymbol{k} & -a_2\boldsymbol{k} \end{bmatrix} \quad \begin{bmatrix} b_1 & -b_2 & b_3\boldsymbol{i} & b_3\boldsymbol{i} \\ b_2 & b_1 & b_3\boldsymbol{i} & -b_3\boldsymbol{i} \\ b_3\boldsymbol{j} & b_3\boldsymbol{j} & b_1\boldsymbol{k} & -b_2\boldsymbol{k} \\ b_3\boldsymbol{j} & -b_3\boldsymbol{j} & b_2\boldsymbol{k} & b_1\boldsymbol{k} \end{bmatrix} \\ &= \begin{bmatrix} X_{11} & X_{12} & X_{13} & X_{14} \\ X_{12}^Q & X_{22} & X_{23} & X_{24} \\ X_{13}^Q & X_{23}^Q & X_{33} & X_{34} \\ X_{14}^Q & X_{24}^Q & X_{34}^Q & X_{44} \end{bmatrix} \\ &= B^Q A, \end{aligned}$$

Where

$$X_{11} = -a_1b_1 + a_2b_2 - 2a_3b_3\,, \qquad X_{12} = a_1b_2 + a_2b_1\,,$$
$$X_{13} = (-a_1b_3 + a_2b_3 + a_3b_1 + a_3b_2)\boldsymbol{i}\,, \qquad X_{14} = (-a_1b_3 - a_2b_3 + a_3b_1 - a_3b_2)\boldsymbol{i}\,,$$
$$X_{22} = a_1b_1 - a_2b_2 - 2a_3b_3\,, \qquad X_{23} = (a_1b_3 + a_2b_3 + a_3b_1 - a_3b_2)\boldsymbol{i}\,,$$
$$X_{24} = (-a_1b_3 + a_2b_3 - a_3b_1 - a_3b_2)\boldsymbol{i}\,, \qquad X_{33} = a_1b_2 - a_2b_1 + 2a_3b_3\,,$$
$$X_{34} = a_1b_1 + a_2b_2 \text{ and} \qquad X_{44} = -a_1b_2 + a_2b_1 + 2a_3b_3\,.$$

Since only quaternion $\boldsymbol{i}$ appears in X, we then set $D = A + B\boldsymbol{i}$ as the new design:

$$D = \begin{bmatrix} -a_1 + b_1\boldsymbol{i} & a_2 - b_2\boldsymbol{i} & a_3\boldsymbol{i} - b_3 & a_3\boldsymbol{i} - b_3 \\ a_2 + b_2\boldsymbol{i} & a_1 + b_1\boldsymbol{i} & a_3\boldsymbol{i} - b_3 & -a_3\boldsymbol{i} + b_3 \\ -a_3\boldsymbol{j} - b_3\boldsymbol{k} & -a_3\boldsymbol{j} - b_3\boldsymbol{k} & -a_2\boldsymbol{k} + b_1\boldsymbol{j} & a_1\boldsymbol{k} - b_2\boldsymbol{j} \\ -a_3\boldsymbol{j} - b_3\boldsymbol{k} & a_3\boldsymbol{j} + b_3\boldsymbol{k} & a_1\boldsymbol{k} + b_2\boldsymbol{j} & a_2\boldsymbol{k} + b_1\boldsymbol{j} \end{bmatrix}.$$

Let complex symbols $z_i = a_i + \boldsymbol{i}b_i$, for $1 \le i \le 3$, then we can write above D as

$$D = \begin{bmatrix} -z_1^* & z_2^* & \boldsymbol{i}z_3 & \boldsymbol{i}z_3 \\ z_2 & z_1 & \boldsymbol{i}z_3 & -\boldsymbol{i}z_3 \\ -\boldsymbol{j}z_3^* & -\boldsymbol{j}z_3^* & -\boldsymbol{k}(a_2 - b_1\boldsymbol{i}) & \boldsymbol{k}(a_1 - b_2\boldsymbol{i}) \\ -\boldsymbol{j}z_3^* & \boldsymbol{j}z_3^* & \boldsymbol{k}(a_1 + b_2\boldsymbol{i}) & \boldsymbol{k}(a_2 + b_1\boldsymbol{i}) \end{bmatrix}.$$

The above design satisfies $D^Q D = (|z_1|^2 + |z_2|^2 + 2|z_3|^2)I_4$ and hence is an $RQOD(4;1,1,2)$ on the complex variables z_1, z_2 and z_3. Note that if an entry in the orthogonal design is a linear combination of variables from the given domain, the design is said to be **with linear processing**. Obviously, the new $RQOD$ design has the property of no zero entries but with linear processing on some entries, i.e the position $(3,3)$ is the quaternion combination of real part of symbol z_2 and imaginary part of symbol z_1.

The following Lemma shows construction of orthogonal designs of quaternions by using symmetric conference matrices.

Lemma 10.5. *Suppose a, b, c, d are real commuting variables. Let N be a symmetric conference matrix of order n and I identity matrix of same order. Then, $X = aI\boldsymbol{i} + bN$ and $Y = cI\boldsymbol{j} + dN\boldsymbol{k}$ are orthogonal designs of quaternions $ODQ(n;1,n-1)$, and $XY^Q + YX^Q = 0$, so X and Y are $AAODQ(n;1,n-1;1,n-1)$ (anti-amicable orthogonal design of quaternions). Hence $\left[\begin{smallmatrix} X & Y \\ Y & X \end{smallmatrix}\right]$ is a $ODQ(2n;1,1,n-1,n-1)$.*

The proof for Lemma 10.5 is straightforward.

Example 10.14. For a symmetric conference matrix N of order 6, we construct the following matrices:

$$X = \begin{bmatrix} a\boldsymbol{i} & b & b & b & b & b \\ b & a\boldsymbol{i} & b & -b & -b & b \\ b & b & a\boldsymbol{i} & b & -b & -b \\ b & -b & b & a\boldsymbol{i} & b & -b \\ b & -b & -b & b & a\boldsymbol{i} & b \\ b & b & -b & -b & b & a\boldsymbol{i} \end{bmatrix} \quad Y = \begin{bmatrix} c\boldsymbol{j} & d\boldsymbol{k} & d\boldsymbol{k} & d\boldsymbol{k} & d\boldsymbol{k} & d\boldsymbol{k} \\ d\boldsymbol{k} & c\boldsymbol{j} & d\boldsymbol{k} & -d\boldsymbol{k} & -d\boldsymbol{k} & d\boldsymbol{k} \\ d\boldsymbol{k} & d\boldsymbol{k} & c\boldsymbol{j} & d\boldsymbol{k} & -d\boldsymbol{k} & -d\boldsymbol{k} \\ d\boldsymbol{k} & -d\boldsymbol{k} & d\boldsymbol{k} & c\boldsymbol{j} & d\boldsymbol{k} & -d\boldsymbol{k} \\ d\boldsymbol{k} & -d\boldsymbol{k} & -d\boldsymbol{k} & d\boldsymbol{k} & c\boldsymbol{j} & d\boldsymbol{k} \\ d\boldsymbol{k} & d\boldsymbol{k} & -d\boldsymbol{k} & -d\boldsymbol{k} & d\boldsymbol{k} & c\boldsymbol{j} \end{bmatrix}.$$

X and Y both are $ODQ(6;1,5)$. They also form a pair of $AAODQ(6;1,5;1,5)$.

Corollary 10.5. *Let $p \equiv 1 \pmod 4$ be a prime power. Then there exist orthogonal designs of quaternions $ODQ(p+1;1,p)$ and $ODQ(2(p+1);1,p,1,p)$, also a pair of anti-amicable orthogonal designs of quaternions $AAODQ(p+1;1,p;1,p)$.*

Corollary 10.5 follows directly from Lemma 10.5.

Lemma 10.6. *For a pair of $AAODQ(n;1,n-1;1,n-1)$ X and Y given in Lemma 10.5, then $D = X + Y\boldsymbol{i}$ is an $RQOD(n;1,n-1)$.*

Proof. We have

$$\begin{aligned} D^Q D &= (X^Q - \boldsymbol{i}Y^Q)(X + Y\boldsymbol{i}) \\ &= X^Q X + X^Q Y\boldsymbol{i} - \boldsymbol{i}Y^Q X - \boldsymbol{i}Y^Q Y\boldsymbol{i} \\ &= (X^Q X + Y^Q Y) + (X^Q Y)\boldsymbol{i} - \boldsymbol{i}(Y^Q X)\,. \end{aligned}$$

For $X = xI\boldsymbol{i} + bN$ and $Y = cI\boldsymbol{j} + dN\boldsymbol{k}$, where N is a conference matrix of order n and I is the identity matrix with same order, we have

$$\begin{aligned} X^Q Y &= (-aI\boldsymbol{i} + bN^T)(cI\boldsymbol{j} + dN\boldsymbol{k}) \\ &= -acI\boldsymbol{k} + adN\boldsymbol{j} + bcN\boldsymbol{j} + bdNN^T\boldsymbol{k} \\ &= -Y^Q X\,, \end{aligned}$$

since only quaternions $\boldsymbol{k}$ and $\boldsymbol{j}$ appear in $X^Q Y$, we have $(X^Q Y)\boldsymbol{i} = \boldsymbol{i}(Y^Q X)$. Hence,

$$D^Q D = X^Q X + Y^Q Y = (a^2 + (n-1)b^2 + c^2 + (n-1)d^2) I_n\,,$$

i.e. D is an $RQOD(n;1,n-1)$. □

Example 10.15. Consider a pair of $AAODQ(6;1,5;1,5)$ given in Example 10.14, we have the following $D = X + Y\boldsymbol{i}$:

$$\begin{bmatrix} \boldsymbol{i}(a-c\boldsymbol{j}) & b+d\boldsymbol{j} & b+d\boldsymbol{j} & b+d\boldsymbol{j} & b+d\boldsymbol{j} & b+d\boldsymbol{j} \\ b+d\boldsymbol{j} & \boldsymbol{i}(a-c\boldsymbol{j}) & b+d\boldsymbol{j} & -(b+d\boldsymbol{j}) & -(b+d\boldsymbol{j}) & b+d\boldsymbol{j} \\ b+d\boldsymbol{j} & b+d\boldsymbol{j} & \boldsymbol{i}(a-c\boldsymbol{j}) & b+d\boldsymbol{j} & -(b+d\boldsymbol{j}) & -(b+d\boldsymbol{j}) \\ b+d\boldsymbol{j} & -(b+d\boldsymbol{j}) & b+d\boldsymbol{j} & \boldsymbol{i}(a-c\boldsymbol{j}) & b+d\boldsymbol{j} & -(b+d\boldsymbol{j}) \\ b+d\boldsymbol{j} & -(b+d\boldsymbol{j}) & -(b+d\boldsymbol{j}) & b+d\boldsymbol{j} & \boldsymbol{i}(a-c\boldsymbol{j}) & b+d\boldsymbol{j} \\ b+d\boldsymbol{j} & b+d\boldsymbol{j} & -(b+d\boldsymbol{j}) & -(b+d\boldsymbol{j}) & b+d\boldsymbol{j} & \boldsymbol{i}(a-c\boldsymbol{j}) \end{bmatrix}.$$

In above design D, if we replace quaternion element $\boldsymbol{j}$ by $\boldsymbol{i}$, $\boldsymbol{i}$ by an undecided quaternion element $\boldsymbol{q}$, and let complex variables $z_1 = a + c\boldsymbol{i}$ and $z_2 = b + d\boldsymbol{i}$, then we have D:

$$\begin{bmatrix} \boldsymbol{q}z_1^* & z_2 & z_2 & z_2 & z_2 & z_2 \\ z_2 & \boldsymbol{q}z_1^* & z_2 & -z_2 & -z_2 & z_2 \\ z_2 & z_2 & \boldsymbol{q}z_1^* & z_2 & -z_2 & -z_2 \\ z_2 & -z_2 & z_2 & \boldsymbol{q}z_1^* & z_2 & -z_2 \\ z_2 & -z_2 & -z_2 & z_2 & \boldsymbol{q}z_1^* & z_2 \\ z_2 & z_2 & -z_2 & -z_2 & z_2 & \boldsymbol{q}z_1^* \end{bmatrix}.$$

$\boldsymbol{q}$ in above D can be chosen from the set $\{\pm\boldsymbol{k}, \pm\boldsymbol{j}\}$ since $\boldsymbol{q}z_1^* z_2^* = z_2 z_1 \boldsymbol{q}$ for any $\boldsymbol{q} \in \{\pm\boldsymbol{k}, \pm\boldsymbol{j}\}$. It is easy to prove $D^Q D = (|z_1|^2 + 5|z_2|^2) I_6$. Hence, D is a restricted quaternion orthogonal design $RQOD(6; 1, 5)$ with no zero entries.

10.7 Le Tran's Complex Orthogonal Designs of Order Eight

Square, Complex Orthogonal Space-Time Block Codes (CO STBCs) are known for the relatively simple receiver structure and minimum processing delay in the case of complex signal constellations. One of the methods to construct square CO STBCs is based on amicable orthogonal designs (AODs). The simplest CO STBC is the Alamouti code [3] for two transmitter (Tx) antennas, which is based on an amicable orthogonal pair of order-2 matrices. The Alamouti code achieves the transmission rate of one for 2 TX antennas, while the CO STBCs for more than 2 Tx antennas cannot provide the rate of one (see [214, Section 2.3] or [148, 149]). However they can still achieve the full diversity for the given number of Tx antennas.

The construction of CO STBCs follows directly from complex orthogonal designs (CODs).

Definition 10.9. A square COD $Z = X + iY$ of order n is an $n \times n$ matrix on the complex indeterminates $s_1, \ldots, s_p$, with entries chosen from $0, \pm s_1, \ldots, \pm s_p$, their conjugates $\pm s_1^*, \ldots, \pm s_p^*$, or their products with $i = \sqrt{-1}$ such that:

$$Z^H Z = \left(\sum_{k=1}^{p} |s_k|^2 \right) I_n \tag{10.1}$$

where Z^H denotes the Hermitian transpose of Z and I_n is the identity matrix of order n.

For the matrix Z to satisfy (10.1), the matrices X and Y must be a pair of AODs, which implies that both X and Y are orthogonal designs themselves and $XY^\top = YX^\top$, where $(.)^\top$ denotes matrix transposition.

It has been shown in [80] that, for $n = 8$, the total number of different variables in the amicable pair X and Y cannot exceed eight.

It has been shown in [203], that the construction of CODs can be faciliated by representing Z as

$$Z = \sum_{j=1}^{p} A_j s_j^R + i \sum_{j=1}^{p} B_j s_j^I \tag{10.2}$$

where s_j^R and s_j^I denote the real and imaginary parts of the complex variables $s_j = s_j^R + i s_j^I$ and A_j and B_j are the real coefficient matrices for s_j^R and s_j^I, respectively. To satisfy (10.1), the matrices $\{A_j\}$ and $\{B_j\}$ of order n must satisfy the following conditions:

$$\begin{aligned} &A_j A_j^\top = I,\ B_j B_j^\top = I,\ \forall j = 1, \ldots, p \\ &A_k A_j^\top = -A_j A_j^\top,\ B_k B_j^\top = -B_j B_k^\top,\ k \neq j \\ &A_k B_j^\top = B_j A_k^\top,\ \forall k,\ j = 1, \ldots, p \end{aligned} \tag{10.3}$$

The conditions in (10.3) are necessary and sufficient for the existence of AODs of order n. Thus, the problem of finding CODs is connected to the theory of AODs.

From the perspective of constructing CO STBCs, the most promising case is that in which both X and Y have four variables. This case has been considered in the conventional, order-8 CO STBCs, corresponding to $COD(8; 1, 1, 1, 1)$ with all four variables appearing *once* in each column of Z. An example is given in Fig. 10.1, (see [209, 210], or [214, Eq.(2.34)]).

Fig. 10.1 A conventional COD of order eight [a]

$$\mathbf{Z}_1 = \begin{bmatrix} s_1 & s_2 & s_3 & 0 & s_4 & 0 & 0 & 0 \\ -s_2^* & s_1^* & 0 & -s_3 & 0 & -s_4 & 0 & 0 \\ -s_3^* & 0 & s_1^* & s_2 & 0 & 0 & -s_4 & 0 \\ 0 & s_3^* & -s_2^* & s_1 & 0 & 0 & 0 & s_4 \\ -s_4^* & 0 & 0 & 0 & s_1^* & s_2 & s_3 & 0 \\ 0 & s_4^* & 0 & 0 & -s_2^* & s_1 & 0 & -s_3 \\ 0 & 0 & s_4^* & 0 & -s_3^* & 0 & s_1 & s_2 \\ 0 & 0 & 0 & -s_4^* & 0 & s_3^* & -s_2^* & s_1^* \end{bmatrix}$$

[a] Tran, Wysocki, Mertins, and Seberry [213, p75] ©Springer

These conventional codes contain numerous zero entries which are undesirable. Note that we use the similar notation to that mentioned in [80], i.e. $COD(8;1,1,1,1)$, to denote a square, order-8 COD containing four complex variables and each variable appearing once in each column. Readers may refer to [80] for more details.

In [186, 212, 256], two new codes of order eight are introduced where some variables appear more often than others (more than once in each column), i.e., codes based on $COD(8;1,1,2,2)$ and $COD(8;1,1,1,4)$. These codes, namely Z_2 and Z_3, are given in Fig. 10.2 and 10.3, respectively. It is easy to check that these codes satisfy the conditions (10.1).

Fig. 10.2 Code Z_2 [a]

$$\mathbf{Z}_2 = \begin{bmatrix}
s_1 & s_2 & \frac{s_3}{\sqrt{2}} & \frac{s_3}{\sqrt{2}} & 0 & 0 & \frac{s_4}{\sqrt{2}} & \frac{s_4}{\sqrt{2}} \\
-s_2^* & s_1^* & \frac{s_3}{\sqrt{2}} & -\frac{s_3}{\sqrt{2}} & 0 & 0 & \frac{s_4}{\sqrt{2}} & -\frac{s_4}{\sqrt{2}} \\
\frac{s_3^*}{\sqrt{2}} & \frac{s_3^*}{\sqrt{2}} & -s_1^R + is_2^I & -s_2^R + is_1^I & \frac{s_4}{\sqrt{2}} & \frac{s_4}{\sqrt{2}} & 0 & 0 \\
\frac{s_3^*}{\sqrt{2}} & -\frac{s_3^*}{\sqrt{2}} & s_2^R + is_1^I & -s_1^R - is_2^I & \frac{s_4}{\sqrt{2}} & -\frac{s_4}{\sqrt{2}} & 0 & 0 \\
0 & 0 & \frac{s_4^*}{\sqrt{2}} & \frac{s_4^*}{\sqrt{2}} & s_1 & s_2 & -\frac{s_3^*}{\sqrt{2}} & -\frac{s_3^*}{\sqrt{2}} \\
0 & 0 & \frac{s_4^*}{\sqrt{2}} & -\frac{s_4^*}{\sqrt{2}} & -s_2^* & s_1^* & -\frac{s_3^*}{\sqrt{2}} & \frac{s_3^*}{\sqrt{2}} \\
\frac{s_4^*}{\sqrt{2}} & \frac{s_4^*}{\sqrt{2}} & 0 & 0 & -\frac{s_3^*}{\sqrt{2}} & -\frac{s_3^*}{\sqrt{2}} & -s_1^R + is_2^I & -s_2^R + is_1^I \\
\frac{s_4^*}{\sqrt{2}} & -\frac{s_4^*}{\sqrt{2}} & 0 & 0 & -\frac{s_3^*}{\sqrt{2}} & \frac{s_3^*}{\sqrt{2}} & s_2^R + is_1^I & -s_1^R - is_2^I
\end{bmatrix}$$

[a] Tran, Wysocki, Mertins, and Seberry [213, p76] ©Springer

Fig. 10.3 Code Z_3 [a]

$$\mathbf{Z}_3 = \begin{bmatrix}
s_1 & 0 & s_3^R + is_2^I & s_2^R + is_3^I & \frac{s_4}{2} & \frac{s_4}{2} & \frac{s_4}{2} & \frac{s_4}{2} \\
0 & s_1 & -s_2^R + is_3^I & s_3^R - is_2^I & \frac{s_4}{2} & -\frac{s_4}{2} & \frac{s_4}{2} & -\frac{s_4}{2} \\
-s_3^R + is_2^I & s_2^R + is_3^I & s_1^* & 0 & \frac{s_4}{2} & \frac{s_4}{2} & -\frac{s_4}{2} & -\frac{s_4}{2} \\
-s_2^R + is_3^I & -s_3^R - is_2^I & 0 & s_1^* & \frac{s_4}{2} & \frac{s_4}{2} & -\frac{s_4}{2} & \frac{s_4}{2} \\
-\frac{s_4^*}{2} & -\frac{s_4^*}{2} & -\frac{s_4^*}{2} & -\frac{s_4^*}{2} & s_1^R - is_3^I & s_2^* & s_3^R - is_1^I & 0 \\
-\frac{s_4^*}{2} & \frac{s_4^*}{2} & -\frac{s_4^*}{2} & \frac{s_4^*}{2} & -s_2 & s_1^R + is_3^I & 0 & s_3^R - is_1^I \\
-\frac{s_4^*}{2} & -\frac{s_4^*}{2} & \frac{s_4^*}{2} & \frac{s_4^*}{2} & -s_3^R - is_1^I & 0 & s_1^R + is_3^I & -s_2^* \\
-\frac{s_4^*}{2} & \frac{s_4^*}{2} & \frac{s_4^*}{2} & -\frac{s_4^*}{2} & 0 & -s_3^R - is_1^I & s_2 & s_1^R - is_3^I
\end{bmatrix}$$

[a] Tran, Wysocki, Mertins, and Seberry [213, p77] ©Springer

All the CO STBCs proposed here achieve the *maximum* code rate for order-8, *square* CO STBCs, which is equal to $\frac{1}{2}$. We would like to recall that, according to Liang's paper [148], the maximum achievable rate of CO STBCs

for $n = 2m-1$ or $n = 2m$ Tx antennas is $R_{\max} = \frac{(m+1)}{2m}$. Particularly, for $n = 8$, i.e., $m = 4$, the maximum achievable rate of CO STBCs is $\frac{5}{8}$.

However, this maximum rate is only achievable for *non-square* constructions. For *square* constructions of orders $n = 2^a(2b+1)$, the maximum achievable rate is $R_{\max} = \frac{(a+1)}{[2^a(2b+1)]}$. For $n = 8$, i.e., $a = 3$ and $b = 0$, the maximum achievable rate of *square* CO STBCs is only $\frac{1}{2}$.

The vague statement on the maximum achievable rate of CO STBCs in Liang's paper [148], which easily makes readers confused, has been pointed out in [214, Remark 2.3.2.1]

A question that could be raised is why *square* CO STBCs are of particular interest. It is because, *square* CO STBCs have a great advantage over *non-square* CO STBCs that they require a much smaller length of the codes, i.e., much smaller processing delay, though, the maximum rate of the former may be smaller than that of the later.

Let us consider CO STBCs for $n = 8$ Tx antennas as an example (also see [214, Example 2.3.2.1]). The *non-square* CO STBC that achieves the maximum rate 5/8 requires the length of 112 STSs as shown by Table 2.6 in [214, p.40]. The [112,8,70] CO STBC given in Appendix E in Liang's paper [55] is an example for this case. As opposed to *non-square* CO STBCs, *square* CO STBCs only require the length of 8 STSs to achieve the maximum rate 1/2, which is slightly smaller than the maximum rate of *non-square* CO STBCs. Clearly, *square* CO STBCs require a much shorter length, especially for a large number of Tx antennas, with the consequence of a slightly lower code rate. For this reason, *square* CO STBCs are of our particular interest.

Apart from having the maximum rate, our proposed CO STBCs Z_2 and Z_3, (see Figures 10.2 and 10.3) have fewer zero entries (compared to the conventional codes) or even no zero entries in the code matrices. This property results in a more uniform transmission power distribution between Tx antennas. Intuitively, due to this property, our proposed CO STBCs require a lower peak power per Tx antenna to achieve the same bit error performance as the conventional CO STBCs containing numerous zeros. Equivalently, with the same peak power at Tx antennas, our proposed codes provide a better bit error performance than the conventional CO STBCs.

In addition, our codes are more amenable to practical implementation than the conventional code, since, transmitter antennas are turned off less frequently or even are not required to be turned off during transmission unlike with the conventional codes.

10.8 Research Problem

Thus we have some methods for building amicable orthogonal designs over the real and quaternion domain, e.g. the way to construct amicable orthogonal

designs of quaternions (AODQ) by using Kronecker product with **real** amicable orthogonal designs or **real** weighing matrices from an amicable family.

This construction ensures that, for any existing **real** amicable orthogonal design generated by using the Kronecker product, we can easily find an AODQ with same order and type. We also showed that if A and B forms a pair of AODQ, then the combined design $A + B\boldsymbol{q}$ for $\boldsymbol{q} \in \{\pm\boldsymbol{i}, \pm\boldsymbol{j}, \pm\boldsymbol{k}\}$is an RQOD by carefully choosing $\boldsymbol{q}$. Our newly constructed AODQs and RQODs, especially those with no zero entries, could have applications as orthogonal space-time-polarization block codes.

However, there are still some problems which need to be solved:

Problem 10.2 (Research Problem 5). Do there exist any new amicable orthogonal designs of quaternions for which there are no such real or complex designs.

Problem 10.3 (Research Problem 6). Determine the maximum number of variables in an AODQ.

It is known that finding the maximum number of variables in an AOD is equivalent to finding the number of members in a *Hurwitz-Radon family* of corresponding type [80], which also implies that the so-called Clifford algebras [29] have a matrix representation of the same order.

Problem 10.4 (Research Problem 7). How can we find a set of anti-commuting real, complex and quaternion matrices representation to determine the maximum number of variables in an AODQ.

Appendix A
Orthogonal Designs in Order 12, 24, 48 and 3.q

Description of Appendices A, B, C, D and E

In Appendices A, B, C, D, and E many times we give the first rows of circulant matrices which can be used in the Goethals-Seidel array (Theorem 4.8) to obtain orthogonal designs of the type described in orders 12, 20, 28, 36 and 44. The results for smaller orders are largely complete but combinatorial explosion makes computer searches for larger orders very time and space dependent. We point the interested reader to the extensive website of relevant results obtained by Koukouvinos [127].

A.1 Number of possible n-tuples

We note the following lemma from Georgiou, Koukouvinos, Mitrouli and Seberry [70] which is useful in determining the size of programs to search for orthogonal designs. The result is obtained by simple counting.

Lemma A.1. *Let $n = 4m$ be the order of an orthogonal design. Then the number of cases (k-tuples, $k = 2,3,4$) which must be studied to determine whether all orthogonal designs exist is*

(i) $\frac{1}{4}n^2$ *when* $2-$*tuples are considered;*
(ii) N*, when* 3*-tuples are considered, where*

- *(a)* $N = \frac{n}{72}(2n^2+3n-6)$ *if* $\frac{1}{4}n \equiv 0 \pmod 3$*;*
- *(b)* $N = \frac{(n+2)}{72}(2n^2-n-4)$ *if* $\frac{1}{4}n \equiv 1 \pmod 3$*;*
- *(c)* $N = \frac{(n-2)}{72}(2n^2+7n+8)$ *if* $\frac{1}{4}n \equiv 2 \pmod 3$.

(iii) N*, when* $4-$*tuples are considered, where*

- *(a)* $N = \frac{1}{576}(n^4+6n^3-2n^2-24n)$ *if* $\frac{1}{4}n \equiv 0 \pmod 3$*;*

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5

(b) $N = \frac{1}{576}(n^4+6n^3-2n^2-24n+64)$ *if* $\frac{1}{4}n \equiv 1 \pmod 3$*;*
(c) $N = \frac{1}{576}(n^4+6n^3-2n^2-24n+64)$ *if* $\frac{1}{4}n \equiv 2 \pmod 3$.

In each of these appendices the format is the same; we first list all 4-tuples which might be the type of an orthogonal design in that order (i. e. not eliminated by any known theorem); this is then followed by a list of 3-tuples which might be the type of an orthogonal design in that order and is not already known to exist because it can be obtained from a known 4-tuple by equating or killing variables. We continue in this fashion with 2-tuples. The blank spaces indicate that we have not been able to construct or prove non-existence of the orthogonal design in question.

These lists were compiled by computer programmes and the constructions of the first rows for smaller orders of existence were done by hand.

We then proceed to give the state of the art for orders $2^t.3, 2^t.5, 2^t.7, 2^t.9$ and $2^t.11$ for small integers t. All care has been taken to present those known in the literature in 2016 but some may have been overlooked and many are not known.

This appendix is a summary for orthogonal designs in order $12, 24, 48, 2^t.3$.

A.2 Some Theorems

Using Geramita and Seberry [80], Robinson [80, p.375] and Holzmann-Kharaghani [100, p.111] we have

Lemma A.2. *All full orthogonal designs* $OD(2^t3; x, y, 2^t3-x-y)$ *exist for any positive integer* $t \geq 3$.

We give a brief glimpse of other great theorems which are known.

Lemma A.3 (Kharaghani [120]). $OD(12(p+1); 3,3,3,3,3p,3p,3p,3p)$ *exist for all* $p \equiv 3 \pmod 4$.

Lemma A.4. *The necessary conditions are sufficient for the existence of orthogonal designs in order 12.*

Lemma A.5 (Holzmann, Kharaghani and Plotkin [100, 101]). *An* $OD(24; 3,3,3,3,3,3,3,3)$ *exists.*

A.3 Orthogonal Designs in Order 12

1. There are 12 possible 4 variable designs in order 12. Table A.1 lists first rows to construct all possible 4-tuples for orthogonal design in order 12 using the Goethals-Seidel array.

2. There are 31 possible 3 variable designs in order 12. Table A.2 gives those not excluded by theory and all may be found from the 4 variable designs by equating variables or setting variables zero.
3. All (s,t) where $s+t \leq 12$, $1 \leq s \leq t$, (36 possible but 3 excluded leaves 33 possibilities) exist and may be found from 4 variable designs by equating variables or setting variables zero. Those not possible are

$$(1,7) \qquad (4,7) \qquad (3,5)\,.$$

4. All 1 variable designs exist.

Table A.1 First rows to construct 4 variable designs in Order 12

Design	A_1	A_2	A_3	A_4
(1, 1, 1, 1)	$a,0,0$	$b,0,0$	$c,0,0$	$d,0,0$
(1, 1, 1, 4)	$a,0,0$	$b,0,0$	$c,d,\bar{d}$	$0,d,d$
(1, 1, 1, 9)	$a,d,\bar{d}$	$b,d,\bar{d}$	$c,d,\bar{d}$	d,d,d
(1, 1, 2, 2)	$a,0,0$	$b,0,0$	$c,d,0$	$c,\bar{d},0$
(1, 1, 2, 8)	$a,d,\bar{d}$	$b,d,\bar{d}$	c,d,d	$\bar{c},d,d$
(1, 1, 4, 4)	$a,c,\bar{c}$	$0,c,c$	$b,d,\bar{d}$	$0,d,d$
(1, 1, 5, 5)	$a,c,\bar{c}$	$b,d,\bar{d}$	c,d,d	$\bar{d},c,c$
(1, 2, 2, 4)	$a,d,\bar{d}$	$0,d,d$	$b,c,0$	$b,\bar{c},0$
(1, 2, 3, 6)	$a,d,\bar{d}$	c,d,d	$c,\bar{d},b$	$c,\bar{b},\bar{d}$
(2, 2, 2, 2)	$a,b,0$	$a,\bar{b},0$	$c,d,0$	$c,\bar{d},0$
(2, 2, 4, 4)	a,c,d	$a,\bar{d},\bar{c}$	$b,c,\bar{d}$	$b,\bar{c},d$
(3, 3, 3, 3)	a,b,c	$\bar{b},a,d$	$\bar{c},\bar{d},a$	$\bar{d},c,\bar{b}$

Table A.2 Existing 3 variable designs in Order 12

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

A.4 Orthogonal Designs in Order 24

This material is from Geramita and Seberry [80] and the more recent designs from Holzmann and Kharaghani [100]. An orthogonal design in order 24 can have at most 8 variables.

Lemma A.6. *There exist orthogonal designs of types* $OD(24;1,1,2,4,4,8)$ *and* $OD(24;3,3,3,3,3,3,3,3)$.

Proof. We note that there is a $(1,4)$ design in order 6 and so an $(1,1,2,4,4,8)$ design exists in order 24. The other design is in Section 4.13 and is the Plotkin array of order 24.

Lemma A.7. *There are orthogonal designs* $OD(24;1,1,1,1,1,5,5,9)$ *and* $OD(24;1,1,1,1,1,2,8,9)$.

Proof. Consider the following matrices, M_1 and M_2:

$$\begin{array}{|c|c|c|c|c|c|}
\hline
x_5 & x_4\bar{x}_8x_6\bar{x}_7 & x_7x_6x_8x_8 & x_6\bar{x}_7\bar{x}_8x_8 & \bar{x}_7\bar{x}_6\bar{x}_8\bar{x}_8 & x_7x_6x_8x_8 \\
\hline
\bar{x}_4x_8\bar{x}_6\bar{x}_7 & \bar{x}_5 & x_6x_7x_8x_8 & \bar{x}_7x_6x_8\bar{x}_8 & \bar{x}_7x_6x_8\bar{x}_8 & x_7\bar{x}_6\bar{x}_8x_8 \\
\hline
\bar{x}_7\bar{x}_6\bar{x}_8x_8 & \bar{x}_6\bar{x}_7\bar{x}_8x_8 & x_7 & x_4x_8x_5x_6 & \bar{x}_8x_8x_7x_7 & x_8x_8\bar{x}_6x_6 \\
\hline
\bar{x}_6x_7x_8x_8 & x_7\bar{x}_6\bar{x}_8\bar{x}_8 & \bar{x}_4\bar{x}_8\bar{x}_5x_6 & \bar{x}_7 & x_8\bar{x}_8x_6x_6 & x_8x_8x_7\bar{x}_7 \\
\hline
x_7x_6x_8\bar{x}_8 & x_7\bar{x}_6\bar{x}_8\bar{x}_8 & x_8\bar{x}_8\bar{x}_7x_7 & \bar{x}_8x_8\bar{x}_7x_7 & x_6 & x_4x_8x_7x_5 \\
\hline
\bar{x}_7\bar{x}_6\bar{x}_8x_8 & \bar{x}_7x_6x_8x_8 & \bar{x}_8\bar{x}_8x_6x_6 & \bar{x}_8\bar{x}_8\bar{x}_7\bar{x}_7 & \bar{x}_4\bar{x}_8\bar{x}_7x_5 & \bar{x}_6 \\
\hline
\end{array} = M_1$$

$$\begin{array}{|c|c|c|c|c|c|}
\hline
x_5 & x_4\bar{x}_6x_8\bar{x}_6 & x_8x_8x_7x_7 & x_8\bar{x}_8\bar{x}_7x_7 & \bar{x}_8\bar{x}_7\bar{x}_8\bar{x}_7 & x_8x_7x_8x_7 \\
\hline
\bar{x}_4x_6\bar{x}_8\bar{x}_6 & \bar{x}_5 & x_8x_8x_7x_7 & \bar{x}_8x_8x_7\bar{x}_7 & x_8\bar{x}_7\bar{x}_8x_7 & x_8\bar{x}_7\bar{x}_8x_7 \\
\hline
\bar{x}_8\bar{x}_8\bar{x}_7x_7 & \bar{x}_8\bar{x}_8\bar{x}_7x_7 & x_7 & x_4x_7x_5x_8 & \bar{x}_7x_7x_8x_8 & x_8x_8\bar{x}_6x_6 \\
\hline
\bar{x}_8x_8x_7x_7 & x_8\bar{x}_8\bar{x}_7\bar{x}_7 & \bar{x}_4\bar{x}_7\bar{x}_5x_8 & \bar{x}_7 & x_8\bar{x}_8x_6x_6 & x_7x_7x_8\bar{x}_8 \\
\hline
x_8x_7x_8\bar{x}_7 & \bar{x}_8x_7x_8x_7 & x_7\bar{x}_7\bar{x}_8x_8 & \bar{x}_8x_8\bar{x}_6x_6 & x_7 & x_4x_7x_8x_5 \\
\hline
\bar{x}_8\bar{x}_7\bar{x}_8x_7 & \bar{x}_8x_7x_8x_7 & \bar{x}_8\bar{x}_8x_6x_6 & \bar{x}_7\bar{x}_7\bar{x}_8\bar{x}_8 & \bar{x}_4x_7x_8x_5 & \bar{x}_7 \\
\hline
\end{array} = M_2$$

Let N_1 and N_2 be the matrices obtained from M_1 and M_2 by replacing the diagonal entries, y, of M, by

$$\begin{array}{cccc}
x_1 & x_2 & x_3 & y \\
x_2 & x_1 & y & x_3 \\
x_3 & y & x_1 & x_2 \\
y & x_3 & x_2 & x_1
\end{array}$$

and the off diagonal block entries $p\ q\ r\ s$ of M_i by

$$\begin{array}{cccc}
p & q & r & s \\
q & \bar{p} & s & \bar{r} \\
r & s & \bar{p} & q \\
s & \bar{r} & q & p.
\end{array}$$

Then N_1 and N_2 give orthogonal designs

$$OD(24;1,1,1,1,1,5,5,9) \quad \text{and} \quad OD(24;1,1,1,1,1,2,8,9)$$

respectively. Thus a $OD(24:1,1,1,1,1,19)$ exists.

First rows to construct orthogonal designs of order 24 are given in Robinson [80, p.375] , Holzmann and Kharaghani [100, p.113] and Geramita and Seberry [80, p.376-377].

Table A.3 Existence of 8 variable orthogonal designs of order 24

(1,1,1,1,1,1,1,1): 8	✓	(1,1,1,1,2,2,8,8): 24	✓	(1,1,2,2,2,2,5,5): 20	
(1,1,1,1,1,1,1,4): 11	✓	(1,1,1,1,2,3,4,6): 19		(1,1,2,2,2,3,4,6): 21	
(1,1,1,1,1,1,1,9): 16		(1,1,1,1,2,3,6,9): 24		(1,1,2,2,2,4,4,8): 24	
(1,1,1,1,1,1,2,2): 10		(1,1,1,1,2,4,4,8): 22		(1,1,2,2,3,3,3,3): 18	
(1,1,1,1,1,1,2,8): 16		(1,1,1,1,2,5,5,8): 24		(1,1,2,2,3,3,6,6): 24	✓
(1,1,1,1,1,1,4,4): 14	✓	(1,1,1,1,3,3,3,3): 16		(1,1,2,2,4,4,4,4): 22	✓
(1,1,1,1,1,1,4,9): 19		(1,1,1,1,3,3,6,6): 22		(1,1,2,2,4,4,5,5): 24	
(1,1,1,1,1,1,5,5): 16		(1,1,1,1,4,4,4,4): 20	✓	(1,1,2,3,3,3,3,8): 24	
(1,1,1,1,1,1,8,8): 22		(1,1,1,1,4,4,5,5): 22		(1,1,3,3,3,3,4,4): 22	
(1,1,1,1,1,1,9,9): 24	✓	(1,1,1,1,5,5,5,5): 24	✓	(1,1,3,3,3,3,5,5): 24	
(1,1,1,1,1,2,2,4): 13		(1,1,1,2,2,2,2,4): 15		(1,2,2,2,2,2,2,4): 17	
(1,1,1,1,1,2,2,9): 18		(1,1,1,2,2,2,2,9): 20		(1,2,2,2,2,2,2,9): 22	
(1,1,1,1,1,2,3,6): 16		(1,1,1,2,2,2,3,6): 18		(1,2,2,2,2,2,3,6): 20	
(1,1,1,1,1,2,4,8): 19		(1,1,1,2,2,2,4,8): 21		(1,2,2,2,2,4,4,4): 21	
(1,1,1,1,1,2,8,9): 24	✓	(1,1,1,2,2,3,6,8): 24		(1,2,2,2,3,4,4,6): 24	
(1,1,1,1,1,3,6,8): 22		(1,1,1,2,2,4,4,4): 19		(1,2,2,3,3,3,3,4): 21	
(1,1,1,1,1,4,4,4): 17	✓	(1,1,1,2,2,4,4,9): 24		(1,2,3,3,3,3,3,6): 24	
(1,1,1,1,1,4,4,9): 22		(1,1,1,2,2,4,5,5): 21		(2,2,2,2,2,2,2,2): 16	✓
(1,1,1,1,1,4,5,5): 19		(1,1,1,2,3,4,4,6): 22		(2,2,2,2,2,2,2,8): 22	
(1,1,1,1,1,5,5,9): 24	✓	(1,1,1,2,3,5,5,6): 24		(2,2,2,2,2,2,4,4): 20	
(1,1,1,1,2,2,2,2): 12	✓	(1,1,1,3,3,3,3,4): 19		(2,2,2,2,2,2,5,5): 22	
(1,1,1,1,2,2,2,8): 18		(1,1,1,3,3,3,3,9): 24		(2,2,2,2,3,3,3,3): 20	
(1,1,1,1,2,2,4,4): 16		(1,1,2,2,2,2,2,2): 14		(2,2,2,2,4,4,4,4): 24	✓
(1,1,1,1,2,2,4,9): 21		(1,1,2,2,2,2,2,8): 20		(2,2,3,3,3,3,4,4): 24	
(1,1,1,1,2,2,5,5): 18		(1,1,2,2,2,2,4,4): 18	✓	(3,3,3,3,3,3,3,3): 24	✓

We now summarize the known results for order 24.

1. Table A.3 lists the 75 8-tuples which are not prohibited from being the type of an orthogonal design in order 24 (the number after the type is the sum of the type numbers). The programme which gave this was devised by Roger Magoon while he was an undergraduate at Queen's University. A "✓" indicates the design has been constructed.
2. Table A.4 show the $OD(24:s_1\ldots,s_7)$ that exist (see Geramita and Seberry [80, p.390] and use Table 3 from Holzmann and Kharaghani [100, p.109].
3. Table A.5 lists the 7-tuples cannot be the type of an orthogonal design in order 24:

Table A.4 Existence of 7 variable orthogonal designs of order 24

1,1,1,1,1,1,1	1,1,1,1,1,9,10	1,1,1,2,2,8,9	1,1,2,3,3,6,8
1,1,1,1,1,1,2	1,1,1,1,2,2,2	1,1,1,2,3,8,8	1,1,2,3,5,6,6
1,1,1,1,1,1,4	1,1,1,1,2,2,4	1,1,1,2,4,4,4	1,1,2,5,5,5,5
1,1,1,1,1,1,5	1,1,1,1,2,2,8	1,1,1,2,5,5,9	1,1,3,3,4,6,6
1,1,1,1,1,1,9	1,1,1,1,2,2,16	1,1,1,4,4,4,4	1,2,2,2,2,4,4
1,1,1,1,1,1,18	1,1,1,1,2,8,8	1,1,1,4,4,4,5	1,2,2,2,2,4,5
1,1,1,1,1,2,4	1,1,1,1,2,8,9	1,1,1,5,5,5,5	1,2,2,2,3,4,4
1,1,1,1,1,2,8	1,1,1,1,2,8,10	1,1,1,5,5,5,6	1,2,2,3,3,6,6
1,1,1,1,1,2,9	1,1,1,1,2,9,9	1,1,2,2,2,2,2	1,2,2,3,3,6,7
1,1,1,1,1,2,17	1,1,1,1,3,8,9	1,1,2,2,2,2,4	1,2,2,3,4,6,6
1,1,1,1,1,4,4	1,1,1,1,4,4,4	1,1,2,2,2,2,8	1,2,3,3,3,6,6
1,1,1,1,1,4,5	1,1,1,1,4,4,5	1,1,2,2,2,4,4	2,2,2,2,2,2,2
1,1,1,1,1,4,8	1,1,1,1,4,4,8	1,1,2,2,2,4,6	2,2,2,2,2,2,4
1,1,1,1,1,5,5	1,1,1,1,4,8,8	1,1,2,2,2,8,8	2,2,2,2,2,4,4
1,1,1,1,1,5,6	1,1,1,1,5,5,5	1,1,2,2,3,3,6	2,2,2,2,4,4,4
1,1,1,1,1,5,9	1,1,1,1,5,5,9	1,1,2,2,3,3,12	2,2,2,2,4,4,8
1,1,1,1,1,5,14	1,1,1,1,5,5,10	1,1,2,2,3,6,6	2,2,2,3,3,6,6
1,1,1,1,1,8,9	1,1,1,1,5,6,9	1,1,2,2,3,6,9	2,2,2,4,4,4,6
1,1,1,1,1,8,11	1,1,1,2,2,2,2	1,1,2,2,4,4,4	2,2,4,4,4,4,4
1,1,1,1,1,9,9	1,1,1,2,2,2,3	1,1,2,2,6,6,6	3,3,3,3,3,3,3
		1,1,2,3,3,6,6	3,3,3,3,3,3,6

Table A.5 7 variable designs not orthogonal designs of order 24

$1,1,1,1,1,a,7$	$a = 1,2,\ldots,12$	1,1,1,1,1,3,4
$1,1,1,1,1,b,15$	$b = 1,2,3,4$	1,1,1,1,1,3,12
1,1,1,1,1,1,14		1,1,1,1,1,4,11
1,1,1,1,1,2,15		1,1,1,1,1,5,10
1,1,1,1,1,2,13		1,1,1,1,1,6,9
		1,1,1,1,1,7,8

4. The following 6 tuples do not correspond to the type of an orthogonal design.

$$1,1,1,1,1,7 \qquad 1,1,1,1,1,15 \qquad 2,2,2,2,2,14\,.$$

5. Some 5 variable designs which have not been derived from 7,8,9 variable designs are given in Wallis [238] and listed in Table A.6.

Table A.6 5 variable designs in order 24 not derived from 7,8,9 variable designs

1,2,6,6,9	1,4,5,6,6	1,3,5,6,9	1,3,4,5,9	1,2,5,5,8
1,2,4,5,10	1,2,5,5,9	1,2,3,5,13	1,2,2,3,16	1,2,2,8,8
1,2,5,6,10	2,2,5,5,8	1,2,3,4,12	1,2,2,8,11	1,2,2,4,13
			1,1,4,4,5	1,2,2,5,14

6. The $OD(24;1,1,2,2,3,3,6,6)$ of Table A.7 and the $OD(24;4,4,5,11)$ of Table A.8 are found using the results from Geramita and Seberry [80, p.391], Robinson [80, p.375], Holzmann and Kharaghani [100, p.110-112]. Hence all full $OD(24:a,b,c,24-a-b-c)$, $0 \le a+b+c \le 24$, exist.
7. ≤ 3 Variables: All $OD(24:a,b,c)$, $OD(24:a,b)$ and $OD(24:a)$ exist, $0 \le a \le b \le c \le 24$.

Table A.7 Holzmann-Kharaghani $OD(24;1,1,2,2,3,3,6,6)$ [a]

$$\begin{bmatrix}
a & d & \bar{d} & g & h & h & \bar{h} & h & e & d & d & c & f & \bar{h} & g & b & \bar{d} & c & \bar{d} & \bar{b} & c & \bar{h} & \bar{f} & g \\
\bar{d} & a & d & h & g & h & h & e & \bar{h} & d & c & d & \bar{h} & g & f & \bar{d} & c & b & \bar{b} & c & \bar{d} & \bar{f} & g & \bar{h} \\
d & \bar{d} & a & h & h & g & e & \bar{h} & h & c & d & d & g & f & \bar{h} & c & b & \bar{d} & c & \bar{d} & \bar{b} & g & \bar{h} & \bar{f} \\
\bar{g} & \bar{h} & \bar{h} & a & d & \bar{d} & d & d & c & h & \bar{h} & \bar{e} & b & \bar{d} & c & \bar{f} & h & \bar{g} & \bar{h} & \bar{f} & g & d & b & \bar{c} \\
\bar{h} & \bar{g} & \bar{h} & \bar{d} & a & d & d & c & d & \bar{h} & \bar{e} & h & \bar{d} & c & b & h & \bar{g} & \bar{f} & \bar{f} & g & \bar{h} & b & \bar{c} & d \\
\bar{h} & \bar{h} & \bar{g} & d & \bar{d} & a & c & d & d & \bar{e} & h & \bar{h} & c & b & \bar{d} & \bar{g} & \bar{f} & h & g & \bar{h} & \bar{f} & \bar{c} & d & b \\
h & \bar{h} & \bar{e} & \bar{d} & \bar{d} & \bar{c} & a & d & \bar{d} & g & h & h & b & d & \bar{c} & \bar{f} & \bar{h} & g & \bar{h} & f & g & d & \bar{b} & \bar{c} \\
\bar{h} & \bar{e} & h & \bar{d} & \bar{c} & \bar{d} & \bar{d} & a & d & h & g & h & d & \bar{c} & b & \bar{h} & g & \bar{f} & f & g & \bar{h} & \bar{b} & \bar{c} & d \\
\bar{e} & h & \bar{h} & \bar{c} & \bar{d} & \bar{d} & d & \bar{d} & a & h & h & g & \bar{c} & b & d & g & \bar{f} & \bar{h} & g & \bar{h} & f & \bar{c} & d & \bar{b} \\
\bar{d} & \bar{d} & \bar{c} & \bar{h} & h & e & \bar{g} & \bar{h} & \bar{h} & a & d & \bar{d} & \bar{f} & \bar{h} & g & \bar{b} & \bar{d} & c & d & \bar{b} & \bar{c} & h & \bar{f} & \bar{g} \\
\bar{d} & \bar{c} & \bar{d} & h & e & \bar{h} & \bar{h} & \bar{g} & \bar{h} & \bar{d} & a & d & \bar{h} & g & \bar{f} & \bar{d} & c & \bar{b} & \bar{b} & \bar{c} & d & \bar{f} & \bar{g} & h \\
\bar{c} & \bar{d} & \bar{d} & e & \bar{h} & h & \bar{h} & \bar{h} & \bar{g} & d & \bar{d} & a & g & \bar{f} & \bar{h} & c & \bar{b} & \bar{d} & \bar{c} & d & \bar{b} & \bar{g} & h & \bar{f} \\
\bar{f} & h & \bar{g} & \bar{b} & d & \bar{c} & \bar{b} & \bar{d} & c & f & h & \bar{g} & a & d & \bar{d} & g & h & h & \bar{h} & h & \bar{e} & d & d & c \\
h & \bar{g} & \bar{f} & d & \bar{c} & \bar{b} & \bar{d} & c & \bar{b} & h & \bar{g} & f & \bar{d} & a & d & h & g & h & h & \bar{e} & \bar{h} & d & c & d \\
\bar{g} & \bar{f} & h & \bar{c} & \bar{b} & d & c & \bar{b} & \bar{d} & \bar{g} & f & h & d & \bar{d} & a & h & h & g & \bar{e} & \bar{h} & h & c & d & d \\
\bar{b} & d & \bar{c} & f & \bar{h} & g & f & h & \bar{g} & b & d & \bar{c} & \bar{g} & \bar{h} & \bar{h} & a & d & \bar{d} & d & d & c & h & \bar{h} & e \\
d & \bar{c} & \bar{b} & \bar{h} & g & f & h & \bar{g} & f & d & \bar{c} & b & \bar{h} & \bar{g} & \bar{h} & \bar{d} & a & d & d & c & d & \bar{h} & e & h \\
\bar{c} & \bar{b} & d & g & f & \bar{h} & \bar{g} & f & h & \bar{c} & b & d & \bar{h} & \bar{h} & \bar{g} & d & \bar{d} & a & c & d & d & e & h & \bar{h} \\
d & b & \bar{c} & h & f & \bar{g} & h & \bar{f} & \bar{g} & \bar{d} & b & c & h & \bar{h} & e & \bar{d} & \bar{d} & \bar{c} & a & d & \bar{d} & g & h & h \\
b & \bar{c} & d & f & \bar{g} & h & \bar{f} & \bar{g} & h & b & c & \bar{d} & \bar{h} & e & h & \bar{d} & \bar{c} & \bar{d} & \bar{d} & a & d & h & g & h \\
\bar{c} & d & b & \bar{g} & h & f & \bar{g} & h & \bar{f} & c & \bar{d} & b & e & h & \bar{h} & \bar{c} & \bar{d} & \bar{d} & d & \bar{d} & a & h & h & g \\
h & f & \bar{g} & \bar{d} & \bar{b} & c & \bar{d} & b & c & \bar{h} & f & g & \bar{d} & \bar{d} & \bar{c} & \bar{h} & h & \bar{e} & \bar{g} & \bar{h} & \bar{h} & a & d & \bar{d} \\
f & \bar{g} & h & \bar{b} & c & \bar{d} & b & c & \bar{d} & f & g & \bar{h} & \bar{d} & \bar{c} & \bar{d} & h & \bar{e} & \bar{h} & \bar{h} & \bar{g} & \bar{h} & \bar{d} & a & d \\
\bar{g} & h & f & c & \bar{d} & \bar{b} & c & \bar{d} & b & g & \bar{h} & f & \bar{c} & \bar{d} & \bar{d} & \bar{e} & \bar{h} & h & \bar{h} & \bar{h} & \bar{g} & d & \bar{d} & a
\end{bmatrix}$$

[a] Holzmann and Kharaghani [100, p110] ©Elsevier

Table A.8 Holzmann-Kharaghani $OD(24;4,4,5,11)$ [a]

c	d	$\bar{d}$	d	d	d	$\bar{d}$	d	c	a	b	c	$\bar{b}$	$\bar{a}$	c	$\bar{d}$	d	c	$\bar{a}$	b	d	a	$\bar{b}$	d
$\bar{d}$	c	d	d	d	d	d	c	$\bar{d}$	b	c	a	$\bar{a}$	c	$\bar{b}$	d	c	$\bar{d}$	b	d	$\bar{a}$	$\bar{b}$	d	a
d	$\bar{d}$	c	d	d	d	c	$\bar{d}$	d	c	a	b	c	$\bar{b}$	$\bar{a}$	c	$\bar{d}$	d	d	$\bar{a}$	b	d	a	$\bar{b}$
$\bar{d}$	$\bar{d}$	$\bar{d}$	c	d	$\bar{d}$	a	b	c	d	$\bar{d}$	$\bar{c}$	$\bar{d}$	d	c	b	a	$\bar{c}$	a	$\bar{b}$	d	a	$\bar{b}$	$\bar{d}$
$\bar{d}$	$\bar{d}$	$\bar{d}$	$\bar{d}$	c	d	b	c	a	$\bar{d}$	$\bar{c}$	d	d	c	$\bar{d}$	a	$\bar{c}$	b	$\bar{b}$	d	a	$\bar{b}$	$\bar{d}$	a
$\bar{d}$	$\bar{d}$	$\bar{d}$	d	$\bar{d}$	c	c	a	b	$\bar{c}$	d	$\bar{d}$	c	$\bar{d}$	d	$\bar{c}$	b	a	d	a	$\bar{b}$	$\bar{d}$	a	$\bar{b}$
d	$\bar{d}$	$\bar{c}$	$\bar{a}$	$\bar{b}$	$\bar{c}$	c	d	$\bar{d}$	d	d	d	$\bar{b}$	a	$\bar{d}$	$\bar{b}$	a	d	$\bar{a}$	$\bar{b}$	c	$\bar{d}$	d	$\bar{c}$
$\bar{d}$	$\bar{c}$	d	$\bar{b}$	$\bar{c}$	$\bar{a}$	$\bar{d}$	c	d	d	d	d	a	$\bar{d}$	$\bar{b}$	a	d	$\bar{b}$	$\bar{b}$	c	$\bar{a}$	d	$\bar{c}$	$\bar{d}$
$\bar{c}$	d	$\bar{d}$	$\bar{c}$	$\bar{a}$	$\bar{b}$	d	$\bar{d}$	c	d	d	d	$\bar{d}$	$\bar{b}$	a	d	$\bar{b}$	a	c	$\bar{a}$	$\bar{b}$	$\bar{c}$	$\bar{d}$	d
$\bar{a}$	$\bar{b}$	$\bar{c}$	$\bar{d}$	d	c	$\bar{d}$	$\bar{d}$	$\bar{d}$	c	d	$\bar{d}$	$\bar{b}$	a	d	b	$\bar{a}$	d	$\bar{d}$	d	$\bar{c}$	a	b	$\bar{c}$
$\bar{b}$	$\bar{c}$	$\bar{a}$	d	c	$\bar{d}$	$\bar{d}$	$\bar{d}$	$\bar{d}$	$\bar{d}$	c	d	a	d	$\bar{b}$	$\bar{a}$	d	b	d	$\bar{c}$	$\bar{d}$	b	$\bar{c}$	a
$\bar{c}$	$\bar{a}$	$\bar{b}$	c	$\bar{d}$	d	$\bar{d}$	$\bar{d}$	$\bar{d}$	d	$\bar{d}$	c	d	$\bar{b}$	a	d	b	$\bar{a}$	$\bar{c}$	$\bar{d}$	d	$\bar{c}$	a	b
b	a	$\bar{c}$	d	$\bar{d}$	$\bar{c}$	b	$\bar{a}$	d	b	$\bar{a}$	$\bar{d}$	c	d	$\bar{d}$	d	d	d	$\bar{d}$	d	$\bar{c}$	b	a	c
a	$\bar{c}$	b	$\bar{d}$	$\bar{c}$	d	$\bar{a}$	d	b	$\bar{a}$	$\bar{d}$	b	$\bar{d}$	c	d	d	d	d	d	$\bar{c}$	$\bar{d}$	a	c	b
$\bar{c}$	b	a	$\bar{c}$	d	$\bar{d}$	d	b	$\bar{a}$	$\bar{d}$	b	$\bar{a}$	d	$\bar{d}$	c	d	d	d	$\bar{c}$	$\bar{d}$	d	c	b	a
d	$\bar{d}$	$\bar{c}$	$\bar{b}$	$\bar{a}$	c	b	$\bar{a}$	$\bar{d}$	$\bar{b}$	a	$\bar{d}$	$\bar{d}$	$\bar{d}$	$\bar{d}$	c	d	$\bar{d}$	b	a	c	d	$\bar{d}$	c
$\bar{d}$	$\bar{c}$	d	$\bar{a}$	c	$\bar{b}$	$\bar{a}$	$\bar{d}$	b	a	$\bar{d}$	$\bar{b}$	$\bar{d}$	$\bar{d}$	$\bar{d}$	$\bar{d}$	c	d	a	c	b	$\bar{d}$	c	d
$\bar{c}$	d	$\bar{d}$	c	$\bar{b}$	$\bar{a}$	$\bar{d}$	b	$\bar{a}$	$\bar{d}$	$\bar{b}$	a	$\bar{d}$	$\bar{d}$	$\bar{d}$	d	$\bar{d}$	c	c	b	a	c	d	$\bar{d}$
a	$\bar{b}$	$\bar{d}$	$\bar{a}$	b	$\bar{d}$	a	b	$\bar{c}$	d	$\bar{d}$	c	d	$\bar{d}$	c	$\bar{b}$	$\bar{a}$	$\bar{c}$	c	d	$\bar{d}$	d	d	d
$\bar{b}$	$\bar{d}$	a	b	$\bar{d}$	$\bar{a}$	b	$\bar{c}$	a	$\bar{d}$	c	d	$\bar{d}$	c	d	$\bar{a}$	$\bar{c}$	$\bar{b}$	$\bar{d}$	c	d	d	d	d
$\bar{d}$	a	$\bar{b}$	$\bar{d}$	$\bar{a}$	b	$\bar{c}$	a	b	c	d	$\bar{d}$	c	d	$\bar{d}$	$\bar{c}$	$\bar{b}$	$\bar{a}$	d	$\bar{d}$	c	d	d	d
$\bar{a}$	b	$\bar{d}$	$\bar{a}$	b	d	d	$\bar{d}$	c	$\bar{a}$	$\bar{b}$	c	$\bar{b}$	$\bar{a}$	$\bar{c}$	$\bar{d}$	d	$\bar{c}$	$\bar{d}$	$\bar{d}$	$\bar{d}$	c	d	$\bar{d}$
b	$\bar{d}$	$\bar{a}$	b	d	$\bar{a}$	$\bar{d}$	c	d	$\bar{b}$	c	$\bar{a}$	$\bar{a}$	$\bar{c}$	$\bar{b}$	d	$\bar{c}$	$\bar{d}$	$\bar{d}$	$\bar{d}$	$\bar{d}$	$\bar{d}$	c	d
$\bar{d}$	$\bar{a}$	b	d	$\bar{a}$	b	c	d	$\bar{d}$	c	$\bar{a}$	$\bar{b}$	$\bar{c}$	$\bar{b}$	$\bar{a}$	$\bar{c}$	$\bar{d}$	d	$\bar{d}$	$\bar{d}$	$\bar{d}$	d	$\bar{d}$	c

[a] Holzmann and Kharaghani [100, p112] ©Elsevier

A.5 Orthogonal Designs in Order 48

There are 73056 possible 8-tuples, 58844 possible 7-tuples, 41024 possible 6-tuples, 23532 possible 5-tuples, 10359 possible 4-tuples, 3164 possible 3-tuples, and 575 possible 2-tuples, before theory is applied to eliminate cases, which might give orthogonal designs in order 48.

We now summarize the known results for order 48. Using a wide variety of construction techniques Holzmann-Kharaghani-Seberry-Tayef-Rezaie [104] have made significant progress into surveying the existence of orthogonal designs in order 48.

1. Theory tells us there are at most 9 variables. The 60 known 9 variable designs listed in [104, p.13]are given in Table A.9.
2. There are 459 known 8 variable designs given in [104, p.14–17].
3. There are 20 known 7 variable designs given in [104, p.17].
4. There are 168 known 6 variable designs given in [104, p.18–19].
5. There are 24 known 5 variable designs given in [104, p.19].
6. This case does not appear to have been published.
7. All the 3-tuples, 2-tuples and 1-tuple are the type of orthogonal design.

Table A.9 9-Variable designs in order 48 [a]

9 – Variables									Ref
1	1	1	1	1	1	1	1	1	Th2, I
1	1	1	1	1	1	1	1	2	16b
1	1	1	1	1	1	1	1	4	Th2, II
1	1	1	1	1	1	1	1	8	16d
1	1	1	1	1	1	1	2	4	Th9, 16b
1	1	1	1	1	1	1	4	4	Th2 II
1	1	1	1	1	1	1	4	8	Th9, 16d
1	1	1	1	1	1	1	9	9	Th2, III
1	1	1	1	1	1	2	2	2	16e
1	1	1	1	1	1	2	2	8	Th9, 16e
1	1	1	1	1	1	2	8	9	Th2, IV
1	1	1	1	1	1	4	4	4	Th2, V
1	1	1	1	1	1	5	5	9	Th2, VI
1	1	1	1	1	1	9	9	9	Th2, III
1	1	1	1	1	1	9	9	18	Th8
1	1	1	1	1	2	2	2	2	16f
1	1	1	1	1	2	2	2	4	Th9, 16e
1	1	1	1	1	2	2	2	8	Th9, 16f
1	1	1	1	1	2	2	8	9	Th2. IV
1	1	1	1	1	2	3	3	3	16g
1	1	1	1	1	2	3	3	12	Th9. 16g
1	1	1	1	1	2	8	8	9	Th2. IV
1	1	1	1	1	2	8	9	9	Th2. IV
1	1	1	1	1	4	4	4	4	Th2. V
1	1	1	1	1	5	5	5	9	Th2, VI
1	1	1	1	1	5	5	9	9	Th2, VI
1	1	1	1	2	2	2	2	2	16h
1	1	1	1	2	2	2	2	4	Th9, 16f
1	1	1	1	2	2	2	2	8	Th9, 16g
1	1	1	1	2	3	3	3	4	Th9, 16h

9 – Variables									Ref
1	1	1	1	2	3	3	3	9	Th9
1	1	1	1	4	4	4	4	4	Th2. VII
1	1	1	2	2	2	2	2	4	Th9. 16h
1	1	1	2	2	2	2	2	8	16f
1	1	1	2	2	2	9	9	9	Th8
1	1	1	2	2	2	9	9	18	Th8
1	1	1	2	2	3	3	3	8	16g
1	1	1	3	3	3	9	9	9	Th8
1	1	1	3	3	3	9	9	18	Th8
1	1	2	2	2	2	2	2	2	Th2, I
1	1	2	2	2	2	2	2	8	Th2. II
1	1	2	2	2	2	2	18	18	Th2. III
1	1	2	2	2	2	4	16	18	Th2, IV
1	1	2	2	2	2	8	8	8	Th2, V
1	1	2	2	2	2	10	10	18	Th2, VI
1	1	2	2	2	8	8	8	8	Th2, VII
1	2	2	2	2	2	2	2	4	Th9, 16i
1	3	3	3	3	3	3	3	3	Th10, VIII
2	2	2	2	2	2	2	2	8	16i
2	2	2	2	2	2	2	4	4	Th2, II
2	2	2	2	2	2	2	16	18	Th2, IV
2	2	2	2	2	2	9	9	18	Th2, III
2	2	2	2	2	4	4	8	8	Th2, V
2	2	2	2	2	4	8	8	18	Th2, IV
2	2	2	2	2	4	9	9	16	Th2, IV
2	2	2	2	2	5	5	10	18	Th2, VI
2	2	2	2	2	9	9	10	10	Th2, VI
2	2	2	2	4	4	8	8	8	Th2, VII
3	3	3	3	3	3	3	3	3	Th2, VIII
3	3	6	6	6	6	6	6	6	Th2, VIII

[a] Holzmann, Kharaghani, Seberry and Tayef-Rezaie [104, p321] ©Elsevier

Appendix B
Orthogonal Designs in Order 20, 40 and 80

B.1 Some Theorems

Lemma B.1. *All 3-tuples* $(a,b,40-a-b)$ *are the types of orthogonal designs in order 40. Hence all 2-tuples* (x,y) *are the types of orthogonal designs in order 40.*

Lemma B.2. *All triples* (a,b,c) *are types of orthogonal designs* $OD(40;a,b,c)$.

Lemma B.3. *All full orthogonal designs* $OD(2^t5;x,y,2^t5-x-y)$ *exist for any positive integer* $t \geq 3$.

B.2 Orthogonal designs in Order 20

We now summarize the known results for order 20

1. Table B.1 gives all the 4 variable orthogonal designs known in order 20 and the first rows that may be used in the Goethals-Seidel array to generate them.
2. For the following 4-tuples it is undecided whether and orthogonal design exists:
$$(1,3,6,8) \qquad (1,4,4,9) \qquad (2,2,5,5)$$
It is not possible to construct designs of these types using the Goethals-Seidel array (Eades).
All other 4-tuples are *not* the types of orthogonal designs.
3. Of the possible 3-tuples Table B.2 lists the 97 that are the types of orthogonal designs (all are constructed using four circulant matrices in the Goethals-Seidel array)
It is undecided whether an orthogonal design exists for the 3-tuple $(3,7,8)$. It cannot be constructed using 4 circulant matrices in the Goethals-Seidel array (Eades).

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5

All other 3-tuples are *not* the types of orthogonal designs.

4. Table B.3 lists the eighty-six (86) 2-tuples are the types of orthogonal designs. All other 2-tuples correspond to non-existent designs. All those that exist are constructed using four circulant matrices in the Goethals-Seidel array.
5. All one variable designs exist in order 20.

B.3 Orthogonal designs in Order 40

We now summarize the known results for order 40.

1. It is a simple matter to find results in n-variables where $3 \leq n \leq 8$ but except for those listed below this has not been done.
   Combining the results of Holzmann and Kharaghani [102] with those of Geramita and Seberry [80, p.380] and Wallis [238], we have the full orthogonal designs that exist in order 40 given in Table B.4.
   The designs are constructed by using the matrices whose first rows are given in Table B.5 in the $(1,1,1,1,1,1,1,1)$ design in order 8; we use the back-circulant matrix constructed from X_1, and the circulant matrices constructed from the other X_i, $i = 2,3,\ldots,8$. Note that $(1,2,3,34)$ is constructed from Lemma 4.20 (iii).
2. Holzmann, Kharaghani and Tayfeh-Rezaie [105] have used amicable sets to show that the following 7- and 6-tuples are the types of orthogonal designs in order 40:
   $$1,1,2,2,17,17$$
   $$1,1,1,2,9,26$$
   $$2,2,2,2,2,2,8$$
   They are not derivable from known 8- and 7-tuples which exist.
3. We shall not list the 8-tuples which are not prohibited from being the type of orthogonal design in order 40 since Magoon's programme yields 703 possibilities.
4. The seven variable designs remain to be studied.
5. The following 6-tuple is the type of an orthogonal design which exists in order 40:
   $$(1,2,2,2,16,17)\,.$$
6. The following 5-tuples correspond to orthogonal designs which exist in order 40:
   $$\begin{array}{lll} (1,1,1,4,20) & (1,2,2,4,25) & (1,4,8,8,16) \\ (1,1,8,8,9) & (1,2,2,11,24) & (1,8,8,8,8) \\ (1,2,6,9,20) & (1,4,9,9,9) & (1,2,2,2,33) \end{array}\,.$$

Table B.1 Orthogonal designs of order 20

Design	A_1	A_2	A_3	A_4
$(1,1,1,1)$	$a0000$	$b0000$	$c0000$	$d0000$
$(1,1,1,4)$	$a0000$	$b0000$	$c0d\bar{d}0$	$00dd0$
$(1,1,1,9)$	$a0d\bar{d}0$	$b0d\bar{d}0$	$c\bar{d}00d$	$ddd00$
$(1,1,2,2)$	$a0000$	$b0000$	$cd000$	$d\bar{c}000$
$(1,1,2,8)$	$a0d\bar{d}0$	$b0d\bar{d}0$	$c0dd0$	$\bar{c}0dd0$
$(1,1,4,4)$	$a0c\bar{c}0$	$00cc0$	$b0d\bar{d}0$	$00dd0$
$(1,1,4,9)$	$a0d\bar{d}0$	$b0d\bar{d}0$	$0dccd\bar{}$	$ddc\bar{c}d$
$(1,1,5,5)$	$a0c\bar{c}0$	$b0d\bar{d}0$	$c0dd0$	$\bar{d}0cc0$
$(1,1,8,8)$	$acdd\bar{c}$	$bc\bar{d}d\bar{c}$	$0cddc$	$0c\bar{d}\bar{d}c$
$(1,1,9,9)$	$acdd\bar{c}$	$bd\bar{c}c\bar{d}$	$\bar{c}cccc$	$\bar{d}dddd$
$(1,2,2,4)$	$a0d\bar{d}0$	$00dd0$	$bc000$	$c\bar{b}000$
$(1,2,2,9)$	$ad00\bar{d}$	$ddd00$	$bcd\bar{d}0$	$c\bar{b}0d\bar{d}$
$(1,2,3,6)$	$a0d\bar{d}0$	$bc0d0$	$b\bar{c}0\bar{d}0$	$c0\bar{d}\bar{d}0$
$(1,2,4,8)$	$a0d\bar{d}0$	$bcdd\bar{c}$	$b0\bar{d}\bar{d}0$	$d\bar{d}c0c$
$(1,2,8,9)$	$adc\bar{c}\bar{d}$	$dddc\bar{c}$	$cbd\bar{d}c$	$b\bar{c}\bar{c}d\bar{d}$
$(1,3,6,8)$	if it exists it cannot be constructed from circulants			
$(1,4,4,4)$	$a0b\bar{b}0$	$00bb0$	$0cd\bar{d}c$	$0cdd\bar{c}$
$(1,4,4,9)$	if it exists it cannot be constructed from circulants			
$(1,4,5,5)$	$ad00\bar{d}$	$\bar{d}c00c$	$cdb\bar{b}d$	$0cbb\bar{c}$
$(1,5,5,9)$	$abc\bar{c}\bar{b}$	$\bar{c}bd\bar{d}b$	$bdcc\bar{d}$	$\bar{d}dddd$
$(2,2,2,2)$	$ab000$	$b\bar{a}000$	$cd000$	$d\bar{c}000$
$(2,2,2,8)$	$adbd\bar{}0$	$ad\bar{b}d0$	$c0d0d$	$c0\bar{d}0\bar{d}$
$(2,2,4,4)$	$ab000$	$b\bar{a}000$	$0cd\bar{d}c$	$0cdd\bar{c}$
$(2,2,4,9)$	$abdd\bar{}0$	$a\bar{b}dd\bar{}0$	$0dccd\bar{}$	$ddc\bar{c}d$
$(2,2,5,5)$	if it exists it cannot be constructed from circulants			
$(2,2,8,8)$	$adcd\bar{c}$	$ad\bar{c}d\bar{c}$	$bc\bar{d}cd$	$b\bar{c}d\bar{c}\bar{d}$
$(2,3,4,6)$	$bda00$	$bd\bar{a}00$	$\bar{b}dc\bar{c}d$	$0dccd\bar{}$
$(2,3,6,9)$	$bdcad\bar{}$	$add\bar{b}\bar{c}$	$\bar{b}dd\bar{c}d$	$ddc\bar{c}d$
$(2,4,4,8)$	$c0bdd$	$c0bd\bar{d}$	$ba\bar{c}d\bar{d}$	$b\bar{a}\bar{c}d\bar{d}$
$(2,5,5,8)$	$cbdd\bar{b}$	$acddc\bar{}$	$\bar{a}bddbarb$	$\bar{b}cdd\bar{c}$
$(3,3,3,3)$	$abc00$	$a\bar{b}0d0$	$a0\bar{c}d0$	$b\bar{c}d00$
$(3,3,6,6)$	$0d\bar{a}c\bar{b}$	$0da\bar{c}\bar{b}$	$bcdd\bar{c}$	$acdd\bar{c}$
$(4,4,4,4)$	$0ab\bar{b}a$	$0abb\bar{a}$	$0cdd\bar{c}$	$0cdd\bar{c}$
$(4,4,5,5)$	$dca\bar{a}c$	$0daad\bar{}$	$0cbb\bar{c}$	$\bar{c}db\bar{b}d$
$(5,5,5,5)$	$abbdd\bar{}$	$\bar{b}aac\bar{c}$	$dcc\bar{a}a$	$\bar{c}ddb\bar{b}b$
$(1,1,13)$	$ac\bar{c}c\bar{c}$	$0c\bar{c}\bar{c}\bar{c}$	$bc00\bar{c}$	$0ccc0$
$(1,2,17)$	$acbarcc\bar{c}$	$bcc\bar{c}\bar{c}$	$b\bar{c}ccc$	$c\bar{c}\bar{c}\bar{c}\bar{c}$
$(1,2,11)$	$a0c\bar{c}0$	$b0c\bar{c}\bar{c}$	$b0\bar{c}cc$	$0c0cc$
$(1,3,14)$	$ac\bar{c}c\bar{c}$	$\bar{b}ccc0$	$cccb\bar{c}$	$cc\bar{c}0b$
$(1,4,13)$	$ac\bar{c}c\bar{c}$	$0c\bar{c}\bar{c}\bar{c}$	$0cbb\bar{c}$	$bccc\bar{b}$
$(1,6,11)$	$acb\bar{b}\bar{c}$	$ccbb\bar{c}$	$c\bar{b}cc0$	$c0c\bar{c}b$
$(1,8,11)$	$ac\bar{b}b\bar{c}$	$\bar{c}cbb\bar{c}$	$c\bar{b}ccb$	$cbc\bar{c}b$
$(2,5,7)$	$cc\bar{c}0\bar{a}$	$acb\bar{b}0$	$bb0c0$	$c\bar{b}0c0$
$(3,6,8)$	$0bc\bar{b}\bar{c}$	$0bcac$	$ab\bar{c}0\bar{c}$	$a\bar{b}c\bar{b}\bar{c}$
$(3,7,8)$	not yet decided			
$(7,10)$	$0aa\bar{b}\bar{b}$	$baa\bar{a}a$	$0aa\bar{a}b$	$b0b\bar{b}a$
(9)	$\bar{a}aaaa$	$0a\bar{a}\bar{a}a$		

Table B.2 Known 3 variable designs in order 20

(1,1,1)	(1,2,6)	(1,4,13)	(2,2,5)	(2,4,8)	(2,9,9)	(4,4,9)
(1,1,2)	(1,2,8)	(1,5,5)	(2,2,8)	(2,4,9)	(3,3,3)	(4,4,10)
(1,1,4)	(1,2,9)	(1,5,6)	(2,2,9)	(2,4,11)	(3,3,6)	(4,5,5)
(1,1,5)	(1,2,11)	(1,5,9)	(2,2,10)	(2,4,12)	(3,3,12)	(4,5,6)
(1,1,8)	(1,2,12)	(1,5,14)	(2,2,13)	(2,5,5)	(3,4,6)	(4,5,9)
(1,1,9)	(1,2,17)	(1,6,8)	(2,2,16)	(2,5,7)	(3,4,8)	(4,6,8)
(1,1,10)	(1,3,6)	(1,6,11)	(2,3,4)	(2,5,8)	(3,6,6)	(4,8,8)
(1,1,13)	(1,3,8)	(1,8,8)	(2,3,6)	(2,5,13)	(3,6,8)	(5,5,5)
(1,1,16)	(1,3,14)	(1,8,9)	(2,3,7)	(2,6,7)	(3,6,9)	(5,5,8)
(1,1,18)	(1,4,4)	(1,8,11)	(2,3,9)	(2,6,9)	(3,6,11)	(5,5,9)
(1,2,2)	(1,4,5)	(1,9,9)	(2,3,10)	(2,6,12)	(3,8,9)	(5,5,10)
(1,2,3)	(1,4,8)	(1,9,10)	(2,3,15)	(2,8,8)	(4,4,4)	(5,6,9)
(1,2,4)	(1,4,9)	(2,2,2)	(2,4,4)	(2,8,9)	(4,4,5)	(5,7,8)
	(1,4,10)	(2,2,4)	(2,4,6)	(2,8,10)	(4,4,8)	(6,6,6)

Table B.3 Known 2 variable designs in order 20

(1,1)	(1,14)	(2,9)	(3,7)	(4,8)	(5,9)	(7,8)
(1,2)	(1,16)	(2,10)	(3,8)	(4,9)	(5,10)	(7,10)
(1,3)	(1,17)	(2,11)	(3,9)	(4,10)	(5,13)	(7,11)
(1,4)	(1,18)	(2,12)	(3,10)	(4,11)	(5,14)	(7,13)
(1,5)	(1,19)	(2,13)	(3,11)	(4,12)	(5,15)	(8,8)
(1,6)	(2,2)	(2,15)	(3,12)	(4,13)	(6,6)	(8,9)
(1,8)	(2,3)	(2,16)	(3,14)	(4,14)	(6,7)	(8,10)
(1,9)	(2,4)	(2,17)	(3,15)	(4,16)	(6,8)	(8,11)
(1,10)	(2,5)	(2,18)	(3,17)	(5,5)	(6,9)	(8,12)
(1,11)	(2,6)	(3,3)	(4,4)	(5,6)	(6,11)	(9,9)
(1,12)	(2,7)	(3,4)	(4,5)	(5,7)	(6,12)	(9,10)
(1,13)	(2,8)	(3,6)	(4,6)	(5,8)	(6,14)	(9,11)
					(7,7)	(10,10)

7. The following 4-tuples correspond to orthogonal designs which exist in order 40:

(1,1,15,23)	(1,2,16,19)	(1,10,14,15)	(2,8,12,18)
(1,2,3,34)	(1,8,12,19)	(2,2,5,31)	(2,10,10,13)
(1,2,10,27)	(1,9,13,15)	(2,2,14,22)	(5,8,12,15)
(1,2,12,25)	(1,10,10,17)	(2,4,11,16)	(5,9,9,15)
(1,2,14,23)	(1,10,10,19)	(2,4,13,21)	(8,10,10,12)

.

8. Holzmann, Kharaghani, Tayfeh-Rezaie [105] give all 1841 possible 3 variable designs. Hence all 2 and 1 variable designs exist.

9. Koukouvinos and Seberry [129] give the following 3-variable designs constructed using NPAF sequences in the Goethals-Seidel array

$$(2,2,34) \quad (2,4,32) \quad (2,12,22)\,.$$

10. Many other orthogonal designs of orders 40 and 80 are given in [102].

Table B.4 The full orthogonal designs that exist in order 40

$(1,2,2,2,16,17)$;	$(1,2,10,27)$;	$(1,1,10,10,18)$;
$(1,10,14,15)$;	$(2,4,13,21)$;	$(1,2,14,23)$;
$(2,2,14,22)$;	$(2,2,5,31)$;	$(1,1,1,1,9,9,9,9)$;
$(1,2,3,34)$;	$(1,2,2,11,24)$;	$(2,2,2,2,8,8,8,8)$;
$(1,8,12,19)$;	$(1,2,12,25)$;	$(2,2,5,5,5,5,8,8)$;
$(5,8,12,15)$;	$(1,10,10,19)$	$(5,5,5,5,5,5,5,5)$

Table B.5 First rows - circulant matrices $OD(40; s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8)$, $\sum_{i=1}^{8} s_i \leq 40$

Design	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8
(1,2,2,2,16,17)	$faa\bar{a}\bar{a}$	$a\bar{a}aa\bar{a}$	$eb\bar{b}\bar{b}b$	$\bar{e}b\bar{b}\bar{b}b$	$da\bar{b}\bar{b}a$	$\bar{d}a\bar{b}\bar{b}a$	$cbaab$	$\bar{c}baab$
(1,10,14,15)	$dbb\bar{b}\bar{b}$	$\bar{b}bb\bar{b}\bar{b}$	$babba$	$aab\bar{b}a$	$b\bar{a}aa\bar{a}$	$ca\bar{a}\bar{a}a$	$\bar{a}c\bar{c}\bar{c}c$	$\bar{c}cccc$
(2,2,14,22)	$cb\bar{b}\bar{b}b$	$\bar{c}b\bar{b}\bar{b}b$	$da\bar{a}\bar{a}a$	$\bar{d}a\bar{a}\bar{a}a$	$\bar{a}aaaa$	$babba$	$aa\bar{b}\bar{b}a$	$b\bar{a}aa\bar{a}$
(1,2,3,34)	$cb\bar{b}b\bar{b}$	$abb\bar{b}\bar{b}$	$abb\bar{b}\bar{b}$	$abb\bar{b}\bar{b}$	$b\bar{b}b\bar{b}$	$b\bar{b}b\bar{b}$	$dbbbb$	$\bar{d}bbbb$
(1,8,12,19)	$abb\bar{b}\bar{b}$	$b\bar{b}bb\bar{b}$	$\bar{c}dccd$	$dd\bar{c}c\bar{d}$	$dc\bar{c}\bar{c}c$	$\bar{d}dddd$	$\bar{b}bbbb$	$\bar{b}bbbb$
(5,8,12,15)	$aba\bar{a}b$	$b\bar{b}aa\bar{b}$	$\bar{c}dccd$	$dd\bar{c}c\bar{d}$	$dc\bar{c}\bar{c}c$	$\bar{d}dddd$	$\bar{a}aaaa$	$aa\bar{a}\bar{a}a$
(1,2,10,27)	$dbb\bar{b}\bar{b}$	$ab\bar{b}\bar{b}b$	$\bar{a}b\bar{b}\bar{b}b$	$bc\bar{c}\bar{c}c$	$\bar{c}b\bar{b}\bar{b}b$	$\bar{c}cccc$	$b\bar{b}bb\bar{b}$	$bbbbb$
(2,4,13,21)	$\bar{a}abb\bar{a}$	$b\bar{a}bb\bar{a}$	$\bar{c}baab$	$cabba$	$cb\bar{b}\bar{b}b$	$c\bar{a}aa\bar{a}$	$db\bar{b}\bar{b}b$	$db\bar{b}\bar{b}b$
(2,2,5,31)	$aabb\bar{a}$	$ba\bar{b}\bar{b}a$	$b\bar{b}bb\bar{b}$	$cb\bar{b}\bar{b}b$	$\bar{c}b\bar{b}\bar{b}b$	$eb\bar{b}\bar{b}b$	$\bar{e}b\bar{b}\bar{b}b$	$bbbbb$
(1,2,2,11,24)	$add\bar{d}\bar{d}$	$be\bar{e}\bar{e}e$	$\bar{b}e\bar{e}\bar{e}e$	$ce\bar{e}\bar{e}e$	$\bar{c}e\bar{e}\bar{e}e$	$\bar{d}eeee$	$dd\bar{e}e\bar{d}$	$dedde$
(1,2,12,25)	$add\bar{d}\bar{d}$	$cc\bar{c}\bar{c}c$	$\bar{d}dd\bar{d}d$	$\bar{c}dddd$	$c\bar{c}dd\bar{c}$	$cdccd$	$bddd\bar{d}d$	$\bar{b}ddd\bar{d}$
(1,10,10,19)	$add\bar{d}\bar{d}$	$\bar{d}dddd$	$\bar{d}dddd$	$dd\bar{d}dd\bar{d}$	$bc\bar{c}\bar{c}c$	$\bar{c}b\bar{b}\bar{b}b$	$\bar{b}bbbb$	$\bar{c}cccc$
(1,2,14,23)	$bdd\bar{d}\bar{d}$	$\bar{a}c\bar{c}\bar{c}c$	$ac\bar{c}\bar{c}c$	$\bar{d}dd\bar{d}\bar{d}$	$\bar{d}dddd$	$dd\bar{c}\bar{c}d$	$cdccd$	$\bar{c}dd\bar{d}\bar{d}$
(2,10,10,13)	$add\bar{d}\bar{d}$	$a\bar{d}ddd\bar{d}$	$d0dd0$	$00dd0$	$cb\bar{b}\bar{b}b$	$\bar{b}c\bar{c}\bar{c}c$	$\bar{b}bbbb$	$\bar{c}cccc$
(5,9,9,15)	$ada\bar{a}d$	$dd\bar{a}aa\bar{d}$	$\bar{d}dddd$	$dd\bar{d}\bar{d}d$	$0b\bar{b}\bar{b}b$	$\bar{b}bbbb$	$0c\bar{c}\bar{c}c$	$\bar{c}cccc$
(1,2,6,9,20)	$a\bar{e}c\bar{c}e$	$0\bar{e}cc\bar{e}$	$ce\bar{e}\bar{e}e$	$ceeee$	$be\bar{e}\bar{e}e$	$\bar{b}e\bar{e}\bar{e}e$	$0dd\bar{d}\bar{d}d$	$\bar{d}dddd$
(1,2,16,19)	$add\bar{d}\bar{d}$	$\bar{d}dddd$	$\bar{d}dddd$	$dd\bar{d}dd\bar{d}$	$bc\bar{c}\bar{c}c$	$b\bar{c}ccc\bar{c}$	$0c\bar{c}\bar{c}c$	$0cccc$
(1,2,2,4,25)	$a0dd\bar{d}0$	$00dd0$	$be\bar{e}\bar{e}e$	$\bar{b}e\bar{e}\bar{e}e$	$ce\bar{e}\bar{e}e$	$\bar{c}e\bar{e}\bar{e}e$	$0eeee$	$\bar{e}eeee$
(1,4,9,9,9)	$a0b\bar{b}0$	$00bb0$	$0c\bar{c}\bar{c}c$	$\bar{c}cccc$	$0dd\bar{d}\bar{d}d$	$\bar{d}dddd$	$0e\bar{e}\bar{e}e$	$\bar{e}eeee$
(2,8,25)	$bcbb\bar{c}$	$bcbb\bar{c}$	$\bar{b}cbbc$	$\bar{b}\bar{c}bb\bar{c}$	$b\bar{b}00\bar{b}$	$0b00b$	$ab\bar{b}\bar{b}b$	$\bar{a}b\bar{b}\bar{b}b$
(1,10,10,17)	$add\bar{d}\bar{d}$	$dd\bar{d}dd\bar{d}$	$0dddd$	$0dd\bar{d}\bar{d}d$	$bc\bar{c}\bar{c}c$	$\bar{c}b\bar{b}\bar{b}b$	$\bar{b}bbbb$	$\bar{c}cccc$
(2,4,11,16)	$c\bar{c}b\bar{b}\bar{c}$	$00bb0$	$c0cc0$	$cc\bar{c}\bar{c}c$	$add\bar{d}\bar{d}d$	$\bar{a}dd\bar{d}\bar{d}d$	$0dd\bar{d}\bar{d}d$	$0dddd$
(1,4,8,8,16)	$acdd\bar{c}$	$0cd\bar{d}c\bar{c}$	$0ce\bar{e}\bar{c}$	$0c\bar{e}e\bar{c}$	$\bar{b}cddc$	$\bar{b}cdd\bar{c}$	$bceec$	$bc\bar{e}\bar{e}c$
(1,8,8,8,8)	$abc\bar{c}\bar{b}$	$0b\bar{c}c\bar{b}$	$0de\bar{e}\bar{d}$	$0d\bar{e}e\bar{d}$	$0bccb$	$0b\bar{c}\bar{c}b$	$0deed$	$0d\bar{e}\bar{e}d$
(1,1,1,4,20)	$ae00\bar{e}$	$b0000$	$c0000$	$0e00e$	$\bar{d}dddd$	$\bar{d}dddd$	$\bar{d}dd\bar{d}\bar{d}$	$ddd\bar{d}\bar{d}$
(1,1,8,8,9)	$a0000$	$b0000$	$0cc\bar{c}c$	$0ccc\bar{c}$	$\bar{e}eeee$	$0e\bar{e}\bar{e}e$	$0ddd\bar{d}$	$0dddd\bar{}$

B.4 Order 80

We now summarize the known results for order 80.

1. Some results given here are from from Cooper and Seberry [33]. Theory tells us there are at most 9 variables.
2. Table B.6 lists many known orthogonal designs that exist in order 80.
3. The designs cited in Table B.7 should be used in designs in order 16 as follows:

   - for 1)–5) use the $(1,1,2,2,2,2,3,3)$ design found in Section 6.1.1;
   - for 6)–20) use the (1,1,1,1,1,2,3,3,3) design found in Example 6.4.

   In all cases the first row of the circulant matrix is given, if the first row does not give a circulant symmetric matrix the back circulant matrix should be used.
4. The following 6-tuples are the types of orthogonal designs in order 80:

$$\begin{array}{ll} (1,1,1,1,9,10) & (1,1,3,3,10,27) \\ (2,2,3,6,32,35) & (1,1,3,3,9,30)\,. \end{array}$$

5. The following 5-tuples are the types of orthogonal designs in order 80:

$$\begin{array}{lll} (1,1,6,16,43) & (1,4,6,19,50) & (1,4,6,34,35) \\ (2,3,4,18,53) & (2,3,4,35,36) & (2,3,12,28,35) \\ (2,3,14,26,35) & (2,3,16,24,35) & (2,3,20,20,35) \\ (1,1,10,c,d) & (1,1,10,3c,3d) & (3,3,30,c,d) \\ (c,d) \in N = \{(8,12),(10,10),(2,13),(2,16),(2,18),(1,11),(9,9)\} & & \\ (1,1,9,a,b) & (1,1,9,3a,3b) & (3,3,27,a,b) \\ (a,b) \in N \text{ or } (a,b) \in M = \{(4,11),(1,19),(1,17),(1,14),(5,15)\}. & & \end{array}$$

6. The following 4-tuples are the types of orthogonal designs in order 80:

$$\begin{array}{lll} (1,2,18,59) & (1,6,15,58) & \\ (1,2,28,45) & (1,6,28,43) & (1,6,29,44) \\ (a,b,c,d) & (a,b,3c,3d) & (3a,3b,c,d) \\ \text{where } (a,b) \in M, (c,d) \in N \text{ or } (a,b) \in N, (c,d) \in M \bigcup N. & & \\ (4,6,11,54) & (4,11,24,36) & (4,11,30,30)\,. \end{array}$$

7. All 3-tuples $(a,b,80-a-b)$ are the types of orthogonal designs except possibly

$(3,13,64)$	$(7,22,51)$	$(12,27,41)$
$(3,15,62)$	$(7,25,48)$	$(12,29,39)$
$(3,21,56)$	$(7,28,45)$	$(13,23,44)$
$(5,11,64)$	$(8,29,43)$	$(14,19,47)$
$(5,17,58)$	$(9,14,57)$	$(14,27,39)$
$(5,31,44)$	$(9,15,56)$	$(16,21,43)$
$(6,9,65)$	$(9,16,55)$	$(16,23,41)$
$(6,31,43)$	$(9,28,43)$	$(16,25,39)$
$(7,8,65)$	$(10,29,41)$	$(18,23,39)$
$(7,9,64)$	$(11,14,55)$	$(19,28,33)$
$(7,12,61)$	$(11,16,53)$	$(21,22,37)$
$(7,16,57)$	$(11,25,44)$	

which are undecided.

8. All 2-tuples are the types of orthogonal designs except possibly

$$(13,64) \qquad (15,62)\,.$$

9. All one variable designs exist.

Remark B.1 (Research Problem 1). As yet no publication has appeared matching the known OD's in orders 40 and 80 against the existence conditions.

Table B.6 Known orthogonal designs in order 80 [a]

1)	$(1,4,6,19,50)$	8)	$(1,6,28,43)$	15)	$(1,1,6,16,43)$
2)	$(1,4,6,34,35)$	9)	$(1,2,18,59)$	16)	$(2,3,14,26,35)$
3)	$(2,3,16,24,35)$	10)	$(3,10,10,57)$	17)	$(2,2,3,6,32,35)$
4)	$(2,3,4,35,36)$	11)	$(1,14,65)$	18)	$(4,6,11,54)$
5)	$(2,3,20,20,35)$	12)	$(1,6,15,58)$	19)	$(4,11,24,36)$
6)	$(2,3,4,18,53)$	13)	$(1,2,28,45)$	20)	$(4,11,30,30)$
7)	$(2,3,12,28,35)$	14)	$(1,6,29,44)$		

[a] Cooper and Wallis [33, p270-271] © Charles Babbage Research Centre

Table B.7 First rows - circulant matrices $OD(80; s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9)$, $\sum_{i=1}^{9} s_i \leq 80$

Design	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9
(1,4,6,19,50)	$fee\bar{e}\bar{e}$	$e\bar{e}ee\bar{e}$	$\bar{e}eeee$	$db\bar{b}\bar{b}b$	$\bar{d}b\bar{b}\bar{b}b$	$bbbbb$	$ab\bar{b}\bar{b}b$	$\bar{a}b\bar{b}\bar{b}b$	
(1,4,6,24,35)	$ecc\bar{c}\bar{c}$	$c\bar{c}cc\bar{c}$	$\bar{d}c\bar{c}\bar{c}c$	$dc\bar{c}\bar{c}c$	$\bar{b}cccc$	$cbbbb$	$ab\bar{b}\bar{b}b$	$\bar{a}b\bar{b}\bar{b}b$	
(2,3,16,24,35)	$ebbbb$	$\bar{e}bbbb$	$\bar{c}dccd$	$c\bar{c}dd\bar{c}$	$cdd\bar{d}\bar{d}d$	$\bar{c}cccc$	$abb\bar{b}\bar{b}$	$b\bar{b}bb\bar{b}$	
(2,3,4,35,36)	$ebbbb$	$\bar{e}bbbb$	$cdd\bar{d}\bar{d}d$	$\bar{c}dd\bar{d}\bar{d}d$	$\bar{d}dddd$	$\bar{d}dddd$	$abb\bar{b}\bar{b}$	$b\bar{b}bb\bar{b}$	
(2,3,20,20,35)	$ebbbb$	$\bar{e}bbbb$	$cdd\bar{d}\bar{d}d$	$\bar{d}c\bar{c}\bar{c}c$	$\bar{c}cccc$	$\bar{d}dddd$	$abb\bar{b}\bar{b}$	$b\bar{b}bb\bar{b}$	
(2,3,4,18,53)	$ab\bar{b}\bar{b}b$	$\bar{a}b\bar{b}\bar{b}b$	$\bar{b}bbbb$	$dc\bar{c}\bar{c}c$	$\bar{d}c\bar{c}\bar{c}c$	$ccccc$	$ecc\bar{c}\bar{c}$	$c\bar{c}cc\bar{c}$	
(2,3,12,28,35)	$ebbbb$	$\bar{e}bbbb$	$\bar{c}cccc$	$\bar{d}c\bar{c}\bar{c}c$	$\bar{c}dd\bar{d}\bar{d}d$	$cdd\bar{d}\bar{d}d$	$\bar{d}dddd$	$abb\bar{b}\bar{b}$	$b\bar{b}bb\bar{b}$
(1,6,28,43)	$caa\bar{a}\bar{a}$	$0aa\bar{a}\bar{a}a$	$0b\bar{b}\bar{b}b$	$a\bar{a}aa\bar{a}$	$bbbbb$	$\bar{b}bbbb$	$\bar{a}aaaa$	$db\bar{b}\bar{b}b$	$\bar{d}b\bar{b}\bar{b}b$
(1,2,18,59)	$edd\bar{d}\bar{d}$	$\bar{a}b\bar{b}\bar{b}b$	$ab\bar{b}\bar{b}b$	$\bar{b}bbbb$	$\bar{b}bbbb$	$ddd\bar{d}\bar{d}$	$dd\bar{d}d\bar{d}$	$\bar{d}dddd$	$\bar{d}dddd$
(3,10,10,57)	$ab\bar{b}\bar{b}b$	$\bar{b}a\bar{a}\bar{a}a$	$\bar{b}bbbb$	$\bar{a}aaaa$	$edd\bar{d}\bar{d}$	$edd\bar{d}\bar{d}$	$dd\bar{d}d\bar{d}$	$\bar{d}dddd$	$\bar{d}dddd$
(1,14,65)	$ebb\bar{b}\bar{b}$	$\bar{a}aaaa$	$b\bar{a}aa\bar{a}$	$b\bar{b}bb\bar{b}$	$\bar{b}bbbb$	$ab\bar{b}b\bar{b}$	$ab\bar{b}\bar{b}b$	$\bar{b}bbbb$	$\bar{b}bbbb$
(1,6,15,58)	$ebb\bar{b}\bar{b}$	$\bar{b}bb\bar{b}\bar{b}$	$babba$	$aab\bar{b}a$	$b\bar{a}aa\bar{a}$	$\bar{a}aaaa$	$da\bar{a}\bar{a}a$	$d\bar{a}aa\bar{a}$	$\bar{a}aaaa$
(1,2,28,45)	$caa\bar{a}\bar{a}$	$0aa\bar{a}\bar{a}a$	$a\bar{a}aa\bar{a}$	$db\bar{b}\bar{b}b$	$\bar{d}b\bar{b}\bar{b}b$	$\bar{b}bbbb$	$0b\bar{b}\bar{b}b$	$\bar{a}aaaa$	$\bar{b}bbbb$
(1,6,29,44)	$caa\bar{a}\bar{a}$	$\bar{b}a\bar{a}\bar{a}a$	$\bar{a}b\bar{b}\bar{b}b$	$a\bar{a}aa\bar{a}$	$bbbbb$	$\bar{b}bbbb$	$\bar{a}aaaa$	$db\bar{b}\bar{b}b$	$\bar{d}b\bar{b}\bar{b}b$
(1,1,6,16,43)	$c0000$	$d0000$	$0b\bar{b}\bar{b}b$	$0aaaa$	$bbbbb$	$\bar{b}bbbb$	$0a\bar{a}\bar{a}a$	$eb\bar{b}\bar{b}b$	$\bar{e}b\bar{b}\bar{b}b$
(2,3,14,26,35)	$ebbbb$	$\bar{e}bbbb$	$\bar{d}c\bar{c}\bar{c}c$	$\bar{c}cccc$	$ddddd$	$\bar{c}dd\bar{d}\bar{d}d$	$cdd\bar{d}\bar{d}d$	$abb\bar{b}\bar{b}$	$b\bar{b}bb\bar{b}$
(2,2,3,6,32,35)	$ebbbb$	$\bar{e}bbbb$	$\bar{c}dd\bar{d}\bar{d}d$	$fdddd$	$\bar{f}dddd$	$\bar{c}dd\bar{d}\bar{d}d$	$cdd\bar{d}\bar{d}d$	$abb\bar{b}\bar{b}$	$b\bar{b}bb\bar{b}$
(4,6,11,54)	$00aa0$	$b\bar{b}a\bar{a}\bar{b}$	$b0bb0$	$bb\bar{b}\bar{b}b$	$cdd\bar{d}\bar{d}d$	$cdd\bar{d}\bar{d}d$	$\bar{c}dd\bar{d}\bar{d}d$	$\bar{d}dddd$	$\bar{d}dddd$
(4,11,24,36)	$00aa0$	$b\bar{b}a\bar{a}\bar{b}$	$b0bb0$	$bb\bar{b}\bar{b}b$	$\bar{c}dccd$	$\bar{c}dccd$	$c\bar{c}dd\bar{c}$	$cdd\bar{d}\bar{d}d$	$\bar{c}cccc$
(4,11,30,30)	$00aa0$	$b\bar{b}a\bar{a}\bar{b}$	$b0bb0$	$bb\bar{b}\bar{b}b$	$cdd\bar{d}\bar{d}d$	$cdd\bar{d}\bar{d}d$	$\bar{c}dd\bar{d}\bar{d}d$	$\bar{c}cccc$	$\bar{d}dddd$

Appendix C
Orthogonal Designs in Order 28 and 56

This appendix is a summary for orthogonal designs in order 28 and 56.

C.1 Some Theorems

We first note from Koukouvinos-Seberry [135, p.2] that

Lemma C.1. *The necessary conditions are sufficient for the existence of three variable* $OD(28;a,b,c)$

From [66] we have

Lemma C.2. *All 261 possible full orthogonal designs in order 56 in three variables exist except for* $(a,b,c)=(1,5,20)$.

Hence we have

Corollary C.1. *All full orthogonal designs* $OD(2^t7;x,y,2^t7-x-y)$ *exist for any* $t \geq 3$.

Many more results are given in Geramita-Seberry [80], Georgiou-Holzmann-Kharaghani-Tayfeh-Rezaie [66], and Georgiou-Koukouvinos-Seberry [71].

C.2 Orthogonal designs in Order 28

We summarize the known results for order 28.

1. There are at most 4 variables in order 28.
2. Table C.1 lists the first rows of 4-tuples, 3-tuples and 2-tuples that are the types of orthogonal designs in order 28 via the Goethals-Seidel designs.
3. The known 4 variables are given in Table C.1.

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5

4. The $OD(14;9,4)$ from [80, p.331] is given in Figure C.1, hence we have an $OD(28;4,4,9,9)$.
5. There are orthogonal designs of types (1,9), (2,2), (2,8), (5,5) and (13) each constructed from two circulant matrices in order 14. Hence there are orthogonal designs of types:

$$(1,9,13) \qquad (2,2,13) \qquad (2,8,13) \qquad (5,5,13)$$

   in order 28.
6. The 236 3-tuples given in Table C.2 are possible types of orthogonal designs in order 28. There are no cases unresolved. We use
   n if they are made from 4-sequences with zero NPAF and length n;
   P if they are made from 4-sequences with zero PAF;
   F if they are made from the $OD(28;4,4,9,9)$;
   X if they are not known because the integer sum-fill matrix does not exist;
   Y if it does not exist by exhaustive search for length 7.
7. The sequences in Tables C.3 and C.4, which have zero periodic and non-periodic autocorrelation function, used as the first rows of the corresponding circulant matrices in the Goethals-Seidel array give orthogonal designs $OD(4n;s_1,s_2,s_3)$, where (s_1,s_2,s_3) is one of the 3-tuples.
8. There are 196 pairs (j,k) such that $j+k \leq 28$. Of these, 27 are eliminated as types of orthogonal designs by Wolfe's Theorem and the Geramita-Verner Theorem. The remaining 169 pairs are the types of an orthogonal design in order 28 and may be constructed using four circulant matrices.
9. The 27 2-tuples that cannot be the types of orthogonal designs in order 28 are:

(1,7)	(3,5)	(4,7)	(5,12)	(7,9)	(8,14)	(11,16)
(1,15)	(3,13)	(4,15)	(5,19)	(7,16)	(9,15)	(12,13)
(1,23)	(3,20)	(4,23)	(5,22)	(7,17)	(10,17)	(12,15).
(2,14)	(3,21)	(5,11)	(6,10)	(7,20)	(11,13)	

10. A11 one variable designs exist in order 28.

Table C.1: Order 28 designs

Design	$\boldsymbol{A_1}$	$\boldsymbol{A_2}$	$\boldsymbol{A_3}$	$\boldsymbol{A_4}$
(1,1,1,1)	$a000000$	$b000000$	$c000000$	$d000000$
(1,1,1,4)	$a000000$	$b000000$	$dc\bar{d}0000$	$d0d0000$
(1,1,1,9)	$da\bar{d}0000$	$db\bar{d}0000$	$d0c0\bar{d}00$	$d0d0d00$
(1,1,1,16)	$add\bar{d}d\bar{d}\bar{d}$	$b0d00\bar{d}0$	$c0d00\bar{d}0$	$0ddd\bar{d}ddd$
(1,1,1,25)	$add\bar{d}d\bar{d}\bar{d}$	$bddd\bar{d}d\bar{d}$	$cddd\bar{d}d\bar{d}$	$\bar{d}dddddd$
(1,1,2,2)	$a000000$	$b000000$	$cd00000$	$c\bar{d}00000$

Continued on Next Page...

Table C.1 – Continued

Design	A_1	A_2	A_3	A_4
(1,1,2,8)	$da\bar{d}0000$	$db\bar{d}0000$	$dcd0000$	$d\bar{c}d0000$
(1,1,2,18)	$abb\bar{b}b\bar{b}\bar{b}$	$cbb\bar{b}b\bar{b}\bar{b}$	$dbb0b00$	$\bar{d}bb0b00$
(1,1,4,4)	$a000000$	$b000000$	$ccd\bar{d}000$	$dd\bar{c}c000$
(1,1,4,9)	$add\bar{d}d\bar{d}\bar{d}$	$0dd0d00$	$b00c\bar{c}00$	$000cc00$
(1,1,4,16)	$b0b0b0b$	$b0ba\bar{b}0\bar{b}$	$bc\bar{b}0\bar{b}cb$	$bc\bar{b}db\bar{c}\bar{b}$
(1,1,5,5)	$a000000$	$b000000$	$cc\bar{c}d0d0$	$ddd\bar{c}0\bar{c}0$
(1,1,8,8)	$cdad\bar{c}00$	$\bar{c}db\bar{d}c00$	$cd0dc00$	$cd\bar{0}d\bar{c}00$
(1,1,8,18)	$\bar{a}bbabaa$	$abb\bar{a}b\bar{a}\bar{a}$	$cbb\bar{b}b\bar{b}\bar{b}$	$dbb\bar{b}b\bar{b}\bar{b}$
(1,1,9,9)	$acc\bar{c}c\bar{c}\bar{c}$	$0cc0c00$	$bddd\bar{d}d\bar{d}\bar{d}$	$0dd0d00$
(1,1,10,10)	$daa\bar{a}a\bar{a}\bar{a}$	$cbb\bar{b}b\bar{b}\bar{b}$	$\bar{a}bb0b00$	$baa0a00$
(1,1,13,13)	$\bar{a}bbabaa$	$\bar{b}\bar{a}\bar{a}b\bar{a}bb$	$caa\bar{a}a\bar{a}\bar{a}$	$dbb\bar{b}b\bar{b}\bar{b}$
(1,2,2,4)	$ba\bar{b}0000$	$b0b0000$	$cd00000$	$cd\bar{0}0000$
(1,2,2,9)	$add\bar{d}d\bar{d}\bar{d}$	$0dd0d00$	$bc00000$	$b\bar{c}00000$
(1,2,2,16)	$add\bar{d}d\bar{d}\bar{d}$	$b0dc0d\bar{0}$	$b0d\bar{c}0d\bar{0}$	$0ddd\bar{d}ddd$
(1,2,3,6)	$abc0000$	$ab\bar{c}0000$	$b\bar{a}b0000$	$bd\bar{b}0000$
(1,2,4,8)	$ca\bar{c}0000$	$c0c0000$	$dbd\bar{d}0d0$	$dbd\bar{d}0d\bar{0}$
(1,2,4,18)				
(1,2,6,12)				
(1,2,8,9)	$add\bar{d}d\bar{d}\bar{d}$	$0dd0d00$	$\bar{b}bbcb00$	$\bar{b}bb\bar{c}b00$
(1,3,6,8)	$\bar{c}cc0cab$	$c\bar{c}\bar{c}0\bar{c}ab$	$b\bar{a}b0000$	$bd\bar{b}0000$
(1,3,6,18)				
(1,4,4,4)	$ba\bar{b}0000$	$b0b0000$	$ccd\bar{d}000$	$dd\bar{c}c000$
(1,4,4,9)	$add\bar{d}d\bar{d}\bar{d}$	$0dd0d00$	$ccb\bar{b}000$	$bb\bar{c}c000$
(1,4,4,16)				
(1,4,5,5)	$ba\bar{b}0000$	$b0b0000$	$cc\bar{c}d0d0$	$ddd\bar{c}0\bar{c}0$
(1,4,8,8)				
(1,4,9,9)				
(1,4,10,10)				
(1,5,5,9)	$add\bar{d}d\bar{d}\bar{d}$	$0dd0d00$	$bb\bar{b}c0c0$	$cc\bar{c}\bar{b}0\bar{b}0$
(1,8,8,9)				
(1,9,9,9)				
(2,2,2,2)	$ab00000$	$a\bar{b}00000$	$cd00000$	$cd\bar{0}0000$
(2,2,2,8)	$ab00000$	$a\bar{b}00000$	$cd\bar{c}c0c0$	$cd\bar{c}\bar{c}0\bar{c}0$
(2,2,2,18)	$add\bar{0}bd\bar{d}$	$add\bar{0}\bar{b}d\bar{d}$	$cddddd\bar{0}0$	$\bar{c}ddddd\bar{0}0$
(2,2,4,9)				
(2,2,4,16)	$ab\bar{a}aca0$	$ab\bar{a}a\bar{c}a0$	$ab\bar{a}\bar{a}d\bar{a}0$	$ab\bar{a}\bar{a}d\bar{a}0$
(2,2,5,5)	$ab00000$	$a\bar{b}00000$	$cc\bar{c}d0d0$	$ddd\bar{c}0\bar{c}0$
(2,2,8,8)	$ab\bar{a}a0a0$	$ab\bar{a}\bar{a}0\bar{a}0$	$cd\bar{c}c0c0$	$cd\bar{c}\bar{c}0\bar{c}0$
(2,2,9,9)	$dbd\bar{c}a\bar{c}0$	$dbd\bar{c}\bar{a}c0$	$dc0cd\bar{c}0$	$\bar{c}d0dcd0$
(2,2,10,10)	$cc\bar{c}dad0$	$cc\bar{c}d\bar{a}d0$	$ddd\bar{c}b\bar{c}0$	$ddd\bar{c}\bar{b}\bar{c}0$

Continued on Next Page...

Table C.1 – Continued

Design	A_1	A_2	A_3	A_4
(2,3,4,6)	$ad0\bar{d}a00$	$adcd\bar{a}00$	$bcd\bar{d}0000$	$\bar{b}cd\bar{d}0000$
(2,3,6,9)				
(2,4,4,8)	$ab\bar{a}a0a0$	$ab\bar{a}\bar{a}0\bar{a}0$	$ccdd\bar{d}000$	$dd\bar{c}c000$
(2,4,4,18)				
(2,4,6,12)	$abcab\bar{c}0$	$abc\bar{a}\bar{b}c0$	$b\bar{a}bbd\bar{b}0$	$b\bar{a}b\bar{b}d\bar{b}0$
(2,4,8,9)				
(2,5,5,8)	$ad\bar{a}a0a0$	$ad\bar{a}\bar{a}0\bar{a}0$	$cc\bar{c}b0b0$	$bb\bar{b}\bar{c}0\bar{c}0$
(2,8,8,8)	$aab\bar{b}cd\bar{c}$	$aab\bar{b}\bar{c}d\bar{c}$	$a\bar{a}bbc0c$	$a\bar{a}bb\bar{c}0\bar{c}$
(2,8,9,9)				
(3,3,3,3)	$ab\bar{c}0000$	$a\bar{b}0d000$	$a0c\bar{d}000$	$bcd0000$
(3,3,3,12)	$\bar{c}cc0cab$	$c\bar{c}\bar{c}d\bar{c}a0$	$c\bar{c}\bar{c}\bar{d}\bar{c}0b$	$000\bar{d}0a\bar{b}$
(3,3,6,6)	$adb\bar{d}a00$	$adcd\bar{a}00$	$cd\bar{a}0\bar{b}00$	$cd\bar{a}0b00$
(3,4,6,8)	$\bar{c}cc0cab$	$c\bar{c}\bar{c}0\bar{c}ab$	$db0\bar{b}d00$	$\bar{d}b\bar{a}bd00$
(3,6,8,9)				
(4,4,4,4)	$abcd000$	$a\bar{b}cd\bar{d}000$	$ab\bar{c}d\bar{d}000$	$a\bar{b}\bar{c}d000$
(4,4,4,9)				
(4,4,4,16)	$cd\bar{c}cacb$	$cd\bar{c}c\bar{a}c\bar{b}$	$cd\bar{c}\bar{c}a\bar{c}\bar{b}$	$cd\bar{c}\bar{c}\bar{a}\bar{c}b$
(4,4,5,5)	$aab\bar{b}000$	$bb\bar{a}a000$	$c0cddd\bar{d}0$	$d0d\bar{c}\bar{c}c0$
(4,4,8,8)	$aab\bar{b}cd0$	$aab\bar{b}\bar{c}d\bar{d}0$	$a\bar{a}bbcd\bar{d}0$	$a\bar{a}bb\bar{c}d0$
(4,4,9,9)	known but not constructed from circulants			
(4,4,10,10)	$bcacddd\bar{d}$	$b\bar{c}a\bar{c}d\bar{d}d$	$bd\bar{a}d\bar{c}\bar{c}c$	$bd\bar{a}d\bar{c}c\bar{c}$
(4,5,5,9)				
(5,5,5,5)	$aa\bar{a}b0b0$	$\bar{b}\bar{b}ba0a0$	$\bar{c}\bar{c}cd\bar{d}0\bar{d}0$	$d\bar{d}dc0c0$
(5,5,8,8)				
(5,5,9,9)				
(6,6,6,6)	$aab\bar{b}cd0$	$\bar{b}\bar{b}a\bar{a}d\bar{c}0$	$\bar{c}\bar{c}d\bar{d}ab0$	$d\bar{d}c\bar{c}\bar{b}a0$
(7,7,7,7)	$aa\bar{a}bcbd$	$\bar{b}\bar{b}badac\bar{c}$	$\bar{c}\bar{c}cd\bar{a}d\bar{b}$	$d\bar{d}dc\bar{b}ca$
(1,2,22)	$ab0bbb\bar{b}$	$a\bar{b}0\bar{b}\bar{b}\bar{b}b$	$0\bar{b}\bar{b}\bar{b}bbb$	$cbb\bar{b}\bar{b}\bar{b}\bar{b}$
(1,3,24)	$ac\bar{c}c\bar{c}c\bar{c}$	$bc\bar{c}\bar{c}\bar{c}\bar{c}\bar{c}$	$b\bar{c}\bar{c}ccccc$	$b\bar{c}cc\bar{c}ccc$
(1,4,20)	$abb\bar{b}b\bar{b}\bar{b}$	$c\bar{c}bbbb0$	$0bb\bar{b}\bar{b}bb$	$c0\bar{b}b\bar{b}bc$
(1,6,12)	$b\bar{b}\bar{b}0\bar{b}aa$	$\bar{b}bb0ba0$	$\bar{b}bb0b0a$	$c00a\bar{a}00$
(1,6,18)	$caab\bar{b}\bar{a}\bar{a}$	$\bar{b}\bar{b}a\bar{a}\bar{a}a0$	$aaa\bar{a}ab0$	$aa\bar{a}aba0$
(1,6,21)	$cb\bar{b}b\bar{b}b\bar{b}$	$abbbb\bar{b}\bar{b}$	$a\bar{a}bb\bar{a}bb$	$aab\bar{b}\bar{b}bb$
(1,9,13)	$abb\bar{b}b\bar{b}\bar{b}$	$0bb0b00$	$0c\bar{c}cc\bar{c}c$	$ccc\bar{c}\bar{c}cc$
(1,10,14)	$c\bar{b}\bar{b}b\bar{b}bb$	$0\bar{b}aaa\bar{a}a$	$0b\bar{a}baba$	$0bba\bar{b}\bar{a}b$
(2,2,13)	$ab00000$	$a\bar{b}00000$	$0c\bar{c}cc\bar{c}c$	$ccc\bar{c}\bar{c}cc$
(2,7,19)	$caaa\bar{a}b\bar{a}$	$\bar{c}aba\bar{a}a\bar{a}$	$b\bar{b}aa\bar{b}aa$	$bba\bar{a}\bar{a}aa$
(2,8,13)	$\bar{b}bbcb00$	$\bar{b}bb\bar{c}b00$	$0a\bar{a}aa\bar{a}a$	$aaa\bar{a}\bar{a}aa$
(4,4,18)	$a\bar{b}\bar{c}\bar{b}\bar{b}b\bar{b}$	$ab\bar{c}bb\bar{b}b$	$a\bar{b}\bar{b}bbc0$	$abb\bar{b}\bar{b}c0$
(5,5,13)	$aa\bar{a}b0b0$	$bb\bar{b}\bar{a}0\bar{a}0$	$0c\bar{c}cc\bar{c}c$	$ccc\bar{c}\bar{c}cc$

Continued on Next Page...

Table C.1 – Continued

Design	A_1	A_2	A_3	A_4
(3,23)	$\bar{a}0bbb\bar{b}\bar{b}b$	$a\bar{b}bbb\bar{b}\bar{b}b$	$abb\bar{b}\bar{b}b0$	$bbbb\bar{b}\bar{b}\bar{b}$
(4,19)	$bb0a0\bar{a}0$	$b\bar{b}a\bar{a}a\bar{a}a$	$0aa0\bar{a}aa$	$aaaaa\bar{a}\bar{a}$
(5,21)	$b\bar{a}ab\bar{b}aa$	$bba\bar{a}\bar{a}a\bar{a}$	$aa\bar{a}\bar{a}\bar{a}a0$	$aaaa\bar{a}a0$
(5,23)	$aa\bar{a}\bar{b}bbb$	$\bar{a}b\bar{a}b\bar{b}b\bar{b}$	$bbbbb\bar{b}\bar{b}$	$bbb\bar{b}bb\bar{b}$
(6,17)	$b\bar{b}aaaa\bar{a}$	$bbaa\bar{a}\bar{a}0$	$ba\bar{a}aa\bar{a}a$	$b0\bar{a}000\bar{a}$
(6,20)	$baba\bar{a}0a$	$ba\bar{b}a0\bar{a}\bar{a}$	$baa\bar{a}\bar{a}a\bar{a}$	$b\bar{a}\bar{a}\bar{a}\bar{a}a\bar{a}$
(7,10)	$a00b000$	$b\bar{a}a00a0$	$a0\bar{b}bb0b$	$\bar{b}bb0b\bar{a}\bar{a}$
(7,15)	$bab\bar{a}\bar{b}0a$	$b\bar{a}0b000$	$b\bar{a}a\bar{a}0aa$	$b\bar{a}\bar{a}\bar{a}aa\bar{a}$
(8,17)	$a\bar{a}a\bar{a}\bar{a}a0$	$aabbb\bar{b}0$	$b\bar{a}\bar{a}\bar{a}b0a$	$baa\bar{a}aab$
(9,16)	$bbbab\bar{a}\bar{b}$	$baaa\bar{b}a0$	$b\bar{b}0aa\bar{a}\bar{a}$	$a\bar{a}a\bar{a}\bar{a}a0$
(9,17)	$a\bar{a}a\bar{a}\bar{a}a0$	$aa\bar{a}\bar{b}\bar{a}\bar{a}b$	$aa\bar{b}baa0$	$ab\bar{a}bbb\bar{b}$
(11,12)	$a\bar{a}aa000$	$\bar{b}aaa\bar{a}\bar{a}a$	$ababb\bar{b}\bar{b}$	$bb\bar{b}b0b0$
(11,15)	$bb\bar{b}b0b\bar{a}$	$bb\bar{b}\bar{b}0b\bar{a}$	$baa\bar{a}\bar{a}aa$	$aaaa\bar{a}aa\bar{a}$
(11,17)	$b\bar{b}bbba\bar{a}$	$b\bar{b}\bar{b}\bar{b}b\bar{a}\bar{a}$	$ba\bar{a}\bar{a}\bar{a}\bar{a}a$	$aaa\bar{a}aa\bar{a}$
(12,14)	$b\bar{a}bb\bar{b}a\bar{a}$	$babab\bar{b}a$	$bb\bar{a}\bar{a}a0\bar{a}$	$aab\bar{a}\bar{b}\bar{a}0$

Fig. C.1 Orthogonal design $OD(14;9,4)$

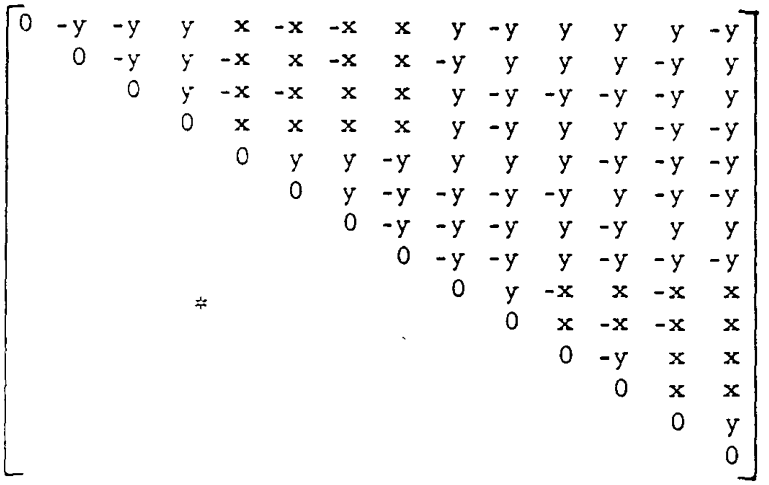


Table C.2 Known 3-variable designs in order 28[a]

(1,1,1)	1	(1,5,16)	7	(2,4,8)	5	(3,4,8)	5	(4,8,12)	7
(1,1,2)	1	(1,5,19)	X	(2,4,9)	5	(3,4,14)∗	P	(4,8,16)	7
(1,1,4)	2	(1,5,20)	Y	(2,4,11)	5	(3,4,18)	7	(4,9,9)	6
(1,1,5)	3	(1,6,8)	5	(2,4,12)	7	(3,6,6)	5	(4,9,10)	7
(1,1,8)	3	(1,6,11)	5	(2,4,16)	7	(3,6,8)	5	(4,9,13)†	7
(1,1,9)	7	(1,6,12)	7	(2,4,17)	7	(3,6,9)	5	(4,10,10)	7
(1,1,10)	3	(1,6,14)	7	(2,4,18)	7	(3,6,11)	5	(4,10,11)	P
(1,1,13)	5	(1,6,18)	7	(2,4,19)	7	(3,6,12)	7	(4,10,14)	7
(1,1,16)	7	(1,6,21)	7	(2,4,22)	P	(3,6,16)†	7	(5,5,5)	7
(1,1,17)∗	P	(1,8,8)	7	(2,5,5)	3	(3,6,17)	P	(5,5,8)	7
(1,1,18)	6	(1,8,9)	5	(2,5,7)	5	(3,6,18)	7	(5,5,9)	5
(1,1,20)	6	(1,8,11)	5	(2,5,8)	5	(3,6,19)	7	(5,5,10)	5
(1,1,25)	P	(1,8,12)	7	(2,5,13)	6	(3,7,8)	6	(5,5,13)	P
(1,1,26)	P	(1,8,16)	7	(2,5,15)	X	(3,7,10)	X	(5,5,16)	7
(1,2,2)	2	(1,8,17)	P	(2,5,18)	7	(3,7,11)	7	(5,5,18)	P
(1,2,3)	2	(1,8,18)	P	(2,6,7)	5	(3,7,15)	P	(5,6,9)	7
(1,2,4)	2	(1,8,19)	P	(2,6,9)	5	(3,7,18)	7	(5,6,14)	X
(1,2,6)	3	(1,9,9)	7	(2,6,11)	X	(3,8,9)	7	(5,6,15)	X
(1,2,8)	3	(1,9,10)	5	(2,6,12)	6	(3,8,10)∗	P	(5,7,8)	7
(1,2,9)	3	(1,9,13)∗	P	(2,6,13)	7	(3,8,15)†	7	(5,7,10)	X
(1,2,11)	5	(1,9,16)	7	(2,6,16)	7	(3,9,14)	7	(5,7,14)	X
(1,2,12)	5	(1,9,18)	7	(2,6,17)	X	(3,10,15)	P	(5,8,8)	7
(1,2,16)	7	(1,10,10)	7	(2,7,10)	7	(3,11,14)	X	(5,8,13)	7
(1,2,17)	5	(1,10,11)	7	(2,7,12)	7	(4,4,4)	3	(5,9,9)∗	P
(1,2,18)	6	(1,10,14)	P	(2,7,13)	7	(4,4,5)	5	(5,9,10)∗	P
(1,2,19)	6	(1,13,13)	P	(2,7,19)	P	(4,4,8)	7	(5,9,14)	P
(1,2,22)	7	(1,13,14)	P	(2,8,8)	5	(4,4,9)	5	(5,10,10)	7
(1,2,25)	P	(2,2,2)	2	(2,8,9)	5	(4,4,10)	5	(6,6,6)	7
(1,3,6)	3	(2,2,4)	2	(2,8,10)	5	(4,4,13)	7	(6,6,12)	7
(1,3,8)	3	(2,2,5)	3	(2,8,13)	7	(4,4,16)	7	(6,7,8)	P
(1,3,14)	6	(2,2,8)	3	(2,8,16)	7	(4,4,17)	7	(6,8,9)	7
(1,3,18)	6	(2,2,9)	5	(2,8,18)	7	(4,4,18)	P	(6,8,11)	X
(1,3,22)	X	(2,2,10)	5	(2,9,9)	5	(4,4,20)	7	(6,8,12)	P
(1,3,24)	7	(2,2,13)	5	(2,9,11)	6	(4,5,5)	5	(6,9,11)	P
(1,4,4)	5	(2,2,16)	7	(2,9,12)	7	(4,5,6)	5	(7,7,7)	7
(1,4,5)	5	(2,2,17)	7	(2,9,17)	P	(4,5,9)	5	(7,7,14)	7
(1,4,8)	5	(2,2,18)	6	(2,10,10)	6	(4,5,14)∗	P	(7,8,10)	P
(1,4,9)	5	(2,2,20)	7	(2,10,12)	6	(4,5,16)	7	(7,8,13)	7
(1,4,10)	5	(2,3,4)	3	(2,11,11)	X	(4,5,19)	X	(7,10,11)	X
(1,4,13)	7	(2,3,6)	3	(2,11,13)	X	(4,6,8)	5	(8,8,8)	7
(1,4,16)	7	(2,3,7)	3	(2,11,15)	X	(4,6,11)†	7	(8,8,9)†	7
(1,4,17)	7	(2,3,9)	5	(2,13,13)	P	(4,6,12)	7	(8,8,10)	7
(1,4,18)	7	(2,3,10)	7	(3,3,3)	3	(4,6,14)	7	(8,9,9)†	7
(1,4,20)	7	(2,3,15)	7	(3,3,6)	3	(4,6,18)	7	(8,9,11)	P
(1,5,5)	3	(2,3,16)	7	(3,3,12)	7	(4,8,8)	7	(8,10,10)	7
(1,5,6)	3	(2,4,4)	3	(3,3,15)	7	(4,8,9)	7	(9,9,9)	P
(1,5,9)	5	(2,4,6)	3	(3,4,6)	5	(4,8,11)	7	(9,9,10)	P
(1,5,14)	5								

[a] for the 3-tuples marked by * the corresponding orthogonal design is known for $n \geq 6$ and orders ≥ 24. † the corresponding orthogonal design is known for $n \geq 7$ from [126].

Table C.3 Order 28: sequences with zero periodic autocorrelation function [a]

Design	A_1	A_2	A_3	A_4
(1,8,17)	$a\ \bar{c}\ \bar{c}\ c\ \bar{c}\ c\ c$	$b\ b\ 0\ \bar{c}\ c\ c\ c$	$b\ b\ \bar{c}\ \bar{c}\ c\ \bar{c}\ 0$	$\bar{b}\ b\ \bar{b}\ c\ b\ c\ c$
(2,4,22)	$\bar{c}\ c\ c\ \bar{c}\ \bar{c}\ \bar{b}\ a$	$\bar{c}\ c\ \bar{c}\ c\ a\ b\ c$	$c\ \bar{c}\ c\ c\ c\ \bar{b}\ c$	$\bar{c}\ c\ c\ c\ c\ b\ \bar{c}$
(2,9,11)	$a\ b\ 0\ \bar{c}\ \bar{b}\ 0\ 0$	$a\ \bar{b}\ c\ c\ b\ \bar{c}\ 0$	$b\ b\ \bar{c}\ c\ b\ 0\ 0$	$c\ \bar{c}\ c\ c\ c\ b\ \bar{b}$
(2,9,17)	$a\ \bar{b}\ c\ \bar{b}\ b\ c\ b$	$a\ c\ \bar{c}\ c\ \bar{c}\ \bar{c}\ \bar{c}$	$b\ b\ \bar{c}\ c\ b\ \bar{c}\ c$	$\bar{b}\ \bar{c}\ b\ c\ c\ c\ c$
(3,6,17)	$a\ b\ \bar{c}\ c\ c\ 0\ c$	$a\ \bar{c}\ b\ c\ \bar{c}\ 0\ \bar{c}$	$a\ \bar{b}\ \bar{b}\ \bar{c}\ \bar{c}\ c\ c$	$\bar{b}\ b\ c\ \bar{c}\ c\ c\ c$
(3,7,11)	$a\ b\ 0\ c\ \bar{c}\ c\ 0$	$a\ b\ 0\ c\ 0\ \bar{c}\ 0$	$c\ c\ b\ \bar{a}\ b\ \bar{c}\ 0$	$c\ b\ \bar{b}\ \bar{b}\ c\ c\ 0$
(3,7,15)	$a\ \bar{b}\ b\ b\ c\ c\ 0$	$a\ b\ \bar{c}\ \bar{c}\ c\ c\ \bar{c}$	$a\ c\ \bar{b}\ \bar{c}\ \bar{b}\ \bar{c}\ 0$	$b\ \bar{c}\ c\ \bar{c}\ 0\ \bar{c}\ \bar{c}$
(3,10,15)	$a\ \bar{b}\ b\ b\ c\ b\ c$	$a\ b\ \bar{b}\ \bar{b}\ c\ \bar{c}\ \bar{c}$	$a\ \bar{c}\ \bar{b}\ \bar{c}\ \bar{c}\ c\ c$	$b\ \bar{c}\ b\ \bar{c}\ c\ \bar{c}\ \bar{c}$
(4,9,13)	$a\ a\ \bar{b}\ \bar{c}\ c\ b\ 0$	$b\ b\ \bar{c}\ c\ b\ \bar{c}\ c$	$c\ c\ c\ c\ \bar{c}\ b\ \bar{b}$	$a\ \bar{a}\ \bar{b}\ \bar{c}\ \bar{c}\ b\ 0$
(4,10,11)	$a\ a\ \bar{b}\ b\ 0\ \bar{c}\ c$	$\bar{a}\ a\ \bar{c}\ b\ c\ c\ \bar{b}$	$b\ b\ b\ c\ \bar{c}\ 0\ \bar{c}$	$\bar{b}\ b\ c\ c\ 0\ b\ c$
(5,5,18)	$a\ b\ \bar{c}\ b\ c\ \bar{c}\ c$	$a\ \bar{c}\ a\ c\ b\ \bar{b}\ \bar{b}$	$a\ \bar{c}\ \bar{a}\ \bar{c}\ \bar{c}\ c\ \bar{c}$	$\bar{c}\ \bar{c}\ c\ c\ c\ c\ c$
(5,9,14)	$a\ \bar{b}\ b\ \bar{c}\ c\ c\ c$	$a\ b\ \bar{c}\ a\ c\ \bar{b}\ \bar{c}$	$b\ \bar{b}\ \bar{b}\ \bar{b}\ \bar{c}\ \bar{b}\ c$	$\bar{a}\ c\ c\ a\ c\ \bar{c}\ c$
(5,10,10)	$\bar{a}\ a\ a\ b\ c\ b\ c$	$a\ 0\ a\ \bar{b}\ \bar{c}\ \bar{c}\ c$	$b\ 0\ \bar{b}\ \bar{b}\ c\ c\ \bar{c}$	$\bar{b}\ b\ b\ \bar{c}\ 0\ \bar{c}\ b$
(6,7,8)	$\bar{c}\ c\ c\ 0\ c\ b\ a$	$c\ \bar{c}\ \bar{c}\ 0\ \bar{c}\ b\ a$	$b\ a\ 0\ \bar{a}\ b\ 0\ 0$	$\bar{b}\ a\ \bar{b}\ a\ b\ 0\ 0$
(6,9,11)	$a\ \bar{c}\ c\ c\ c\ 0\ c$	$a\ \bar{b}\ b\ c\ \bar{c}\ 0\ \bar{c}$	$a\ b\ \bar{c}\ a\ \bar{b}\ \bar{b}\ b$	$\bar{a}\ b\ b\ a\ c\ b\ \bar{c}$
(7,8,10)	$\bar{a}\ a\ a\ b\ b\ \bar{c}\ 0$	$\bar{a}\ b\ b\ c\ \bar{c}\ c\ 0$	$a\ \bar{b}\ \bar{c}\ \bar{c}\ b\ \bar{b}\ b$	$a\ \bar{c}\ a\ c\ c\ 0\ c$
(8,9,11)	$\bar{c}\ b\ \bar{b}\ a\ c\ \bar{c}\ a$	$b\ a\ a\ c\ a\ \bar{a}\ \bar{b}$	$c\ \bar{a}\ b\ b\ b\ \bar{c}\ a$	$\bar{c}\ c\ c\ c\ b\ c\ \bar{b}$
(9,9,10)	$a\ a\ a\ \bar{b}\ b\ \bar{c}\ c$	$\bar{b}\ b\ c\ b\ b\ b\ \bar{c}$	$a\ b\ \bar{a}\ \bar{b}\ c\ \bar{c}\ \bar{c}$	$\bar{a}\ a\ \bar{a}\ c\ a\ c\ c$

[a] Koukouvinos and Seberry [135, p107]© Charles Babbage Research Centre

C.3 Order 56

We summarize the known results for order 56.

1. There are at most 8 variables.
2. Table C.5 gives the known twenty four 8-tuples of orthogonal designs in order 56 (see [59] and [120]).
3. Table C.6 gives the known twenty six 7-tuples of orthogonal designs in order 56 (see [59]).
4. All $OD(56;1,k)$ are known.
5. All one variable designs exist in order 56.

C.4 Further Research

Remark C.1 (Research Problem 1). No effort has been made to investigate whether the necessary conditions are sufficient for orthogonal designs in order 56.

Remark C.2 (Research Problem 2). It is not yet known, after almost 40 years, whether orthogonal designs $OD(28;a,b,c,d)$ exist for

Table C.4 Order 28: sequences with zero non-periodic autocorrelation function

Design	A_1	A_2	A_3	A_4
$(1,1,17)$	$\bar{c}\ a\ c\ 0\ 0\ 0\ 0$	$\bar{c}\ b\ c\ 0\ 0\ 0\ 0$	$c\ c\ c\ \bar{c}\ \bar{c}\ c\ \bar{c}$	$c\ c\ c\ 0\ c\ \bar{c}\ c$
$(1,3,14)$	$\bar{c}\ 0\ \bar{c}\ a\ c\ 0\ c$	$c\ 0\ 0\ 0\ b\ \bar{c}\ c$	$c\ c\ \bar{c}\ 0\ 0\ c\ b$	$\bar{c}\ \bar{c}\ 0\ 0\ \bar{c}\ 0\ b$
$(1,8,16)$	$\bar{c}\ \bar{b}\ c\ a\ \bar{c}\ b\ c$	$b\ b\ 0\ c\ \bar{c}\ c\ \bar{c}$	$b\ \bar{c}\ \bar{c}\ 0\ b\ c\ c$	$\bar{c}\ \bar{b}\ b\ \bar{c}\ 0\ \bar{c}\ \bar{c}$
$(1,9,16)$	$\bar{c}\ \bar{b}\ c\ a\ \bar{c}\ b\ c$	$c\ b\ \bar{c}\ b\ \bar{c}\ b\ c$	$\bar{c}\ 0\ \bar{c}\ b\ \bar{c}\ \bar{b}\ \bar{c}$	$c\ 0\ c\ b\ \bar{c}\ \bar{b}\ \bar{c}$
$(2,7,10)$	$\bar{c}\ 0\ a\ 0\ c\ b\ \bar{c}$	$b\ a\ \bar{b}\ 0\ \bar{b}\ c\ 0$	$\bar{c}\ 0\ 0\ b\ \bar{c}\ 0\ 0$	$\bar{c}\ b\ c\ 0\ c\ b\ c$
$(2,7,13)$	$a\ b\ \bar{c}\ 0\ \bar{c}\ 0\ 0$	$a\ \bar{b}\ c\ 0\ c\ 0\ 0$	$c\ \bar{c}\ \bar{b}\ b\ b\ c\ c$	$c\ c\ b\ \bar{c}\ b\ c\ \bar{c}$
$(2,8,18)$	$b\ c\ c\ a\ \bar{c}\ \bar{c}\ b$	$\bar{b}\ \bar{c}\ c\ a\ \bar{c}\ c\ \bar{b}$	$b\ c\ \bar{c}\ c\ c\ c\ \bar{b}$	$b\ c\ c\ c\ \bar{c}\ c\ \bar{b}$
$(3,4,14)$	$c\ c\ a\ \bar{c}\ c\ \bar{c}\ 0$	$c\ b\ 0\ a\ 0\ \bar{b}\ c$	$\bar{c}\ c\ a\ \bar{c}\ \bar{c}\ \bar{c}\ 0$	$c\ b\ 0\ 0\ 0\ b\ \bar{c}$
$(3,6,16)$	$c\ b\ c\ a\ \bar{c}\ 0\ \bar{c}$	$c\ b\ \bar{c}\ 0\ c\ a\ \bar{c}$	$c\ b\ \bar{c}\ b\ \bar{c}\ \bar{a}\ c$	$c\ 0\ c\ \bar{b}\ c\ b\ c$
$(3,7,11)$	$c\ 0\ a\ b\ 0\ c\ \bar{c}$	$c\ 0\ \bar{c}\ 0\ a\ b\ 0$	$\bar{c}\ \bar{c}\ \bar{b}\ a\ \bar{b}\ c\ 0$	$\bar{c}\ 0\ \bar{c}\ \bar{b}\ b\ b\ \bar{c}$
$(3,8,10)$	$b\ c\ c\ 0\ a\ \bar{c}\ b$	$\bar{b}\ \bar{c}\ c\ 0\ a\ c\ \bar{b}$	$b\ \bar{c}\ 0\ a\ 0\ \bar{c}\ \bar{b}$	$b\ c\ 0\ 0\ 0\ c\ \bar{b}$
$(3,8,15)$	$b\ c\ c\ 0\ a\ \bar{c}\ b$	$b\ c\ \bar{c}\ 0\ \bar{a}\ \bar{c}\ b$	$b\ \bar{c}\ \bar{c}\ a\ c\ \bar{c}\ \bar{b}$	$b\ c\ c\ c\ \bar{c}\ c\ \bar{b}$
$(3,9,14)$	$c\ \bar{b}\ 0\ b\ c\ c\ a$	$\bar{c}\ b\ \bar{c}\ a\ \bar{c}\ \bar{b}\ c$	$\bar{c}\ b\ 0\ \bar{b}\ \bar{c}\ c\ a$	$\bar{c}\ b\ c\ b\ c\ b\ \bar{c}$
$(4,4,13)$	$a\ \bar{c}\ \bar{c}\ 0\ c\ c\ a$	$b\ \bar{c}\ c\ 0\ \bar{c}\ c\ b$	$a\ c\ 0\ 0\ 0\ c\ \bar{a}$	$b\ c\ 0\ c\ 0\ c\ \bar{b}$
$(4,5,14)$	$a\ 0\ \bar{b}\ 0\ b\ 0\ a$	$c\ 0\ \bar{c}\ b\ c\ 0\ c$	$a\ \bar{c}\ b\ c\ b\ \bar{c}\ \bar{a}$	$c\ c\ c\ c\ \bar{c}\ c\ \bar{c}$
$(4,6,11)$	$b\ 0\ a\ 0\ a\ 0\ \bar{b}$	$c\ c\ c\ b\ \bar{c}\ c\ 0$	$c\ \bar{c}\ c\ b\ \bar{c}\ \bar{c}\ 0$	$b\ 0\ \bar{a}\ \bar{c}\ a\ 0\ b$
$(5,5,13)$	$b\ c\ c\ a\ \bar{c}\ \bar{c}\ b$	$a\ \bar{c}\ c\ \bar{b}\ \bar{c}\ c\ a$	$a\ c\ 0\ 0\ 0\ c\ \bar{a}$	$b\ c\ 0\ c\ 0\ c\ \bar{b}$
$(5,10,10)$	$b\ c\ c\ a\ c\ \bar{c}\ b$	$\bar{b}\ 0\ \bar{b}\ a\ \bar{c}\ a\ b$	$c\ \bar{c}\ \bar{c}\ 0\ \bar{b}\ b\ b$	$b\ 0\ \bar{c}\ \bar{a}\ b\ a\ \bar{c}$
$(7,8,13)$	$\bar{c}\ b\ \bar{a}\ a\ a\ b\ \bar{c}$	$\bar{a}\ c\ b\ \bar{c}\ c\ b\ c$	$a\ \bar{c}\ \bar{b}\ c\ c\ b\ c$	$\bar{c}\ b\ a\ c\ a\ \bar{b}\ c$
$(8,8,9)$	$b\ \bar{c}\ a\ c\ b\ 0\ a$	$b\ \bar{c}\ b\ c\ \bar{a}\ 0\ \bar{a}$	$b\ \bar{c}\ \bar{a}\ \bar{c}\ \bar{b}\ \bar{c}\ a$	$b\ \bar{c}\ \bar{b}\ 0\ a\ c\ \bar{a}$
$(8,9,9)$	$a\ c\ c\ 0\ c\ \bar{c}\ a$	$a\ b\ \bar{c}\ 0\ \bar{c}\ \bar{b}\ a$	$a\ b\ \bar{b}\ b\ b\ b\ \bar{a}$	$a\ c\ b\ \bar{c}\ \bar{b}\ c\ \bar{a}$
$(4,22)$	$b\ 0\ a\ a\ \bar{b}\ \bar{b}\ b$	$\bar{b}\ 0\ \bar{a}\ a\ b\ b\ b$	$b\ b\ \bar{b}\ b\ \bar{b}\ b\ b$	$\bar{b}\ b\ b\ b\ \bar{b}\ b\ b$
$(5,23)$	$b\ \bar{b}\ \bar{a}\ a\ a\ b\ b$	$\bar{b}\ \bar{b}\ a\ \bar{b}\ a\ b\ b$	$b\ b\ \bar{b}\ b\ \bar{b}\ b\ b$	$\bar{b}\ b\ b\ b\ \bar{b}\ b\ b$
$(11,14)$	$\bar{a}\ a\ a\ \bar{b}\ \bar{b}\ b\ b$	$b\ b\ a\ 0\ b\ \bar{a}\ a$	$a\ 0\ a\ a\ \bar{b}\ b\ \bar{b}$	$\bar{b}\ b\ a\ b\ b\ 0\ \bar{a}$
$(11,15)$	$a\ b\ \bar{b}\ a\ b\ b\ \bar{a}$	$a\ b\ b\ 0\ \bar{a}\ \bar{b}\ a$	$a\ b\ \bar{b}\ 0\ a\ \bar{b}\ a$	$a\ b\ b\ b\ \bar{b}\ b\ \bar{a}$
$(11,17)$	$\bar{a}\ a\ a\ \bar{b}\ b\ b\ b$	$b\ a\ \bar{b}\ \bar{b}\ \bar{a}\ a\ \bar{b}$	$\bar{b}\ b\ a\ a\ b\ a\ \bar{b}$	$a\ b\ \bar{b}\ b\ \bar{a}\ b\ b$

Table C.5 Orthogonal designs of order 56, 8-tuples

$(1,1,1,1,1,1,1,1)$	$(1,1,1,1,1,1,2,2)$	$(1,1,1,1,1,1,4,4)$
$(1,1,1,1,2,2,2,2)$	$(1,1,1,1,2,2,4,4)$	$(1,1,1,1,4,4,4,4)$
$(1,1,1,1,5,5,5,5)$	$(1,1,2,2,2,2,2,2)$	$(1,1,2,2,2,2,4,4)$
$(1,1,2,2,4,4,4,4)$	$(1,1,2,2,5,5,5,5)$	$(1,1,4,4,4,4,4,4)$
$(2,2,2,2,2,2,2,2)$	$(2,2,2,2,2,2,4,4)$	$(2,2,2,2,4,4,4,4)$
$(2,2,2,2,5,5,5,5)$	$(2,2,4,4,5,5,5,5)$	$(4,4,4,4,4,4,4,4)$
$(4,4,4,4,5,5,5,5)$	$(5,5,5,5,5,5,5,5)$	$(2,2,2,2,8,8,8,8)$
$(2,2,4,4,4,4,8,8)$	$(5,5,5,5,8,8,8,8)$	$(7,7,7,7,7,7,7,7)$

Table C.6 Orthogonal designs of order 56, 7-tuples

(1,1,1,1,1,1,13)	(1,1,1,1,2,2,13)	(1,1,1,1,3,3,12)
(1,1,1,1,4,4,13)	(1,1,1,1,4,4,16)	(1,1,2,2,2,2,13)
(1,1,2,2,3,3,12)	(1,1,2,2,4,4,13)	(1,1,2,2,4,4,16)
(1,1,3,3,4,4,12)	(1,1,4,4,4,4,13)	(1,1,4,4,4,4,16)
(1,1,5,5,5,5,13)	(2,2,2,2,2,2,13)	(2,2,2,2,3,3,12)
(2,2,2,2,4,4,13)	(2,2,2,2,4,4,16)	(2,2,3,3,4,4,12)
(2,2,4,4,4,4,13)	(2,2,4,4,4,4,16)	(2,2,5,5,5,5,13)
(3,3,4,4,4,4,12)	(3,3,5,5,5,5,12)	(4,4,4,4,4,4,16)
(4,4,5,5,5,5,13)	(4,4,5,5,5,5,16)	

1,2,4,18	1,4,4,16	1,8,8,9	2,4,4,18	4,4,4,9
1,2,6,12	1,4,8,8	1,9,9,9	2,4,8,9	4,5,5,9
1,3,6,18	1,4,9,9	2,2,4,9	2,8,9,9	5,5,8,8
	1,4,10,10	2,3,6,9	3,6,8,9	5,5,9,9

Remark C.3 (Research Problem 3).

The challenge now is to find other 7 and 8 variable orthogonal designs in order 56.

Appendix D
Orthogonal Designs in Order 36 and 72

D.1 Some theorems

Theorem D.1. *All orthogonal designs* $OD(2^t.9; x, y, 2^t.9 - x - y)$ *exist for* $t \geq 3$ *[80].*

D.2 Orthogonal designs in Order 36

We now summarize the known results for order 36.

1. There are at most 4 variables in order 36.
2. There are 1347 possible 3-tuples. Table D.1 lists the 433 3-tuples which may correspond to designs in order 36: 914 cases correspond to 3-tuples eliminated by number theory. The design is known to be able to be constructed using four circulant matrices in the Goethals-Seidel array for 429 cases. For 4 cases, if designs exist for the corresponding 3-tuple, they cannot be constructed using circulant matrices (Y). P indicates that 4-PAF sequences with length 9 exist; n indicates 4-$NPAF$ sequences with length n exist.
3. Table D.2 lists the 54 cases of an $OD(36; s_1, s_2, 36 - s_1 - s_2)$ constructed using four circulant matrices.
4. All $(1, k)$ variables exist, $k \in \{x | 1 \leq x \leq 35, \quad x = a^2 + b^2 + c^2\}$ [80].
5. There are no orthogonal designs $OD(4n; s_1, s_2)$ where (s_1, s_2) is one of the 2-tuples

$$(3, 29), \quad (11, 20), \quad (11, 21), \quad (13, 19), \quad (15, 17)$$

   constructed using four circulant matrices in the Goethals-Seidel array [131].
6. From Georgiou, Koukouvinos, Mitrouli and Seberry [70] we see that there are no unresolved cases for 2 variable designs in order 36.

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5

7. All 1 variable designs exist [80].
8. From Georgiou, Koukouvinos, Mitrouli and Seberry [70] there are no 4-NPAF (x, y) sequences of length 9 for

$$(3,31), \quad (5,30), \quad (6,29), \quad (8,27), \quad \text{or } (13,22).$$

D.3 Order 72

We now summarize the known results for order 72.

1. Let $n = 4m = 72$ be the order of an orthogonal design then the number of cases which must be studied to determine whether all orthogonal designs exist is
   (i) $\frac{1}{4}n^2 = 1296$ when 2−tuples are considered;
   (ii) $\frac{n}{72}(2n^2 + 3n - 6) = 10578$ when 3-tuples are considered;
   (iii) $\frac{1}{5776}(n^4 + 6n^3 - 2n^2 - 24n) = 50523$ when 4−tuples are considered [73].
2. There are at most 8 variables in order 72.
3. All designs $(1, k)$ for $k = 1, 2, \ldots, 71$ are known [238].
4. All $OD(72; s_1, 72 - s_1)$ are known [73].
5. Of 2700 possible tuples $OD(72; s_1, s_2, 72 - s_1 - s_2)$, 355 are known [73].
6. Of 432 possible tuples $OD(72; s_1, s_2, s_3, 72 - s_1 - s_2 - s_3)$, 355 are known [73].
7. [73] gives the orders and constructions for those known.
8. All one variable designs exist.

Table D.1 The existence of $OD(36; s_1, s_2, s_3)$ [a]

s_1,s_2,s_3	n	s_1,s_2,s_3	n	s_1,s_2,s_3	n	s_1,s_2,s_3	n	s_1,s_2,s_3	n
(1,1,1)	1	(1,1,2)	1	(1,1,4)	2	(1,1,5)	3	(1,1,8)	3
(1,1,9)	7	(1,1,10)	3	(1,1,13)	5	(1,1,16)	7	(1,1,17)	7
(1,1,18)	6	(1,1,20)	6	(1,1,25)	9	(1,1,26)	P	(1,1,29)	P
(1,1,32)	9	(1,1,34)	P	(1,2,2)	2	(1,2,3)	2	(1,2,4)	2
(1,2,6)	3	(1,2,8)	3	(1,2,9)	3	(1,2,11)	5	(1,2,12)	5
(1,2,16)	7	(1,2,17)	5	(1,2,18)	6	(1,2,19)	6	(1,2,22)	7
(1,2,24)	9	(1,2,25)	9	(1,2,27)	9	(1,2,32)	P	(1,2,33)	9
(1,3,6)	3	(1,3,8)	3	(1,3,14)	6	(1,3,18)	6	(1,3,24)	7
(1,3,26)	9	(1,3,32)	9	(1,4,4)	5	(1,4,5)	5	(1,4,8)	5
(1,4,9)	5	(1,4,10)	5	(1,4,13)	7	(1,4,16)	7	(1,4,17)	7
(1,4,18)	7	(1,4,20)	7	(1,4,25)	9	(1,4,26)	P	(1,4,29)	9
(1,5,5)	3	(1,5,6)	3	(1,5,9)	5	(1,5,14)	5	(1,5,16)	7
(1,5,20)	9	(1,5,21)	P	(1,5,24)	9	(1,5,25)	P	(1,5,30)	P
(1,6,8)	5	(1,6,11)	5	(1,6,12)	7	(1,6,14)	7	(1,6,18)	7
(1,6,20)	9	(1,6,21)	7	(1,6,27)	P	(1,6,29)	P	(1,8,8)	7
(1,8,9)	5	(1,8,11)	5	(1,8,12)	7	(1,8,16)	7	(1,8,17)	9
(1,8,18)	9	(1,8,19)	P	(1,8,22)	P	(1,8,24)	P	(1,8,25)	P
(1,8,27)	P	(1,9,9)	7	(1,9,10)	5	(1,9,13)	9	(1,9,16)	7
(1,9,17)	P	(1,9,18)	7	(1,9,20)	9	(1,9,25)	P	(1,9,26)	9
(1,10,10)	7	(1,10,11)	7	(1,10,14)	P	(1,10,16)	P	(1,10,19)	9
(1,10,25)	P	(1,11,18)	P	(1,11,22)	P	(1,11,24)	P	(1,12,14)	P
(1,12,18)	P	(1,13,13)	9	(1,13,14)	P	(1,13,16)	P	(1,13,17)	P
(1,13,22)	P	(1,14,19)	P	(1,14,21)	P	(1,16,16)	9	(1,16,17)	9
(1,17,17)	P	(1,17,18)	9	(2,2,2)	2	(2,2,4)	2	(2,2,5)	3
(2,2,8)	3	(2,2,9)	5	(2,2,10)	5	(2,2,13)	5	(2,2,16)	7
(2,2,17)	7	(2,2,18)	6	(2,2,20)	7	(2,2,25)	P	(2,2,26)	9
(2,2,29)	P	(2,2,32)	9	(2,3,4)	3	(2,3,6)	3	(2,3,7)	3
(2,3,9)	5	(2,3,10)	7	(2,3,15)	7	(2,3,16)	7	(2,3,22)	P
(2,3,24)	9	(2,3,25)	9	(2,3,28)	9	(2,3,31)	P	(2,4,4)	3
(2,4,6)	3	(2,4,8)	5	(2,4,9)	5	(2,4,11)	5	(2,4,12)	7
(2,4,16)	7	(2,4,17)	7	(2,4,18)	7	(2,4,19)	7	(2,4,22)	9
(2,4,24)	9	(2,4,25)	P	(2,4,27)	P	(2,5,5)	3	(2,5,7)	5
(2,5,8)	5	(2,5,13)	6	(2,5,18)	7	(2,5,20)	P	(2,5,22)	P
(2,5,23)	P	(2,6,7)	5	(2,6,9)	5	(2,6,12)	6	(2,6,13)	7
(2,6,16)	7	(2,6,19)	P	(2,6,21)	P	(2,6,25)	P	(2,6,27)	P
(2,6,28)	P	(2,7,10)	7	(2,7,12)	7	(2,7,13)	7	(2,7,19)	P
(2,7,20)	P	(2,7,21)	P	(2,7,24)	P	(2,7,27)	P	(2,8,8)	5
(2,8,9)	5	(2,8,10)	5	(2,8,13)	7	(2,8,16)	7	(2,8,17)	P
(2,8,18)	7	(2,8,20)	9	(2,8,25)	Y	(2,8,26)	9	(2,9,9)	5
(2,9,11)	6	(2,9,12)	7	(2,9,16)	P	(2,9,17)	P	(2,9,18)	P
(2,9,19)	P	(2,9,22)	P	(2,9,25)	P	(2,10,10)	6	(2,10,12)	6
(2,10,15)	9	(2,10,18)	9	(2,11,16)	P	(2,11,22)	P	(2,11,23)	P
(2,12,15)	9	(2,12,16)	9	(2,12,22)	P	(2,13,13)	P	(2,13,15)	9
(2,13,18)	P	(2,13,21)	P	(2,16,16)	9	(2,16,18)	9	(2,17,17)	P

[a] Georgiou, Koukouvinos, Mitrouli, and Seberry [70, p338-339]

Table D.1 The existence of $OD(36; s_1, s_2, s_3)$ [a] *(continued)*

s_1,s_2,s_3	n	s_1,s_2,s_3	n	s_1,s_2,s_3	n	s_1,s_2,s_3	n	s_1,s_2,s_3	n
(3,3,3)	3	(3,3,6)	3	(3,3,12)	7	(3,3,15)	7	(3,3,24)	9
(3,3,27)	P	(3,3,30)	9	(3,4,6)	5	(3,4,8)	5	(3,4,14)	7
(3,4,18)	7	(3,4,24)	P	(3,4,26)	P	(3,6,6)	5	(3,6,8)	5
(3,6,9)	5	(3,6,11)	5	(3,6,12)	7	(3,6,16)	7	(3,6,17)	9
(3,6,18)	7	(3,6,19)	7	(3,6,22)	P	(3,6,24)	9	(3,6,25)	P
(3,6,27)	9	(3,7,8)	6	(3,7,11)	7	(3,7,15)	P	(3,7,18)	7
(3,7,23)	P	(3,8,9)	7	(3,8,10)	7	(3,8,15)	7	(3,8,16)	P
(3,8,22)	P	(3,8,24)	P	(3,8,25)	P	(3,9,14)	7	(3,9,18)	P
(3,9,24)	9	(3,10,15)	9	(3,10,17)	9	(3,10,18)	P	(3,10,23)	P
(3,11,19)	P	(3,11,22)	P	(3,12,12)	P	(3,12,15)	9	(3,14,16)	P
(3,15,15)	P	(3,15,18)	P	(4,4,4)	3	(4,4,5)	5	(4,4,8)	7
(4,4,9)	5	(4,4,10)	5	(4,4,13)	7	(4,4,16)	7	(4,4,17)	7
(4,4,18)	9	(4,4,20)	7	(4,4,25)	P	(4,4,26)	9	(4,5,5)	5
(4,5,6)	5	(4,5,9)	5	(4,5,14)	7	(4,5,16)	7	(4,5,20)	9
(4,5,21)	9	(4,5,24)	P	(4,5,25)	9	(4,6,8)	5	(4,6,11)	7
(4,6,12)	7	(4,6,14)	7	(4,6,18)	7	(4,6,20)	8	(4,6,21)	P
(4,8,8)	7	(4,8,9)	7	(4,8,11)	7	(4,8,12)	7	(4,8,16)	7
(4,8,17)	9	(4,8,18)	8	(4,8,19)	P	(4,8,22)	9	(4,8,24)	P
(4,9,9)	6	(4,9,10)	7	(4,9,13)	9	(4,9,16)	P	(4,9,17)	P
(4,9,18)	P	(4,9,20)	P	(4,10,10)	7	(4,10,11)	P	(4,10,14)	7
(4,10,16)	9	(4,10,19)	P	(4,11,18)	P	(4,12,14)	8	(4,12,18)	9
(4,13,13)	P	(4,13,14)	P	(4,13,16)	P	(4,13,17)	P	(4,16,16)	9
(5,5,5)	7	(5,5,8)	7	(5,5,9)	5	(5,5,10)	5	(5,5,13)	7
(5,5,16)	7	(5,5,17)	P	(5,5,18)	9	(5,5,20)	9	(5,5,25)	P
(5,5,26)	P	(5,6,9)	7	(5,6,16)	P	(5,6,25)	P	(5,7,8)	7
(5,7,18)	9	(5,7,22)	P	(5,8,8)	7	(5,8,13)	7	(5,8,18)	P
(5,8,20)	P	(5,8,23)	P	(5,9,9)	P	(5,9,14)	P	(5,9,16)	P
(5,9,20)	P	(5,10,10)	7	(5,10,15)	9	(5,13,13)	P	(5,13,18)	P
(6,6,6)	7	(6,6,12)	7	(6,6,15)	P	(6,6,24)	9	(6,7,8)	P
(6,7,18)	P	(6,7,21)	Y	(6,7,23)	P	(6,8,9)	7	(6,8,12)	7
(6,8,13)	P	(6,8,16)	8	(6,8,19)	P	(6,9,11)	P	(6,9,12)	P
(6,9,14)	P	(6,9,18)	P	(6,9,21)	P	(6,11,12)	P	(6,11,16)	P
(6,12,12)	8	(6,12,16)	9	(6,12,18)	9	(6,14,16)	P	(6,15,15)	P
(7,7,7)	7	(7,7,14)	7	(7,8,10)	P	(7,8,12)	P	(7,8,13)	7
(7,8,19)	P	(7,8,21)	P	(7,11,12)	P	(7,12,15)	P	(8,8,8)	7
(8,8,9)	7	(8,8,10)	7	(8,8,13)	9	(8,8,16)	9	(8,8,17)	P
(8,8,18)	9	(8,8,20)	P	(8,9,9)	7	(8,9,11)	P	(8,9,12)	P
(8,9,16)	P	(8,9,17)	Y	(8,9,18)	P	(8,9,19)	P	(8,10,10)	7
(8,10,12)	8	(8,10,15)	P	(8,10,18)	9	(8,12,16)	P	(8,13,13)	P
(8,13,15)	P	(9,9,9)	9	(9,9,10)	P	(9,9,13)	P	(9,9,16)	P
(9,9,18)	9	(9,10,10)	P	(9,10,11)	P	(9,10,14)	P	(9,13,13)	Y
(9,13,14)	P	(10,10,10)	9	(10,10,13)	P	(10,10,16)	P	(10,11,15)	9
(10,13,13)	P	(11,11,11)	P	(12,12,12)	9				

[a] Georgiou, Koukouvinos, Mitrouli, and Seberry [70, p338-339]

Table D.2 The 54 cases of $OD(36; s_1, s_2, 36 - s_1 - s_2)$

(1,1,34)	(1,13,22)	(2,11,23)	(3,10,23)	(6,6,24)	(8,10,18)
(1,2,33)	(1,14,21)	(2,12,22)	(3,11,22)	(6,7,23)	(8,12,16)
(1,3,32)	(1,17,18)	(2,13,21)	(3,15,18)	(6,9,21)	(8,13,15)
(1,5,30)	(2,2,32)	(2,16,18)	(4,8,24)	(6,12,18)	(9,9,18)
(1,6,29)	(2,3,31)	(2,17,17)	(4,16,16)	(6,14,16)	(9,13,14)
(1,8,27)	(2,6,28)	(3,3,30)	(5,5,26)	(6,15,15)	(10,10,16)
(1,9,26)	(2,7,27)	(3,6,27)	(5,6,25)	(7,8,21)	(10,11,15)
(1,10,25)	(2,8,26)	(3,8,25)	(5,8,23)	(8,8,20)	(10,13,13)
(1,11,24)	(2,9,25)	(3,9,24)	(5,13,18)	(8,9,19)	(12,12,12)

Appendix E
Orthogonal Designs in order 44

The main authors who have studied order 44 are Georgiou, Karabelas, Koukouvinos, Mitrouli and Seberry [68, 129, 130]. No systematic study of order 88 has been undertaken. Such a study is feasible given current computer technology.

E.1 Some theorems

We know

Lemma E.1. *All full orthogonal designs* $OD(2^t 11; x, y, 2^t 11 - x - y)$ *exist for any* $t \geq 3$.

Lemma E.2 (Geramita-Seberry [80]). *There are* $OD(44; 1, k)$, *for* $k \in \{0 \leq x \leq 43,\ x = a^2 + b^2 + c^2,\ x \neq 42\}$. $OD(44; 1, 42)$ *cannot exist.*

E.2 Orthogonal designs in Order 44

We summarize the known results for order 44.

1. We note from [135] that we have to test $\frac{1}{4}n^2 = 484$ cases. Hence 404 cases have been found, 67 2-tuples correspond to designs eliminated by number theory (NE) and 12 cases cannot be constructed using four circulant matrices. Table E.1 lists the 404 which correspond to designs which exist in order 44.
2. Table E.2 lists the $2-$tuple (s_1, s_2) designs for which an $OD(44; s_1, s_2)$ cannot exist.
3. A computer search, which we believe was exhaustive, was carried out which leads us to believe that

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5

a. there are no 4-$NPAF(2,41)$ sequences of length 11. This means that there are also no 4-$NPAF(1,2,41)$ sequences of length 11.
b. there are no 4-$NPAF(6,37)$ sequences of length 11.

4. The following $OD(44;1,a,43-a)$ and $OD(44;a,43-a)$ cannot be constructed using four circulant matrices in the Goethals-Seidel array:

$$\begin{array}{llllll} (5,38) & (8,35) & (12,31) & (14,29) & (16,27) & (20,23) \\ (1,5,38) & (1,8,35) & (1,12,31) & (1,14,29) & (1,16,27) & (1,20,23) \\ (6,37) & (10,33) & (13,30) & (15,28) & (19,24) & (21,22) \\ (1,6,37) & (1,10,33) & (1,13,30) & (1,15,28) & (1,19,24) & (1,21,22). \end{array}$$

5. The sequences given in [68] together with those in [129] can be used to construct the appropriate designs to establish that the necessary conditions for the existence of an $OD(44;s_1,s_2)$ are sufficient, except possibly for the following 12 cases which the Geramita-Verner Theorem and the Sum-Fill Theorem show cannot be constructed from four circulant matrices;

$$\begin{array}{llllll} (5,38) & (6,37) & (8,35) & (10,33) & (12,31) & (13,30) \\ (14,29) & (15,28) & (16,27) & (19,24) & (20,23) & (21,22). \end{array}$$

6. The necessary conditions for the existence of $OD(44;s_1,s_2)$ constructed from four circulant matrices in the Goethals-Seidel Theorem are sufficient.
7. There are 484 possible 2−tuples. Table E.1 lists the 404 which correspond to designs which exist in order 44: 68 2-tuples correspond to designs eliminated by number theory (NE).
   For 12 cases, if the designs exist, they cannot be constructed using circulant matrices (Y).
   P indicates that 4-PAF sequences with length 11 exist; n indicates 4-$NPAF$ sequences with length n exist.
8. Georgiou, Koukouvinos, Mitrouli and Seberry [68] give the first rows for the periodic and non-periodic sequences of lengths 10 and 11, noted in Table E.1, to use in the Goethals-Seidel array to find the designs.
9. From [129] we have the first rows to use in the Goethals-Seidel array to construct the 4-variable and 3-variable designs of lengths 10 and 11 given in Tables E.3 and E.4
10. The 238 4-tuples which satisfy the necessary conditions for existence in order 44 found by Magoon are given in Table E.5. Those marked * are known to exist from Chapter 4.

Table E.1: The existence of $OD(44;s_1,s_2)$.

s_1	s_2	n	s_1	s_2	n	s_1	s_2	n	s_1	s_2	n	s_1	s_2	n
1	1	1	3	15	5	5	38	Y	9	11	5	13	16	10
1	2	1	3	16	7	5	39	11	9	12	7	13	17	9
1	3	1	3	17	5	6	6	3	9	13	6	13	18	9
1	4	2	3	18	7	6	7	5	9	14	7	13	19	NE
1	5	2	3	19	7	6	8	5	9	15	NE	13	20	9

Continued on Next Page...

Table E.1 – Continued

s_1	s_2	n	s_1	s_2	n	s_1	s_2	n	s_1	s_2	n	s_1	s_2	n
1	6	3	3	20	NE	6	9	5	9	16	7	13	21	9
1	7	NE	3	21	NE	6	10	NE	9	17	7	13	22	P
1	8	3	3	22	7	6	11	5	9	18	7	13	23	9
1	9	3	3	23	7	6	12	5	9	19	7	13	24	P
1	10	3	3	24	7	6	13	7	9	20	9	13	25	P
1	11	3	3	25	7	6	14	5	9	21	9	13	26	P
1	12	4	3	26	9	6	15	7	9	22	9	13	27	NE
1	13	5	3	27	9	6	16	7	9	23	NE	13	28	P
1	14	5	3	28	9	6	17	7	9	24	9	13	29	P
1	15	NE	3	29	NE	6	18	7	9	25	9	13	30	Y
1	16	5	3	30	9	6	19	7	9	26	9	13	31	P
1	17	5	3	31	10	6	20	7	9	27	9	14	14	7
1	18	5	3	32	9	6	21	7	9	28	NE	14	15	P
1	19	5	3	33	9	6	22	7	9	29	P	14	16	8
1	20	7	3	34	10	6	23	9	9	30	$P,20$	14	17	P
1	21	7	3	35	11	6	24	8	9	31	NE	14	18	NE
1	22	7	3	36	11	6	25	9	9	32	$P,15$	14	19	9
1	23	NE	3	37	NE	6	26	NE	9	33	$P,20$	14	20	9
1	24	7	3	38	11	6	27	9	9	34	P	14	21	9
1	25	7	3	39	11	6	28	9	9	35	P	14	22	9
1	26	9	3	40	NE	6	29	P	10	10	5	14	23	P
1	27	7	3	41	11	6	30	9	10	11	7	14	24	P
1	28	NE	4	4	2	6	31	10	10	12	7	14	25	P
1	29	9	4	5	3	6	32	10	10	13	7	14	26	10
1	30	11	4	6	3	6	33	$P,20$	10	14	7	14	27	P
1	31	NE	4	7	NE	6	34	10	10	15	7	14	28	$P,12$
1	32	9	4	8	3	6	35	P	10	16	7	14	29	Y
1	33	9	4	9	5	6	36	11	10	17	NE	14	30	P
1	34	11	4	10	5	6	37	Y	10	18	7	15	15	9
1	35	11	4	11	5	6	38	11	10	19	P	15	16	NE
1	36	11	4	12	5	7	7	4	10	20	8	15	17	NE
1	37	11	4	13	5	7	8	6	10	21	9	15	18	9
1	38	11	4	14	5	7	9	NE	10	22	NE	15	19	9
1	39	NE	4	15	NE	7	10	5	10	23	9	15	20	NE
1	40	11	4	16	5	7	11	7	10	24	NE	15	21	9
1	41	11	4	17	7	7	12	7	10	25	9	15	22	P
1	42	NE	4	18	7	7	13	5	10	26	9	15	23	P
1	43	11	4	19	7	7	14	7	10	27	P	15	24	P
2	2	1	4	20	7	7	15	7	10	28	10	15	25	NE
2	3	2	4	21	7	7	16	NE	10	29	P	15	26	P
2	4	2	4	22	7	7	17	NE	10	30	10	15	27	$P,20$
2	5	3	4	23	NE	7	18	7	10	31	P	15	28	Y
2	6	2	4	24	7	7	19	8	10	32	11	15	29	P
2	7	3	4	25	9	7	20	9	10	33	Y	16	16	8
2	8	3	4	26	8	7	21	7	10	34	11	16	17	9
2	9	5	4	27	9	7	22	9	11	11	6	16	18	9
2	10	3	4	28	NE	7	23	9	11	12	7	16	19	NE
2	11	5	4	29	9	7	24	9	11	13	NE	16	20	9
2	12	5	4	30	9	7	25	NE	11	14	7	16	21	11
2	13	5	4	31	NE	7	26	9	11	15	7	16	22	10

Continued on Next Page...

Table E.1 – Continued

s_1	s_2	n	s_1	s_2	n	s_1	s_2	n	s_1	s_2	n	s_1	s_2	n
2	14	NE	4	32	9	7	27	9	11	16	NE	16	23	NE
2	15	5	4	33	10	7	28	NE	11	17	7	16	24	10
2	16	5	4	34	10	7	29	9	11	18	9	16	25	P
2	17	5	4	35	11	7	30	P	11	19	9	16	26	11
2	18	5	4	36	10,11	7	31	10	11	20	NE	16	27	Y
2	19	7	4	37	P	7	32	11	11	21	NE	16	28	NE
2	20	6	4	38	11	7	33	NE	11	22	9	17	17	9
2	21	7	4	39	NE	7	34	P	11	23	9	17	18	9
2	22	7	4	40	11	7	35	P	11	24	9	17	19	9
2	23	7	5	5	3	7	36	NE	11	25	9	17	20	11
2	24	7	5	6	3	7	37	11	11	26	P	17	21	P
2	25	9	5	7	3	8	8	5	11	27	P	17	22	P
2	26	7	5	8	5	8	9	5	11	28	P	17	23	NE
2	27	9	5	9	5	8	10	5	11	29	NE	17	24	P
2	28	8	5	10	5	8	11	5	11	30	P	17	25	P
2	29	9	5	11	NE	8	12	5	11	31	P	17	26	P
2	30	NE	5	12	NE	8	13	7	11	32	P	17	27	P
2	31	9	5	13	5	8	14	NE	11	33	P	18	18	9
2	32	9	5	14	5	8	15	7	12	12	7	18	19	P
2	33	9	5	15	5	8	16	7	12	13	NE	18	20	10
2	34	9	5	16	7	8	17	7	12	14	7	18	21	P
2	35	10	5	17	7	8	18	7	12	15	NE	18	22	10
2	36	10,11	5	18	7	8	19	9	12	16	7	18	23	P
2	37	11	5	19	NE	8	20	7	12	17	9	18	24	11
2	38	10,11	5	20	7	8	21	9	12	18	8	18	25	P
2	39	11	5	21	7	8	22	8	12	19	9	18	26	P
2	40	11	5	22	9	8	23	9	12	20	NE	19	19	P
2	41	P	5	23	7	8	24	9	12	21	NE	19	20	NE
2	42	11	5	24	9	8	25	9	12	22	9	19	21	NE
3	3	2	5	25	9	8	26	9	12	23	NE	19	22	P
3	4	3	5	26	9	8	27	P	12	24	9	19	23	P
3	5	NE	5	27	NE	8	28	9	12	25	P	19	24	Y
3	6	3	5	28	9	8	29	P	12	26	P	19	25	P
3	7	3	5	29	9	8	30	NE	12	27	20	20	20	10
3	8	3	5	30	10	8	31	P	12	28	10	20	21	P
3	9	3	5	31	9	8	32	10	12	29	NE	20	22	11
3	10	5	5	32	10	8	33	P	12	30	P,13	20	23	Y
3	11	5	5	33	10	8	34	11	12	31	Y	20	24	11
3	12	5	5	34	P	8	35	Y	12	32	11	21	21	11
3	13	NE	5	35	NE	8	36	11	13	13	7	21	22	Y
3	14	5	5	36	11	9	9	5	13	14	9	21	23	P
			5	37	11	9	10	5	13	15	7	22	22	11

Table E.2 $OD(44; s_1, s_2)$ cannot exist for the following 2−tuples (s_1, s_2) [a]

(1,7)	(3,5)	(4,23)	(6,26)	(9,15)	(11,21)	(15,16)
(1,15)	(3,13)	(4,28)	(7,9)	(9,23)	(11,29)	(15,17)
(1,23)	(3,20)	(4,31)	(7,16)	(9,28)	(12,13)	(15,20)
(1,28)	(3,21)	(4,39)	(7,17)	(9,31)	(12,15)	(15,25)
(1,31)	(3,29)	(5,11)	(7,25)	(10,17)	(12,20)	(16,19)
(1,39)	(3,37)	(5,12)	(7,28)	(10,22)	(12,21)	(16,23)
(1,42)	(3,40)	(5,19)	(7,33)	(10,24)	(12,29)	(16,28)
(2,14)	(4,7)	(5,27)	(7,36)	(11,13)	(13,19)	(17,23)
(2,30)	(4,15)	(5,35)	(8,14)	(11,16)	(13,27)	(19,20)
			(8,30)	(11,20)	(14,18)	(19,21)

[a] Koukouvinos, Mitrouli, and Seberry [129, p267-268] © Charles Babbage Research Centre

Table E.3 Some order 44 4-variable sequences with zero and non-periodic autocorrelation function [a]

Design	A_1 A_2	A_3 A_4
(1,4,10,10)	$b\ a\ \bar{b}\ 0\ 0\ 0\ 0\ 0\ 0\ 0$	$c\ \bar{c}\ \bar{c}\ c\ d\ c\ b\ b\ b\ \bar{b}$
	$b\ 0\ b\ 0\ 0\ 0\ 0\ 0\ 0\ 0$	$c\ \bar{c}\ \bar{c}\ \bar{c}\ d\ c\ d\ \bar{d}\ \bar{d}\ \bar{d}$
(1,4,16,16)	$c\ d\ 0\ d\ \bar{c}\ a\ c\ \bar{d}\ 0\ \bar{d}\ \bar{c}$	$c\ \bar{d}\ b\ d\ c\ 0\ c\ d\ \bar{b}\ \bar{d}\ c$
	$c\ d\ 0\ d\ \bar{c}\ 0\ \bar{c}\ d\ 0\ d\ c$	$c\ \bar{d}\ b\ d\ c\ 0\ \bar{c}\ \bar{d}\ b\ d\ \bar{c}$
(2,2,4,36)	$b\ a\ a\ a\ \bar{a}\ a\ a\ \bar{a}\ d\ a\ \bar{a}$	$b\ \bar{a}\ \bar{a}\ \bar{a}\ a\ \bar{a}\ \bar{a}\ \bar{a}\ \bar{c}\ a\ a$
	$b\ a\ a\ a\ \bar{a}\ a\ \bar{a}\ a\ \bar{d}\ \bar{a}\ a$	$b\ \bar{a}\ \bar{a}\ \bar{a}\ a\ \bar{a}\ a\ a\ c\ \bar{a}\ \bar{a}$
(2,2,8,32)	$a\ d\ c\ \bar{d}\ d\ \bar{d}\ d\ \bar{d}\ \bar{d}\ c\ d$	$b\ d\ c\ \bar{d}\ d\ d\ d\ d\ d\ \bar{c}\ \bar{d}$
	$a\ \bar{d}\ \bar{c}\ d\ \bar{d}\ d\ \bar{d}\ d\ d\ \bar{c}\ \bar{d}$	$b\ \bar{d}\ \bar{c}\ d\ \bar{d}\ \bar{d}\ \bar{d}\ \bar{d}\ \bar{d}\ c\ d$
(2,2,18,18)	$d\ c\ a\ \bar{c}\ \bar{d}\ c\ \bar{c}\ c\ c\ c$	$c\ \bar{d}\ b\ d\ \bar{c}\ d\ \bar{d}\ d\ d\ d$
	$d\ c\ a\ \bar{c}\ \bar{d}\ \bar{c}\ c\ \bar{c}\ \bar{c}\ \bar{c}$	$c\ \bar{d}\ b\ d\ \bar{c}\ \bar{d}\ d\ \bar{d}\ \bar{d}\ \bar{d}$
(2,2,20,20)	$\bar{a}\ a\ a\ a\ b\ a\ b\ \bar{b}\ \bar{b}\ b\ c$	$b\ \bar{b}\ \bar{b}\ \bar{b}\ a\ \bar{b}\ a\ \bar{a}\ \bar{a}\ a\ d$
	$\bar{a}\ a\ a\ a\ b\ a\ b\ \bar{b}\ \bar{b}\ b\ \bar{c}$	$b\ \bar{b}\ \bar{b}\ \bar{b}\ a\ \bar{b}\ a\ \bar{a}\ \bar{a}\ a\ \bar{d}$
(2,4,16,18)	$d\ c\ a\ \bar{c}\ \bar{d}\ b\ c\ \bar{d}\ c\ d$	$d\ c\ d\ \bar{c}\ d\ b\ \bar{c}\ d\ \bar{c}\ \bar{d}$
	$d\ c\ a\ \bar{c}\ \bar{d}\ \bar{b}\ \bar{c}\ d\ \bar{c}\ \bar{d}$	$d\ c\ d\ \bar{c}\ d\ \bar{b}\ c\ \bar{d}\ c\ d$
(2,6,12,16)	$d\ 0\ b\ 0\ d\ \bar{c}\ d\ c\ a\ \bar{c}\ \bar{d}$	$d\ 0\ \bar{d}\ 0\ b\ \bar{c}\ b\ c\ \bar{d}\ c\ d$
	$d\ 0\ b\ 0\ d\ \bar{c}\ \bar{d}\ \bar{c}\ \bar{a}\ c\ d$	$d\ 0\ \bar{d}\ 0\ b\ \bar{c}\ \bar{b}\ \bar{c}\ d\ \bar{c}\ \bar{d}$
(2,8,16,16)	$b\ d\ c\ \bar{c}\ \bar{d}\ b\ d\ \bar{c}\ 0\ \bar{c}\ d$	$b\ \bar{d}\ \bar{c}\ \bar{c}\ \bar{d}\ \bar{b}\ \bar{d}\ c\ a\ \bar{c}\ d$
	$b\ d\ c\ \bar{c}\ \bar{d}\ b\ \bar{d}\ c\ 0\ c\ \bar{d}$	$b\ \bar{d}\ \bar{c}\ \bar{c}\ \bar{d}\ \bar{b}\ d\ \bar{c}\ \bar{a}\ c\ \bar{d}$
(2,10,10,18)	$d\ \bar{c}\ a\ c\ \bar{d}\ b\ d\ \bar{c}\ \bar{d}\ \bar{c}$	$b\ \bar{d}\ b\ d\ c\ d\ b\ d\ \bar{b}\ d$
	$d\ \bar{c}\ a\ c\ \bar{d}\ \bar{b}\ \bar{d}\ c\ d\ c$	$b\ \bar{d}\ b\ d\ c\ \bar{d}\ \bar{b}\ \bar{d}\ b\ \bar{d}$
(4,4,16,16)	$a\ d\ c\ d\ \bar{c}\ a\ \bar{d}\ \bar{c}\ \bar{d}\ c$	$b\ c\ \bar{d}\ c\ d\ b\ \bar{c}\ d\ \bar{c}\ \bar{d}$
	$a\ d\ c\ d\ \bar{c}\ \bar{a}\ d\ c\ d\ \bar{c}$	$b\ c\ \bar{d}\ c\ d\ \bar{b}\ c\ \bar{d}\ c\ d$

[a] Koukouvinos, Mitrouli, and Seberry [129, p278-279] © Charles Babbage Research Centre

Table E.3 Some order 44 4-variable sequences with zero and non-periodic autocorrelation function [a] *(continued)*

Design	A_1	A_2	A_3	A_4
$(4,6,12,18)$	$b\ a\ \bar{d}\ c\ d\ d\ a\ \bar{b}\ \bar{c}\ \bar{d}$		$d\ c\ \bar{d}\ c\ \bar{b}\ d\ \bar{c}\ d\ c\ d$	
	$b\ a\ \bar{d}\ c\ d\ \bar{d}\ \bar{a}\ b\ c\ d$		$d\ c\ \bar{d}\ c\ \bar{b}\ \bar{d}\ c\ \bar{d}\ \bar{c}\ \bar{d}$	
$(4,8,8,16)$	$d\ c\ a\ \bar{c}\ d\ d\ b\ \bar{a}\ \bar{b}\ d$		$d\ b\ 0\ b\ \bar{d}\ d\ c\ 0\ c\ \bar{d}$	
	$d\ c\ a\ \bar{c}\ d\ \bar{d}\ \bar{b}\ a\ b\ \bar{d}$		$d\ b\ 0\ b\ \bar{d}\ \bar{d}\ \bar{c}\ 0\ \bar{c}\ d$	
$(4,10,10,16)$	$b\ c\ a\ \bar{c}\ b\ b\ d\ \bar{a}\ \bar{d}\ b$		$b\ c\ d\ c\ \bar{b}\ b\ d\ \bar{c}\ d\ \bar{b}$	
	$b\ c\ a\ \bar{c}\ b\ \bar{b}\ \bar{d}\ a\ d\ \bar{b}$		$b\ c\ d\ c\ \bar{b}\ \bar{b}\ \bar{d}\ c\ \bar{d}\ b$	
$(8,8,10,10)$	$a\ c\ 0\ \bar{c}\ a\ a\ c\ d\ c\ \bar{a}$		$b\ d\ 0\ \bar{d}\ b\ b\ d\ \bar{c}\ d\ \bar{b}$	
	$a\ c\ 0\ \bar{c}\ a\ \bar{a}\ \bar{c}\ \bar{d}\ \bar{c}\ a$		$b\ d\ 0\ \bar{d}\ b\ \bar{b}\ \bar{d}\ c\ \bar{d}\ b$	
$(10,10,10,10)$	$a\ b\ b\ d\ \bar{d}\ \bar{b}\ a\ a\ c\ \bar{c}$		$d\ c\ c\ \bar{a}\ a\ \bar{c}\ d\ d\ \bar{b}\ b$	
	$a\ b\ b\ d\ \bar{d}\ b\ \bar{a}\ \bar{a}\ \bar{c}\ c$		$d\ c\ c\ \bar{a}\ a\ c\ \bar{d}\ \bar{d}\ b\ \bar{b}$	

[a] Koukouvinos, Mitrouli, and Seberry [129, p278-279] © Charles Babbage Research Centre

Table E.4 Some order 44 3-variable sequences with zero and non-periodic autocorrelation function [a]

Design	A_1	A_2	A_3	A_4
$(1,4,32)$	$b\ \bar{b}\ \bar{b}\ \bar{b}\ a\ a\ b\ b\ b\ \bar{b}$		$b\ b\ \bar{b}\ b\ c\ \bar{b}\ b\ \bar{b}\ \bar{b}\ 0$	
	$b\ \bar{b}\ \bar{b}\ \bar{b}\ a\ \bar{a}\ \bar{b}\ \bar{b}\ \bar{b}\ b$		$b\ b\ \bar{b}\ b\ 0\ b\ \bar{b}\ b\ b\ 0$	
$(1,9,34)$	$b\ \bar{b}\ \bar{b}\ b\ b\ 0\ \bar{b}\ \bar{b}\ b\ b\ \bar{b}$		$b\ b\ b\ b\ b\ b\ b\ \bar{b}\ b\ \bar{b}\ \bar{b}$	
	$a\ \bar{a}\ \bar{a}\ \bar{a}\ b\ b\ \bar{b}\ b\ \bar{b}\ \bar{a}\ \bar{b}$		$a\ \bar{a}\ b\ \bar{b}\ \bar{a}\ \bar{b}\ \bar{b}\ \bar{b}\ b\ a\ \bar{b}$	
$(1,11,32)$	$b\ \bar{b}\ b\ b\ b\ 0\ \bar{b}\ \bar{b}\ \bar{b}\ b\ \bar{b}$		$a\ b\ b\ \bar{b}\ \bar{b}\ b\ \bar{b}\ b\ b\ b\ b$	
	$a\ a\ \bar{b}\ a\ b\ \bar{b}\ b\ b\ \bar{b}\ \bar{b}\ b$		$a\ a\ \bar{a}\ \bar{a}\ b\ b\ \bar{a}\ a\ \bar{a}\ b\ b$	
$(1,17,26)$	$a\ a\ a\ \bar{a}\ a\ 0\ \bar{a}\ a\ \bar{a}\ \bar{a}\ \bar{a}$		$b\ b\ b\ b\ b\ \bar{b}\ b\ b\ \bar{b}\ a\ \bar{b}$	
	$a\ a\ b\ a\ b\ \bar{b}\ \bar{b}\ a\ \bar{b}\ b\ \bar{b}$		$b\ b\ b\ a\ b\ \bar{b}\ \bar{b}\ b\ b\ \bar{b}\ \bar{a}$	
$(1,18,25)$	$a\ a\ a\ \bar{a}\ a\ 0\ \bar{a}\ a\ \bar{a}\ \bar{a}\ \bar{a}$		$a\ a\ b\ \bar{b}\ b\ a\ \bar{b}\ \bar{b}\ \bar{b}\ b\ b$	
	$a\ a\ \bar{b}\ a\ \bar{b}\ \bar{b}\ b\ b\ \bar{b}\ b\ b$		$a\ \bar{a}\ \bar{b}\ \bar{b}\ \bar{b}\ b\ \bar{b}\ b\ \bar{b}\ \bar{b}\ \bar{b}$	
$(2,2,34)$	$c\ c\ c\ \bar{c}\ \bar{c}\ c\ \bar{c}\ \bar{c}\ a\ c$		$c\ c\ c\ 0\ c\ \bar{c}\ c\ \bar{c}\ b\ c$	
	$c\ c\ c\ \bar{c}\ \bar{c}\ c\ \bar{c}\ c\ \bar{a}\ \bar{c}$		$c\ c\ c\ 0\ c\ \bar{c}\ c\ c\ \bar{b}\ \bar{c}$	
$(2,4,32)$	$b\ b\ \bar{b}\ b\ a\ a\ \bar{b}\ \bar{b}\ b\ \bar{b}$		$b\ \bar{b}\ b\ b\ 0\ c\ b\ \bar{b}\ b\ b$	
	$b\ b\ b\ \bar{b}\ a\ \bar{a}\ \bar{b}\ \bar{b}\ \bar{b}\ b$		$b\ b\ b\ \bar{b}\ 0\ \bar{c}\ b\ b\ b\ \bar{b}$	
$(2,12,22)$	$b\ c\ c\ 0\ c\ \bar{c}\ b\ a\ \bar{b}\ c$		$b\ c\ \bar{c}\ 0\ \bar{c}\ \bar{c}\ b\ c\ b\ \bar{c}$	
	$b\ c\ c\ 0\ c\ c\ \bar{b}\ \bar{a}\ b\ \bar{c}$		$b\ c\ \bar{c}\ 0\ \bar{c}\ c\ \bar{b}\ \bar{c}\ \bar{b}\ c$	

[a] Koukouvinos, Mitrouli, and Seberry [129, p276-280] © Charles Babbage Research Centre

Table E.5 The theoretically possible 4-tuples for order 44.

1: (1,1,1,1) : 4	60: (1,4,8,8) : 21	119: (2,3,6,16) : 27	179: (4,4,4,25) : 37
2: (1,1,1,4) : 7	61: (1,4,8,18) : 31	120: (2,3,6,25) : 36	180: (4,4,5,5) : 18
3: (1,1,1,9) : 12	62: (1,4,9,9) : 23	121: (2,3,9,24) : 38	181: (4,4,5,20) : 33
4: (1,1,1,16) : 19	63: (1,4,9,16) : 30	122: (2,3,10,15) : 30	182: (4,4,8,8) : 24
5: (1,1,1,25) : 28	64: (1,4,9,25) : 39	123: (2,4,4,8) : 18	183: (4,4,8,18) : 34
6: (1,1,1,36) : 39	65: (1,4,10,10) : 25	124: (2,4,4,18) : 28	184: (4,4,9,9) : 26
7: (1,1,2,2) : 6	66: (1,4,13,13) : 31	125: (2,4,4,32) : 42	185: (4,4,9,16) : 33
8: (1,1,2,8) : 12	67: (1,4,16,16) : 37	126: (2,4,6,12) : 24	186: (4,4,9,25) : 42
9: (1,1,2,18) : 22	68: (1,4,17,17) : 39	127: (2,4,6,27) : 39	187: (4,4,10,10) : 28
10: (1,1,2,32) : 36	69: (1,4,18,18) : 41	128: (2,4,8,9) : 23	188: (4,4,13,13) : 34
11: (1,1,4,4) : 10	70: (1,5,5,9) : 20	129: (2,4,8,16) : 30	189: (4,4,16,16) : 40
12: (1,1,4,9) : 15	71: (1,5,5,16) : 27	130: (2,4,8,25) : 39	190: (4,4,17,17) : 42
13: (1,1,4,16) : 22	72: (1,5,5,25) : 36	131: (2,4,9,18) : 33	191: (4,4,18,18) : 44
14: (1,1,4,25) : 31	73: (1,5,6,30) : 42	132: (2,4,11,22) : 39	192: (4,5,5,9) : 23
15: (1,1,4,36) : 42	74: (1,5,9,20) : 35	133: (2,4,12,24) : 42	193: (4,5,5,16) : 30
16: (1,1,5,5) : 12	75: (1,5,16,20) : 42	134: (2,4,16,18) : 40	194: (4,5,5,25) : 39
17: (1,1,5,20) : 27	76: (1,6,8,12) : 27	135: (2,5,5,8) : 20	195: (4,5,9,20) : 38
18: (1,1,8,8) : 18	77: (1,6,8,27) : 42	136: (2,5,5,18) : 30	196: (4,6,8,12) : 30
19: (1,1,8,18) : 28	78: (1,6,12,18) : 37	137: (2,5,5,32) : 44	197: (4,6,12,18) : 40
20: (1,1,8,32) : 42	79: (1,6,14,21) : 42	138: (2,5,8,20) : 35	198: (4,8,8,9) : 29
21: (1,1,9,9) : 20	80: (1,8,8,9) : 26	139: (2,6,7,21) : 36	199: (4,8,8,16) : 36
22: (1,1,9,16) : 27	81: (1,8,8,16) : 33	140: (2,6,9,12) : 29	200: (4,8,9,18) : 39
23: (1,1,9,25) : 36	82: (1,8,8,25) : 42	141: (2,6,9,27) : 44	201: (4,9,9,9) : 31
24: (1,1,10,10) : 22	83: (1,8,9,18) : 36	142: (2,6,12,16) : 36	202: (4,9,9,16) : 38
25: (1,1,13,13) : 28	84: (1,8,11,22) : 42	143: (2,8,8,8) : 26	203: (4,9,10,10) : 33
26: (1,1,16,16) : 34	85: (1,9,9,9) : 28	144: (2,8,8,18) : 36	204: (4,9,13,13) : 39
27: (1,1,17,17) : 36	86: (1,9,9,16) : 35	145: (2,8,9,9) : 28	205: (4,10,10,16) : 40
28: (1,1,18,18) : 38	87: (1,9,9,25) : 44	146: (2,8,9,16) : 35	206: (5,5,5,5) : 20
29: (1,1,20,20) : 42	88: (1,9,10,10) : 30	147: (2,8,9,25) : 44	207: (5,5,5,20) : 35
30: (1,2,2,4) : 9	89: (1,9,13,13) : 36	148: (2,8,10,10) : 30	208: (5,5,8,8) : 26
31: (1,2,2,9) : 14	90: (1,9,16,16) : 42	149: (2,8,13,13) : 36	209: (5,5,8,18) : 36
32: (1,2,2,16) : 21	91: (1,9,17,17) : 44	150: (2,8,16,16) : 42	210: (5,5,9,9) : 28
33: (1,2,2,25) : 30	92: (1,10,10,16) : 37	151: (2,8,17,17) : 44	211: (5,5,9,16) : 35
34: (1,2,2,36) : 41	93: (2,2,2,2) : 8	152: (2,9,9,18) : 38	212: (5,5,9,25) : 44
35: (1,2,3,6) : 12	94: (2,2,2,8) : 14	153: (2,9,11,22) : 44	213: (5,5,10,10) : 30
36: (1,2,3,24) : 30	95: (2,2,2,18) : 24	154: (2,10,10,18) : 40	214: (5,5,13,13) : 36
37: (1,2,4,8) : 15	96: (2,2,2,32) : 38	155: (2,10,12,15) : 39	215: (5,5,16,16) : 42
38: (1,2,4,18) : 25	97: (2,2,4,4) : 12	156: (3,3,3,3) : 12	216: (5,5,17,17) : 44
39: (1,2,4,32) : 39	98: (2,2,4,9) : 17	157: (3,3,3,12) : 24	217: (5,8,8,20) : 41
40: (1,2,6,12) : 21	99: (2,2,4,26) : 24	158: (3,3,3,27) : 36	218: (6,6,6,6) : 24
41: (1,2,6,27) : 36	100: (2,2,4,25) : 33	159: (3,3,6,6) : 18	219: (6,6,6,24) : 41
42: (1,2,8,9) : 20	101: (2,2,4,36) : 44	160: (3,3,6,24) : 36	220: (6,6,12,12) : 36
43: (1,2,8,16) : 27	102: (2,2,5,5) : 14	161: (3,3,12,12) : 30	221: (6,6,15,15) : 42
44: (1,2,8,25) : 36	103: (2,2,5,20) : 29	162: (3,3,15,15) : 36	222: (6,7,8,21) : 42
45: (1,2,9,18) : 30	104: (2,2,8,8) : 20	163: (3,4,6,8) : 21	223: (6,8,9,12) : 35
46: (1,2,9,32) : 44	105: (2,2,8,18) : 30	164: (3,4,6,18) : 31	224: (6,8,12,16) : 42
47: (1,2,11,22) : 36	106: (2,2,8,32) : 44	165: (3,4,8,24) : 39	225: (7,7,7,7) : 28
48: (1,2,12,24) : 39	107: (2,2,9,9) : 22	166: (3,6,6,12) : 27	226: (7,7,14,14) : 42
49: (1,2,16,18) : 37	108: (2,2,9,16) : 29	167: (3,6,6,27) : 42	227: (8,8,8,8);32
50: (1,3,6,8) : 18	109: (2,2,9,25) : 38	168: (3,6,8,9) : 26	228: (8,8,8,′18);42
51: (1,3,6,18) : 28	110: (2,2,10,10) : 24	169: (3,6,8,16) : 33	229: (8,8,9,9) : 34
52: (1,3,6,32) : 42	111: (2,2,13,13) : 30	170: (3,6,8,25) : 42	230: (8,8,9,16) : 41
53: (1,3,8,24) : 36	112: (2,2,16,16) : 36	171: (3,6,9,18) : 36	231: (8,8,10,10) : 36
54: (1,4,4,4) : 13	113: (2,2,17,17) : 38	172: (3,6,11,22) : 42	232: (8,8,13,13) : 42
55: (1,4,4,9) : 18	114: (2,2,18,18) : 40	173: (3,8,9,24) : 44	233: (8,9,9,18) : 45
56: (1,4,4,16) : 25	115: (2,2,20,20) : 44	174: (3,8,10,15) : 36	234: (9,9,9,9) : 36
57: (1,4,4,25) : 34	116: (2,3,4,6) : 15	175: (3,12,12,12) : 39	235: (9,9,10,10) : 38
58: (1,4,5,5) : 15	117: (2,3,4,24) : 33	176: (4,4,4,4) : 16	236: (9,9,13,13) : 44
59: (1,4,5,20) : 30	118: (2,3,6,9) : 20	177: (4,4,4,9) : 21	237: (10,10,10,10) : 40
		178: (4,4,4,16) : 28	238: (11,11,11,11) : 44

Appendix F
Orthogonal Designs in Powers of 2, Especially Order 16, 32 and 64

F.1 Some Theorems

Theorem F.1 (P.J. Robinson). [80, p.268] *There is an orthogonal design* $OD(2^t;1,1,1,1,2,2,4,4,\ldots,2^{t-2},2^{t-2})$.

Using Corollary 6.8 we have

Lemma F.1. *All four variable designs* $OD(32;a,b,c,32-a-b-c)$, $OD(64;a,b,c,64-a-b-c)$, $OD(128;a,b,c,128-a-b-c)$ *exist.*

By equating variables we obtain:

Lemma F.2 (P.J. Robinson). *All orthogonal designs of type* $(1,1,a,b,c)$, $a+b+c=2^t-2$, *exist in order* 2^t, $t>3$.

Hence we have the following results of Wallis.

Lemma F.3. *All orthogonal designs of type* $(a,b,2^t-a-b)$ *(i.e. full orthogonal designs) exist in order* 2^t.

Lemma F.4. *All orthogonal designs on two variables exist in orders* 2^t.

From [122] and Tables 8.1 and 8.2 we have

Theorem F.2 (Robinson Kharaghani Tayfeh-Rezaie). *An* $OD(n;1,1,1,1,1,n-5)$ *exists if and only if* $n=8,16,24,32,40$.

Theorem F.3 (Kharaghani Tayfeh-Rezaie). *There exist* $OD(32;1,1,1,1,1,1,12,15)$ *and* $OD(32;1,1,1,1,1,1,9,9,9)$. *Hence there exists an* $OD(32;1,1,1,1,1,1,27)$.

We now consider specific powers of two.

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5

F.2 Orthogonal Designs in Order 16

We summarize the known results for order 16.

1. The Radon number is 9.
2. Table F.1 lists all 9-tuples for orthogonal design in order 16.
3. All designs on n variables, $n \leq 9$, which exist can be obtained by equating and killing variables in the 9 variable designs which exist and the 8 variable designs listed in Table F.2.
4. Many 9 and 8 tuples are proved non-existent by theorems of Shapiro and Geramita-Verner. The remainder are proved non-existent by combinatorial arguments in the PhD thesis of Peter J. Robinson [166].
5. Table F.3 lists the 9-tuples which cannot be the type of an orthogonal design in order 16.
6. Table F.4 gives the 16 cases of 9-tuples in order 16 which are excluded by P. Robinson.
7. The $(1,1,1,1,1,1,1,1,1)$ design is exhibited in section 4.2 and the (1,1,2,2,2,2,2,2,2) design is obtained by using Theorem 4.3 on the (1,1,1,1,1,1,1,1) design in order 8 exhibited in Section 4.2.
8. The (1,1,1,1,1,1,3,3) and (1,1,1,1,2,2,3,3) designs are given in Example 6.6. The (1,1,1,2,2,3,3,3), (1,1,1,1,1,2,2,2,2), (1,1,1,1,1,1,1,1,2) and (1,1,2,2,2,2,3,3) designs are given in Example 6.4.
9. There are 67 8-tuples which might be the type of an orthogonal design in order 16. The following 4 cannot be the types of orthogonal designs by the results of Geramita and Verner:

$$(1,1,1,1,1,3,3,4) \quad (1,1,1,1,2,2,2,5) \quad (1,1,1,2,2,2,3,3)$$
$$(1,1,2,2,2,2,2,3).$$

10. We exhibit the remaining designs of the enunciation but we first consider the matrix

$$PR = \left[\begin{array}{cccc|cccc|cccc|cccc}
X_1 & X_2 & X_3 & M & X_4 & N & Q & P & A & B & C & D & E & F & G & H \\
\bar{X}_2 & X_1 & M & \bar{X}_3 & N & \bar{X}_4 & P & \bar{Q} & B & \bar{A} & D & \bar{C} & F & \bar{E} & H & \bar{G} \\
\bar{X}_3 & \bar{M} & X_1 & X_2 & Q & \bar{P} & \bar{X}_4 & N & C & \bar{D} & \bar{A} & B & G & \bar{H} & \bar{E} & F \\
\bar{M} & X_3 & \bar{X}_2 & X_1 & \bar{P} & \bar{Q} & N & X_4 & \bar{D} & \bar{C} & B & A & \bar{H} & \bar{G} & F & E \\
\hline
\bar{X}_4 & \bar{N} & \bar{Q} & P & X_1 & X_2 & X_3 & \bar{M} & E & \bar{F} & \bar{G} & H & \bar{A} & B & C & \bar{D} \\
\bar{N} & X_4 & P & Q & \bar{X}_2 & X_1 & \bar{M} & \bar{X}_3 & \bar{F} & \bar{E} & H & G & B & A & \bar{D} & \bar{C} \\
\bar{Q} & \bar{P} & X_4 & \bar{N} & \bar{X}_3 & M & X_1 & X_2 & \bar{G} & \bar{H} & \bar{E} & \bar{F} & C & D & A & B \\
\bar{P} & Q & \bar{N} & \bar{X}_4 & M & X_3 & \bar{X}_2 & X_1 & \bar{H} & G & \bar{F} & E & D & \bar{C} & B & \bar{A} \\
\hline
\bar{A} & \bar{B} & \bar{C} & D & \bar{E} & F & G & H & X_1 & X_2 & X_3 & R & X_4 & S & T & U \\
\bar{B} & A & D & C & F & E & H & \bar{G} & \bar{X}_2 & X_1 & R & \bar{X}_3 & S & \bar{X}_4 & U & \bar{T} \\
\bar{C} & \bar{D} & A & \bar{B} & G & \bar{H} & E & F & \bar{X}_3 & \bar{R} & X_1 & X_2 & T & \bar{U} & \bar{X}_4 & S \\
\bar{D} & C & \bar{B} & \bar{A} & \bar{H} & \bar{G} & F & \bar{E} & \bar{R} & X_3 & \bar{X}_2 & X_1 & \bar{U} & \bar{T} & S & X_4 \\
\hline
\bar{E} & \bar{F} & \bar{G} & H & A & \bar{B} & \bar{C} & \bar{D} & \bar{X}_4 & \bar{S} & \bar{T} & U & X_1 & X_2 & X_3 & \bar{R} \\
\bar{F} & E & H & G & \bar{B} & \bar{A} & \bar{D} & C & \bar{S} & X_4 & U & T & \bar{X}_2 & X_1 & \bar{R} & \bar{X}_3 \\
\bar{G} & \bar{H} & E & \bar{F} & \bar{C} & D & \bar{A} & \bar{B} & \bar{T} & \bar{U} & X_4 & \bar{S} & \bar{X}_3 & R & X_1 & X_2 \\
\bar{H} & G & \bar{F} & \bar{E} & D & C & \bar{B} & A & \bar{U} & T & \bar{S} & \bar{X}_4 & R & X_3 & \bar{X}_2 & X_1
\end{array}\right]$$

This matrix is an orthogonal design if and only if the following conditions are satisfied:

$$\{|M|, |N|, |Q|, |P|\} = \{|R|, |S|, |T|, |U|\}$$

$$\begin{aligned}
(M+R)D + (N+S)F + (Q+T)G + (P+U)H &= 0 \\
(M+R)C + (N+S)E + (Q-T)H - (P-U)G &= 0 \\
(M+R)B + (N-S)H - (Q+T)E - (P-U)F &= 0 \\
(M+R)A + (N-S)G - (Q-T)F + (P+U)E &= 0 \\
(R-M)H + (N+S)B + (Q+T)C + (P-U)D &= 0 \\
(R-M)G + (N+S)A + (Q-T)D - (P+U)C &= 0 \\
(R-M)F + (N-S)D - (Q+T)A - (P+U)B &= 0 \\
(R-M)E + (N-S)C - (Q-T)B + (P-U)A &= 0 \\
AH - BG + CF - DE &= 0
\end{aligned}$$

11. The following designs can be obtained by choosing the variables of PR in the manner indicated:

$(1,1,1,1,1,1,1,1,4)$ $M = S = x_5, \quad N = T = x_6,$
$R = \bar{Q} = x_7, \quad P = U = x_8,$
$A = D = G = \bar{F} = x_9,$ a11 others zero;

$(1,1,1,1,1,1,1,1,8)$ $M = S = x_5, \quad N = T = x_6,$
$R = P = x_7, \quad Q = U = x_8,$
$A = \bar{B} = D = C = G = \bar{H} = \bar{E} = \bar{F} = x_9;$

$(1,1,1,1,1,1,2,2,2)$ $A = x_5, \quad P = U = x_6, \quad R = \bar{D} = \bar{M} = x_7,$
$N = \bar{S} = F = x_8, \; Q = \bar{T} = G = x_9,$ all others zero;

$(1,1,1,1,1,1,4,4)$ $M = S = x_5, \quad R = \bar{Q} = x_6, \; A = G = D = \bar{F} = x_7,$
$B = H = C = \bar{E} = x_8,$ all others zero;

$(1,1,1,1,1,1,5,5)$ $M = S = x_5, \quad N = U = x_6,$
$A = G = P = R = C = \bar{E} = x_7,$
$B = H = D = \bar{F} = \bar{Q} = \bar{T} = x_8,$

$(1,1,1,1,2,2,4,4)$ $D = F = x_5, \quad G = H = x_6,$
$M = R = E = C = \bar{N} = \bar{S} = x_7,$
$Q = T = B = A = \bar{P} = \bar{U} = x_8.$

12. Table F.5 gives orthogonal design of type $(1,1,1,1,2,2,2,2,2)$ in order 16.
13. There are 45 possible 9-tuples that might be the type of orthogonal designs.
14. Table F.6 lists the 30 8-variable designs that do not exist as an orthogonal design in order 16.
15. There are 94 possible 7-tuples. The following 13 do not exist - all others are known:

$(1,1,1,1,1,1,7)$	$(1,1,1,1,1,4,6)$	$(1,1,1,1,2,4,5)$	$(1,1,1,2,2,2,7)$
$(1,1,1,1,1,2,7)$	$(1,1,1,1,1,4,7)$	$(1,1,1,1,3,4,4)$	$(1,1,1,2,2,3,5)$
$(1,1,1,1,1,3,7)$	$(1,1,1,1,2,2,7)$	$(1,1,1,2,2,2,6)$	$(1,1,2,2,2,2,5)$
			$(1,1,2,2,2,3,4)$

16. Of 125 possible 6-tuples, all are the types of orthogonal designs in order 16 except $(1,1,1,1,4,7)$ and $(1,1,2,2,2,7)$ which do not exist.
17. All n-tuples $n = 1,2,3,4,5$ are the types of orthogonal designs in order 16.

Table F.1 9 variable designs in Order 16

$(1,1,1,1,1,1,1,1,1)$	$(1,1,1,1,1,1,1,1,8)$	$(1,1,1,1,2,2,2,2,2)$
$(1,1,1,1,1,1,1,1,2)$	$(1,1,1,1,1,2,2,2,2)$	$(1,1,2,2,2,2,2,2,2)$
$(1,1,1,1,1,1,1,1,4)$	$(1,1,1,1,1,2,3,3,3)$	$(1,1,1,1,1,1,2,2,2)$

Table F.2 Known 8-variable designs in order 16

(1,1,1,1,1,1,1,1)	(1,1,1,1,1,2,2,2)	(1,1,1,2,2,3,3,3)
(1,1,1,1,1,1,1,2)	(1,1,1,1,1,2,2,3)	(1,1,1,1,2,3,3,4)
(1,1,1,1,1,1,1,3)	(1,1,1,1,1,2,2,4)	(1,1,1,1,3,3,3,3)
(1,1,1,1,1,1,1,4)	(1,1,1,1,1,2,3,3)	(1,1,1,2,2,2,2,2)
(1,1,1,1,1,1,1,5)	(1,1,1,1,1,2,3,6)	(1,1,1,2,2,2,2,3)
(1,1,1,1,1,1,1,8)	(1,1,1,1,1,3,3,3)	(1,1,1,2,2,3,3,3)
(1,1,1,1,1,1,1,9)	(1,1,1,1,1,3,3,5)	(1,1,2,2,2,2,2,2)
(1,1,1,1,1,1,2,2)	(1,1,1,1,2,2,2,2)	(1,1,2,2,2,2,2,4)
(1,1,1,1,1,1,2,4)	(1,1,1,1,2,2,2,3)	(1,1,2,2,2,2,3,3)
(1,1,1,1,1,1,2,8)	(1,1,1,1,2,2,2,4)	(1,2,2,2,2,2,2,2)
(1,1,1,1,1,1,3,3)	(1,1,1,1,2,2,3,3)	(1,2,2,2,2,2,2,3)
(1,1,1,1,1,1,4,4)	(1,1,1,1,2,2,4,4)	(2,2,2,2,2,2,2,2)
(1,1,1,1,1,1,5,5)		

Table F.3 9-tuple designs which cannot be the type of an orthogonal design in order 16

(1,1,1,1,1,1,1,1,7)	(1,1,1,1,1,1,2,2,5)	(1,1,1,1,1,2,2,2,5)
(1,1,1,1,1,1,1,2,3)	(1,1,1,1,1,1,2,3,3)	(1,1,1,1,1,2,2,3,3)
(1,1,1,1,1,1,1,2,5)	(1,1,1,1,1,1,2,3,4)	(1,1,1,1,2,2,2,2,3)
(1,1,1,1,1,1,1,2,6)	(1,1,1,1,1,1,3,3,3)	(1,1,1,1,2,2,2,3,3)
(1,1,1,1,1,1,1,3,3)	(1,1,1,1,1,1,3,3,4)	(1,1,1,2,2,2,2,2,2)
(1,1,1,1,1,1,1,3,5)	(1,1,1,1,1,2,2,2,3)	(1,1,1,2,2,2,2,2,3)
(1,1,1,1,1,1,1,4,4)	(1,1,1,1,1,2,2,2,4)	

Table F.4 9-tuple designs excluded by Robinson in order 16

(1,1,1,1,1,1,1,1,3)	(1,1,1,1,1,1,1,3,4)	(1,1,1,1,1,1,2,3,5)
(1,1,1,1,1,1,1,1,5)	(1,1,1,1,1,1,1,3,6)	(1,1,1,1,1,1,2,4,4)
(1,1,1,1,1,1,1,1,6)	(1,1,1,1,1,1,1,4,5)	(1,1,1,1,1,2,2,3,4)
(1,1,1,1,1,1,1,2,2)	(1,1,1,1,1,1,2,2,3)	
(1,1,1,1,1,1,1,2,4)	(1,1,1,1,1,1,2,2,4)	(1,1,1,1,2,2,2,2,4)
(1,1,1,1,1,1,1,2,7)	(1,1,1,1,1,1,2,2,6)	

Table F.5 $OD(16;1,1,1,1,2,2,2,2,2)$

$$
\left[\begin{array}{cccc|cccc|cccccccc}
x_5 & x_5 & x_1 & x_3 & x_2 & x_4 & 0 & 0 & x_6 & x_7 & x_8 & x_9 & x_7 & x_6 & x_9 & x_8 \\
\bar{x}_5 & x_5 & x_3 & \bar{x}_1 & x_4 & \bar{x}_2 & 0 & 0 & x_7 & \bar{x}_6 & \bar{x}_9 & x_8 & \bar{x}_6 & \bar{x}_7 & x_8 & x_9 \\
\bar{x}_1 & \bar{x}_3 & x_5 & x_5 & 0 & 0 & \bar{x}_2 & x_4 & x_9 & x_8 & \bar{x}_6 & x_7 & \bar{x}_8 & x_9 & \bar{x}_7 & \bar{x}_6 \\
\bar{x}_3 & x_1 & \bar{x}_5 & x_5 & 0 & 0 & x_4 & x_2 & \bar{x}_8 & x_9 & x_7 & x_6 & \bar{x}_9 & \bar{x}_8 & \bar{x}_6 & x_7 \\
\hline
\bar{x}_2 & \bar{x}_4 & 0 & 0 & x_5 & x_5 & x_1 & \bar{x}_3 & x_7 & x_6 & x_8 & \bar{x}_9 & \bar{x}_6 & x_7 & x_9 & x_8 \\
\bar{x}_4 & x_2 & 0 & 0 & \bar{x}_5 & x_5 & \bar{x}_3 & \bar{x}_1 & x_6 & \bar{x}_7 & x_9 & x_8 & x_7 & x_6 & \bar{x}_8 & x_9 \\
0 & 0 & x_2 & \bar{x}_4 & \bar{x}_1 & x_3 & x_5 & x_5 & \bar{x}_9 & x_8 & \bar{x}_7 & x_6 & x_8 & x_9 & x_6 & x_7 \\
0 & 0 & \bar{x}_4 & \bar{x}_2 & x_3 & x_1 & \bar{x}_5 & x_5 & \bar{x}_8 & \bar{x}_9 & x_6 & x_7 & \bar{x}_9 & x_8 & x_7 & \bar{x}_6 \\
\hline
\bar{x}_6 & \bar{x}_7 & \bar{x}_8 & \bar{x}_9 & \bar{x}_7 & \bar{x}_6 & \bar{x}_8 & x_9 & x_5 & x_5 & x_1 & 0 & x_2 & \bar{x}_4 & x_3 & 0 \\
\bar{x}_6 & \bar{x}_7 & \bar{x}_8 & \bar{x}_9 & \bar{x}_7 & \bar{x}_6 & \bar{x}_8 & x_9 & \bar{x}_5 & x_5 & 0 & \bar{x}_1 & \bar{x}_4 & \bar{x}_2 & 0 & \bar{x}_3 \\
\bar{x}_9 & \bar{x}_8 & x_6 & \bar{x}_7 & x_9 & \bar{x}_8 & x_7 & \bar{x}_6 & \bar{x}_1 & 0 & x_5 & x_5 & x_3 & 0 & \bar{x}_2 & \bar{x}_4 \\
x_8 & \bar{x}_9 & \bar{x}_7 & \bar{x}_6 & x_8 & x_9 & x_6 & x_7 & 0 & x_1 & \bar{x}_5 & x_5 & 0 & \bar{x}_3 & \bar{x}_4 & x_2 \\
\bar{x}_7 & x_6 & \bar{x}_9 & x_8 & x_6 & \bar{x}_7 & \bar{x}_9 & \bar{x}_8 & \bar{x}_2 & x_4 & \bar{x}_3 & 0 & x_5 & x_5 & x_1 & 0 \\
x_6 & x_7 & \bar{x}_8 & \bar{x}_9 & \bar{x}_7 & \bar{x}_6 & x_8 & \bar{x}_9 & x_4 & x_2 & 0 & x_3 & \bar{x}_5 & x_5 & 0 & \bar{x}_1 \\
x_8 & \bar{x}_9 & x_7 & x_6 & \bar{x}_8 & \bar{x}_9 & \bar{x}_6 & \bar{x}_7 & \bar{x}_3 & 0 & x_2 & \bar{x}_4 & \bar{x}_1 & 0 & x_5 & x_5 \\
x_9 & x_8 & x_6 & x_7 & x_9 & x_8 & x_7 & x_6 & 0 & x_3 & x_4 & \bar{x}_2 & 0 & x_1 & \bar{x}_5 & x_5
\end{array}\right]
$$

Table F.6 8-variable designs that do not exist as an orthogonal design in order 16

$(1,1,1,1,1,1,1,6)$	$(1,1,1,1,1,1,4,5)$	$(1,1,1,1,1,3,4,4)$
$(1,1,1,1,1,1,1,7)$	$(1,1,1,1,1,1,4,6)$	$(1,1,1,1,2,2,2,5)$
$(1,1,1,1,1,1,2,3)$	$(1,1,1,1,1,2,2,5)$	$(1,1,1,1,2,2,2,6)$
$(1,1,1,1,1,1,2,5)$	$(1,1,1,1,1,2,2,6)$	$(1,1,1,1,2,2,3,4)$
$(1,1,1,1,1,1,2,6)$	$(1,1,1,1,1,2,2,7)$	$(1,1,1,1,2,2,3,5)$
$(1,1,1,1,1,1,2,7)$	$(1,1,1,1,1,2,3,4)$	$(1,1,1,2,2,2,2,4)$
$(1,1,1,1,1,1,3,4)$	$(1,1,1,1,1,2,3,5)$	$(1,1,1,2,2,2,3,3)$
$(1,1,1,1,1,1,3,5)$	$(1,1,1,1,1,2,4,4)$	$(1,1,1,2,2,2,2,5)$
$(1,1,1,1,1,1,3,6)$	$(1,1,1,1,1,2,4,5)$	$(1,1,1,2,2,2,3,4)$
$(1,1,1,1,1,1,3,7)$	$(1,1,1,1,1,3,3,4)$	$(1,1,2,2,2,2,2,3)$

F.3 Orthogonal designs in Order 32

We summarize the known results for order 32.

1. There are at most 10 variables for this order.
2. In Tables F.7, F.8, F.10, F.11 and F.12 we give 10, 9, 8 and 7 tuples for which orthogonal designs exist in order 32. The results of Table F.7 are given in Street [202]. These designs were constructed in one of the following two ways:
   (a) using product designs and amicable orthogonal designs in Theorem 6.6, or
   (b) using a doubling construction (Theorem 4.3) with orthogonal designs in order 16.
3. Table F.7 lists 10-tuples which are orthogonal designs of order 32, as are the full 10-tuples designs listed in Table F.8.
4. The following 9-tuples are the types of orthogonal designs:

$$(1,1,1,2,2,4,a,a,a) \qquad a = 1,2,3,4,5,6 \text{ or } 7;$$

   as are the 9-tuples given in Table F.10. Table F.9 gives the construction method for 9 variables.
5. Table F.11 gives the construction of 8 variable designs in order 32.
6. Kharaghani and Tayfeh-Rezaie [122] showed by complete computer search that "there is a full $OD(32;1,1,1,1,1,u_1,\ldots,u_k)$ if and only if $(u_1,\ldots,u_k) = (9,9,9)$, $(9,18)$, $(12,15)$ or (27)."
7. Some full 7-tuples are listed in Table F.12.
8. The 86 types of orthogonal designs given in Table F.13 have not been resolved.
9. All full 6-tuples are the type of an orthogonal design.
10. All possible n-tuples, $n = 1,2,3,4,5$ are the types of orthogonal designs.

Table F.7 10-tuple design in order 32 [a]

(1,1,1,1,1,1,1,3,3,3),	(1,1,1,1,1,2,2,2,4,4),	(1,1,2,2,2,2,2,2,2,4),
(1,1,1,1,1,1,2,2,2,4),	(1,1,1,1,1,2,2,4,4,4),	(1,1,2,2,2,2,2,3,3,3),
(1,1,1,1,1,1,2,2,4,8),	(1,1,1,1,1,2,2,5,5,5),	(1,1,2,2,2,2,2,3,3,6),
(1,1,1,1,1,1,2,3,3,6),	(1,1,1,1,1,2,3,6,6,6),	(1,1,2,2,2,2,2,4,4,4),
(1,1,1,1,1,1,2,4,4,4),	(1,1,1,2,2,2,2,3,3,3),	(1,1,2,2,2,2,4,4,4,4),
(1,1,1,1,1,1,3,3,4,12),	(1,1,1,2,2,2,4,4,4,4),	(1,1,2,2,3,3,3,3,3,3),
(1,1,1,1,1,1,4,4,4,4),	(1,1,1,2,2,2,4,5,5,5),	(1,1,2,3,3,3,3,3,3,3),
(1,1,1,1,1,1,4,5,5,5),	(1,1,1,3,3,3,3,3,3,3),	(1,1,2,3,3,3,3,4,4,4),
(1,1,1,1,1,1,4,6,6,6),	(1,1,1,3,3,3,4,4,4,4),	(2,2,2,2,2,2,2,2,2,2),
	(1,1,2,2,2,2,2,2,2,2),	(2,2,2,2,2,2,2,4,4,4).

[a] D. Street [202, p135] © D. Street

Table F.8 Full 10 variable design in order 32

Type	**Construction**
(1,1,1,1,2,2,3,3,9,9)	(1,1,2,3;1,3,3;1) and ((1,3);(1,1,2)) in (a)
(1,1,1,1,2,2,4,4,8,8)	(1,1,1,1,2;2,4;2,4,4) and ((1,1);(1,1)) in (a)
(1,1,1,2,3,3,3,3,6,9)	(1,1,1,2;1,1,3;3) and ((1,3);(1,1,2)) in (a)
(1,1,2,2,2,2,2,2,2,16)	(1,1,1,1,1,1,1,8) in (b)
(1,1,2,2,2,2,4,6,6,6)	(1,1,1,1,1,2,3,3,3) in (b)
(1,1,2,4,4,4,4,4,4,4)	(1,1,2,2,2,2,2,2,2) in (b)
(1,1,3,3,3,3,3,3,6,6)	(1,1,1,2;1,1,3;3) and ((3,1);(1,1,2)) in (a)
(1,2,2,2,2,2,3,6,6,6)	(1,2,2,2,3;2,2,6;6) and ((1,1);(1,1)) in (a)
(2,2,2,2,2,2,2,2,8,8)	(8,1,1,1,1,1,1,1,1) in (b)
(2,2,2,2,2,2,2,6,6,6)	(2,1,1,1,1,1,3,3,3) in (b)
(2,2,2,2,2,3,3,4,6,6)	(3,1,1,1,1,1,2,3,3) in (b)
(2,2,2,2,4,4,4,4,4,4)	(2,1,1,2,2,2,2,2,2) in (b)

Table F.9 Full 9 variable design in order 32 construction

Type	**Construction**
$(1,1,1,1,2,2,3,7,14)$	$(1,1,2,3;7;1)$ and $((1,1,2);(1,1,2))$ in (a)
$(1,1,1,1,2,2,4,10,10)$	$(1,1,1,1,2;2,4;10)$ and $((1,1));(1,1))$ in (a)
$(1,1,1,1,2,4,7,7,8)$	$(1,1,1,2,4;1,8;7)$ and $((1,1);(1,1))$ in (a)
$(1,1,1,1,4,4,6,6,8)$	$(1,1,1,1;2,2;4)$ and $((1,3);(1,1,2))$ in (a)
$(1,1,1,2,2,3,4,6,12)$	$(1,1,1,2,2;3,4;3,6)$ and $((1,1);(2))$ in (a)
$(1,1,1,2,2,3,6,8,8)$	$(1,1,1,2,3;2,6;8)$ and $((1,l);(2))$ in (a)
$(1,1,1,2,2,4,7,7,7)$	$(1,1,1;1,1,1;1)$ and $((1,7);(2,2,4))$ in (a)
$(1,1,1,3,3,3,5,5,10)$	$(1,1,1;1,1,1;5)$ and $((1,3);(1,1,2))$ in (a)
$(1,1,1,2,3,3,5,6,10)$	$(1,1,1,2;5;3)$ and $((1,1,2);(1,1,2))$ in (a)
$(1,1,2,2,2,4,6,7,7)$	$(1,1,2,3;7;1)$ and $((2,1,1);(1,1,2))$ in (a)
$(1,1,2,3,3,4,4,6,8)$	$(1,1,2,3,4;3,8;2,3)$ and $((1,1);(2))$ in (a)
$(1,1,2,3,3,4,5,5,8)$	$(1,1,2,3,4;3,8;5)$ and $((1,1);(1,1))$ in (a)
$(2,2,2,3,3,4,5,5,6)$	$(1,1,1,2;5;3)$ and $((2,1,1);(1,1,2))$ in (a)
$(2,2,3,3,3,3,4,4,8)$	$(1,1,1,1;2,2;2,2)$ and $((3,1);(1,1,2))$ in (a)
$(2,2,3,3,3,4,5,5,5)$	$(1,1,1;1,1,1;1)$ and $((3,5);(2,2,4))$ in (a)
$(1,1,2,2,2,2,2,10,10)$	$(1,1,1,1,1,1,5,5)$ in (b)
$(2,2,2,2,2,2,5,5,10)$	$(5,1,1,1,1,1,1,5)$ in (b)
$(2,2,3,3,4,4,4,4,6)$	$(3,1,1,2,2,2,2,3)$ in (b)
$(2,2,2,2,2,2,2,9,9)$	$(9,1,1,1,1,1,1,1)$ in (b)
$(2,2,2,2,2,5,5,6,6)$	$(5,1,1,1,1,1,3,3)$ in (b)
$(2,2,2,2,4,4,4,6,6)$	$(4,1,1,1,1,2,3,3)$ in (b)
$(2,3,3,4,4,4,4,4,4)$	$(3,1,2,2,2,2,2;2)$ in (b)
$(1,1,1,1,2,3,3,5,15)$	(Example 5.121)

Table F.10 Known 9 Full Variable Designs in Order 32

1	1	1	1	2	2	3	3	18
1	1	1	1	2	2	3	7	14
1	1	1	1	2	2	3	9	12
1	1	1	1	2	2	4	4	16
1	1	1	1	2	2	4	8	12
1	1	1	1	2	2	4	10	10
1	1	1	1	2	2	6	9	9
1	1	1	1	2	2	8	8	8
1	1	1	1	2	3	3	5	15
1	1	1	1	2	3	3	9	11
1	1	1	1	2	3	5	9	9
1	1	1	1	2	4	4	8	10
1	1	1	1	2	4	6	8	8
1	1	1	1	2	4	7	7	8
1	1	1	1	3	3	4	9	9
1	1	1	1	4	4	4	8	8
1	1	1	1	4	4	6	6	8
1	1	1	2	2	3	3	9	10
1	1	1	2	2	3	4	6	12
1	1	1	2	2	3	4	9	9
1	1	1	2	2	3	6	8	8
1	1	1	2	2	4	4	8	9
1	1	1	2	2	4	5	8	8
1	1	1	2	2	4	7	7	7
1	1	1	2	3	3	3	3	15
1	1	1	2	3	3	3	6	12
1	1	1	2	3	3	3	9	9
1	1	1	2	3	3	5	6	10
1	1	1	2	3	3	6	6	9
1	1	1	2	3	4	4	8	8
1	1	1	3	3	3	3	6	11
1	1	1	3	3	3	3	8	9

1	1	1	3	3	3	5	5	10
1	1	1	3	3	3	5	6	9
1	1	2	2	2	2	2	2	18
1	1	2	2	2	2	2	4	16
1	1	2	2	2	2	2	10	10
1	1	2	2	2	2	4	6	12
1	1	2	2	2	2	6	6	10
1	1	2	2	2	3	3	9	9
1	1	2	2	2	4	4	8	8
1	1	2	2	2	4	6	6	8
1	1	2	2	2	4	6	7	7
1	1	2	2	2	6	6	6	6
1	1	2	2	4	4	6	6	6
1	1	2	3	3	3	3	6	10
1	1	2	3	3	3	3	7	9
1	1	2	3	3	3	4	6	9
1	1	2	3	3	4	4	6	8
1	1	2	3	3	4	5	5	8
1	1	2	4	4	4	4	4	8
1	1	3	3	3	3	3	3	12
1	1	3	3	3	3	3	6	9
1	1	3	3	3	3	6	6	6
1	1	4	4	4	4	4	4	6
1	2	2	2	2	2	2	2	17
1	2	2	2	2	2	2	3	16
1	2	2	2	2	2	2	3	12
1	2	2	2	2	2	2	6	9
1	2	2	2	2	2	3	6	8
1	2	2	2	2	2	4	6	7
1	2	2	2	2	2	5	6	6
1	2	2	2	3	3	3	4	12
1	2	2	2	3	4	6	6	6

1	2	2	3	3	3	3	6	9
1	2	4	4	4	4	4	4	5
1	3	3	3	3	3	3	6	7
1	3	3	3	3	3	4	6	6
1	3	4	4	4	4	4	4	4
2	2	2	2	2	2	2	2	16
2	2	2	2	2	2	2	6	12
2	2	2	2	2	2	2	8	10
2	2	2	2	2	2	2	9	9
2	2	2	2	2	2	4	8	8
2	2	2	2	2	2	5	5	10
2	2	2	2	2	2	6	6	8
2	2	2	2	2	3	3	4	12
2	2	2	2	2	3	3	6	10
2	2	2	2	2	3	4	6	9
2	2	2	2	2	3	6	6	7
2	2	2	2	2	4	6	6	6
2	2	2	2	3	3	4	6	8
2	2	2	2	3	3	6	6	6
2	2	2	2	3	4	5	6	6
2	2	2	2	4	4	4	4	8
2	2	2	2	4	4	4	6	6
2	2	2	3	3	4	4	6	6
2	2	2	3	3	4	5	5	6
2	2	2	4	4	4	4	4	6
2	2	3	3	3	3	4	4	8
2	2	3	3	3	4	5	5	5
2	2	3	3	4	4	4	4	6
2	2	4	4	4	4	4	4	4
2	3	3	3	3	3	3	6	6
2	3	3	4	4	4	4	4	4

[a] D. Street [202, p138-143] ©D. Street

Table F.11 8 variable designs in order 32

Weight	Type	Construction
32	(1,1,1,1,7,7,7,7)	(1,1,7;1,1,7;7) and ((1,1);(1,1)) in (a)
32	(1,1,1,2,6,6,6,9)	Geramita Seberry [80, p. 394]
32	(1,1,1,2,6,7,7,7)	”
32	(1,1,1,3,6,6,6,8)	(1,1,1;3;1) and ((1,1,2,2,2);(8)) in (a)
32	(1,2,3,3,4,4,5,10)	(1,2,3,3;4,5;2,5) and ((1,1);(2)) in (a)
32	(1,2,3,3,4,5,7,7)	(1,2,3,3;4,5;7) and ((1,1);(1,1)) in (a)
32	(2,2,2,4,4,5,5,8)	(5,1,1,1,2,2,4) in (b)
32	(2,2,3,3,3,3,4,12)	[80, p. 394]
32	(2,2,3,4,5,5,5,6)	”
32	(2,2,4,4,4,5,5,6)	(5,1,1,2,2,2,3) in (b)
32	(2,3,3,3,3,6,6,6)	[80, p. 394]
32	(2,3,3,3,5,5,5,6)	”
32	(4,4,4,4,4,4,4,4)	”

Table F.12 Full 7 variable design in order 32

Type	Construction
(1,2,2,2,3,11,11)	(1,2,2;2,3;11) and ((1,1);(1,1)) in (a)
(1,1,1,2,5,11,11)	(1,1,1,2;5;11) and ((1,1);(1,1)) in (a)

Table F.13 Unknown Full 7 Variable Designs in Order 32

1	1	1	1	1	1	26
1	1	1	1	1	2	25
1	1	1	1	1	3	24
1	1	1	1	1	4	23
1	1	1	1	1	5	22
1	1	1	1	1	6	21
1	1	1	1	1	7	20
1	1	1	1	1	8	19
1	1	1	1	1	9	18
1	1	1	1	1	10	17
1	1	1	1	1	11	16
1	1	1	1	1	12	15
1	1	1	1	1	13	14
1	1	1	1	2	13	13
1	1	1	1	3	6	19
1	1	1	1	4	5	19
1	1	1	1	4	11	13
1	1	1	1	5	10	13
1	1	1	2	2	2	23
1	1	1	2	5	5	17
1	1	1	3	4	5	17
1	1	1	4	5	7	13
1	1	1	5	5	5	14
1	1	1	5	5	7	12
1	1	1	5	5	8	11
1	1	1	5	6	7	11
1	1	2	2	2	5	19
1	1	2	5	5	5	13

1	1	3	4	4	4	15
1	1	4	4	4	5	13
1	1	4	4	4	7	11
1	1	4	4	5	5	12
1	1	4	4	6	7	10
1	1	4	5	5	7	9
1	1	5	5	5	5	10
1	1	5	5	5	6	9
1	1	5	5	6	7	7
1	1	5	6	6	6	7
1	2	2	2	3	5	17
1	2	2	2	5	5	15
1	2	2	2	5	9	11
1	2	2	3	3	8	13
1	2	2	3	5	5	14
1	2	2	3	5	8	11
1	2	2	4	4	4	15
1	2	2	4	4	5	14
1	2	2	4	5	5	13
1	2	2	4	5	7	11
1	2	2	5	5	5	12
1	2	2	5	5	6	11
1	2	2	5	5	7	10
1	2	4	4	4	7	10
1	2	4	4	5	7	9
1	2	4	5	5	5	10
1	2	5	5	5	5	9
1	2	5	5	5	7	7
1	2	5	5	6	6	7

1	3	3	3	3	5	14
1	3	3	3	7	7	8
1	3	3	4	4	4	13
1	3	4	4	4	5	11
1	3	4	4	4	7	9
1	3	4	5	6	6	7
1	3	5	5	5	6	7
1	3	5	5	6	6	6
1	4	4	4	5	5	9
1	4	4	4	5	7	7
1	4	4	5	5	6	7
1	4	5	5	5	5	7
1	4	5	5	5	6	6
1	5	5	5	5	5	6
2	2	2	3	7	7	9
2	2	2	4	4	7	11
2	2	2	5	5	5	11
2	2	4	5	5	7	7
2	2	5	5	5	5	8
2	3	3	3	3	5	13
2	3	3	3	7	7	7
2	4	4	5	5	5	7
2	5	5	5	5	5	5
3	3	3	3	4	5	11
3	3	3	3	5	7	8
3	3	4	4	4	5	9
3	3	4	4	4	7	7
3	4	4	4	5	5	7
4	4	4	5	5	5	5

F.4 Orthogonal designs in Order 64

We use the following corollary to Theorem 6.6.

Corollary F.1. *Suppose there are amicable orthogonal designs of types* $AOD(n;(u_1,\ldots,u_p);(v_1,\ldots,v_q))$. *Then there exist orthogonal designs of type*

(i) $(u_1,u_1,u_1,2u_1,w,w,3w,3v_1,\ldots,3v_q)$
(ii) $(u_1,u_1,u_1,2u_1,5u_2,\ldots,5u_p,3v_1,\ldots,3v_q)$
(iii) $(u_1,u_1,u_1,w,w,w,5v_1,5v_2,\ldots,5v_q)$
(iv) $(u_1,u_1,u_1,3u_2,\ldots,3u_p,5v_1,\ldots,5v_q)$
(v) $(u_1,u_1,2u_1,3u_1,7u_2,\ldots,7u_p,v_1,\ldots,v_q)$

in order $8n$ *where* $w=u_2+u_3+\cdots+u_p$.

Proof. For (i) and (ii) use the theorem with the product design of type $POD(8:1,1,1,2;1,1,3;3)$. For (iii) and (iv) use the product design of type $POD(8:1,1,1;1,1,1;5)$ and for (v) use the product design of type $POD(8:1,1,2,3;7;1)$. □

We now summarize the known results for order 64.

1. There are at most 12 variables in this order.
2. All full orthogonal designs on five variables that exist in order 64 constructed using product designs, and amicable orthogonal designs are listed in Table F.14.
3. Every 3-tuple of the form $(a,b,64-a-b)$ is the type of an orthogonal design.
4. All possible n-tuples, $n=1,2$, are the types of orthogonal designs.

Table F.14 Orthogonal designs of order 64

Orthogonal design	Product design	Amicable design
(1,1,1,1,2,2,4,4,8,8,16,16)	(1,1,1,1,2,4;2,8;2,4,8,8)	((1,1);(2))
(1,1,1,2,2,3,4,6,8,12,24)	(1,1,1,2,2,4;3,8;3,6,12)	((1,1);(2))
(1,1,1,2,2,9,9,9,12,18)	(1,1,1,2,2;3,4;9)	((1,3);(1,1,2))
(1,1,1,2,4,7,7,9,14,18)	(1,1,1,2,4;9;7)	((1,1,2);(1,1,2))
(1,1,1,2,5,6,6,10,12,20)	(1,1,1,2;5;3)	((1,1,2,4);(2,2,4))
(1,1,1,2,6,6,7,7,12,21)	(1,1,1,2;1,1,3;3)	((1,7);(2,2,4))
(1,1,2,2,2,3,4,7,14,28)	(1,1,2,3;7;1)	((1,1,2,4);(2,2,4))
(1,1,2,3,4,5,5,10,11,22)	(1,1,2,3,4;11;5)	((1,1,2);(1,1,2))
(1,1,3,6,6,7,7,7,12,14)	(1,1,1,2;1,1,3;3)	((7,1);(2,2,4))
(1,2,3,3,4,5,8,8,10,20)	(1,2,3,3,4;5,8;4,5,10)	((1,1);(2))
(1,3,3,3,4,6,8,8,12,16)	(1,1,1,2,4;1,8;1,2,4)	((3,1);(4))
(2,2,3,3,4,5,6,9,15,15)	(1,1,2,3;1,3,3;1)	((3,5);(2,2,4))
(2,3,3,3,3,4,6,8,16,16)	(1,1,1,1,2;2,4;2,4,4)	((3,1);(4))
(3,3,3,5,5,6,6,6,12,15)	(1,1,1,2;1,1,3;3)	((3,5);(2,2,4))
(3,3,3,5,5,6,8,9,10,12)	(1,1,2,3,4;3,8;5)	((3,1);(1,1,2))
(3,3,5,5,5,6,6,9,10,12)	(1,1,1,2;1,1,3;3)	((5,3);(2,2,4))
(1,1,1,2,3,7,7,21,21)	(1,1,1,2;1,1,3;3)	((7);(1,7))
(1,1,1,2,5,10,10,10,24)	(1,1,1,2;5;3)	((1,1,2,2,2);(8))
(1,1,1,2,6,10,10,15,18)	(1,1,1,2;5;3)	((1,2,2,3);(2,6))
(1,1,1,3,6,10,10,12,20)	(1,1,1;3;5)	((1,1,2,4);(2,2,4))
(1,1,1,7,7,7,10,10,20)	(1,1,1;1,1,1;5)	((1,7);(2,2,4))
(1,1,2,2,3,6,14,14,21)	(1,1,2,3;7;1)	((1,2,2,3);(2,6))
(1,1,2,3,7,8,14,14,14)	(1,1,2,3;7;1)	((1,1,2,2,2);(8))
(1,1,2,4,8,8,8,8,8,8,8)	Kotsireas and Koukouvinos [a]	
(1,1,3,3,7,7,7,14,21)	(1,1,1,2;1,1,3;3)	((7,1);(1,7))
(1,2,2,3,4,4,6,14,28)	(1,1,2,3;7;1)	((2,2,4);(3,1,4))
(1,2,3,3,7,7,12,14,15)	(1,2,3,3;4,5;7)	((1,3);(1,1,2))
(1,3,4,8,8,8,8,8,8,8)	Kotsireas and Koukouvinos [a]	
(2,2,3,3,4,6,7,9,28)	(1,1,2,3;7;1)	((3,1,4);(2,2,4))
(2,2,4,5,5,7,10,14,15)	(1,1,2,3;7;1)	((5,1,2);(2,2,4))
(3,3,6,6,7,9,14,14)	(1,1,2,3;7;1)	((3,1,2,2);(2,6))
(3,3,4,4,8,13,13,13)	(1,1,1;1,1,1;1)	((3,13);(4,4,8))
(3,3,3,5,5,5,10,10,20)	(1,1,1;3;5)	((3,5);(2,2,4))
(3,3,3,5,6,6,6,12,20)	(1,1,1,2;5;3)	((3,1,4);(2,2,4))
(3,3,3,5,6,6,10,10,18)	(1,1,1,2;5;3)	((3,1,2,2);(2,6))
(3,4,4,6,8,9,9,9,12)	(1,1,1;3;1)	((9,1,2,4);(4,4,8))
(4,4,5,5,5,8,11,11,11)	(1,1,1;1,1,1;1)	((5,11);(4,4,8))
(5,5,5,5,6,6,10,10,12)	(1,1,1,2;5;3)	((5,1,2);(2,2,4))
(1,1,1,3,6,6;6,40)	(1,1,1;3;5)	((1,1,2,2,2);(8))
(1,1,1,5,7,7,7,35)	(1,1,1;1,1,1;5)	((1,7);(1,7))
(1,1,1,6,6,9,10,30)	(1,1,1;1,1,1;5)	((1,2,2,3);(2,6))
(2,4,7,7,7,14,21)	(1,1,2,3;7;1)	((7,1);(2,2,4))
(3,3,3,6,6,10,30)	(1,1,1;1,1,1;5)	((3,1,2,2);(2,6))
(3,3,3,3,10,10,12,20)	(1,1,1;1,1,1;5)	((3,1,4);(2,2,4))

[a] See Kotsireas and Koukouvinos [125]

Appendix G
Some Complementary Sequences

The sequences given in Tables G.4—G.7 can be used to form first rows of circulant matrices which can then be used in the Goethals-Seidel Array (Theorem 4.8) if there are four sequences, or, if there are two sequences in the "two-circulant" construction (see Definitions 4.8 and 4.9).

For example: Suppose we wish to form an orthogonal design of type $OD(20;2,12)$. We use the sequences given in Table G.4 as follows:

$$abb\bar{b}0 \quad a\bar{b}\bar{b}b0, \quad bbb00, \quad b\bar{b}b00$$

give the first rows of 5×5 circulant matrices which may be used in the Goethals-Seidel array to obtain the design we want. Complementary sequences have elements, $\{\pm 1\}$, while ternary complementary sequences have elements, $\{0, \pm 1\}$, both have $NPAF = 0$.

Craigen and Koukouvinos [37] say in Table G.3, it is not only for theoretical reasons that weight (the number of non-zero elements) is the principal issue. In combinatorics one uses sequences with zero autocorrelation to construct orthogonal designs having difficult weights. Once a weight is established this way for some length, this length can be increased arbitrarily by the operation we have called shifting. Thus, weight is fundamental, and length is arbitrarily large.

In signal processing, one is likely to ask first what strength of received signal (corresponding to weight) is desired before one considers its duration (corresponding to length); deficiency (the number of zeros) is a measure of inefficiency resulting from one's choice of weight. Minimum deficiency with respect to weight appears more useful in this setting than with respect to length.

For Table G.6 the process is similar but is designed for the "two-circulant" construction.

In Table G.7 the positioning of the zeroes is a bit more delicate and we use 0_t to denote t consecutive zeroes.

Note that "$\bar{b}$" means "$-b$".

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5

Table G.1 Some small weight Golay sequences

Length	# of pairs	Equivalence classes	Primitive pairs
1	4	1	1
2	8	1	0
4	32	1	0
8	192	5	0
10	128	2	2
16	1536	36	0
20	1088	25	1
26	64	1	1
32	15,360	336	0
34	0	0	0
40	9728	220	0
50	0	0	0
52	512[a]	12[a]	0[a]
58	0	0	0
64	184,320[a]	3840[a]	0[a]
68	0	0	0
74	0[a]	0[a]	0[a]
80	102,912[a]	?	0[a]
82	0[a]	0[a]	0[a]

a work done at Simon Frazer University

Table G.2 Some small weight PAF pairs for orders not Golay numbers

Periodic Golay pair	Source	Periodic Golay pair	Source	Periodic Golay pair	Source
34	[44][a]	90	[51][e]	212	[51][e]
50	[46][b], [125][h]	106	”	218	”
58	[49][d]	130	”	234	”
68	[48][c] [75][g]	146	”	250	”
72	[50][f]	170	”	274	”
74	[51][e]	178	”	290	”
82	[223][i]	180	”	292	”
		194	”	298	”

a Đoković [44] *b* Đoković [46] *c* Đoković, et al [48] *d* Đoković and Kotsireas [49] *e* Đoković and Kotsireas [51] *f* Đoković and Kotsireas [50] *g* Georgiou, et al [75] *h* Kotsireas and Koukouvinos [125] *i* Vollrath [223]

Table G.3 Ternary Complementary Sequences of Length $n \leq 14$ [37]

n	k	Primitive Pair	Type (n,w)	σ	Source
1	1	$(1);(0)$	$TCP(1,1)$	1	Trivial
2	2	$(1);(1)$	$TCP(1,2)$	0	Trivial
3	5	$(11-);(101)$	$TCP(3,5)$	1	[37]
4	10	$(1010001);(111--1-)$	$TCP(7,10)$	4	[65]
5	10	$(10110-01);(11000-1-)$	$TCP(8,10)$	6	[37]
6	8	$(1100000-1);(10001010-)$	$TCP(9,8)$	10	Can derive from [94]
7	10	$(100--00-1);(10100011-)$	$TCP(9,10)$	8	[37]
8	10	$(11011-0-1);(10000010-)$	$TCP(9,10)$	8	[37]
9	12	$(10-1-0011);(100---1-)$	$TCP(9,13)$	5	Can derive from [56]
10	10	$(1000-01-001);(1110000001-)$	$TCP(11,10)$	12	[37]
11	13	$(1110-110-1-);(1000-000101)$	$TCP(11,13)$	9	Can derive from [90]
12	10	$(10000-10-001);(11100000001-)$	$TCP(12,10)$	14	[37]
13	16	$(100--0-11-01);(1101100-101-)$	$TCP(12,16)$	8	[37]
14	10	$(1000000000011);(1001-100010--)$	$TCP(13,10)$	16	[37]
15	16	$(10--0-010-101);(1110001-0101-)$	$TCP(13,16)$	10	[37]
16	16	$(100-001-11011);(101000-0-11--)$	$TCP(13,16)$	10	[37]
17	17	$(1-10-00011101);(-0-0110-011-1)$	$TCP(13,17)$	9	[134]
18	10	$(1-00000-000011);(1000100001010-)$	$TCP(14,10)$	18	[37]
19	13	$(100-0-10010011);(110-100001000-)$	$TCP(14,13)$	15	[37]
20	16	$(1-00001-001111);(1010-0-10-010-)$	$TCP(14,16)$	12	[37]
21	17	$(-10100110010-1);(-100--0111001-)$	$TCP(14,17)$	11	[134]
22		$(1-1-010-011011);(100100---1000-)$	$TCP(14,17)$	11	[37]
23		$(1-101000-01011);(100111--01-00-)$	$TCP(14,17)$	11	[37]
24	17	$(1000110---01-1);(1010100011-01-)$	$TCP(14,17)$	11	[37]
25	20	$(1-1--00-0--011);(10100-11-1110-)$	$TCP(14,20)$	8	[37]
26	20	$(10--11101-11-1);(10010---0-001-)$	$TCP(14,20)$	8	[37]

[a] Craigen and Koukouvinos [37, p.360] © Elsevier

Table G.4 Some small weight designs with non-periodic auto-correlation function

$(1,1,1,1)$	$a,\ b,\ c,\ d$
$(1,1,1,4)$	$a,\ b,\ dc\bar{d},\ d0d$
$(1,1,2,2)$	$a,\ b,\ cd,\ c\bar{d}$
$(1,1,2,8)$	$da\bar{d},\ db\bar{d},\ dcd,\ d\bar{c}d$
$(1,1,4,4)$	$ba\bar{b},\ b0b,\ dc\bar{d},\ d0d$
$(1,2,2,4)$	$ba\bar{b},\ b0b,\ cd,\ c\bar{d}$
$(1,2,3,6)$	$abc,\ ab\bar{c},\ b\bar{a}b,\ bd\bar{b}$
$(2,2,2,2)$	$ab,\ a\bar{b},\ cd,\ c\bar{d}$
$(1,1,1,9)$	$da\bar{d},\ db\bar{d},\ d0c0\bar{d},\ d0d0d$
$(1,1,8,8)$	$cda\bar{d}\bar{c},\ \bar{c}db\bar{d}c,\ cd0dc,\ c\bar{d}0\bar{d}c$
$(1,1,9,9)$	$bca\bar{c}\bar{b},\ c\bar{b}db\bar{c},\ ccc\bar{c}c,\ bbb\bar{b}b$
$(1,4,4,4)$	$ba\bar{b},\ b0b,\ ccd\bar{d},\ dd\bar{c}c$
$(2,2,4,4)$	$ab,\ a\bar{b},\ ccd\bar{d},\ dd\bar{c}c$
$(2,3,4,6)$	$ad0\bar{d}a,\ adcd\bar{a},\ bc\bar{d},\ b\bar{c}d$
$(3,3,3,3)$	$abc,\ a\bar{b}0d,\ a0c\bar{d},\ bcd$
$(3,3,6,6)$	$adb\bar{d}a,\ adcd\bar{a},\ c\bar{d}a0\bar{b},\ c\bar{d}\bar{a}0b$
$(4,4,4,4)$	$abcd,\ a\bar{b}c\bar{d},\ ab\bar{c}\bar{d},\ a\bar{b}\bar{c}d$
$(2,12)$	$abb\bar{b},\ a\bar{b}\bar{b}b,\ bbb,\ b\bar{b}b$
$(1,1,4,16)$	$a0a0a0a,\ a0ab\bar{a}0\bar{a},\ ac\bar{a}0\bar{a}ca,\ ac\bar{a}da\bar{c}\bar{a}$
$(1,1,5,5)$	$a,\ b,\ cc\bar{c}d0d, dd\bar{d}\bar{c}0\bar{c}$
$(1,2,4,8)$	$ca\bar{c},\ c0c,\ db\bar{d}d0d,\ db\bar{d}\bar{d}0\bar{d}$
$(1,2,6,12)$	$ab0ba,\ abd\bar{b}\bar{a},\ b\bar{a}bbc\bar{b},\ b\bar{a}b\bar{b}\bar{c}b$
$(1,4,5,5)$	$ba\bar{b},\ b0b, cc\bar{c}d0d,\ dd\bar{d}\bar{c}0\bar{c}$
$(2,2,2,8)$	$ab,\ a\bar{b},\ cd\bar{c}c0c,\ cd\bar{c}\bar{c}0\bar{c}$
$(2,2,4,16)$	$ab\bar{a}aca,\ ab\bar{a}a\bar{c}a,\ ab\bar{a}\bar{a}d\bar{a},\ ab\bar{a}\bar{a}d\bar{a}$
$(2,2,5,5)$	$ab,\ a\bar{b},\ cc\bar{c}d0d,\ dd\bar{d}\bar{c}0\bar{c}$
$(2,2,8,8)$	$ab\bar{a}a0a,\ ab\bar{a}\bar{a}0\bar{a},\ cd\bar{c}c0c,\ cd\bar{c}\bar{c}0\bar{c}$
$(2,2,9,9)$	$db\bar{d}cac,\ db\bar{d}\bar{c}\bar{a}c,\ dc0c\bar{d}c,\ \bar{c}d0dcd$
$(2,2,10,10)$	$cc\bar{c}dad,\ cc\bar{c}d\bar{a}d,\ ddd\bar{c}b\bar{c},\ ddd\bar{c}\bar{b}\bar{c}$
$(2,4,4,8)$	$ab\bar{a}a0a,\ ab\bar{a}\bar{a}0\bar{a},\ cd\bar{d}c,\ \bar{c}ddc$
$(2,4,6,12)$	$ab\bar{c}abc,\ ab\bar{c}\bar{a}\bar{b}\bar{c},\ b\bar{a}bbd\bar{b},\ b\bar{a}b\bar{b}d\bar{b}$
$(2,5,5,8)$	$ad\bar{a}a0a,\ ad\bar{a}\bar{a}0\bar{a},\ cc\bar{c}b0b,\ bb\bar{b}\bar{c}0\bar{c}$
$(2,8,8,8)$	$aab\bar{b}cd\bar{c},\ aab\bar{b}\bar{c}d\bar{c},\ a\bar{a}bbc0c,\ a\bar{a}bb\bar{c}0\bar{c}$
$(4,4,4,16)$	$cd\bar{c}cacb,\ cd\bar{c}c\bar{a}c\bar{b},\ cd\bar{c}\bar{c}a\bar{c}\bar{b},\ cd\bar{c}\bar{c}\bar{a}\bar{c}b$
$(4,4,5,5)$	$aab\bar{b},\ bb\bar{a}a,\ c0cddd\bar{d},\ d0d\bar{c}\bar{c}c$
$(4,4,8,8)$	$aab\bar{b}cd,\ aab\bar{b}\bar{c}\bar{d},\ a\bar{a}bbcd,\ a\bar{a}bb\bar{c}d$
$(4,4,10,10)$	$bcacddd\bar{d},\ bc\bar{a}c\bar{d}\bar{d}d,\ bd\bar{a}d\bar{c}\bar{c}c,\ bd\bar{a}\bar{d}cc\bar{c}$
$(5,5,5,5)$	$aa\bar{a}b0b,\ \bar{b}\bar{b}ba0a,\ \bar{c}\bar{c}cd\bar{0}\bar{d},\ \bar{d}\bar{d}dc0c$
$(6,6,6,6)$	$aab\bar{b}cd,\ \bar{b}\bar{b}a\bar{a}d\bar{c},\ \bar{c}\bar{c}\bar{d}dab,\ \bar{d}\bar{d}c\bar{c}\bar{b}a$
$(7,7,7,7)$	$aa\bar{a}bcbd,\ \bar{b}\bar{b}bada\bar{c},\ \bar{c}\bar{c}cd\bar{a}d\bar{b},\ \bar{d}\bar{d}dc\bar{b}ca$

Table G.5 Some small weight designs with zero non-periodic auto-correlation function. See [80, 128, 132] (more are given in [133]).

$(1,1,17,17)$	$aaa\bar{a}0a\bar{a}\bar{a}bbb\bar{b}\bar{b}\bar{b}\bar{b}b$, $bbb\bar{b}0b\bar{b}\bar{b}\bar{a}\bar{a}\bar{a}a\bar{a}\bar{a}\bar{a}$, $a0c0\bar{a}$, $b0d0\bar{b}$
(21)	$aaaa\bar{a}\bar{a}$, $aa\bar{a}aa\bar{a}$, $aa\bar{a}aa$, $aa0\bar{a}a$
(23)	$a\bar{a}aaaa\bar{a}$, $aa\bar{a}\bar{a}\bar{a}a\bar{a}$, $a\bar{a}\bar{a}0\bar{a}\bar{a}a$, $a0a000a$
$(2,26)$	$abb\bar{b}\bar{b}\bar{b}\bar{b}$, $\bar{a}bb\bar{b}\bar{b}\bar{b}\bar{b}$, $bbb\bar{b}bbb$, $bb\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}$
$(1,24)$	$aa\bar{a}ba\bar{a}\bar{a}$, $aaa0\bar{a}\bar{a}a$, $aa\bar{a}a\bar{a}a$, $aaaa\bar{a}a$
$(1,27)$	$aa\bar{a}ba\bar{a}\bar{a}$, $aa\bar{a}a\bar{a}a\bar{a}$, $aa\bar{a}\bar{a}\bar{a}\bar{a}a$, $aa\bar{a}aaaa$
(29)	$aaa\bar{a}\bar{a}a\bar{a}\bar{a}$, $aaa\bar{a}a\bar{a}\bar{a}a$, $aaa\bar{a}a\bar{a}a$, $aaa0\bar{a}aa$
(30)	$aaa\bar{a}aa\bar{a}\bar{a}$, $aaaa\bar{a}aa$, $aa\bar{a}\bar{a}a\bar{a}a$, $aaaa\bar{a}\bar{a}a$
(31)	$aa\bar{a}aaa\bar{a}a\bar{a}$, $aa\bar{a}a0\bar{a}a\bar{a}a$, $aaaaa\bar{a}\bar{a}$, $aaa\bar{a}\bar{a}aa$
$(1,1,32)$	$aa\bar{a}ab\bar{a}a\bar{a}\bar{a}$, $aaa\bar{a}ca\bar{a}\bar{a}$, $aa\bar{a}a0a\bar{a}aa$, $aaa\bar{a}0\bar{a}aaa$
$(1,33)$	$aaa\bar{a}ba\bar{a}\bar{a}\bar{a}$, $aaa\bar{a}\bar{a}a\bar{a}\bar{a}a$, $aaa\bar{a}a\bar{a}aa$, $aaa\bar{a}a\bar{a}aa$
$(1,34)$	$b\bar{b}bbba\bar{b}\bar{b}\bar{b}\bar{b}$, $bbb000\bar{b}\bar{b}00b$, $bb0b00bb\bar{b}0\bar{b}$, $b\bar{b}bbb\bar{b}\bar{b}bbb\bar{b}$
$(1,35)$	$aa\bar{a}ab\bar{a}a\bar{a}\bar{a}$, $aaa\bar{a}\bar{a}\bar{a}a\bar{a}\bar{a}$, $aa\bar{a}a\bar{a}a\bar{a}aa$, $aaaaa\bar{a}\bar{a}aa$
$(1,36)$	$aa\bar{a}aaaa\bar{a}a\bar{a}$, $aa\bar{a}aa\bar{a}\bar{a}a\bar{a}a$, $aaa\bar{a}ba\bar{a}\bar{a}\bar{a}$, $aaa\bar{a}0\bar{a}aaa$
$(1,37)$	$b\bar{b}bbba\bar{b}\bar{b}\bar{b}\bar{b}$, $bb0\bar{b}bb0bbb0$, $bb0\bar{b}bb\bar{b}\bar{b}\bar{b}0$, $b\bar{b}bb0\bar{b}\bar{b}\bar{b}\bar{b}b$
(39)	$aaa\bar{a}a\bar{a}aa\bar{a}\bar{a}\bar{a}$, $aaa\bar{a}a0aa\bar{a}aa$, $aaa\bar{a}\bar{a}a\bar{a}\bar{a}a$, $aaa\bar{a}a\bar{a}\bar{a}\bar{a}a$
$(1,2,2,36)$	$aaa\bar{a}ad\bar{a}a\bar{a}\bar{a}$, $aaa\bar{a}a0a\bar{a}aaa$, $aab\bar{a}\bar{a}a\bar{a}ca\bar{a}$, $aab\bar{a}\bar{a}\bar{a}a\bar{c}\bar{a}a$
$(1,1,40)$	$a0aaa\bar{a}ba\bar{a}\bar{a}\bar{a}0\bar{a}$, $a0a\bar{a}\bar{a}ac\bar{a}aa\bar{a}0\bar{a}$, $a0aaa\bar{a}0\bar{a}aaa0a$, $a0a\bar{a}\bar{a}a0a\bar{a}\bar{a}a0a$
$(1,42)$	$0a0a\bar{a}\bar{a}ab\bar{a}aa\bar{a}0\bar{a}0$, $a00aaa0a\bar{a}0a\bar{a}00a$, $00aa0aaaa\bar{a}a\bar{a}\bar{a}\bar{a}a$, $\bar{a}0\bar{a}aaa0\bar{a}\bar{a}a0a\bar{a}0a$
$(1,43)$	$aaa\bar{a}ab\bar{a}a\bar{a}\bar{a}\bar{a}$, $aaaa\bar{a}\bar{a}aa\bar{a}a\bar{a}$, $aaaa\bar{a}\bar{a}a\bar{a}a\bar{a}a$, $aaa\bar{a}aa\bar{a}\bar{a}aa$
$(1,44)$	$aa\bar{a}\bar{a}a\bar{a}a\bar{a}\bar{a}\bar{a}\bar{a}a$, $aa\bar{a}\bar{a}a\bar{a}\bar{a}aaaa\bar{a}$, $a\bar{a}aaab\bar{a}\bar{a}\bar{a}a\bar{a}$, $a\bar{a}aaa0aaa\bar{a}a$
(47)	$aaa\bar{a}aa\bar{a}aaa\bar{a}\bar{a}\bar{a}$, $aaa\bar{a}aa\bar{a}0\bar{a}a\bar{a}\bar{a}aa$, $aaa\bar{a}aaaa\bar{a}\bar{a}a$, $aaa\bar{a}a\bar{a}\bar{a}aa\bar{a}aa$
$(1,48)$	$aaa\bar{a}\bar{a}a\bar{a}ba\bar{a}aa\bar{a}\bar{a}\bar{a}$, $a0a\bar{a}aa\bar{a}00a0\bar{a}aaa0$, $a\bar{a}aa0a00aaaa\bar{a}0\bar{a}0$, $aa\bar{a}\bar{a}\bar{a}aa\bar{a}0aa\bar{a}aaaa$
(48)	$aaa\bar{a}aa\bar{a}aaa\bar{a}\bar{a}\bar{a}$, $aaaa\bar{a}a\bar{a}\bar{a}aa\bar{a}\bar{a}$, $aaa\bar{a}\bar{a}a\bar{a}a\bar{a}\bar{a}aa$, $aaaa\bar{a}aa\bar{a}aaaa$
(50)	$aaaa\bar{a}a\bar{a}\bar{a}aa\bar{a}\bar{a}\bar{a}$, $aaaa\bar{a}aa\bar{a}\bar{a}aa\bar{a}\bar{a}\bar{a}$, $aaa\bar{a}\bar{a}a\bar{a}a\bar{a}\bar{a}aa$, $aaaaa\bar{a}aa\bar{a}aa$
$(1,51)$	$aaa\bar{a}a\bar{a}ba\bar{a}a\bar{a}\bar{a}\bar{a}$, $aaa\bar{a}aa\bar{a}\bar{a}a\bar{a}a\bar{a}\bar{a}$, $aaa\bar{a}a\bar{a}aaa\bar{a}\bar{a}aa$, $aaaaa\bar{a}\bar{a}a\bar{a}\bar{a}aa$
$(1,2,66)$	$aaa\bar{a}ba\bar{a}\bar{a}\bar{a}aaa\bar{a}\bar{a}a\bar{a}\bar{a}a$, $aaa\bar{a}ba\bar{a}\bar{a}\bar{a}\bar{a}\bar{a}\bar{a}aaa\bar{a}aa\bar{a}$, $aaa\bar{a}a\bar{a}aa0aa\bar{a}a\bar{a}aaa$, $aaa\bar{a}a\bar{a}aac\bar{a}\bar{a}a\bar{a}a\bar{a}\bar{a}\bar{a}$

Table G.6 Some small weight sequences with zero non-periodic auto-correlation function

1	$(1,1)$	$a,\ b$
2	$(2,2)$	$ab,\ a\bar{b}$
3	$(1,4)$	$ba\bar{b},\ b0b$
4	$(4,4)$	$aab\bar{b},\ bb\bar{a}a$
6	$(2,8)$	$ab\bar{a}a0a,\ ab\bar{a}\bar{a}0\bar{a}$
6	$(5,5)$	$aa\bar{a}b0b,\ bb\bar{b}\bar{a}0\bar{a}$
8	$(8,8)$	$aaa\bar{a}bb\bar{b}b,\ \bar{b}\bar{b}\bar{b}baa\bar{a}a$
10	$(4,16)$	$ab\bar{a}a\bar{a}a\bar{a}\bar{a}ba,\ ab\bar{a}aaaaa\bar{b}\bar{a}$
10	$(10,10)$	$a\bar{a}\bar{a}ababb\bar{b}\bar{b},\ b\bar{b}\bar{b}b\bar{a}b\bar{a}\bar{a}\bar{a}a$
11	(13)	$aaa0\bar{a}aa0\bar{a}a\bar{a},\ a0a000\bar{a}000a$
14	$(13,13)$	$aaab\bar{a}aa\bar{b}\bar{a}a\bar{a}b0b,\ bbb\bar{a}\bar{b}bba\bar{b}b\bar{b}\bar{a}0\bar{a}$

Table G.7 Some sequences with zero periodic auto-correlation function

$n \geq 5$	$(1,14)$	$a0_{\frac{1}{2}(n-5)}b\bar{b}\bar{b}\bar{b}0_{\frac{1}{2}(n-5)}$, $b\bar{b}\bar{b}b0_{n-4}$, $\bar{b}bb0_{n-3}$, $b\bar{b}b0_{n-3}$
$n \geq 7$	$(1,1,1,16)$	$a0_{\frac{1}{2}(n-7)}b\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}0_{\frac{1}{2}(n-7)}$, $c0_{\frac{1}{2}(n-5)}b00\bar{b}0_{\frac{1}{2}(n-5)}$, $d0_{\frac{1}{2}(n-5)}b00\bar{b}0_{\frac{1}{2}(n-5)}$, $b\bar{b}\bar{b}bbb0_{n-7}$
	$(1,1,13,13)$	$b0_{\frac{1}{2}(n-7)}c\bar{c}\bar{c}c\bar{c}\bar{c}0_{\frac{1}{2}(n-7)}$, $ccd\bar{c}dcd0_{n-7}$, $dd\bar{c}d\bar{c}dc\bar{c}0_{n-7}$, $a0_{\frac{1}{2}(n-7)}dd\bar{d}d\bar{d}\bar{d}0_{\frac{1}{2}(n-57)}$
	$(1,1,26)$	$a0_{\frac{1}{2}(n-7)}b\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}0_{\frac{1}{2}(n-7)}$, $c0_{\frac{1}{2}(n-7)}b\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}0_{\frac{1}{2}(n-7)}$, $bbb\bar{b}\bar{b}bbb0_{n-7}$, $b\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}0_{n-7}$
	$(1,22)$	$a0_{\frac{1}{2}(n-7)}b\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}0_{\frac{1}{2}(n-7)}$, $b\bar{b}\bar{b}\bar{b}\bar{b}b0_{n-6}$, $b\bar{b}\bar{b}bb0_{n-5}$, $b\bar{b}\bar{b}bb0_{n-5}$
$n \geq 9$	$(1,25)$	$a0_{\frac{1}{2}(n-7)}b0b\bar{b}0\bar{b}0_{\frac{1}{2}(n-7)}$, $b0bb0bbb\bar{b}0_{n-9}$, $b0b\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}b0_{n-9}$, $b\bar{b}\bar{b}\bar{b}\bar{b}b0_{n-6}$
	$(1,30)$	$a0_{\frac{1}{2}(n-9)}b\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}0_{\frac{1}{2}(n-9)}$, $bbbb\bar{b}\bar{b}\bar{b}\bar{b}b0_{n-8}$, $bbb\bar{b}bbbb0_{n-7}$, $b\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}0_{n-7}$
$n \geq 11$	$(1,4,13)$	$ab\bar{a}0_{n-3}$, $a0a0_{n-3}$, $ccc0\bar{c}cc0\bar{c}c\bar{c}0_{n-11}$, $c0c000\bar{c}000c0_{n-11}$
	$(1,1,40)$	$a0_{\frac{1}{2}(n-11)}\bar{b}bbbb\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}0_{\frac{1}{2}(n-11)}$, $c0_{\frac{1}{2}(n-11)}b\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}0_{\frac{1}{2}(n-11)}$, $b\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}b0_{n-10}$, $\bar{b}bbbbbbbbb\bar{b}0_{n-10}$
$n \geq 13$	$(1,1,25)$	$a0_{\frac{1}{2}(n-13)}bbbb\bar{b}0b\bar{b}\bar{b}\bar{b}\bar{b}0_{\frac{1}{2}(n-13)}$, $c0_{\frac{1}{2}(n-5)}b00\bar{b}0_{\frac{1}{2}(n-5)}$, $b00000b00b0_{n-10}$, $bbb0\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}0bb0_{n-12}$
	$(1,1,50)$	$a0_{\frac{1}{2}(n-13)}bbb\bar{b}bb\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}0_{\frac{1}{2}(n-13)}$, $c0_{\frac{1}{2}(n-13)}bbb\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}0_{\frac{1}{2}(n-13)}$, $bbbb\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}b0_{n-13}$,
$n \geq 15$	$(1,4,26)$	$ab\bar{a}0_{n-3}$, $a0a_{n-3}$, $ccc\bar{c}\bar{c}ccc\bar{c}c\bar{c}\bar{c}0\bar{c}0_{n-14}$, $ccccc\bar{c}ccc\bar{c}\bar{c}c\bar{c}c0c0_{n-14}$
	$(1,1,29)$	$a0_{\frac{1}{2}(n-15)}b000\bar{b}0000b000\bar{b}0_{\frac{1}{2}(n-15)}$, $c0_{\frac{1}{2}(n-13)}bbb0\bar{b}bb\bar{b}0\bar{b}\bar{b}\bar{b}0_{\frac{1}{2}(n-13)}$, $bb00bb\bar{b}0\bar{b}bb00bo_{n-14}$, $b\bar{b}000\bar{b}000\bar{b}b0\bar{b}0_{n-13}$
	$(1,1,58)$	$a0_{\frac{1}{2}(n-15)}bbbb\bar{b}\bar{b}bb\bar{b}bb\bar{b}\bar{b}\bar{b}\bar{b}0_{\frac{1}{2}(n-15)}$, $c0_{\frac{1}{2}(n-15)}b\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}0_{\frac{1}{2}(n-15)}$, $b\bar{b}bbb\bar{b}\bar{b}\bar{b}\bar{b}bbb\bar{b}\bar{b}\bar{b}0_{n-15}$, $bbb\bar{b}bbb\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}0_{n-15}$
	$(1,52)$	$a0_{\frac{1}{2}(n-13)}bb\bar{b}\bar{b}\bar{b}\bar{b}bb\bar{b}\bar{b}\bar{b}0_{\frac{1}{2}(n-13)}$, $bb\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}bbb0_{n-12}$, $bbb\bar{b}bbbbb\bar{b}\bar{b}\bar{b}\bar{b}\bar{b}o_{n-14}$, $bbb\bar{b}bbb\bar{b}\bar{b}bbb\bar{b}\bar{b}0_{n-14}$

Table G.8 4-complementary sequences A, B, C, D such that $\frac{1}{2}(A+B)$, $\frac{1}{2}(A-B)$, $\frac{1}{2}(C+D)$, $\frac{1}{2}(C-D)$ are also 4-complementary sequences

$\mathbf{L}^a$	$\mathbf{W}^b$	A, B, C, D
3	10	$11-,\ 11-,\ 101,\ 101$
3	12	$111,\ 1-1,\ 11-,\ 11-$
4	14	$111-,\ 1--1,\ 111,\ 1-1$
5	18	$11-11,\ 11-1-,\ 111-,\ 111-$
5	20	$1-11-,\ 111--,\ 111-1,\ 111-1$
6	10	$101--1,\ 10111-$
6	12	$101--1,\ 10111-,\ 1,1$
6	14	$101--1,\ 10111-,\ 11,1-$
6	16	$11-1--,\ 11-111,\ 100-,\ 100-$
6	18	$11-1--,\ 11-111,\ 110-,\ 1-0-$
6	20	$111-1-,\ 1-1111,\ 1--1,\ 11--$
6	22	$11--1-,\ 1----1,\ 1-111,\ 1-111$
6	24	$11-1--,\ 11--11,\ 111-1-,\ 1-1111$
7	26	$111-111,\ 11---1-,\ 11-1--,\ 11-1--$
7	28	$1--1111,\ 1--1-1-,\ 11-111-,\ 1----1$
9	28	$1---0-11-,\ 1--101--1,\ 10110111,\ 101-0---$
9	30	$11-10111-,\ 11--0---1,\ 101101--1,\ 101-0-11-$
9	34	$111-01---,\ 111--1--1,\ 111-1-11,\ 111-1-11$
14	26	$111--111-1--0-,\ 1111-11--1-10$

a Length b Weight

Table G.9 2-complementary disjointable sequences

Length	**Type**	
1	(1,1)	$a,\ b$
2	(2,2)	$ab,\ a\bar{b}$
4	(4,4)	$aab\bar{b},\ a\bar{a}bb$
6	(2,8)	$ab\bar{a}a0a,\ ab\bar{a}\bar{a}0\bar{a}$
8	(8,8)	$aaa\bar{a}bb\bar{b}b,\ a\bar{a}aab\bar{b}\bar{b}\bar{b}$
10	(4,16)	$ab\bar{a}a\bar{a}a\bar{a}\bar{a}ba,\ ab\bar{a}aaaaa\bar{b}\bar{a}$
10	(10,10)	$a\bar{a}\bar{a}abab\bar{b}\bar{b}\bar{b},\ a\bar{a}\bar{a}\bar{a}b\bar{a}\bar{b}\bar{b}\bar{b}b$
14	(26)	$aaaa\bar{a}aa\bar{a}\bar{a}\bar{a}\bar{a}a0a,\ aaa\bar{a}\bar{a}aaa\bar{a}a\bar{a}\bar{a}0a$

Appendix H
Product Designs

Table H.1 Product designs of order 16

Product designs	Construction	
$(1,1,2,3;1,1,2,3;9)$	$((1,1,2);(1,3))$	$((1,1,2);(1,3))$
$(1,1;2,9;1,3,3,6;3)$	$((1,1,2);(3,1))$	$((1,1,2);(1,3))$
$(1,1,7;1,1,7;7)$	$((1,7);(1,7))$	$((1,1);(1,1))$
$(1,2,2,2,3;2,2,6;6)$	$((1,2,2,3);(2,6))$	$((1,1);(1,1))$
$(2,2,2,4;1,1,2,6;6)$	$((1,1,2);(1,3))$	$((1,1,2);(2,2))$
$(2,2,4,5;3,5,5;3)$	$((2,2,4);(5,3))$	$((1,1);(1,1))$
$(2,2,4,6;2,3,3,6;2)$	$((1,1,2);(3,1))$	$((1,1,2);(2,2))$
$(2,2,4,7;1,7,7;1)$	$((2,2,4);(7,1))$	$((1,1);(1,1))$
$(2,6,6;1,1,2,4,6;2)$	$((1,1);(1,1))$	$((1,1,2,4);(2,6))$
$(4,4,4;1,1,2,4,4;4)$	$((1,1);(1,1))$	$((1,1,2,4);(4,4))$
$(1,1,1,1,2;2,4;2,4,4)$	$(1,1,1,1;2,2;2,2)$	
$(1,1,1,2,2;3,4;3,6)$	$(1,1,1,2;2,3;3)$	
$(1,1,1,2,3;2,6;2,6)$	$(1,1,2,3;1,6;1)$	
$(1,1,1,2,4;1,8;1,2,4)$	$(1,1,1,2;4,1;1,2)$	
$(1,1,1,2;5;3,3,5)$	$(1,1,1,2;5;3)$	
$(1,1,2,3,4;3,8;2,3)$	$(1,1,2,3;4,3;1)$	
$(1,1,2,3,6;1,12;1,2)$	$(1,1,2,3;6,1;1)$	
$(1,2,2;2,3;3,4,4)$	$(2,2;1,3;2,2)$	
$(1,2,3,3;4,5;2,5)$	$(1,3,3;2,5;1)$	
$(2,2,2,5;1,10;1,4)$	$(2,2,2;5,1;2)$	

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5

Table H.2 Product designs of order 32

Product designs	**Construction**	
$(13,3,13;4,4,8,13;3)$	$((1,1);(1,1))$	$((4,4,8);(3,13))$
$(3,5,5,10;2,2,2,4,15;9)$	$((1,1,2);(1,3))$	$((2,2,4);(5,3))$
$(4,4,8,12;3,3,4,6,12;4)$	$((1,1,2);(3,1))$	$((1,1,2,4);(4,4))$
$(7,7,9;4,4,7,8;9)$	$((1,1);(1,1))$	$((4,4,8);(7,9))$
$(1,1,1,1,2,4;2,8;2,4,8,8)$	$(1,1,1,1,2;4,2;2,4,4)$	
$(1,1,1,2,2,4;3,8:3,6,12)$	$(1,1,1,2,2;4,3;3,6)$	
$(1,1,1,2,4,8;1,16;1,2,4,8)$	$(1,1,1,2,4;8,1;1,2,4)$	
$(1,1,2,2,3;4,5;5,18)$	$(1,1,2,3;2,5;9)$	
$(1,1,2,3,4,11;22;4,6)$	$(1,1,2,3,4;11;2,3)$	
$(1,1,2,3,4,8;3,16;3,4,6)$	$(1,1,2,3,4;8,3;2,3)$	
$(1,1,2,3,6,12;1,24;1,2,4)$	$(1,1,2,3,6;12,1;1,2)$	
$(1,1,2,6,9;7,12;6,7)$	$(1,1,2,9;6,7;3)$	
$(1,1,2,3,9;6,10;6,10)$	$(1,1,2,9;3,10;3)$	
$(1,1,2,9,10;3,20;3,6)$	$(1,1,2,9;10,3;3)$	
$(1,2,3,3,4;5,8;4,5,10)$	$(1,2,3,3;4,5;2,5)$	
$(1,2,3,3,6;4,11;6,11)$	$(1,3,3,6;2,11;3)$	
$(1,3,3,6,10;3,20;3,6)$	$(1,3,3,6;10,3;3)$	
$(1,3,3,6,11;2,22;2,6)$	$(1,3,3,6;11,2;3)$	
$(1,3,3,6,9;4,18;4,6)$	$(1,3,3,6;9,4;3)$	
$(1,4,7,7;8,11;2,11)$	$(1,7,7;4,11;1)$	
$(1,6,7,7;9,12;2,9)$	$(1,7,7;6,9;1)$	
$(2,2,2,4,9;1,18;1,12)$	$(2,2,2,4;9,1;6)$	
$(2,2,2,5,10;1,20;1,2,8)$	$(2,2,2,5;10,1;1,4)$	
$(2,2,4,5,10;3,20;3,6)$	$(2,2,4,5;10,3;3)$	
$(2,2,4,5,8;5,16;5,6)$	$(2,2,4,5;8,5;3)$	
$(2,2,4,6,11;3,22;3,4)$	$(2,2,4,6;11,3;2)$	
$(2,2,4,6,9;5,18;4,5)$	$(2,2,4,6;9,5;2)$	
$(2,2,4,7,8;7,16;2,7)$	$(2,2,4,7;8,7;1)$	
$(2,6,6,13;1,26;1,4)$	$(2,6,6;13,1;2)$	
$(4,4,4,7;5,14;5,8)$	$(4,4,4;7,5;4)$	

Table H.3 Product designs of order 64

Product designs	**Construction**
$(1,1,1,1,2,2,4;4,8;4,8,8,16,16)$	$(1,1,1,1,2,4;2,8;2,4,8,8)$
$(1,1,1,2,2,3,4;6,8:6,8,12,24)$	$(1,1,1,2,2,4;3,8;3,6,12)$
$(1,1,1,2,4,8,16;1,32;1,2,4,8,16)$	$(1,1,1,2,4,8;16,1;1,2,4,8)$
$(1,1,2,2,3,4;5,8;5,10,36)$	$(1,1,2,2,3;4,5;5,18)$
$(1,1,2,3,4,8,16;3,32;3,6,8,12)$	$(1,1,2,3,4,8;16,3;3,4,6)$
$(1,1,2,3,6,9;10,12;10,12,20)$	$(1,1,2,3,9;6,10;6,10)$
$(1,1,2,6,7,9;12,14;12,12,14)$	$(1,1,2,6,9;7,12;6,7)$
$(1,2,3,3,4,5;8,10;8,8,10,20)$	$(1,2,3,3,4;5,8;4,5,10)$
$(1,2,3,3,6,11;4,22;4,12,22)$	$(1,2,3,3,6;11,4;6,11)$
$(1,3,3,6,9,18;4,36;4,8,12)$	$(1,3,3,6,9;18,4;4,6)$
$(1,4,7,7,8;11,16;4,11,22)$	$(1,4,7,7;8,11;2,11)$
$(1,6,7,7,12;9,24;4,9,18)$	$(1,6,7,7;12,9;2,9)$
$(2,2,2,5,10,20;1,40;1,2,4,16)$	$(2,2,2,5,10;20,1;1,2,8)$
$(2,2,4,6,9,18;5,36;5,8,10)$	$(2,2,4,6,9;18,5;4,5)$
$(2,2,4,7,8,16;7,32;7,18)$	$(2,2,4,7,8;16,7;9)$
$(2,3,5,5,10;4,21;18,21)$	$(3,5,5,10;2,21;9)$
$(2,6,6,13,26;1,52:1,2,8)$	$(2,6,6,13;26,1;1,4)$
$(3,4,13,13;8,25;6,25)$	$(3,13,13;4,25;3)$
$(4,4,4,7,14;5,28;5,10,16)$	$(4,4,4,7;14,5;5,8)$
$(4,4,7,8,12;14,21;8,21)$	$(4,4,8,12;7,21;4)$
$(7,7,9,12;11,24;11,18)$	$(7,7,9;12,11;9)$

References

1. Adams, S.S.: A journey of discovery: Orthogonal matrices and wireless communications. Communicating Mathematics **479**, 1–10 (2009)
2. Adams, S.S., Seberry, J., Karst, N., Pollack, J., Wysocki, T.A.: Quaternion orthogonal designs from complex companion designs. Linear Algebra and its Applications **428**(4), 1056–1071 (2008)
3. Alamouti, S.: A simple transmit diversity technique for wireless communications. IEEE J. Select. Areas Commun. **16**(8), 1451–1458 (1998)
4. Albert, A.: Structure of Algebras, *American Mathematical Society colloquium publications*, vol. 24. American Mathematical Society, Rhode Island, USA (1939)
5. Andres, T.H.: Some combinatorial properties of complementary sequences. M.Sc. Thesis, University of Manitoba, Winnipeg (1977)
6. Ang, M.H.: Group weighing matrices. Ph.D. Thesis, National University of Singapore, Singapore (2003)
7. Ang, M.H., Arasu, K., Ma, S.L., Strassler, Y.: Study of proper circulant weighing matrices with weight 9. Discrete Mathematics **308**(13), 2802 – 2809 (2008). Combinatorial Designs: A tribute to Jennifer Seberry on her 60th Birthday
8. Ang, R., Seberry, J., Wysocki, B., Wysocki, T.: Application of nega-cyclic matrices to generate spreading sequences. In: Proceedings of the Seventh International Symposium on Communications Theory and Applications (ISCTA2003). ISCTA2003, HW Communications Limited, Ambleside, UK (2003)
9. Arasu, K.T., Ma, S.L.: Some new results on circulant weighing matrices. Journal of Algebraic Combinatorics **14**(2), 91–101 (2001)
10. Arasu, K.T., Seberry, J.: Circulant weighing designs. Journal of Combinatorial Designs **4**(6), 439–447 (1996)
11. Arasu, K.T., Seberry, J.: On circulant weighing matrices. Australasian J. Combin. **17**, 21–37 (1998)
12. Artin, E.: Geometric Algebra, *Interscience Tracts in Pure and Applied Mathematics*, vol. 3. Wiley, New York-London (1974)
13. Awyzio, G.: Negacyclic matrices of orders 7,9, and 11. Private communication (2016)
14. Baumert, L., Hall Jr, M.: A new construction for Hadamard matrices. Bull. Amer. Math. Soc. **71**, 169–170 (1965)
15. Baumert, L.D.: Hadamard matrices of orders 116 and 232. Bull. Amer. Math. Soc. **72**, 237 (1966)
16. Baumert, L.D.: Cyclic Difference Sets, *Lecture Notes in Mathematics*, vol. 182. Springer-Verlag, Berlin-Heidelberg-New York (1971)
17. Baumert, L.D., Golomb, S.W., Hall Jr, M.: Discovery of an Hadamard matrix of order 92. Bull. Amer. Math. Soc. **68**, 237–238 (1962)

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5

18. Baumert, L.D., Hall, Jr., M.: Hadamard matrices of the Williamson type. Math. of Comp. **19**, 442–447 (1965)
19. Belevitch, V.: Theory of $2n$-terminal networks with applications to conference telephony. Electr. Commun. **27**(3), 231–244 (1950)
20. Belevitch, V.: Conference networks and Hadamard matrices. Ann. Soc. Scientifique Brux. **T82**, 13–32 (1968)
21. Berman, G.: Families of skew-circulant weighing matrices. Ars Combinatoria **4**, 293–307 (1977)
22. Berman, G.: Weighing matrices and group divisible designs determined by $EG(t, p^r)$, $p > 2$. Utilitas Math. **12**, 183–191 (1977)
23. Blake, I.: On a generalization of the Pless symmetry codes. Information and control **27**, 369–373 (1975)
24. Blatt, D., Szekeres, G.: A skew Hadamard matrix of order 52. Canad. J. Math. **21**, 1319–1322 (1969)
25. Borwein, P.B., Ferguson, R.A.: A complete description of Golay pairs for lengths up to 100. Math. Comp. **73**(246), 967–985 (electronic) (2004)
26. Bose, R.C.: On the construction of balanced incomplete block designs. Ann. of Eugenice **9**, 353–399 (1939)
27. Bourbaki, N.: Algebra (Algèbre) OR Commutative algebra (Algèbre commutative), *Elements of Mathematics (Éléments de mathématique)*, vol. VII, english edn. École normale supérieure, Paris (1989). Nicolas Bourbaki is the collective pseudonym under which a group of (mainly French) 20th-century mathematicians wrote a series of books presenting an exposition of modern advanced mathematics, beginning in 1935.
28. Calderbank, R., Das, S., Al-dhahir, N., Diggavi, S.: Construction and analysis of a new quaternionic space-time code for 4 transmit antennas. In: Commun. Inf. Syst., vol. 5, pp. 97–1225 (2005)
29. Clifford, W.: Applications of Grassman's extensive algebra. Amer. J. Math. **1**, 350–358 (1878)
30. Cooper, J.: Some investigations of combinatorial integer matrices using cyclotomy. Ph.D. Thesis, University of Newcastle, Australia (1974)
31. Cooper, J., Milas, J., Wallis, W.: Equivalence of Hadamard matrices. In: Combinatorial Mathematics Proceedings of International Conference on Combinatorial Theory, Canberra 1977, *Lecture Notes in Mathematics*, vol. 686, pp. 126–135. Springer-Verlag (1978)
32. Cooper, J., Wallis, J.S.: A construction for Hadamard arrays. Bull. Austral. Math. Soc. **7**, 269–278 (1972)
33. Cooper, J., Wallis, J.S.: A note on orthogonal designs in order eighty. Ars. Combinatoria **1**, 267–274 (1976)
34. Craigen, R.: Signed groups, sequences and the asymptotic existence of Hadamard matrices. J. Combin. Theory **71**, 241–254 (1995)
35. Craigen, R., Holzmann, W., Kharaghani, H.: Complex Golay sequences: structure and applications. Discrete Mathematics **252**(1), 73 – 89 (2002)
36. Craigen, R., Holzmann, W.H., Kharaghani, H.: On the asymptotic existence of complex Hadamard matrices. J. Combin. Designs **5**, 319–327 (1996)
37. Craigen, R., Koukouvinos, C.: A theory of ternary complementary pairs. J. Combin. Theory, Series A **96**(2), 358 – 375 (2001)
38. Curtis Charles, W.: Linear Algebra - an Introductory Approach, 3rd edn. Allyn and Bacon, Boston (1974)
39. Delsarte, P., Goethals, J.M., Seidel, J.J.: Orthogonal matrices with zero diagonal II. Canad. J. Math. **23**, 816–832 (1971)
40. Dembowski, P.: Finite Geometries. Springer-Verlag (1968)
41. Đoković, D.Ž.: Skew-Hadamard matrices of order 4×37 and 4×43. J. Combin. Theory **61**, 319–321 (1992)

42. Đoković, D.Ž.: Good matrices of order 33, 35 and 127 exist. J. Combin. Math. Combin. Comput **14**, 145–152 (1993)
43. Đoković, D.Ž.: Equivalence classes and representatives of Golay sequences. Discrete Math. **189**(1-3), 79–93 (1998)
44. Đoković, D.Ž.: Note on periodic complementary sets of binary sequences. Designs, Codes, and Cryptography **13**(3), 251–256 (1998)
45. Đoković, D.Ž.: Skew-Hadamard matrices of orders 188 and 388 exist. International Mathematical Forum **3**(22), 1063–1068 (2008)
46. Đoković, D.Ž.: Cyclic $(v; r, s; \lambda)$ difference families with two base blocks and $v \leq 50$. Ann. Comb. **15**(2), 233–254 (2011)
47. Đoković, D.Ž.: Regarding good matrices of order 41. Email communication to author, 23rd July 2014 (2014)
48. Đoković, D.Ž., Kotsireas, I., Recoskie, D., Sawada, J.: Charm bracelets and their application to the construction of periodic Golay pairs. ArXiv e-prints (2014)
49. Đoković, D.Ž., Kotsireas, I.S.: Compression of periodic complementary sequences and applications. Designs, Codes, and Cryptography **74**(2), 365–377 (2013)
50. Đoković, D.Ž., Kotsireas, I.S.: Periodic Golay Pairs of length 72, *Algebraic Design Theory and Hadamard Matrices: ADTHM, Lethbridge, Alberta, Canada, July 2014*, vol. 133, pp. 83–92 (2015)
51. Đoković, D.Ž., Kotsireas, I.S.: Some new periodic Golay pairs. Numerical Algorithms **69**(3), 523–530 (2015)
52. Eades, P.: On the existence of orthogonal designs. Ph.D. Thesis, Australian National University, Canberra, Australia (1977)
53. Eades, P.: Integral quadratic forms and orthogonal designs. Journal of the Australian Mathematical Society **30**(3), 297–306 (1981)
54. Eades, P., Hain, R.M.: On circulant weighing matrices. Ars. Combinatoria **2**, 265–284 (1976)
55. Edmondson, G.M., Seberry, J., Anderson, M.R.: On the existence of Turyn sequences of length less than 43. Math. Computation **62**, 351–362 (1994)
56. Eliahou, S., Kervaire, M., Saffari, B.: A new restriction on the lengths of Golay complementary sequences. J. Combin. Theory **55**, 49–59 (1990)
57. Eliahou, S., Kervaire, M., Saffari, B.: On Golay polynomial pairs. Adv in Appl. Math. **12**, 235–292 (1991)
58. Erdös, P., Odlyzko, A.: On the density of odd integers of the form $(p-1)2^{-n}$ and related questions pp. 257–263
59. Evangelaras, H., Georgiou, S., Koukouvinos, C.: New orthogonal designs of order 56. J. Combin. Designs **10**(6), 387–393 (2002)
60. Finlayson, K., Seberry, J., Wysocki, T., Xia, T.: Orthogonal designs with quaternion elements. In: ISCTA'05, Proceedings of 8^{th} International Symposium on Communication Theory and Applications, Ambleside, UK, 17-22 July 2005, pp. 270–272. HW Communications (2005)
61. Fletcher, R.J., Koukouvinos, C., Seberry, J.: New skew-Hadamard matrices of order $4 \cdot 59$ and new D-optimal designs of order $2 \cdot 59$. Discrete Mathematics **286**(3), 251–253 (2004)
62. Gabel, M.R.: Generic orthogonal stably-free projectives. J. of Algebra **29**, 477–488 (1974)
63. Gastineau-Hills, H.: Systems of orthogonal designs and quasi Clifford algebras. Ph.D. Thesis, University of Sydney, Australia (1980)
64. Gastineau-Hills, H.M.: Quasi clifford algebras and systems of orthogonal designs. Journal of the Australian Mathematical Society. Series A. Pure Mathematics and Statistics **32**(1), 1–23 (1982)
65. Gavish, A., Lempel, A.: On ternary complementary sequences. IEEE Trans. Inf. Theory **40**, 522–526 (1994)

66. Georgiou, S., Holzmann, W., Kharaghani, H., Tayfeh-Rezaie, B.: Some tables for: Three variable full orthogonal designs of order 56. University of Lethbridge: `http://www.cs.uleth.ca/~holzmann/cgi-bin/ODall.pl/table.pdf` (2007)
67. Georgiou, S., Holzmann, W., Kharaghani, H., Tayfeh-Rezaie, B.: Three variable full orthogonal designs of order 56. Journal of Statistical Planning and Inference **137**(2), 611–618 (2007)
68. Georgiou, S., Koukouvinos, C., Mitrouli, M., Seberry, J.: Necessary and sufficient conditions for two variable orthogonal designs in order 44: Addendum. JCMCC **34**, 59–64 (2000)
69. Georgiou, S., Koukouvinos, C., Mitrouli, M., Seberry, J.: A new algorithm for computer searches for orthogonal designs. J. Combin. Math Combin. Comput **39**, 49–63 (2001)
70. Georgiou, S., Koukouvinos, C., Mitrouli, M., Seberry, J.: Necessary and sufficient conditions for three and four variable orthogonal designs in order 36,. J. Statistical Planning and Inference **106**(1), 329–352 (2002)
71. Georgiou, S., Koukouvinos, C., Seberry, J.: On full orthogonal designs in order 56. Ars Combin. **65**, 79–89 (2002)
72. Georgiou, S., Koukouvinos, C., Seberry, J.: Short amicable sets. International Journal of Applied Mathematics **9**, 161–187 (2002)
73. Georgiou, S., Koukouvinos, C., Seberry, J.: On full orthogonal designs in order 72. JCMCC **44**, 11–21 (2003)
74. Georgiou, S., Koukouvinos, C., Stylianou, S.: On good matrices, skew Hadamard matrices and optimal designs. Computational Statistics and Data Analysis **41**(1), 171–184 (2002)
75. Georgiou, S.D., Stylianou, S., Drosou, K., Koukouvinos, C.: Construction of orthogonal and nearly orthogonal designs for computer experiments. Biometrika **101**(3), 741–747 (2014)
76. Geramita, A., Geramita, J.M.: Complex orthogonal designs. J. Combin. Theory **25**(3), 211–225 (1978)
77. Geramita, A.V., Geramita, J.M., Wallis, J.S.: Orthogonal designs. Linear and Multilinear Algebra **3**, 281–306 (1975)
78. Geramita, A.V., Pullman, N.J.: Radon's function and Hadamard arrays. Linear and Multilinear Algebra **2**, 147–150 (1974)
79. Geramita, A.V., Pullman, N.J., Wallis, J.S.: Families of weighing matrices. Bull. Austral. Math. Soc. **10**, 109–112 (1974)
80. Geramita, A.V., Seberry, J.: Orthogonal Designs: Quadratic forms and Hadamard matrices, *Lecture Notes in Pure and Applied Mathematics*, vol. 45, 1st edn. Marcel Dekker, New York-Basel (1979)
81. Geramita, A.V., Seberry Wallis, J.: Orthogonal designs IV: Existence questions. J. Combinatorial Theory **Ser. A**(19), 66–83 (1975)
82. Geramita, A.V., Verner, J.H.: Orthogonal designs with zero diagonal. Canad. J. Math. **28**, 215–225 (1976)
83. Geramita, A.V., Wallis, J.S.: Some new constructions for orthogonal designs. In: L.R.A. Casse, W.D. Wallis (eds.) Combinatorial Mathematics IV: Proceedings of the Fourth Australian Conference, *Lecture Notes in Mathematics*, vol. 560, pp. 46–54. Springer-Verlag, Berlin-Heidelberg-New York (1976)
84. Ghaderpour, E.: Some constructions for amicable orthogonal designs. Australas. J. Combin. **63**(3), 374–384 (2015)
85. Ghaderpour, E.: Some nonexistence and asymptotic existence results for weighing matrices. Int. J. Comb. p. 6 (2016)
86. Ghaderpour, E., Kharaghani, H.: The asymptotic existence of orthogonal designs. Australas. J. Combin. **58**, 333–346 (2014)
87. Glynn, D.: . Ph.D. Thesis, University of Adelaide, Australia (1980)
88. Goethals, J.M., Seidel, J.J.: Orthogonal matrices with zero diagonal. Canad. J. Math. **19**, 1001–1010 (1967)

89. Goethals, J.M., Seidel, J.J.: A skew-Hadamard matrix of order 36. J. Austral. Math. Soc. **11**, 343–344 (1970)
90. Golay, M.J.E.: Note on complementary series. Proc. IRE **50**, 84 (1962)
91. Goldberg, K.: Hadamard matrices of order cube plus one. Proc. Amer. Math. Soc. **17**, 744–746 (1966)
92. Gordon, B.: A note on unequivalent Hadamard matrices. J. Reine Angew. Math. pp. 427–433 (1974)
93. Griffin, M.: There are no golay sequences of length 2.9^t. Aequationes Math. **15**, 73–77 (1977)
94. Gysin, M., Seberry, J.: On ternary complementary pairs. Austral. J. Combin. **23**, 153–170 (2001)
95. Hadamard, J.: Résolution d'une question relative aux déterminants. Bull. des Sciences Math. **17**, 240–246 (1893)
96. Hain, R.: Private communication (1976)
97. Hall Jr, M.: Combinatorial Theory, 1st edn. Blaisdell Ginn and Co., Waltham, Massachusetts (1967)
98. Hedayat, A., Wallis, W.D.: Hadamard matrices and their applications. Annals of Statistics **6**, 1184–1238 (1978)
99. Herstein, I.N.: Non-commutative rings, *Carus Mathematical Monographs*, vol. 15. Mathematical Association of America (1968). (distributed by John Wiley and Sons).
100. Holzmann, W.H., Kharaghani, H.: On the orthogonal designs of order 24. Discrete Applied Mathematics **102**(1-2), 103–114 (2000)
101. Holzmann, W.H., Kharaghani, H.: On the Plotkin arrays. Australas. J. Combin. **22**, 287–299 (2000)
102. Holzmann, W.H., Kharaghani, H.: On the orthogonal designs of order 40. Journal of Statistical Planning and Inference **96**(2), 415 – 429 (2001)
103. Holzmann, W.H., Kharaghani, H.: Sequences and arrays involving free variables. J. Combinatorial Designs **9**(1), 17–27 (2001)
104. Holzmann, W.H., Kharaghani, H., Seberry, J., Tayfeh-Rezaie, B.: On orthogonal designs in order 48. Journal of Statistical Planning and Inference **128**(1), 311 – 325 (2005)
105. Holzmann, W.H., Kharaghani, H., Tayfeh-Rezaie, B.: All triples for orthogonal designs of order 40. Discrete Mathematics **308**(13), 2796–2801 (2008)
106. Holzmann, W.H., Kharaghani, H., Tayfeh-Rezaie, B.: Williamson matrices up to order 59. Designs, Codes and Cryptography **46**(3), 343–352 (2008)
107. Horton, J., Seberry, J.: When the necessary conditions are not sufficient: sequences with zero autocorrelation function. Bull ICA **27**, 51–61 (1999)
108. Hughes, D.R., Piper, F.C.: Projective Planes, *Graduate Texts in Mathematics*, vol. 6. Springer-Verlag, Berlin-Heidelberg-New York (1970)
109. Hunt, D.C.: Skew-Hadamard matrices of order less than 100. In: Proc. First Aust. Conf. on Combinatorial Math., pp. 55–59. TUNRA, Newcastle, Aust. (1972)
110. Hunt, D.C., Wallis, J.: Cyclotomy, Hadamard arrays and supplementary difference sets. In: Proceedings of the Second Manitoba Conference on Numerical Mathematics, *Congressus Numerantium*, vol. 7, pp. 351–381. University of Manitoba, Winnipeg, Canada (1973)
111. Hurwitz, A.: Über die Komposition der Quadratischen Formen. Math. Ann. **88**, 1–25 (1923)
112. Ibbett, R., Aspinall, D., Grainger, J.F.: Real-time multiplexing of dispersed spectra in any wavelength region. Appl. Optics. **7**, 1089–1093 (1968)
113. Isaeva, O.M., Sarytchev, V.A.: Quaternion presentations polarization state. In: Proc. 2nd IEEE Topical Symposium of Combined Optical-Microwave Earth and Atmosphere Sensing, pp. 195–196 (1995)
114. Ito, N.: On Hadamard groups III. Kyushu J. Math.J **51**, 369–379 (1997)

115. Ito, N.: On Hadamard groups IV. Journal of Algebra **234**, 651–663 (2000)
116. James, M.: Golay sequences. Honours Thesis, University of Sydney, Australia (1987)
117. Janko, Z., Kharaghani, H.: A block negacyclic Bush-type Hadamard matrix and two strongly regular graphs. J. Combin. Theory, Series A **98**(1), 118–126 (2002)
118. Jauregui Jr, S.: Complementary sequences of length 26. IRE. Trans. Information Theory **8**(4), 323 (1962)
119. Kawada, Y., Iwahori, N.: On the structure and representations of Clifford algebras. J. Math. Soc. Japan **2**, 34–43 (1950)
120. Kharaghani, H.: Arrays for orthogonal designs. J. Combin. Designs **8**(3), 166–173 (2000)
121. Kharaghani, H.: On a class of symmetric balanced generalized weighing matrices. Designs, Codes and Cryptography **30**(2), 139–149 (2003)
122. Kharaghani, H., Tayfeh-Rezaie, B.: Some new orthogonal designs in orders 32 and 40. Discrete Mathematics **279**(1-3), 317 – 324 (2004)
123. Kharaghani, H., Tayfeh-Rezaie, B.: A Hadamard matrix of order 428. J. Combin Designs **13**(6), 435–440 (2005)
124. Kimura, H.: Classification of Hadamard matrices of order 28. Discrete Mathematics **133**(1-3), 171–180 (1994)
125. Kotsireas, I.S., Koukouvinos, C.: Periodic complementary binary sequences of length 50. Int. J. Appl. Math. **21**(3), 509–514 (2008)
126. Koukouvinos, C.: Some new three and four variable orthogonal designs in order 36. Journal of Statistical Planning and Inference **73**(1-2), 21–27 (1998)
127. Koukouvinos, C.: Designs. `http://www.math.ntua.gr/~ckoukouv/Designs/Hadamardmatrices` (2016). Visited 23 September 2016
128. Koukouvinos, C.: Skew-sequences. private communication (2016)
129. Koukouvinos, C., Mitrouli, M., Seberry, J.: Some necessary and sufficient conditions for two variable orthogonal designs in order 44. JCMCC **28**, 267–287 (1998)
130. Koukouvinos, C., Mitrouli, M., Seberry, J., Karabelas, P.: On sufficient conditions for some orthogonal designs and sequences with zero autocorrelation function. Australas. J. Combin. **13**, 197–216 (1996)
131. Koukouvinos, C., Platis, N., Seberry, J.: Necessary and sufficient conditions for some two variable orthogonal designs in order 36. Congressus Numerantium **114**, 129–140 (1996)
132. Koukouvinos, C., Seberry, J.: On weighing matrices. Utilitas Math. **43**, 101–127 (1993)
133. Koukouvinos, C., Seberry, J.: New weighing matrices. Sankhya, Series B **58**, 221–230 (1996)
134. Koukouvinos, C., Seberry, J.: New weighing matrices and orthogonal designs constructed using two sequences with zero autocorrelation function - a review. Journal of Statistical Planning and Inference **81**(1), 153 – 182 (1999)
135. Koukouvinos, C., Seberry, J.: New orthogonal designs and sequences with two and three variables in order 28. Ars Combinatoria **54**, 97–108 (2000)
136. Koukouvinos, C., Seberry, J.: Infinite families of orthogonal designs: I. Bull. ICA **33**, 35–41 (2001)
137. Koukouvinos, C., Seberry, J.: Orthogonal designs of Kharaghani type: I. Ars Combinatoria **67**, 89–96 (2003)
138. Koukouvinos, C., Stylianou, S.: On skew-Hadamard matrices. Discrete Math. **308**(13), 2723–2731 (2008)
139. Kruskal, J.B.: Golay's complementary series. IRE. Trans. Information Theory **7**(4), 273–276 (1961)
140. Lakein, R.B., Wallis, J.S.: On the matrices used to construct Baumert-Hall arrays. In: Combinatorial Mathematics: III, *Lecture Notes in Mathematics*, vol. 452, pp. 156–170. Springer-Verlag, Berlin-Heidelberg-New York (1975)
141. Lam, C.W.H.: The search for a finite projective plane of order 10. Amer. Math. Monthly **98**(4), 305–318 (1991)

142. Lam, T.Y.: The Algebraic Theory of Quadratic Forms. Mathematics lecture note. Benjamin/Cummings Publishing, Reading, Mass. (1973)
143. de Launey, W.: On the asymptotic existence of Hadamard matrices. ArXiv e-prints (2010). Also published in J. Combinatorial Theory, Series A 116 (2009) 1002-1008
144. de Launey, W., Gordon, D.M.: On the density of the set of known Hadamard orders. ArXiv e-prints (2010)
145. de Launey, W., Kharaghani, H.: On the asymptotic existence of cocyclic Hadamard matrices. J. Combin. Theory **116**(6), 1140–1153
146. de Launey, W., Levin, D.A.: A fourier-analytic approach to counting partial Hadamard matrices. ArXiv e-prints (2010)
147. Lawson, S.: Light appears at end of fast Wi-Fi tunnel. IDG News Service: `http://www.pcworld.com/article/124369/article.html` (2006). Accessed on 05/09/2006
148. Liang, X.B.: Orthogonal designs with maximal rates. IEEE Trans. Inform. Theory **49**(10), 2468–2503 (2003)
149. Liang, X.B., Xia, X.G.: On the nonexistence of rate-one generalized complex orthogonal designs. IEEE Transactions on Information Theory **49**(11), 2984–2988 (2003)
150. van Lint, J.H., Seidel, J.J.: Equilateral point sets in elliptic geometry. In: Proceedings of the Koninklijke Nederlandse Akademie van Wetenschappen: Series A (and Indag. Math., 28), *Mathematical Sciences*, vol. 69, pp. 335–348 (1966)
151. Marcus, M., Minc, H.: A Survey of Matrix Theory and Matrix Inequalities. Allyn and Bacon series in advanced mathematics. Allyn and Bacon, Boston (1964)
152. Mullin, R.C.: Normal affine resolvable designs and orthogonal matrices. Utilitas Math. **6**(6), 195–208 (1974)
153. Mullin, R.C.: A note on balanced weighing matrices, *Lecture Notes in Mathematics*, vol. 452, pp. 28–41. Springer-Verlag, Berlin-Heidelberg-New York (1975)
154. Mullin, R.C., Stanton, R.G.: Balanced weighing matrices and group divisible designs. Utilitas Math. **8**, 303–310 (1975)
155. Mullin, R.C., Stanton, R.G.: Group matrices and balanced weighing designs. Utilitas Math. **8**, 277–301 (1975)
156. Ohmori, H.: Classification of weighing matrices of small orders. Hiroshima Math. J. **22**, 129–176 (1992)
157. Ohmori, H.: Classification of weighing matrices of order 13 and weight 9. Discrete Mathematics **116**(1-3), 55–78 (1993)
158. Ohmori, H., Miyamoto, T.: Construction of weighing matrices $W(17,9)$ having the intersection number 8. Designs, Codes and Cryptography **15**(3), 259–269 (1998)
159. O'Meara, O.T.: Introduction to Quadratic Forms, *Die Grundlehren der mathematischen Wissenschaften*, vol. 117, 3rd corrected printing (english) edn. Springer-Verlag, Berlin-Heidelberg-New York (1973)
160. Paley, R.E.A.C.: On orthogonal matrices. J. Math. Phys. **12**, 311–320 (1933)
161. Plotkin, M.: Decomposition of Hadamard matrices. J. Combinatorial Theory **ser A.**(13), 127–130 (1972)
162. Radon, J.: Lineare Scharen Orthogonaler Matrizen. Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **1**(1), 1–14 (1922)
163. Raghavarao, D.: Some aspects of weighing designs. Ann. Math. Stat. **31**, 878–884 (1960)
164. Raghavarao, D.: Constructions and Combinatorial Problems in Design of Experiments. Wiley series in probability and mathematical statistics. John Wiley and Sons Inc., New York (1971)
165. Robinson, P.J.: Amicable orthogonal designs. Bull. Austral. Math. Soc. **14**, 303–314 (1976)
166. Robinson, P.J.: Concerning the existence and construction of orthogonal designs. Ph.D. Thesis, Australian National University, Canberra, Australia (1977)
167. Robinson, P.J.: The existence of orthogonal designs in order sixteen. Ars Combinatoria **3**, 209–218 (1977)

168. Robinson, P.J.: Using product designs to construct orthogonal designs. Bull. Austral. Math. Soc. **16**, 297–305 (1977)
169. Robinson, P.J., Seberry, J.: Orthogonal designs in powers of two. Ars Combinatoria **4**, 43–57 (1977)
170. Robinson, P.J., Seberry, J.: On the structure and existence of some amicable orthogonal designs. J. Austral. Math. Soc. **Series A**(25), 118–128 (1978)
171. Ryser, H.J.: Combinatorial Mathematics, *Carus Mathematical Monographs*, vol. 14. Mathematical Association of America, Buffalo distributed by Wiley New York (1963)
172. Samuel, P.: Algebraic Theory of Numbers, English translation - Houghton Mifflin, Boston, 1970 edn. Hermann, Paris (1967)
173. Schafer, R.D.: An Introduction to Nonassociative Algebras. No. 22 in Pure and Applied Mathematics. Academic Press, New York-London (1966)
174. Scharlau, W.: Quadratic forms, *Queen's Papers on Pure and Applied Mathematics*, vol. 22. Queen's University, Kingston, Ont. (1969)
175. Schellenberg, P.J.: Private communication (1976)
176. Schmidt, B.: Review mr2372843 (2008i:05025) of w. h. holzmann, h. kharaghani, b. tayfeh-rezaie, [106]. `http://www.ams.org/mathscinet/search/publdoc.html?b=2372843` (2008)
177. Seberry, J.: Some remarks on generalized Hadamard matrices and theorems of Rajkundlia on SBIBDs. In: Combinatorial Mathematics VI, *Lecture Notes in Mathematics*, vol. 748, pp. 154–164. Springer-Verlag (1979)
178. Seberry, J.: Good matrices online resource. `http://www.uow.edu.au/~jennie/good.html` (1999)
179. Seberry, J.: New families of amicable Hadamard matrices. J. Statistical Theory and Practice **7**(4), 650–657 (2013). In memory of Jagdish N Srivastava
180. Seberry, J.: Strongly amicable Hadamard matrices and amicable orthogonal designs. Australasian J Combinatorics **55**, 5–13 (2013)
181. Seberry, J., Adams, S.: The amicable-Kronecker construction of quaternion orthogonal designs. Australasian J. Combin. **50**, 243–258 (2011)
182. Seberry, J., Balonin, N.: The propus construction for symmetric Hadamard matrices. to appear
183. Seberry, J., Craigen, R.: Orthogonal Designs, 1st edn., chap. 31, pp. 400–406. CRC Press series on discrete mathematics and its applications. CRC Press, Boca Raton, FL (1996)
184. Seberry, J., Finlayson, K., Adams, S.S., Wysocki, T.A., Xia, T., Wysocki, B.J.: The theory of quaternion orthogonal designs. IEEE Trans. Signal Proc. **56**(1), 256–265 (2008)
185. Seberry, J., Spence, S., Wysocki, T.: A construction technique for generalized complex orthogonal designs and applications to wireless communications. Linear Alg. and Applic. **405**, 163–176 (2005)
186. Seberry, J., Wang, Y., Wysocki, B., Wysocki, T., Xia, T.: New complex orthogonal space-time block codes of order eight. In: B. Honary, T. Wysocki, B. Wysocki (eds.) Signal Processing for Telecommunications and Multimedia, *Multimedia systems and applications*, vol. 27, pp. 173–182. Springer, New York (2004)
187. Seberry, J., Whiteman, A.: New Hadamard matrices and conference matrices obtained via Mathon's construction. Graphs and Combin. **4**, 355–377 (1988)
188. Seberry, J., Yamada, M.: Hadamard matrices, sequences and block designs, pp. 431–560. Wiley (1992)
189. Serre, J.P.: A Course in Arithmetic. Springer-Verlag, Berlin-Heidelberg-New York, (English Translation, Graduate Texts in Mathematics) (1973)
190. Shapiro, D.: Similarities, quadratic forms and Clifford algebras. Ph.D. Thesis, University of California, Berkeley (1970)
191. Shapiro, D.: Private communication (1975)

192. Shapiro, D.: Spaces of similarities I - the Hurwitz problem. J. of Algebra **46**, 148–170 (1977)
193. Shapiro, D.: Spaces of similarities II - pfister forms. J. of Algebra **46**, 171–180 (1977)
194. Shapiro, D.: Spaces of similarities IV - (s,t)-families. Pac. J. Math. **69**, 223–244 (1977)
195. Sloane, N.J.A., Harwit, M.: Masks for Hadamard transform optics and weighing designs. Appl. Optics **15**, 107–114 (1975)
196. Speiser, A.: Theorie der Gruppen von endliches ordnung. Springer-Verlag, Berlin (1937)
197. Spence, E.: A new class of Hadamard matrices. Glasgow J. **8**, 59–62 (1967)
198. Spence, E.: Hadamard matrices from relative difference sets. J. Combin. Theory **Ser. A,**(19), 287–300 (1975)
199. Squire, W.D., Whitehouse, H.J., Alsup, J.M.: Linear signal processing and ultrasonic transversal filters. IEEE Trans. Microwave Theory and Technol. **MTT-17**(11), 1020–1040 (1969)
200. Storer, T.: Cyclotomy and Difference Sets, *Lectures in Advanced Mathematics*, vol. 2. Markham Pub. Co., Chicago (1967)
201. Strassler, Y.: The classification of circulant weighing matrices of weight 9. Ph.D. Thesis, Bar-Ilan University, Ramat-Gan, Israel (1997)
202. Street, D.: Cyclotomy and designs. Ph.D. Thesis, University of Sydney, Australia (1981)
203. Street, D.: Amicable orthogonal designs of order eight. J. Australian Mathematical Society **Series A**(33), 23–29 (1982)
204. Sylvester, J.J.: Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tesselated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers. Phil. Mag. **34**(4), 461–475 (1867)
205. Szekeres, G.: Tournaments and Hadamard matrices. Enseignment Math. **15**, 269–278 (1969)
206. Szekeres, G.: A note on skew type orthogonal ± 1 matrices. Coll. Math. Soc. Janos Bolyai **52**, 489–498 (1987). Presented at the Combinatorics Conference, Eger (Hungary).)
207. Taki, Y., Miyakawa, H., Hatori, M., Namba, S.: Even shift orthogonal sequences. IEEE Trans. Information Theory **15**(2), 295–300 (1969)
208. Tarokh, V., Jafarkhani, H., Calderbank, A.: Space-time block coding for wireless communications: performance results. IEEE J. Select Areas Commun. **17**(3), 451–460 (1999)
209. Tarokh, V., Jafarkhani, H., Calderbank, A.: Space-time block coding from orthogonal designs. IEEE Trans. Inform. Theory **45**(5), 1456–1467 (1999)
210. Tirkkonen, O., Hottien, A.: Square-matrix embeddable space-time block codes for complex signal constellations. IEEE Trans. Inform. Theory **48**(2), 384–395 (2002)
211. Todd, J.A.: A combinatorial problem. J. Math. and Physics **12**, 321 (1933)
212. Tran, L., Seberry, J., Wysocki, B., Wysocki, T., Xia, T., Zhao, Y.: Two new complex orthogonal space-time codes for 8 trnsmit antennas. IEEE Electronics Lett. **40**(1), 55–56 (2004)
213. Tran, L., Wysocki, T., Mertins, A., Seberry, J.: Complex Orthogonal Space-Time Processing in Wireless Communications. Springer-Verlag, New York (2006)
214. Tran, L.C.: Complex orthogonal space-time processing in wireless communications. Ph.D. Thesis, University of Wollongong, Australia (2006)
215. Tseng, C.C.: Signal multiplexing in surface-wave delay lines using orthogonal pairs of Golay's complementary sequences. IEEE Trans. Sonics and Ultrasonics **SU-18**(2), 103–107 (1971)
216. Turyn, R.J.: Ambiguity functions of complementary sequences. IEEE Trans. Information Theory **IT-9**(1), 46–47 (1963)

217. Turyn, R.J.: On C-matrices of arbitrary powers. Bull. Canad. Math. Soc. **23**, 531–535 531–535 (1971)
218. Turyn, R.J.: An infinite class of Williamson matrices. J. Combinatorial Theory **12**, 319–321 (1972)
219. Turyn, R.J.: Computation of certain Hadamard matrices. Notices Amer. Math. Soc. **20**, A–1 (1973)
220. Turyn, R.J.: Four-phase Barker codes. IEEE Trans. Information Theory **IT-20**(3), 366–371 (1974)
221. Turyn, R.J.: Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compressions and surface wave encodings. J. Combinatorial Theory **Ser. A**(16), 313–333 (1974)
222. Vial, P., Wysocki, B., Raad, I., Wysocki, T.: Space time spreading with modified Walsh-Hadamard sequences. In: Spread Spectrum Techniques and Applications, 2004 IEEE Eighth International Symposium on, pp. 943–946 (2004)
223. Vollrath, A.: A modification of periodic Golay sequence pairs. Indiana University REU (2008). Available online: `http://mypage.iu.edu/worrick/reubook08-1.pdf`
224. Wallis, J.: A class of Hadamard matrices. J. Combinatorial Theory **6**, 40–44 (1969)
225. Wallis, J.: A note of a class of Hadamard matrices. J. Combinatorial Theory **6**, 222–223 (1969)
226. Wallis, J.: Hadamard designs. Bull. Austral. Math. Soc. **2**, 45–54 (1970)
227. Wallis, J.: (v, k, λ)-configurations and Hadamard matrices. J. Austral. Math. Soc. **11**, 297–309 (1970)
228. Wallis, J.: Amicable Hadamard matrices. J. Combinatorial Theory **Ser. A**(11), 296–298 (1971)
229. Wallis, J.: A skew-Hadamard matrix of order 92. Bull. Austral. Math. Soc. **5**, 203–204 (1971)
230. Wallis, J.: Some $(1, -1)$ matrices. J. Combinatorial Theory **Ser. B**(10), 1–11 (1971)
231. Wallis, J.: Combinatorics: Room squares, sum-free sets, Hadamard matrices, *Lecture Notes in Mathematics*, vol. 292, chap. Hadamard matrices, pp. 273–489. Springer-Verlag, Berlin-Heidelberg-New York (1972)
232. Wallis, J.: Orthogonal $(0, 1, -1)$ matrices. In: Proceedings of the First Australian Conference on Combinatorial Mathematics, pp. 61–84. TUNRA Ltd. Newcastle, Australia (1972)
233. Wallis, J.: A note on amicable Hadamard matrices. Utilitas Mathematica **3**, 119–125 (1973)
234. Wallis, J.: Some remarks on supplementary difference sets. Colloquia Mathematica Societatis Janos Bolyai **Infinite and finite sets**(10), 1503–1526 (1973)
235. Wallis, J.: Williamson matrices of even order. In: D.A. Holton (ed.) Combinatorial Mathematics: Proceedings of the Second Australian Conference, *Lecture Notes in Mathematics*, vol. 403, pp. 132–142. Springer-Verlag, Berlin-Heidelberg-New York (1974)
236. Wallis, J.: Construction of Williamson type matrices. J. Linear and Multilinear Algebra **3**, 197–207 (1975)
237. Wallis, J.: On the existence of Hadamard matrices. J. Combinatorial Th. **Ser. A**(21), 444–451 (1976)
238. Wallis, J.: Orthogonal designs V: Orders divisible by eight. Utilitas Math. **9**, 263–281 (1976)
239. Wallis, J.S.: Combinatorial matrices. Bull. Austral. Math. Soc. **5**, 285–286 (1971)
240. Wallis, J.S.: Combinatorial matrices. Ph.D. Thesis, La Trobe University, Melbourne, Australia (1971)
241. Wallis, J.S., Whiteman, A.L.: Some classes of Hadamard matrices with constant diagonal. Bull. Austral. Math. Soc. **7**, 233–249 (1972)
242. Wallis, J.S., Whiteman, A.L.: Some results on weighing matrices. Bull. Austral. Math. Soc. **12**(12), 433–447 (1975)

243. Welch, L.R.: Unpublished paper (1971). University of Southern California
244. Williamson, J.: Hadamard's determinant theorem and the sum of four squares. Duke Math. J. **11**, 65–81 (1944)
245. Williamson, J.: Note on Hadamard's determinant theorem. Bull. Amer. Math. Soc. **53**, 608–613 (1947)
246. Wilson, R.M.: Cyclotomy and difference families in elementary abelian groups. J. Number Theory **4**, 17–47 (1972)
247. Wolfe, W.W.: Orthogonal designs - amicable orthogonal designs - some algebraic and combinatorial techniques. Ph.D. Thesis, Queen's University, Kingston, Ontario (1975)
248. Wolfe, W.W.: Rational quadratic forms and orthogonal designs. Queen's Mathematical Preprint **No. 1975-22** (1975)
249. Wysocki, B.J., Wysocki, T.A.: Modified Walsh-Hadamard sequences for DS CDMA wireless systems. International Journal of Adaptive Control and Signal Processing **16**(8), 589–602 (2002)
250. Xia, T.: Negacyclic matrices of orders 7,9, and 11. Private communication (2016)
251. Xia, T., Xia, M.Y., Seberry, J.: Hadamard matrices constructed from circulant and nega-cyclic matrices. Australasian J. Comb. **34**, 105–116 (2006)
252. Xing, C., Arasu, K., Leung, K., Ma, S., Nabavi, A., Ray-Chaudhuri, D.: Determination of all possible orders of weight 16 circulant weighing matrices. Finite Fields and Their Applications **12**(4), 498 – 538 (2006). Special Issue Celebrating Prof. Zhe-Xian Wan's 80th Birthday
253. Yang, C.: Maximal binary matrices and sum of two squares. Math. of Computation **30**(133), 148–153 (1976)
254. Yuen, C., Guan, Y., Tjhung, T.: Orthogonal space-time block code from amicable complex orthogonal design. In: Acoustics, Speech, and Signal Processing, 2004. Proceedings. (ICASSP '04). IEEE International Conference on, vol. 4, pp. 469–472 (2004)
255. Yuen, C., Guan, Y., Tjhung, T.: Amicable complex orthogonal designs. Australasian J. Combin. **44**, 111–121 (2009)
256. Zhao, Y., Seberry, J., Xia, T., Wang, Y., Wysocki, B., Wysocki, T., Tran, L.: On amicable orthogonal designs of order 8 for complex space-time block codes. Australas. J. Combin. **34**, 137–144 (2006)
257. Zhao, Y., Seberry, J., Xia, T., Wysocki, B., Wysocki, T.: Amicable orthogonal designs of quaternions. In: 17th Australasian Workshop on Combinatorial Algorithms (AWOCA 2006), pp. 187–197 (2006). CDROM
258. Zhao, Y., Wang, Y., Seberry, J.: On amicable orthogonal designs of order 8. Australas. J. Combin. **34**, 321–329 (2006)

Index

J. Seberry, *Orthogonal Designs*,
DOI 10.1007/978-3-319-59032-5

D

H

O

P

Q

R

T

W