

2013

Asymptotic existence of orthogonal designs

Ghaderpour, Ebrahim

Lethbridge, Alta. : University of Lethbridge, Dept. of Mathematics and Computer Science

<http://hdl.handle.net/10133/3595>

Downloaded from University of Lethbridge Research Repository, OPUS

ASYMPTOTIC EXISTENCE OF ORTHOGONAL DESIGNS

EBRAHIM GHADERPOUR
M.Sc., Isfahan University of Technology, 2010

A Thesis
Submitted to the School of Graduate Studies
of the University of Lethbridge
in Partial Fulfillment of the
Requirements for the Degree

DOCTOR OF PHILOSOPHY

Department of Mathematics and Computer Science
University of Lethbridge
LETHBRIDGE, ALBERTA, CANADA

© Ebrahim Ghaderpour, 2013

Abstract

An *orthogonal design* of order n and type (s_1, \dots, s_ℓ) , denoted $OD(n; s_1, \dots, s_\ell)$, is a square matrix X of order n with entries from $\{0, \pm x_1, \dots, \pm x_\ell\}$, where the x_j 's are commuting variables, that satisfies $XX^t = \left(\sum_{j=1}^{\ell} s_j x_j^2\right) I_n$, where X^t denotes the transpose of X , and I_n is the identity matrix of order n .

An asymptotic existence of orthogonal designs is shown. More precisely, for any ℓ -tuple (s_1, \dots, s_ℓ) of positive integers, there exists an integer $N = N(s_1, \dots, s_\ell)$ such that for each $n \geq N$, there is an $OD(2^n(s_1 + \dots + s_\ell); 2^n s_1, \dots, 2^n s_\ell)$. This result of Chapter 5 complements a result of Peter Eades et al. which in turn implies that if the positive integers s_1, s_2, \dots, s_ℓ are all *highly* divisible by 2, then there is a full orthogonal design of type $(s_1, s_2, \dots, s_\ell)$.

Some new classes of orthogonal designs related to weighing matrices are obtained in Chapter 3.

In Chapter 4, we deal with product designs and amicable orthogonal designs, and a construction method is presented.

Signed group orthogonal designs, a natural extension of orthogonal designs, are introduced in Chapter 6. Furthermore, an asymptotic existence of signed group orthogonal designs is obtained and applied to show the asymptotic existence of orthogonal designs.

Acknowledgments

I would like to thank my examination committee members, Professors Akbary, Craigen, Holzmann, Kharaghani, Ng, Walton and Yazdani for their kind suggestions. Sean Legge was quite generous in his time to help me with the grammatical changes.

Professor Craigen was extremely generous in spending long late hours and making many essential suggestions.

I am specially thankful to my supervisor, Professor Kharaghani, for taking me as a student, providing me with problems for my thesis and helping me whenever I needed help. Without his guidance, I would not be able to finish this thesis.

I also would like to thank my family who are always supporting me.

Financial support from the University of Lethbridge is greatly appreciated.

Contents

Abstract	ii
Acknowledgments	iii
Table of Contents	iv
1 Introduction and statement of results	1
2 Preliminaries	9
2.1 Weighing matrices	9
2.2 Orthogonal designs	11
2.3 Type 1 and type 2 matrices	14
2.4 Autocorrelation functions	19
2.5 Amicable and anti-amicable matrices	21
2.6 Product designs	24
3 Asymptotic existence of weighing matrices	26
3.1 Non-existence results for weighing matrices	26
3.2 Asymptotic existence of weighing matrices	29
4 Some notes on amicable orthogonal designs	38
4.1 A non-existence result for product designs	38
4.2 Some full amicable orthogonal designs	39
4.3 An infinite class of full amicable orthogonal designs	45
4.4 Amicable full orthogonal designs in 16 variables	46
5 Asymptotic existence of orthogonal designs	48
5.1 Asymptotic existence of orthogonal designs	49
5.2 Asymptotic existence of amicable orthogonal designs	58
6 Signed group orthogonal designs and their applications	63
6.1 Signed groups and remreps	63
6.2 Signed group orthogonal designs	67
6.3 Real and complex Golay pairs in two variables	73

6.4	Some applications of signed group orthogonal designs	78
6.5	Signed group orthogonal designs of order 2^n and an application to the construction of orthogonal designs	97
Appendix Some amicable orthogonal designs		103
Bibliography		112

Chapter 1

Introduction and statement of results

A *complex orthogonal design* of order n and type (s_1, \dots, s_ℓ) , denoted $COD(n; s_1, \dots, s_\ell)$, is a square matrix X of order n with entries from $\{0, \epsilon_1 x_1, \dots, \epsilon_\ell x_\ell\}$, where the x_j 's are commuting variables and $\epsilon_j \in \{\pm 1, \pm i\}$ for each j , that satisfies

$$XX^* = \left(\sum_{j=1}^{\ell} s_j x_j^2 \right) I_n,$$

where X^* denotes the conjugate transpose of X , and I_n is the identity matrix of order n . A complex orthogonal design (COD) in which $\epsilon_j \in \{\pm 1\}$ for all j is called an *orthogonal design*, denoted $OD(n; s_1, \dots, s_\ell)$. An orthogonal design (OD) in which there is no zero entry is called a *full* OD.

COD's and OD's have many applications in space-time block codes [47], wireless network connections [26], quadratic forms [45, 52], and they also have applications in electronics engineering [37].

A *Hadamard matrix* of order n is a square $\{\pm 1\}$ -matrix H of order n such that $HH^t = nI_n$, where H^t is the transpose of H . Equating all variables to 1 in any full

OD results in a Hadamard matrix.

Hadamard matrices were first studied by Sylvester in 1867 under the name of *anallagmatic pavement* 26 years before Hadamard considered them in 1893 [20]. It is conjectured that a Hadamard matrix of order $4n$ exists for each $n \geq 1$ [39]. Hadamard matrices are well known up to order 668. Hadi Kharaghani and Behruz Tayfeh-Rezaie in [31] constructed a Hadamard matrix of order 428.

A *Weighing matrix* of order n and weight k is a square $\{0, \pm 1\}$ -matrix W of order n such that $WW^t = kI_n$. Equating all variables to 1 in any OD of order n results in a weighing matrix of order n and weight k , denoted $W(n, k)$, where k is the number of ± 1 in each row (column) of the weighing matrix. It is conjectured that there exists a $W(4t, k)$ for each $1 \leq k \leq 4t$ [18].

Hadamard matrices and weighing matrices have applications in balanced incomplete block designs [21], tournaments [41], codes, graphs and statistics [2, 27, 34].

The credit for the consideration of *asymptotic existence* results should be given to Seberry [18, 50] for her fundamental approach in showing that for each positive integer p , there is a Hadamard matrix of order $2^n p$ for each $n \geq 2 \log_2(p-3)$. Two of Seberry's students, Peter Robinson [43] and Peter Eades [13], did extensive work on ODs in their Ph.D. theses and made significant advances towards showing the asymptotic existence of a number of ODs. The work of Warren Wolfe [53] provided enough ammunition to other researchers to pursue a different approach to the asymptotic existence of ODs. There are now a number of asymptotic existence results for orthogonal designs and thus Hadamard matrices [5, 7, 9, 10, 11, 15, 24].

It was shown [18, 40] that the number of variables in an OD of order $n = 2^a b$, b odd, cannot exceed $\rho(n)$ (Radon's number), where $\rho(n)$ is defined as follows:

$$\rho(n) := 8c + 2^d, \quad \text{where } a = 4c + d, \quad 0 \leq d < 4.$$

A *rational family* of order n and type (s_1, \dots, s_k) , where the s_i 's are positive rational numbers, is a collection of k rational matrices of order n , A_1, \dots, A_k , satisfying

- $A_i A_i^t = s_i I_n$, $1 \leq i \leq k$;
- $A_i A_j^t = -A_j A_i^t$, $1 \leq i \neq j \leq k$.

Peter Eades [14], Daniel Shapiro [45] and Warren Wolfe [52, 53] made a connection between quadratic forms over rational numbers and orthogonal designs, and they obtained some non-existence results for orthogonal designs.

Theorem 1.1 (Rational Family Theorem [45, 53]). *Suppose that $n = 2^a b$ where b is odd. Then there is a rational family of type (s_1, s_2, \dots, s_u) and order n if and only if*

- (i) $u \leq \rho(n)$,
- (ii) *there is a $u \times 2^\alpha$ rational matrix P such that $PP^t = \text{diag}(s_1, s_2, \dots, s_u)$.*

The conditions (i) and (ii) are called the algebraic necessary conditions for the existence of orthogonal designs. By numerical evidence, it is conjectured that if n is sufficiently larger than $s_1 + s_2 + \dots + s_u$, then the algebraic necessary conditions (i) and (ii) are sufficient for existence of ODs of order n and type (s_1, s_2, \dots, s_u) .

Conjecture 1.2 (Asymptotic Sufficiency Conjecture [13]). *Suppose that α is a non-negative integer and s_1, s_2, \dots, s_u are positive integers such that $u \leq \rho(2^\alpha)$ and there is a $u \times 2^\alpha$ rational matrix P such that $PP^t = \text{diag}(s_1, s_2, \dots, s_u)$. Then there is an integer N such that for each $n \geq N$, there is an*

$$OD(2^\alpha n; s_1, s_2, \dots, s_u).$$

The case $\alpha = 0$ of this conjecture first was proved by Geramita and Wallis [17]. The cases $\alpha = 1, 2, 3$ was proved by Eades [13]. We discuss these cases by slightly different methods in Chapter 3.

Throughout this thesis, we use the notation $u_{(k)}$ to show that u repeats k times.

It is shown in Theorem 3.7 that if k cannot be written as the sum of three integer squares, then there does not exist any skew-symmetric $W(4n, k)$, for any odd number n . Then by using Lemma 3.13, which indicates the existence of symmetric $OD(2^k; 1_{(k)})$ for any positive integer k , it is shown in Theorem 3.18 that if k is a square, then there is an integer $N = N(k)$ such that for each $n \geq N$ there is a symmetric $W(n, k)$. We prove Theorems 3.19 and 3.22 by slightly different methods:

- Suppose that $k = k_1^2 + k_2^2$, where k_1 and k_2 are two nonzero integers. Then there is an integer $N = N(k)$ such that for each $n \geq N$ there is an $OD(2n; k_1^2, k_2^2)$.
- Suppose that $k = k_1^2 + k_2^2 + k_3^2 + k_4^2$, where k_1, k_2, k_3 and k_4 are nonzero integers. Then there is an integer $N = N(k)$ such that for each $n \geq N$ there is an $OD(4n; k_1^2, k_2^2, k_3^2, k_4^2)$.

In Corollary 3.21, it is shown that if d is an integer square, then there exists an integer $N = N(d)$ such that for each $n \geq N$, there is a skew-symmetric $W(2n, d)$.

In Corollary 3.25, it is shown that if d is the sum of three integer squares, then there exists an integer $N = N(d)$ such that for each $n \geq N$, there is a skew-symmetric $W(4n, d)$.

In Corollary 3.26, it is shown that if d is any positive integer, then there exists an integer $N = N(d)$ such that for each $n \geq N$, there is a skew-symmetric $W(8n, d)$.

Corollaries 3.21, 3.25 and 3.26 are improvements to the results that Eades in [13] obtained.

Suppose that A is an $OD(n; a_1, \dots, a_k)$ on variables x_1, \dots, x_k , and B is an $OD(n; b_1, \dots, b_t)$ on variables y_1, \dots, y_t , where the two sets of variables are disjoint. Then $(A; B)$ are called an *amicable orthogonal design*, denoted

$$AOD(n; a_1, \dots, a_k; b_1, \dots, b_t),$$

if $AB^t = BA^t$.

Let M_1 be an $OD(n; a_1, \dots, a_r)$ on variables x_1, \dots, x_r , M_2 be an $OD(n; b_1, \dots, b_s)$ on variables y_1, \dots, y_s , and N be an $OD(n; c_1, \dots, c_t)$ on variables z_1, \dots, z_t , where the three sets of variables are disjoint. Then $(M_1; M_2; N)$ is called a *product design* of type $(a_1, \dots, a_r; b_1, \dots, b_s; c_1, \dots, c_t)$ and order n if the following conditions hold:

- (i) $M_1 * N = M_2 * N = 0$ ($*$ is the entrywise multiplication),
- (ii) $M_1 + N$ and $M_2 + N$ are orthogonal designs, and
- (iii) $M_1 M_2^t = M_2 M_1^t$.

We denote this product design by $PD(n; a_1, \dots, a_r; b_1, \dots, b_s; c_1, \dots, c_t)$.

Product designs were first introduced by Robinson [43]. They are useful to construct full orthogonal designs with maximum number of variables for some orders and types.

In Theorem 4.5, we show that there does not exist any

$$PD(n; 1, 1, 1; 1, 1, 1; n - 3)$$

for all $n > 12$. However, Robinson in [43] showed that for each n , $n \in \{4, 8, 12\}$, there is a $PD(n; 1, 1, 1; 1, 1, 1; n - 3)$. Then we extend $PD(n; 1, 1, 1; 1, 1, 1; n - 3)$ for the cases $n = 8$ and $n = 12$ to construct new full amicable orthogonal designs with maximum number of variables in some small orders. The methods are slightly similar to [23]. Some of these amicable orthogonal designs are displayed in Appendix.

In Construction 4.14, we show that there exist

$$AOD(16; 2, 2, 2, 10; 2, 2, 2, 10) \quad \text{and} \quad AOD(24; 2, 2, 2, 18; 2, 2, 2, 18),$$

and consequently, we find an infinite class of full amicable orthogonal designs:

$$AOD\left(2^n; 2_{(3)}^{n-3}, 10, 10, 5 \cdot 2^2, \dots, 5 \cdot 2^{n-4}; 2_{(3)}^{n-3}, 5 \cdot 2^{n-3}\right), \quad n > 4,$$

$$AOD\left(2^n \cdot 3; 2_{(3)}^{n-2}, 18, 18, 9 \cdot 2^2, \dots, 9 \cdot 2^{n-3}; 2_{(3)}^{n-2}, 9 \cdot 2^{n-2}\right), \quad n > 3.$$

Conjecture 1.3 (see [29]). *There is a full (non-zero entries) $OD(2^{2^{n+1}-1}; a, \dots, a)$ in 2^{n+2} variables for each $n \geq 1$.*

Only case $n = 1$ of this conjecture is known, i.e, $OD(8; 1_{(8)})$. In the last section of Chapter 4, using a slightly different method from [29], we show that there exist full amicable orthogonal designs in 16 variables of order 2^9 , and so an $OD(2^{10}; 2_{(16)}^6)$.

The following general construction method is shown in [13, 15].

Theorem 1.4. *Suppose that r and n are positive integers, b_1, b_2, \dots, b_ℓ are powers of 2, and there is an orthogonal design of type $(b_1, b_2, \dots, b_\ell)$ and order $2^r n$. If s_1, s_2, \dots, s_u are positive integers with sum $2^d(b_1 + b_2 + \dots + b_\ell)$ for some $d \geq 0$, then there is an integer N such that for each $a \geq N$, there is an*

$$OD(2^{a+d+r}n; 2^a s_1, 2^a s_2, \dots, 2^a s_u).$$

In Chapter 5, we prove the above theorem without requiring the existence of an orthogonal design of type $(b_1, b_2, \dots, b_\ell)$ and order $2^r n$.

In Proposition 5.2, we show that for any given sequence of positive integers $(b, a_1, a_2, \dots, a_k)$, there exists a full COD of type $(2^m \cdot 1_{(b)}, 2^m \cdot 2_{(4)}^{a_1}, \dots, 2^m \cdot 2_{(4)}^{a_k})$, where $m = 4k + b + 2$ if b is even, and $m = 4k + b + 1$ if b is odd.

In Theorem 5.7, we prove that for any ℓ -tuple (s_1, \dots, s_ℓ) of positive integers,

there is an integer $N = N(s_1, \dots, s_\ell)$ such that for each $n \geq N$, there is an

$$OD\left(2^n(s_1 + \dots + s_\ell); 2^n s_1, \dots, 2^n s_\ell\right).$$

In Theorem 5.11, we also show that for any s -tuple (u_1, u_2, \dots, u_s) and any t -tuple (v_1, v_2, \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 $n \geq N$.

Robert Craigen introduced and studied signed group Hadamard matrices extensively in [5, 8]. Ivan Livinskyi [38], following Craigen's lead, studied and provided a better estimate for the asymptotic existence of signed group Hadamard matrices and consequently improved the asymptotic existence of Hadamard matrices.

In Chapter 6, in order to improve these results, we introduce and study signed group orthogonal designs. The main results include a method for finding signed group orthogonal designs for any k -tuple of positive integers, and then an application to obtain orthogonal designs from signed group orthogonal designs. Therefore, we show that for any k -tuple (u_1, \dots, u_k) of positive integers, there is a circulant quasisymmetric signed group orthogonal design of order $4(u_1 + \dots + u_k)$ and type $(4u_1, \dots, 4u_k)$ for some signed group S that admits a remrep of degree 2^n , where $n \leq \frac{3}{13} \sum_{i=1}^k \log(u_i) + 8k + 2$ or $n \leq \frac{1}{5} \sum_{i=1}^k \log(u_i) + 10k + 2$. Then we use Theorem 6.26 which describes a method to obtain orthogonal designs from signed group orthogonal designs to find some other bounds for the asymptotic existence of orthogonal designs, namely, for any k -tuple (u_1, \dots, u_k) of positive integers, there is an integer N such that for each $n \geq N$, there is a full OD of type

$(2^n u_1, \dots, 2^n u_k)$, where $n \leq \frac{3}{13} \sum_{i=1}^k \log(u_i) + 8k + 4$ or $n \leq \frac{1}{5} \sum_{i=1}^k \log(u_i) + 10k + 4$ (see Definitions 6.1, 6.3, 6.4, 6.5 and 6.8 for more details).

In the last section of Chapter 6, we show that for each $n > 2$, there is a signed group orthogonal design of order 2^n and type $(1_{(2^n)})$, and then in Theorem 6.49, we show that if r is a Golay number and $k_1, k_2, \dots, k_{2^{n-3}-1}$ are complex Golay numbers, $n > 2$, then there is a complex orthogonal design of order $2^q m$ and type $(2^q, 2^q r, 2^{q+1} k_1, \dots, 2^{q+1} k_{2^{n-3}-1})$, where $m = 2 \sum_{j=1}^{2^{n-3}-1} k_j + r + 1$ and $q = 2^{n-1} + n - 1$.

Chapter 2

Preliminaries

The definitions, theorems and statements of this chapter can be all found in [18, 43, 53].

2.1 Weighing matrices

Definition 2.1. A *Hadamard matrix* of order n is a square matrix H of order n with entries from $\{\pm 1\}$ such that $HH^t = nI_n$, where H^t is the transpose of H , and I_n is the identity matrix of order n .

A *weighing matrix* of weight k and order n , denoted $W(n, k)$, is a square matrix W of order n with entries from $\{0, \pm 1\}$ such that $WW^t = kI_n$.

Remark 2.2. If $n = k$, then a $W(n, n)$ is literally a Hadamard matrix.

Proposition 2.3 ([18]). *If there exists a $W(n, k)$ for some odd n , then k must be an integer square.*

Proof. Suppose that n is an odd number and W is a $W(n, k)$. We have $WW^t = kI_n$, therefore $\det(W)^2 = k^n$. Since n is odd, we conclude that k must be an integer square. □

The following two lemmas are well known from linear algebra [36].

Lemma 2.4. *The eigenvalues of a symmetric matrix with real entries are real.*

Proof. Let A be a symmetric matrix and λ be an eigenvalue of A . Then there is a nonzero vector x such that $Ax = \lambda x$. We have

$$\begin{aligned}\bar{\lambda}x^* &= (\lambda x)^* &= (Ax)^* \\ &= x^*A^* \\ &= x^*A.\end{aligned}$$

The last equality holds because A is symmetric and has real entries. Therefore, $\bar{\lambda}x^*x = x^*Ax = \lambda x^*x$. Hence $\bar{\lambda}\|x\|^2 = \lambda\|x\|^2$. Since $x \neq 0$, $\lambda = \bar{\lambda}$. Thus, λ is real. \square

Lemma 2.5. *The eigenvalues of a skew-symmetric matrix with real entries are of the form $\pm ib$, where b is a real number.*

Proof. Suppose that B is a skew-symmetric matrix with eigenvalue λ . Then there is a nonzero vector x such that $Bx = \lambda x$. We have

$$\begin{aligned}\bar{\lambda}x^* &= (\lambda x)^* &= (Bx)^* \\ &= x^*B^* \\ &= -x^*B.\end{aligned}$$

The last equality follows from the fact that B is skew-symmetric with real entries. So, $\bar{\lambda}x^*x = -x^*Bx = -\lambda x^*x$. Since $x \neq 0$, $\lambda + \bar{\lambda} = 0$. Therefore, $\lambda = ib$, for some real number b . \square

Lemma 2.6 ([18]). *The absolute values of the eigenvalues of a weighing matrix $W(n, k)$ are \sqrt{k} .*

Proof. Let λ be an eigenvalue of $W = W(n, k)$. So, $Wx = \lambda x$ for some $x \neq 0$. Thus,

$$\bar{\lambda}x^* = (\lambda x)^* = (Wx)^* = x^*W^t.$$

Multiplying W from the left to the above equality and using $W^tW = kI_n$, one concludes $\bar{\lambda}x^*W = kx^*$ and so $\bar{\lambda}x^*Wx = kx^*x$. Hence, $\bar{\lambda}\lambda x^*x = kx^*x$. Since $x \neq 0$, $k = |\lambda|^2$. Therefore, $|\lambda| = \sqrt{k}$. \square

2.2 Orthogonal designs

Definition 2.7. A *complex orthogonal design* (COD) of order n and type (s_1, \dots, s_ℓ) , denoted $COD(n; s_1, \dots, s_\ell)$, is a matrix X with entries from $\{0, \epsilon_1 x_1, \dots, \epsilon_\ell x_\ell\}$, where the x_j 's are commuting variables and $\epsilon_j \in \{\pm 1, \pm i\}$ for each j , that satisfies

$$XX^* = \left(\sum_{j=1}^{\ell} s_j x_j^2 \right) I_n,$$

where X^* denotes the conjugate transpose of X and I_n is the identity matrix of order n . A complex orthogonal design in which $\epsilon_j \in \{\pm 1\}$ for all j is called an *orthogonal design* (OD), denoted $OD(n; s_1, \dots, s_\ell)$. An orthogonal design in which there is no zero entry is called a *full* OD.

The domain of variables in this work are taken in \mathbb{R} , and they are assumed to be commuting.

Example 2.8. It can be seen that the following matrices are $OD(4; 1, 1, 1, 1)$ and $COD(6; 1, 5)$, respectively,

$$\begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ -x_2 & x_1 & x_4 & -x_3 \\ -x_3 & -x_4 & x_1 & x_2 \\ -x_4 & x_3 & -x_2 & x_1 \end{bmatrix}, \quad \begin{bmatrix} ix_1 & x_2 & x_2 & x_2 & x_2 & x_2 \\ x_2 & ix_1 & x_2 & -x_2 & -x_2 & x_2 \\ x_2 & x_2 & ix_1 & x_2 & -x_2 & -x_2 \\ x_2 & -x_2 & x_2 & ix_1 & x_2 & -x_2 \\ x_2 & -x_2 & -x_2 & x_2 & ix_1 & x_2 \\ x_2 & x_2 & -x_2 & -x_2 & x_2 & ix_1 \end{bmatrix}.$$

Remark 2.9. Equating all variables to 1 in any full OD results in a Hadamard matrix.

Equating all variables to 1 in any OD of order n results a weighing matrix $W(n, k)$, where k is the number of nonzero entries in each row (column) of the weighing matrix.

Definition 2.10. The *Hadamard product* of two $m \times n$ matrices $A = [a_{ij}]$ and $B = [b_{ij}]$, denoted $A * B$, is an $m \times n$ matrix computed via entrywise multiplication of A and B , i.e, $A * B = [a_{ij}b_{ij}]$. A and B are called *disjoint* if $A * B = 0$. Pairwise disjoint matrices such that their sum has no zero entries are called *supplementary*.

Proposition 2.11 ([18]). *A necessary and sufficient condition that there exists an OD($n; u_1, \dots, u_k$) is that there exists a family $\{A_1, \dots, A_k\}$ of pairwise disjoint square matrices of order n with entries from $\{0, \pm 1\}$ satisfying*

- (i) A_i is a $W(n, u_i)$, $1 \leq i \leq k$,
- (ii) $A_i A_j^t = -A_j A_i^t$, $1 \leq i \neq j \leq k$.

Definition 2.12 ([18]). *A rational family of order n and type (s_1, \dots, s_k) , where the s_i 's are positive rational numbers, is a collection of k rational matrices of order n , A_1, \dots, A_k , satisfying*

- (i) $A_i A_i^t = s_i I_n$, $1 \leq i \leq k$,

$$(ii) A_i A_j^t = -A_j A_i^t, \quad 1 \leq i \neq j \leq k.$$

Theorem 2.13 ([18, 40]). *The maximum number of variables in an orthogonal design of order $n = 2^a b$, b odd, is $\rho(n) = 8c + 2^d$, where $a = 4c + d$, $0 \leq d < 4$. $\rho(n)$ is called Radon's number.*

Example 2.14. The maximum number of variables in orthogonal designs of order 2, 4, 8, 16, 32, 64, and 128 are 2, 4, 8, 9, 10, 12, and 16, respectively.

Definition 2.15. The *Kronecker product* of two matrices $A = [a_{ij}]$ and B of orders $m \times n$ and $r \times s$, respectively, is denoted by $A \otimes B$, and it is the matrix of order $mr \times ns$ defined by

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & & & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}.$$

The *direct sum* of A and B is denoted by $A \oplus B$, and it is the matrix of order $(m + r) \times (n + s)$ which is defined as follows

$$A \oplus B = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix},$$

where 0 represents a zero matrix of appropriate size.

Lemma 2.16 ([36]). *Suppose that A, B, C, D and L are matrices of orders $m \times n$, $r \times s$, $n \times p$, $s \times t$ and $\alpha \times \beta$, respectively. Then*

- (i) $(A + B) \otimes L = A \otimes L + B \otimes L$ if $(m, n) = (r, s)$,
- (ii) $(A \otimes B)(C \otimes D) = AC \otimes BD$ of order $mr \times pt$,
- (iii) $(A \otimes B)^t = A^t \otimes B^t$,

$$(iv) (A \oplus B)^t = A^t \oplus B^t.$$

2.3 Type 1 and type 2 matrices

Definition 2.17 ([18]). Suppose that G is an additive abelian group of order n , with elements ordered g_1, \dots, g_n . Let ψ and φ be two functions from G to a commutative ring. The square matrices $C = [c_{ij}]$ and $B = [b_{ij}]$ of order n are called *type 1* and *type 2* matrices, respectively, if $c_{ij} = \psi(g_j - g_i)$ and $b_{ij} = \varphi(g_i + g_j)$.

Example 2.18. Consider $G = \mathbb{Z}/7\mathbb{Z}$ with elements

$$g_0 = 0, g_1 = 1, g_2 = 2, g_3 = 3, g_4 = 4, g_5 = 5, g_6 = 6.$$

Let ψ and φ be the inclusion maps from G to the commutative ring $\mathbb{Z}/7\mathbb{Z}$.

If $c_{ij} = g_j - g_i$ and $b_{ij} = g_j + g_i$ reduced modulus 7, $0 \leq i, j \leq 6$, then the matrix $C = [c_{ij}]$ is a type 1 matrix, and the matrix $B = [b_{ij}]$ is a type 2 matrix displayed as follows:

$$C = \begin{matrix} & \begin{matrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{matrix} \\ \begin{matrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{matrix} & \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 \\ 5 & 6 & 0 & 1 & 2 & 3 & 4 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \end{pmatrix} \end{matrix} \quad \text{and} \quad B = \begin{matrix} & \begin{matrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{matrix} \\ \begin{matrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{matrix} & \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 \\ 5 & 6 & 0 & 1 & 2 & 3 & 4 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} \end{matrix}. \quad (2.1)$$

Definition 2.19 ([1]). Suppose that q is an odd prime power. The *quadratic character*

of $GF(q)$ (the Galois field of order q) is defined by

$$\chi(x) = \begin{cases} 0 & \text{if } x = 0, \\ 1 & \text{if } x \text{ is a quadratic residue,} \\ -1 & \text{otherwise.} \end{cases}$$

It is well known that χ is a multiplicative function and $\chi(-1) = (-1)^{(q-1)/2}$ (see [49]). Consider g_1, \dots, g_q are the ordered elements of $GF(q)$. Then the square matrix $Q = [q_{ij}]$ of order q defined by $q_{ij} = \chi(g_j - g_i)$ is a type 1 matrix, and it is called the *Jacobsthal* matrix [1].

Theorem 2.20 ([18]). *Suppose Q is a Jacobsthal matrix as in Definition 2.19. Then*

- (i) $QJ = JQ = 0$,
- (ii) $Q^t = (-1)^{(q-1)/2}Q$,
- (iii) $QQ^t = qI - J$.

Proof. It is well known (see [49]) that half of the non-zero elements of $GF(q)$ are quadratic residues or squares and half of them are quadratic non-residues or non-squares, thus (i) follows. Since

$$q_{ji} = \chi(g_i - g_j) = \chi(-1)\chi(g_j - g_i) = (-1)^{(q-1)/2}q_{ij},$$

one has $Q^t = (-1)^{(q-1)/2}Q$. To see the last part, one observes that, for each $b \neq 0$,

$$\begin{aligned} \sum_{a \in GF(q)} \chi(a)\chi(a+b) &= \sum_{\substack{a \in GF(q) \\ a \neq 0}} \chi(1+ba^{-1}) \\ &= \sum_{\substack{a \in GF(q) \\ a \neq 1}} \chi(a) = \sum_{a \in GF(q)} \chi(a) - \chi(1) = -1. \end{aligned}$$

□

Corollary 2.21 (Paley [18]). *Suppose that e is the $1 \times q$ vector of all ones and let*

$$W = \begin{bmatrix} 0 & e \\ (-1)^{(q-1)/2} e^t & Q \end{bmatrix}.$$

If $q \equiv 3 \pmod{4}$, then $W + I_{q+1}$ forms a Hadamard matrix of order $q + 1$, and if $q \equiv 1 \pmod{4}$, then

$$\begin{bmatrix} W + I_{q+1} & W - I_{q+1} \\ W - I_{q+1} & -W - I_{q+1} \end{bmatrix}$$

forms a Hadamard matrix of order $2(q + 1)$.

Example 2.22. Consider $GF(7)$. It can be seen that 1, 2 and 4 are square in $GF(7)$. Replacing these numbers by 1 and the numbers 3, 5, 6 by -1 (denoted by $-$) in the matrix C , (2.1), one gets the following matrix.

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

From Corollary 2.21, since $7 \equiv 3 \pmod{4}$, $W + I_8$ gives the following Hadamard matrix of order 8.

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

Lemma 2.23 ([18]). *Suppose that G is an additive abelian group of order n with elements ordered g_1, \dots, g_n . Let ϕ, ψ and φ be functions from G to some commutative ring R . Define $n \times n$ matrices $A = [a_{ij}]$, $C = [c_{ij}]$ and $B = [b_{ij}]$ by $a_{ij} = \phi(g_j - g_i)$, $c_{ij} = \psi(g_j - g_i)$ and $b_{ij} = \varphi(g_j + g_i)$, respectively. Then*

- (i) $B^t = B$,
- (ii) $AC = CA$,
- (iii) $CB^t = BC^t$.

Proof. Part (i) is trivial because $b_{ij} = \varphi(g_j + g_i) = \varphi(g_i + g_j) = b_{ji}$. To see part (ii) one observes that

$$\begin{aligned} (AC)_{ij} &= \sum_{t \in G} \phi(t - g_i) \psi(g_j - t) \\ &= \sum_{h \in G} \phi(g_j - h) \psi(h - g_i) && \text{(putting } h = g_i + g_j - t) \\ &= \sum_{h \in G} \psi(h - g_i) \phi(g_j - h) && \text{(because } R \text{ is commutative)} \\ &= (CA)_{ij}. \end{aligned}$$

Finally, for part (iii),

$$\begin{aligned}
(CB^t)_{ij} &= \sum_{t \in G} \psi(t - g_i) \varphi(g_j + t) \\
&= \sum_{h \in G} \psi(h - g_j) \varphi(g_i + h) && \text{(putting } h = g_j + t - g_i) \\
&= \sum_{h \in G} \varphi(g_i + h) \psi(h - g_j) && \text{(because } R \text{ is commutative)} \\
&= (BC^t)_{ij}.
\end{aligned}$$

□

Definition 2.24. Let $A = (a_1, \dots, a_n)$. The square matrix $C = [c_{ij}]$ of order n is called *circulant* if $c_{ij} = a_{j-i+1}$, denoted $\text{circ}(a_1, \dots, a_n)$, where $j-i$ is reduced modulo n .

The square matrix $B = [b_{ij}]$ of order n is called *back-circulant* if $b_{ij} = a_{i+j-1}$, denoted $\text{backcirc}(a_1, \dots, a_n)$, where $i+j-2$ is reduced modulo n .

Remark 2.25. (i) Any type 1 matrix defined on $\mathbb{Z}/n\mathbb{Z}$ (with its standard ordering) is circulant because

$$c_{ij} = \psi(j - i) = \psi(j - i + 1 - 1) = c_{1, j-i+1}.$$

(ii) Any type 2 matrix defined on $\mathbb{Z}/n\mathbb{Z}$ (with its standard ordering) is back-circulant because

$$b_{ij} = \varphi(i + j) = \varphi(i + j - 1 + 1) = b_{1, i+j-1}.$$

Using the properties of type 1 and type 2 matrices in Lemma 2.23 combined with Remark 2.25, one has the following.

Corollary 2.26 ([18]). *Suppose that A and C are circulant matrices of order n and B is a back-circulant matrix of order n . Then*

- (i) $B = B^t$,
- (ii) $AC = CA$,
- (iii) $BC^t = CB^t$.

Definition 2.27. A set Ω of commuting matrices with $AB^t = B^tA$ for all $A, B \in \Omega$ is called a set of *near type 1* matrices [23].

Example 2.28. The set of order one matrices in a single variable, and the set of order two circulant or negacirculant matrices in two variables, $\begin{bmatrix} x & y \\ -y & x \end{bmatrix}$, are sets of near type 1 matrices.

2.4 Autocorrelation functions

Definition 2.29 ([18]). The *non-periodic autocorrelation function* of a $(0, \pm 1, \pm i)$ -sequence $A = (a_1, \dots, a_n)$ is defined by

$$N_A(j) := \begin{cases} \sum_{i=1}^{n-j} a_{i+j} \bar{a}_i & \text{if } j = 0, 1, 2, \dots, n-1 \\ 0 & j \geq n \end{cases}$$

where \bar{a}_i denotes the complex conjugate of a_i .

A set $\{A_1, A_2, \dots, A_\ell\}$ of $(0, \pm 1, \pm i)$ -sequences (not necessarily of the same length) is said to have *zero autocorrelation* with weight w if

$$N_{A_1}(j) + N_{A_2}(j) + \dots + N_{A_\ell}(j)$$

is zero for all $j > 0$, and is w for $j = 0$. Sequences having zero autocorrelation are called *complementary*.

Example 2.30. Let $A = (1, 1, -)$ and $B = (1, i, 1)$. Then $N_A(0) = N_B(0) = 3$, $N_A(1) = N_B(1) = 0$, $N_A(2) = -1$ and $N_B(2) = 1$. Thus, A and B are complementary with weight 6.

Definition 2.31 ([18]). For $j = 0, 1, 2, \dots, n-1$, the *periodic autocorrelation function* of a $(0, \pm 1, \pm i)$ -sequence $A = (a_1, \dots, a_n)$ is defined by

$$P_A(j) := \sum_{i=1}^n a_{i+j} \bar{a}_i,$$

where $i + j - 1$ is reduced modulo n .

Lemma 2.32 ([18]). Let $A = (a_1, a_2, \dots, a_n)$ be a $(0, \pm 1, \pm i)$ -sequence. Then for all $j = 0, 1, \dots, n-1$,

$$P_A(j) = N_A(j) + N_{A_R}(n-j),$$

where $A_R = (a_n, \dots, a_2, a_1)$, the reverse of sequence A .

Remark 2.33. Lemma 2.32 implies that $(0, \pm 1, \pm i)$ -sequences of the same length with zero autocorrelation have also zero periodic autocorrelation. But the reverse is not true. As an example, the sequences $A = (1, i)$ and $B = (1, i)$ have zero periodic autocorrelation; however, they do not have zero autocorrelation as

$$N_A(1) + N_B(1) = i + i = 2i \neq 0.$$

Definition 2.34 ([18]). Let $A = (x_1, \dots, x_n)$ be a sequence of commuting variables. Then the *non-periodic autocorrelation function* of A is defined by

$$N_A(j) := \begin{cases} \sum_{i=1}^{n-j} x_{i+j} x_i & \text{if } j = 0, 1, 2, \dots, n-1 \\ 0 & j \geq n \end{cases}$$

A set $\{A_1, A_2, \dots, A_\ell\}$ of sequences involving commuting variables (not necessarily of the same length) is said to have *zero autocorrelation* with weight w if

$$N_{A_1}(j) + N_{A_2}(j) + \dots + N_{A_\ell}(j)$$

is zero for all $j > 0$, and is w for $j = 0$. Sequences involving commuting variables that have zero autocorrelation are also called *complementary*.

Definition 2.35. Two complementary (± 1) -sequences are called *Golay sequences*.

Two complementary $(\pm x, \pm y)$ -sequences of length ℓ are called a *Golay pair* of length ℓ in two variables x and y .

Example 2.36. The sequences $A_1 = (x, y)$ and $B_1 = (x, -y)$ form a Golay pair of length 2 in two variables x and y . We will use the Golay pair $(A_1; B_1)$ in Chapter 5, Lemma 5.1.

The sequences $A_2 = (x, y)$ and $B_2 = (y, -x)$ form a Golay pair of length 2 in two variables x and y . We will use the Golay pair $(A_2; B_2)$ in Chapter 6, Lemma 6.6.

Definition 2.37. A square matrix C is called *Hermitian* if $C = C^*$, where C^* is the conjugate transpose of C .

2.5 Amicable and anti-amicable matrices

Definition 2.38 ([18]). Two real matrices A and B are called *amicable* if $AB^t = BA^t$.

They are called *anti-amicable* if $AB^t = -BA^t$.

Two complex matrices C and D are called *complex amicable* if $CD^* = DC^*$.

They are called *complex anti-amicable* if $CD^* = -DC^*$.

Let M be an $OD(n; c_1, \dots, c_k)$ on variables x_1, \dots, x_k , and N be an $OD(n; d_1, \dots, d_m)$ on variables y_1, \dots, y_m , where the two sets of variables are disjoint. Then $(M; N)$ is

called an *amicable orthogonal design*, denoted

$$AOD(n; c_1, \dots, c_k; d_1, \dots, d_m),$$

if $MN^t = NM^t$. $(M; N)$ is called *anti-amicable* if $MN^t = -NM^t$.

Let X be a $COD(n; c_1, \dots, c_k)$ on variables x_1, \dots, x_k , and Y be a $COD(n; d_1, \dots, d_m)$ on variables y_1, \dots, y_m , where the two sets of variables are disjoint. Then $(X; Y)$ is called a *complex amicable orthogonal design*, denoted

$$ACOD(n; c_1, \dots, c_k; d_1, \dots, d_m),$$

if $XY^* = YX^*$.

Example 2.39. Let $P := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $Q := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $R := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, and I be the identity matrix of order 2. Then

$$PQ^t = -QP^t, RI^t = -IR^t, PR^t = RP^t, PI^t = IP^t, QI^t = IQ^t, RQ^t = QR^t.$$

Throughout this work P, Q, R and I are these 2 by 2 matrices.

Example 2.40. It can be seen that the matrices $\begin{bmatrix} a & b \\ b & -a \end{bmatrix}$ and $\begin{bmatrix} c & d \\ -d & c \end{bmatrix}$ form an $AOD(2; 1, 1; 1, 1)$, and the following matrices form an $AOD(4; 1, 1, 2; 1, 1, 2)$,

$$\begin{bmatrix} a & b & c & c \\ -b & a & c & -c \\ c & c & -a & -b \\ c & -c & b & -a \end{bmatrix}, \quad \begin{bmatrix} e & f & g & g \\ f & -e & g & -g \\ -g & -g & f & e \\ -g & g & e & -f \end{bmatrix}.$$

Theorem 2.41 (W. Wolfe [53]). *If $(A; B)$ is an amicable orthogonal design in order $n = 2^a b$, b odd, then the total number of variables in A and B is less than or equal to $2a + 2$, and this bound is achieved for all values of n .*

Theorem 2.42 (see [18]). *For each positive integer n , there is a set*

$$A = \left\{ I_n, A_1, A_2, \dots, A_{\rho(n)-1} \right\}$$

of pairwise disjoint anti-amicable signed permutation matrices of order n , and equivalently there is an $OD(n; 1_{(\rho(n))})$, where $\rho(n)$ is Radon's number.

Theorem 2.43 (W. Wolfe [53]). *Given an integer $n = 2^s d$, where d is odd and $s \geq 1$, there exist 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 anti-amicable, mutually disjoint matrices,*
- (ii) *B consists of pairwise anti-amicable, mutually disjoint matrices,*
- (iii) *for each i and j , A_i and B_j are amicable.*

Proof. For each k , $2 \leq k \leq s + 1$, let

$$A_1 = \left(\otimes_{i=1}^s I \right) \otimes I_d, \quad A_k = \left(\otimes_{i=1}^{k-2} I \right) \otimes R \otimes \left(\otimes_{i=k}^s P \right) \otimes I_d,$$

and

$$B_1 = \left(\otimes_{i=1}^s P \right) \otimes I_d, \quad B_k = \left(\otimes_{i=1}^{k-2} I \right) \otimes Q \otimes \left(\otimes_{i=k}^s P \right) \otimes I_d,$$

where P, Q, R, I are the same 2 by 2 matrices as in Example 2.39, and I_d is the identity matrix of order d . Then the matrices A_i and B_i ($1 \leq i \leq s + 1$) satisfy the three properties (i), (ii) and (iii). □

2.6 Product designs

Definition 2.44 (P. Robinson [43]). Let M_1 be an $OD(n; a_1, \dots, a_r)$ on variables x_1, \dots, x_r , M_2 be an $OD(n; b_1, \dots, b_s)$ on variables y_1, \dots, y_s , and N be an $OD(n; c_1, \dots, c_t)$ on variables z_1, \dots, z_t , where the three sets of variables are disjoint. Then $(M_1; M_2; N)$ is called a *product design* of type $(a_1, \dots, a_r; b_1, \dots, b_s; c_1, \dots, c_t)$ and order n if the following conditions hold:

- (i) $M_1 * N = M_2 * N = 0$,
- (ii) $M_1 + N$ and $M_2 + N$ are orthogonal designs, and
- (iii) $M_1 M_2^t = M_2 M_1^t$.

We denote this product design by $PD(n; a_1, \dots, a_r; b_1, \dots, b_s; c_1, \dots, c_t)$.

Example 2.45. It can be verified that $(M_1; M_2; N)$ is a $PD(4; 1, 1, 1; 1, 1, 1; 1)$, where

$$M_1 = \begin{bmatrix} 0 & b & c & d \\ -b & 0 & d & -c \\ -c & -d & 0 & b \\ -d & c & -b & 0 \end{bmatrix}, M_2 = \begin{bmatrix} 0 & e & f & g \\ -e & 0 & -g & f \\ -f & g & 0 & -e \\ -g & -f & e & 0 \end{bmatrix} \text{ and } N = \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & a \end{bmatrix}.$$

The following theorem of Peter Robinson [43] shows how to construct orthogonal designs by combining amicable orthogonal designs and product designs.

Theorem 2.46 (P. Robinson [43]). *Suppose that $(S; yR + P)$ is an*

$$AOD(m; u_1, \dots, u_j; v, w_1, \dots, w_k),$$

where R is a $W(m, v)$ and P is an $OD(m; w_1, \dots, w_k)$. Let $(M_1; M_2; N)$ be a $PD(n; a_1, \dots, a_r; b_1, \dots, b_s; c_1, \dots, c_t)$. Also, let b, c, u, w be the sums of the b_i 's, c_i 's, u_i 's and w_i 's, respectively. Then there are

- (i) $OD(mn; va_1, \dots, va_r, wb_1, \dots, wb_s, uc_1, \dots, uc_t),$
- (ii) $OD(mn; va_1, \dots, va_r, wb_1, \dots, wb_s, u_1c, \dots, u_jc),$
- (iii) $OD(mn; va_1, \dots, va_r, w_1b, \dots, w_kb, uc_1, \dots, uc_t),$
- (iv) $OD(mn; va_1, \dots, va_r, w_1b, \dots, w_kb, u_1c, \dots, u_jc).$

Chapter 3

Asymptotic existence of weighing matrices

Peter Eades in his Ph.D. thesis showed some existence results for weighing matrices. He showed that when the order of orthogonal designs and weighing matrices are *much larger* than the number of nonzero entries in each row, the necessary conditions for existence of orthogonal designs and weighing matrices are also sufficient. In this chapter, we show some non-existence results on weighing matrices and some asymptotic results for existence of weighing matrices. Our main references in this chapter are [13] and [18].

3.1 Non-existence results for weighing matrices

Theorem 3.1 ([5]). *There does not exist any symmetric weighing matrix with zero diagonal of odd order.*

Proof. Suppose that $W = W(n, k)$, n odd, is a symmetric weighing matrix with zero diagonal. From Linear Algebra, $\text{tr}(W) = \sum_{t=1}^n \lambda_t$, where λ_t 's are eigenvalues of W . By

Lemma 2.4 and 2.6, since $\lambda_t = \pm\sqrt{k}$,

$$\text{tr}(W) = \sum_{t=1}^n \lambda_t = c\sqrt{k}.$$

Since n is odd, c must be odd and therefore nonzero, but, by assumption, $\text{tr}(W) = 0$, which is a contradiction. □

Theorem 3.2 ([5]). *There is no skew-symmetric weighing matrix of odd order.*

Proof. Assume that $W = W(n, k)$ is a skew-symmetric weighing matrix of odd order. From Lemma 2.5 and 2.6, eigenvalues of W are in form $\pm i\sqrt{k}$. Therefore,

$$\text{tr}(W) = \sum_{t=1}^n \lambda_t = ci\sqrt{k}.$$

Since n is odd, c must be odd and so nonzero, but since W is skew-symmetric, $\text{tr}(W) = 0$ which is a contradiction. □

Next, we show that if n is any odd number and k cannot be written as the sum of three integer squares, then there is no skew-symmetric weighing matrix $W(4n, k)$. The following well known results, due to Gauss, are taken from [44].

Theorem 3.3 ([44]). *A positive integer can be written as the sum of three integer squares if and only if it is not of the form $4^\ell(8k + 7)$, where $\ell, k \geq 0$.*

Lemma 3.4 ([44]). *A positive integer is the sum of three rational squares if and only if it is the sum of three integer squares.*

Proof. Suppose that a positive integer n is the sum of three rational squares. Reducing the three rational numbers to the same denominator, one may write

$$m^2n = \alpha^2 + \beta^2 + \gamma^2,$$

where α, β and γ are integers. Suppose that n cannot be written as the sum of three integer squares. From Theorem 3.3, there exist nonnegative integers k, ℓ such that $n = 4^\ell(8k + 7)$. One may write m as $2^r(2s + 1)$, for some nonnegative integers r, s . Thus, $m^2 = 4^r(4(s^2 + s) + 1) = 4^r(8b + 1)$, where $b = \frac{s^2 + s}{2}$ is a nonnegative integer, and so

$$m^2n = 4^{r+\ell}(8k + 7)(8b + 1) = 4^{r+\ell}(8c + 7),$$

where $c = 8kb + k + 7b$. This is a contradiction because by Theorem 3.3, m^2n cannot be written as the sum of three integer squares, whereas by assumption $m^2n = \alpha^2 + \beta^2 + \gamma^2$. Therefore, the result follows. \square

Theorem 3.5 (D. Shapiro [45]). *There is a rational family in order $n = 2^m t$, t odd, of type (s_1, \dots, s_k) if and only if there is a rational family of the same type in order 2^m .*

Lemma 3.6 (Geramita-Wallis [18]). *A necessary and sufficient condition that there be a rational family of type $[1, k]$ in order 4 is that k be a sum of three rational squares.*

Proof. Suppose that $\{A, B\}$ is a rational family of type $[1, k]$ in order 4. Then $\{I = A^t A, D = A^t B\}$ is also a rational family of the same type and order. Thus $D = -D^t$ and $DD^t = kI$. Since D is skew-symmetric, the diagonal of D is zero, so k is a sum of three rational squares.

Now let $k = a^2 + b^2 + c^2$, where a, b and c are rational numbers. If we let

$$D = \begin{bmatrix} 0 & a & b & c \\ -a & 0 & -c & b \\ -b & c & 0 & -a \\ -c & -b & a & 0 \end{bmatrix},$$

then $\{I, D\}$ is a rational family of type $[1, k]$ and order 4. \square

We use Lemmas 3.6 and 3.4 and Theorem 3.5 to prove the following nonexistence result.

Theorem 3.7. *Suppose that positive integer k cannot be written as the sum of three integer squares. Then there does not exist a skew-symmetric $W(4n, k)$, for any odd number n .*

Proof. If there is a skew-symmetric $W = W(4n, k)$ for some odd number n , then $\{I_{4n}, W\}$ is a rational family of type $[1, k]$ and order $4n$. Thus, by Theorem 3.5, there is a rational family of type $[1, k]$ and order 4. Lemmas 3.4 and 3.6 imply that k must be the sum of three integer squares. □

3.2 Asymptotic existence of weighing matrices

The following lemma, due to Sylvester, is known [46].

Lemma 3.8. *Let x and y be two relatively prime positive integers. Then every integer $N \geq xy$ can be written in the form $ax + by$, where a and b are nonnegative integers.*

Proof. Let N be an integer greater than or equal to xy . Since x and y are relatively prime, there are integers c and d such that $cx + dy = N$ (see [44]). So,

$$(c + jy)x + (d - jx)y = N,$$

where $j \in \mathbb{Z}$. One can choose j such that $0 \leq c + jy \leq y - 1$. For such j , we let $a = c + jy$ and $b = d - jx$. The condition $N \geq xy$ implies that b must be positive. □

The following lemma shows how to construct orthogonal designs of higher orders by using two orthogonal designs of the same types but different orders.

Lemma 3.9 ([18]). *Suppose that there are $OD(n_1; u_1, \dots, u_m)$ and $OD(n_2; u_1, \dots, u_m)$. Let $h = \gcd(n_1, n_2)$. Then there is an integer N such that for each $t \geq N$, there is an $OD(ht; u_1, \dots, u_m)$.*

Proof. Let $x = \frac{n_1}{h}$ and $y = \frac{n_2}{h}$. Then x and y are relatively prime. Let $N = xy$, and t be a positive integer $\geq N$. By Lemma 3.8, there are nonnegative integers a and b such that $t = ax + by$. Since there exist $OD(n_1; u_1, \dots, u_m)$ and $OD(n_2; u_1, \dots, u_m)$, there are families $\{A_1, \dots, A_m\}$ of order n_1 and $\{B_1, \dots, B_m\}$ of order n_2 satisfying the conditions in Proposition 2.11. We define the family

$$\{(I_a \otimes A_1 \oplus I_b \otimes B_1), \dots, (I_a \otimes A_m \oplus I_b \otimes B_m)\}$$

of order $an_1 + bn_2 = ht$. It can be seen that this family satisfies the conditions of Proposition 2.11, therefore it makes an $OD(ht; u_1, \dots, u_m)$. \square

Corollary 3.10. *If the first two OD 's in Lemma 3.9 are symmetric, then there is an integer N such that for all $t \geq N$, there is a symmetric $OD(ht; u_1, \dots, u_m)$.*

Proof. Same argument as proof of Lemma 3.9. Note that

$$((A \otimes B) \oplus (C \otimes D))^t = (A^t \otimes B^t) \oplus (C^t \otimes D^t).$$

\square

Theorem 3.11 (Seberry-Whiteman [51]). *Let q be a prime power. Then there is a circulant $W(q^2 + q + 1, q^2)$.*

Corollary 3.12 ([13, 18]). *Suppose that q is a prime power and c is any positive integer. Then there is a circulant $W(c(q^2 + q + 1), q^2)$.*

Proof. Let c be a fixed positive integer. From Theorem 3.11, we know that there exists a circulant $W(q^2 + q + 1, q^2)$. Suppose that the first row of this matrix is $(a_1, a_2, \dots, a_{q^2+q+1})$. Let

$$\phi(x) = \sum_{i=1}^{q^2+q+1} a_i x^i.$$

Thus, $\phi(\xi)\phi(\xi^{-1}) = q^2$, where ξ is a primitive root of unity and $\xi^{q^2+q+1} = 1$. For $1 \leq j \leq c(q^2 + q + 1)$ define

$$b_j := \begin{cases} a_{\lceil \frac{j}{c} \rceil} & j \equiv 1 \pmod{c} \\ 0 & \text{otherwise} \end{cases},$$

where $\lceil x \rceil$ is the smallest integer greater than or equal to x .

We show that if $W = \text{circ}(b_1, b_2, \dots, b_{c(q^2+q+1)})$, then W is a $W(c(q^2 + q + 1), q^2)$.

To see this, let

$$\psi(y) = \sum_{j=1}^{c(q^2+q+1)} b_j y^j.$$

So,

$$\psi(y) = \sum_{i=1}^{q^2+q+1} a_i y^{c(i-1)+1} = y^{1-c} \sum_{i=1}^{q^2+q+1} a_i y^{ci}.$$

Since $\phi(\xi)\phi(\xi^{-1}) = q^2$, for all ξ such that $\xi^{q^2+q+1} = 1$, $\psi(\xi)\psi(\xi^{-1}) = q^2$, for all ξ such that $\xi^{q^2+q+1} = 1$. Applying the finite Parseval relation

$$\sum_{i=1}^{c(q^2+q+1)} b_i b_{i+r} = \frac{1}{c(q^2 + q + 1)} \sum_{j=1}^{c(q^2+q+1)} |\psi(\xi^j)|^2 \xi^{jr},$$

where $i + r - 1$ is reduced modulo $c(q^2 + q + 1)$, for $r = 0$ gives

$$\sum_{i=1}^{c(q^2+q+1)} b_i^2 = \frac{1}{c(q^2 + q + 1)} (c(q^2 + q + 1)q^2) = q^2,$$

and for $1 \leq r \leq c(q^2 + q + 1) - 1$, $\sum_{i=1}^{c(q^2+q+1)} b_i b_{i+r} = 0$. Therefore, W is a circulant $W(c(q^2 + q + 1), q^2)$. \square

The next lemma shows how to make a symmetric orthogonal design to be used for Theorem 3.18.

Lemma 3.13. *Let k be a positive integer. Then there exists a symmetric $OD(2^k; 1_{(k)})$.*

Proof. Define $A_1 = \otimes_{m=1}^k P$ and for $2 \leq n \leq k$, $A_n = \otimes_{m=1}^{n-2} I \otimes Q \otimes_{m=n}^k P$, where P and Q are the same matrices as in Example 2.39. It can be directly verified that the family $\{A_1, \dots, A_k\}$ of order 2^k satisfies the conditions of Proposition 2.11, and therefore it makes a symmetric $OD(2^k; 1_{(k)})$. Note that P, Q and I are symmetric. \square

Theorem 3.14 (P. J. Robinson [43]). *All $OD(2^t; 1, 1, a, b, c)$ exist, where $a + b + c = 2^t - 2$ and $t \geq 3$.*

We prove the following well known lemma by giving a proof which is different from the proof in [18].

Lemma 3.15. *For any sequence (k_1, k_2, k_3, k_4) of positive integers, there is a positive integer d such that there is a skew-symmetric $OD(2^d; k_1, k_2, k_3, k_4)$.*

Proof. Let t_1 and t_2 be the smallest positive integers such that $1 + k_1 + k_2 \leq 2^{t_1}$ and $1 + k_3 + k_4 \leq 2^{t_2}$. By Theorem 3.14, there are $A = OD(2^{t_1}; 1, k_1, k_2)$ and $B = OD(2^{t_2}; 1, k_3, k_4)$. Without loss of generality, assume that $\{I_{2^{t_1}}, A_1, A_2\}$ and $\{I_{2^{t_2}}, B_1, B_2\}$ are two families corresponding to A and B satisfying the conditions of Proposition 2.11. It can be directly verified that the family

$$\{I_{2^{t_2}} \otimes A_1 \otimes P, I_{2^{t_2}} \otimes A_2 \otimes P, B_1 \otimes I_{2^{t_1}} \otimes Q, B_2 \otimes I_{2^{t_1}} \otimes Q\}$$

of four skew-symmetric matrices satisfies all conditions of Proposition 2.11, and so it makes a skew-symmetric $OD(2^{t_1+t_2+1}; k_1, k_2, k_3, k_4)$. \square

Corollary 3.16 ([18]). *Given any sequence (k_1, k_2, k_3, k_4) of positive integers, there exists a positive integer d such that there is an $OD(2^d; 1, k_1, k_2, k_3, k_4)$.*

The following theorem was first proved by Geramita and Wallis [18].

Theorem 3.17 (Geramita and Wallis [18]). *Suppose that k is a square. Then there is an integer $N = N(k)$ such that for each $n \geq N$, there is a $W(n, k)$.*

We use a slightly different method to the proof of Theorem 3.17 to give a proof of the following improved result.

Theorem 3.18. *Suppose that k is a square. Then there is an integer $N = N(k)$ such that for each $n \geq N$, there is a symmetric $W(n, k)$.*

Proof. Assume that $k = \prod_{i=1}^m q_i^2$, where q_i is either 1 or a prime power. By Theorem 3.11, for each i there exists a circulant $W_i = W(q_i^2 + q_i + 1, q_i^2)$. Let

$$W = \otimes_{i=1}^m W_i R.$$

It can be seen that W is a symmetric $W\left(\prod_{i=1}^m (q_i^2 + q_i + 1), \prod_{i=1}^m q_i^2\right)$.

Thus, there is an odd number $t = \prod_{i=1}^m (q_i^2 + q_i + 1)$ such that there is a symmetric $W(t, k)$. Moreover, from Lemma 3.13, there exists a symmetric $OD(2^k; 1_{(k)})$ and so a symmetric $W(2^k, k)$. Now since t is odd, $\gcd(2^k, t) = 1$. Corollary 3.10 implies that there is a positive integer $N = N(k)$ such that for each $n \geq N$, there exists a symmetric $W(n, k)$. \square

We prove the following theorem by a slightly different method to the proof that first was given by Eades [13].

Theorem 3.19. *Suppose that $k = k_1^2 + k_2^2$, where k_1 and k_2 are two nonzero integers. Then there is an integer $N = N(k)$ such that for each $n \geq N$, there is an $OD(2n; k_1^2, k_2^2)$.*

Proof. For $j = 1, 2$, let $k_j^2 = \prod_{i=1}^m q_{ij}^2$, where q_{ij} is either 1 or a prime power. For each i , $1 \leq i \leq m$, let $b_i = \text{lcm}\{q_{i1}^2 + q_{i1} + 1, q_{i2}^2 + q_{i2} + 1\}$. From Corollary 3.12, for each j , $j = 1, 2$, and each i , $1 \leq i \leq m$, there exists a circulant $W_{ij} = W(b_i, q_{ij}^2)$. It can be seen that the following $2q \times 2q$ matrix is an $OD(2q; k_1^2, k_2^2)$,

$$\begin{bmatrix} x \otimes_{i=1}^m W_{i1} R_i & y \otimes_{i=1}^m W_{i2} \\ y \otimes_{i=1}^m W_{i2} & -x \otimes_{i=1}^m W_{i1} R_i \end{bmatrix},$$

where R_i is the back diagonal matrix of order b_i , and $q = \prod_{i=1}^m b_i$ is an odd number.

From Theorem 3.14, one can choose the smallest positive integer k such that there is an $OD(2^k; k_1^2, k_2^2)$. Since $\text{gcd}(2q, 2^k) = 2$, Lemma 3.9 implies that there is an integer $N = N(k)$ such that for each $n \geq N$, there is an $OD(2n; k_1^2, k_2^2)$. \square

Using Theorem 3.19, we prove the following two corollaries given by Eades [13].

Corollary 3.20. *Suppose that k is the sum of two nonzero integer squares. Then there is an integer $N = N(k)$ such that for each $n \geq N$, there is a $W(2n, k)$.*

Proof. Let $k = k_1^2 + k_2^2$, where k_1 and k_2 are integers. From Theorem 3.19, there is an integer $N = N(k)$ such that for any $n \geq N$, there is an $OD(2n; k_1^2, k_2^2)$, and so a $W(2n, k)$. \square

Corollary 3.21. *Suppose that d is an integer square. Then there exists an integer $N = N(d)$ such that for each $n \geq N$, there is a skew-symmetric $W(2n, d)$.*

Proof. Suppose that $d = a^2$. Let $k_1 = 1$ and $k_2 = a$. By Theorem 3.19, there exists an integer $N = N(d)$ such that for each $n \geq N$, there is an $OD(2n; 1, d)$, and so a skew-symmetric $W(2n, d)$. \square

We Use a different method to show Theorem 3.22 and consequently Corollaries 3.24, 3.25 and 3.26 first proven by Eades [13].

Theorem 3.22. *Suppose that $k = k_1^2 + k_2^2 + k_3^2 + k_4^2$, where k_1, k_2, k_3 and k_4 are nonzero integers. Then there is an integer $N = N(k)$ such that for each $n \geq N$, there is an $OD(4n; k_1^2, k_2^2, k_3^2, k_4^2)$.*

Proof. Assume that $k = k_1^2 + k_2^2 + k_3^2 + k_4^2$ and k_1, k_2, k_3 and k_4 are nonzero integers. Let $k_j^2 = \prod_{i=1}^m q_{ij}^2$, where q_{ij} is either 1 or a prime power. For each i , $1 \leq i \leq m$, let $b_i = \text{lcm}\{q_{ij}^2 + q_{ij} + 1; j = 1, 2, 3, 4\}$. From Corollary 3.12, for each j , $1 \leq j \leq 4$, and each i , $1 \leq i \leq m$, there exists a circulant $W_{ij} = W(b_i, q_{ij}^2)$. Putting

$$A = \otimes_{i=1}^m W_{i1} R_i, \quad B = \otimes_{i=1}^m W_{i2}, \quad C = \otimes_{i=1}^m W_{i3}, \quad D = \otimes_{i=1}^m W_{i4},$$

in the following array (Goethals-Seidel [19]) gives an $OD(4q; k_1^2, k_2^2, k_3^2, k_4^2)$,

$$\begin{bmatrix} xA & yB & zC & uD \\ -yB & xA & uD^t & -zC^t \\ -zC & -uD^t & xA & yB^t \\ -uD & zC^t & -yB^t & xA \end{bmatrix},$$

where $q = \prod_{i=1}^m b_i$ which is an odd number.

By Lemma 3.15, there is an $OD(2^d; k_1^2, k_2^2, k_3^2, k_4^2)$ for some suitable integer $d \geq 2$. Since for $d \geq 2$, $\text{gcd}(4q, 2^d) = 4$, Lemma 3.9 implies that there is an integer $N = N(k)$ such that for each $n \geq N$, there is an $OD(4n; k_1^2, k_2^2, k_3^2, k_4^2)$. \square

Remark 3.23. If some of the k_i 's are zero in Theorem 3.22, then consider the circulant zero matrices.

Corollary 3.24. *Suppose that d is any positive integer. Then there is an integer $N = N(d)$ such that for each $n \geq N$, there is a $W(4n, d)$.*

Proof. It is a well known theorem of Lagrange [25] that every positive integer can be written in the sum of four integer squares. Let $d = k_1^2 + k_2^2 + k_3^2 + k_4^2$. From Theorem 3.22, there is an integer $N = N(k)$ such that for each $n \geq N$, there is an $OD(4n; k_1^2, k_2^2, k_3^2, k_4^2)$, and therefore a $W(4n, d)$. \square

Corollary 3.25. *Suppose that d is the sum of three integer squares. Then there exists an integer $N = N(d)$ such that for each $n \geq N$, there is a skew-symmetric $W(4n, d)$.*

Proof. Consider $d = a^2 + b^2 + c^2$, for some integers a, b and c . Substituting $k_1 = a$, $k_2 = b$, $k_3 = c$ and $k_4 = 1$ in Theorem 3.22 gives the result. Note that the existence of an $OD(n; 1, h)$ is equivalent to existence of a skew-symmetric $W(n, h)$. \square

Corollary 3.26. *Suppose that d is any positive integer. Then there exists an integer $N = N(d)$ such that for each $n \geq N$, there is a skew-symmetric $W(8n, d)$.*

Proof. By Lagrange's theorem [49], one can write $d = k_1^2 + k_2^2 + k_3^2 + k_4^2$, where k_i 's are nonnegative integers. Let A, B, C and D be the same matrices as in Theorem 3.22. It can be seen that the following matrix gives an $OD(8q; 1, k_1^2, k_2^2, k_3^2, k_4^2)$, where q is obtained as in Theorem 3.22, and is an odd number:

$$\begin{bmatrix} xA & yB & zC & uD & wI_q & 0 & 0 & 0 \\ -yB & xA & uD^t & -zC^t & 0 & wI_q & 0 & 0 \\ -zC & -uD^t & xA & yB^t & 0 & 0 & wI_q & 0 \\ -uD & zC^t & -yB^t & xA & 0 & 0 & 0 & wI_q \\ wI_q & 0 & 0 & 0 & -xA & yB^t & zC^t & uD^t \\ 0 & wI_q & 0 & 0 & -yB^t & -xA & uD & -zC \\ 0 & 0 & wI_q & 0 & -zC^t & -uD & -xA & yB \\ 0 & 0 & 0 & wI_q & -uD^t & zC & -yB & -xA \end{bmatrix}.$$

From Corollary 3.16, there is an $OD(2^d; 1, k_1^2, k_2^2, k_3^2, k_4^2)$ for some suitable integer

$d \geq 3$. Since for $d \geq 3$, $\gcd(8q, 2^d) = 8$, Lemma 3.9 implies that there is an integer $N = N(d)$ such that for any $n \geq N$, there is an $OD(8n; 1, k_1^2, k_2^2, k_3^2, k_4^2)$, and so a skew-symmetric $W(8n, d)$.

□

Example 3.27. Suppose that $k = 92$. Let $k_1 = 2$, $k_2 = 4$, $k_3 = 6$ and $k_4 = 6$ in Theorem 3.22. Also, let $q_{11} = 2$, $q_{21} = 1$, $q_{12} = 4$, $q_{22} = 1$, $q_{13} = 2$, $q_{23} = 3$, $q_{14} = 2$ and $q_{24} = 3$. Then $b_1 = \text{LCM}\{7, 21, 7, 7\} = 21$, and $b_2 = \text{LCM}\{3, 3, 13, 13\} = 39$.

By Theorem 3.22, there is an $OD(4 \cdot 21 \cdot 39; 2^2, 4^2, 6^2, 6^2)$. From Lemma 3.15, there is an $OD(2^{13}; 2^2, 4^2, 6^2, 6^2)$. Thus, $N(92) \leq 2^{13} \cdot 3^2 \cdot 7 \cdot 13$, and so for each $n \geq N(92)$, there are a $W(4n, 92)$ and a skew-symmetric $W(8n, 92)$.

Chapter 4

Some notes on amicable orthogonal designs

4.1 A non-existence result for product designs

Peter J. Robinson [43] showed that there exist product designs $PD(4; 1, 1, 1; 1, 1, 1; 1)$, $PD(8; 1, 1, 1; 1, 1, 1; 5)$ and $PD(12; 1, 1, 1; 1, 1, 1; 9)$. In this section, we will show that there does not exist any $PD(n; 1, 1, 1; 1, 1, 1; n - 3)$ for all $n > 12$. In doing so, we first mention the following well known theorems.

Theorem 4.1 (see [49]). *Suppose that a, a', b and c are nonzero p -adic numbers and p is a prime number. Define $(a, b)_p$, the p -adic Hilbert symbol, to be 1 if there are p -adic numbers x and y such that $ax^2 + by^2 = 1$, and -1 otherwise. Then*

$$(i) \quad (a, b)_p = (b, a)_p, \quad (a, c^2)_p = 1,$$

$$(ii) \quad (a, -a)_p = 1, \quad (a, 1 - a)_p = 1,$$

$$(iii) \quad (aa', b)_p = (a, b)_p(a', b)_p,$$

and if $p \neq 2$, then

$$(iv) \quad (r, s)_p = 1 \text{ if } r \text{ and } s \text{ are relatively prime to } p,$$

(v) $(r, p)_p = (r/p)$, the Legendre symbol, if r and p are relatively prime,

(vi) $(p, p)_p = (-1/p)$,

where r and s are positive integers.

Theorem 4.2 (Shapiro [18, 45]). *There is a rational family of type (s_1, \dots, s_9) in order 16 if and only if $S_p(s_1, \dots, s_9) := \prod_{i < j} (s_i, s_j)_p = 1$ for every prime p .*

Theorem 4.3 (Robinson [42]). *There does not exist any $OD(n; 1_{(5)}, n - 5)$ for $n > 40$.*

Theorem 4.4 (Kharaghani and Tayfeh-Rezaie [30]). *There is a full $OD(32; 1_{(5)}, u_1, \dots, u_k)$ if and only if $(u_1, \dots, u_k) = (9, 9, 9)$ or $(9, 18)$ or $(12, 15)$ or (27) .*

Theorem 4.5. *There does not exist any $PD(n; 1, 1, 1; 1, 1, 1; n - 3)$ for all $n > 12$.*

Proof. If there exists a $PD(n; 1, 1, 1; 1, 1, 1; n - 3)$ for some $n > 20$, then by Theorem 2.46 and $AOD(2; 1, 1; 1, 1)$, there is an $OD(2n; 1_{(6)}, 2n - 6)$ which contradicts Theorem 4.3. Clearly, there are no $PD(n; 1, 1, 1; 1, 1, 1; n - 3)$ for $n = 13, 14, 15, 17, 18, 19$.

If $n = 16$, then there is an $OD(32; 1_{(6)}, 26)$ which is impossible by Theorem 4.4. Now suppose that there is a $PD(20; 1, 1, 1; 1, 1, 1; 17)$. Using Theorem 2.46 and $AOD(4; 1, 1, 2; 1, 1, 2)$, there is an $OD(80; 1, 1, 1, 3, 3, 3, 17, 17, 34)$. From Theorem 3.5, there is a rational family in order 16 and type $(1, 1, 1, 3, 3, 3, 17, 17, 34)$. By Theorem 4.1, $S_{17}(1, 1, 1, 3, 3, 3, 17, 17, 34) = -1$. This contradicts Theorem 4.2. \square

4.2 Some full amicable orthogonal designs

We apply techniques similar to those used in [18, 23] to obtain some classes of full amicable orthogonal designs.

Construction 4.6. Suppose that $A_1, A_2, B, C, D, E, F, G$ are square matrices of order n . Let

$$M_1 = \begin{bmatrix} 0 & D & B & C & 0 & 0 & 0 & 0 \\ -D & 0 & -C & B & 0 & 0 & 0 & 0 \\ B & -C & 0 & D & 0 & 0 & 0 & 0 \\ C & B & -D & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -D & B & C \\ 0 & 0 & 0 & 0 & D & 0 & -C & B \\ 0 & 0 & 0 & 0 & B & -C & 0 & -D \\ 0 & 0 & 0 & 0 & C & B & D & 0 \end{bmatrix},$$

$$M_2 = \begin{bmatrix} 0 & G & E & F & 0 & 0 & 0 & 0 \\ -G & 0 & F & -E & 0 & 0 & 0 & 0 \\ E & F & 0 & -G & 0 & 0 & 0 & 0 \\ F & -E & G & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -E & F & G \\ 0 & 0 & 0 & 0 & E & 0 & G & -F \\ 0 & 0 & 0 & 0 & F & G & 0 & E \\ 0 & 0 & 0 & 0 & G & -F & -E & 0 \end{bmatrix},$$

$$N_i = \begin{bmatrix} A_i & 0 & 0 & 0 & A_i & -A_i & A_i & A_i \\ 0 & A_i & 0 & 0 & A_i & A_i & A_i & -A_i \\ 0 & 0 & -A_i & 0 & -A_i & -A_i & A_i & -A_i \\ 0 & 0 & 0 & -A_i & -A_i & A_i & A_i & A_i \\ -A_i & -A_i & -A_i & -A_i & A_i & 0 & 0 & 0 \\ A_i & -A_i & -A_i & A_i & 0 & A_i & 0 & 0 \\ A_i & A_i & -A_i & -A_i & 0 & 0 & -A_i & 0 \\ A_i & -A_i & A_i & -A_i & 0 & 0 & 0 & -A_i \end{bmatrix},$$

for $i = 1, 2$. Now suppose that matrices A_1, A_2, B, C, D, E, F and G which are pairwise amicable (not necessary orthogonal designs), and satisfy the following properties

$$(i) \quad 5A_1A_1^t + BB^t + CC^t + DD^t = kI_n,$$

$$(ii) \quad 5A_2A_2^t + EE^t + FF^t + GG^t = sI_n.$$

Then the following matrices may be used to construct a disjoint amicable orthogonal design of order $16n$:

$$U = N_1 \otimes I + M_1 \otimes Q, \quad V = N_2 \otimes P + M_2 \otimes R^t, \quad (4.1)$$

where P, Q, R and I are 2×2 matrices described in Example 2.39.

To see this, one observes that $N_1N_2^t = N_2N_1^t$, $M_1M_2^t = M_2M_1^t$ and for $i, j \in \{1, 2\}$, $M_jN_i^t = -N_iM_j^t$. Also, matrices I and Q are disjoint with matrices P and R , while matrices M_1 and M_2 are disjoint with matrices N_1 and N_2 .

Assume that the matrices A_1, A_2, B, C, D, E, F and G are full (no zero entries) pairwise amicable, and H is a Hadamard matrix of order 2. Then the following matrices may be used to construct a full amicable orthogonal design of order $16n$:

$$U_H = N_1 \otimes H + M_1 \otimes QH, \quad V_H = N_2 \otimes PH + M_2 \otimes R^tH. \quad (4.2)$$

Example 4.7. Consider $A_1 = \text{backcirc}(x, -b, b)$, $A_2 = \text{circ}(-d, d, d)$, $B = \text{circ}(b, b, b)$, $C = \text{circ}(-a, b, b)$, $D = \text{circ}(a, b, b)$, $E = \text{circ}(d, d, d)$, $F = \text{circ}(-c, d, d)$ and $G = \text{circ}(c, d, d)$. It can be seen that the conditions of Construction 4.6 hold, and therefore matrices in (4.2) are $AOD(48; 4, 10, 34; 4, 44)$. See Appendix, page 106.

Construction 4.8. Suppose that $A_1, A_2, B, C, D, E, F, G$ are square matrices of order n . Let

$$M_1 = \begin{bmatrix} B & C & D & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -C & B & 0 & -D & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -D & 0 & B & C & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & D & -C & B & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & B & C & D & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -C & B & 0 & -D & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -D & 0 & B & C & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & D & -C & B & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & B & C & D & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -C & B & 0 & -D \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -D & 0 & B & C \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & D & -C & B \end{bmatrix},$$

$$M_2 = \begin{bmatrix} E & F & G & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ F & -E & 0 & -G & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ G & 0 & -E & F & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -G & F & E & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & F & G & E & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & G & -F & 0 & -E & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & E & 0 & -F & G & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -E & G & F & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & G & -E & -F & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -E & -G & 0 & F \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -F & 0 & -G & -E \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & F & -E & G \end{bmatrix},$$

$$N_i = \begin{bmatrix} 0 & 0 & 0 & -A_i & A_i & A_i & A_i & -A_i & A_i & -A_i & A_i & -A_i \\ 0 & 0 & -A_i & 0 & A_i & -A_i & -A_i & -A_i & -A_i & -A_i & -A_i & -A_i \\ 0 & A_i & 0 & 0 & A_i & A_i & -A_i & A_i & A_i & A_i & -A_i & -A_i \\ A_i & 0 & 0 & 0 & A_i & -A_i & A_i & A_i & A_i & -A_i & -A_i & A_i \\ -A_i & -A_i & -A_i & -A_i & 0 & 0 & 0 & -A_i & A_i & A_i & -A_i & A_i \\ -A_i & A_i & -A_i & A_i & 0 & 0 & -A_i & 0 & A_i & -A_i & A_i & A_i \\ -A_i & A_i & A_i & -A_i & 0 & A_i & 0 & 0 & -A_i & -A_i & -A_i & A_i \\ A_i & A_i & -A_i & -A_i & A_i & 0 & 0 & 0 & -A_i & A_i & A_i & A_i \\ -A_i & A_i & -A_i & -A_i & -A_i & -A_i & A_i & A_i & 0 & 0 & 0 & -A_i \\ A_i & A_i & -A_i & A_i & -A_i & A_i & A_i & -A_i & 0 & 0 & -A_i & 0 \\ -A_i & A_i & A_i & A_i & A_i & -A_i & A_i & -A_i & 0 & A_i & 0 & 0 \\ A_i & A_i & A_i & -A_i & -A_i & -A_i & -A_i & -A_i & A_i & 0 & 0 & 0 \end{bmatrix},$$

for $i = 1, 2$. Suppose matrices A_1, A_2, B, C, D, E, F and G are pairwise amicable (not

necessarily orthogonal designs) and satisfy the following properties :

$$(i) \quad 9A_1A_1^t + BB^t + CC^t + DD^t = uI_n,$$

$$(ii) \quad 9A_2A_2^t + EE^t + FF^t + GG^t = vI_n.$$

Then, as in Construction 4.6, the matrices U and V in (4.1) along with these new matrices, M_1, M_2, N_1, N_2 , form a disjoint amicable orthogonal design of order $24n$. Also, matrices U_H and V_H in (4.2) along with these new matrices, M_1, M_2, N_1, N_2 , form a full amicable orthogonal design of order $24n$, provided the matrices A_1, A_2, B, C, D, E, F and G in this construction are full and pairwise amicable.

Example 4.9. Suppose that $A_1 = \text{backcirc}(x, -b, b)$, $A_2 = \text{circ}(-d, d, d)$, $B = \text{circ}(b, b, b)$, $C = \text{circ}(b, b, b)$, $D = \text{circ}(b, b, b)$, $E = \text{circ}(d, d, d)$, $F = \text{circ}(d, d, d)$ and $G = \text{circ}(d, d, d)$. Then they satisfy all conditions in Construction 4.8, and therefore matrices U_H and V_H in (4.2) form an $AOD(72; 18, 54; 72)$.

Example 4.10. Suppose that $A_1 = \text{backcirc}(a, -a, -a, a, -a, a, a)$, $A_2 = \text{circ}(c, -c, -c, c, -c, c, c)$, $B = \text{circ}(b, a, a, a, a, a, a)$, $C = \text{circ}(-b, a, a, a, a, a, a)$, $D = \text{circ}(a, -a, -a, a, -a, a, a)$, $E = \text{circ}(d, c, c, c, c, c, c)$, $F = \text{circ}(-d, c, c, c, c, c, c)$ and $G = \text{circ}(c, -c, -c, c, -c, c, c)$. It can be directly verified that Construction 4.8 forms an $AOD(168; 4, 164; 4, 164)$.

Remark 4.11. If we replace matrices A_1, B, C, D, E, F and G by variables in Constructions 4.6 and 4.8, then matrices M_1, M_2 and N_1 will construct product designs $PD(8; 1, 1, 1; 1, 1, 1; 5)$ and $PD(12; 1, 1, 1; 1, 1, 1; 9)$, respectively.

4.3 An infinite class of full amicable orthogonal designs

The following theorem is an application to an algebraic result that Kawada and Iwahori obtained in [28].

Theorem 4.12 (see [18]). *Suppose that $(A; B)$ is an amicable orthogonal design of order n . Let t be the number of variables in B and $\rho_t(n)$ be the number of variables in A . Also, $n = 2^{4a+b}d$, where $0 \leq b < 4$ and d is an odd number. Then*

$$\rho_t(n) \leq 8a - t + \delta + 1,$$

where the values of δ are given in the following table :

b	0	1	2	3
$t \equiv 0 \pmod{4}$	0	1	3	7
$t \equiv 1 \pmod{4}$	1	2	3	5
$t \equiv 2 \pmod{4}$	-1	3	4	5
$t \equiv 3 \pmod{4}$	-1	1	5	6

Theorem 4.13 (see [53]). *Suppose there is an AOD($n; u_1, u_2, \dots, u_r; v_1, v_2, \dots, v_s$).*

Then for each $t \geq 1$, there is an

$$\text{AOD}\left(2^t n; u_1, u_1, 2u_1, \dots, 2^{t-1}u_1, 2^t u_2, \dots, 2^t u_r; 2^t v_1, 2^t v_2, \dots, 2^t v_s\right).$$

Construction 4.14. *Replacing A_1, B, C, D, A_2, E, F and G by variables in Constructions 4.6 and 4.8, respectively, one obtains*

$$\text{AOD}(16; 2, 2, 2, 10; 2, 2, 2, 10) \quad \text{and} \quad \text{AOD}(24; 2, 2, 2, 18; 2, 2, 2, 18).$$

Applying Theorem 4.13 for these amicable orthogonal designs, one obtains an infinite class of full amicable orthogonal designs :

$$AOD\left(2^n; 2_{(3)}^{n-3}, 10, 10, 5 \cdot 2^2, \dots, 5 \cdot 2^{n-4}; 2_{(3)}^{n-3}, 5 \cdot 2^{n-3}\right), \quad n > 4,$$

$$AOD\left(2^n \cdot 3; 2_{(3)}^{n-2}, 18, 18, 9 \cdot 2^2, \dots, 9 \cdot 2^{n-3}; 2_{(3)}^{n-2}, 9 \cdot 2^{n-2}\right), \quad n > 3.$$

Example 4.15. From Construction 4.14, we obtain

- (i) $AOD(24; 2, 2, 2, 18; 2, 2, 2, 18)$,
- (ii) $AOD(48; 4, 4, 4, 18, 18; 4, 4, 4, 36)$,
- (iii) $AOD(96; 8, 8, 8, 18, 18, 36; 8, 8, 8, 72)$.

See Appendix, pages 104, 107 and 108. According to Theorem 4.12, these amicable orthogonal designs have taken the maximum number of variables.

We also display the following amicable orthogonal designs in Appendix, pages 103 and 105 :

$$AOD(16; 2, 2, 2, 10; 2, 2, 2, 10) \quad \text{and} \quad AOD(32; 4, 4, 4, 10, 10; 4, 4, 4, 20).$$

4.4 Amicable full orthogonal designs in 16 variables

Lemma 4.16. *There exists an $AOD(2^9; 2_{(8)}^6; 2_{(8)}^6)$.*

Proof. Suppose that $A = \{A_1, \dots, A_8\}$ and $B = \{B_1, \dots, B_8\}$ are two sets of signed permutation matrices of order 2^7 satisfying conditions (i), (ii) and (iii) of Theorem

2.43. Let H be a Hadamard matrix of order 2^7 . For each $1 \leq j \leq 4$, let

$$X_j = \frac{1}{2}x_{2j-1}(A_{2j-1} - A_{2j})H + \frac{1}{2}x_{2j}(A_{2j-1} + A_{2j})H$$

and

$$Y_j = \frac{1}{2}y_{2j-1}(B_{2j-1} - B_{2j})H + \frac{1}{2}y_{2j}(B_{2j-1} + B_{2j})H.$$

Note that for $1 \leq i \neq j \leq 4$, $X_i X_j^t = -X_j X_i^t$ and $Y_i Y_j^t = -Y_j Y_i^t$. For $1 \leq i, j \leq 4$, $X_i Y_j^t = Y_j X_i^t$. Also, for each $1 \leq j \leq 4$,

$$X_j X_j^t = 2^6(x_{2j-1}^2 + x_{2j}^2)I_{2^7} \quad \text{and} \quad Y_j Y_j^t = 2^6(y_{2j-1}^2 + y_{2j}^2)I_{2^7}.$$

Let

$$C = I \otimes I \otimes X_1 + I \otimes P \otimes X_2 + P \otimes I \otimes X_3 + P \otimes P \otimes X_4,$$

$$D = I \otimes I \otimes Y_1 + I \otimes P \otimes Y_2 + P \otimes I \otimes Y_3 + P \otimes P \otimes Y_4.$$

It can be directly verified that $CC^t = \left(2^6 \sum_{i=1}^8 x_i^2\right)I_{2^9}$, $DD^t = \left(2^6 \sum_{i=1}^8 y_i^2\right)I_{2^9}$ and $CD^t = DC^t$. Therefore, C and D are an $AOD(2^9; 2^6_{(8)}; 2^6_{(8)})$ \square

Theorem 4.17. *There is an $OD(2^{10}; 2^6_{(16)})$.*

Proof. Let C and D be the matrices constructed in the proof of Lemma 4.16. Then $\begin{bmatrix} C & D \\ D & -C \end{bmatrix}$ is an $OD(2^{10}; 2^6_{(16)})$. \square

According to Theorems 2.41 and 4.12, there does not exist any $AOD(2^6; 2^3_{(8)}; 2^3_{(8)})$; however, it is not known whether or not there exists an $AOD(2^7; 2^4_{(8)}; 2^4_{(8)})$.

Chapter 5

Asymptotic existence of orthogonal designs

We need the following well known lemma from [23] for our main construction.

Lemma 5.1. *For any positive integer n , there is a Golay pair of length 2^n in two variables each appearing 2^{n-1} times in each of sequences.*

Proof. Consider $n = 1$. The sequences $A_1 = (x, y)$ and $B_1 = (x, -y)$ of commuting variables x and y is a Golay pair of length 2 in two variables in which each variable appears one time in A_1 and B_1 . Let A_{n-1} and B_{n-1} be a Golay pair of length 2^{n-1} in two variables each appearing 2^{n-2} times in both A_{n-1} and B_{n-1} . Then

$$A_n = (A_{n-1}, B_{n-1}) \quad \text{and} \quad B_n = (A_{n-1}, -B_{n-1})$$

form a Golay pair of length 2^n in two variables as desired, where (A, B) means the sequence A followed by the sequence B .

□

5.1 Asymptotic existence of orthogonal designs

Following similar techniques in [23], we have the following proposition.

Proposition 5.2. *For any given sequence of positive integers $(b, a_1, a_2, \dots, a_k)$, there exists a full COD of type $(2^m \cdot 1_{(b)}, 2^m \cdot 2_{(4)}^{a_1}, \dots, 2^m \cdot 2_{(4)}^{a_k})$, where $m = 4k + b + 2$ if b is even, and $m = 4k + b + 1$ if b is odd.*

Proof. Let $(b, a_1, a_2, \dots, a_k)$ be a sequence of positive integers. We distinguish two cases:

Case 1. b is even. Suppose that x_i , $0 \leq i \leq \frac{b}{2}$, y_j and z_j , $1 \leq j \leq k$ are commuting variables. In the end of proof, we will replace these variables by the near type 1 matrices of order 2. For each j , $1 \leq j \leq k$, let G_{j1} and G_{j2} be a Golay pair in y_j and z_j of lengths 2^{a_j} . Let

$$s_1 = 0 \quad \text{and} \quad s_j = 2 \sum_{r=1}^{j-1} 2^{a_r}, \quad 2 \leq j \leq k+1. \quad (5.1)$$

Let $d = \frac{b}{2} + s_{k+1}$ and consider

$$\begin{aligned} M_0 &= \text{circ}(0_{(d)}, x_0, 0_{(d-1)}), & M_1 &= \text{circ}(x_1, 0_{(2d-1)}), \\ M_h &= \text{circ}(0_{(h-1)}, x_h, 0_{(2d-h)}), & & 2 \leq h \leq \frac{b}{2}. \end{aligned} \quad (5.2)$$

For each j , $1 \leq j \leq k$, define

$$N_{2j-1} := \text{circ}\left(0_{\left(\frac{b}{2}+s_j\right)}, G_{j1}, 0_{\left(2d-\frac{b}{2}-s_j-2^{a_j}\right)}\right), \quad N_{2j} := \text{circ}\left(0_{\left(\frac{b}{2}+s_j+2^{a_j}\right)}, G_{j2}, 0_{\left(2d-\frac{b}{2}-s_{j+1}\right)}\right).$$

Let $m = 4k + b + 2$ and let $A = \{A_1, \dots, A_m\}$ be the collection of mutually disjoint anti-amicable signed permutation matrices of order 2^{m-1} constructed in Theorem

2.43, and suppose H is a Hadamard matrix of order 2^{m-1} . Let

$$\begin{aligned}
C &= \frac{1}{2}(M_0 + M_0^t) \otimes A_1 H + \frac{i}{2}(M_0 - M_0^t) \otimes A_2 H \\
&+ \frac{1}{2}(M_1 + M_1^t) \otimes A_3 H + \frac{i}{2}(M_1 - M_1^t) \otimes A_4 H \\
&+ \sum_{h=2}^{\frac{b}{2}} \left((M_h + M_h^t) \otimes \frac{1}{2}(A_{2h+1} + A_{2h+2}) H + i(M_h - M_h^t) \otimes \frac{1}{2}(A_{2h+1} - A_{2h+2}) H \right) \\
&+ \sum_{j=1}^{2k} \left((N_j + N_j^t) \otimes \frac{1}{2}(A_{2j+b+1} + A_{2j+b+2}) H + i(N_j - N_j^t) \otimes \frac{1}{2}(A_{2j+b+1} - A_{2j+b+2}) H \right),
\end{aligned} \tag{5.3}$$

We show that

$$CC^* = 2^m \omega I_{2^m d}. \tag{5.4}$$

where $\omega = \frac{1}{2}x_0x_0^t + \frac{1}{2}x_1x_1^t + x_2x_2^t + \cdots + x_{\frac{b}{2}}x_{\frac{b}{2}}^t + 2^{a_1}y_1y_1^t + 2^{a_1}z_1z_1^t + \cdots + 2^{a_k}y_ky_k^t + 2^{a_k}z_kz_k^t$.

To this end, we first note that each of the sets

$$\left\{ \frac{1}{2}(M_0 + M_0^t), \frac{i}{2}(M_0 - M_0^t), \frac{1}{2}(M_1 + M_1^t), \frac{i}{2}(M_1 - M_1^t) \right\},$$

$$\left\{ (M_h + M_h^t), (N_j + N_j^t); 2 \leq h \leq \frac{b}{2}, 1 \leq j \leq 2k \right\}$$

and

$$\left\{ i(M_h - M_h^t), i(N_j - N_j^t); 2 \leq h \leq \frac{b}{2}, 1 \leq j \leq 2k \right\}$$

consist of mutually disjoint Hermitian circulant matrices. Moreover, for $u = 0, 1$, we

have

$$\frac{1}{4}(M_u + M_u^t)(M_u + M_u^t)^t + \frac{1}{4}(M_u - M_u^t)(M_u - M_u^t)^t = x_u x_u^t I_{2d}$$

and for each h , $2 \leq h \leq \frac{b}{2}$,

$$(M_h + M_h^t)(M_h + M_h^t)^t + (M_h - M_h^t)(M_h - M_h^t)^t = 4x_h x_h^t I_{2d}.$$

Also, for each j , $1 \leq j \leq k$, we have

$$\begin{aligned} \sum_{r=2j-1}^{2j} \left((N_r + N_r^t)(N_r + N_r^t)^t + (N_r - N_r^t)(N_r - N_r^t)^t \right) &= 2 \sum_{r=2j-1}^{2j} (N_r N_r^t + N_r^t N_r) \\ &= 2^{a_j+2} (y_j y_j^t + z_j z_j^t) I_{2d}. \end{aligned}$$

Note that for each j , $3 \leq j \leq \frac{b}{2} + 2k + 1$, the matrices $\frac{1}{2}(A_{2j-1} + A_{2j})H$ and $\frac{1}{2}(A_{2j-1} - A_{2j})H$ are disjoint with $0, \pm 1$ entries. Furthermore, since the set A consists of mutually anti-amicable matrices, the set

$$\left\{ A_1 H, A_2 H, A_3 H, A_4 H, \frac{1}{2}(A_{2j-1} \pm A_{2j})H \quad (3 \leq j \leq \frac{b}{2} + 2k + 1) \right\}$$

consists of mutually anti-amicable matrices. Since for each j , $3 \leq j \leq \frac{b}{2} + 2k + 1$,

$$\begin{aligned} \left(\frac{1}{2}(A_{2j-1} \pm A_{2j})H \right) \left(\frac{1}{2}(A_{2j-1} \pm A_{2j})H \right)^t &= \frac{2^{m-1}}{4} (A_{2j-1} \pm A_{2j})(A_{2j-1} \pm A_{2j})^t I_{2^{m-1}} \\ &= 2^{m-2} I_{2^{m-1}}, \end{aligned}$$

the validity of equation (5.4) follows.

In the equation (5.4), if we replace the x_0 by $\begin{bmatrix} \alpha & \alpha \\ -\alpha & \alpha \end{bmatrix}$, the x_1 by $\begin{bmatrix} \beta & \beta \\ -\beta & \beta \end{bmatrix}$, the x_h by $\begin{bmatrix} \alpha_h & \beta_h \\ -\beta_h & \alpha_h \end{bmatrix}$, $2 \leq h \leq \frac{b}{2}$, the y_j by $\begin{bmatrix} \alpha'_j & \beta'_j \\ -\beta'_j & \alpha'_j \end{bmatrix}$, and the z_j by $\begin{bmatrix} \alpha''_j & \beta''_j \\ -\beta''_j & \alpha''_j \end{bmatrix}$,

$1 \leq j \leq k$, then the matrix C will be a full COD of type

$$\left(2^m \cdot 1_{(b)}, 2^m \cdot 2_{(4)}^{a_1}, \dots, 2^m \cdot 2_{(4)}^{a_k}\right),$$

where the α , β , α_h 's, β_h 's, α_j 's, β_j 's, α_j'' 's and β_j'' 's are 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 (5.1),

$$\begin{aligned} M_1 &= \text{circ}(x_1, 0_{(2d)}), \\ M_h &= \text{circ}(0_{(h-1)}, x_h, 0_{(2d-h+1)}), \quad 2 \leq h \leq \frac{b+1}{2}. \end{aligned}$$

For each $1 \leq j \leq k$, assume

$$\begin{aligned} N_{2j-1} &= \text{circ}\left(0_{\left(\frac{b+1}{2}+s_j\right)}, G_{j1}, 0_{\left(2d-\frac{b-1}{2}-s_j-2^{a_j}\right)}\right), \\ N_{2j} &= \text{circ}\left(0_{\left(\frac{b+1}{2}+s_j+2^{a_j}\right)}, G_{j2}, 0_{\left(2d-\frac{b-1}{2}-s_{j+1}\right)}\right). \end{aligned}$$

The rest of proof is similar to Case 1, and so $m = 4k + b + 1$. □

Corollary 5.3. *Let $(b, a_1, a_2, \dots, a_k)$ be a sequence of positive integers and let $\ell' = b + 4 \sum_{i=1}^k 2^{a_i}$. Then for every $\ell \geq \ell'$, there is a*

$$COD\left(2^m \ell; 2^m \cdot 1_{(b)}, 2^m \cdot 2_{(4)}^{a_1}, \dots, 2^m \cdot 2_{(4)}^{a_k}\right),$$

where $m \leq 4k + b + 2$.

Proof. In the proof of Proposition 5.2, depending on ℓ , we may add an appropriate amount of zeros to the circulant matrices in Case 1 or Case 2 as the same way as we add the x_h 's in (5.2) to obtain circulant matrices of order ℓ . The rest of proof is

similar. It can be seen that $m \leq 4k + b + 2$. \square

Let (u_1, \dots, u_ℓ) 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 , $i = 1, 2, \dots, \ell$. Using the binary expansion of each u_i , one can write

$$\begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_\ell \end{bmatrix} = E \begin{bmatrix} 1 \\ 2 \\ \vdots \\ 2^t \end{bmatrix}, \quad (5.5)$$

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, \dots, u_ℓ) .

For simplicity and in order to make the first column of the binary matrix E nonzero, in Lemma 5.4 and Corollary 5.5, we assume that the ℓ -tuples of positive integers have at least one odd element. Then we show Lemma 5.6.

Lemma 5.4. *Suppose that (u_1, \dots, u_ℓ) is an ℓ -tuple of positive integers such that at least one of the u_i 's is odd. Then there is an integer $m = m(u_1, \dots, u_\ell)$ such that there is a*

$$COD\left(2^m(u_1 + \dots + u_\ell); 2^m u_1, \dots, 2^m u_\ell\right).$$

Proof. Let (u_1, \dots, u_ℓ) be an ℓ -tuple of positive integers such that at least one of u_i 's is odd, and let $d = u_1 + \dots + u_\ell$. We form the $\ell \times (t + 1)$ binary matrix $E = [e_{ij}]$ corresponding to the ℓ -tuple (u_1, \dots, u_ℓ) , where t is the largest exponent appearing in the binary expansions of u_i , $i = 1, 2, \dots, \ell$. Let

$$\gamma_{j-1} := \sum_{i=1}^{\ell} e_{ij}, \quad 1 \leq j \leq t + 1. \quad (5.6)$$

We may use the following algorithm:

$$k := t; \gamma'_t := \left\lfloor \frac{\gamma_t}{4} \right\rfloor; \quad (\lfloor x \rfloor \text{ is the floor of } x) \quad (5.7)$$

while $k > 0$ do

$$\{\beta_k := \gamma_k \pmod{4};$$

$$k := k - 1;$$

$$\gamma_k := \gamma_k + 2\beta_{k+1};$$

if $k \neq 0$ then

$$\gamma'_k := \left\lfloor \frac{\gamma_k}{4} \right\rfloor;$$

else

$$\gamma'_k := \gamma_k; \}$$

Now we apply Proposition 5.2 to the sequence $(\gamma'_0, 1_{(\gamma'_1)}, 2_{(\gamma'_2)}, \dots, t_{(\gamma'_t)})$. Thus, there is an integer m , such that there is a

$$COD\left(2^m d; 2^m \cdot 1_{(\gamma'_0)}, 2^m \cdot 2_{(4\gamma'_1)}, 2^m \cdot 2^2_{(4\gamma'_2)}, \dots, 2^m \cdot 2^t_{(4\gamma'_t)}\right). \quad (5.8)$$

Indeed, if γ'_0 is even or odd, then we take $m = 4 \sum_{j=1}^t \gamma'_j + \gamma'_0 + 2$ or $m = 4 \sum_{j=1}^t \gamma'_j + \gamma'_0 + 1$, respectively. Note that the algorithm (5.7) breaks the binary expansion of the ℓ -tuple (u_1, \dots, u_ℓ) such that we can use Proposition 5.2. Therefore, the elements of the ℓ -tuple (u_1, \dots, u_ℓ) can be obtained by adding the elements of the sequence $(1_{(\gamma'_0)}, 2_{(4\gamma'_1)}, 2^2_{(4\gamma'_2)}, \dots, 2^t_{(4\gamma'_t)})$ in a suitable way. Thus, equating variables in the COD (5.8) in an appropriate way, we obtain a $COD(2^m d; 2^m u_1, \dots, 2^m u_\ell)$. \square

Corollary 5.5. *Let (u_1, \dots, u_ℓ) be an ℓ -tuple of positive integers such that at least one of u_i 's is odd, and let $d = u_1 + \dots + u_\ell$. Then for $d' \geq d$, there is an integer*

$m = m(u_1, \dots, u_\ell)$ such that there is a

$$COD\left(2^m d'; 2^m u_1, \dots, 2^m u_\ell\right).$$

Proof. We use Corollary 5.3 instead of Proposition 5.2 in the proof of Lemma 5.4. □

Lemma 5.6. *For any ℓ -tuple (s_1, \dots, s_ℓ) of positive integers, there is an integer $r = r(s_1, \dots, s_\ell)$ such that there is a*

$$COD\left(2^r (s_1 + \dots + s_\ell); 2^r s_1, \dots, 2^r s_\ell\right).$$

Proof. Suppose that (s_1, \dots, s_ℓ) is an ℓ -tuple of positive integers and let

$$(s_1, \dots, s_\ell) = 2^q (u_1, \dots, u_\ell), \tag{5.9}$$

where q is a unique nonnegative integer such that one of u_i 's is odd. By Lemma 5.4, there is an integer $m = m(u_1, \dots, u_\ell)$ such that there is a

$$COD\left(2^m (u_1 + \dots + u_\ell); 2^m u_1, \dots, 2^m u_\ell\right).$$

Now if $m \geq q$, then we choose $r = m - q$, and if $m < q$, then $A \otimes H$ is a

$$COD\left(2^q (u_1 + \dots + u_\ell); 2^q u_1, \dots, 2^q u_\ell\right) = COD\left(s_1 + \dots + s_\ell; s_1, \dots, s_\ell\right),$$

where H is a Hadamard matrix of order 2^{q-m} , and therefore we may choose $r = 0$. □

We now show an asymptotic existence result for ODs. In Chapter 6, we also give some other bounds for N in the following theorem by a different method.

Theorem 5.7. For any ℓ -tuple (s_1, \dots, s_ℓ) of positive integers, there is an integer $N = N(s_1, \dots, s_\ell)$ such that for each $n \geq N$ there is an

$$OD\left(2^n(s_1 + \dots + s_\ell); 2^n s_1, \dots, 2^n s_\ell\right).$$

Proof. Let (s_1, \dots, s_ℓ) be a ℓ -tuple of positive integers. From Lemma 5.6, there is an integer $r = r(s_1, \dots, s_\ell)$ such that there is a

$$COD\left(2^r(s_1 + \dots + s_\ell); 2^r s_1, \dots, 2^r s_\ell\right).$$

Let A be the above COD. We may write A as $X + iY$, where X and Y are disjoint and amicable matrices such that $XX^t + YY^t = AA^*$. It can be seen that

$$B = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes X + \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix} \otimes Y$$

is an

$$OD\left(2^{r+1}(s_1 + \dots + s_\ell); 2^{r+1} s_1, 2^{r+1} s_2, \dots, 2^{r+1} s_\ell\right). \quad (5.10)$$

We choose $N = r + 1$, and so for each $n \geq N$, the Kronecker product of a Hadamard matrix of order 2^{n-N} with the OD (5.10) gives us an

$$OD\left(2^n(s_1 + \dots + s_\ell); 2^n s_1, \dots, 2^n s_\ell\right).$$

□

Example 5.8. Consider the 5-tuple $(8, 12, 20, 68, 136)$. Write this as $2^2(2, 3, 5, 17, 34)$.

Apply the equation (5.5) 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 equation (5.6), we have $\gamma_0 = 3, \gamma_1 = 3, \gamma_2 = 1, \gamma_3 = 0, \gamma_4 = 1$ and $\gamma_5 = 1$. If we apply the algorithm (5.7), then we find $\gamma'_0 = 5, \gamma'_1 = 1, \gamma'_2 = 1, \gamma'_3 = 1, \gamma'_4 = 0$ and $\gamma'_5 = 0$. Apply Proposition 5.2 to the sequence $(b, a_1, a_2, a_3) = (5, 1, 2, 3)$. Since b is odd, we use Case 2 of Proposition 5.2, and so $m = 4 \times 3 + 5 + 1 = 18$. Therefore, there is a

$$COD\left(2^{18} \cdot 61; 2^{18} \cdot 1_{(5)}, 2^{18} \cdot 2_{(4)}, 2^{18} \cdot 2_{(4)}^2, 2^{18} \cdot 2_{(4)}^3\right).$$

By equating variables, we obtain a

$$COD\left(2^{18} \cdot 61; 2^{16} \cdot 8, 2^{16} \cdot 12, 2^{16} \cdot 20, 2^{16} \cdot 68, 2^{16} \cdot 136\right).$$

Example 5.9. We apply the equation (5.5) 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 equation (5.6), we have $\gamma_0 = 4, \gamma_1 = 1, \gamma_2 = 2, \gamma_3 = 0, \gamma_4 = 1$. Now if we apply the algorithm (5.7), then we find $\gamma'_0 = 6, \gamma'_1 = 1, \gamma'_2 = 1, \gamma'_3 = 0, \gamma'_4 = 0$. So, we apply Proposition 5.2 to the sequence $(b, a_1, a_2) = (6, 1, 2)$. Since b is even, we use Case 1 of Proposition 5.2, and so $m = 4 \times 2 + 6 + 2 = 16$. Thus, there is a

$$COD\left(2^{16} \cdot 30; 2^{16} \cdot 1_{(6)}, 2^{16} \cdot 2_{(4)}, 2^{16} \cdot 2_{(4)}^2\right).$$

By equating variables we obtain a

$$COD\left(2^{16} \cdot 30; 2^{16} \cdot 1, 2^{16} \cdot 5, 2^{16} \cdot 7, 2^{16} \cdot 17\right).$$

5.2 Asymptotic existence of amicable orthogonal designs

We now include an asymptotic existence result for amicable ODs by following similar techniques in [23].

Lemma 5.10. *If there is an ACOD($n; u_1, \dots, u_s; v_1, \dots, v_t$), then there is an*

$$AOD(2n; 2u_1, \dots, 2u_s; 2v_1, \dots, 2v_t).$$

Proof. Suppose that $(X; Y)$ is a complex amicable OD. We may write $X = A + iB$ and $Y = C + iD$, where A and B (C and D) are disjoint and amicable matrices such that $AA^t + BB^t = XX^*$ and $CC^t + DD^t = YY^*$. Let $R = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and

$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Since $(X; Y)$ is a complex amicable OD,

$$AC^t + BD^t = CA^t + DB^t, \quad AD^t - BC^t = CB^t - DA^t.$$

Let $X' = A \otimes RH + B \otimes H$ and $Y' = C \otimes RH + D \otimes H$. Then

$$X'Y'^t = 2(AC^t + BD^t) \otimes I + 2(AD^t - BC^t) \otimes R$$

$$Y'^t X' = 2(CA^t + DB^t) \otimes I + 2(CB^t - DA^t) \otimes R.$$

Therefore $(X'; Y')$ is an amicable OD as desired. \square

Theorem 5.11. *For any two sequences (u_1, u_2, \dots, u_s) and (v_1, v_2, \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, u_2, \dots, u_s) and (v_1, v_2, \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 $u'_1 + \dots + u'_s = c_1$ and $v'_1 + \dots + v'_t = c_2$. We may use the algorithm (5.7) in the proof of Lemma 5.4 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 $(\beta, \alpha_1, \alpha_2, \dots, \alpha_\ell)$ 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 assume that $c_1 \geq c_2$, and b and β are even. Let $m = \max\{4k + b + 2, 4\ell + \beta + 2\}$.

Suppose that $A = \{A_1, \dots, A_m\}$ and $B = \{B_1, \dots, B_m\}$ are the same set of

matrices of order 2^{m-1} as in Theorem 2.43.

Apply Proposition 5.2 to the sequence $(b, a_1, a_2, \dots, a_k)$ by using the set A . Thus there is a COD, C , of order $2^m c_1$ and type $\left(2^m \cdot 1_{(b)}, 2^m \cdot 2_{(4)}^{a_1}, \dots, 2^m \cdot 2_{(4)}^{a_k}\right)$.

Apply Corollary 5.3 to the sequence $(\beta, \alpha_1, \alpha_2, \dots, \alpha_\ell)$ by using the set B . It can be seen that there is a COD, D , of order $2^m c_1$ and type $\left(2^m \cdot 1_{(\beta)}, 2^m \cdot 2_{(4)}^{\alpha_1}, \dots, 2^m \cdot 2_{(4)}^{\alpha_\ell}\right)$.

Note that $c_1 \geq c_2$.

Since the circulant matrices used to construct C and D in (5.3) are Hermitian of order c_1 and $A_i B_j^t = B_j A_i^t$ for $1 \leq i, j \leq m$, $(C; D)$ is an

$$ACOD\left(2^m c_1; 2^m \cdot 1_{(b)}, 2^m \cdot 2_{(4)}^{a_1}, \dots, 2^m \cdot 2_{(4)}^{a_k}; 2^m \cdot 1_{(\beta)}, 2^m \cdot 2_{(4)}^{\alpha_1}, \dots, 2^m \cdot 2_{(4)}^{\alpha_\ell}\right).$$

Equating variables in C and D in an appropriate way, we obtain an

$$ACOD\left(2^m c_1; 2^m u'_1, \dots, 2^m u'_s; 2^m v'_1, \dots, 2^m v'_t\right),$$

and so by Lemma 5.10, there exists an

$$AOD\left(2^{m'} c_1; 2^{m'} u'_1, \dots, 2^{m'} u'_s; 2^{m'} v'_1, \dots, 2^{m'} v'_t\right), \quad (5.11)$$

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 $q_1 \leq q_2 \leq m'$, then we choose $h = c_1$, $h_1 = -q_1$, $h_2 = -q_2$ and $N = m'$. For cases $q_1 \leq m' \leq q_2$ and $m' \leq q_1 \leq q_2$, the Kronecker product of a Hadamard matrix of order $2^{q_2 - m'}$ with amicable orthogonal designs (5.11) implies $h = 2^{q_2} c_1$, $h_1 = q_2 - q_1$ and $h_2 = N = 0$. Therefore, there exists an

$$AOD\left(2^n h; 2^{n+h_1} u_1, \dots, 2^{n+h_1} u_s; 2^{n+h_2} v_1, \dots, 2^{n+h_2} v_t\right),$$

for each $n \geq N$.

If β and b are not both even, then we may use Case 2 in Proposition 5.2 with the same argument. \square

Example 5.12. Let $(u_1, u_2, u_3, u_4, u_5) = (8, 12, 20, 68, 136)$ and $(v_1, v_2, v_3, v_4) = (1, 5, 7, 17)$ be the sequences in Examples 5.8 and 5.9. We have $(u'_1, u'_2, u'_3, u'_4, u'_5) = (2, 3, 5, 17, 34)$, $(v'_1, v'_2, v'_3, v'_4) = (1, 5, 7, 17)$, $q_1 = 2$, $q_2 = 0$, $c_1 = 61$ and $c_2 = 30$.

Apply Proposition 5.2 to the sequences

$$(b, a_1, a_2, a_3) = (5, 1, 2, 3) \quad \text{and} \quad (\beta + c_1 - c_2, \alpha_1, \alpha_2) = (6 + 31, 1, 2).$$

We may choose $m = \max\{4 \cdot 3 + b + 1, 4 \cdot 2 + \beta + 2\} = \max\{18, 16\} = 18$. Thus, there exists an

$$ACOD\left(2^{18} \cdot 61; 2^{18} \cdot 1_{(5)}, 2^{18} \cdot 2_{(4)}, 2^{18} \cdot 2_{(4)}^2, 2^{18} \cdot 2_{(4)}^3; 2^{18} \cdot 1_{(6)}, 2^{18} \cdot 2_{(4)}, 2^{18} \cdot 2_{(4)}^2\right),$$

and so there exists an

$$AOD\left(2^{19} \cdot 61; 2^{19} \cdot 1_{(5)}, 2^{19} \cdot 2_{(4)}, 2^{19} \cdot 2_{(4)}^2, 2^{19} \cdot 2_{(4)}^3; 2^{19} \cdot 1_{(6)}, 2^{19} \cdot 2_{(4)}, 2^{19} \cdot 2_{(4)}^2\right).$$

Equating variables, we obtain an

$$AOD\left(2^{19} \cdot 61; 2^{19} \cdot 2, 2^{19} \cdot 3, 2^{19} \cdot 5, 2^{19} \cdot 17, 2^{19} \cdot 34; 2^{19} \cdot 1, 2^{19} \cdot 5, 2^{19} \cdot 7, 2^{19} \cdot 17\right).$$

Since $q_2 \leq q_1 \leq 19$, we choose $N = 19, h = 61, h_1 = -2, h_2 = 0$, and therefore for all $n \geq 19$, there exists an

$$AOD\left(2^n \cdot 61; 2^{n-2} \cdot 8, 2^{n-2} \cdot 12, 2^{n-2} \cdot 20, 2^{n-2} \cdot 68, 2^{n-2} \cdot 136; 2^n \cdot 1, 2^n \cdot 5, 2^n \cdot 7, 2^n \cdot 17\right).$$

Example 5.13. Consider 3-tuples $(1, 1, 1)$ and $(1, 1, 1)$. Let $M_1 = \text{circ}(x_1, 0, 0)$, $M_2 = \text{circ}(0, x_2, 0)$, $N_1 = \text{circ}(y_1, 0, 0)$, $N_2 = (0, y_2, 0)$ and let $A = \{A_1, A_2, A_3, A_4\}$ and $B = \{B_1, B_2, B_3, B_4\}$ be the sets of signed permutation matrices of order 2^3 satisfying the conditions (i), (ii) and (iii) in Theorem 2.43. Suppose that H is a Hadamard matrix of order 2^3 . Then

$$C = \frac{1}{2}(M_1 + M_1^t) \otimes A_1 H + \frac{i}{2}(M_1 - M_1^t) \otimes A_2 H \\ + (M_2 + M_2^t) \otimes \frac{1}{2}(A_3 + A_4) H + i(M_2 - M_2^t) \otimes \frac{1}{2}(A_3 - A_4) H$$

and

$$D = \frac{1}{2}(N_1 + N_1^t) \otimes B_1 H + \frac{i}{2}(N_1 - N_1^t) \otimes B_2 H \\ + (N_2 + N_2^t) \otimes \frac{1}{2}(B_3 + B_4) H + i(N_2 - N_2^t) \otimes \frac{1}{2}(B_3 - B_4) H$$

after replacing $x_1 = \begin{bmatrix} a & a \\ -a & a \end{bmatrix}$, $x_2 = \begin{bmatrix} b & c \\ -c & b \end{bmatrix}$, $y_1 = \begin{bmatrix} d & d \\ -d & d \end{bmatrix}$, $y_2 = \begin{bmatrix} e & f \\ -f & e \end{bmatrix}$
and $0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ form an $ACOD(2^4 \cdot 3; 2^4, 2^4, 2^4; 2^4, 2^4, 2^4)$, and so from Lemma 5.10, one obtains an

$$AOD(2^5 \cdot 3; 2^5, 2^5, 2^5; 2^5, 2^5, 2^5).$$

We display this amicable orthogonal design in Appendix, page 110.

Remark 5.14. Applying Proposition 5.2 to the 6-tuple $(1, 1, 1, 1, 1, 1)$, there is a $COD(2^8 \cdot 6; 2_{(6)}^8)$, and so an $OD(2^9 \cdot 6; 2_{(6)}^9)$. However, in Example 5.13, $\begin{bmatrix} C & D \\ D & -C \end{bmatrix}$ is an $OD(2^5 \cdot 6; 2_{(6)}^5)$.

Chapter 6

Signed group orthogonal designs and their applications

6.1 Signed groups and remreps

Robert Craigen introduced and studied signed group Hadamard matrices in [5, 8]. In this section, we start by the definition of signed groups.

Definition 6.1 ([5]). A *signed group* S is a group with a distinguished central element of order two. We denote the unit of a group as 1 and the distinguished central element of order two as -1 . In every signed group, the set $\{1, -1\}$ is a normal subgroup, and we call the number of elements in the quotient group $S/\langle -1 \rangle$ the order of signed group S . Thus, a signed group of order n is a group of order $2n$.

A signed group T is called a *signed subgroup* of a signed group S , if T is a subgroup of S and the distinguished central elements of S and T coincide. We denote this relation by $T \leq S$. If $T \leq S$ and $T \neq S$, then T is a proper signed subgroup, and we denote it by $T < S$.

Example 6.2. Here are some important examples of signed groups:

- (i) The trivial signed group $S_{\mathbb{R}} = \{1, -1\}$ which is a signed group of order one.
- (ii) The complex signed group $S_{\mathbb{C}} = \langle i; i^2 = -1 \rangle = \{\pm 1, \pm i\}$ is a signed group of order two.
- (iii) The Quaternion signed group, S_Q , is a signed group of order 4,

$$S_Q = \langle j, k; j^2 = k^2 = -1, jk = -kj \rangle = \{ \pm 1, \pm j, \pm k, \pm jk \}.$$

- (iv) The set of all monomial $\{0, \pm 1\}$ -matrices of order n , SP_n , forms a group of order $2^n n!$ and a signed group of order $2^{n-1} n!$.

Definition 6.3 ([5]). Let S and T be two signed groups. A *signed group homomorphism* $\phi : S \rightarrow T$ is a map with the following properties

- (i) $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in S$,
- (ii) $\phi(-1) = -1$.

An *isomorphism* of signed groups is a homomorphism having an inverse map, which is also a signed group homomorphism. A *remrep* (*real monomial representation*) is a signed group homomorphism $\pi : S \rightarrow SP_n$. A *faithful remrep* is a one to one remrep.

Let R be a ring which has a unit 1_R , and let S be a signed group with distinguished central element -1_S . Then the signed group ring, $R[S]$, is defined as follows

$$R[S] = \left\{ \sum_{i=1}^n r_i s_i; \quad r_i \in R, \quad s_i \in P \right\},$$

where P is a set of coset representatives of S modulus $\langle -1_S \rangle$ and for $r \in R$, $s \in P$, we make the identification $-rs = r(-s)$. Addition is defined termwise, and multiplication is defined by linear extension. As an example $r_1 s_1 (r_2 s_2 + r_3 s_3) = r_1 r_2 s_1 s_2 + r_1 r_3 s_1 s_3$, where $r_i \in R$ and $s_i \in P$, $1 \leq i \leq 3$.

In this work, we choose $R = \mathbb{R}$. Suppose that $x \in R[S]$. Then $x = \sum_{i=1}^n r_i s_i$, where

$r_i \in R$, $s_i \in P$. The *conjugation* of x , denoted \bar{x} , is defined as $\bar{x} := \sum_{i=1}^n r_i s_i^{-1}$. Clearly, the conjugation is an involution, i.e., $\bar{\bar{x}} = x$ for all $x \in \mathbb{R}[S]$, and $\overline{xy} = \bar{y}\bar{x}$ for all $x, y \in \mathbb{R}[S]$. As an example, $\overline{\sqrt{2}j + 3jk} = \sqrt{2}j^{-1} + 3(jk)^{-1} = -\sqrt{2}j - 3jk$, where $j, k \in S_Q$.

For an $m \times n$ matrix $A = [a_{ij}]$ with entries in $\mathbb{R}[S]$ define its adjoint as an $n \times m$ matrix $A^* = \bar{A}^t = [\bar{a}_{ji}]$.

Definition 6.4. Let S be a signed group, and let $A = [a_{ij}]$ be a square matrix such that $a_{ij} \in \{0, \epsilon_1 x_1, \dots, \epsilon_k x_k\}$, where $\epsilon_\ell \in S$ and x_ℓ is a variable, $1 \leq \ell \leq k$. For each $a_{ij} = \epsilon_\ell x_\ell$ or 0, let $\bar{a}_{ij} = \bar{\epsilon}_\ell x_\ell$ or 0, and $|a_{ij}| = |\epsilon_\ell x_\ell| = x_\ell$ or 0. We define $\text{abs}(A) := [|a_{ij}|]$. We call A *quasisymmetric*, if

$$\text{abs}(A) = \text{abs}(A^*),$$

where $A^* = [\bar{a}_{ji}]$. Also, A is called *normal* if $AA^* = A^*A$.

The *support* of A (see [5]) is defined by

$$\text{supp}(A) := \{\text{positions of all nonzero entries of } A\}.$$

Definition 6.5. Suppose that $A = (a_1, a_2, \dots, a_n)$ and $B = (b_1, b_2, \dots, b_n)$ are two sequences with elements from $\{0, \epsilon_1 x_1, \dots, \epsilon_k x_k\}$, where the x_k 's are variables and $\epsilon_k \in S$ ($1 \leq k \leq n$) for some signed group S . We use $A_{\bar{R}}$ to denote the sequence whose elements are those of A , conjugated and in reverse order (see [6]), i.e., $A_{\bar{R}} = (\bar{a}_n, \dots, \bar{a}_2, \bar{a}_1)$. We say A is *quasireverse* to B if $\text{abs}(A_{\bar{R}}) = \text{abs}(B)$.

A circulant matrix $C = \text{circ}(a_1, a_2, \dots, a_n)$ can be written as

$$C = a_1 I_n + a_2 U + \dots + a_n U^{n-1},$$

where $U = \text{circ}(0, 1, 0, \dots, 0)$. Therefore, any two circulant matrices of order n with commuting entries commute. If $C = \text{circ}(a_1, a_2, \dots, a_n)$, then $C^* = \text{circ}(\bar{a}_1, \bar{a}_n, \dots, \bar{a}_2)$.

Suppose that A and B are two sequences of length n such that A is quasireverse to B .

Let $D = \text{circ}(0_{(a+1)}, A, 0_{(2b+1)}, B, 0_{(a)})$, where a and b are nonnegative integers and let $m = 2a + 2b + 2n + 2$. Then $D^* = \text{circ}(0_{(a+1)}, B_{\bar{R}}, 0_{(2b+1)}, A_{\bar{R}}, 0_{(a)})$ and

$$\text{abs}(D) = \text{abs}(D^*).$$

Hence, D is a quasisymmetric circulant matrix of order m .

Lemma 6.6. *For every positive integer of the form 2^n , there is a Golay pair $(A; B)$ of length 2^n in two variables such that each variable appears 2^{n-1} times in A and B . Moreover, A is quasireverse to B .*

Proof. The proof is similar to the proof of Lemma 5.1. The only difference is that the initial Golay sequences are $A_1 = (x, y)$ and $B_1 = (y, -x)$. \square

Theorem 6.7. *Suppose that A is an $m \times n$ and B is an $n \times r$ matrices with entries in the signed group ring $\mathbb{R}[G]$. Then $(AB)^* = B^*A^*$.*

Proof. We must show that $(AB)^*[i, j] = (B^*A^*)[i, j]$ for any fixed $1 \leq i \leq r$ and $1 \leq j \leq m$. We have

$$\begin{aligned}
(AB)^*[i, j] &= \overline{(AB)[j, i]} \\
&= \overline{\sum_{k=1}^n A[j, k]B[k, i]} \\
&= \sum_{k=1}^n \overline{A[j, k]B[k, i]} \\
&= \sum_{k=1}^n \overline{B[k, i]A[j, k]} \\
&= \sum_{k=1}^n B^*[i, k]A^*[k, j] \\
&= (B^*A^*)[i, j].
\end{aligned}$$

□

6.2 Signed group orthogonal designs

Definition 6.8. A *signed group orthogonal design*, SOD, of type (u_1, \dots, u_k) , where u_1, \dots, u_k are positive integers, and of order n , is a square matrix X of order n with entries from $\{0, \epsilon_1 x_1, \dots, \epsilon_k x_k\}$, where the x_i 's are variables and $\epsilon_j \in S$, $1 \leq j \leq k$, for some signed group S , that satisfies

$$XX^* = \left(\sum_{i=1}^k u_i x_i^2 \right) I_n.$$

We denote it by $SOD(n; u_1, \dots, u_k)$.

Equating all variables to 1 in any SOD of order n , results a *signed group weighing matrix* of order n and weight w which is denoted by $SW(n, w)$, where w is the number of nonzero entries in each row (column) of the SOD.

We call a SOD with no zero entries a full SOD. Equating all variables to 1 in any full SOD of order n results a *signed group Hadamard matrix* of order n which is denoted by $SH(n, S)$.

Craigen [5] proved the following fundamental theorem and applied it to demonstrate a novel and new method for the asymptotic existence of signed group Hadamard matrices and consequently Hadamard matrices.

Theorem 6.9. *For any odd positive integer p , there exists a circulant*

$$SH(2p, SP_{2^{2N(p)-1}}).$$

Remark 6.10. A signed group orthogonal design over the Quaternion signed group S_Q is called a *Quaternion orthogonal design*, QOD.

A signed group orthogonal design over the complex signed group S_C is called a *complex orthogonal design*, COD.

A signed group orthogonal design over the trivial signed group $S_{\mathbb{R}}$ is called an *orthogonal design*, OD.

Lemma 6.11. *Every $SW(n, w)$ over a finite signed group is normal.*

Proof. Suppose that $WW^* = wI_n$, where the entries in W belong to a signed group S of order m . We show that $WW^* = W^*W$. The space of all square matrices of order n with entries in $\mathbb{R}[S]$ has the standard basis with mn^2 elements over the field \mathbb{R} . Thus, there exists an integer u such that

$$c_1W + c_2W^2 + \cdots + c_uW^u = 0,$$

where $c_u \neq 0$, and $c_i \in \mathbb{R}$ ($1 \leq i \leq u$). Multiplying the above equality from the right

by $(W^*)^{u-1}$,

$$c_1 w(W^*)^{u-2} + c_2 w^2(W^*)^{u-3} + \cdots + c_u w^{u-1} W = 0.$$

Hence W is a polynomial in W^* , and so $WW^* = W^*W$. \square

Theorem 6.12. *A necessary and sufficient condition that there is a $SOD(n; u_1, \dots, u_k)$ over a signed group S , is that there exists a family $\{A_1, \dots, A_k\}$ of pairwise disjoint square matrices of order n with entries from $\{0, S\}$ satisfying*

$$A_i A_i^* = u_i I_n, \quad 1 \leq i \leq k, \quad (6.1)$$

$$A_i A_j^* = -A_j A_i^*, \quad 1 \leq i \neq j \leq k. \quad (6.2)$$

Proof. Suppose that there is a $A = SOD(n; u_1, \dots, u_k)$ over a signed group S . One can write

$$A = x_1 A_1 + \cdots + x_k A_k, \quad (6.3)$$

where the A_i 's are square matrices of order n with entries from $\{0, S\}$. Since the entries in A are linear monomials in the x_i , the A_i 's are disjoint. Since A is a SOD,

$$AA^* = \left(\sum_{i=1}^k u_i x_i^2 \right) I_n, \quad (6.4)$$

and so by using (6.3),

$$x_1^2 A_1 A_1^* + \cdots + x_k^2 A_k A_k^* + \sum_{i=1}^k \sum_{j=i+1}^k x_i x_j (A_i A_j^* + A_j A_i^*) = \left(\sum_{i=1}^k u_i x_i^2 \right) I_n. \quad (6.5)$$

In the above equality, for each $1 \leq i \leq k$, let $x_i = 1$ and $x_j = 0$ for all $1 \leq j \leq k$ and $j \neq i$, to get (6.1) and therefore (6.2).

On the other hand, if $\{A_1, \dots, A_k\}$ are pairwise disjoint square matrices of order

n with entries from $\{0, S\}$ which satisfy (6.1) and (6.2), then the left hand side of the equality (6.5) gives us (6.4). \square

Remark 6.13. Equation (6.4) implies Equations (6.1) and (6.2). Multiply Equation (6.2) from the left by A_i^* and then from the right by A_i to get $A_j^*A_i = -A_i^*A_j$ for $1 \leq i \neq j \leq k$. Therefore, by Lemma 6.11,

$$A^*A = x_1^2A_1^*A_1 + \cdots + x_k^2A_k^*A_k + \sum_{i=1}^k \sum_{j=i+1}^k x_ix_j(A_i^*A_j + A_j^*A_i) = \left(\sum_{i=1}^k u_ix_i^2 \right) I_n.$$

Thus, $AA^* = A^*A$. It means that every signed group orthogonal design over a finite signed group is normal.

As a corollary to Theorem 6.12, we refer the reader to Proposition 2.11.

Lemma 6.14 ([8]). *Suppose that A is a SOD over a signed group S . Then*

- (i) *Permutations of the rows or columns of A do not affect the orthogonality of A .*
- (ii) *Multiplication of each row or column of A by an element in S do not affect the orthogonality of A .*

The following lemma is shown in [5].

Lemma 6.15. *There does not exist any full SOD of order $n > 1$, if n is odd.*

Proof. Assume that there is a full SOD of order $n > 1$ over a signed group S . Equating all variables to 1 in the SOD, one obtains a $SH(n, S) = [h_{ij}]_{i,j=1}^n$. From part (ii) of Lemma 6.14, we may multiply each column of the $SH(n, S)$, from the right, by the inverse of corresponding entry of its first row, \bar{h}_{1j} , to get an equivalent $SH(n, S)$ with the first row all 1 (see [5, 6] for the definition of equivalence). By orthogonality of the rows of the $SH(n, S)$, the number of occurrences of a given element $s \in S$ in each subsequent row must be equal to the number of occurrences of $-s$. Therefore, n has to be even. \square

Lemma 6.16. *There exists no $SOD(6; 3, 3)$ and no $SOD(6; 2, 2, 2)$.*

Proof. To show that there is no $SOD(6; 3, 3)$, it suffices to prove that there is no $SW(6, 3)$. Assume that A is a $SW(6, 3)$ over a signed group S . From Lemma 6.14, we may permute the rows and columns of A to obtain

$$A_1 = \begin{bmatrix} * & * & * & 0 & 0 & 0 \\ * & & & & & \\ * & & & & & \\ 0 & & & & & \\ 0 & & & & & \\ 0 & & & & & \end{bmatrix}.$$

Using orthogonality of the first and second rows and also the first and second columns of A_1 as in the proof of Lemma 6.15 and permuting the rows and columns of A_1 , one obtains

$$A_2 = \begin{bmatrix} * & * & * & 0 & 0 & 0 \\ * & * & 0 & * & 0 & 0 \\ * & 0 & & & & \\ 0 & * & & & & \\ 0 & 0 & & & & \\ 0 & 0 & & & & \end{bmatrix}.$$

Finally, as in the proof of Lemma 6.15, orthogonality of the first and second rows with the third row of A_2 forces A_2 to be of the form

$$A_2 = \begin{bmatrix} * & * & * & 0 & 0 & 0 \\ * & * & 0 & * & 0 & 0 \\ * & 0 & * & * & 0 & 0 \\ 0 & * & & & & \\ 0 & 0 & & & & \\ 0 & 0 & & & & \end{bmatrix},$$

which contradicts orthogonality of the fifth and sixth columns of A_2 . Therefore, there is no $SOD(6; 3, 3)$.

Now suppose that B is a $SOD(6; 2, 2, 2)$ over a signed group S . By Lemma 6.14, if we permute the rows and columns of B , then we get one of the following forms:

$$\begin{bmatrix} \epsilon_{11}a & \epsilon_{12}a & \epsilon_{13}b & \epsilon_{14}b & \epsilon_{15}c & \epsilon_{16}c \\ \epsilon_{21}a & \epsilon_{22}a & \epsilon_{23}b & \epsilon_{24}b & \epsilon_{25}c & \epsilon_{26}c \\ \epsilon_{31}b & \epsilon_{32}b & \epsilon_{33}c & \epsilon_{34}c & \epsilon_{35}a & \epsilon_{36}a \\ \epsilon_{41}b & \epsilon_{42}b & \epsilon_{43}c & \epsilon_{44}c & \epsilon_{45}a & \epsilon_{46}a \\ \epsilon_{51}c & \epsilon_{52}c & \epsilon_{53}a & \epsilon_{54}a & \epsilon_{55}b & \epsilon_{56}b \\ \epsilon_{61}c & \epsilon_{62}c & \epsilon_{63}a & \epsilon_{64}a & \epsilon_{65}b & \epsilon_{66}b \end{bmatrix} \text{ or } \begin{bmatrix} \gamma_{11}a & \gamma_{12}a & \gamma_{13}b & \gamma_{14}b & \gamma_{15}c & \gamma_{16}c \\ \gamma_{21}a & \gamma_{22}a & \gamma_{23}c & \gamma_{24}c & \gamma_{25}b & \gamma_{26}b \\ \gamma_{31}b & \gamma_{32}b & \gamma_{33}a & \gamma_{34}a & \gamma_{35}c & \gamma_{36}c \\ \gamma_{41}b & \gamma_{42}b & \gamma_{43}c & \gamma_{44}c & \gamma_{45}a & \gamma_{46}a \\ \gamma_{51}c & \gamma_{52}c & \gamma_{53}a & \gamma_{54}a & \gamma_{55}b & \gamma_{56}b \\ \gamma_{61}c & \gamma_{62}c & \gamma_{63}b & \gamma_{64}b & \gamma_{65}a & \gamma_{66}a \end{bmatrix},$$

where $\epsilon_{ij}, \gamma_{ij} \in S$, $1 \leq i, j \leq 6$. For the left matrix, consider $\epsilon_{11} = \epsilon_{12} = 1$, so as in the proof of Lemma 6.15, orthogonality of the first row with the second and third rows forces ϵ_{21} to be $-\epsilon_{22}$ and ϵ_{31} to be $-\epsilon_{32}$. Thus, the second and third rows will not be orthogonal, which is a contradiction.

For the right matrix, consider $\gamma_{21} = \gamma_{22} = 1$, so as in the proof of Lemma 6.15, orthogonality of the second row with the third and sixth rows forces γ_{31} to be $-\gamma_{32}$ and γ_{61} to be $-\gamma_{62}$. Thus, the third and sixth rows will not be orthogonal, which is a contradiction. Thus, there is no $SOD(6; 2, 2, 2)$. \square

From Lemmas 6.15 and 6.16, we know that there do not exist $SOD(3; 1, 1, 1)$, $SOD(6; 2, 2, 2)$ and $SOD(9; 3, 3, 3)$. However, in the next section, we show that there exists a $SOD(12; 4, 4, 4)$ over some signed group. We will also show that for any k -tuple (u_1, \dots, u_k) of positive integers, there exists a $SOD(4u; 4u_1, \dots, 4u_k)$ over some signed group, where $u = u_1 + \dots + u_k$.

6.3 Real and complex Golay pairs in two variables

Two complementary (± 1) -sequences are called *Golay sequences* or a *Golay pair*. The length of a Golay sequence is called a *Golay number*. We denote the set of all pairs of Golay sequences of length ℓ by $GP(\ell)$. As an example, $GP(1)$ has four pairs which are pairs of real units. $GP(2)$ has eight pairs which can be obtained from the pair $A = (1, 1)$ and $B = (1, -)$ by replacing, reversing, or negating one of the sequences (see [8, 38]). Consider the following sequences:

$$A_1 = (1, 1, -, 1, -, 1, -, -, 1, 1), \quad B_1 = (1, 1, -, 1, 1, 1, 1, 1, -, -), \quad (6.6)$$

$$A_2 = (1, 1, 1, 1, -, 1, 1, -, -, 1, -, 1, -, -, 1, -, 1, 1, 1, -, -, 1, 1, 1), \quad (6.7)$$

$$B_2 = (1, 1, 1, 1, -, 1, 1, -, -, 1, -, 1, 1, 1, 1, 1, -, 1, -, -, -, 1, 1, -, -, -).$$

Then the pair $(A_1; B_1)$ is a Golay pair of length 10, and the pair $(A_2; B_2)$ is a Golay pair of length 26.

Definition 6.17. The Kronecker product of two sequences $A = (a_1, a_2, \dots, a_n)$ and $B = (b_1, b_2, \dots, b_m)$ is denoted by $A \otimes B$, and it is defined as follows

$$\begin{aligned} A \otimes B &= (a_1 B, a_2 B, \dots, a_n B) \\ &= (a_1 b_1, a_1 b_2, \dots, a_1 b_m, a_2 b_1, a_2 b_2, \dots, a_2 b_m, \dots, a_n b_1, a_n b_2, \dots, a_n b_m). \end{aligned}$$

The following theorem, described by Turyn [48], shows how a Golay pair of length mn can be constructed from Golay pairs of lengths m and n .

Theorem 6.18. *If $(A; B)$ is a Golay pair of length m and $(C; D)$ is a Golay pair of length n , then*

$$\left(\frac{1}{2}(A+B) \otimes C + \frac{1}{2}(A-B) \otimes D_{\overline{R}}; \frac{1}{2}(A+B) \otimes D - \frac{1}{2}(A-B) \otimes C_{\overline{R}} \right)$$

is a Golay pair of length mn .

By using this theorem, all numbers of the form $2^a 10^b 26^c$ are Golay numbers. These are the only Golay numbers found until 2013. All Golay numbers up to 100 were considered in [3]. In [16], it is shown that no Golay number is divisible by a number congruent to 3 modulo 4.

We denote by $GP(n; x, y)$, the set of all Golay pairs of length n such that each Golay pair has two variables x and y in such away that each variable appears $\frac{n}{2}$ times in each of the sequences of the Golay pair, and also one sequence is quasireverse to the other. As an example, $(A; B) \in GP(2; x, y)$, where $A = (x, y)$ and $B = (y, -x)$.

We distinguish between the definition of $GP(n; x, y)$ and $GP(1; x, y)$. So if $A = (x)$ and $B = (y)$, then we say $(A; B) \in GP(1; x, y)$.

The Golay pairs of lengths 10 and 26 in (6.6) and (6.7) have the nice property that $\frac{1}{2}(A_j + B_j)$ is quasireverse to $\frac{1}{2}(A_j - B_j)$, $j = 1, 2$. We may modify Theorem 6.18 to show the following Theorem.

Theorem 6.19. *Suppose that $(C; D)$ is a Golay pair of length n in two variables. Then*

$$\left(\frac{1}{2}(A+B) \otimes C + \frac{1}{2}(A-B) \otimes D_{\overline{R}}; \frac{1}{2}(A+B) \otimes D - \frac{1}{2}(A-B) \otimes C_{\overline{R}} \right)$$

is a Golay pair of length mn in two variables, where A and B are one of the followings

- $m = 2$, $A = (1, 1)$ and $B = (1, -)$,
- $m = 10$, $A = A_1$ and $B = B_1$ in (6.6),
- $m = 26$, $A = A_2$ and $B = B_2$ in (6.7).

Example 6.20. Suppose that $(A_1; B_1)$ and $(A_2; B_2)$ are the Golay pairs in (6.6) and (6.7), and $C = (x)$ and $D = (y)$. Also, let $A_3 = (1, 1)$ and $B_3 = (1, -)$. For $j = 1, 2, 3$, let

$$\begin{aligned} C_j &= \frac{1}{2}(A_j + B_j) \otimes C + \frac{1}{2}(A_j - B_j) \otimes D_{\overline{R}}, \\ D_j &= \frac{1}{2}(A_j + B_j) \otimes D - \frac{1}{2}(A_j - B_j) \otimes C_{\overline{R}}. \end{aligned}$$

Therefore,

$$\begin{aligned} C_1 &= (x, x, -x, x, -y, x, -y, -y, y, y), & D_1 &= (y, y, -y, y, x, y, x, x, -x, -x), \\ C_2 &= (x, x, x, x, -x, x, x, -x, -x, x, -x, x, -y, x, -y, -y, y, -y, y, y, y, -y, -y, y, y, y), \\ D_2 &= (y, y, y, y, -y, y, y, -y, -y, y, -y, y, x, y, x, x, -x, x, -x, -x, -x, x, x, -x, -x, -x), \\ C_3 &= (x, y), & D_3 &= (y, -x). \end{aligned}$$

We observe that for $j = 1, 2, 3$, $\text{abs}(C_{j\overline{R}}) = \text{abs}(D_j)$. Thus, $(C_1; D_1) \in GP(10; x, y)$, $(C_2; D_2) \in GP(26; x, y)$ and $(C_3; D_3) \in GP(2; x, y)$.

Using Theorem 6.19 and induction with the initial Golay pairs $(C_j; D_j)$, $j = 1, 2, 3$, in the above example, one has the following.

Corollary 6.21. *The set $GP(n; x, y)$ is not empty for each $n = 2^a 10^b 26^c$, where a, b and c are non-negative integers.*

Two complementary $(\pm 1, \pm i)$ -sequences are called *complex Golay sequences* or a *complex Golay pair*. The length of a complex Golay sequence is called a *complex Golay number*. We denote the set of all pairs of Golay sequences of length ℓ by $CGP(\ell)$. If $(A; B)$ is a complex Golay pair, then $(xA; xB)$ is called a *complex Golay pair in one variable*, where x is a variable. The following complex Golay sequences of length p are known.

$$\begin{aligned}
p = 2; & \quad A = (1, 1), & \quad B = (1, -), \\
p = 3; & \quad A_1 = (1, 1, -), & \quad B_1 = (1, i, 1), \\
p = 5; & \quad A_2 = (i, i, 1, -, 1), & \quad B_2 = (i, 1, 1, i, -), \\
p = 11; & \quad A_3 = (1, i, -, 1, -, i, \bar{i}, -, i, i, 1), \\
& \quad B_3 = (1, 1, \bar{i}, \bar{i}, \bar{i}, 1, 1, i, -, 1, -), \\
p = 13; & \quad A_4 = (1, 1, 1, i, -, 1, 1, \bar{i}, 1, -, 1, \bar{i}, i), \\
& \quad B_4 = (1, i, -, -, -, i, -, 1, 1, \bar{i}, -, 1, \bar{i}),
\end{aligned}$$

Complex Golay sequences of lengths 11 and 13 were found in [6, 22]. We extended the group $\{\pm 1, \pm i\}$ to the group of eighth roots of unity, i.e,

$$S = \left\{ e^{\frac{k\pi i}{4}}; 0 \leq k < 8, k \text{ is an integer} \right\},$$

and by an exhaustive computer search could not find any Golay sequences over S of lengths 7 and 9.

Some constructions that work for Golay sequences can be generalized to the complex case.

Theorem 6.22 ([4]). *If $(A; B)$ is a complex Golay pair of length m and $(C; D)$ is a*

complex Golay pair of length n , then

$$\left((A \otimes C, B \otimes D_{\overline{R}}); (A \otimes D, -B \otimes C_{\overline{R}}) \right)$$

is a complex Golay pair of length $2mn$. Moreover, if A and B are real, then

$$\left(\frac{1}{2}(A+B) \otimes C + \frac{1}{2}(A-B) \otimes D_{\overline{R}}; \frac{1}{2}(A+B) \otimes D - \frac{1}{2}(A-B) \otimes C_{\overline{R}} \right)$$

is a complex Golay pair of length mn .

Craigen, Holzmann and Kharaghani in [6] showed that if g_1 and g_2 are complex Golay numbers and g is a Golay number, then gg_1g_2 is a complex Golay number. Using this, they showed the following theorem.

Theorem 6.23. *All numbers of the form $m = 2^{a+u}3^b5^c11^d13^e$ are complex Golay numbers, where a, b, c, d, e and u are non-negative integers such that $u \leq c + e$ and $b + c + d + e \leq a + 2u + 1$.*

By an exhaustive computer search in [6], they could also show that there is no complex Golay pair of lengths 7, 9, 15, 17, 19 and 21. However, other complex Golay numbers may exist.

We use $CGP(n; x, y)$ to denote the set of all complex Golay pairs of length n such that each pair has two variables x and y such that each variable appears $\frac{n}{2}$ times in each sequence of the complex Golay pair, and also one sequence is quasireverse to the other. $CGP(n; x, y)$ is well defined when $n > 1$ is an even number. From Theorem 6.22, we have the following.

Lemma 6.24. *Assume that $(A; B)$ is a complex Golay pair of length m . Then $((xA, yB); (yA, -xB))$ is a complex Golay pair of length $2m$ in variables x and y .*

From Theorem 6.23 and Lemma 6.24, we have the following result.

Corollary 6.25. *The set $CGP(n; x, y)$ is not empty for each $n = 2^{a+u+1}3^b5^c11^d13^e$ where a, b, c, d, e and u are non-negative integers such that $b + c + d + e \leq a + 2u + 1$ and $u \leq c + e$.*

6.4 Some applications of signed group orthogonal designs

In this section, we adapt the methods of I. Livinsky [38] to obtain generalizations and improvements of his results about Hadamard matrices in the much more general setting of orthogonal designs.

Suppose that we have a remrep $\pi : S \rightarrow SP_m$. We extend this remrep to a ring homomorphism $\pi : \mathbb{R}[S] \rightarrow M_m[\mathbb{R}]$ linearly by

$$\pi(r_1s_1 + \cdots + r_ns_n) = r_1\pi(s_1) + \cdots + r_n\pi(s_n).$$

Since for every matrix $A \in SP_m$ we have $A^{-1} = A^t$, for every $s \in S$ we have $\pi(\bar{s}) = \pi(s)^{-1} = \pi(s)^t$. In the following Theorem, we show how one can obtain OD's from SOD's by using remreps.

Theorem 6.26. *Suppose that there exists a $SOD(n; u_1, \dots, u_k)$ for some signed group S equipped with a remrep π of degree m , where m is the order of a Hadamard matrix. Then there is an $OD(mn; mu_1, \dots, mu_k)$.*

Proof. Suppose there exists a $SOD(n; u_1, \dots, u_k)$ for some signed group S . By Theorem 6.12, there are pairwise disjoint matrices A_1, \dots, A_k of order n with entries in

$\{0, S\}$ such that

$$A_\alpha A_\alpha^* = u_\alpha I_n, \quad 1 \leq \alpha \leq k, \quad (6.8)$$

$$A_\alpha A_\beta^* = -A_\beta A_\alpha^*, \quad 1 \leq \alpha \neq \beta \leq k. \quad (6.9)$$

Let $\pi : S \rightarrow SP_m$ be a remrep of degree m , and H be a Hadamard matrix of degree m . Also, for each $1 \leq \alpha \leq k$, let

$$B_\alpha = \left[\pi(A_\alpha[i, j]) H \right]_{i, j=1}^n.$$

By Proposition 2.11, it is sufficient to show that B_α 's are pairwise disjoint matrices of order mn , with $\{0, \pm 1\}$ entries such that

$$B_\alpha B_\alpha^t = m u_\alpha I_{mn}, \quad 1 \leq \alpha \leq k, \quad (6.10)$$

$$B_\alpha B_\beta^t = -B_\beta B_\alpha^t, \quad 1 \leq \alpha \neq \beta \leq k. \quad (6.11)$$

Since A_α 's are pairwise disjoint, so are B_α 's. Let $1 \leq \alpha \neq \beta \leq k$ and $1 \leq i, j \leq n$.

Then

$$\begin{aligned} (B_\alpha B_\beta^t)[i, j] &= \sum_{k=1}^n \pi(A_\alpha[i, k]) H H^t \pi(A_\beta[j, k])^t \\ &= m \sum_{k=1}^n \pi(A_\alpha[i, k]) \pi(\overline{A_\beta}[j, k]) \\ &= m \pi \left(\sum_{k=1}^n A_\alpha[i, k] \overline{A_\beta}[j, k] \right) \\ &= m \pi \left((A_\alpha A_\beta^*)[i, j] \right) \end{aligned} \quad (6.12)$$

$$\begin{aligned} &= m \pi \left((-A_\beta A_\alpha^*)[i, j] \right) \quad \text{from (6.9)} \\ &= -m \pi \left((A_\beta A_\alpha^*)[i, j] \right) \end{aligned} \quad (6.13)$$

On the other hand, similarly,

$$\begin{aligned}
(B_\beta B_\alpha^t)[i, j] &= \sum_{k=1}^n \pi(A_\beta[i, k]) H H^t \pi(A_\alpha[j, k])^t \\
&= m \sum_{k=1}^n \pi(A_\beta[i, k]) \pi(\bar{A}_\alpha[j, k]) \\
&= m \pi\left(\sum_{k=1}^n A_\beta[i, k] \bar{A}_\alpha[j, k]\right) \\
&= m \pi\left((A_\beta A_\alpha^*)[i, j]\right). \tag{6.14}
\end{aligned}$$

Thus, (6.13) and (6.14) are equal, which proves (6.11). If $\alpha = \beta$ in (6.12), then for $1 \leq i, j \leq n$,

$$\begin{aligned}
(B_\alpha B_\alpha^t)[i, j] &= m \pi\left((A_\alpha A_\alpha^*)[i, j]\right) \\
&= m \pi(\gamma_{ij} u_\alpha \cdot 1_S) \quad \text{from (6.8)} \\
&= m \gamma_{ij} u_\alpha I_m,
\end{aligned}$$

where $\gamma_{ij} = 1$ if $i = j$, and 0 otherwise. Whence (6.10) follows. \square

Corollary 6.27. *If there is a COD($n; u_1, \dots, u_k$), then there is an OD($2n; 2u_1, \dots, 2u_k$).*

Proof. A COD($n; u_1, \dots, u_k$) can be viewed as a SOD($n; u_1, \dots, u_k$) over the complex signed group $S_{\mathbb{C}}$. It can be seen that $\pi : S_{\mathbb{C}} \rightarrow SP_2$ defined by

$$i \longrightarrow R = \begin{bmatrix} 0 & 1 \\ - & 0 \end{bmatrix}$$

is a remrep of degree 2, and so by Theorem 6.26, there exists an OD($2n; 2u_1, \dots, 2u_k$). \square

Corollary 6.28. *If there is a QOD($n; u_1, \dots, u_k$), then there is an OD($4n; 4u_1, \dots, 4u_k$).*

Proof. A QOD($n; u_1, \dots, u_k$) can be viewed as a SOD($n; u_1, \dots, u_k$) over the Quaternion signed group S_Q . It can be seen that $\pi : S_Q \rightarrow SP_4$ defined by

$$j \longrightarrow R \otimes I_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ - & 0 & 0 & 0 \\ 0 & - & 0 & 0 \end{bmatrix} \quad \text{and} \quad k \longrightarrow P \otimes R = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & - & 0 \\ 0 & 1 & 0 & 0 \\ - & 0 & 0 & 0 \end{bmatrix},$$

is a remrep of degree 4, and so by Theorem 6.26, there exists an OD($4n; 4u_1, \dots, 4u_k$).

□

Following similar techniques in [5, 7, 38], we have the following Lemma.

Lemma 6.29. *Suppose that A and B are two disjoint circulant matrices of order d with entries from $\{0, \epsilon_1 x_1, \dots, \epsilon_k x_k\}$, where the x_ℓ 's are variables, $\epsilon_\ell \in S$ ($1 \leq \ell \leq k$) for A and $\epsilon_\ell \in Z(S)$, the center of S , ($1 \leq \ell \leq k$) for B . Also, assume A is normal.*

If

$$C = \begin{bmatrix} A + B & A - B \\ A^* - B^* & -A^* - B^* \end{bmatrix},$$

then $CC^ = C^*C = 2I_2 \otimes (AA^* + BB^*)$.*

Moreover, if A and B are both quasisymmetric and S has a faithful remrep of degree m , then there exists a circulant quasisymmetric normal matrix D of order d with entries from $\{0, \epsilon'_1 x_1, \dots, \epsilon'_k x_k\}$ and the same support as $A+B$ such that $DD^ = AA^* + BB^*$, where $\epsilon'_\ell \in S'$ ($1 \leq \ell \leq k$), and $S' \geq S$ is a signed group having a faithful remrep of degree $2m$.*

Proof. It may be verified directly that $CC^* = C^*C = 2I_2 \otimes (AA^* + BB^*)$. To find matrix D , first reorder the rows and columns of C to get matrix D_0 which is a

partitioned matrix of order $2d$ into 2×2 blocks whose entries are the (i, j) , $(i + d, j)$, $(i, j + d)$ and $(i + d, j + d)$ entries of C , $1 \leq i, j \leq d$. Applying the same reordering to $2I_2 \otimes (AA^* + BB^*)$, one obtains $(AA^* + BB^*) \otimes 2I_2$. Since A and B are disjoint and quasisymmetric, each non-zero block of D_0 will have one of the following forms

$$\begin{bmatrix} \epsilon_i x_i & \epsilon_i x_i \\ \epsilon_j x_i & -\epsilon_j x_i \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} \epsilon_i x_i & -\epsilon_i x_i \\ \epsilon_j x_i & \epsilon_j x_i \end{bmatrix},$$

where $\epsilon_\ell \in S$. Multiplying D_0 on the right by $\frac{1}{2}I_d \otimes \begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix}$ yields a matrix D_1 of order $2d$ with entries from $\{0, \epsilon_1 x_1, \dots, \epsilon_k x_k\}$ whose non-zero 2×2 blocks have one of the forms $A_i x_i$ or $B_i x_i$, where

$$A_i = \begin{bmatrix} \epsilon_i & 0 \\ 0 & \epsilon_j \end{bmatrix} \quad \text{or} \quad B_i = \begin{bmatrix} 0 & \epsilon_i \\ \epsilon_j & 0 \end{bmatrix}, \quad (6.15)$$

and such that $D_1 D_1^* = D_1^* D_1 = (AA^* + BB^*) \otimes I_2$. The A_i 's and B_i 's in (6.15) form another signed group, S' . Now matrices of the form

$$\epsilon \otimes I_2 = \begin{bmatrix} \epsilon & 0 \\ 0 & \epsilon \end{bmatrix}, \quad \epsilon \in S,$$

form a signed subgroup of S' which is isomorphic to S . Therefore, one can identify this signed subgroup with S itself and consider S' as an extension of S . Replacing every 2×2 block of D_1 which is one the forms in (6.15) or zero with corresponding $\epsilon'_i x_i$, $\epsilon'_i \in S'$ or zero, gives the required matrix D . Note that we identify $\epsilon \otimes I_2 \in S'$ with $\epsilon \in S$.

Now if $\pi : S \rightarrow SP'_m \leq SP_m$ is a faithful remrep of degree m , then it can be

verified directly that the map $\pi' : S' \rightarrow SP'_{2m} \leq SP_{2m}$ which is uniquely defined by

$$\begin{bmatrix} \epsilon_i & 0 \\ 0 & \epsilon_j \end{bmatrix} \rightarrow \begin{bmatrix} \pi(\epsilon_i) & 0_m \\ 0_m & \pi(\epsilon_j) \end{bmatrix}, \quad \begin{bmatrix} 0 & \epsilon_i \\ \epsilon_j & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 0_m & \pi(\epsilon_i) \\ \pi(\epsilon_j) & 0_m \end{bmatrix},$$

is a faithful remrep of degree $2m$, where 0_m denotes the zero matrix of order m .

Finally, since A and B are circulant, C consists of four circulant blocks, so D_0 and D_1 are block-circulant with block size 2×2 ; whence D is circulant and quasisymmetric. \square

We now use Lemma 6.29, and follow similar techniques in [5, 38] to show the following Theorem.

Theorem 6.30. *Suppose that B_1, \dots, B_n are disjoint quasisymmetric circulant matrices of order d with entries from $\{0, \epsilon_1 x_1, \dots, \epsilon_k x_k\}$, where $\epsilon_\ell \in S_{\mathbb{C}}$, and the x_ℓ 's are variables ($1 \leq \ell \leq k$), such that*

$$B_1 B_1^* + \dots + B_n B_n^* = \left(\sum_{\ell=1}^k u_\ell x_\ell^2 \right) I_d,$$

where the u_ℓ 's are positive integers. Then there exists a quasisymmetric circulant $SOD(d; u_1, \dots, u_k)$ for a signed group S that admits a faithful remrep of degree 2^n .

Proof. $S_{\mathbb{C}}$ has a faithful remrep $\pi : S_{\mathbb{C}} \rightarrow SP'_2 \leq SP_2$ of degree 2 uniquely determined by $\pi(i) = R$, where $SP'_2 = \langle R; R^2 = -I \rangle$. Applying Lemma 6.29 to matrices B_1 and B_2 , one obtains a quasisymmetric normal circulant matrix A_1 of order d with entries from $\{0, \epsilon_1^{(1)} x_1, \dots, \epsilon_k^{(1)} x_k\}$, where $\epsilon_\ell^{(1)} \in S_1$ ($1 \leq \ell \leq k$) such that $S_1 \geq S_{\mathbb{C}}$ is a signed group with a faithful remrep of degree 2^2 . Also, $A_1 A_1^* = B_1 B_1^* + B_2 B_2^*$. Since $\text{supp}(A_1)$ is the union of $\text{supp}(B_1)$ and $\text{supp}(B_2)$, A_1 is disjoint from B_3, \dots, B_n .

Suppose that one has constructed a circulant quasisymmetric normal matrix A_r

of order d with entries from $\{0, \epsilon_1^{(r)}x_1, \dots, \epsilon_k^{(r)}x_k\}$, where $\epsilon_\ell^{(r)} \in S_r$ ($1 \leq \ell \leq k$) such that $S_r \geq S_{r-1}$ is a signed group with a faithful remrep $\pi_r : S_r \rightarrow SP'_{2^{r+1}} \leq SP_{2^{r+1}}$ of degree 2^{r+1} . Moreover, A_r is disjoint from B_{r+2}, \dots, B_n and

$$A_r A_r^* = B_1 B_1^* + \dots + B_{r+1} B_{r+1}^*.$$

By the assumption, B_{r+2} is a quasisymmetric normal circulant matrix with entries from $\{0, \epsilon_1 x_1, \dots, \epsilon_k x_k\}$, where $\epsilon_\ell \in S_{\mathbb{C}}$ ($1 \leq \ell \leq k$). One can view the ϵ_ℓ 's as elements in $Z(S_r)$ because we identified these elements as blocks $\pm I_{2^r} \otimes R$ and $\pm I_{2^{r+1}}$ in the proof of Lemma 6.29 which commute with $\pi_r(\epsilon_\ell^{(r)})$, $1 \leq \ell \leq k$. Therefore, by Lemma 6.29, there is a quasisymmetric normal circulant matrix A_{r+1} with entries from $\{0, \epsilon_1^{(r+1)}x_1, \dots, \epsilon_k^{(r+1)}x_k\}$, where $\epsilon_\ell^{(r+1)} \in S_{r+1}$ ($1 \leq \ell \leq k$) such that $S_{r+1} \geq S_r$ is a signed group with a faithful remrep of degree 2^{r+2} . Also,

$$A_{r+1} A_{r+1}^* = A_r A_r^* + B_{r+2} B_{r+2}^* = B_1 B_1^* + \dots + B_{r+1} B_{r+1}^* + B_{r+2} B_{r+2}^*,$$

and by the same argument A_{r+1} is disjoint from B_{r+3}, \dots, B_n .

Applying this procedure $n - 2$ times, there is a quasisymmetric normal circulant matrix A_{n-1} of order d such that

$$A_{n-1} A_{n-1}^* = B_1 B_1^* + \dots + B_n B_n^* = \left(\sum_{\ell=1}^k u_\ell x_\ell^2 \right) I_d,$$

which is a circulant quasisymmetric $SOD(d; u_1, \dots, u_k)$ with the signed group

$S = S_{n-1} \geq S_{n-2} \geq \dots \geq S_{\mathbb{C}}$ that admits a faithful remrep of degree 2^n . \square

Remark 6.31. The circulant matrices in Theorem 6.30 are taken on the abelian signed group $S_{\mathbb{C}}$; however, if the signed group is not abelian, the circulant matrices that obtain from Lemma 6.29 do not necessarily commute, and Theorem 6.30 may

fail. As an example, if $B_1 = \text{circ}(j, 0)$ and $B_2 = \text{circ}(0, k)$, where $j, k \in S_Q$, then since $jk = -kj$, $B_1B_2 \neq B_2B_1$. Therefore, Lemma 6.29 does not apply in this case.

Theorem 6.32. *Suppose that B_1, \dots, B_n are disjoint quasisymmetric circulant matrices of order d with entries from $\{0, \epsilon_1x_1, \dots, \epsilon_kx_k\}$, where $\epsilon_\ell \in S_{\mathbb{R}}$, and the x_ℓ 's are variables ($1 \leq \ell \leq k$), such that*

$$B_1B_1^* + \dots + B_nB_n^* = \left(\sum_{\ell=1}^k u_\ell x_\ell^2 \right) I_d,$$

where the u_ℓ 's are positive integers. Then there exists a circulant quasisymmetric $SOD(d; u_1, \dots, u_k)$ for a signed group S that admits a faithful remrep of degree 2^{n-1} .

Proof. Similar to the proof of Theorem 6.30, but in here since $S_{\mathbb{R}}$ has the trivial remrep of degree 1, the final signed group S will have a remrep of degree 2^{n-1} . \square

Example 6.33. We explain how to use Theorem 6.32 to find a $SOD(12; 4, 4, 4)$ for a signed group S that admits a remrep of degree 8. Consider the following disjoint quasisymmetric circulant matrices of order 12:

$$B_1 = \text{circ}(a, 0, 0, 0, 0, 0, a, 0, 0, 0, 0, 0),$$

$$B_2 = \text{circ}(0, 0, 0, a, 0, 0, 0, 0, 0, 0, -a, 0),$$

$$B_3 = \text{circ}(0, b, c, 0, 0, 0, 0, 0, 0, 0, c, -b),$$

$$B_4 = \text{circ}(0, 0, 0, 0, c, -b, 0, -b, -c, 0, 0, 0).$$

Thus, $B_1B_1^* + B_2B_2^* + B_3B_3^* + B_4B_4^* = (4a^2 + 4b^2 + 4c^2)I_{12}$. Apply Lemma 6.29 to B_1 and B_2 to get a quasisymmetric normal circulant matrix of order 12:

$$A_1 = \text{circ}(1a, 0, 0, \delta a, 0, 0, 1a, 0, 0, -\delta a, 0, 0),$$

where δ is in the signed group of order 2:

$$S_1 = \langle -1, \delta; \delta^2 = 1 \rangle$$

which admits a remrep of degree 2 uniquely determined by $1 \rightarrow I_2$ and $\delta \rightarrow P$. Since B_1 and B_2 are complementary, it follows that $A_1 A_1^* = 4a^2 I_{12}$.

Applying Lemma 6.29 again to A_1 and B_3 , there is a quasisymmetric normal circulant matrix of order 12:

$$A_1 = \text{circ}(1a, \gamma_1 b, \gamma_2 c, \gamma_3 a, 0, 0, 1a, 0, 0, -\gamma_3 a, \gamma_2 c, -\gamma_1 b),$$

where $\gamma_1, \gamma_2, \gamma_3$ belong to the signed group of order 2^3 :

$$S_2 = \langle \gamma_1, \gamma_2, \gamma_3; \gamma_1^2 = -\gamma_2^2 = \gamma_3^2 = 1, \alpha\beta = -\beta\alpha; \alpha, \beta \in \{\gamma_1, \gamma_2, \gamma_3\} \rangle,$$

with a remrep of degree 4 which is uniquely determined by

$$\gamma_1 \rightarrow P \otimes I_2, \quad \gamma_2 \rightarrow R \otimes I_2, \quad \gamma_3 \rightarrow Q \otimes P.$$

Note that A_2 is not a SOD because B_1, B_2 and B_3 are not complementary.

Finally, apply Lemma 6.29 to A_2 and B_4 to get a quasisymmetric normal circulant matrix of order 12:

$$A_3 = \text{circ}(1a, \epsilon_1 b, \epsilon_2 c, \epsilon_3 a, \epsilon_4 c, -\epsilon_5 b, 1a, -\epsilon_5 b, -\epsilon_4 c, -\epsilon_3 a, \epsilon_2 c, -\epsilon_1 b),$$

where ϵ_j , $1 \leq j \leq 5$ belong to the signed group of order 2^5 :

$$S = \langle \epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4, \epsilon_5; \epsilon_1^2 = -\epsilon_2^2 = \epsilon_3^2 = \epsilon_4^2 = -\epsilon_5^2 = 1, \alpha\beta = -\beta\alpha; \alpha, \beta \in \{\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4, \epsilon_5\} \rangle,$$

with a remrep of degree 8 which is uniquely determined by

$$\epsilon_1 \rightarrow Q \otimes P \otimes I_2, \quad \epsilon_2 \rightarrow Q \otimes R \otimes I_2, \quad \epsilon_3 \rightarrow Q \otimes Q \otimes P, \quad \epsilon_4 \rightarrow P \otimes I_2 \otimes I_2, \quad \epsilon_5 \rightarrow R \otimes I_2 \otimes I_2.$$

Therefore, A_3 is a quasisymmetric circulant $SOD(12; 4, 4, 4)$. By Theorem 6.26, there is an $OD(8 \cdot 12; 8 \cdot 4, 8 \cdot 4, 8 \cdot 4)$.

For u a positive integer, denote by $lc(u)$ the least number of complex Golay numbers that add up to u . Let $lc(0) = 0$. Also, denote by $l'c(u)$ the least number of complex Golay numbers in two variables that add up to u . Indeed, $l'c(2u) \leq lc(u)$. Note that Lemma 6.24 insures the existence of a complex Golay pair in two variables of length $2m$ if there exists a complex Golay pair of length m .

In the following lemma, we show how to use complex Golay pair and complex Golay pairs in two variables to construct SODs.

Lemma 6.34. *Let $(1, v_1, \dots, v_q, w_1, w_1, \dots, w_t, w_t)$ be a sequence of positive integers, where $1 \leq v_1 < \dots < v_q$ and let*

$$1 + \sum_{\beta=1}^q v_{\beta} + 2 \sum_{\delta=1}^t w_{\delta} = u.$$

Then there exists a full circulant quasisymmetric

$$SOD(4u; 4, 4v_1, \dots, 4v_q, 4w_1, 4w_1, \dots, 4w_t, 4w_t)$$

for some signed group S that admits a remrep of degree 2^n , where

$$n \leq 2 + 2 \sum_{\beta=1}^q lc(v_{\beta}) + 2 \sum_{\delta=1}^t lc(w_{\delta}).$$

Proof. For each β , $1 \leq \beta \leq q$, and each α , $1 \leq \alpha \leq lc(v_{\beta})$, let $(A[\alpha, v_{\beta}]; B[\alpha, v_{\beta}])$ be

a complex Golay pair in one variable, x_β , of length $V[\alpha, v_\beta]$. From the definition of $\ell c(v_\beta)$, for each β , $1 \leq \beta \leq q$, $\sum_{\alpha=1}^{\ell c(v_\beta)} V[\alpha, v_\beta] = v_\beta$. Let

$$S[\alpha, \beta] := \sum_{i=1}^{\alpha-1} V[i, v_\beta] + \sum_{j=1}^{\beta-1} v_j.$$

Also, for each δ , $1 \leq \delta \leq t$, and each γ , $1 \leq \gamma \leq \ell'c(2w_\delta)$, let $(C[\gamma, w_\delta]; D[\gamma, w_\delta])$ be a complex Golay pair of length $W[\gamma, w_\delta]$ in two variables y_δ and z_δ . From the definition of $\ell'c(2w_\delta)$, for each δ , $1 \leq \delta \leq t$, $\sum_{\gamma=1}^{\ell'c(2w_\delta)} W[\gamma, w_\delta] = 2w_\delta$. Let

$$S'[\gamma, \delta] := \sum_{i=1}^{\gamma-1} W[i, w_\delta] + 2 \sum_{j=1}^{\delta-1} w_j.$$

For each β , $1 \leq \beta \leq q$, and each α , $1 \leq \alpha \leq \ell c(v_\beta)$, and for each δ , $1 \leq \delta \leq t$ and each γ , $1 \leq \gamma \leq \ell'c(2w_\delta)$, the following are $n = 2 + 2 \sum_{\beta=1}^q \ell c(v_\beta) + 2 \sum_{\delta=1}^t \ell'c(2w_\delta)$ circulant matrices of order $4u$:

$$\begin{aligned} M_1 &= \text{circ}\left(x, 0_{(2u-1)}, x, 0_{(2u-1)}\right), \\ M_2 &= \text{circ}\left(0_{(u)}, -x, 0_{(2u-1)}, x, 0_{(u-1)}\right), \\ X_{\alpha\beta} &= \text{circ}\left(0_{(S[\alpha,\beta]+1)}, A[\alpha, v_\beta], 0_{(4u-2S[\alpha+1,\beta]-1)}, B[\alpha, v_\beta], 0_{(S[\alpha,\beta])}\right), \\ Y_{\alpha\beta} &= \text{circ}\left(0_{(2u-S[\alpha+1,\beta])}, -B[\alpha, v_\beta], 0_{(2S[\alpha,\beta]+1)}, A[\alpha, v_\beta], 0_{(2u-S[\alpha+1,\beta]-1)}\right), \\ Z_{\gamma\delta} &= \text{circ}\left(0_{(v+S'[\gamma,\delta]+1)}, C[\gamma, w_\delta], 0_{(4u-2v-2S'[\gamma+1,\delta]-1)}, D[\gamma, w_\delta], 0_{(v+S'[\gamma,\delta])}\right), \\ T_{\gamma\delta} &= \text{circ}\left(0_{(2u-v-S'[\gamma+1,\delta])}, -D[\gamma, w_\delta], 0_{(2S'[\gamma,\delta]+2v+1)}, C[\gamma, w_\delta], 0_{(2u-v-S'[\gamma+1,\delta]-1)}\right). \end{aligned}$$

It can be directly seen that the above circulant matrices are disjoint and quasisymmetric such that

$$\begin{aligned}
& \sum_{i=1}^2 M_i M_i^* + \sum_{\beta=1}^q \sum_{\alpha=1}^{\ell c(v_\beta)} (X_{\alpha\beta} X_{\alpha\beta}^* + Y_{\alpha\beta} Y_{\alpha\beta}^*) + \sum_{\delta=1}^t \sum_{\gamma=1}^{\ell' c(2w_\delta)} (Z_{\gamma\delta} Z_{\gamma\delta}^* + T_{\gamma\delta} T_{\gamma\delta}^*) \\
&= 4 \left(x^2 + \sum_{\beta=1}^q (v_\beta x_\beta^2) + \sum_{\delta=1}^t (w_\delta y_\delta^2 + w_\delta z_\delta^2) \right) I_{4u}.
\end{aligned}$$

Thus, by Theorem 6.30, there exists a full circulant quasisymmetric

$$SOD(4u; 4, 4v_1, \dots, 4v_q, 4w_1, 4w_1, \dots, 4w_t, 4w_t)$$

for a signed group S which admits a remrep of degree 2^n , where

$$n = 2 + 2 \sum_{\beta=1}^q \ell c(v_\beta) + 2 \sum_{\delta=1}^t \ell' c(2w_\delta) \leq 2 + 2 \sum_{\beta=1}^q \ell c(v_\beta) + 2 \sum_{\delta=1}^t \ell c(w_\delta).$$

□

Example 6.35. Consider the 4-tuple $(1, v_1, v_2, v_3) = (1, 5, 7, 17)$. By Lemma 6.34, there is a circulant quasisymmetric

$$SOD(4 \cdot 30; 4 \cdot 1, 4 \cdot 5, 4 \cdot 7, 4 \cdot 17),$$

which admits a remrep of degree 2^n , where $n = 2 + 2\ell c(5) + 2\ell c(7) + 2\ell c(17) = 2 + 2 + 4 + 4 = 12$. By Theorem 6.26, there is an

$$OD(2^{14} \cdot 30; 2^{14} \cdot 1, 2^{14} \cdot 5, 2^{14} \cdot 7, 2^{14} \cdot 17).$$

Therefore, for the 4-tuple $(1, 5, 7, 17)$, we found an integer m , $m = 14$, such that there is an $OD(2^m \cdot 30; 2^m \cdot 1, 2^m \cdot 5, 2^m \cdot 7, 2^m \cdot 17)$. In Example 5.9, it can be seen that $m = 17$.

Example 6.36. Let $(1, w_1, w_1, w_2, w_2, w_3, w_3, w_4, w_4) = (1, 3, 3, 5, 5, 11, 11, 13, 13)$. By Lemma 6.34, there is a circulant quasisymmetric

$$SOD(4 \cdot 65; 4 \cdot 1, 4 \cdot 3_{(2)}, 4 \cdot 5_{(2)}, 4 \cdot 11_{(2)}, 4 \cdot 13_{(2)}),$$

which admits a remrep of degree 2^n , where $n = 2 + 2lc(3) + 2lc(5) + 2lc(11) + 2lc(13) = 10$. By Theorem 6.26, there is an

$$OD\left(2^{12} \cdot 65; 2^{12} \cdot 1, 2^{12} \cdot 3_{(2)}, 2^{12} \cdot 5_{(2)}, 2^{12} \cdot 11_{(2)}, 2^{12} \cdot 13_{(2)}\right).$$

Remark 6.37. Applying Proposition 5.2 to any sequence (b, a_1, \dots, a_k) of positive integers, gives a full orthogonal design of type

$$\left(2^m \cdot 1_{(b)}, 2^m \cdot 2_{(4)}^{a_1}, \dots, 2^m \cdot 2_{(4)}^{a_k}\right),$$

where $m = 4k + b + 2$ if b is odd, and $m = 4k + b + 3$ if b is even.

For the sequence $(1_{(b)}, 2_{(4)}^{a_1}, \dots, 2_{(4)}^{a_k})$, if we use Golay pairs constructed in Lemma 6.6 in the proof of Lemma 6.34, and apply Theorem 6.26, then we obtain the same m .

As an example, for the 3-tuple $(1, 1, 1)$ both methods give $OD(2^5 \cdot 3; 2^5 \cdot 1, 2^5 \cdot 1, 2^5 \cdot 1)$.

See Examples 5.13 and 6.33. Note that for Golay pairs, the degree of the remrep in Lemma 6.34 would be 2^{n-1} not 2^n . Using Golay pairs, we apply Lemma 6.34 to the

6-tuple $(1, 1, 1, 1, 1, 1)$. So, by Theorem 6.26, there is an $OD(2^9 \cdot 6; 2^9 \cdot 1_{(6)})$.

However, in Example 5.13, using amicable orthogonal designs, we showed that there is an $OD(2^5 \cdot 6; 2^5 \cdot 1_{(6)})$.

Theorem 6.38. *Suppose that (u_1, u_2, \dots, u_k) is a k -tuple of positive integers and let $u_1 + \dots + u_k = u$. Assume j is such that $lc(u_j) - lc(u_j - 1)$ is maximum possible. Then there is a full circulant quasisymmetric*

$$SOD(4u; 4u_1, 4u_2, \dots, 4u_k)$$

for some signed group S that admits a remrep of degree 2^n , where

$$n = 2 + 2\ell c(u_j - 1) + 2 \sum_{\substack{i=1 \\ i \neq j}}^k \ell c(u_i).$$

Proof. Apply Lemma 6.34 to the $(k+1)$ -tuple $(1, u_1, \dots, u_{j-1}, u_j - 1, u_{j+1}, \dots, u_k)$.

□

For u a positive integer, denote by $\ell r(u)$, the least number of Golay numbers that add up to u . Let $\ell r(0) = 0$.

Using Golay pairs, we have a similar result to Theorem 6.38.

Corollary 6.39. *Suppose that (u_1, u_2, \dots, u_k) is a k -tuple of positive integers and let $u_1 + \dots + u_k = u$. Assume j is such that $\ell c(u_j) - \ell c(u_j - 1)$ is maximum possible. Then there exists a full circulant quasisymmetric*

$$SOD(4u; 4u_1, 4u_2, \dots, 4u_k)$$

for some signed group S that admits a remrep of degree 2^{n-1} , where

$$n = 2 + 2\ell r(u_j - 1) + 2 \sum_{\substack{i=1 \\ i \neq j}}^k \ell r(u_i).$$

We define $\log 0 = 0$, and whenever we write $\log a$, we mean $\log_2 a$.

Let $sr(n)$ be the smallest positive integer that is not the sum of at most n Golay numbers of the form $2^a 10^b 26^c$, where a, b and c are nonnegative integers. Also, let $gr(n)$ be the greatest Golay number of the same form not exceeding $sr(n)$.

The following table is obtained by Ivan Livinskyi [38].

n	$sr(n)$	$gr(n)$
2	7	4
3	39	32
4	199	160
5	11999	10816
6	637399	562432
7	233963479	224972800

Let u be a positive integer. We follow a similar technique in [38] to obtain upper bounds for $lr(u)$ and $lc(u)$. Writing the expansion of u to the base $gr(n)$, one gets

$$u = a_0 + a_1(gr(n)) + a_2(gr(n))^2 + \dots + a_m(gr(n))^m,$$

where $0 \leq a_i < gr(n)$ ($0 \leq i \leq m$) and $m = \lfloor \log_{gr(n)} u \rfloor$. Since each a_i ($0 \leq i \leq m$) is sum of at most n Golay numbers, u is a sum of at most $n \lfloor \log_{gr(n)} u \rfloor + n$ Golay numbers. Therefore,

$$lr(u) \leq n \lfloor \log_{gr(n)} u \rfloor + n.$$

As an example, $lr(u) \leq 3 \lfloor \log_{32} u \rfloor + 3 \leq \frac{3}{5} \log u + 3$. If one takes the base $gr(7)$, then a better bound for $lr(u)$ is obtained, i.e.,

$$lr(u) \leq 7 \lfloor \log_{224972800} u \rfloor + 7 < 0.2525 \log u + 7.$$

To get a better upper bound for the degree of remrep for any k -tuple (u_1, u_2, \dots, u_k) of positive integers, from now on, we assume that $lr(u_1) - lr(u_1 - 1)$ is greater than or equal to $lr(u_i) - lr(u_i - 1)$ for all $2 \leq i \leq k$.

For any k -tuple (u_1, u_2, \dots, u_k) of positive integers, write the expansion of u_i 's to the base $gr(7)$, to obtain the following upper bound for the degree of remrep in Corollary 6.39.

Corollary 6.40. *Suppose that (u_1, u_2, \dots, u_k) is a k -tuple of positive integers and let $u_1 + \dots + u_k = u$. Then there is a full circulant quasisymmetric*

$$SOD(4u; 4u_1, 4u_2, \dots, 4u_k)$$

for some signed group S that admits a remrep of degree 2^{n-1} , where

$$n \leq 0.505 \log(u_1 - 1) + 0.505 \sum_{i=2}^k \log(u_i) + 14k + 2.$$

By a computer search, each positive integer u is presented as sum of at most $3 \lceil \log_{26} u \rceil + 4$ complex Golay numbers of the form mentioned in Theorem 6.23 [38]. Thus

$$\ell c(u) \leq 3 \left\lceil \frac{1}{26} \log u \right\rceil + 4 \leq \frac{3}{26} \log u + 4. \quad (6.16)$$

Using this and Theorem 6.38, one has the following upper bound for the degree of remrep.

Corollary 6.41. *Suppose that (u_1, u_2, \dots, u_k) is a k -tuple of positive integers and let $u_1 + \dots + u_k = u$. Then there is a full circulant quasisymmetric*

$$SOD(4u; 4u_1, 4u_2, \dots, 4u_k)$$

for some signed group S that admits a remrep of degree 2^n , where

$$n \leq \frac{3}{13} \log(u_1 - 1) + \frac{3}{13} \sum_{i=2}^k \log(u_i) + 8k + 2.$$

Remark 6.42. One may present any given k -tuple (u_1, u_2, \dots, u_k) of positive integers as a $(k+1)$ -tuple $(1, u_1 - 1, u_2, \dots, u_k)$, and then sort its elements to get the $(k+1)$ -

tuple $(1, v_1, \dots, v_q, w_1, w_1, \dots, w_t, w_t)$, where $1 \leq v_1 < \dots < v_q$. Thus, from Theorem 6.38,

$$\begin{aligned} n &= 2 + 2 \sum_{i=1}^q \ell c(v_i) + 2 \sum_{j=1}^t \ell c(w_j) \\ &\leq 2 + \frac{3}{13} \sum_{i=1}^q \log(v_i) + \frac{3}{13} \sum_{j=1}^t \log(w_j) + 8(q+t). \end{aligned}$$

By Theorem 6.26 and Corollary 6.41, we obtain another bound for the asymptotic existence of orthogonal designs.

Theorem 6.43. *Suppose that (u_1, u_2, \dots, u_k) is a k -tuple of positive integers and let $u_1 + \dots + u_k = u$. Then for each $n \geq N$ there is an*

$$OD(2^n u; 2^n u_1, \dots, 2^n u_k),$$

where $N \leq \frac{3}{13} \log(u_1 - 1) + \frac{3}{13} \sum_{i=2}^k \log(u_i) + 8k + 4$.

Ivan Livinskyi in [38] used complex Golay, Base, Normal and other sequences (see [12, 32, 33, 35]) to show that each positive integer u can be presented as sum of

$$s \leq \frac{1}{10} \log u + 5 \tag{6.17}$$

pairs $(A_k[u]; B_k[u])$ for $1 \leq k \leq s$ such that $A_k[u]$ and $B_k[u]$ have the same length for each k , $1 \leq k \leq s$, with elements from $\{\pm 1, \pm i\}$, and the set

$$\{A_1[u], B_1[u], \dots, A_s[u], B_s[u]\} \tag{6.18}$$

is a set of complex complementary sequences with weight $2u$. In the following theorem, we use this set of complex complementary sequences.

Theorem 6.44. *Suppose that (v_1, v_2, \dots, v_k) is a k -tuple of positive integers and let $v_1 + \dots + v_k = v$. Then for each $n \geq N$, there is an*

$$OD(2^n v; 2^n v_1, \dots, 2^n v_k),$$

where $N \leq \frac{1}{5} \log(v_1 - 1) + \frac{1}{5} \sum_{i=2}^k \log(v_i) + 10k + 4$.

Proof. Suppose (v_1, v_2, \dots, v_k) is a k -tuple of positive integer. Let $v_1 + \dots + v_k = v$. For simplicity, we assume that $u_1 = v_1 - 1$ and $u_i = v_i$ for $2 \leq i \leq k$.

For each β , $1 \leq \beta \leq k$, let $\{A_1[u_\beta], B_1[u_\beta], \dots, A_{s_\beta}[u_\beta], B_{s_\beta}[u_\beta]\}$ be a set of complex complementary sequences with weight $2u_\beta$ such that for each α , $1 \leq \alpha \leq s_\beta$, $A_\alpha[u_\beta]$ and $B_\alpha[u_\beta]$ have the same length, $V[\alpha, u_\beta]$. From (6.17), for each β , $1 \leq \beta \leq k$,

$$s_\beta \leq \frac{1}{10} \log u_\beta + 5. \quad (6.19)$$

Suppose that x and x_β , $1 \leq \beta \leq k$ are variables. Let $M_1 = \text{circ}(x, 0_{(2v-1)}, x, 0_{(2v-1)})$ and $M_2 = \text{circ}(0_{(v)}, -x, 0_{(2v-1)}, x, 0_{(v-1)})$. For each β , $1 \leq \beta \leq k$, and each α , $1 \leq \alpha \leq s_\beta$, let

$$\begin{aligned} X_{\alpha\beta} &= \text{circ}\left(0_{(S[\alpha,\beta]+1)}, x_\beta A_\alpha[u_\beta], 0_{(4v-2S[\alpha+1,\beta]-1)}, x_\beta B_\alpha[u_\beta], 0_{(S[\alpha,\beta])}\right), \\ Y_{\alpha\beta} &= \text{circ}\left(0_{(2v-S[\alpha+1,\beta])}, -x_\beta B_\alpha[u_\beta], 0_{(2S[\alpha,\beta]+1)}, x_\beta A_\alpha[u_\beta], 0_{(2v-S[\alpha+1,\beta]-1)}\right), \end{aligned}$$

where $S[1, 1] = 0$ and $S[a, b] = \sum_{j=1}^{a-1} \sum_{i=1}^b V[j, u_i]$, for $1 \leq b \leq k$ and $1 < a \leq s_b + 1$.

It can be seen that the above circulant matrices are disjoint and quasisymmetric of order $4v$ such that

$$\sum_{i=1}^2 M_i M_i^* + \sum_{\beta=1}^k \sum_{\alpha=1}^{s_\beta} (X_{\alpha\beta} X_{\alpha\beta}^* + Y_{\alpha\beta} Y_{\alpha\beta}^*) = 4 \left(x^2 + \sum_{\beta=1}^k (u_\beta x_\beta^2) \right) I_{4v}.$$

Thus, by Theorem 6.30, there exists a full circulant quasisymmetric

$$SOD(4v; 4, 4u_1, \dots, 4u_k)$$

for a signed group S which admits a remrep of degree 2^m , where $m = 2 + 2 \sum_{\beta=1}^k s_\beta$.

By Theorem 6.26 and the upper bounds for the s_β 's, (6.19), there exists an

$$OD(2^n v; 2^n, 2^n u_1, \dots, 2^n u_k),$$

and so there exists an

$$OD(2^n v; 2^n v_1, \dots, 2^n v_k),$$

where $n \leq \frac{1}{5} \log(v_1 - 1) + \frac{1}{5} \sum_{i=2}^k \log(v_i) + 10k + 4$. □

Example 6.45. Let p be a prime number. Consider the 1-tuple (p) . By Theorem 6.44, for each $n \geq \frac{1}{5} \log(p - 1) + 14$, there is a Hadamard matrix of order $2^n p$.

In the next example, we modify Theorem 6.44, and decrease the bound in Example 6.45 from $\frac{1}{5} \log(p - 1) + 14$ to $\frac{1}{5} \log \frac{p - 1}{2} + 13$. The latter bound is obtained first by Ivan Livinskyi [38].

Example 6.46. Consider the 2-tuple $(1, v) = \left(1, \frac{p - 1}{2}\right)$, where p is prime. Let $\{A_1[v], B_1[v], \dots, A_s[v], B_s[v]\}$ be a set of complex complementary sequences with total weight $p - 1$, where $s \leq \frac{1}{10} \log v + 5$ and for each α , $1 \leq \alpha \leq s$, the lengths $A_\alpha[v]$ and $B_\alpha[v]$ are the same and equal to some integer ℓ_α .

Let $M_1 = \text{circ}(x, 0_{(2p-1)})$ and $M_2 = \text{circ}(0_{(p)}, x, 0_{(p-1)})$. Also, for $1 \leq \alpha \leq s$, let

$$X_\alpha = \text{circ}\left(0_{(S_\alpha+1)}, x_1 A_\alpha[v], 0_{(2p-2S_\alpha+1)}, x_1 B_\alpha[v], 0_{(S_\alpha)}\right),$$

$$Y_\alpha = \text{circ}\left(0_{(p-S_\alpha+1)}, -x_1 B_\alpha[v], 0_{(2S_\alpha+1)}, x_1 A_\alpha[v], 0_{(p-S_\alpha-1)}\right),$$

where x and x_1 are variables, $S_1 = 0$ and $S_\beta = \sum_{i=1}^{\beta-1} \ell_i$ for $2 \leq \beta \leq s+1$. It can be seen that the above circulant matrices are quasisymmetric matrices of order $2p$ such that

$$\sum_{i=1}^2 M_i M_i^* + \sum_{\alpha=1}^s (X_\alpha X_\alpha^* + Y_\alpha Y_\alpha^*) = (2x + (2p-2)x_1) I_{2p}.$$

By Theorem 6.30, there is a $SOD(2p; 2, 2p-2)$ for a signed group S which admits a remrep of degree 2^n , where $n = 2 + 2s \leq \frac{1}{5} \log \frac{p-1}{2} + 12$. Therefore, by Theorem 6.26, there is an

$$OD\left(2^{n+1}p; 2^n \cdot 2, 2^n(2p-2)\right),$$

and by equating variables in the above OD, one concludes that there is a Hadamard matrix of order $2^{n+1}p$, for each $n \geq \frac{1}{5} \log \frac{p-1}{2} + 12$.

6.5 Signed group orthogonal designs of order 2^n and an application to the construction of orthogonal designs

In the previous section, SODs obtain over signed groups that were inductively generated. In this section, we make SODs over specific signed groups.

Theorem 6.47. *There is a $SOD(2^n; 1_{(2^n)})$ over a signed group S that admits a remrep of degree $2^{2^{n-1}-1}$, $n > 2$.*

Proof. Let $m = 2^{2^{n-1}-1}$. It can be seen that $\rho(m) = 2^n$, for $n > 2$. By Theorem 2.42, there is a set $A = \{I_m, A_1, A_2, \dots, A_{\rho(m)-1}\}$ of pairwise disjoint anti-amicable signed permutation matrices of order m . Let $T = \langle A_1, \dots, A_{\rho(m)-1} \rangle$. Clearly, T is a signed

subgroup of SP_m . Let

$$S = \langle s_1, \dots, s_{\rho(m)-1}; s_\alpha^2 = -1, s_\alpha s_\beta = -s_\beta s_\alpha, 1 \leq \alpha \neq \beta \leq \rho(m) - 1 \rangle. \quad (6.20)$$

Let $\pi : S \longrightarrow T$ be a map defined by $\pi(s_\alpha) = A_\alpha$ for $1 \leq \alpha \leq \rho(m) - 1$. It can be seen that π is a remrep of degree m .

Let $B = \{B_0, B_1, \dots, B_{2^n-1}\}$ be a set of supplementary matrices which obtain by n times the Kronecker product of I and P . It is easy to see that the matrices in the set B are pairwise amicable of order 2^n . Therefore,

$$D = x_0 B_0 + s_1 x_1 B_1 + \dots + s_{2^n-1} x_{2^n-1} B_{2^n-1},$$

is a $SOD(2^n; 1_{(2^n)})$ over the signed group S admitting the remrep π , where the x_i 's are variables. □

Example 6.48. We show that there is a $SOD(2^3; 1_{(2^3)})$ over a signed group S that admits a remrep of degree 2^3 . Let

$$\begin{aligned} B_0 &= I \otimes I \otimes I, & B_4 &= I \otimes P \otimes P, \\ B_1 &= I \otimes I \otimes P, & B_5 &= P \otimes I \otimes P, \\ B_2 &= I \otimes P \otimes I, & B_6 &= P \otimes P \otimes I, \\ B_3 &= P \otimes I \otimes I, & B_7 &= P \otimes P \otimes P. \end{aligned}$$

Let S be the signed group in (6.20), $m = 8$. It can be seen that $D = x_0 B_0 + \sum_{i=1}^7 s_i x_i B_i$ is the desired SOD, where the x_i 's are variables.

Following similar techniques in [29], we show the following theorem.

Theorem 6.49. *Suppose that r is a Golay number, and $k_1, k_2, \dots, k_{2^{n-3}-1}$ are complex Golay numbers, where $n > 2$. Let $m = 2 \sum_{j=1}^{2^{n-3}-1} k_j + r + 1$. Then there is a*

$$COD\left(2^q m; 2^q, 2^q r, 2^{q+1} k_1, \dots, 2^{q+1} k_{2^{n-3}-1}\right),$$

where $q = 2^{n-1} + n - 1$.

Proof. Let n be a positive integer greater than 2. Suppose that H is a Hadamard matrix of order 2^{n-2} , $(A; B)$ is a Golay pair of length r , and $(C^{(j)}; D^{(j)})$ is a complex Golay pair of length k_j ($1 \leq j \leq 2^{n-3} - 1$). Let $m = 2 \sum_{j=1}^{2^{n-3}-1} k_j + r + 1$. Consider the following 2^{n-2} -dimensional row vectors:

$$\begin{aligned} E &= \left(y, x_1 C^{(1)}, \dots, x_{2^{n-3}-1} C^{(2^{n-3}-1)}, zA, x_{2^{n-3}-1} C_{\overline{R}}^{(2^{n-3}-1)}, \dots, x_1 C_{\overline{R}}^{(1)} \right), \\ F &= \left(y, x_1 D^{(1)}, \dots, x_{2^{n-3}-1} D^{(2^{n-3}-1)}, zB, x_{2^{n-3}-1} D_{\overline{R}}^{(2^{n-3}-1)}, \dots, x_1 D_{\overline{R}}^{(1)} \right), \end{aligned}$$

where the x_j 's, y and z are variables. Let e be the 2^{n-2} -dimensional column vector of ones. For each j , $1 \leq j \leq 2^{n-2}$, let E_j and F_j be the circulant matrices of order m whose first rows are the j -th rows of $eE \odot H$ and $eF \odot H$, respectively, where \odot is entrywise multiplication (note that eE and eF are matrices of order 2^{n-2} whose entries are sequences). It can be verified that

$$\sum_{j=1}^{2^{n-2}} (E_j E_j^* + F_j F_j^*) = 2^{n-1} \left(y^2 + rz^2 + 2 \sum_{j=1}^{2^{n-3}-1} k_j x_j^2 \right) I_m, \quad (6.21)$$

see [29]. For each j , $1 \leq j \leq 2^{n-2}$, let $E'_j = \frac{1}{2}(E_j + E_j^*)$, $E''_j = \frac{i}{2}(E_j - E_j^*)$, $F'_j = \frac{1}{2}(F_j + F_j^*)$ and $F''_j = \frac{i}{2}(F_j - F_j^*)$.

Now it can be seen that the set

$$\Omega = \left\{ E'_j - E''_j, E'_j + E''_j, F'_j - F''_j, F'_j + F''_j; \quad 1 \leq j \leq 2^{n-2} \right\}$$

consists of 2^n Hermitian circulant matrices. Moreover,

$$\begin{aligned} & \sum_{j=1}^{2^{n-2}} \left((E'_j - E''_j)(E'_j - E''_j)^* + (E'_j + E''_j)(E'_j + E''_j)^* \right) \\ & + (F'_j - F''_j)(F'_j - F''_j)^* + (F'_j + F''_j)(F'_j + F''_j)^* \\ & = 2 \sum_{j=1}^{2^{n-2}} \left(E_j'^2 + E_j''^2 + F_j'^2 + F_j''^2 \right) \\ & = \frac{1}{2} \sum_{j=1}^{2^{n-2}} \left((E_j + E_j^*)^2 - (E_j - E_j^*)^2 + (F_j + F_j^*)^2 - (F_j - F_j^*)^2 \right) \\ & = 2 \sum_{j=1}^{2^{n-2}} (E_j E_j^* + F_j F_j^*) \quad \text{from (6.21)} \\ & = 2^n \left(y^2 + rz^2 + 2 \sum_{j=1}^{2^{n-3}-1} k_j x_j^2 \right) I_m. \end{aligned}$$

From Theorem 6.47, there is a $SOD(2^n; 1_{(2^n)})$ over a signed group S that admits a remrep of degree $2^{2^{n-1}-1}$. By Theorem 6.26, there is an $OD(2^q; 2_{(2^n)}^{2^{n-1}-1})$, where $q = 2^{n-1} + n - 1$. Replacing variables in this OD by the Hermitian circulant matrices in the set Ω , we obtain the desired COD. \square

Example 6.50. Using Theorem 6.49, we show that there is a

$$COD(2^{11} \cdot 31; 2^{11} \cdot 1, 2^{11} \cdot 8, 2^{11} \cdot 22).$$

Let e be the 4-dimensional column vector of all ones, $(A; B)$ be a Golay pair of length

8, and $(C; D)$ be a complex Golay pair of length 11 as follow:

$$\begin{aligned} A &= (1, 1, 1, -, 1, 1, -, 1), & B &= (1, 1, 1, -, -, -, 1, -), \\ C &= (1, i, -, 1, -, i, \bar{i}, -, i, i, 1), & D &= (1, 1, \bar{i}, \bar{i}, \bar{i}, 1, 1, i, -, 1, -), \end{aligned}$$

$$\text{Let } E = (y, xC, zA, xC_{\overline{R}}), F = (y, xD, zB, xD_{\overline{R}}) \text{ and } H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ 1 & 1 & - & - \\ 1 & - & - & 1 \end{bmatrix}.$$

We have

$$eE \odot H = \begin{bmatrix} y & xC & zA & xC_{\overline{R}} \\ y & -xC & zA & -xC_{\overline{R}} \\ y & xC & -zA & -xC_{\overline{R}} \\ y & -xC & -zA & xC_{\overline{R}} \end{bmatrix} \text{ and } eF \odot H = \begin{bmatrix} y & xD & zB & xD_{\overline{R}} \\ y & -xD & zB & -xD_{\overline{R}} \\ y & xD & -zB & -xD_{\overline{R}} \\ y & -xD & -zB & xD_{\overline{R}} \end{bmatrix}.$$

Let

$$\begin{aligned} E_1 &= \text{circ}(y, xC, zA, xC_{\overline{R}}), & F_1 &= \text{circ}(y, xD, zB, xD_{\overline{R}}), \\ E_2 &= \text{circ}(y, -xC, zA, -xC_{\overline{R}}), & F_2 &= \text{circ}(y, -xD, zB, -xD_{\overline{R}}), \\ E_3 &= \text{circ}(y, xC, -zA, -xC_{\overline{R}}), & F_3 &= \text{circ}(y, xD, -zB, -xD_{\overline{R}}), \\ E_4 &= \text{circ}(y, -xC, -zA, xC_{\overline{R}}), & F_4 &= \text{circ}(y, -xD, -zB, xD_{\overline{R}}). \end{aligned}$$

From each of E_j and F_j ($1 \leq j \leq 4$), we obtain two Hermitian circulant matrices.

As an example E_3 is the circulant matrix with the following first row:

$$(y, x, ix, \underline{x}, x, \underline{x}, ix, \bar{i}x, \underline{x}, ix, ix, x, \underline{z}, \underline{z}, \underline{z}, \underline{z}, \underline{z}, \underline{z}, \underline{z}, \underline{z}, \underline{x}, ix, ix, x, \bar{i}x, ix, x, \underline{x}, x, ix, \underline{x}),$$

where \underline{u} means $-u$. The following rows are the first rows of the supplementary Hermitian circulant matrices $E'_3 = \frac{1}{2}(E_3 + E_3^*)$ and $E''_3 = \frac{i}{2}(E_3 - E_3^*)$, respectively:

$$(y, 0_{(11)}, \underline{z}, 0, \underline{z}, 0, 0, \underline{z}, 0, \underline{z}, 0_{(11)}),$$

$$(0, ix, \underline{x}, \bar{i}x, ix, \bar{i}x, \underline{x}, x, \bar{i}x, \underline{x}, \underline{x}, ix, 0, \bar{i}z, 0, iz, \bar{i}z, 0, iz, 0, \bar{i}x, \underline{x}, \underline{x}, ix, x, \underline{x}, ix, \bar{i}x, ix, \underline{x}, \bar{i}x).$$

Therefore, $E'_3 + E''_3$ and $E'_3 - E''_3$ are the desired two Hermitian circulant matrices obtained from E_3 . Continuing this process, we find 16 complementary Hermitian circulant matrices of order 31. Replacing these matrices with variables in $OD(2^{11}; 2^7_{(16)})$ obtained from Theorem 6.47 and 6.26, we find a

$$COD(2^{11} \cdot 31; 2^{11} \cdot 1, 2^{11} \cdot 8, 2^{11} \cdot 22).$$

Remark 6.51. Replacing the 16 complementary Hermitian circulant matrices in the above example with variables in $OD(2^{10}; 2^6_{(16)})$ obtained in Theorem 4.17, we get a

$$COD(2^{10} \cdot 31; 2^{10} \cdot 1, 2^{10} \cdot 8, 2^{10} \cdot 22).$$

Appendix Some amicable orthogonal designs

$AOD(16; 2, 2, 2, 10; 2, 2, 2, 10)$ as constructed in Construction 4.14 (note that \bar{x} means $-x$).

$$\begin{bmatrix} a & a & d & d & b & b & c & c & a & a & \bar{a} & \bar{a} & a & a & a & a \\ a & \bar{a} & \bar{d} & d & \bar{b} & b & \bar{c} & c & a & \bar{a} & \bar{a} & a & a & \bar{a} & a & \bar{a} \\ \bar{d} & \bar{d} & a & a & \bar{c} & c & \bar{b} & b & a & a & a & a & a & \bar{a} & \bar{a} & a \\ d & \bar{d} & a & \bar{a} & c & \bar{c} & \bar{b} & b & a & \bar{a} & a & \bar{a} & a & \bar{a} & \bar{a} & a \\ b & b & \bar{c} & \bar{c} & \bar{a} & \bar{a} & d & d & \bar{a} & \bar{a} & \bar{a} & \bar{a} & a & a & \bar{a} & \bar{a} \\ \bar{b} & b & c & \bar{c} & \bar{a} & a & \bar{d} & d & \bar{a} & a & \bar{a} & a & a & \bar{a} & \bar{a} & a \\ c & c & b & b & \bar{d} & \bar{d} & \bar{a} & \bar{a} & \bar{a} & \bar{a} & a & a & a & a & a & a \\ \bar{c} & c & \bar{b} & b & d & \bar{d} & \bar{a} & \bar{a} & a & \bar{a} & a & \bar{a} & a & \bar{a} & a & \bar{a} \\ \bar{a} & \bar{a} & \bar{a} & \bar{a} & \bar{a} & \bar{a} & \bar{a} & \bar{a} & a & a & \bar{d} & \bar{d} & b & b & c & c \\ \bar{a} & a & \bar{a} & a & \bar{a} & a & \bar{a} & a & a & \bar{a} & d & \bar{d} & \bar{b} & b & \bar{c} & c \\ a & a & \bar{a} & \bar{a} & \bar{a} & \bar{a} & a & d & d & a & a & \bar{c} & \bar{c} & b & b & b \\ a & \bar{a} & \bar{a} & a & \bar{a} & a & a & \bar{d} & \bar{d} & a & \bar{a} & c & \bar{c} & \bar{b} & b & b \\ a & a & a & a & \bar{a} & \bar{a} & \bar{a} & b & b & \bar{c} & \bar{c} & \bar{a} & \bar{a} & \bar{d} & \bar{d} & \bar{d} \\ a & \bar{a} & a & \bar{a} & \bar{a} & a & \bar{a} & b & c & \bar{c} & \bar{c} & \bar{a} & a & d & \bar{d} & \bar{d} \\ a & a & \bar{a} & \bar{a} & a & a & \bar{a} & \bar{a} & c & b & d & d & \bar{a} & \bar{a} & \bar{a} & \bar{a} \\ a & \bar{a} & \bar{a} & a & a & \bar{a} & \bar{a} & a & \bar{c} & \bar{c} & \bar{b} & b & d & \bar{d} & \bar{d} & \bar{a} & a \\ a & x & \bar{x} & \bar{z} & z & \bar{e} & e & \bar{y} & y & x & \bar{x} & \bar{x} & x & x & \bar{x} & x & \bar{x} \\ x & x & z & z & e & e & y & y & x & x & \bar{x} & \bar{x} & x & x & \bar{x} & x & x \\ z & \bar{z} & x & \bar{x} & \bar{y} & y & e & \bar{e} & x & \bar{x} & x & \bar{x} & x & \bar{x} & x & \bar{x} & x \\ \bar{z} & \bar{z} & x & x & y & y & \bar{e} & \bar{e} & x & x & x & x & x & \bar{x} & x & \bar{x} & \bar{x} \\ \bar{e} & e & \bar{y} & y & \bar{x} & x & z & \bar{z} & \bar{x} & \bar{x} & x & \bar{x} & x & x & \bar{x} & \bar{x} & x \\ e & e & y & y & \bar{x} & \bar{x} & \bar{z} & \bar{z} & \bar{x} & \bar{x} & \bar{x} & \bar{x} & x & x & \bar{x} & \bar{x} & \bar{x} \\ \bar{y} & y & e & \bar{e} & \bar{z} & z & \bar{x} & x & \bar{x} & \bar{x} & x & \bar{x} & x & \bar{x} & x & \bar{x} & \bar{x} \\ y & y & \bar{e} & \bar{e} & z & z & \bar{x} & \bar{x} & \bar{x} & \bar{x} & x & \bar{x} & x & x & x & \bar{x} & x \\ \bar{x} & x & \bar{x} & x & \bar{x} & \bar{x} & x & x & \bar{x} & \bar{x} & x & \bar{x} & e & \bar{e} & \bar{y} & y & \bar{z} & z \\ \bar{x} & \bar{x} & \bar{x} & \bar{x} & \bar{x} & \bar{x} & \bar{x} & \bar{x} & \bar{x} & \bar{x} & x & x & \bar{e} & \bar{e} & y & y & z & z \\ x & \bar{x} & \bar{x} & x & \bar{x} & x & x & \bar{x} & \bar{e} & e & x & \bar{x} & \bar{e} & e & z & y & \bar{y} & \bar{y} \\ x & x & \bar{x} & \bar{x} & \bar{x} & \bar{x} & \bar{x} & \bar{x} & x & e & e & x & x & z & z & \bar{y} & \bar{y} \\ x & \bar{x} & x & x & \bar{x} & \bar{x} & x & \bar{x} & x & \bar{y} & y & \bar{z} & z & \bar{x} & \bar{x} & e & e \\ x & x & x & x & \bar{x} & \bar{x} & \bar{x} & \bar{x} & \bar{x} & y & y & z & z & \bar{x} & \bar{x} & e & e \\ x & \bar{x} & \bar{x} & x & x & \bar{x} & \bar{x} & x & z & z & y & \bar{y} & e & \bar{e} & \bar{x} & \bar{x} & x \\ x & x & \bar{x} & \bar{x} & x & x & \bar{x} & \bar{x} & z & z & \bar{y} & \bar{y} & e & \bar{e} & \bar{x} & \bar{x} & \bar{x} \end{bmatrix},$$

ddddd... (A large block of repetitive text consisting of many lines of 'd' characters and some 'e' characters, appearing as a dense grid of characters.)

Bibliography

- [1] E. F. Assmus, Jr. and J. D. Key. *Designs and their codes*, volume 103 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1992.
- [2] Ian F. Blake and Ronald C. Mullin. *The mathematical theory of coding*. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], New York-London, 1975.
- [3] P. B. Borwein and R. A. Ferguson. A complete description of Golay pairs for lengths up to 100. *Math. Comp.*, 73(246):967–985 (electronic), 2004.
- [4] R. Craigen. Complex Golay sequences. *J. Combin. Math. Combin. Comput.*, 15:161–169, 1994.
- [5] R. Craigen. Signed groups, sequences, and the asymptotic existence of Hadamard matrices. *J. Combin. Theory Ser. A*, 71(2):241–254, 1995.
- [6] R. Craigen, W. Holzmann, and H. Kharaghani. Complex Golay sequences: structure and applications. *Discrete Math.*, 252(1-3):73–89, 2002.
- [7] R. Craigen, W. H. Holzmann, and H. Kharaghani. On the asymptotic existence of complex Hadamard matrices. *J. Combin. Des.*, 5(5):319–327, 1997.
- [8] Robert Craigen. *Constructions for orthogonal matrices*. 1991. Thesis (Ph.D.)–University of Waterloo.
- [9] Warwick de Launey. On the asymptotic existence of Hadamard matrices. *J. Combin. Theory Ser. A*, 116(4):1002–1008, 2009.
- [10] Warwick de Launey and Dane Flannery. *Algebraic design theory*, volume 175 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2011.
- [11] Warwick de Launey and H. Kharaghani. On the asymptotic existence of cocyclic Hadamard matrices. *J. Combin. Theory Ser. A*, 116(6):1140–1153, 2009.
- [12] Dragomir Ž. Doković. On the base sequence conjecture. *Discrete Math.*, 310(13-14):1956–1964, 2010.

- [13] Peter Eades. Some asymptotic existence results for orthogonal designs. *Ars Combinatoria*, 1(1):109–118, 1976.
- [14] Peter Eades. Integral quadratic forms and orthogonal designs. *J. Austral. Math. Soc. Ser. A*, 30(3):297–306, 1980/81.
- [15] Peter Eades, Peter J. Robinson, Jennifer Seberry Wallis, and Ian S. Williams. An algorithm for orthogonal designs. In *Proceedings of the Fifth Manitoba Conference on Numerical Mathematics (Univ. Manitoba, Winnipeg, Man., 1975)*, pages 279–292. Congressus Numerantium, No. XVI. Utilitas Math. Publ., Winnipeg, Man., 1976.
- [16] Shalom Eliahou, Michel Kervaire, and Bahman Saffari. A new restriction on the lengths of Golay complementary sequences. *J. Combin. Theory Ser. A*, 55(1):49–59, 1990.
- [17] Anthony V. Geramita, Joan Murphy Geramita, and Jennifer Seberry Wallis. Orthogonal designs. *Linear and Multilinear Algebra*, 3(4):281–306, 1975/76.
- [18] Anthony V. Geramita and Jennifer Seberry. *Orthogonal designs*, volume 45 of *Lecture Notes in Pure and Applied Mathematics*. Marcel Dekker Inc., New York, 1979. Quadratic forms and Hadamard matrices.
- [19] J.-M. Goethals and J. J. Seidel. Orthogonal matrices with zero diagonal. *Canad. J. Math.*, 19:1001–1010, 1967.
- [20] J. Hadamard. Resolution d’une question relative aux determinants. *Bull. des Sci. Math*, 17:240–246, 1893.
- [21] Marshall Hall, Jr. *Combinatorial theory*. Blaisdell Publishing Co. Ginn and Co., Waltham, Mass.-Toronto, Ont.-London, 1967.
- [22] W. H. Holzmann and H. Kharaghani. A computer search for complex Golay sequences. *Australas. J. Combin.*, 10:251–258, 1994.
- [23] W. H. Holzmann and H. Kharaghani. On the amicability of orthogonal designs. *J. Combin. Des.*, 17(3):240–252, 2009.
- [24] K. J. Horadam. *Hadamard matrices and their applications*. Princeton University Press, Princeton, NJ, 2007.
- [25] Kenneth Ireland and Michael I. Rosen. *Elements of number theory. Including an introduction to equations over finite fields*. Bogden & Quigley, Inc., Publishers, Tarrytown-on-Hudson, N.Y., 1972.
- [26] Yindi Jing and Hamid Jafarkhani. Using orthogonal and quasi-orthogonal designs in wireless relay networks. *IEEE Trans. Inform. Theory*, 53(11):4106–4118, 2007.

- [27] Dieter Jungnickel and H. Kharaghani. Balanced generalized weighing matrices and their applications. *Matematiche (Catania)*, 59(1-2):225–261 (2006), 2004.
- [28] Yukiyoji Kawada and Nagayosi Iwahori. On the structure and representations of Clifford algebras. *J. Math. Soc. Japan*, 2:34–43, 1950.
- [29] H. Kharaghani. On the asymptotic existence of complex Williamson Hadamard matrices. *Australas. J. Combin.*, 10:225–230, 1994.
- [30] H. Kharaghani and B. Tayfeh-Rezaie. Some new orthogonal designs in orders 32 and 40. *Discrete Math.*, 279(1-3):317–324, 2004. In honour of Zhu Lie.
- [31] H. Kharaghani and B. Tayfeh-Rezaie. A Hadamard matrix of order 428. *J. Combin. Des.*, 13(6):435–440, 2005.
- [32] C. Koukouvinos, S. Kounias, J. Seberry, C. H. Yang, and J. Yang. Multiplication of sequences with zero autocorrelation. *Australas. J. Combin.*, 10:5–15, 1994.
- [33] C. Koukouvinos, S. Kounias, and K. Sotirakoglou. On base and Turyn sequences. *Math. Comp.*, 55(192):825–837, 1990.
- [34] Christos Koukouvinos and Jennifer Seberry. Weighing matrices and their applications. *J. Statist. Plann. Inference*, 62(1):91–101, 1997.
- [35] S. Kounias and K. Sotirakoglou. Construction of orthogonal sequences. *Proceedings of the 14th Greek Statistical Conference*, (192):229–236, 2001.
- [36] Alan J. Laub. *Matrix analysis for scientists and engineers*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2005.
- [37] Xue-Bin Liang and Xiang-Gen Xia. On the nonexistence of rate-one generalized complex orthogonal designs. *IEEE Trans. Inform. Theory*, 49(11):2984–2989, 2003.
- [38] Ivan Livinskyi. *Asymptotic existence of Hadamard matrices*. 2012. Thesis (M.Sc.)—University of Manitoba, Winnipeg.
- [39] R. E. A. C. Paley. On orthogonal matrices. *J. Math. Phys.*, 12:311–320, 1933.
- [40] J. Radon. Lineare scharen orthogonaler matrizen. *Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universitat*, 1:1–14, 1922.
- [41] K. B. Reid and Ezra Brown. Doubly regular tournaments are equivalent to skew Hadamard matrices. *J. Combinatorial Theory Ser. A*, 12:332–338, 1972.
- [42] Peter J. Robinson. A non-existence theorem for orthogonal designs. *Utilitas Math.*, 10:179–184, 1976.

- [43] Peter J. Robinson. Using product designs to construct orthogonal designs. *Bull. Austral. Math. Soc.*, 16(2):297–305, 1977.
- [44] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.
- [45] Daniel Byron Shapiro. *Similarities, quadratic forms, and Clifford algebras*. ProQuest LLC, Ann Arbor, MI, 1974. Thesis (Ph.D.)—University of California, Berkeley.
- [46] J. J. Sylvester. Thoughts on inverse orthogonal matrices, simultaneous sign-successions, and tessellated pavements in two or more colors, with applications to Newton’s rule, ornamental tile-work, and the theory of numbers. *Phil. Mag.*, 34:461–475, 1867.
- [47] Vahid Tarokh, Hamid Jafarkhani, and A. R. Calderbank. Space-time block codes from orthogonal designs. *IEEE Trans. Inform. Theory*, 45(5):1456–1467, 1999.
- [48] R. J. Turyn. Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings. *J. Combinatorial Theory Ser. A*, 16:313–333, 1974.
- [49] I. M. Vinogradov. *Elements of number theory*. Dover Publications Inc., New York, 1954. Translated by S. Kravetz.
- [50] Jennifer Seberry Wallis. On the existence of Hadamard matrices. *J. Combinatorial Theory Ser. A*, 21(2):188–195, 1976.
- [51] Jennifer Seberry Wallis and Albert Leon Whiteman. Some results on weighing matrices. *Bull. Austral. Math. Soc.*, 12(3):433–447, 1975.
- [52] Warren Wolfe. Rational quadratic forms and orthogonal designs. In *Number theory and algebra*, pages 339–348. Academic Press, New York, 1977.
- [53] Warren William Wolfe. *Orthogonal designs- amicable orthogonal designs, some algebraic and combinatorial techniques*. ProQuest LLC, Ann Arbor, MI, 1975. Thesis (Ph.D.)—Queen’s University (Canada).