2004

On orthogonal matrices

Behbahani, Majid

Lethbridge, Alta. : University of Lethbridge, Faculty of Arts and Science, 2004

ON ORTHOGONAL MATRICES

MAJID BEHBAHANI
Bachelor of Engineering, Shahid Beheshti University, 2002

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

MASTER OF SCIENCE

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

ABSTRACT

On Orthogonal Matrices
Majid Behbahani
Department of Mathematics and Computer Science
University of Lethbridge
M. Sc. Thesis, 2004

Our main aim in this thesis is to study and search for orthogonal matrices which have a certain kind of block structure. The most desirable class of matrices for our purpose are orthogonal designs constructible from 16 circulant matrices. In studying these matrices, we show that the $OD(12; 1, 1, 1, 9)$ is the only orthogonal design constructible from 16 circulant matrices of type $OD(4n; 1, 1, 1, 4n-3)$, whenever $n > 1$ is an odd integer. We then use an exhaustive search to show that the only orthogonal design constructible from 16 circulant matrices of order 12 on 4 variables is the $OD(12; 1, 1, 1, 9)$. It is known that by using of T–matrices and orthogonal designs constructible from 16 circulant matrices one can produce an infinite family of orthogonal designs. To complement our studies we reproduce an important recent construction of T-matrices by Xia and Xia.

We then turn our attention to the applications of orthogonal matrices. In some recent works productive regular Hadamard matrices are used to construct many new infinite families of symmetric designs. We show that for each integer n for which $4n$ is the order of a Hadamard matrix and $8n^2 - 1$ is a prime, there is a productive regular Hadamard matrix of order $16n^2(8n^2 - 1)^2$. As a corollary, we get many new infinite classes of symmetric designs whenever either of $4n(8n^2 - 1) - 1$, $4n(8n^2 - 1) + 1$ is a prime power. We also review some other constructions of productive regular Hadamard matrices which are related to our work.

To My Parents

ACKNOWLEDGEMENTS

First I would like to thank my family for always supporting me.

I would like to extend my warmest gratitude to my supervisor, Dr. Hadi Kharaghani, for his immense amount of support, advice, and guidance throughout the process. I couldn't have done any of this without his support.

Acknowledgement also needs to be extended to my co–supervisor, Dr. Wolf Holzmann, for his constant help and continued support.

My special thanks also to the members of my defence committee, Dr. Saurya Das, Dr. Wolf Holzmann, Dr. Yury J. Ionin, Dr. Hadi Kharaghani, and Dr. Mark Walton, for their valuable comments, suggestions, and corrections.

I am grateful to Dr. Amir Akbary for his helpful conversations and valuable suggestions. His help is greatly appreciated.

I also acknowledge Dr. Hadi Kharaghani as well as the university of Lethbridge for supporting me financially.

I am grateful to Sean Legge and Stephen Ney for doing the proofreading and providing helpful suggestions.

Contents

Chapter 1

Introduction and statements of results

Definition 1.1 *A Hadamard matrix H of order n is an $n \times n$ matrix with ± 1 entries such that: $HH^t = nI_n$, where I_n is the identity matrix of order n.*

The order of a Hadamard matrix must be 1, 2 or a multiple of 4. The conjecture that all Hadamard matrices of order $4n$ exist for every positive integer n is still an important open problem. One way to generalise Hadamard matrices is by means of orthogonal designs.

Definition 1.2 *An orthogonal design A of order n and type $u_1, ..., u_t$, where each u_i is a positive integer, denoted $OD(n; u_1, ..., u_t)$, is an $n \times n$ matrix with entries from $\{0, \pm x_1, ..., \pm x_t\}$ (the x_i commuting indeterminates) satisfying*

$$AA^t = \left(\sum_{i=1}^{t} u_i x_i^2 \right) I_n.$$

Despite extensive work on the existence and properties of orthogonal designs, not many significant results are known about these matrices. One very useful constructive method for orthogonal designs is by means of T–matrices.

Definition 1.3 *Four type-1 $\{0, \pm 1\}$ matrices T_1, T_2, T_3, and T_4 of order n are T–matrices if they satisfy the following conditions:*

1. *$T_i \cap T_j = 0$ where $i \neq j$;*
2. *$\sum_{i=1}^{4} |T_i| = J$;*
3. *$\sum_{i=1}^{4} T_i T_i^t = nI$.*

By combining orthogonal designs constructible from 16 circulant matrices with T–matrices one can construct a large family of very useful orthogonal designs. Although there is an orthogonal design of order 20 constructible from 16 circulant matrices, nothing is known about the existence of such matrices of order 12. In chapter 2 we will show that $OD(12; 1, 1, 1, 9)$ and $OD(4; 1, 1, 1, 1)$ are the only orthogonal designs of type $OD(4n; 1, 1, 1, 4n - 3)$ constructible from 16 circulant matrices when n is odd. We also use an exhaustive search to show that $OD(12; 1, 1, 1, 9)$ is the only orthogonal design of order 12 on 4 variables constructible from 16 circulant matrices.

The existence of amicable set of T–matrices has proven to be instrumental in the construction of orthogonal designs.

Definition 1.4 *The T–matrices T_1, T_2, T_3, and T_4 of order n are amicable T–matrices if they satisfy the amicability condition:*

$$T_1T_2^t - T_2T_1^t + T_3T_4^t - T_4T_3^t = 0.$$

(Note that there is no specific order for T_is, and we can rename them to satisfy the amicability condition in this order.)

In part of chapter 2 we show that amicable T–matrices of *odd order* do not exist. We then conclude the chapter by a very important recent result concerning finite fields [17]. Our hope is to develop and use this result in the future to produce some positive results on the existence of T–matrices.

We devote the remaining chapters to the applications of Hadamard matrices in the construction of symmetric designs.

Definition 1.5 *A* symmetric (v, k, λ)–design *is an incidence system $(P, \mathcal{B})$ in which $P = \{p_1, p_2, \ldots, p_v\}$ is a set of v points and $\mathcal{B} = \{b_1, \ldots, b_v\}$ is a set of v blocks, each block being a k–subset of P such that any two points of P are incident with exactly λ blocks of $\mathcal{B}$.*

Symmetric designs can be expressed by their incidence matrices.

Definition 1.6 *The incidence matrix of a symmetric (v, k, λ)–design is a $v \times v$ matrix $A = [a_{ij}]$ such that*

$$a_{ij} = \begin{cases} 1 & \textit{if } p_i \in b_j \\ 0 & \textit{otherwise.} \end{cases}$$

A $(0, 1)$–matrix A is an incidence matrix of a symmetric (v, k, λ) design if and only if

$$AA^t = (k - \lambda)I + \lambda J.$$

In this thesis we only study symmetric designs constructed from productive regular Hadamard matrices. The class of productive Hadamard matrices was defined by Yury Ionin in [4].

A regular Hadamard matrix is a Hadamard matrix with constant row sum.

Definition 1.7 *A regular Hadamard matrix H with row sum $2h$ is* productive *if there is a set $\mathcal{H}$ of matrices with row sum $2h$ and a cyclic group $G =< \delta >$ where $\delta : \mathcal{H} \rightarrow \mathcal{H}$ is a bijection, such that*

1. *$H \in \mathcal{H}$;*
2. *For any $H_1, H_2 \in \mathcal{H}$, $(\delta H_1)(\delta H_2)^t = H_1 H_2^t$;*
3. *$|G| = 4|h|$;*
4. *$\sum_{\sigma \in G} \sigma H = 2\frac{h}{|h|}J$.*

Productive Hadamard matrices are normally used in Balanced Generalised Weighing matrices over cyclic groups.

Definition 1.8 *Let G be a multiplicatively written group. A* balanced generalised weighing matrix *$BGW(v, k, \lambda)$ is a matrix $W = [w_{ij}]$ of order v with $w_{ij} \in G \cup \{0\}$ such that each row and each column of W contains exactly k non–zero entries and such that for any $h \neq i$, the multiset $\{w_{hj}w_{ij}^{-1} : 1 \leq j \leq v, w_{hj} \neq 0, w_{ij} \neq 0\}$ contains exactly $\lambda/|G|$ copies of every element of G.*

A large class of balanced generalised weighing matrices of the type

$$BGW((q^m-1)/(q-1), q^{m-1}, q^{m-1}-q^{m-2})$$

over a cyclic group G, where q is a prime power, m is a positive integer and the order of G divides $q-1$, is known to exist.
A classical construction due to Ionin is as follows:

Theorem 1.9 *If there is a productive regular Hadamard matrix H with row sum $2h$ and if $q = (2h-1)^2$ is a prime power then for any positive integer m there is a symmetric design with parameters:*

$$\left(\frac{4h^2(q^{m+1}-1)}{q-1}, (2h^2-h)q^m, (h^2-h)q^m\right).$$

Bush–type Hadamard matrices are all known to be productive.

Definition 1.10 *A regular Hadamard matrix $H = [H_{ij}]$ of order $4n^2$ where H_{ij} are blocks of order $2n$ is Bush-type if $H_{ii} = J_{2n}$ and $H_{ij}J_{2n} = J_{2n}H_{ij} = 0$, for $i \neq j$, $1 \leq i, j \leq 2n$.*

The class of Bush–type Hadamard matrices is the largest class of productive regular Hadamard matrices that is known to exist. Indeed, it is known that there is a Bush–type Hadamard matrix of order $16n^2$ for all n for which there is a Hadamard matrix of order $4n$.

In chapter 4 we construct a new class of regular Hadamard matrices by combining the class of Mathon matrices with Bush–type Hadamard matrices and then construct a new family of productive regular Hadamard matrices.

Our main results in chapter 4 are as follows.

Theorem 1.11 *If there is a Hadamard matrix of order $4n$ and $m = 8n^2 - 1$ is prime then there is a productive regular Hadamard matrix of order $16n^2m^2$.*

Corollary 1.12 *If $m = 8n^2 - 1$ is prime and if $q = (4nm-1)^2$ is a prime power then there is a symmetric design with parameters:*

$$(16n^2m^2(q^t + q^{t-1} + \cdots + 1), (8n^2m^2 - 2nm)q^t, (4n^2m^2 - 2nm)q^t),$$

for any positive integer t*. Likewise if* $q = (4nm+1)^2$ *is a prime power then there is a symmetric design with parameters:*

$$(16n^2m^2(q^t + q^{t-1} + \cdots + 1), (8n^2m^2 + 2nm)q^t, (4n^2m^2 + 2nm)q^t),$$

for any positive integer t*.*

Chapter 2

Orthogonal matrices

2.1 Orthogonal designs

This chapter will be devoted to orthogonal matrices and more specifically to orthogonal designs. We begin with the definition of two important classes of matrices. We will follow Geramita and Seberry [3] for the following definition and lemma:

Definition 2.1 *Let G be an additive abelian group of order t, order the elements of G as $z_1, \ldots, z_t$ and let Ψ and Φ be two functions from G into a commutative ring. We define two matrices $M = [m_{ij}]$ and $N = [n_{ij}]$ of order t as follows:*

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

M and N are called type–1 and type–2 matrices respectively on the group G.

Lemma 2.2 *If X and Y are type–1 matrices and Z is a type–2 matrix on an abelian group G of order n with elements ordered $z_1, \ldots, z_n$, and $R = [r_{ij}]$ is defined as:*

$$r_{ij} = \begin{cases} 1 & \text{if } z_i + z_j = 0, \\ 0 & \text{otherwise} \end{cases}$$

then:

- *$XY = YX$;*
- *$Z^t = Z$;*

- *$XZ^t = ZX^t$;*

- *X^t is a type-1 matrix;*

- *$X + Y$ and $X - Y$ are type-1 matrices;*

- *XR is a type-2 matrix and ZR is a type-1 matrix.*

Definition 2.3 *Matrices A and C of order n are circulant and back-circulant matrices if they are type-1 and type-2 matrices, respectively, on the cyclic group Z_n.*

Example 1. A is a circulant matrix of order 5 and C is a back circulant matrix of order 5, where

$$A = \begin{bmatrix} a & b & c & d & e \\ e & a & b & c & d \\ d & e & a & b & c \\ c & d & e & a & b \\ b & c & d & e & a \end{bmatrix}, \quad C = \begin{bmatrix} a & b & c & d & e \\ b & c & d & e & a \\ c & d & e & a & b \\ d & e & a & b & c \\ e & a & b & c & d \end{bmatrix}$$

□

Definition 2.4 *Four type-1 $\{0, \pm 1\}$ matrices T_1, T_2, T_3, and T_4 of order n are T-matrices if they satisfy the following conditions:*

(i) *$T_i \cap T_j = 0$;*

(ii) *$\sum_i |T_i| = J$;*

(iii) *$\sum_i T_i T_i^t = nI$.*

Example 2. Matrices T_1, T_2, T_3, and T_4 are circulant T-matrices of order 3.

$$T_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad T_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad T_3 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad T_4 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

□

Definition 2.5 *An orthogonal design of order n and type $s_1, ..., s_l$, where s_i are positive integers denoted $OD(n; s_1, ..., s_l)$, is an $n \times n$ matrix A with entries from $\{0, \pm x_1, ..., \pm x_l\}$ (the x_i commuting indeterminates) satisfying*

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

There are several ways to construct orthogonal designs; one way is to use four circulant or type–1 matrices in the Goethals–Seidel array as follows.

Theorem 2.6 *Suppose there exist four circulant (type–1) matrices A, B, C, and D of order n with entries from the set $\{0, \pm x_1, \ldots, \pm x_t\}$ and suppose further that*

$$AA^t - BB^t + CC^t + DD^t = \sum_{i=1}^{t} s_i x_i^2 I_n$$

Let R be the back-diagonal (equivalent type–2) matrix of order n. Then

$$\begin{pmatrix} A & BR & CR & DR \\ -BR & A & D^tR & -C^tR \\ -CR & -D^tR & A & B^tR \\ -DR & C^tR & -B^tR & A \end{pmatrix} \tag{2.1}$$

is an $OD(4n; s_1, ..., s_t)$.

A method to produce the proper matrices A, B, C, and D to be plugged into a Goethals–Seidel array is to use T–matrices and orthogonal designs constructible from 16 circulant matrices. Turyn [15], was the first to use T–matrices and orthogonal designs constructible from 16 circulant blocks to construct new orthogonal designs.

Theorem 2.7 *If there is an $OD(4s; u_1, ..., u_n)$ constructible from 16 circulant $s \times s$ blocks in variables $x_1, ..., x_n$ and there are T–matrices of order t, then there is an $OD(4st; tu_1, ..., tu_n)$.*

Proof Let

$$P = \begin{bmatrix} P_{11} & P_{12} & P_{13} & P_{14} \\ P_{21} & P_{22} & P_{23} & P_{24} \\ P_{31} & P_{32} & P_{33} & P_{34} \\ P_{41} & P_{42} & P_{43} & P_{44} \end{bmatrix}$$

be an $OD(4n; u_1, ..., u_n)$ constructible from 16 circulant matrices P_{ij}, $1 \leq i, j \leq 4$. We have

$$P_{i1}P_{j1}^t + P_{i2}P_{j2}^t + P_{i3}P_{j3}^t + P_{i4}P_{j4}^t = \begin{cases} \sum_{k=1}^n u_k x_k^2, & i = j; \\ 0, & i \neq j. \end{cases}$$

Suppose that T_1, T_2, T_3, and T_4 are T–matrices of order t. Let

$$A = T_1 \otimes P_{11} + T_2 \otimes P_{21} + T_3 \otimes P_{31} + T_4 \otimes P_{41},$$

$$B = T_1 \otimes P_{12} + T_2 \otimes P_{22} + T_3 \otimes P_{32} + T_4 \otimes P_{42},$$

$$C = T_1 \otimes P_{13} + T_2 \otimes P_{23} + T_3 \otimes P_{33} + T_4 \otimes P_{43},$$

$$D = T_1 \otimes P_{14} + T_2 \otimes P_{24} + T_3 \otimes P_{34} + T_4 \otimes P_{44}.$$

It is easy to see that

$$AA^t + BB^t + CC^t + DD^t = \sum_{k=1}^{n} t u_k x_k^2 I_{st},$$

and A, B, C, and D are type–1 matrices. Thus they can be plugged into a Goethals–Seidel array to give an $OD(4st; tu_1, ..., tu_n)$. □

Despite the fact that there is a Welch array of order 20 constructible from 16 circulant matrices and an Ono–Sawade–Yumamoto array of order 36 constructible from 16 block circulant matrices [14], nothing similar is known for order 12. We will first study and settle the case for order 12.

The following orthogonal design is an $OD(12;1,1,1,9)$ constructible from 16 circulant matrices.

$$\begin{bmatrix}
\eta & \eta & \eta & a & \overline{\eta} & \eta & b & \overline{\eta} & \eta & c & \overline{\eta} & \eta \\
\eta & \eta & \eta & \eta & a & \overline{\eta} & \eta & b & \overline{\eta} & \eta & c & \overline{\eta} \\
\eta & \eta & \eta & \overline{\eta} & \eta & a & \overline{\eta} & \eta & b & \overline{\eta} & \eta & c \\
 & & & & & & & & & & & \\
a & \overline{\eta} & \eta & \overline{\eta} & \overline{\eta} & \overline{\eta} & \bar{c} & \overline{\eta} & \eta & b & \eta & \overline{\eta} \\
\eta & a & \overline{\eta} & \overline{\eta} & \overline{\eta} & \overline{\eta} & \eta & \bar{c} & \overline{\eta} & \overline{\eta} & b & \eta \\
\overline{\eta} & \eta & a & \overline{\eta} & \overline{\eta} & \overline{\eta} & \overline{\eta} & \eta & \bar{c} & \eta & \overline{\eta} & b \\
 & & & & & & & & & & & \\
\bar{b} & \eta & \overline{\eta} & \bar{c} & \overline{\eta} & \eta & \eta & \eta & \eta & a & \eta & \overline{\eta} \\
\overline{\eta} & \bar{b} & \eta & \eta & \bar{c} & \overline{\eta} & \eta & \eta & \eta & \overline{\eta} & a & \eta \\
\eta & \overline{\eta} & \bar{b} & \overline{\eta} & \eta & \bar{c} & \eta & \eta & \eta & \eta & \overline{\eta} & a \\
 & & & & & & & & & & & \\
c & \overline{\eta} & \eta & \bar{b} & \overline{\eta} & \eta & a & \eta & \overline{\eta} & \overline{\eta} & \overline{\eta} & \overline{\eta} \\
\eta & c & \overline{\eta} & \eta & \bar{b} & \overline{\eta} & \overline{\eta} & a & \eta & \overline{\eta} & \overline{\eta} & \overline{\eta} \\
\overline{\eta} & \eta & c & \overline{\eta} & \eta & \bar{b} & \eta & \overline{\eta} & a & \overline{\eta} & \overline{\eta} & \overline{\eta}
\end{bmatrix}$$

We will first show that $OD(12;1,1,1,9)$ and the trivial $OD(4;1,1,1,1)$ are the only orthogonal designs of type $OD(4n;1,1,1,4n-3)$ constructible from 16 circulant matrices whenever n is an odd number. We will then show, by an exhaustive computer search, that this $OD(12;1,1,1,9)$ is the only orthogonal design in four variables constructible from 16 circulant matrices.

Theorem 2.8 *If n is an odd number then $OD(12;1,1,1,9)$ and $OD(4;1,1,1,1)$ are the only orthogonal designs of the form $OD(4n;1,1,1,4n-3)$ constructible from 16 circulant matrices.*

Proof Let

$$P = \begin{pmatrix} P_{11} & P_{12} & P_{13} & P_{14} \\ P_{21} & P_{22} & P_{23} & P_{24} \\ P_{31} & P_{32} & P_{33} & P_{34} \\ P_{41} & P_{42} & P_{43} & P_{44} \end{pmatrix} \tag{2.2}$$

be an $OD(4n;1,1,1,4n-3)$ constructible from 16 circulant matrices P_{ij}, $1 \leq i,j \leq 4$. Let a,b,c be the variables that appear once in each row (and column) of P and let η

be the variable that appears $4n-3$ times in each row. We have

$$\sum_{1\leq j\leq 4} P_{ij}P_{ij}^t = (a^2+b^2+c^2+(4n-3)\eta^2)I, \quad 1\leq i\leq 4 \tag{2.3}$$

and

$$\sum_{1\leq j\leq 4} P_{ij}P_{kj}^t = 0, \quad 1\leq i,k\leq 4, \quad i\neq k. \tag{2.4}$$

Since P_{ij} is a circulant matrix satisfying (2.3), each of a, b, or c can appear only in one block P_{ij}. For convenience we will denote the block containing x by X_l, and call it x–type, for $x\in\{a,b,c\}$. The block whose entries are only $\pm\eta$ will be called η–type. So the matrix P in the new notation is of the form:

$$P=\begin{pmatrix} M_1 & A_1 & B_1 & C_1 \\ A_2 & -M_2 & -C_2 & B_2 \\ -B_3 & -C_3 & M_3 & A_3 \\ C_4 & -B_4 & A_4 & -M_4 \end{pmatrix}, \tag{2.5}$$

where each A_i, B_i, C_i, M_i is an a, b, c, η–type matrix respectively. Since A_i, B_i, and C_i are circulant matrices, by shifting the rows or columns we can always put the variables a, b, and c on the diagonal of the corresponding matrix and then the matrix will be called a diagonal matrix. By column permutations on block columns 2, 3, and 4 of the matrix P we can make A_1, B_1, and C_1 diagonal matrices. By row permutations on block rows 2, 3, and 4 of P we can make B_2, A_3, and A_4 diagonal matrices and then by column shifts on block row 1 make A_2 a diagonal matrix. It is easy to see that the fact that B_1, C_1, and B_2 being diagonal matrices together with condition (2.4) implies that C_2 is a diagonal matrix. By the same reasoning, C_3, B_3, B_4, and C_4 are diagonal matrices. Because A_1, B_1, and C_1 are diagonal matrices we have:

$$M_1=M, A_1=A=aI+A', B_1=B=bI+B', \text{ and } C_1=C=cI+C'$$

where A', B', and C' are $\{0,\pm\eta\}$ matrices. Then by (2.3) we have:

$$\begin{aligned} MM^t+(aI+A')(aI+A'^t)+(bI+B')(bI+B'^t)+(cI+C')(cI+C'^t) \\ =MM^t+A'A'^t+B'B'^t+C'C'^t+(a^2+b^2+c^2)I \\ +a(A'+A'^t)+b(B'+B'^t)+c(C'+C'^t) \\ =(a^2+b^2+c^2+(4n-3)\eta^2)I, \end{aligned}$$

so we get $A''^t = -A'$, $B''^t = -B'$, and $C''^t = -C'$ and also

$$MM^t - A'^2 - B'^2 - C'^2 = (4n-3)\eta^2 I. \tag{2.6}$$

As A_2, B_2, and C_2 are diagonal matrices we can write $A_2 = aI + A_2'$, $B_2 = bI + B_2'$, and $C_2 = cI + C_2'$ where A_2', B_2', and C_2' are $\{0, \pm\eta\}$ matrices. Considering block rows 1 and 2, by (2.4) we can write

$$\begin{aligned} MA_2^t - AM_2^t - BC_2^t + CB_2^t &= M(aI + A_2''^t) - (aI + A')M_2^t \\ &\quad -(bI + B')(cI + C_2''^t) + (cI + C')(bI + B_2''^t) \\ &= a(M - M_2^t) + MA_2''^t - A'M_2^t \\ &\quad +b(C' - C_2''^t) + c(B_2''^t - B') - B'C_2''^t + C'B_2''^t \\ &= 0. \end{aligned} \tag{2.7}$$

Thus $M_2 = M^t$, $B_2' = B''^t$, and $C_2' = C''^t$. As $B_2 = (bI + B_2')$ and $C_2 = (cI + C_2')$ we have $B_2 = B^t$ and $C_2 = C^t$. By checking the orthogonality of block rows 1 and 3 we get $M_3 = M^t$ and by checking block rows 2 and 3 we get $M^t = M_3 = M_2^t = (M^t)^t = M$, so it follows that

$$M = M^t.$$

By checking the orthogonality of the other block rows and columns we achieve a similar result for the other blocks so the matrix P can be converted to the form

$$P' = \begin{bmatrix} M & A & B & C \\ A & -M & -C^t & B^t \\ -B & -C^t & M & A^t \\ C & -B^t & A^t & -M \end{bmatrix} \tag{2.8}$$

By (2.7) we have $MA_2''^t - A'M_2^t = MA''^t - A'M^t = MA''^t - A'M = 0$, but we also know that $A''^t = -A'$, so $M(A''^t - A') = -2MA' = 0$ and thus

$$MA' = 0. \tag{2.9}$$

Now we want to find all the solutions of (2.9). As n is odd and A' is a circulant matrix and $A''^t = -A'$, the row sum and column sum of each row and column of the matrix

A' is 0 and thus it is clear that $\pm\eta J$ is a solution of equation (2.9).

We will now show that $\pm\eta J$ is the only solution of (2.9). We know M is a $\pm\eta$–matrix and A' is a $\{0, \pm\eta\}$–matrix. Let $A' = \eta\mathcal{A}$ and $M = \eta\mathcal{M}$. So $\mathcal{M}$ is a ± 1 and $\mathcal{A}$ is a $\{0, \pm 1\}$ matrix. By (2.9) we have $\mathcal{M}\mathcal{A} = 0$. ηJ is a solution of (2.9) so $J\mathcal{A} = 0$. By adding these two equations we have $(\mathcal{M} + J)\mathcal{A} = 0$. Let $\mathcal{N} = (\mathcal{M} + J)/2$. Then $\mathcal{N}$ is a $\{0, 1\}$ matrix and

$$\mathcal{N}\mathcal{A} = 0. \tag{2.10}$$

If $\mathcal{N}$ is a solution of (2.10) in $\mathbb{Z}$ it should be a solution of (2.10) in $\mathbb{Z}_2$. In $\mathbb{Z}_2$, $\mathcal{A} = circ(0, 1, \ldots, 1) = J - I$. In $\mathbb{Z}_2$ by (2.10) we have

$$\mathcal{N}\mathcal{A} = \mathcal{N}(J - I) = 0,$$

so

$$\mathcal{N} = \mathcal{N}J.$$

As $\mathcal{N}$ is a circulant matrix it has constant row sum and column sum. It is clear that $\mathcal{N}J$ is either 0 or J. So, $\mathcal{N}$ is either 0 or J.

Thus $\pm J$ is the only solution for $\mathcal{M}$ and $\pm\eta J$ is the only solution for M. As $M = \pm\eta J$ by (2.6) we have

$$\eta^2 J^2 - A'^2 - B'^2 - C'^2 = (4n - 3)\eta^2 I \tag{2.11}$$

Let e_n be an nx1 vector of all ones. Since the row sums and column sums of the matrices A', B', and C' are zero we have $e_n A' = e_n B' = e_n C' = 0$. By multiplying the two sides of equation (2.11) by e_n we have

$$\eta^2 n^2 e_n = \eta^2(4n - 3)e_n.$$

Thus $(n - 3)(n - 1) = 0$ and $n = 1$ or 3, and this completes the proof. □

2.2 An exhaustive search

We were able to prove using an exhaustive search that the only orthogonal design of order 12 constructible from 16 circulant blocks on 4 variables is $OD(12; 1, 1, 1, 9)$. The main technique in this exhaustive search is the *reversing process* which was introduced for the first time in [11]. In order to find the desired orthogonal designs, first we characterise all Hadamard matrices of order 12 constructible from 16 circulant blocks. We start by finding all 3×12, $\{\pm 1\}$ matrices

$$H'' = \begin{bmatrix} H_{11} & H_{12} & H_{13} & H_{14} \end{bmatrix}$$

constructible from four circulant blocks H_{11}, H_{12}, H_{13}, and H_{14} such that:

$$H''H''^t = 12I_3.$$

Let $\mathcal{H}''$ be the set of matrices H'' that we have found. Now by checking all the pairs $H_1'', H_2'' \in \mathcal{H}''$ such that

$$H_1''H_2''^t = 0$$

we are able to find all 6×12, $\{\pm 1\}$ matrices

$$H' = \begin{bmatrix} H_{11} & H_{12} & H_{13} & H_{14} \\ H_{21} & H_{22} & H_{23} & H_{24} \end{bmatrix}$$

constructible from 8 circulant blocks H_{ij}, $i = 1, 2$ and $j = 1, 2, 3, 4$ such that

$$H'H'^t = 12I_6.$$

Continuing the same method by checking all the pairs of above matrices that satisfy the orthogonality condition we can find all Hadamard matrices $H = [H_{ij}]$, $1 \le i, j \le 4$ constructible from 16 circulant blocks. Now we implement the reversing process. Consider that $H_1 = [h_{ij}]$ and $H_2 = [k_{ij}]$ are two Hadamard matrices of order 12 constructible from 16 circulant blocks. Let $D = [d_{ij}]$ such that:

$$d_{ij} = \begin{cases} \pm a \text{ if } h_{ij} = \pm 1 \text{ and } k_{ij} = \pm 1 \\ \pm b \text{ if } h_{ij} = \pm 1 \text{ and } k_{ij} = \mp 1. \end{cases}$$

Then D is a candidate for an orthogonal design of order 12 constructible from 16 circulant blocks on 2 variables a and b. If D is orthogonal we are done. Comparing all possible pairs of matrices H_1 and H_2 we classify all desired orthogonal designs on 2 variables. All we found were one of each of $OD(12; 9, 3)$, $OD(12; 10, 2)$, and $OD(12; 11, 1)$. From this fact it is clear that $OD(12; 1, 1, 1, 9)$ is the only orthogonal design of order 12 constructible from 16 circulant blocks. We tried to use the same method to classify orthogonal designs of order 20 constructible from 16 circulant blocks. Because in the first stage the number of 5×20 matrices H'' constructible from 4 circulant blocks such that $H''H''^t = 20I_5$ is huge, we were not able to run the second stage. However we did a random search instead of an exhaustive search and found an $OD(20; a, b)$ constructible from 16 circulant blocks for each pair (a, b), such that $1 \leq a, b \leq 19$ and $a + b = 20$.

2.3 A non–existence theorem

In this section we show that there do not exist amicable T–matrices of odd order.

Theorem 2.9 *There are no four full circulant T-matrices T_1, T_2, T_3, and T_4 of order n if n is odd satisfying:*

$$T_1T_2^t - T_2T_1^t + T_3T_4^t - T_4T_3^t = 0 \tag{2.12}$$

Proof Assume otherwise for a contradiction. Reduce the matrices mod 2, (notice that $A \equiv -A$ for every matrix A.) Let $U = T_1 + T_2$ and $V = T_3 + T_4$. Then using the complementary and amicability conditions we obtain:

$$UU^t + VV^t = (\sum_i T_iT_i^t) + T_1T_2^t + T_2T_1^t + T_3T_4^t + T_4T_3^t = I.$$

We have $U + V = J$, so $V = U + J$. Using that $T_iJ^t = JT_i^t$ for circulant matrices T_i we have

$$\begin{aligned} I &\equiv UU^t + VV^t \\ &\equiv UU^t + UU^t + UJ^t + JU^t + JJ^t \\ &\equiv JJ^t \\ &\equiv J. \end{aligned}$$

This is a contradiction. □

2.4 A family of T–matrices

In this section we introduce an infinite family of T–matrices. These matrices were introduced by Xia and Xia in [17]. The method is to divide $GF(q^2)$ where $q = 8m + 3$ is a prime power into so called C–*partitions. Note that we are reproducing the work of Xia and Xia in [17] and [16] here in this thesis with some minor modifications.*

In order to construct such matrices we show that a special class of supplementary difference sets exists. Supplementary difference set (SDS) is a generalisation of difference set. Let G be an abelian group with addition $\oplus$, subtraction $\ominus$, and zero element θ. Consider the group ring $\mathbb{Z}[G]$ of the group G over the ring of integers; the elements of $Z[G]$ can be expressed as polynomials

$$\sum_i a_i g_i$$

where $a_i \in \mathbb{Z}$ and $g_i \in G$. In $\mathbb{Z}[G]$ addition is defined by:

$$\left(\sum_i a_i g_i\right) + \left(\sum_i b_i g_i\right) = \sum_i (a_i + b_i) g_i.$$

If G is a finite field multiplication is defined by:

$$\left(\sum_i a_i g_i\right)\left(\sum_i b_i g_i\right) = \sum_k \left(\sum_{g_i g_j = g_k} a_i b_j\right) g_k.$$

Let

$$T = \sum_{g \in G} g \text{ and } T^* = T - \theta.$$

For non–empty subsets A and B of G we define:

$$A \ominus B = \sum_{a \in A,\ b \in B} (a \ominus b),$$

$$\Delta A = A \ominus A,$$

$$\Delta(A, B) = (A \ominus B) + (B \ominus A),$$

$$\Delta\emptyset = \Delta(\emptyset, A) = 0.$$

It is easy to see that $\Delta(A, A) = 2\Delta(A)$.
The following trivial identitics are useful:
If $B \cap C = \emptyset$ then

$$\Delta(A, B \cup C) = \Delta(A, B) + \Delta(A, C), \tag{2.13}$$

$$\Delta(B \cup C) = \Delta(B) + \Delta(B, C) + \Delta(C). \tag{2.14}$$

Definition 2.10 *A k-subset D of an abelian group G of order v is called a (v, k, λ)-difference set if*

$$\Delta D = (k - \lambda)\theta + \lambda T$$

for some non-negative integer λ.

Definition 2.11 *A collection of subsets $\{D_1, D_2, \ldots, D_r\}$ of an abelian group G of order v such that $|D_i| = k_i$ is called a $(v, k_1, k_2, \ldots, k_r, \lambda)$-supplementary difference set if*

$$\Delta D = \left(\sum_{i=1}^{r} k_i - \lambda \right) \theta + \lambda T$$

for some non-negative integer λ.

Clearly if $r = 1$ the supplementary difference set is equivalent to a difference set.

If $r = 4$ and $\lambda = \sum_{i=1}^{4} k_i - v$ the collection $\{D_1, D_2, D_3, D_4\}$ is called an SDS of type H. Now we show that an SDS of type H exists where $G = GF(q^2)$, $q \equiv 3 (\text{mod } 8)$ is a prime power, and every element of G appears an even number of times in the system of $\{D_1, D_2, D_3, D_4\}$. Later we prove that one can construct T-matrices using this particular type of SDS.

Consider that $v = q^2$, $q = 4m + 3$ is a prime power, and g is a generator of the multiplicative group of $G = GF(v)$. Define

$$E_i := \{g^{8(m+1)j+i} | j = 0, \ldots, 2m\}, \ i = 0, 1, \ldots, 8m + 7,$$

$$S_i := E_i \cup E_{i+4m+4}, \ T_i := \sum_{h \in S_i} h, \ i = 0, 1, \ldots, 4m + 3.$$

We have:

$$\begin{aligned}
\sum_{i=0}^{4m+3} T_i &= \sum_{i=0}^{4m+3} \sum_{h \in S_i} h \\
&= \sum_{i=0}^{4m+3} \sum_{j=0}^{2m} (g^{4(m+1)(2j)+i} + g^{4(m+1)(2j+1)+i}) \\
&= \sum_{k=0}^{16m^2+24m+8} g^k \\
&= \sum_{k=0}^{q^2-1} g^k \\
&= T^*.
\end{aligned}$$

Define

$$E_i = E_j \text{ as } i \equiv j (\text{mod } 8\text{m} + 8),$$

$$S_i = S_j,\ T_i = T_j \text{ as } i \equiv j (\text{mod } 4\text{m} + 4).$$

It is easy to see that $gE_i = E_{i+1}$, $gS_i = S_{i+1}$, and $gT_i = T_{i+1}$. Define

$$\Phi_0 = \Delta E_0,$$

$$\Phi_i = \Delta(E_0, E_i),\ i = 1, 2, \ldots, 8m + 7,$$

$$\Phi_i = \Phi_j \text{ as } i \equiv j (\text{mod } 8\text{m} + 8).$$

We have

$$\begin{aligned}
\Delta E_i &= \sum_{j=0}^{2m} \sum_{j'=0}^{2m} g^{8(m+1)j+i} \ominus g^{8(m+1)j'+i} \\
&= \sum_{j=0}^{2m} \sum_{j'=0}^{2m} g^i (g^{8(m+1)j} \ominus g^{8(m+1)j'}) \\
&= g^i \sum_{j=0}^{2m} \sum_{j'=0}^{2m} g^{8(m+1)j} \ominus g^{8(m+1)j'} \\
&= g^i \Phi_0
\end{aligned}$$

for $i = 0, 1, \ldots, 8m + 8$. Similarly we can show that

$$\Delta(E_i, E_j) = g^i \Phi_{j-i}$$

for $i \neq j$, and also

$$\Phi_i = g^i \Phi_{-i} = g^i \Phi_{8m+8-i}$$

for $i = 1, 2, \ldots, 8m + 7$.

Lemma 2.12 *Let $G = GF(q^2)$ be an extension of $GF(q)$ then*

$$E_0 \cup E_{4m+4} = GF(q)^*.$$

Proof It is sufficient to show that $g^{4(m+1)} \in GF(q)$. Consider the polynomial $x^{q-1} \ominus 1 = 0$ in $GF(q^2)$. Clearly this polynomial has $q - 1$ roots, since the order of the multiplicative group of $GF(q)$ is $q - 1$ we have $x^{q-1} = 1$ for all $x \in GF(q)$. Thus all the roots of the polynomial $x^{q-1} \ominus 1 = 0$ are in $GF(q)$. On the other hand we have

$$(g^{4(m+1)})^{q-1} \ominus 1 = g^{q^2-1} \ominus 1 = 1 \ominus 1 = 0.$$

Since $g^{4(m+1)}$ is one of the roots of the polynomial $x^{q-1} \ominus 1 = 0$, it is in $GF(q)$. By a simple counting we have:

$$E_0 \cup E_{4m+4} = GF(q)^*.$$

□

Here we need to show that:

Lemma 2.13 *[1] The set of all non-zero squares in $GF(q)$ form a $\left(q, \frac{1}{2}(q-1), \frac{1}{4}(q-3)\right)$-difference set.*

Proof Let α be a primitive element of $GF(q)$ and let D be the set of all non-zero squares in $GF(q)$. We have $D = \{\alpha^0, \alpha^2, \ldots, \alpha^{4m}\}$. Since $q \equiv 3 (\text{mod } 4)$ we have $-1 \notin D$ and $-D = \{\alpha, \alpha^3, \ldots, \alpha^{4m+1}\}$. Let a_i and b_i, $i = 1, \ldots n$ be the set of all integers such that

$$1 = \alpha^{2a_i} \ominus \alpha^{2b_i}.$$

Then for any $\alpha^{2t} \in D$ we have

$$\alpha^{2t} = \alpha^{2(a_i+t)} \ominus \alpha^{2(b_i+t)}.$$

So every representation of 1 as the difference of the elements of D gives us a representation of α^{2t} as the difference of the elements of D and vice versa. For any element $\alpha^{2t+1} \notin D$ we have $\alpha^{2t+1} \in -D$ so $\alpha^{2t+1} = -\alpha^{2t'}$ for some integer t', we have

$$\alpha^{2t+1} = \alpha^{2(b_i+t')} \ominus \alpha^{2(2_i+t')}.$$

Thus every representation of 1 as the difference of the elements of D gives us a representation of α^{2t+1} as the difference of the elements of D and vice versa. So D is a difference set in $GF(q)$. Clearly $k = |D| = \frac{1}{2}(q-1)$. Since we have $k(k-1)$ differences in D and each of the $q-1$ non–zero elements of $GF(q)$ appears λ times we have $k(k-1) = \lambda(q-1)$ so we have $\lambda = \frac{1}{4}(q-3)$. □

Lemma 2.14 *The polynomials Φ_i satisfy the following properties:*

(i) $\Phi_0 = (2m+1)\theta + mT_0$;

(ii) $\Phi_{4m+4} = (2m+1)T_0$;

(iii) $\Phi_i + \Phi_{i+4m+4} = T^* - T_0 - T_i,\ i = 1, 2, \ldots, 4m+3$.

Proof To prove (i) using Lemma 2.12 and 2.13 we get

$$\Phi_0 = \Delta E_0 = |E_0|\theta + mT_0 = (2m+1)\theta + mT_0.$$

To prove (ii) we have:

$$\begin{aligned}
\Phi_{4m+4} &= \Delta(E_0, E_{4m+4}) \\
&= \Delta(E_0, GF(q) \setminus (E_0 \cup \theta)) \\
&= \Delta(E_0, GF(q)) - \Delta(E_0, E_0) - \Delta(E_0, \theta) \\
&= 2|E_0|(T_0 + \theta) - 2\Delta(E_0) - T_0 \\
&= 2(2m+1)T_0 + 2(2m+1)\theta - 2(2m+1)\theta - 2mT_0 - T_0 \\
&= (2m+1)T_0.
\end{aligned}$$

Since $q \equiv 3 (\mathrm{mod}\ 4)$ the polynomial $x^2 \oplus 1$ is irreducible in $GF(q)$ and the elements of $GF(q^2)$ can be represented by polynomials $ai \ominus b$, $a, b \in GF(q)$ where $i^2 = -1$. Let

$h = g^{4(m-1)}$, we know that h is a primitive element of $GF(q)$. We have $(g^{2(m+1)})^2 = h^1 = -h^{2t} = i^2h^{2t}$ for some integer t, so

$$g^{2m+2} = h^t i.$$

Thus we have:

$$E_0 = \{h^{2j} | j = 0, \ldots, 2m\},$$
$$S_{2m+2} = \{h^j i | j = 0, \ldots, 4m-1\}.$$

Now we have:

$$\begin{aligned}
\Phi_{2m+2} + \Phi_{6m+6} &= \Delta(E_0, E_{2m+2}) + \Delta(E_0, E_{6m+6}) \\
&= \Delta(E_0, S_{2m+2}) \\
&= \sum_{\substack{0 \le j \le 4m-1 \\ 0 \le k \le 2m}} \left((h^{2k} \ominus h^j i) + (h^j i \ominus h^{2k})\right) \\
&= \sum_{\substack{0 \le j \le 4m-1 \\ 0 \le k \le 2m}} \left((h^{2k} \oplus h^j i) + (h^j i \oplus h^{2k+1})\right) \\
&= \sum_{0 \le j,k \le 4m+1} (h^j i \oplus h^k) \\
&= T^* - T_0 - T_{2m+2}.
\end{aligned}$$

For $1 \le l \le 4m+3$ and $l \ne 2m+2$ we have $g^l = h^\alpha i \oplus h^\beta$ for some integers α and β. We have:

$$S_l = E_l \cup E_{l+4m+4} = \{h^{\alpha+j} i \oplus h^{\beta+j} | j = 0, \ldots 4m-1\}.$$

Thus

$$\begin{aligned}
\Phi_l + \Phi_{l+4m+4} &= \Delta(E_0, S_l) \\
&= \sum_{\substack{0\le j\le 4m+1 \\ 0\le k\le 2m}} \left((h^{2k} \ominus (h^{\alpha+j} i \oplus h^{\beta+j})) + ((h^{\alpha+j} i \ominus h^{\beta+j}) \ominus h^{2k})\right) \\
&= \sum_{\substack{0\le j\le 4m+1 \\ 0\le k\le 2m}} \left((h^{2k} \ominus h^{\alpha+j} i \oplus h^{\beta+j}) + (h^{\alpha+j} i \ominus h^{\beta+j} \oplus h^{2k-1})\right) \\
&= \sum_{0\le j,k\le 4m+1} \left(h^{\alpha+j} i \ominus (h^{\beta+j} \oplus h^{k})\right) \\
&= \sum_{\substack{0\le j\le 4m+1 \\ a\in GF(q)}} (h^{\alpha+j} i \ominus a) - \sum_{0\le j\le 4m+1} (h^{\alpha+j} i \ominus h^{\beta+j}) \\
&= T^* - T_0 - T_i.
\end{aligned}$$

□

Lemma 2.15 *If* $D = \cup_{i=0}^{2t} E_{a_i} \cup (\cup_{j=1}^{2m+1-t} S_{b_j})$, $0 \le t \le 2m+1$, *where* $a_i \not\equiv a_j (\text{mod } 4\text{m}+4)$ *for* $i \ne j (\text{mod } 4\text{m}+4)$, *and* $a_i \not\equiv b_j$, $i = 0, \ldots, 2t$, $j = 1, \ldots, 2m+1-t$, *then*

$$\begin{aligned}
\Delta D &= 2(2m+1)(2m+1-t)\theta + (4m^2+4m+1-t^2)T^* \\
&\quad +(t-2m-1)\sum_{i=0}^{2t} T_{a_i} + \Delta(\cup_{i=0}^{2t} E_{a_i})
\end{aligned}$$

Proof We have:

$$\begin{aligned}
\Delta(E_{a_i}, S_{b_j}) &= \Delta(E_{a_i}, E_{b_j}) + \Delta(E_{a_i}; E_{b_j+4m+4}) \\
&= g^{a_i}\Phi_{b_j-a_i} + g^{a_i}\Phi_{b_j-a_i+4m+4} \\
&= g^{a_i}(\Phi_{b_j-a_i} + \Phi_{b_j-a_i+4m+4}) \\
&= g^{a_i}(T^* - T_0 - T_{b_j-a_i}) \\
&= T^* - T_{a_i} - T_{b_j}.
\end{aligned}$$

Thus

$$\begin{aligned}
\Delta(\cup_{i=0}^{2t} E_{a_i}, \cup_{j=1}^{2m+1-t} S_{b_j}) &= \sum_{i=0}^{2t} \sum_{j=1}^{2m+1-t} \Delta(E_{a_i}, S_{b_j}) \\
&= \sum_{i=0}^{2t} \sum_{j=1}^{2m+1-t} (T^* - T_{a_i} - T_{b_j}) \\
&= (2t+1)(2m+1-t)T^* - (2t+1) \sum_{j=1}^{2m+1-t} T_{b_j} \\
&\quad -(2m+1-t) \sum_{i=0}^{2t} T_{a_i}.
\end{aligned}$$

We have:

$$\begin{aligned}
\Delta(S_{b_j}) &= \Delta(E_{b_j}) + \Delta(E_{b_j+4m+4}) + \Delta(E_{b_j}, E_{b_j+4m+4}) \\
&= g^{b_j}\Phi_0 + g^{b_j+4m+4}\Phi_0 + g^{b_j}\Phi_{4m+4} \\
&= g^{b_j}[(2m+1)\theta + mT_0] + g^{b_j}g^{4m+4}[(2m+1)\theta + mT_0] + g^{b_j}(2m+1)T_0 \\
&= (2m+2)\theta + (4m+1)T_{b_j}.
\end{aligned}$$

If $i \neq j$ we have

$$\begin{aligned}
\Delta(S_{b_i}, S_{b_j}) &= \Delta(E_{b_i}, E_{b_j}) + \Delta(E_{b_i}, E_{b_j+4m+4}) + \Delta(E_{b_i+4m+4}, E_{b_j}) \\
&\quad +\Delta(E_{b_i+4m+4}, E_{b_j+4m+4}) \\
&= g^{b_i}(\Phi_{b_j-b_i} + \Phi_{b_j-b_i+4m+4}) + g^{b_i+4m+4}(\Phi_{b_j-b_i} + \Phi_{b_j-b_i+4m+4}) \\
&= g^{b_i}(T^* - T_0 - T_{b_j-b_i}) + g^{b_i}g^{4m+4}(T^* - T_0 - T_{b_j-b_i}) \\
&= 2g^{b_i}(T^* - T_0 - T_{b_j-b_i}) \\
&= 2(T^* - T_{b_i} - T_{b_j}).
\end{aligned}$$

Thus

$$
\begin{aligned}
\Delta(\cup_{j=1}^{2m+1-t} S_{b_j}) &= \sum_{j=1}^{2m+1-t} \Delta S_{b_j} + \sum_{i=1}^{2m-t} \sum_{j=i+1}^{2m+1-t} \Delta(S_{b_i}, S_{b_j}) \\
&= (2m+1-t)(4m+2)\theta + (4m+1) \sum_{j=1}^{2m+1-t} T_{b_j} \\
&\quad + \sum_{i=1}^{2m-t} \sum_{j=i+1}^{2m+1-t} 2(T^* - T_{b_i} - T_{b_j}) \\
&= (2m+1-t)(4m+2)\theta + (2t+1) \sum_{j=1}^{2m+1-t} T_{b_j} \\
&\quad +(2m-t)(2m+1-t)T^*.
\end{aligned}
$$

Now we have:

$$
\begin{aligned}
\Delta D &= \Delta(\cup_{i=0}^{2t} E_{a_i}) + \Delta(\cup_{j=1}^{2m+1-t} S_{b_j}) + \Delta(\cup_{i=0}^{2t} E_{a_i}, \cup_{j=1}^{2m+1-t} S_{b_j}) \\
&= 2(2m+1)(2m+1-t)\theta + (4m^2+4m+1-t^2)T^* \\
&\quad +(t-2m-1)\sum_{i=0}^{2t} T_{a_i} + \Delta(\cup_{i=0}^{2t} E_{a_i}).
\end{aligned}
$$

□

Let $m = 2r$. We have $q = 8r - 3$ is a prime power. Define:

$$
F_i := \cup_{j=0}^{2r} E_{8j+i}, \; i = 0, 1, \ldots, 7
$$

$$
G_i := \sum_{a \in F_i \cup F_{i+4}} a, \; i = 0, 1, 2, 3.
$$

Lemma 2.16 *The subsets F_i, $i = 0, \ldots, 7$, have the following properties:*

(i) $\Delta(F_0, F_5) = \Delta(F_1, F_4)$;

(ii) $2(\sum_{i=0}^{3} g^i)\Delta F_0 = 8(2r+1)(4r+1)\theta + ((2r+1)(4r+1) - 1)T^*$;

(iii) $(\sum_{i=0}^{3} g^i)\Delta(F_0, F_3) = (2r+1)(4r+1)T^*$;

(iv) $\Delta(F_0, F_2 \cup F_6) = (2r+1)^2 T^* - (2r+1)(G_0 + G_2)$.

Proof To prove (i) first we have to show that

$$h\Phi_i = \Phi_i$$

where $h = g^{4m+4}$. We have:

$$\begin{aligned} h\Phi_i &= h\Delta(E_0, E_i) = \Delta(hE_0, hE_i) \\ &= \Delta(\ominus E_0, \ominus E_i) = \Delta(E_0, E_i) \\ &= \Phi_i. \end{aligned}$$

Now we have:

$$\begin{aligned} \Delta(F_1, F_4) &= \sum_{i=0}^{2r}\sum_{j=0}^{2r} \Delta(E_{8i+1}, E_{8j+4}) \\ &= \sum_{i=0}^{2r}\sum_{j=0}^{2r} \Delta(E_{8(i-r)+1}, E_{8(j+r)+4}) \\ &= \sum_{i=0}^{2r}\sum_{j=0}^{2r} g^{8j+8r+4}\Phi_{8(j-i+2r)+3} \\ &= \sum_{i=0}^{2r}\sum_{j=0}^{2r} g^{8j+4m+4}\Phi_{8m+8-8(j-i+m)-3} \\ &= \sum_{i=0}^{2r}\sum_{j=0}^{2r} g^{8j}g^{4m+4}\Phi_{8(i-j)+5} \\ &= \sum_{i=0}^{2r}\sum_{j=0}^{2r} g^{8j}\Phi_{8(i-j)+5} \\ &= \sum_{i=0}^{2r}\sum_{j=0}^{2r} \Delta(E_{8j}, E_{8i+5}) \\ &= \Delta(F_0, F_5). \end{aligned}$$

To prove (ii) we follow the proof of Lemma 2.13. Let a_i and b_i, $i = 1, \ldots n$ be the set of all integers such that

$$g^l = g^{8a_i} \ominus g^{8b_i}, l = 0, 1, 2, 3.$$

Then for any g^{8t+l} we have

$$g^{8t+l} = g^{8(a_i+t)} \ominus g^{8(b_i+t)}.$$

So every representation of g^l as the difference of the elements of F_0 gives us a representation of g^{8t+l} as the difference of the elements of F_0 and vice versa. For any element g^{8t+l+4} we have $g^{8t+l+4} = \ominus g^{8t'+l}$ for some integer t', thus

$$g^{8t+l+4} = g^{8(b_i+t')} \ominus g^{8(a_i+t')}.$$

So every representation of g^l as the difference of the elements of F_0 gives us a representation of g^{8t+l+4} as the difference of the elements of F_0 and vice versa. So we have:

$$\Delta F_0 = (2r+1)(4r+1)\theta + \sum_{i=0}^{3} \alpha_i G_i.$$

Now by counting the number of terms of the two sides of the above equation we have:

$$(2r+1)^2(4r+1)^2 = (2r+1)(4r+1) + 2(2r+1)(4r+1)\sum_{i=0}^{3} \alpha_i,$$

so

$$\sum_{i=0}^{3} \alpha_i = \frac{1}{2}[(2r+1)(4r+1) - 1].$$

Thus we have:

$$2(\sum_{i=0}^{3} g^i)\Delta F_0 = 8(2r+1)(4r+1)\theta + ((2r+1)(4r+1) - 1)T^*.$$

To prove (iii), using the same argument one can say that:

$$\Delta(F_0, F_3) = \sum_{i=0}^{3} \alpha_i G_i.$$

Counting the number of terms of the two sides of the above equation we have:

$$2(2r+1)^2(4r+1)^2 = 2(2r+1)(4r+1)\sum_{i=0}^{3} \alpha_i.$$

Thus

$$\sum_{i=0}^{3} \alpha_i = (2r+1)(4r+1).$$

Now we have:

$$(\sum_{i=0}^{3} g^i)\Delta(F_0, F_3) = (2r+1)(4r+1)T^*.$$

To prove (iv) we have:

$$\begin{aligned}
\Delta(F_0, F_2 \cup F_6) &= \sum_{i=0}^{2r}\sum_{j=0}^{2r} \Delta(E_{8i}, E_{8j+2} \cup E_{8(j+r)+6}) \\
&= \sum_{i=0}^{2r}\sum_{j=0}^{2r} g^{8i}(\Phi_{8(j-i)+2} + \Phi_{8(j-i)+8r+6}) \\
&= \sum_{i=0}^{2r} g^{8i} \sum_{j=0}^{2r} (T^* - T_0 - T_{8(j-i)+2}) \\
&= (2r+1)^2 T^* - (2r+1)\sum_{i=0}^{2r}(T_{8i} + T_{8i+2}) \\
&= (2r+1)^2 T^* - (2r+1)(G_0 + G_2).
\end{aligned}$$

□

Theorem 2.17 *There is an SDS $\{D_1, D_2, D_3, D_4\}$ of type H in $GF(q)$ such that every element of $GF(q)$ appears an even number of times in the system of $\{D_1, D_2, D_3, D_4\}$, where $q = 8r + 3$ is a prime power.*

Proof Let

$$D_1 = (\cup_{i=0}^{r-1} S_{8i+1}) \cup F_0 \cup F_3 \cup F_6,$$

$$D_2 = (\cup_{i=0}^{r-1} S_{8i}) \cup (\cup_{i=r}^{2r} S_{8i+2}) \cup (\cup_{i=0}^{r-1} S_{8i+3}) \cup F_1,$$

$$D_3 = (\cup_{i=0}^{r-1} S_{8i+3}) \cup F_0 \cup F_2 \cup F_5,$$

$$D_4 = (\cup_{i=0}^{r-1} S_{8i}) \cup (\cup_{i=r}^{2r} S_{8i+1}) \cup (\cup_{i=0}^{r-1} S_{8i+2}) \cup F_3.$$

It is easy to see that each of the subsets D_1, D_2, D_3, and D_4 satisfies the conditions of Lemma 2.15, so we have:

$$\begin{aligned}
\Delta D_1 &= 2r(4r+1)\theta + (7r^2+2r)T^* - r(G_0+G_2+G_3) + \Delta(F_0 \cup F_3 \cup F_6), \\
\Delta D_2 &= 2(4r+1)(3r+1)\theta + [(4r+1)^2 - r^2]T^* - (3r+1)G_1 + \Delta F_1, \\
\Delta D_3 &= 2r(4r+1)\theta + (7r^2+2r)T^* - r(G_0+G_1+G_2) + \Delta(F_0 \cup F_2 \cup F_5), \\
\Delta D_4 &= 2(4r+1)(3r+1)\theta + [(4r+1)^2 - r^2]T^* - (3r+1)G_3 + \Delta F_3.
\end{aligned}$$

Following the proof of Lemma 2.16 part (iii) one can easily show that $\Delta F_1 = \Delta F_5$ and $\Delta F_2 = \Delta F_6$. Now we have

$$\begin{aligned}
\sum_{i=1}^{4} \Delta D_i &= 4(4r+1)^2\theta + 2(22r^2+10r+1)T^* - 2r(G_0+G_1+G_2+G_3) \\
&\quad -(2r+1)(G_1+G_3) + 2\Delta F_0 + 2\Delta F_3 + \Delta F_1 + \Delta F_2 + \Delta F_5 + \Delta F_6 \\
&\quad +\Delta(F_0,F_3) + \Delta(F_0,F_5) + \Delta(F_2,F_5) + \Delta(F_3,F_6) + \Delta(F_0,F_2) + \Delta(F_0,F_6) \\
&= 4(4r+1)^2\theta + 2(22r^2+9r+1)T^* - (2r+1)(G_1+G_3) \\
&\quad +2(\Delta F_0 + \Delta F_1 + \Delta F_2 + \Delta F_3) + \Delta(F_0,F_3) + \Delta(F_1,F_4) + \Delta(F_2,F_5) \\
&\quad +\Delta(F_3,F_6) + \Delta(F_0, F_2 \cup F_6) \\
&= 4(4r+1)^2\theta + 2(22r^2+9r+1)T^* - (2r+1)(G_1+G_3) \\
&\quad +2(\sum_{i=0}^{3} g^i)\Delta F_0 + (\sum_{i=0}^{3} g^i)\Delta(F_0,F_3) + \Delta(F_2,F_5) \\
&= 4(8r+3)(4r+1)\theta + (64r^2+32r+3)T^* \\
&= q^2\theta + q(q-2)T.
\end{aligned}$$

It is easy to check that every element of G appears an even number of times in the system of $\{D_1, D_2, D_3, D_4\}$ and the proof is complete. □

Next we want to show the relationship between SDSs and T–matrices. In order to make the connection we should introduce the concept of a C–partition of an abelian group. We construct T–matrices from C–partitions and C–partitions from supplementary difference sets of type H such that every element of the abelian group appears an even number of times in the system of our SDS.

Definition 2.18 *The family of subsets $(A_1, A_2, \ldots, A_8)$ of an abelian group G of order v is called a C-partition if it satisfies the following conditions:*

(i) $A_i \cap A_j = \emptyset$;

(ii) $\cup_{i=1}^{8} A_i = G$;

(iii) $\sum_{i=1}^{8} \Delta A_i = v\theta + \sum_{i=1}^{4} \Delta(A_i, A_{i+4})$.

Theorem 2.19 *There is a C-partition $(A_1, A_2, \ldots, A_8)$ of an abelian group G of order v if and only if there is an SDS $\{D_1, D_2, D_3, D_4\}$ of type H in G such that every element of G appears an even number of times in the system of $\{D_1, D_2, D_3, D_4\}$.*

Proof Let

$$\begin{aligned} D_1 &= A_1 \cup A_2 \cup A_3 \cup A_4, \\ D_2 &= A_1 \cup A_2 \cup A_7 \cup A_8, \\ D_3 &= A_1 \cup A_6 \cup A_3 \cup A_8, \\ D_4 &= A_1 \cup A_6 \cup A_7 \cup A_4. \end{aligned}$$

During this construction using 2.13, 2.14, and the fact that $G = \cup_{i=1}^{8} A_i$, it is not hard to show that:

$$\begin{aligned} \sum_{i=1}^{4} \Delta D_i &= \Delta(A_1, G) - \Delta(A_5, G) + \sum_{i=1}^{8} A_i - \sum_{i=1}^{4} \Delta(A_i, A_{i+4}) + \Delta G \\ &= v\theta + (2(|A_1| - |A_5|) + v)T \\ &= v\theta + (\sum_{i=1}^{4} |D_i| - v)T. \end{aligned} \tag{2.15}$$

Thus $\{D_1, D_2, D_3, D_4\}$ is an SDS of type H; it is clear that every element of G appears an even number of times in the system of $\{D_1, D_2, D_3, D_4\}$.

Conversely, let $\{D_1, D_2, D_3, D_4\}$ be an SDS of type H in G such that every element of G appears an even number of times in the system of $\{D_1, D_2, D_3, D_4\}$. Let

$$A_1 = D_1 \cap D_2 \cap D_3 \cap D_4, \;\; A_5 = \bar{D}_1 \cap \bar{D}_2 \cap \bar{D}_3 \cap \bar{D}_4,$$

$$A_2 = (D_1 \cap D_2) \setminus A_1,\ A_6 = (D_3 \cap D_4) \setminus A_1,$$
$$A_3 = (D_1 \cap D_3) \setminus A_1,\ A_7 = (D_2 \cap D_4) \setminus A_1,$$
$$A_4 = (D_1 \cap D_4) \setminus A_1,\ A_6 = (D_2 \cap D_3) \setminus A_1.$$

Let λ_x be the number of times that the element $x \in G$ appears in the system of $\{D_1, D_2, D_3, D_4\}$. We know that λ_x is either 0, 2 or 4; we have the following cases:

- If $\lambda_x = 0$ then $x \in A_5$ and $x \notin A_i$ for all $1 \leq i \leq 8$, $i \neq 5$.
- If $\lambda_x = 4$ then $x \in A_1$ and $x \notin A_i$ for all $1 \leq i \leq 8$, $i \neq 1$.
- If $\lambda_x = 2$ without loss of generality consider that $x \in D_1$ and $x \in D_2$. Since $\lambda_x = 2$ we know that $x \notin D_3$ and $x \notin D_4$ thus $x \in A_2$ and $x \notin A_i$ for all $1 \leq i \leq 8$, $i \neq 2$.

So for any element x of G we can say that x is exactly in one of the subsets A_i, $i = 1, \ldots, 8$. So we have

$$A_i \cap A_j = \emptyset, \text{ for } i \neq j,\ 1 \leq i, j \leq 8,$$
$$\cup_{i=1}^{8} A_i = G.$$

Thus the subsets $(A_1 \ldots A_8)$ satisfy the first two conditions of Definition 2.18. Now we show that they satisfy the last condition too. It is clear that:

$$\begin{aligned} D_1 &= A_1 \cup A_2 \cup A_3 \cup A_4, \\ D_2 &= A_1 \cup A_2 \cup A_7 \cup A_8, \\ D_3 &= A_1 \cup A_6 \cup A_3 \cup A_8, \\ D_4 &= A_1 \cup A_6 \cup A_7 \cup A_4. \end{aligned}$$

From 2.15 we have

$$\begin{aligned}
v\theta + \big(\sum_{i=1}^{4} |D_i| - v\big)T &= \sum_{i=1}^{4} \Delta D_i \\
&= \Delta(A_1, G) - \Delta(A_5, G) + \sum_{i=1}^{8} A_i - \sum_{i=1}^{4} \Delta(A_i, A_{i+4}) + \Delta G \\
&= \big(2(|A_1| - |A_5|) + v\big)T + \sum_{i=1}^{8} A_i - \sum_{i=1}^{4} \Delta(A_i, A_{i+4}) \\
&= \big(\sum_{i=1}^{4} |D_i| - v\big)T + \sum_{i=1}^{8} A_i - \sum_{i=1}^{4} \Delta(A_i, A_{i+4})
\end{aligned}$$

So we have:

$$\sum_{i=1}^{8} \Delta A_i = v\theta + \sum_{i=1}^{4} \Delta(A_i, A_{i+4}).$$

Thus $(A_1, \ldots, A_8)$ satisfies the condition (iii) of 2.18 and the proof is complete. □

Theorem 2.20 *If there is a C–partition $(A_1, \ldots, A_8)$ of an abelian group G of order v then there are T–matrices of order v.*

Proof Let

$$T_i = [t_{jk}^{(i)}], \ i = 1, 2, 3, 4, \ 1 \leq j, k \leq v,$$

where

$$t_{jk}^{(i)} = \begin{cases} 1, & \text{if } \ g_k \ominus g_j \in A_i, \\ -1, & \text{if } \ g_k \ominus g_j \in A_{i+4}, \\ 0, & \quad\ \text{otherwise.} \end{cases}$$

It is not hard to see that:

- The matrices T_i are type one matrices;
- $T_i \cap T_j = 0$;
- $\sum_i |T_i| = J$.

To complete the proof we have to show that $\sum_{i=1}^{4} T_iT_i^t = vI$. It is sufficient to show that $[\sum_{i=1}^{4} T_iT_i^t]_{jj'} = 0$ for $1 \leq j, j' \leq v$, $j \neq j'$. We count the number of times that $t_{jk}^{(i)}t_{j'k}^{(i)} = 1$ and $t_{jk}^{(i)}t_{j'k}^{(i)} = -1$ for fixed j and j' such that $j \neq j'$, $i = 1, 2, 3, 4$, and $k = 1, \ldots, v$. If $t_{jk}^{(i)} = 1$ and $t_{j'k}^{(i)} = 1$ we have $g_k \ominus g_j \in A_i$ and $g_k \ominus g_{j'} \in A_i$. Since $(g_k \ominus g_j) \ominus (g_k \ominus g_{j'}) = g_{j'} \ominus g_j$ we see that the number of times that $t_{jk}^{(i)} = 1$ and $t_{j'k}^{(i)} = 1$ is equal to the coefficient of $g_{j'} \ominus g_j$ in ΔA_i for a fixed i. Similarly we can show that the number of times that $t_{jk}^{(i)} = -1$ and $t_{j'k}^{(i)} = -1$ is equal to the coefficient of $g_{j'} \ominus g_j$ in ΔA_{i+4} for a fixed i. Thus the number of times that $t_{jk}^{(i)}t_{j'k}^{(i)} = 1$ for $i = 1, 2, 3, 4$ is equal to the coefficient of $g_{j'} \ominus g_j$ in $\sum_{i=1}^{8} \Delta A_i$. By the same argument one can say that the number of times that $t_{jk}^{(i)}t_{j'k}^{(i)} = -1$ for $i = 1, 2, 3, 4$ is equal to the coefficient of $g_{j'} \ominus g_j$ in $\sum_{i=1}^{4} \Delta(A_i, A_{i+4})$. So using

$$\sum_{i=1}^{8} \Delta A_i - \sum_{i=1}^{4} \Delta(A_i, A_{i+4}) = v\theta$$

we have

$$\sum_{i=1}^{4} T_iT_i^t = vI.$$

□

Theorem 2.21 *If $q = 8m + 3$ is a prime power then there are T–matrices of order $v = q^2$.*

Proof By Theorems 2.17, 2.19, and 2.20 we can produce T–matrices of order q^2 where $q = 8m + 3$ is a prime power. □

Chapter 3

Productive Regular Hadamard Matrices and Symmetric Designs

3.1 Introduction

One of the most outstanding results in the production of many new symmetric designs belongs to Yury Ionin.

The use of a special regular Hadamard matrix of order 36 in a class of balanced generalised weighing matrices was initiated by Ionin in [5] and this was the beginning of a number of very successful papers like [5], [4], [7], and [6] in which many new classes of symmetric designs were introduced. The hardest part of Ionin's construction was the introduction of a group of symmetry related to each single design. Hadi Kharaghani in [10] reintroduced the class of Bush–type Hadamard matrices and demonstrated that the group of symmetry for these matrices was trivial. Furthermore, it was through these works that he was led to *twin designs* [10] and *Siamese twin designs* [9]. In a recent work Yury Ionin introduced the class of productive regular Hadamard matrices. His method is now applied straight to Hadamard matrices. In this chapter we will introduce Bush–type Hadamard matrices and productive regular Hadamard matrices and show that Bush–type Hadamard matrices are productive. The methods used here borrow from both Ionin and Kharaghani.

We first need to introduce balanced generalised weighing matrices. We begin with a definition.

Definition 3.1 *Let G be a multiplicatively written group. A balanced generalised weighing matrix $BGW(v, k, \lambda)$ is a matrix $W = [w_{ij}]$ of order v with $w_{ij} \in G \cup \{0\}$ such that each row and each column of W contains exactly k non-zero entries and for any $h \neq i$, the multiset $\{w_{hj}w_{ij}^{-1} : 1 \leq j \leq v, w_{hj} \neq 0, w_{ij} \neq 0\}$ contains exactly $\lambda/|G|$ copies of every element of G.*

Here we explain Gerald Berman's method [2] to show that a specific class of balanced generalised weighing matrices exists.

Definition 3.2 *Let m be a positive integer and q be a prime power. The affine geometry of dimension m over the field $F_q = GF(q)$, denoted $AG(m, q)$ is the vector space $(F_q)^m$. The points of $AG(m, q)$ are m-tuples $x = (x_1, \dots, x_m)$, $x_i \in F_q$ and hyper-planes of $AG(m, q)$ are the set of points that satisfy*

$$u_1x_1 + \cdots + u_mx_m = u, \qquad u, u_i \in F_q.$$

Theorem 3.3 (Berman 1978) *If q is a prime power and G is a cyclic group such that the order of G divides $q - 1$ then there is a*

$$BGW((q^m - 1)/(q - 1), q^{m-1}, q^{m-1} - q^{m-2})$$

over G, for every positive integer m.

Proof Let $E = AG(m, q)$ and let P be the set of points of E on removing a point p. We have $|P| = q^m - 1$ and let H be the set of those hyper-planes of E that do not include the point p. Without loss of generality let $p = (0, 0, \dots, 0)$, then every hyper-plane of $u \in H$ can be expressed by the linear equation $u_1x_1 + \cdots + u_mx_m = 1$ where the coefficients u_i, $i = 1, \dots, m$ are not all zero. Thus every hyper-plane $u \in H$ can be expressed by an m-tuple $u = (u_1, \dots, u_m)$, $u_i \in \mathrm{GF}(q)$, $i = 1, \dots, m$. Using this notation it is clear that $|H| = q^m - 1$. A point $x \in P$ is on a hyper-plane $u \in H$ if and only if $x \cdot u = 1$. In order to count the number of points on a hyper-plane $u = (u_1, \dots, u_m)$, if one fixes the first $m - 1$ coordinates of $x = (x_1, \dots, x_m)$ then one can find x_m such that $x \cdot u = 1$ and it follows that every hyper-plane has q^{m-1} points and every point is on q^{m-1} hyper-planes. Let λ be an element of $\mathrm{GF}(q)$ of order $q - 1$, define the map $\phi_\lambda : P \rightarrow P$ such that

$$\phi_\lambda x = \lambda x = (\lambda x_1, \dots, \lambda x_m).$$

Let x be a point on a hyper-plane u. Since $(\lambda x) \cdot (\lambda^{-1} u) = 1$, ϕ_λ maps the hyper-plane u onto $\lambda^{-1} u$ and we have $\phi_\lambda u = \lambda^{-1} u$. It is clear that the order of ϕ_λ is $q - 1$. As every point $x \in P$ or every hyper-plane $u \in H$ has at least one non-zero coordinate the map ϕ_λ has no fixed point or fixed hyper-plane. Let

$$[x] = \{\phi_\lambda^k x : k = 0, \ldots, q-1\}, \quad x \in P,$$

$$[u] = \{\phi_\lambda^k u : k = 0, \ldots, q-1\}, \quad u \in H.$$

It is clear that $y \in [x]$ if and only if $x \in [y]$ so one can choose the points $x^1, x^2, \ldots, x^n \in P$, $n = (q^m - 1)/(q - 1)$ such that $[x^1] \cup [x^2] \cup \ldots \cup [x^n]$ is a partition of P and hyper-planes $u^1, u^2, \ldots, u^n \in H$ such that $[u^1] \cup [u^2] \cup \ldots \cup [u^n]$ is a partition of H. Since the hyper-planes $\phi_\lambda^k u^i$ are parallel, the point x^j lies on at most one of them. If x^j is a point of $\phi_\lambda^l u^i$ then $\phi_\lambda^k x^j$ is a point of $\phi_\lambda^{l+k} u^i$ so we can write $[x^j] \in [u^i]$ if the points of $[x^j]$ lie on the hyper-planes of $[u^i]$. If $[x^j] \in [u^i]$ then there is a unique integer $h = \nu(u^i, x^j)$ such that $\phi_\lambda^h x^j \in u^i$. Let G be a multiplicatively written cyclic group of order d such that $d | q - 1$ and let ω be a generator of G. Let $A = A(\phi_\lambda, x^1, \ldots, x^n, u^1, \ldots, u^n, \omega)$ denote the $n \times n$ matrix a_{ij} defined by

$$a_{ij} = \begin{cases} \omega^{\nu(u^i, x^j)} & \text{if } [x^j] \in [u^i] \\ 0 & \text{otherwise.} \end{cases} \tag{3.1}$$

for $i = 1, \ldots, n$.

To complete the proof we show that A is a $BGW((q^m - 1)/(q - 1), q^{m-1}, q^{m-1} - q^{m-2})$ over G. Since every hyper-plane has q^{m-1} points every row of A has exactly q^{m-1} non-zero entries. Since $(q^m - 1)/(q - 1) - q^{m-1} < q^{m-1}$ any two different rows of A have at least one point in common and for $i \neq k$, u^i and u^k are not parallel. Consider two hyper-planes $u^i = (u_1^i, \ldots, u_m^i)$ and $u^k = (u_1^k, \ldots, u_m^k)$ that are not parallel. There are integers $1 \leq e < f \leq m$ such that $u_e^i / u_e^k \neq u_f^i / u_f^k$. If the point $x = (x_1, \ldots, x_m)$ is on both hyper-planes u^i and u^k then by fixing the coordinates x_t, $t \neq e, f$ one can find the proper x_e and x_f that satisfy the equations $x \cdot u^i = 1$ and $x \cdot u^k = 1$. So if u^i and u^k are not parallel they have q^{m-2} points in common. Thus u^i intersects each of the hyper-planes $\phi_\lambda^h u^k$, $h = 0, \ldots, q-1$ in q^{m-2} points and the multiset $\{a_{ij} a_{kj}^{-1} : 1 \leq j \leq n, a_{ij} \neq 0, a_{kj} \neq 0\}$ contains exactly $(q - 1) q^{m-2} = q^{m-1} - q^{m-2}$ non-zero elements.

For any point $\phi_\lambda^l x^j$ on u^i and $\phi_\lambda^h u^k$ we have

$$u^i(\phi_\lambda^l x^j) = 1, \quad (\phi_\lambda^h u^k)(\phi_\lambda^l x^j) = u^k(\varphi_\lambda^{l-h} x^j) = 1$$

so $\nu(u^i, x^j) = l$, $\nu(u^k, x^j) = l - h$ and $a_{ij}a_{kj}^{-1} = \omega^h$ for $h = 0, \ldots, q-1$ so the multiset $\{a_{ij}a_{kj}^{-1} : 1 \leq j \leq n, a_{ij} \neq 0, a_{kj} \neq 0\}$ contains exactly q^{m-2} times of each element ω^h and this completes the proof. □

Definition 3.4 *A regular Hadamard matrix H with row sum $2h$ is productive if there is a set $\mathcal{H}$ of matrices with row sum $2h$ and a cyclic group $G =< \delta >$ where $\delta : \mathcal{H} \to \mathcal{H}$ is a bijection, such that*

(i) *$H \in \mathcal{H}$;*

(ii) *For any $H_1, H_2 \in \mathcal{H}$, $(\delta H_1)(\delta H_2)^t = H_1 H_2^t$;*

(iii) *$|G| = 4|h|$;*

(iv) *$\sum_{\sigma \in G} \sigma H = 2\frac{h}{|h|} J$.*

Lemma 3.5 *If H is productive then $-H$ is also productive.*

Proof The proof is straightforward. □

Theorem 3.6 (Ionin) *If there is a productive regular Hadamard matrix H with row sum $2h$ and $q = (2h-1)^2$ is a prime power then for any positive integer m there is a symmetric design with parameters:*

$$\left(\frac{4h^2(q^{m+1} - 1)}{q - 1}, (2h^2 - h)q^m, (h^2 - h)q^m \right).$$

Proof Let $W = [w_{ij}]$ be a $BGW((q^{m+1} - 1)/(q - 1), q^m, q^m - q^{m-1})$ over G and let

$$M = \frac{1}{2}(J - H).$$

We know that M is the incidence matrix of a symmetric $(4h^2, 2h^2 - h, h^2 - h)$–design. If $H_1 \in \mathcal{H}$, $M_1 = \frac{1}{2}(J - H_1)$, and $\delta \in G$ we define:

$$\delta M_1 = \frac{1}{2}(J - \delta H_1).$$

If $H_1, H_2 \in \mathcal{H}$, $M_1 = \frac{1}{2}(J - H_1)$, and $M_2 = \frac{1}{2}(J - H_2)$ we have:

$$\begin{aligned}
(\delta M_1)(\delta M_2)^t &= \frac{1}{4}(J - \delta H_1)(J - \delta H_2)^t \\
&= \frac{1}{4}(J^2 - (\delta H_1)J - J(\delta H_2)^t + (\delta H_1)(\delta H_2)^t) \\
&= \frac{1}{4}(J^2 - H_1 J - J H_2^t + H_1 H_2^t) \\
&= M_1 M_2^t.
\end{aligned}$$

It can also easily be seen that $\sum_{\delta \in G} \delta M = (2|h| - \frac{h}{|h|})J$. We prove that $W \otimes M$ is the incidence matrix of a symmetric $(4h^2(q^{m+1} - 1)/(q - 1), (2h^2 - h)q^m, (h^2 - h)q^m)$-design. It suffices to show that for $i, j = 1, 2, \ldots, (q^{m+1} - 1)/(q - 1)$,

$$\sum_{k=1}^{(q^{m+1}-1)/(q-1)} (w_{ik}M)(w_{jk}M)^t = \begin{cases} h^2 q^m I + (h^2 - h)q^m J & \text{if i = j,} \\ (h^2 - h)q^m J & \text{otherwise.} \end{cases}$$

If $i = j$ then for some $\delta_k \in G$ we have:

$$\begin{aligned}
\sum_{k=1}^{(q^{m+1}-1)/(q-1)} (w_{ik}M)(w_{jk}M)^t &= \sum_{k=1}^{q^m} (\delta_k M)(\delta_k M)^t \\
&= \sum_{k=1}^{q^m} M M^t \\
&= q^m M M^t \\
&= h^2 q^m I + (h^2 - h)q^m J.
\end{aligned}$$

If $i \neq j$ then for some $\delta_k, \tau_k \in G$,

$$\begin{aligned}
\sum_{k=1}^{(q^{m+1}-1)/(q-1)} (w_{ik}M)(w_{jk}M)^t &= \sum_{k=1}^{q^m-q^{m-1}} (\delta_k M)(\tau_k M)^t \\
&= \sum_{k=1}^{q^m-q^{m-1}} (\tau_k^{-1}\delta_k M)M^t \\
&= \frac{q^m - q^{m-1}}{4|h|}(\sum_{\sigma \in G} \sigma M)M^t \\
&= \frac{q^m - q^{m-1}}{4|h|}(2|h| - \frac{h}{|h|})JM^t \\
&= \frac{q^m - q^{m-1}}{4|h|}(2|h| - \frac{h}{|h|})(2h^2 - h)J \\
&= \frac{1}{4}(q^m - q^{m-1})qJ = q^m(h^2 - h)J.
\end{aligned}$$

□

3.2 Bush–type Hadamard matrices

Definition 3.7 *A regular Hadamard matrix $H = [H_{ij}]$ of order $4n^2$ where H_{ij} are blocks of order $2n$ is Bush–type if $H_{ii} = J_{2n}$ and $H_{ij}J_{2n} = J_{2n}H_{ij} = 0$, for $i \neq j$, $1 \leq i, j \leq 2n$.*

We will now show that there are many Bush-type Hadamard matrices and each Bush–type Hadamard matrix is a productive regular Hadamard matrix.

Theorem 3.8 (Kharaghani 1985 [8]) *If there is a Hadamard matrix of order $4n$ then there is a Bush–type Hadamard matrix of order $16n^2$.*

Proof Let K be a normalised Hadamard matrix of order $4n$ and let $r_1, r_2, \ldots, r_{4n}$ be the rows of K. Let $C_i = r_i^t r_i$, $i = 1, \ldots, 4n$. It is easy to see that:

(i) $C_i = C_i^t$ for $i = 1, 2, \ldots, 4n$;

(ii) $C_1 = J_{4n}$, $C_i J_{4n} = J_{4n} C_i = 0$, for $i = 1, \ldots, 4n$;

(iii) $C_iC_j^t = 0$ if $i \neq j$;

(iv) $\sum_{i=1}^{4n} C_iC_i^t = 16n^2 I_{4n}$.

Following Seberry, Yamada [14], we call the matrices C_i above as Kharaghani matrices. Let $H = circ(C_1, C_2, \ldots, C_{4n})$ then H is a Bush–type Hadamard matrix of order $16n^2$. □

Example 3. Let

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

Then,

$$\begin{aligned} r_1 &= [\ 1\ \ 1\ \ 1\ \ 1\ ] \\ r_2 &= [\ 1\ \ 1\ \ -\ \ -\ ] \\ r_3 &= [\ 1\ \ -\ \ 1\ \ -\ ] \\ r_4 &= [\ 1\ \ -\ \ -\ \ 1\ ] \end{aligned}$$

$$C_1 = r_1^t r_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$C_2 = r_2^t r_2 = \begin{bmatrix} 1 & 1 & - & - \\ 1 & 1 & - & - \\ - & - & 1 & 1 \\ - & - & 1 & 1 \end{bmatrix}$$

$$C_3 = r_3^t r_3 = \begin{bmatrix} 1 & - & 1 & - \\ - & 1 & - & 1 \\ 1 & - & 1 & - \\ - & 1 & - & 1 \end{bmatrix}$$

$$C_4 = r_4^t r_4 = \begin{bmatrix} 1 & - & - & 1 \\ - & 1 & 1 & - \\ - & 1 & 1 & - \\ 1 & - & - & 1 \end{bmatrix}$$

$$B = \left[\begin{array}{cccc@{\quad}cccc@{\quad}cccc@{\quad}cccc}
1 & 1 & 1 & 1 & 1 & 1 & - & - & 1 & - & 1 & - & 1 & - & - & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & - & - & - & 1 & - & 1 & - & 1 & 1 & - \\
1 & 1 & 1 & 1 & - & - & 1 & 1 & 1 & - & 1 & - & - & 1 & 1 & - \\
1 & 1 & 1 & 1 & - & - & 1 & 1 & - & 1 & - & 1 & 1 & - & - & 1 \\[1ex]
1 & - & - & 1 & 1 & 1 & 1 & 1 & 1 & 1 & - & - & 1 & - & 1 & - \\
- & 1 & 1 & - & 1 & 1 & 1 & 1 & 1 & 1 & - & - & - & 1 & - & 1 \\
- & 1 & 1 & - & 1 & 1 & 1 & 1 & - & - & 1 & 1 & 1 & - & 1 & - \\
1 & - & - & 1 & 1 & 1 & 1 & 1 & - & - & 1 & 1 & - & 1 & - & 1 \\[1ex]
1 & - & 1 & - & 1 & - & - & 1 & 1 & 1 & 1 & 1 & 1 & 1 & - & - \\
- & 1 & - & 1 & - & 1 & 1 & - & 1 & 1 & 1 & 1 & 1 & 1 & - & - \\
1 & - & 1 & - & - & 1 & 1 & - & 1 & 1 & 1 & 1 & - & - & 1 & 1 \\
- & 1 & - & 1 & 1 & - & - & 1 & 1 & 1 & 1 & 1 & - & - & 1 & 1 \\[1ex]
1 & 1 & - & - & 1 & - & 1 & - & 1 & - & - & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & - & - & - & 1 & - & 1 & - & 1 & 1 & - & 1 & 1 & 1 & 1 \\
- & - & 1 & 1 & 1 & - & 1 & - & - & 1 & 1 & - & 1 & 1 & 1 & 1 \\
- & - & 1 & 1 & - & 1 & - & 1 & 1 & - & - & 1 & 1 & 1 & 1 & 1
\end{array}\right]$$

□

Theorem 3.9 *Bush–type Hadamard matrices are productive.*

Proof Let $H = [H_{ij}]$, $1 \leq i, j \leq 2n$ be a Bush–type Hadamard matrix of order $4n^2$ with block size $2n$, and let $\mathcal{H}$ be a family of block matrices $X = [X_{ij}]$, $1 \leq i, j \leq 2n$ of order $4n^2$, satisfying the following conditions:

(i) for each i there is exactly one block X_{ij_0} such that $X_{ij_0} = J_{2n}$;

(ii) if $j \neq j_0$ then $X_{ij}J = JX_{ij} = 0$.

It is clear that $H \in \mathcal{H}$. We define a bijection $\sigma : \mathcal{H} \longrightarrow \mathcal{H}$ by $\sigma X = X'$ such that:

(i) for $1 \leq i \leq 2n$ and $2 \leq j \leq 2n$, $X'_{ij} = X_{i,j-1}$;

(ii) for $1 \leq i \leq 2n$ if $X_{i,2n} = J$, then $X'_{i1} = J$;

(iii) for $1 \leq i \leq 2n$ if $X_{i,2n}J = JX_{i,2n} = 0$, then $X'_{i1} = -X_{i,2n}$.

Let $G =< \sigma >$ then it is clear that $|G| = 4n$.
Let $P, Q \in \mathcal{H}$ and let $P' = \sigma P$ and $Q' = \sigma Q$, to show that $(\sigma P)(\sigma Q)^t = PQ^t$ it is enough to show that

$$P_{i,2n}Q^t_{j,2n} = P'_{i1}Q'^t_{j1}.$$

There are four cases:

1. If $P_{i,2n} = J$ and $Q_{j,2n} = J$ then $P'_{i1} = J$ and $Q'_{j1} = J$ so $P_{i,2n}Q^t_{j,2n} = P'_{i1}Q'^t_{j1} = J^2$.

2. If $P_{i,2n}J = JP_{i,2n} = 0$ and $Q_{j,2n} = J$ then $P'_{i1} = -P_{i,2n}$ and $Q'_{j1} = J$ so $P_{i,2n}Q^t_{j,2n} = P_{i,2n}J = 0$ and $P'_{i1}Q'^t_{j1} = -P_{i,2n}J = 0$.

3. If $P_{i,2n} = J$ and $Q_{j,2n}J = JQ_{i,2n} = 0$ then $P'_{i1} = P_{i,2n} = J$ and $Q'_{j1} = -Q_{j,2n}$ so $P_{i,2n}Q^t_{j,2n} = JQ^t_{j,2n} = 0$ and $P'_{i1}Q'^t_{j1} = -JQ^t_{j,2n} = 0$.

4. If $P_{i,2n}J = JP_{i,2n} = 0$ and $Q_{j,2n}J = JQ_{j,2n} = 0$ then $P'_{i1} = -P_{i,2n}$ and $Q'_{j1} = -Q_{j,2n}$ so $P'_{i1}Q'^t_{j1} = (-P_{i,2n})(-Q_{j,2n})^t = P_{i,2n}Q^t_{j,2n}$.

Since also $\sum_{\delta \in G} \delta H = 2J$, the proof is complete.

□

Corollary 3.10 *If there is a Bush–type Hadamard matrix of order* $4n^2$ *and* $q = (2n - 1)^2$ *is a prime power then for every positive integer* m *there is a symmetric design with parameters*

$$\left(\frac{4n^2(q^{m+1} - 1)}{q - 1}, q^m(2n^2 - n), q^m(n^2 - n)\right) \tag{3.2}$$

and if $q = (2n + 1)^2$ *is a prime power then for every positive integer* m *there is a symmetric design with parameters*

$$\left(\frac{4n^2(q^{m+1} - 1)}{q - 1}, q^m(2n^2 + n), q^m(n^2 + n)\right) \tag{3.3}$$

Proof Suppose that H is a Bush–type Hadamard matrix of order $4n^2$. For the case where $q = (2n - 1)^2$, since the matrix H has row sum $2n$, the proof follows from Theorems 3.6 and 3.9. For the case where $q = (2n + 1)^2$, since the matrix $-H$ has row sum $-2n$, the proof follows from Lemma 3.5, Theorem 3.6, and Theorem 3.9. □

Theorem 3.8 shows that the existence of a Hadamard matrix of order $4n$ implies the existence of a Bush–type Hadamard matrix of order $16n^2$. It has been conjectured that Bush–type Hadamard matrices of order $4n^2$ exist for all integers n. For odd values of n this conjecture seems to be difficult and only known for $n = 3, 5$, and 9.

3.3 The Kronecker product of Bush–type Hadamard matrices and productive regular Hadamard matrices

Ionin in a recent paper [4] showed that the Kronecker product of a Bush–type Hadamard matrix B and a productive regular Hadamard matrix H namely $M = B \otimes H$ is also a productive regular Hadamard matrix. In this section we introduce his method.

Let B be a Bush–type Hadamard matrix of order $4n^2$ and let H be a productive regular Hadamard matrix with row sum $2h$ and cyclic group $G =< \delta >$. Let

$$\mathcal{H} = \{\delta^i H | i = 0, 1, \ldots, 4|h| - 1\}.$$

By the definition we have:

- For any H_1 and H_2 in $\mathcal{H}$, $(\delta H_1)(\delta H_2)^t = H_1 H_2^t$;
- $\sum_{X \in \mathcal{H}} X = 2\frac{h}{|h|}J$.

Let $\mathcal{Z} = \{Z | ZJ = JZ = 0\}$, $\mathcal{R} = \{J \otimes K | K \in \mathcal{H}\}$, and $\mathcal{S} = \{Z \otimes H | Z \in \mathcal{Z}\}$, where J and Z are of order $2n$. We define the map $\rho : \mathcal{R} \cup \mathcal{S} \to \mathcal{R} \cup \mathcal{S}$ by

$$\begin{array}{rcll} \rho(Z \otimes H) & = & -Z \otimes H & \text{for each} \quad Z \in \mathcal{Z} \\ \rho(J \otimes K) & = & J \otimes (\delta K) & \text{for each} \quad K \in \mathcal{H}. \end{array}$$

It is easy to see that the cyclic group generated by ρ has order $4|h|$. For $R \in \mathcal{R}$ we have:

$$\begin{aligned}
\sum_{i=0}^{4|H|} \rho^i R &= \sum_{i=0}^{4|h|} \rho^i J \otimes \delta^j H \\
&= \sum_{i=0}^{4|h|} J \otimes (\delta^{i+j} H) \\
&= \sum_{i=0}^{4|h|} J \otimes (\delta^i H) \\
&= J \otimes (\sum_{i=0}^{4|h|} \delta^i H) \\
&= J \otimes (2\frac{h}{|h|} J) \\
&= 2\frac{h}{|h|} J \otimes J.
\end{aligned}$$

For $S \in \mathcal{S}$ it is easy to see that

$$\sum_{i=0}^{4|h|} \rho^i S = 0.$$

Let $M = B \otimes H$. It is clear that the matrix M is a regular Hadamard matrix with row sum $4hn$. Let $\mathcal{M}$ be the set of block matrices $D = [D_{ij}]$, $i, j = 1, \ldots, 2n$, such that:

1. for each $i = 1, \ldots, 2n$, there is a unique $h_i = h_i(D) \in \{1, \ldots, 2n\}$, such that for $j = h_i$, $D_{ij} \in \mathcal{R}$;

2. for $i = 1, \ldots, 2n$, and for $j \neq h_i$, $D_{ij} \in \mathcal{S}$.

Clearly M is an element of $\mathcal{M}$. Define a bijection $\sigma : \mathcal{M} \to \mathcal{M}$ by $\sigma D = D' = [D'_{ij}]$ such that:

1. for $i = 1, \ldots, 2n$, and $j = 2, \ldots, 2n$, $D'_{ij} = D_{i,j-1}$;

2. for $i = 1, \ldots, 2n$, $D'_{i1} = \rho D_{i,2n}$.

It follows from the fact that $\rho^{4|h|} = 1$ and from the number of blocks of D that the order of the cyclic group G generated by σ is $8n|h|$.

Lemma 3.11 *For $X, Y \in \mathcal{M}$, $(\sigma X)(\sigma Y)^t = XY^t$.*

Proof Let $X, Y \in \mathcal{M}$ and let $X' = \sigma X$ and $Y' = \sigma Y$. It is sufficient to show that, for $i, i' = 1, \ldots, 2n$,

$$X'_{i1} Y'^t_{i'1} = X_{i,2n} Y^t_{i',2n}.$$

It is obvious that $X_{i,2n}$ and $Y_{i',2n}$ are either in $\mathcal{R}$ or in $\mathcal{S}$. We have to check the following cases:

- If $X_{i,2n} \in \mathcal{S}$ and $Y_{i',2n} \in \mathcal{S}$ then $X'_{i1} Y'^t_{i'1} = (-X_{i,2n})(-Y_{i',2n})^t = X_{i,2n} Y^t_{i',2n}$.
- If $X_{i,2n} \in \mathcal{R}$ and $Y_{i',2n} \in \mathcal{S}$ then for some $K \in \mathcal{H}$ and $Z \in \mathcal{Z}$ we have:

$$\begin{aligned} X_{i,2n} Y^t_{i',2n} &= (J \otimes K)(Z^t \otimes H^t) \\ &= (JZ^t) \otimes (KH^t) \\ &= 0, \end{aligned}$$

  and

$$\begin{aligned} X'_{i1} Y'^t_{i'1} &= (J \otimes (\delta K))(-Z^t \otimes H^t) \\ &= (-JZ^t) \otimes ((\delta K)H^t) \\ &= 0. \end{aligned}$$

- The proof for the case $X_{i,2n} \in \mathcal{S}$ and $Y_{i',2n} \in \mathcal{R}$ is similar and we omit it.
- If $X_{i,2n} \in \mathcal{R}$ and $Y_{i',2n} \in \mathcal{R}$ then for some K_1 and K_2 in $\mathcal{R}$ we have:

$$\begin{aligned} X'_{i1} Y'^t_{i'1} &= (J \otimes (\delta K_1))(J^t \otimes (\delta K_2)^t) \\ &= (JJ^t) \otimes ((\delta K_1)(\delta K_2)^t) \\ &= (JJ^t) \otimes (K_1 K_2^t) \\ &= X_{i,2n} Y^t_{i',2n}. \end{aligned}$$

□

Lemma 3.12 $\sum_{g=0}^{8n|h|-1} \sigma^g H = 2J$.

Proof For some $R \in \mathcal{R}$ and $S_k \in \mathcal{S}$, $1 \leq k \leq 2n-1$, we see that the (i,j)-block of the matrix $\sum_{g=0}^{8n|h|-1} \sigma^g M$ is:

$$\begin{aligned}
[\sum_{l=0}^{8n|h|-1} \sigma^l M]_{ij} &= \sum_{\alpha=0}^{4|h|-1} \rho^\alpha R + \sum_{k=1}^{2n-1} \sum_{\alpha=0}^{4|h|-1} \rho^\alpha S_k \\
&= 2\frac{h}{|h|} J + \sum_{k=1}^{2n-1} 0 \\
&= 2\frac{h}{|h|} J.
\end{aligned}$$

□

Theorem 3.13 *Let B be a Bush–type Hadamard matrix and H be a productive regular Hadamard matrix then the matrix $M = B \otimes H$ is productive.*

Proof Using Lemmas 3.11 and 3.12 we see that the matrix M, the set $\mathcal{M}$ and the bijection σ satisfy all of the conditions of definition 3.4. □

Chapter 4

A New Class of Productive Regular Hadamard Matrices

In this chapter we introduce a new class of productive regular Hadamard matrices. We show that for each integer n for which $4n$ is the order of a Hadamard matrix and $8n^2 - 1$ is a prime, there is a productive regular Hadamard matrix of order $16n^2(8n^2-1)^2$. As a corollary, by applying a recent result of Ionin, we get many new infinite classes of symmetric designs provided that either $4n(8n^2-1)-1$, or $4n(8n^2-1)+1$ (or both) are prime powers.

4.1 Introduction

We begin this section by introducing a fascinating class of matrices, originally generated by Mathon [12] and subsequently generalised by Seberry and Whiteman [13].

Definition 4.1 *A regular s–set of matrices of order m^2 is a set of matrices A_1, A_2, …, A_s such that:*

- $A_iA_j = J$, *for every* i, j;
- $A_iA_j^t = A_j^tA_i = J, \quad i \neq j$;
- $A_iJ = mJ$, *for every* i;

- $\sum_{i=1}^{s}(A_iA_i^t + A_i^tA_i) = 2sm^2I$.

It is shown in Seberry and Whiteman [13] that:

Theorem 4.2 (Seberry–Whiteman) *If $m \equiv 3 \pmod 4$ is a prime power, then there is a regular $\frac{1}{2}(m+1)$–set of order m^2.*

See Lemmas 4.5 and 4.6 for a proof of this theorem.

4.2 A regular class of Hadamard matrices

Let K be a normalised Hadamard matrix of order $4n$. Let $r_1, r_2, ..., r_{4n}$ be the row vectors of K. Let $C_i = r_i^t r_i$, $i = 1, ..., 4n$, be Kharaghani matrices. These matrices can be used in a Latin square to generate a Bush–type Hadamard matrix of order $16n^2$ (see Theorem 3.8 for details). For the matrices $C = [c_{ij}]$ and $D = [d_{ij}]$, we denote the matrix $[c_{ij}d_{ij}]$ by $C * D$, whenever the product $c_{ij}d_{ij}$ is defined.

We are now ready for the main result of this section.

Theorem 4.3 *Let n be an integer for which there is a Hadamard matrix of order $4n$ and $m = 8n^2 - 1$ be a prime power. Then there is a regular Hadamard matrix of order $16n^2m^2$.*

Proof Let A_i, $i = 1, 2, \cdots, 4n^2$, be a regular $4n^2$–set of matrices of order m^2 from Theorem 4.2. Let

$$L_i = \begin{cases} circ(A_{4(i-1)n+1}, \cdots, A_{4in}) & \text{if } 1 \le i \le n \\ circ(A^t_{4(i-n-1)n+1}, \cdots, A^t_{4(i-n)n}) & \text{if } n < i \le 2n. \end{cases}$$

Let C_is be Kharaghani matrices defined above. Let $K_i := C_i * L_i$ and $K_i' := C_{i+2n} * L_i$ for $1 \le i \le 2n$. Using the properties of the regular s–set of matrices, it is not hard to see that the matrices K_i and K_i' have the following properties for every i and j:

1. $K_iK_j^t = K_i'K_j'^t = 0$ if $i \ne j$
2. $K_iK_j'^t = K_j'K_i^t = 0$ if $i \ne j$
3. $K_iK_i'^t = K_i'K_i^t$

Let $M = circ(K_1, K_2, \ldots, K_{2n})$ and $M' = circ(K'_1, K'_2, \ldots, K'_{2n})$. Let

$$H = \begin{bmatrix} M & M' \\ -M' & M \end{bmatrix}$$

Let e be the column vector of all ones. The fact that $K_1 e = 4nm$ and $K_i e = 0$ for all i, $2 \le i \le 2n$, implies that $Me = 4nm$. On the other hand, $K'_i e = 0$ for all i, $1 \le i \le 2n$, so $M'e = 0$. This shows that H is a regular matrix of order $16n^2m^2$. It remains to show that H is a Hadamard matrix. Using properties 1 and 2 above, it is not hard to see that MM^t and $M'M'^t$ are both diagonal matrices. Furthermore, property 3 can be used to show that $MM'^t = M'M^t$. It is easy now to see that H is a Hadamard matrix. □

Example 4. For $n = 1$ we have:

$$L_1 = \begin{bmatrix} A_1 & A_2 & A_3 & A_4 \\ A_4 & A_1 & A_2 & A_3 \\ A_3 & A_4 & A_1 & A_2 \\ A_2 & A_3 & A_4 & A_1 \end{bmatrix}$$

$$L_2 = \begin{bmatrix} A_1^t & A_2^t & A_3^t & A_4^t \\ A_4^t & A_1^t & A_2^t & A_3^t \\ A_3^t & A_4^t & A_1^t & A_2^t \\ A_2^t & A_3^t & A_4^t & A_1^t \end{bmatrix}$$

$$C_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$C_2 = \begin{bmatrix} 1 & 1 & - & - \\ 1 & 1 & - & - \\ - & - & 1 & 1 \\ - & - & 1 & 1 \end{bmatrix}$$

$$C_3 = \begin{bmatrix} 1 & - & 1 & - \\ - & 1 & - & 1 \\ 1 & - & 1 & - \\ - & 1 & - & 1 \end{bmatrix}$$

$$C_4 = \begin{bmatrix} 1 & - & - & 1 \\ - & 1 & 1 & - \\ - & 1 & 1 & - \\ 1 & - & - & 1 \end{bmatrix}$$

After superimposing the signs of entries of C_1, C_2, C_3 and C_4 over on the blocks of the matrices L_1, L_2, L_1 and L_2 respectively we get the matrix H below:

$$K_1 = C_1 * L_1 = \begin{bmatrix} A_1 & A_2 & A_3 & A_4 \\ A_4 & A_1 & A_2 & A_3 \\ A_3 & A_4 & A_1 & A_2 \\ A_2 & A_3 & A_4 & A_1 \end{bmatrix}$$

$$K_2 = C_2 * L_2 = \begin{bmatrix} A_1^t & A_2^t & -A_3^t & -A_4^t \\ A_4^t & A_1^t & -A_2^t & -A_3^t \\ -A_3^t & -A_4^t & A_1^t & A_2^t \\ -A_2^t & -A_3^t & A_4^t & A_1^t \end{bmatrix}$$

$$K_1' = C_3 * L_1 = \begin{bmatrix} A_1 & -A_2 & A_3 & -A_4 \\ -A_4 & A_1 & -A_2 & A_3 \\ A_3 & -A_4 & A_1 & -A_2 \\ -A_2 & A_3 & -A_4 & A_1 \end{bmatrix}$$

$$K_2' = C_4 * L_2 = \begin{bmatrix} A_1^t & -A_2^t & -A_3^t & A_4^t \\ -A_4^t & A_1^t & A_2^t & -A_3^t \\ -A_3^t & A_4^t & A_1^t & -A_2^t \\ A_2^t & -A_3^t & -A_4^t & A_1^t \end{bmatrix}$$

$$H = \begin{bmatrix} K_1 & K_2 & K_1' & K_2' \\ K_2 & K_1 & K_2' & K_1' \\ -K_1' & -K_2' & K_1 & K_2 \\ -K_2' & -K_1' & K_2 & K_1 \end{bmatrix} =$$

$$\left[\begin{array}{cccccccccccccccc}
A_1 & A_2 & A_3 & A_4 & A_1^t & A_2^t & -A_3^t & -A_4^t & A_1 & -A_2 & A_3 & -A_4 & A_1^t & -A_2^t & -A_3^t & A_4^t \\
A_4 & A_1 & A_2 & A_3 & A_4^t & A_1^t & -A_2^t & -A_3^t & -A_4 & A_1 & -A_2 & A_3 & -A_4^t & A_1^t & A_2^t & -A_3^t \\
A_3 & A_4 & A_1 & A_2 & -A_3^t & -A_4^t & A_1^t & A_2^t & A_3 & -A_4 & A_1 & -A_2 & -A_3^t & A_4^t & A_1^t & -A_2^t \\
A_2 & A_3 & A_4 & A_1 & -A_2^t & -A_3^t & A_4^t & A_1^t & -A_2 & A_3 & -A_4 & A_1 & A_2^t & -A_3^t & -A_4^t & A_1^t \\
 & & & & & & & & & & & & & & & \\
A_1^t & A_2^t & -A_3^t & -A_4^t & A_1 & A_2 & A_3 & A_4 & A_1^t & -A_2^t & -A_3^t & A_4^t & A_1 & -A_2 & A_3 & -A_4 \\
A_4^t & A_1^t & -A_2^t & -A_3^t & A_4 & A_1 & A_2 & A_3 & -A_4^t & A_1^t & A_2^t & -A_3^t & -A_4 & A_1 & -A_2 & A_3 \\
-A_3^t & -A_4^t & A_1^t & A_2^t & A_3 & A_4 & A_1 & A_2 & -A_3^t & A_4^t & A_1^t & -A_2^t & A_3 & -A_4 & A_1 & -A_2 \\
-A_2^t & -A_3^t & A_4^t & A_1^t & A_2 & A_3 & A_4 & A_1 & A_2^t & -A_3^t & -A_4^t & A_1^t & -A_2 & A_3 & -A_4 & A_1 \\
 & & & & & & & & & & & & & & & \\
-A_1 & A_2 & -A_3 & A_4 & -A_1^t & A_2^t & A_3^t & -A_4^t & A_1 & A_2 & A_3 & A_4 & A_1^t & A_2^t & -A_3^t & -A_4^t \\
A_4 & -A_1 & A_2 & -A_3 & A_4^t & -A_1^t & -A_2^t & A_3^t & A_4 & A_1 & A_2 & A_3 & A_4^t & A_1^t & -A_2^t & -A_3^t \\
-A_3 & A_4 & -A_1 & A_2 & A_3^t & -A_4^t & -A_1^t & A_2^t & A_3 & A_4 & A_1 & A_2 & -A_3^t & -A_4^t & A_1^t & A_2^t \\
A_2 & -A_3 & A_4 & -A_1 & -A_2^t & A_3^t & A_4^t & -A_1^t & A_2 & A_3 & A_4 & A_1 & -A_2^t & -A_3^t & A_4^t & A_1^t \\
 & & & & & & & & & & & & & & & \\
-A_1^t & A_2^t & A_3^t & -A_4^t & -A_1 & A_2 & -A_3 & A_4 & A_1^t & A_2^t & -A_3^t & -A_4^t & A_1 & A_2 & A_3 & A_4 \\
A_4^t & -A_1^t & -A_2^t & A_3^t & A_4 & -A_1 & A_2 & -A_3 & A_4^t & A_1^t & -A_2^t & -A_3^t & A_4 & A_1 & A_2 & A_3 \\
A_3^t & -A_4^t & -A_1^t & A_2^t & -A_3 & A_4 & -A_1 & A_2 & -A_3^t & -A_4^t & A_1^t & A_2^t & A_3 & A_4 & A_1 & A_2 \\
-A_2^t & A_3^t & A_4^t & -A_1^t & A_2 & -A_3 & A_4 & -A_1 & -A_2^t & -A_3^t & A_4^t & A_1^t & A_2 & A_3 & A_4 & A_1
\end{array}\right]$$

□

4.3 A productive class of regular Hadamard matrices

In this section we show that most of the regular Hadamard matrices constructed in section 2 are productive. We also need to mention some of the properties of a class of regular $\frac{1}{2}(m+1)$–set of matrices as given in [13], whenever $m \equiv 3 (\mathrm{mod}\ 4)$ is a prime. Let T be the circulant shift matrix of order m defined by

$$T = [t_{ij}] \text{ where } t_{ij} = \begin{cases} 1 & \text{if } i - j \equiv 1 (\text{mod m}) \\ 0 & \text{otherwise.} \end{cases} \tag{4.1}$$

Let R be the back–circulant shift matrix of order m defined by

$$R = [r_{ij}] \text{ where } r_{ij} = \begin{cases} 1 & \text{if } i + j \equiv 1 (\text{mod m}) \\ 0 & \text{otherwise.} \end{cases} \tag{4.2}$$

Then the following properties are immediate.

$$T^m = I,\ (T^k)^t = T^{m-k},\ I + T + T^2 + \cdots + T^{m-1} = J,\ R^2 = I,$$
$$RT^k = R^t T^k = T^{m-k}R,\ JT^k = JR^k = J.$$

Let χ be the so–called quadratic character on the field $GF(m)$ defined by

$$\chi(x) := \begin{cases} 0 & \text{if } \ x = 0, \\ 1 & \text{if } \ x \text{ is a square,} \\ -1 & \text{if } \ x \text{ is a non–square.} \end{cases}$$

Let

$$W = [w_{ij}] \text{ where } w_{ij} = \chi(j-i), \text{ for } i,j = 0,\ldots,m-1.$$

By the definition it is clear that the matrix W is a circulant matrix. Since $m \equiv 3 (\mathrm{mod}\ 4)$ we have $\chi(-1) = -1$ and $\chi(-x) = -\chi(x)$, thus the matrix W is skew–symmetric ($W^t = -W$). The following properties are immediate:

$$WT = TW, \quad WR = R^tW^t = RW^t = -RW$$

Since the number of squares in $GF(m)$ is the same as the number of non–squares we have

$$WJ = 0.$$

Also for any $0 \neq y \in GF(m)$ we have:

$$\begin{aligned}\sum_{x\in GF(m)} \chi(x)\chi(x+y) &= \sum_{x\in GF(m)\backslash 0} \chi(x)\chi(x)\chi(1+yx^{-1}) \\ &= \sum_{x\in GF(m)\backslash 0} \chi(1+yx^{-1}) \\ &= 0 - \chi(1) \\ &= -1\end{aligned}$$

So it follows that $WW^t = mI - J$. Let

$$M := I + W$$

with top row $(b_0, b_1, \cdots, b_{m-1})$. Then we have :

$$MM^t = (m+1)I - J, \quad MJ = J. \qquad (4.3)$$

Let $e = e_m = (1, 1, \ldots, 1)$ be a vector of m 1's. Define the matrix

$$\begin{aligned} N &:= e^t(b_0, b_1, \cdots, b_{m-1}) \\ &= \begin{bmatrix} b_0 & b_1 & \cdots & b_{m-1} \\ b_0 & b_1 & \cdots & b_{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ b_0 & b_1 & \cdots & b_{m-1} \end{bmatrix}\end{aligned}$$

Using 4.3 since each of the rows of the matrix N is the same as the first row of M we have:

$$NT^kN^t = \begin{cases} mJ & \text{if} \quad k=0, \\ -J & \text{if} \quad 1 \leq k \leq m-1 \end{cases} \tag{4.4}$$

The following useful properties are also obvious:

$$NJ = J, \ JN = mN, \ MN = T^kN = R^kN = N.$$

We now define the matrices B_j and C which play a key role in what follows:

$$B_j := \sum_{i=0}^{m-1} RT^i \otimes MT^{ij} \quad (j = 1, ..., n-1) \tag{4.5}$$

$$C := N(I, T, T^2, ..., T^{m-1})^t e = \begin{bmatrix} N & N & \cdots & N \\ NT & NT & \cdots & NT \\ \vdots & \vdots & \ddots & \vdots \\ NT^{m-1} & NT^{m-1} & \cdots & NT^{m-1} \end{bmatrix} \tag{4.6}$$

We will show that matrices B_i and C are an $(m+1)/2$–set of matrices and that they also satisfy some additional properties that let us show that the matrix H, as defined in the previous section, is productive as well as regular. In order to show that the matrix H is productive we should define a map that satisfies the properties of a productive regular Hadamard matrix. For convenience we define mappings on smaller blocks of the matrix H step by step and then we introduce the final map using these maps.

Definition 4.4 *Let E be a $(1, -1)$ matrix of order m^2 and I the identity matrix of order m. Define the map δ as follows:*

$$\delta E := E(I \otimes T)$$

As a consequence of the properties above, for all non–negative integers α:

1. $\delta^\alpha B_j = \delta(\delta^{\alpha-1} B_j) = B_j(I \otimes T^\alpha) = \sum_{i=0}^{m-1} RT^i \otimes MT^{ij+\alpha}$.

2. $\delta^\alpha C = C(I \otimes T^\alpha) = NT^\alpha(I, T, T^2, ..., T^{m-1})^t e$.

Lemma 4.5 *Let $\mathcal{F} = \{C, B_1, \cdots, B_{(m-1)/2}\}$, and $\mathcal{G} = \{C, C^t, B_1, B_1^t, \cdots, B_{(m-1)/2}, B^t_{(m-1)/2}\}$. Then $\mathcal{F}$, $\mathcal{G}$ and δ satisfy the following conditions:*

(i) $\delta^m X = X$ *for all* X *in* $\mathcal{F}$;

(ii) $(\delta^\alpha X)(Y)^t = J$ *for all* $X \in \mathcal{F}$, $Y \in \mathcal{G}$, $X \neq Y$ *and* $\alpha \in \{0, 1, ..., m-1\}$;

(iii) $\sum_{i=0}^{m-1} \delta^i X = J$ *for all* $X \in \mathcal{F}$;

(iv) $(\delta X)(\delta Y)^t = XY^t$ *for every matrices* X, Y *of order* m^2.

Proof The proof of condition (i) follows from the fact that $T^m = I$.
To prove condition (ii) we have to consider the following sub–cases.
For all positive integers j, k not exceeding $(m-1)/2$:

(ii$_1$) $(\delta^\alpha B_j)(B_k^t)^t = J$;

(ii$_2$) $(\delta^\alpha B_j)(B_k)^t = J$ if $(j \neq k)$;

(ii$_3$) $(\delta^\alpha B_k)(C^t)^t = J$;

(ii$_4$) $(\delta^\alpha C)(B_k^t)^t = J$;

(ii$_5$) $(\delta^\alpha C)(B_k)^t = J$;

(ii$_6$) $(\delta^\alpha C)(C^t)^t = J$.

The proofs of these properties parallel proofs given in [13].

(ii$_1$)

$$\begin{aligned}
(\delta^\alpha B_j)(B_k) &= \sum_{i=0}^{m-1}\sum_{h=0}^{m-1} RT^iRT^h \otimes MT^{ij+\alpha}MT^{hk} \\
&= \sum_{h=0}^{m-1}\sum_{i=0}^{m-1} T^{m+h-i} \otimes M^2T^{ij+hk+\alpha} \\
&= \sum_{z=0}^{m-1}\sum_{i=0}^{m-1} T^z \otimes M^2T^{i(j+k)+zk+\alpha} \qquad (\text{ where } z = h-i) \\
&= \sum_{z=0}^{m-1} T^z \otimes M^2 J \\
&= J \otimes J.
\end{aligned}$$

Note that $j + k \neq m$ since $j, k \leq (m-1)/2$.

(ii_2)

$$\begin{aligned}
(\delta^\alpha B_j)(B_k)^t &= \sum_{i=0}^{n-1}\sum_{h=0}^{n-1} RT^i(RT^h)^t \otimes MT^{ij+\alpha}(MT^{hk})^t \\
&= \sum_{i=0}^{n-1}\sum_{h=0}^{n-1} T^{h-i} \otimes MM^tT^{ij-hk+\alpha} \\
&= \sum_{z=0}^{n-1}\sum_{h=0}^{n-1} T^{z} \otimes MM^tT^{i(j-k)-zk+\alpha} \qquad (\text{ where } z = h-i) \\
&= \sum_{z=0}^{n-1} T^z \otimes J \\
&= J \otimes J.
\end{aligned}$$

(ii_3)

$$\begin{aligned}
[(\delta^\alpha B_k)(C)]_{ij} &= \sum_{h=0}^{m-1} T^{(i+h)k}(MT^\alpha)NT^h \\
&= MN\sum_{h=0}^{m-1} T^h \\
&= MNJ = J.
\end{aligned}$$

(ii_4)

$$\begin{aligned}
[(\delta^\alpha C)(B_k)]_{ij} &= (NT^\alpha)T^iM\sum_{h=0}^{n-1} T^{(j+h)k} \\
&= NT^{i+\alpha}MJ \\
&= NT^{i+\alpha}J \\
&= NJ = J.
\end{aligned}$$

(ii$_5$)

$$\begin{aligned}
[(\delta^\alpha C)(B_k)^t]_{ij} &= \sum_{h=0}^{n-1}(\delta^\alpha C)_{ih}(B_k)^t_{hj} \\
&= \sum_{h=0}^{n-1}(NT^\alpha)T^i(T^{(h+j)k}M)^t \\
&= \sum_{h=0}^{n-1} NT^{\alpha+i}T^{n-(h+j)k}M^t \\
&= NM^t\sum_{h=0}^{n-1}T^{\alpha+i-(h+j)k} \\
&= NM^tJ \\
&= NJ = J.
\end{aligned}$$

(ii$_6$)

$$\begin{aligned}
[(\delta^\alpha C)(C)]_{ij} &= (NT^\alpha)T^iN\sum_{h=0}^{m-1}T^h \\
&= NT^{i+\alpha}NJ \\
&= NNJ = J.
\end{aligned}$$

To prove condition (iii) we have:

$$\begin{aligned}
\sum_{\alpha=0}^{m-1}\delta^\alpha B_i &= \sum_{\alpha=0}^{m-1}\sum_{i=0}^{m-1}RT^i\otimes MT^{ij+\alpha} \\
&= \sum_{i=0}^{m-1}RT^i\otimes(\sum_{\alpha=0}^{m-1}MT^{ij+\alpha}) \\
&= \sum_{i=0}^{m-1}RT^i\otimes(MJ) \\
&= J\otimes J.
\end{aligned}$$

Also

$$\begin{aligned}\sum_{\alpha=0}^{m-1}\delta^{\alpha}C &= \sum_{\alpha=0}^{m-1}(NT^{\alpha})(I,T,T^2,\dots,T^{m-1})^t e\\ &= (NJ)(I,T,T^2,\dots,T^{m-1})^t e\\ &= J(I,T,T^2,\dots,T^{m-1})^t e\\ &= J\otimes J.\end{aligned}$$

To prove condition (iv) we have :

$$\begin{aligned}(\delta X)(\delta Y)^t &= (X(I\otimes T))(Y(I\otimes T))^t\\ &= X(I\otimes T)(I\otimes T^{n-1})Y^t\\ &= X(I\otimes I)Y^t\\ &= XY^t.\end{aligned}$$

□

To prove that matrices B_i and C defined above form a regular s-set using Lemma 4.5 part (ii) it is sufficient to prove the next lemma

Lemma 4.6

$$\sum_{i=1}^{(m-1)/2}(B_iB_i^t + B_i^tB_i) + CC^t + C^tC = n^2(n+1)I$$

Proof

$$\begin{aligned}[CC^t]_{ij} &= mNT^iT^{m-i}N^t\\ &= mNT^{i-j}N^t\\ &= \begin{cases} m^2J & \text{if } i=j\\ -mJ & \text{otherwise.}\end{cases}\end{aligned}$$

So

$$CC^t = m(m+1)I\otimes J - mJ\otimes J. \tag{4.7}$$

We know that each row of matrix N is the vector $(b_0, b_1, \cdots, b_{m-1})$, where $b_0 = 1$ and $b_i = \chi(i)$ so we have:

$$[\sum_{k=0}^{m-1} T^k(N^tN)T^{-k}]_{ij} = m\sum_{k=0}^{m-1} b_{i+k}b_{j+k}.$$

If $i = j$:

$$[\sum_{k=0}^{m-1} T^k(N^tN)T^{-k}]_{ii} = m\sum_{k=0}^{m-1} b_{i+k}^2 = m^2.$$

If $i \neq j$:

$$[\sum_{k=0}^{m-1} T^k(N^tN)T^{-k}]_{ij} = m(b_0b_{j-1} + b_{i-j}b_0) + m\sum_{k=0}^{m-1} \chi(i+k)\chi(j+k) = -m.$$

So

$$\sum_{k=0}^{m-1} T^k(N^tN)T^{-k} = m(m+1)I - mJ$$

Now we are able to calculate C^tC.

$$\begin{aligned} C^tC &= J \otimes \sum_{k=0}^{m-1} (NT^k)^t(NT^k) \\ &= J \otimes \sum_{k=0}^{m-1} T^{-k}(N^tN)T^k \\ &= J \otimes \sum_{k=0}^{m-1} T^k(N^tN)T^{-k} \\ &= mJ \otimes ((m+1)I - J). \end{aligned} \tag{4.8}$$

To calculate $B_jB_j^t$ and $B_j^tB_j$ as well we have:

$$\begin{aligned}
B_jB_j^t &= \sum_{i=1}^{m-1}\sum_{h=0}^{m-1} RT^i(RT^h)^h \otimes MT^{ij}(MT^{hj})^t \\
&= \sum_{i=0}^{m-1}\sum_{h=0}^{m-1} T^{h-i} \otimes MM^tT^{ij-hj} \\
&= \sum_{z=0}^{m-1}\sum_{i=0}^{m-1} T^z \otimes MM^tT^{-zj} \qquad (z = h - i) \\
&= m\sum_{z=0}^{m-1} T^z \otimes MM^tT^{-zj}
\end{aligned}$$

Similarly one can show that:

$$B_j^tB_j = m\sum_{z=0}^{m-1} T^z \otimes MM^tT^{zj}$$

Now we have:

$$\begin{aligned}
\sum_{i=1}^{(m-1)/2} (B_iB_i^t + B_i^tB_i) &= m\sum_{z=0}^{m-1}\sum_{i=1}^{(m-1)/2} T^z \otimes MM^tT^{-zi} + m\sum_{z=0}^{m-1}\sum_{i=1}^{(m-1)/2} T^z \otimes MM^tT^{zi} \\
&= m\sum_{z=0}^{m-1}\sum_{j=1}^{m-1} T^z \otimes MM^tT^{-zj} \\
&= m\left(I \otimes (m-1)MM^t + \sum_{z=1}^{m-1} T^z \otimes MM^t(J - I)\right) \\
&= I \otimes m(m-1)MM^t + (J - I) \otimes mMM^t(J - I) \\
&= (I \otimes MM^t)(m^2I \otimes I - mI \otimes J - mJ \otimes I + m(J \otimes J)) \\
&= m^2(m+1)I \otimes I - m(m+1)J \otimes I \\
&\quad -m(m+1)I \otimes J + 2mJ \otimes J \qquad (4.9)
\end{aligned}$$

Using 4.7, 4.8, and 4.9 the result follows □

Lemma 4.7 *There is a permutation matrix P_i such that $C_iP_i = -C_i$, $P_i^2 = I$ for all $2 \leq i \leq 4n$.*

Proof Noting that $C_i = r_i^t r_i$, as defined in section 4.2, where r_i is any row of a normalised Hadamard matrix of order $4n$. Since $r_i r_1^t = 0$ there are exactly $2n$ ones in r_i. Let τ_1 be any permutation that moves the $+1$'s of r_i to the left and -1's to the right. Thus

$$\tau_1 r_i = 11\cdots 1 - - \cdots -$$

Let $\tau_2 = (1\ \ 2n{+}1)(2\ \ 2n{+}2)\cdots(2n\ \ 4n)$. We have $\tau_2\tau_1 r_i = -\tau_1 r_i$. So $\tau_1^{-1}\tau_2\tau_1 r_i = -r_i$. Let $\tau = \tau_1^{-1}\tau_2\tau_1$, we have $\tau r_i = -r_i$. The matrix P_i of the permutation τ is the required permutation matrix, $r_i^t r_i P_i = -r_i^t r_i$ and $P_i^2 = I$. □

Let

$$V := P_{2n+1} \otimes I_{m^2}$$

then $V^2 = I$ and $V^t = V$.

Definition 4.8 *Let E be a $(1,-1)$ matrix of order $4nm^2$ and I the identity matrix of order $4nm$. Define the map ρ as follows:*

$$\rho E := E(I \otimes T)V$$

Lemma 4.9 *Let $\mathcal{R} = \{K_1, K_1'\}$ and $\mathcal{S} = \{K_2, \cdots, K_{2n}, K_2', \cdots, K_{2n}'\}$, where K_i's are matrices of order $4nm^2$ as defined on page 47. Then $\mathcal{S}$, $\mathcal{R}$, and ρ satisfy the following properties:*

(i) $\rho^{2m}X = I$ *for every matrix X of size $2nm^2$;*

(ii) $(\rho^\alpha X)(Y)^t = 0$ *for all $X \in \mathcal{R}$, $Y \in \mathcal{S}$, $\alpha = 0, \cdots, 2m-1$;*

(iii) $(\rho X)(\rho Y)^t = XY^t$ *for all matrices X, and Y of size $4nm^2$;*

(iv) $\sum_{i=0}^{2m-1} \rho^i K_1 = 2J$ *and* $\sum_{i=0}^{2m-1} \rho^i K_1' = 0$.

Proof It is easy to see the validity of properties (i) and (iii). The proof of (ii) is an immediate consequence of Lemma 4.5 and properties of K_is and K_i's.
To prove (iv), we use Lemma 4.5 part (iii) to get

$$\sum_{i=0}^{m-1} L_1(I \otimes T^i) = J \otimes J.$$

Now we have:

$$\begin{aligned}\sum_{i=0}^{2m-1} \rho^i K_1 &= \sum_{i=0}^{m-1} L_1(I \otimes T^i) + \sum_{i=0}^{m-1} L_1(I \otimes T^i)V \\ &= J \otimes J + (J \otimes J)V \\ &= 2J \otimes J.\end{aligned}$$

$$\begin{aligned}\sum_{i=0}^{2m-1} \rho^i K_1' &= \sum_{i=0}^{m-1} C_{2n+1} * L_1(I \otimes T^i) + \sum_{i=0}^{m-1} C_{2n+1} * L_1(I \otimes T^i)V \\ &= C_{2n+1} * (J \otimes J) + C_{2n+1} * (J \otimes J)V \\ &= C_{2n+1} \otimes J + (C_{2n+1} \otimes J)V \\ &= C_{2n+1} \otimes J + (C_{2n+1} \otimes J)(P_{2n+1} \otimes I) \\ &= C_{2n+1} \otimes J + (C_{2n+1}P_{2n+1}) \otimes J \\ &= C_{2n+1} \otimes J - C_{2n-1} \otimes J = 0.\end{aligned}$$

□

Following a notation of Ionin [5], we let $\mathcal{M}$ be the set of block matrices $D = [D_{ij}], i, j = 1, ..., 4n$, such that:

(i) for each $i = 1, \cdots, 4n$, there is a unique $h_i = h_i(D) \in \{1, \cdots, 4n\}$, such that for $j = h_i$, $D_{ij} = \rho^\alpha K_1$ for some integer α;

(ii) for each i, $i = 1, \cdots, 4n$, there is a unique $h_i' = h_i'(D) \in \{1, \cdots, 4n\}$, $h_i' \neq h_i$ such that for $j = h_i'$, $D_{ij} = \pm\rho^\alpha K_1'$ for some integer α;

(iii) for $i = 1, \cdots, 4n$, and for $j \neq h_i$ and $j \neq h_i'$, $D_{ij} = \pm K_l$ or $\pm K_l'$ for $l = 2, \cdots, 2n$.

Clearly H is an element of $\mathcal{M}$. Define a bijection $\sigma : \mathcal{M} \to \mathcal{M}$ by $\sigma D = D' = [D_{ij}']$ where:

(i) for $i = 1, ..., 4n$, and $j = 2, ..., 4n$, $D_{ij}' = D_{i,j-1}$;

(ii) for $i = 1, ..., 4n$, if $h_i(D) = 4n$ or $h_i'(D) = 4n$ then $D_{i1}' = \rho D_{i,4n}$;

(iii) for $i = 1, \ldots, 4n$, if $h_i(D) \neq 4n$ and $h'_i(D) \neq 4n$ then $D'_{i1} = -D_{i,4n}$.

It follows from the fact that $\rho^{2m} = 1$ and from the number of blocks of D that the order of the cyclic group G generated by σ is $8nm$.

Lemma 4.10 *For $X, Y \in \mathcal{M}$, $(\sigma X)(\sigma Y)^t = XY^t$.*

Proof Let $X, Y \in \mathcal{M}$ and let $X' = \sigma X$ and $Y' = \sigma Y$. It is sufficient to show that, for $i, i' = 1, \ldots, 4n$,

$$X'_{i1}Y'^t_{i'1} = X_{i,4n}Y^t_{i',4n}.$$

Let $\mathcal{R}' = \{\rho^\alpha K_1, \pm\rho^\alpha K'_1 | \alpha = 0, \cdots, 2m-1\}$ and let $\mathcal{S}' = \{\pm K_l, \pm K'_l | l = 2, \cdots, 2n\}$. It is obvious that $X_{i,4n}$ and $Y_{i',4n}$ are either in $\mathcal{R}'$ or in $\mathcal{S}'$. We have to check the following cases:

- If $X_{i,4n} \in \mathcal{S}'$ and $Y_{i',4n} \in \mathcal{S}'$ then $X'_{i1}Y'^t_{i'1} = (-X_{i,4n})(-Y_{i',4n})^t = X_{i,4n}Y^t_{i',4n}$.
- If $X_{i,4n} \in \mathcal{R}'$ and $Y_{i',4n} \in \mathcal{S}'$ then using Lemma 4.9 we can see that $X'_{i1}Y'^t_{i'1} = X_{i.4n}Y^t_{i',4n} = 0$.
- The proof for the case $X_{i,4n} \in \mathcal{S}'$ and $Y_{i',4n} \in \mathcal{R}'$ is similar and we omit it.
- If $X_{i,4n} \in \mathcal{R}'$ and $Y_{i',4n} \in \mathcal{R}'$ then $X'_{i1}Y'^t_{i'1} = (\rho X_{i,4n})(\rho Y_{i',4n})^t = X_{i,4n}Y^t_{i',4n}$.

□

Lemma 4.11 $\sum_{g=0}^{8nm-1} \sigma^g H = 2J$.

Proof Using Lemma 4.9, if $1 \leq i \leq 2n$ we see that the (i,j)-block of the matrix $\sum_{g=1}^{8nm} \sigma^g H$ is:

$$\begin{aligned}[\sum_{l=0}^{8nm-1} \sigma^l H]_{ij} &= \sum_{\alpha=0}^{2m-1} \rho^\alpha K_1 + \sum_{\alpha=0}^{2m-1} \rho^\alpha K'_1 \\ &= 2J + 0 = 2J.\end{aligned}$$

If $2n < i \leq 4n$ we have:

$$\begin{aligned}[\sum_{l=0}^{8nm-1} \sigma^l H]_{ij} &= \sum_{\alpha=0}^{2m-1} \rho^\alpha K_1 - \sum_{\alpha=0}^{2m-1} \rho^\alpha K'_1 \\ &= 2J - 0 = 2J.\end{aligned}$$

□

Theorem 4.12 *The matrix H is productive.*

Proof Using lemmas 4.10 and 4.11 we see that the matrix H, the set $\mathcal{M}$ and the bijection σ satisfy all of the conditions of definition 3.4. $\square$

We are now ready to apply a recent result of Ionin [4] to construct many new classes of symmetric designs. We start with a definition.

Let $m = 8n^2 - 1$ be a prime number. Then the matrix H above, and consequently the matrix $-H$, has a group of symmetry. Let G be the group of symmetry defined above. Upon Theorem 3.6, we get the following corollary.

Corollary 4.13 *Let $m = 8n^2 - 1$ be a prime number.*

- *If $q = (4nm - 1)^2$ is a prime power, then there is a symmetric design with parameters*

$$(16n^2m^2(q^t + q^{t-1} + ... + 1), (8n^2m^2 - 2nm)q^t, (4n^2m^2 - 2nm)q^t),$$

  for every nonnegative integer t.

- *If $q = (4nm + 1)^2$ is a prime power then there is a symmetric design with parameters*

$$(16n^2m^2(q^t + q^{t-1} + ... + 1), (8n^2m^2 + 2nm)q^t, (4n^2m^2 + 2nm)q^t),$$

  for every nonnegative integer t.

Remark 4.14 We need to close the thesis with an explanation to link our work in different chapters of this document. Our original aim was to use the T–matrices introduced in chapter 2 to generate a productive class of regular Hadamard matrices. Soon after we were convinced that this was a very tough project requiring longer time. We then turned our attention to Mathon matrices and Kharaghani matrices and our search was successful. We end this thesis with high hopes of getting an opportunity to spend more time on techniques akin to Xia and Xia and developing it into another productive class of regular Hadamard matrices.

.

Bibliography

[1] Ian Anderson, *Combinatorial designs: Construction methods*, Ellid Horwood Limited, 1990.

[2] Gerald Berman, *Families of generalized weighing matrices*, Canad. J. Math. **30** (1978), no. 5, 1016–1028.

[3] A. V. Geramita and J. Seberry, *Orthogonal designs, quadratic forms and Hadamard matrices*, Marcel Dekker, 1979.

[4] Yury J. Ionin, *Regular hadamard matrices generating infinite families of symmetric designs*, Preprint.

[5] ———, *New symmetric designs from regular hadamard matrices*, Electron. J. Combin **5** (1998), no. 1, Research Paper 1, 8 pp. (electronic).

[6] ———, *A technique for constructing symmetric designs*, Des. Codes Cryptogr. **14** (1998), no. 2, 147–158.

[7] ———, *Applying balanced generalized weighing matrices to construct block designs*, Electron. J. Combin **8** (2001), no. 1, Research Paper 12, 15 pp. (electronic).

[8] H. Kharaghani, *New class of weighing matrices*, Ars Combin. **19** (1985), 69–72.

[9] ———, *On the siamese twin designs*, Finite fields and applications (1999), 303–312.

[10] ———, *On the twin designs with the ionin-type parameters*, Electron. J. Combin. **7** (2000), no. 1, Research Paper 1, 11 pp. (electronic).

[11] H. Kharaghani and B. Tayfeh-Rezaie, *Some new orthogonal designs in orders 32 and 40*, Discrete Math., to appear.

[12] R. Mathon, *Symmetric conference matrices of order $pq^2 + 1$*, Canad. J. Math. **30** (1978), 321–331.

[13] Jennifer Seberry and Albert Leon Whiteman, *New hadamard matrices and conference matrices obtained via mathon's construction*, Graphs and Combinatorics **4** (1988), 355–377.

[14] Jennifer Seberry and Mieko Yamada, *Hadamard matrices, sequences, and block designs. contemporary design theory*, Wiley-Intersci. Ser. Discrete Math. Optim., 1992.

[15] R. J. Turyn, *Hadamard matrices, baumert-hall units, four symbol sequences, pulse compression and surface wave encodings*, J. Combin. Theory A **16** (1974), 313–333.

[16] Mingyuan Xia, *Some new families of sdss and hadamard matrices*, Acta Math. Sci. (English Ed.) **16** (1996), no. 2, 153–161.

[17] Ming yuan Xia and Tianbing Xia, *A family of C-partitions and t-matrices*, J. Combin. Des. **7** (1999), no. 4, 269–281.