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

## 4.1 Introduction

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

## 4.2 Some Orthogonal Designs Exist

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

**Table 4.2** Values for $X$ and $W$

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

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

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

*Proof.* This follows immediately from Theorem 1.2. □

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

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

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

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

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

*Example 4.1.*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 4.3 Some Basic Matrix Results

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(c) A matrix $A = (a_{ij})$ of order $n$ will be called *back circulant* if $a_{ij} = a_{1,i+j-1}$ where $i+j-1$ is reduced modulo $n$. For example:

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

*Remark 4.3.* (i) Any type 1 matrix defined on $Z_t$ (with its usual ordering) is circulant since:

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

(ii) Any type 2 matrix defined on $Z_t$ (with its usual ordering) is back circulant since:

$$n_{ij} = \phi(i+j) = \phi(i+j-1+1) = n_{1,i+j-1}.$$

Clearly, any circulant matrix is a type 1 matrix, and any back circulant matrix is a type 2 matrix. In any case:

- A type 1 matrix is analogous to a circulant matrix;
- A type 2 matrix is analogous to a back circulant matrix.

Thus, all propositions proved about type 1 and type 2 matrices have corollaries about circulant and back circulant matrices.

**Lemma 4.4.** *Suppose $G$ is an additive abelian group of order $v$ with elements ordered $z_1, z_2, \ldots, z_v$. Let $\phi$, $\psi$, and $\mu$ be functions from $G$ to some commutative ring $R$.*

Define $A = (a_{ij})$, $B = (b_{ij})$ and $C = (c_{ij})$ by $a_{ij} = \phi(z_j - z_i)$, $b_{ij} = \psi(z_j - z_i)$ and $c_{ij} = \mu(z_j + z_i)$. Then

$$\text{(i)} \quad C^\top = C, \qquad \text{(ii)} \quad AB = BA, \qquad \text{(iii)} \quad AC^\top = CA^\top.$$

*Proof.* (i) $c_{ij} = \mu(z_j + z_i) = \mu(z_i + z_j) = c_{ji}$.

(ii) $(AB)_{ij} = \sum_{g \in G} \phi(g - z_i)\psi(z_j - g)$.

Putting $h = z_i - z_j - g$, it is clear that as $g$ ranges through $G$, so does $h$, and the above expression becomes

$$\sum_{h \in G} \phi(z_j - h)\psi(h - z_i) \;=\; \sum_{n \in G} \psi(h - z_i)\phi(z_j - h)$$

(since $R$ is commutative); this is $(BA)_{ij}$.

$$\begin{aligned} \text{(iii)}\ (AC^\top)_{ij} &= \textstyle\sum_{g \in G} \phi(g - z_i)\psi(z_j + g) \\ &= \textstyle\sum_{h \in G} \phi(h - z_j)\mu(z_i + h) \qquad (h = z_j + g - z_i) \\ &= (CA^\top)_{ij}. \end{aligned}$$

□

**Corollary 4.4.** *If $X$ and $Y$ are type 1 matrices and $Z$ is a type 2 matrix, all defined on the same abelian group with a fixed ordering, then (i) $Z^\top = Z$, (ii) $XY = YX$, (iii) $XZ^\top = ZX^\top$.*

**Lemma 4.5.** *(i) If $X$ is a type 1, $i = 1, 2$, matrix, then so is $X^\top$.*
*(ii) If $X$ and $Y$ are type 1 matrices, $i = 1, 2$, both defined on the same abelian group with a fixed ordering, then so is $X + Y$ and $X - Y$.*

*Proof.* (i.a) If $X = (x_{ij})$ is type 2 defined using a function $\phi$, then $X_{ij} = \phi(z_i + z_j) = \phi(z_j + z_i) = X_{ji}$. So $X^\top$ is also defined as type 2 using $\phi$.

(i.b) If $X = (x_{ij})$ is of type 1 defined using $\psi$, then $x_{ij} = \psi(z_j - z_i)$. Now define a type 1 matrix $M = (m_{ij})$ using $\mu$, where $\mu(x) = \psi(-x)$. Then $m_{ij} = \mu(z_j - z_i) = \psi(z_i - z_j) = x_{ji}$. Thus $M = X^\top$.

(ii.a) If $X$ and $Y$ are type 2 defined using $\phi_1$ and $\phi_2$, then the type 2 matrices defined using $\phi_1+\phi_2$ and $\phi_1-\phi_2$ respectively, give $X+Y$ and $X-Y$, respectively.

(ii.b) Similarly, if $X$ and $Y$ are type 1 defined using $\psi_1$ and $\psi_2$, define type 1 matrices using $\mu_1+\mu_2$ and $\mu_1-\mu_2$, respectively, to obtain $X+Y$ and $X-Y$, respectively, where $\mu_i(x)=\psi_i(-x)$. □

**Corollary 4.5.** *(i) If $X$ and $Y$ are type 1 matrices, defined on the same abelian group with a fixed ordering, then*

$$\begin{array}{ll} XY=YX & XY^\top=Y^\top X \\ X^\top Y=YX^\top & X^\top Y^\top=Y^\top X^\top \end{array}.$$

*(ii) If $P$ is a type 1 matrix and $Q$ is a type 2 matrix, both defined on the same abelian group with a fixed ordering, then*

$$\begin{array}{ll} PQ^\top=QP^\top & P^\top Q^\top=QP \\ PQ=Q^\top P^\top & P^\top Q=Q^\top P \end{array}.$$

We now summarize the most used results for circulants.

**Corollary 4.6.** *(i) Two circulant matrices of the same order commute.*
*(ii) A back circulant matrix is symmetric.*
*(iii) The product of a back circulant matrix with a circulant matrix of the same order is symmetric. In particular, if $B$ is back circulant and $A$ is circulant,*

$$AB^\top=BA^\top.$$

*$A$ and $B$ are amicable matrices (see Chapter 5)*

**Remark**. From now on, whenever we refer to a collection of type 1 and type 2 matrices all defined on the same abelian group $G$, we shall assume that the ordering of the group elements has been fixed.

**Lemma 4.6.** *(i) Let $X$ and $Y$ be type 2 $(d,e,f)$ incidence matrices generated by subsets $A$ and $B$ of an additive abelian group $G$. Suppose, further, that*

$$a\in A\Rightarrow -a\in A \quad \textit{and} \quad b\in B\Rightarrow -b\in B\,.$$

*Then,*

$$XY=YX \quad \textit{and} \quad XY^\top=YX^\top\,.$$

*(ii) The same result holds if $X$ and $Y$ are type 1.*

*Proof.* (i) Since $X$ and $Y$ are symmetric, we only have to prove that $XY^\top=YX^\top$. Suppose $X=(x_{ij})$ and $Y=(y_{ij})$ are defined by

$$x_{ij}=\phi(z_i+z_j), \qquad y_{ij}=\psi(z_i+z_j)\,,$$

where $z_1, z_2, \ldots$ are the elements of $G$. Then

$$\begin{aligned}
(XY^\top)_{ij} &= \sum_k \phi(z_i + z_k)\psi(z_k + z_j) \\
&= \sum_k \phi(-z_i - z_k)\psi(z_k + z_j) && \text{since } a \in A \Rightarrow -a \in A \\
&= \sum_\ell \phi(z_j + z_\ell)\psi(-z_\ell - z_i - z_j + z_j) && z_\ell = -z_k - z_i - z_j \\
&= \sum_\ell \phi(z_j + z_\ell)\psi(z_\ell + z_i) && \text{since } b \in B \Rightarrow -b \in B \\
&= (YX^\top)_{ij}\,.
\end{aligned}$$

(ii) The additional hypotheses on $A$ and $B$ force $X$ and $Y$ to be symmetric. The proof, then, is similar to (i), and we leave it to the reader as an easy exercise. □

**Lemma 4.7.** *Let $R = (r_{ij})$ be the permutation matrix of order $n$, defined on an additive abelian group $G = \{g_i\}$ of order $n$ by*

$$r_{k,j} = \begin{cases} 1 & \text{if } g_k + g_j = 0 \\ 0 & \text{otherwise.} \end{cases}$$

*(i) If $M$ is a type 1 matrix defined on $G$, then $MR$ is a type 2 matrix defined on $G$.*
*(ii) If $N$ is a type 2 matrix defined on $G$, then $NR$ is a type 1 matrix defined on $G$.*
*(iii) If $X$ is a subset of $G$ where $0 \notin X$ and $M$ is the type 1 $(a,b,c)$ incidence matrix generated by $X$, then $MR$ is the type 2 $(a,b,c)$ incidence matrix generated by $-X$.*
*(iv) If $X$ is as in (3) and $N$ is the type 2 $(a,b,c)$ incidence matrix generated by $X$, then $NR$ is the type 1 $(a,b,c)$ incidence matrix generated by $-X$.*

*Proof.* 1.) Let $M = (m_{ij})$ be defined by $m_{ij} = \psi(g_j - g_i)$, and let $\mu(x) = \psi(-x)$. We claim that $MR$ is the type 2 matrix defined by $\mu$, for

$$\begin{aligned}
(MR)_{ij} &= \sum_k m_{ik} r_{kj} = m_{i\ell}, \text{ where } g_\ell + g_j = 0, \\
&= \psi(g_\ell - g_i) = \psi(-g_j - g_i) = \mu(g_j + g_i)\,.
\end{aligned}$$

2.) follows from a similar argument.
3.) and 4.) are clear from 1.) and 2.) and the relationship between $\psi$ and $\mu$. □

**Corollary 4.7.** *Let $G$ be an additive abelian group and $X$ a subset of $G$ where $0 \notin X$. Let $M$ be the type 1 $(a,b,c)$ incidence matrix generated by $X$, and $N$ the type 2 $(a,b,c)$ incidence matrix generated by $-X$. Then*

$$MM^\top = NN^\top .$$

*Proof.* Lemma 4.7 gives that $M = NR$, where $R$ is the permutation matrix appropriate to $G$. The corollary follows since $RR^\top = 1$. □

### *4.3.1 Supplementary Difference Sets, their Incidence Matrices and their Uses as Suitable Matrices*

**Definition 4.3.** Let $S_1, S_2, \ldots, S_n$ be subsets of $V$, an additive abelian group of order $v$. Let $|S| = k_i$ and $S_i = s_{i1}, s_{i2}, \ldots, s_{ik_i}$. If the equation

$$g = s_{ij} - s_{im}$$

has exactly $\lambda$ solutions for each non-zero element $g$ of $V$, then $S_1, S_2, \ldots, S_n$ will be called $n - \{v; k_l, k_2, \ldots, k_n; \lambda\}$ *supplementary difference sets* or sds. If $k_1 = k_2 = \cdots = k_n = k$, we write $n - \{v; k; \lambda\}$ sds.

**Lemma 4.8.** *Suppose $A_1, \ldots, A_n$ are the type 1 $(0,1)$ incidence matrices generated by $S_1, \ldots, S_n$, where $S_1, \ldots, S_n$ are $n - \{v; k; \lambda\}$ sds. Then*

$$\sum_{i=1}^{n} A_i A_i^\top = \left( \sum_{i=1}^{n} k_i - \lambda \right) I + \lambda J .$$

*Proof.* This follows from the definition by a simple counting argument. (See Wallis [231, p.290] for a fuller proof.) □

*Example 4.4.* $S_1 = \{0,2,3\}$ and $S_2 = \{0,1,4\}$ are $2 - \{5;3;3\}$ sds in $Z_5$. Their type 1 $(1,0)$ incidence matrices are the circulants

$$A_1 = \begin{bmatrix} 1\,0\,1\,1\,0 \\ 0\,1\,0\,1\,1 \\ 1\,0\,1\,0\,1 \\ 1\,1\,0\,1\,0 \\ 0\,1\,1\,0\,1 \end{bmatrix} \quad \text{and} \quad A_2 = \begin{bmatrix} 1\,1\,0\,0\,1 \\ 1\,1\,1\,0\,0 \\ 0\,1\,1\,1\,0 \\ 0\,0\,1\,1\,1 \\ 1\,0\,0\,1\,1 \end{bmatrix}$$

which satisfy

$$A_1 A_1^\top + A_2 A_2^\top = 3I + 3J .$$

We observe that for these subsets of $Z_5$, $x \in S_i \Rightarrow -x \in S_i$. So, if $R$ is the back diagonal matrix of order 5 (see Lemma 4.7), we see $A_1 R = B_1$ and $A_2 R = B_2$ are the type 2 $(1,0)$ incidence matrices generated by $S_1$ and respectively.

$$B_1 = A_1R = \begin{bmatrix} 1\,0\,1\,1\,0 \\ 0\,1\,1\,0\,1 \\ 1\,1\,0\,1\,0 \\ 1\,0\,1\,0\,1 \\ 0\,1\,0\,1\,1 \end{bmatrix} \quad \text{and} \quad B_2 = A_2R = \begin{bmatrix} 1\,1\,0\,0\,1 \\ 1\,0\,0\,1\,1 \\ 0\,0\,1\,1\,1 \\ 0\,1\,1\,1\,0 \\ 1\,1\,1\,0\,0 \end{bmatrix}.$$

Using Lemma 4.6 (or directly), we obtain

$$B_1B_2 = B_2B_1 \text{ and } B_1B_2^\top = B_2B_1^\top.$$

Also

$$A_1A_2 = A_2A_1 \text{ and } A_1A_2^\top = (B_1R)(B_2R)^\top = B_2B_1^\top.$$

We also observe that

$$A_1B_2^\top = B_2A_1^\top \text{ and } A_iA_i^\top = B_iB_i^\top.$$

**Lemma 4.9.** *Let $A_1,\ldots,A_n$ be type 1 $(1,0)$ incidence matrices generated by $S_1,\ldots,S_n$ where $S_1,\ldots,S_n$ are $n-\{v;k_1,\ldots,k_n;\lambda\}$ sds.*

Let $B_i = A_i - J$. Then

$$\sum_{i=1}^{n} B_iB_i^\top = 4\left(\sum_{j=1}^{n} k_j - \lambda\right) I + \left[nv - 4\left(\sum_{j=1}^{n} k_j - \lambda\right)\right] J.$$

We are constantly searching for $(0,1,-1)$ matrices to substitute for the variables in an orthogonal design. We shall be precise about what is needed.

**Definition 4.4.** A set of $m$ $(0,1,-1)$ matrices $A_1, A_2, \ldots, A_m$ of order $n$ will be called *suitable plug-in matrices* for the orthogonal design of type $OD(n; s_1, s_2, \ldots, s_m)$ if

$$\begin{aligned} &1) \quad A_iA_j^\top = A_jA_i^\top, \quad 1 \le i, \quad j \le m; \\ &2) \quad \sum_{i=1}^{m} s_iA_iA_i^\top = kI_n. \end{aligned}$$

2) is called the *additive property*. So suitable matrices are pairwise amicable and satisfy the additive property.

**Theorem 4.4.** *Let $S_1, S_2, S_3, S_4$ be $4-\{t;k_1,k_2,k_3,k_4;\sum_{j=1}^{4} k_j - t\}$ sds for which $x \in S_i \Rightarrow -x \in S_i$, and let $A_l, A_2, A_3, A_4$ be the type 1 $(1,-1)$ incidence matrices of these sets. Then $A_1, A_2, A_3, A_4$ are suitable matrices for an orthogonal design $OD(4st; s, s, s, s)$.*

*Proof.* Since $x \in S_i \Rightarrow -x \in S_i$ we see that $A_i$, $i = 1,2,3,4$, are symmetric and commuting. Using Lemma 4.9, we have

$$\sum_{i=1}^{4} A_i A_i^\top = 4\left(\sum_{j=1}^{4} k_j - \sum_{j=1}^{4} k_j + t\right) I + \left(4t - 4\left(\sum_{j=1}^{4} k_j - \sum_{j=1}^{4} k_j + t\right)\right) J$$
$$= 4tI.$$

In particular,

$$\sum_{i=1}^{4} sA_i A_i^\top = 4stI\,.$$

If the variables of the orthogonal design are replaced by the $A_i$, $i = 1,2,3,4$, we have a weighing matrix of weight $4st$. □

If the orthogonal design of the theorem is of order $4s$, then the weighing matrix obtained will be of order $4st$ and weight $4st$, in other words, an Hadamard matrix of order $4st$. In this case the symmetric matrices of Theorem 4.4 are a special kind of what will be called Williamson matrices (see also Definition 4.16).

## 4.4 Existence of Weighing Matrices

In 1972 at the first Australian conference on Combinatorial Mathematics, Seberry Wallis gave her first paper on weighing matrices [232]. Weighing matrices also caused interest at Queen' s University that year. It was observed that in order to establish existence in all orders for a given weight we needed to consider weighing matrices in odd orders.

We noticed that there was a circulant $W(7,4)$. It has first row $-110100$.

Then D. Gregory found a non-circulant $W(13,9)$. After observing that the zeros of this matrix give the incidence matrix of a finite projective plane, we found a circulant $W(13,9)$ with first row $0010111-01-1$.

At the Fifth South-eastern Conference on Combinatorics, Graph Theory and Computing in Boca Raton, Florida, in 1972, Rick Wilson and R.C. Mullin said they thought $W(q^2+q+1,q^2)$ might exist when $q$ was a prime power.

At that time Mullin [153] was writing a book on Coding Theory with Ian Blake [23], who quickly saw the possibilities of using weighing matrices and especially circulant matrices $W$ to form generator matrices $[I,W]$ of codes over $GF(3)$ which would generalise the Pless symmetry codes.

Wallis and Whiteman (Theorem 4.6) finally showed that circulant $W(q^2+q+1,q^2)$ existed when $q$ was a prime power.

In writing this section it seemed that the proof of Wallis and Whiteman was too circuitous and a prettier, more direct proof was desirable. Our colleague, L.G. Kovacs, has given three proofs; the second is illustrated by Example

4.8 and we feel is intrinsically very beautiful. The first proof is illustrated by Example 4.9. The proof we have given here is the shortest, but hides to some extent the delightful intimacy between circulant weighing matrices and cyclic projective planes. The work of David Glynn gives more insight. (See Glynn [87].)

It was Kovacs' work that allowed Hain and Eades [54] to establish that there are only two equivalence classes of circulant $W(13,9)$. Many others [6, 7, 9–11, 153, 201, 252] have continued this study of circulant weighing matrices, but the full story is not yet known.

If $A$ is a $W(n,k)$, then $(\det A)^2 = k^n$. Thus if $n$ is odd and a $W(n,k)$ exists, then $k$ must be a perfect square.

In Proposition 2.3 it is shown that

$$(n-k)^2 - (n-k) + 2 > n$$

must also hold. It is noted there that the "boundary" values of this condition are of special interest, that is, if

$$(n-k)^2 - (n-k) + 1 = n,$$

for in this case the zeros of $A$ occur such that the incidence between any pair of rows is exactly one. So if we let $B = J_n - AA^\top$, $B$ satisfies

$$BB^\top = (n-k-1)I_n + J_n, \quad BJ_n = (n-k)J_n;$$

that is, $B$ is the incidence matrix of the projective plane of order $n-k-1$.

Thus the non-existence of the projective plane of order $n-k-1$ implies the non-existence of the $W(n,k)$ when $n = (n-k)^2 - (n-k) + 1$. So we rewrite the Bruck-Ryser-Chowla Theorem from Hall [97, p.107–112] to allow us to consider the non-existence of projective planes.

**Theorem 4.5 (Bruck-Ryser).** *If there exists a projective plane of order $s$, then the Diophantine equation*

$$x^2 = sy^2 + (-1)^{\frac{(s^2+2)}{2}} z^2$$

*has a solution in the integers not all zero. That is, the Hilbert symbol*

$$\left( (-1)^{\frac{(s^2+2)}{2}}, s \right)_p = +1$$

*for all primes $p$, including $p = \infty$.*

*Example 4.5.* Consider $s = n-k-1 = 6$ , $s^2+s+1 = n = 43$, $s^2 = k = 36$. The Bruck-Ryser Theorem says that there is a projective plane only if

$$\left(-1^{21}, 6\right)_p = (-1, 6)_p = +1 \quad \text{at all primes } p.$$

But at $p = 3$

$$(-1,6)_3 = (-1,2)_3(-1,3)_3 = \left(\tfrac{2}{3}\right) = -1\,.$$

So there is no projective plane of order 6 and no $W(43,36)$.

Similarly, if $s = 2t = n-k-1$, $s^2+s+1 = n$, $s^2 = k$, where $t \equiv 3 \pmod 4$ is a prime, there is no projective plane of order $2t$ and no $W(4t^2+2t+1, 4t^2)$.

Before we prove our result on circulant weighing matrices, we prove the following more general result.

**Lemma 4.10 (Blake [23]).** *Let $q$ be the power of an odd prime and $k$ any integer $k \geq 3$. Then there exists a*

$$W\left(\frac{(q^k-1)}{q-1}, q^{k-1}\right).$$

*Proof.* Let $G$ be a $kX(q^k-1)$ matrix whose columns contain all the distinct non-zero $k$-tuples over the finite field $GF(q)$. In coding terms, the row space of $G$, denoted by $C$, is equivalent to a maximum length cyclic code. It is known that the weight of every non-zero codeword in $C$ is $(q-1)q^{k-1}$. If $G^1$ is the $k \times (q^k-1)$ matrix whose rows are any set of $k$ linearly independent codewords of $C$, then every non-zero $k$-tuple over $GF(q)$ appears as a column of $G^1$.

Let $H$ be a $k \times n$ submatrix of $G$, $n = \frac{q^k-1}{q-1}$, with the property that any two of its columns are linearly independent. We assume that $H$ is normalized in the sense that the first non-zero element in each column is unity. Let $A$ be an $n \times n$ matrix whose rows are chosen from the non-zero vectors of the row space of $H$ and have the property that any two distinct rows are linearly independent. Assume for convenience that the first $k$ rows of $A$ are rows of $H$. It follows readily from observations on $G$ that every row of $A$ has weight $q^{k-1}$. It is not difficult to show that if $H$ is the $(0,1)$ matrix obtained from $H$ by replacing each non-zero element by unity, then the rows of $H^1$ are the incidence vectors of the compliments of the hyperplanes of the geometry $PG(k-1,q)$.

Let $x_1$ and $x_2$ be two distinct rows of $A$. Since they are independent, they can be extended to a basis $x_i$ , $i = 1,\ldots,k$, each vector of which is a row of $A$. Let B be the $k \times n$ matrix whose $i$-th row is $x_i$, $i = 1,\ldots,k$ . Assume $B$ has been normalized by multiplying each column so that the first non-zero element in each column is unity. let $B^1$ be the $k \times q^{k-1}$ submatrix of $B$ consisting of those columns with unity in the first row. Every $(k-1)$-tuple over $GF(q)$, including the a1l-zeros $(k-1)$-tuple, appears in the columns of $B$ in rows 2 through $k$. Each element of $GF(q)$ appears $q^{k-2}$ times in the second row of $B$. In the matrix $A$, replace $\alpha \in GF(q)$ by $\chi(\alpha)$, where $\chi$ is the usual quadratic character, and call the resulting matrix $S(q^{k1})$. We now show that over the real numbers

$$S\left(q^{k-1}\right) S\left(q^{k-1}\right)^t = q^{k-1} I_n$$

and thus that $S(q^{k-1})$ is the required $W\left(\frac{q^k-1}{q-1}, q^{k-1}\right)$.

Since every row of $A$ is of weight $q^{k-1}$ and each non-zero element of $GF(q)$ is either a square or a non-square, the inner product over the reals of any row of $S(q^{k-1})$ with itself is $q^{k-1}$. Let $x_1 = (\alpha_l, \ldots, \alpha_n)$, $x_2 = (\beta_1, \ldots, \beta_n)$ be two distinct rows of $A$. If $y_1 = (\chi(\beta_1), \ldots, \chi(\beta_n))$ and $y_2 = (\chi(\alpha_1), \ldots, \chi(\alpha_n))$ are the corresponding rows of $S(q^{k-1})$, then the inner product of $y_1$ and $y_2$ over the reals is the number of non-zero coordinate positions for which $\chi(\alpha_i) = \chi(\beta_i)$ less the number of non-zero coordinate positions for which $\chi(\alpha_i) \neq \chi(\beta_i)$. Since $\chi$ is multiplicative, i.e. , $\chi(\alpha)\chi(\beta) = \chi(\alpha\beta)$, multiplication of a coordinate position by a non-zero element of $GF(q)$ does not change the agreement or disagreement between coordinate positions of $y_1$ and $y_2$. As before, assume that $x_1$ and $x_2$ are the first two rows of the matrix $B$, which is assumed in normalized form. In the non-zero positions of $x_1$, each element of $GF(q)$ appears in $x_2$, $q^{k-2}$ times. Thus the inner product of the corresponding vectors $y_1$ and $y_2$ is zero, which completes the lemma. □

We now show how to construct circulant weighing matrices based on the fact that an oval in a projective plane can meet a line in only one of three ways: 0 (it misses it entirely), 1 (it is a tangent), 2 (it intersects the oval). This observation is true for any projective plane of prime power order (even or odd). These will be used extensively in later theorems.

**Theorem 4.6 (Wallis-Whiteman [242], proof by L. G. Kovacs).** *Let $q$ be a prime power. Then there is a circulant $W(q^2+q+1, q^2)$.*

*Proof.* Let $D$ be a cyclic planar difference set with parameters $(q^2+q+1, q+1, 1)$. (See Baumert [16] for definition.) These always exist for $q$ a prime power, and the incidence matrix of $D$ is the incidence matrix of the projective plane of order $q$.

Without loss of generality, we assume $0 \in D$. We note that $d$ and $-d$ cannot both be in $D$ because $d - 0 = 0 - (-d)$, contradicting the uniqueness of differences in $D$.

Let

$$\psi(x) = \sum_{d \in D} x^d$$

be the Hall polynomial of $D$. (see Baumert [16, p.8]) Then

$$\psi^2(x) = \sum_{d \in D} x^{2d} + 2 \sum_{\substack{e,f \in D \\ e \neq f}} x^{e+f}$$

We wish to show the coefficients of $x^i$ in $\chi^2(x)$ are 0, 1, 2, i.e. , that $2d \neq 2e$ unless $d = e$, $e + f \neq e' + f'$ unless $e = e'$ and $f = f'$ , and $2d \neq e + f$ unless $d = e = f$.

Clearly, $2d \neq 2e$ for $d \neq e$. If $e + f = e' + f'$, then $e - e' = f - f'$, and by the uniqueness of differences in $D$ either $e = f$ and $e' = f'$ or $e = -f'$ and

$e' = -f$. In the first case $2e = 2e'$ , $e = e'$, $f = f'$, and in the second case $e+f = -(e+f)$, i.e. , $e+f = 0$ and $e$ and $-e \in D$, which is not possible. If $2d = e+f$, then $d-e = f-d$, and by the uniqueness of differences in $D$, either $d = f$, $e = d$ or $d = -d$, $e = -f$. In the first case there is nothing to prove, and in the second case $e$ and $-e \in D$, which is not possible.

Hence if $B$ is the cyclic incidence matrix of $D$, then $B^2$ has elements 0, 1, 2, and $B^2 - J$ has elements 0, 1, -1.

Now

$$\begin{aligned}\left(B^2 - J\right)\left(B^2 - J\right)^\top &= BBB^\top B^\top - BBJ + J^2 .\\ &= (qI + J)^2 - 2(q+1)^2 J + (q^2+q+1)J .\\ &= q^2 I\end{aligned}$$

So $B^2 - J$ is the required $W(q^2+q+1, q^2)$. □

*Example 4.6.* $\{0,1,3,9\}$ is a difference set modulo 13, whose circulant incidence matrix $B$ has first row

$$1\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0.$$

$B^2$ is a circulant matrix with first row

$$1\ 2\ 1\ 2\ 2\ 1\ 1\ 0\ 0\ 2\ 2\ 0\ 2,$$

and $B^2 - J$ is the required circulant matrix with first row

$$0\ 1\ 0\ 1\ 1\ 0\ 0\ -\ -\ 1\ 1\ -\ 1.$$

*Example 4.7.* David Glynn [87] has further generalized this construction by observing that if $A$ and $B$ are the circulant incidence matrices of two projective planes of the same order and $C = AB - J$ is a $(0,1,-1)$ matrix, then $C$ is a circulant weighing matrix.

In the above example, $B$, of order 13, has Hall polynomial

$$\psi(x) = x^0 + x^1 + x^3 + x^9 ,$$

and

$$\psi(x^2) = x^0 + x^2 + x^5 + x^6 .$$

We can form the two inequivalent weighing matrices of order 13 by forming

$$B^2 - J \text{ and } AB^\top - J ,$$

where $A$ and $B^\top$ have Hall polynomials $\psi(x^2)$ and $\psi(x^{-1})$, respectively. Hence we obtain circulant weighing matrices with Hall polynomials

$$\alpha(x) = x^1 + x^3 + x^4 - x^7 - x^8 + x^9 + x^{10} - x^{11} - x^{12}$$

and

$$\beta(x) = x^2 + x^4 + x^5 + x^6 - x^7 - x^8 + x^{10} - x^{11} + x^{12}\,.$$

The first rows of the weighing matrices for $\alpha(x)$ and $\beta(x^2)$ are

$$0\ 1\ 0\ 1\ 1\ 0\ 0\ -\ -\ 1\ 1\ -\ 1$$

and

$$0\ -\ 0\ -\ 1\ 0\ 0\ 1\ 1\ -\ 1\ 1\ 1,$$

which are clearly inequivalent.

*Example 4.8 (Kovacs' second method).* (We refer the reader to Hughes and Piper [108] or Dembowski [40] for any unexplained terms in this and the next example.) $L_i = \{0+i, 1+i, 3+i, 9+i\}$ are the lines of a projective geometry. $L^2 = \{0,2,5,6\}$ is an oval with the property that any two of its translates $\{0+i, 2+i, 5+i, 6+i\}$ have precisely one point in common. We form a circulant matrix $W$ with first row $(a_{1j})$ by choosing

$$a_{1j} = |L_j \cap L^2| - 1\,.$$

Hence the first row of $W$ is

$$0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ -\ \ -\ \ 0\ \ 1\ \ -\ \ 1\ \ 0.$$

*Example 4.9 (Kovacs' first method–for q odd).* $(0,1,3,9)$ is a difference set modulo 13, so $L_i = \{0+i, 1+i, 3+i, 9+i\}$ are the lines of the projective geometry of order 3. Now $L_0^2 = \{0,2,5,6\}$ is an oval and, $L_j^2 = \{0+j, 2+j, 5+j, 6+j\}$ are also ovals, any two of which have precisely one common tangent. The tangents of $L_0^2$ are $L_0$, $L_1$, $L_3$ and $L_9$, so 1, 3, 4, 9, 10, 12 are exterior points, 0, 2, 5, 6 are on the oval, while 7, 8, 11 are interior to the oval.

We form our circulant weighing matrix by choosing the first row to have -1, 0, 1 in the $(0,i)$ position $(i = 0,1,\ldots,12)$ according as $i$ is interior on or exterior to the oval, i.e.,

$$\begin{array}{cccccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & - & - & 1 & 1 & - & 1 \end{array} \tag{4.1}$$

The translates of the oval $L_0^{-1} = \{0,4,10,12\}$ also satisfy the unique common tangent condition; from this oval, we get the first row

$$0\ \ 1\ \ -\ \ 1\ \ 0\ \ -\ \ -\ \ 1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0. \tag{4.2}$$

Map $i \mapsto -2i$; then 4.2 becomes

$$0\ -\ 0\ -\ 1\ 0\ 0\ 1\ 1\ -\ 1\ 1\ 1. \tag{4.3}$$

Now 4.1 and 4.3 are inequivalent.

*Remark 4.4.* Choosing $r = 2$ and $-1$ in the example gives inequivalent $W(13,9)$. It is interesting to consider what values of $r$ will give different solutions.

## 4.5 Constructions for Hadamard Matrices, $W(h,h)$, and Weighing Matrices, $W(h,h-1)$

**Definition 4.5.** A matrix $A = I + S$ will be called *skew-type* if $S^\top = -S$.

We recall the following:

**Definition 4.6.** A $(0,1,-1)$ matrix $W = W(p,k)$ of order $p$ satisfying

$$WW^\top = kI_p$$

is called a *weighing matrix of order* $p$ and *weight* $k$ or simply a *weighing matrix*. A $W(p,p)$ is called an *Hadamard matrix*. A $W = W(p,k)$ for which $W^\top = -W$ is called a *skew-weighing matrix*, and an Hadamard matrix $H = I + S$ for which $S^\top = -S$ is called a *skew-Hadamard matrix*. A $W = W(p,p-1)$ satisfying $W^\top = W$, $p \equiv 2 \pmod 4$ is called a *symmetric conference matrix*.

**Definition 4.7 ($C$-Matrix).** A $(0,\pm 1)$ matrix, $M$, will be called a *$C$-matrix* if $\frac{1}{2}(M \pm M^\top)$ is also a $(0,\pm 1)$ matrix.

*Remark 4.5.* To help the reader compare with other literature we note conference matrices ($M = M^\top$) and skew-Hadamard matrices ($M = -M^\top$) are also called $C$-matrices.

Weighing matrices have long been studied in order to find optimal solutions to the problem of weighing objects whose weights are small relative to the weights of the moving parts of the balance being used. It was shown by Raghavarao [163], [164] that if the variance of the errors in the weights obtained by individual weighings is $\sigma^2$ (it is assumed the balance is not biased and the errors are mutually independent and normal), then using a $W(p,k)$ to design an experiment to weigh $p$ objects will give a variance of $\frac{\sigma^2}{k}$. Indeed, for an Hadamard matrix the variance is $\frac{\sigma^2}{p}$, which is optimal for $p \equiv 0 \pmod 4$, and for a symmetric conference matrix the variance is $\frac{\sigma^2}{p-1}$, which is optimal for $p \equiv 2 \pmod 4$.

Sloane and Harwitt [195] survey the application of weighing matrices to improve the performance of optical instruments such as spectrometers.

Spectrometers measure the intensity of a dispersed spectrum at a finite number (n, say) of wavelengths. According to Ibbett, et al [112], either one detector scans the screen, making the $n$ measurements sequentially, or else the $n$ measurements are made simultaneously by a detector with spatial resolution. The first method has the disadvantage of not being able to compensate for variations in the intensity of the signal, while the second approach suffers the disadvantage of a lower signal-to-noise ratio (Ibbett, et al [112]).

A modification can be made to the second system which improves the signal-to-noise ratio. This is achieved by using a weighing matrix as square mask, where 1 is clear, 0 is opaque and $-1$ is a mirror (180° phase shift). Again the variance of the estimates of the wavelengths made using a mask of weight is $\frac{1}{n}$ of the estimates when measured separately.

Sloane and Harwitt [195] also indicate that weighing designs are applicable to other problems of measurements (such as lengths, voltages, resistances, concentrations of chemicals, etc.) in which the measure of several objects is the sum (or a linear combination) of the individual measurements.

The following properties of Hadamard matrices and weighing matrices are easily proved.

**Lemma 4.11.** *Let $U = U(p_1,k_1)$ and $V = V(p_2,k_2)$ be weighing matrices. Then $W = U \times V$ is a weighing matrix of order $p_1p_2$ and weight $k_1k_2$.*

**Corollary 4.8.** *Since $\left[\begin{smallmatrix} 1 & 1 \\ 1 & - \end{smallmatrix}\right]$ is a $W(2,2)$, there are Hadamard matrices of order $2^t$, $t$ a positive integer.*

**Lemma 4.12 (Paley Lemma or Paley Core).** *Let $p$ be a prime power. Then there is a $W = W(p+1,p)$ for which $W^\top = (-1)^{\frac{1}{2}(p-1)}W$. If $p \equiv 3 \pmod 4$, then $W + I_p$ is a $W(p+1,p+1)$.*

*Proof.* Let $a_0, a_1, \ldots, a_{p-1}$ be the elements of $GF(p)$ numbered so that

$$a_0 = 0, \quad a_{p-i} = -a_i, \quad i = 1, \ldots, p-1\,.$$

Define $Q = (x_{ij})$ by

$$x_{ij} = \chi(a_j - a_i) = \begin{cases} 0 & \text{if } i = j, \\ 1 & \text{if } a_j - a_i = y^2 \text{ for some } y \in GF(p), \\ -1 & \text{otherwise.} \end{cases}$$

Now $Q$ is a type 1 matrix with the properties that

$$\begin{aligned} QQ^\top &= pI - J, \\ QJ &= JQ = 0, \\ Q^\top &= (-1)^{\frac{1}{2}(p-1)}Q. \end{aligned}$$

This follows since exactly half of $a_1, \ldots, a_{p-1}$ are squares, $-1$ is a square for $p \equiv 1 \pmod 4$ but not for $p \equiv 3 \pmod 4$, and

$$\sum_y \chi(y)\chi(y+c) \;=\; \sum_y \chi\left(y^2\right)\chi\left(1+cy^{-1}\right) \;=\; \sum_{z\neq 1}\chi(x) \;=\; -1.$$

Let $e$ be the $1 \times p$ vector of all ones. Then

$$W = \begin{bmatrix} 0 & e \\ (-1)^{\frac{1}{2}(p-1)}e^\top & Q \end{bmatrix}$$

is the required matrix. If $p \equiv 3 \pmod 4$, $W + I_p$ is a $W(p+1, p+1)$. □

**Notation 4.2.** $Q$ is known as the *Paley core.*

**Corollary 4.9.** *There are Hadamard matrices of order $p+1$ where $p \equiv 3 \pmod 4$ is a prime power, and of order $2(p+1)$ where $p \equiv 1 \pmod 4$ is a prime power.*

*Proof.* For $p \equiv 3 \pmod 4$ use $W + I$; for $p \equiv 1 \pmod 4$ use $\begin{bmatrix} W+I & W-I \\ W-I & -W-I \end{bmatrix}$. □

**Corollary 4.10.** *There are Hadamard matrices of order $2^t \prod (p_i^{r_i} + 1)$ where $p_i^{r_i}$ are prime powers and $t$, an integer, is $> 0$ if $p_j^{r_j} \equiv 1 \pmod 4$, for some $j$, and $\geq 0$ otherwise.*

*Proof.* Use Lemma 4.11 and Corollary 4.10. □

It is conjectured that:

*Conjecture 4.1 (**Hadamard Conjecture**).* There exists an Hadamard matrix of order 4t for every positive integer $t$.

*Conjecture 4.2 (Jennifer Wallis [232]).* There exists a weighing matrix $W(4t, k)$, $k = 0, 1, \ldots, 4t$, for every positive integer $t$.

This conjecture, of course, includes the Hadamard Conjecture.

*Remark 4.6.* There is now considerable literature devoted to *circulant weighing matrices.* Some of the authors are Ang, Arasu, Hain, Mac, Ma, Mullin, Seberry and Strassler [6, 7, 9–11, 153, 201] . We do not pursue this topic, though extremely interesting, here.

**Definition 4.8.** We say that the weighing matrix $W = W(2n, k)$ is *constructed from two circulant matrices $M$, $N$* of order $n$ if

$$W = \begin{bmatrix} M & N \\ N^\top & -M^\top \end{bmatrix}.$$

*Example 4.10.*

$$M = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \qquad \text{and} \qquad N = \begin{bmatrix} - & 1 & 1 \\ 1 & - & 1 \\ 1 & 1 & - \end{bmatrix}$$

of order 3 satisfy $MM^\top + NN^\top = 5I$. Then

$$W = \begin{bmatrix} M & N \\ N^\top & -M^\top \end{bmatrix} = \left[\begin{array}{ccc|ccc} 0 & 1 & 1 & - & 1 & 1 \\ 1 & 0 & 1 & 1 & - & 1 \\ 1 & 1 & 0 & 1 & 1 & - \\ \hline - & 1 & 1 & 0 & - & - \\ 1 & - & 1 & - & 0 & - \\ 1 & 1 & - & - & - & 0 \end{array}\right]$$

is a $W(6,5)$ constructed from two circulant matrices.

**Theorem 4.7 (Goethals and Seidel [88]).** *Let $q \equiv 1 \pmod 4$ be a prime power; then there is a $W(q+1,q)$ of the form*

$$S = \begin{bmatrix} A & B \\ B & -A \end{bmatrix}$$

*with zero diagonal and square circulant sub-matrices $A$ and $B$.*

*Proof.* Let $z$ be any primitive element of $GF(q^2)$, the quadratic extension of $GF(q)$. We choose any basis of $V$ the vector space of dimension 2 over $GF(q^2)$. With respect to this basis, $v$ is defined by the matrix

$$(v) - \tfrac{1}{2} \begin{bmatrix} z^{q-1} + z^{1-q} & (z^{q-1} - z^{1-q}) z^{\frac{1}{2}(q+1)} \\ (z^{q-1} - z^{1-q}) z^{-\frac{1}{2}(q+1)} & z^{q-1} + z^{1-q} \end{bmatrix},$$

which actually has its elements in $GF(q)$. Then $\det(v) = 1$, and the eigenvalues of $v$ are $z^{q-1}$ and $z^{1-q}$, both elements of $GF(q^2)$ whose $\frac{1}{2}(q+1)$-th power, and no smaller, belongs to $GF(q)$. Hence $v$ acts on the projective line $PG(1,q)$ as a permutation with period $\frac{1}{2}(q+1)$ without fixed points. This divides the points of $PG(1,q)$ into two sets of transitivity, each containing $\frac{1}{2}(q+1)$ points. In addition, $w$ defined by the matrix

$$(w) = \begin{bmatrix} 0 & z^{q+1} \\ 1 & 0 \end{bmatrix}$$

has $\chi \det(w) = -\chi(-1)$. The eigenvalues of $w$ are $\pm z^{\frac{1}{2}(q+1)}$ elements of $GF(q^2)$ whose square is in $GF(q)$. Hence $w$ acts on $PG(1,q)$ as a permutation of period 2, which maps any point of one set of transitivity, defined above by $v$, into the other set. Indeed, for $i = 1, \ldots, \frac{1}{2}(q+1)$, the mapping $v^i w$ has no eigenvalue in $GF(q)$. Note $vw = wv$.

Finally, we represent the $q+1$ points of $PG(1,q)$, $x_0, x_1, \ldots, x_q$, by the following $q+1$ vectors in $V$:

$$x, v(x), v^2(x), \ldots, v^{\frac{1}{2}(q-1)}(x), w(x), vw(x), \ldots, v^{\frac{1}{2}(q-1)}w(x).$$

We define

$$S = \chi \det(x_i, x_j).$$

Observing that any linear mapping $u\colon V \to V$ satisfies

$$\det(u(x), u(y)) = \det u \cdot det(x, y),$$

for all $x, y \in V$, we see that

$$\det(v^i w(x), v^j w(x)) = \det(w) \cdot \det(v^i(x), v^j(x)) = \det(w) \cdot \det(x, v^{j-i}(x)),$$
$$\det(v^i(x), v^j w(x)) = -\det(v^i w(x), v^j(x)) = \det(v^j(x), v^i w(x)),$$
$$\det(v^i(x), v^j(x)) = -\det(v^{\frac{1}{2}(q+1)+i}, v^j(x)),$$

and so $S$ has the required form. □

*Example 4.11.* Let $q = 5$ and $z$ be a root of $z^2 + z + 2 = 0$ (a primitive polynomial over $GF(5^2)$). Then

$$z^4 = 3z+2, \quad z^{-4} = z^{20} = 2z+4, \quad z^3 = 4z+2, \quad z^{-3} = z^{21} = 2z+1, \quad z^6 = 2.$$

Hence

$$(v) = \tfrac{1}{2}\begin{bmatrix} z^4 + z^{-4} & (z^4 - z^{-4})z^3 \\ (z^4 - z^{-4})z^{-3} & z^4 + z^{-4} \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix}$$

and

$$(w) = \begin{bmatrix} 0 & z^6 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}.$$

We now choose some vector $x$, say, $x = \left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$. Then

$$x_0 = x = \left[\begin{smallmatrix}1\\0\end{smallmatrix}\right], \quad x_1 = v(x) = \left[\begin{smallmatrix}3\\2\end{smallmatrix}\right], \quad x_3 = v^2(x) = \left[\begin{smallmatrix}2\\2\end{smallmatrix}\right],$$
$$x_4 = w(x) = \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right], \quad x_5 = vw(x) = \left[\begin{smallmatrix}4\\3\end{smallmatrix}\right], \quad x_6 = v^2 w(x) = \left[\begin{smallmatrix}4\\2\end{smallmatrix}\right].$$

Since $\chi(1) = \chi(4) = 1$ and $\chi(2) = \chi(3) = -1$,

$$\det(x_i, x_j) = \left[\begin{array}{ccc|ccc} 0 & 2 & 2 & 1 & 3 & 2 \\ 3 & 0 & 2 & 3 & 1 & 3 \\ 3 & 3 & 0 & 2 & 3 & 1 \\ \hline 4 & 2 & 3 & 0 & 1 & 1 \\ 2 & 4 & 2 & 4 & 0 & 1 \\ 3 & 2 & 4 & 4 & 4 & 0 \end{array}\right] \text{ and } \chi\det(x_i x_j) = \left[\begin{array}{ccc|ccc} 0 & - & - & 1 & - & - \\ - & 0 & - & - & 1 & - \\ - & - & 0 & - & - & 1 \\ 1 & - & - & 0 & 1 & 1 \\ - & - & 1 & 1 & 1 & 0 \end{array}\right].$$

The next corollary was first explicitly stated by Turyn.

**Corollary 4.11 (Turyn [218]).** *Let $p \equiv 1 \pmod 4$ be a prime power. Then there exist four circulant symmetric matrices*

$$X_1 = I + A, \quad X_2 = I - A, \quad X_3 = X_4 = B$$

*of order $\frac{1}{2}(p+1)$ which satisfy*

$$\sum_{i=1}^{4} X_i X_i^\top = 2(p+1) I_{\frac{1}{2}(p+1)}\,.$$

These four matrices will be called *Williamson matrices* as they are circulant and symmetric.

*Proof.* Construct $A$ and $B$ as in the theorem. □

Note that the next four matrices satisfy the additive property but are not circulant but pairwise amicable, so are called *Williamson type matrices* (see Definition 4.16).

**Corollary 4.12 (J. Wallis [235]).** *Let $p \equiv 1 \pmod 4$ be a prime power; then there exist four symmetric $(1,-1)$ matrices $X_1$, $X_2$, $X_3$, $X_4$ of order $\frac{1}{2}p(p+1)$ which satisfy*

$$\sum_{i=1}^{4} X_i X_i^\top = 2p(p+1) I_{\frac{1}{2}p(p+1)}, \quad X_i X_j^\top = X_j X_i^\top\,.$$

*Equivalently, there are Williamson type matrices of order $\frac{1}{2}p(p+1)$.*

*Proof.* Construct $A$ and $B$ as in the theorem, and $Q$ of order $p$ as in the proof of Lemma 4.12. Then

$$\begin{aligned} X_1 &= (I \times J) + (A \times (I+Q))\,,\\ X_2 &= B \times (I+Q)\,,\\ X_3 &= (I \times J) + (A \times (I-Q))\,,\\ X_4 &= B \times (I-Q) \end{aligned}$$

are the required matrices. These type 1 matrices are symmetric. □

There are two very tough problems concerning skew Hadamard matrices. The first being the existence and construction of such matrices, the second being the number of equivalence classes. Existence results fall into two types: those constructed using four suitable complementary sequences and those constructed using linear algebra and number theory. Although the existence problem, via algebraic and number theoretic methods, has been widely studied by many researchers including Spence, Whiteman and Yamada, there many orders for which skew Hadamard matrices have not been constructed yet

(indeed there is no asymptotic existence theorem known for skew Hadamard matrices, see Chapter 9.)

*Good matrices*, which are four circulant $\pm 1$ matrices of order $n$, constructed using four suitable complementary sequences and used in the Goethals-Seidel array to construct skew Hadamard matrices of smaller order $4n$ (orders $\leq 400$), first appeared in the PhD Thesis of Jennifer (Seberry) Wallis [240]: there the matrices were given no name. Extensive computer searches have been carried out by many authors including Blatt, Đoković, Fletcher, Georgiou, Goethals, Hunt, Kotserias, Koukouvinos, Seberry, W. D. Smith, Seidel, Stylianou, Szekeres and X-M Zhang (also K. Balasubramanian in chemistry) see, for example, [24, 41, 42, 61].

In [240] good matrices were given for $n = 1, \cdots, 15, 19$ and in [229] for $n = 23$. Hunt [109] gave the matrices for $n = 1, \cdots, 25$. Later Szekeres [206] gave a list for orders $n = 1, \cdots, 31$. Đoković [42, 45] provided orders $n = 33$, 35, 43, 47, 97 and 127. Then Georgiou, Koukouvinos and Stylianou [74] provided 37, 39. Đoković [47] says that only one set of supplementary difference sets, (41;20,20,16,16;31), for 41 remains to be searched. Fletcher, Koukouvinos and Seberry [61] provided order 59.

We note that while there are no Williamson matrices of order 35 and 59 there are good matrices of order 35 and 59. [178, 236].

These results are summarised (partly) in part SV of the table of existence theorems. Suitable complementary sequences have not yet been found for orders 69 and 89 (however skew Hadamard matrices are known for orders $8 \times 69$ and $16 \times 89$ by algebraic methods).

**Summary 4.1.** Table 4.4 summarizes the existence of skew-Hadamard matrices.

The more recent status on known results and open problems on the existence of skew-Hadamard matrices of order $2^t n$, $n$ odd, $n \leq 500$, are given in Table 1 of [138]. In Table 4.5, we write $n(t)$ if the skew-Hadamard matrix of order $2^t n$ exists. An $n(.)$ means that a skew-Hadamard matrix of order $2^t n$ is not yet known for any $t$. The values $n < 500$, missing from Table 4.5, indicate that a skew-Hadamard matrix of order $4n$ exists. Seberry Wallis [230] conjectured that skew-Hadamard matrices exist for all dimensions divisible by 4.

Table 4.5 modifies that of Koukouvinos and Stylianou [138] with more recent results.

Table 4.6 gives the current knowledge of existence for Hadamard matrices not in Geramita-Seberry [80, p.416], nor in Seberry-Yamada [188, p.543-544] which are unresolved.

**Table 4.4** Skew-Hadamard existence

| | | |
|---|---|---|
| $SI$ | $2^t \prod k_i$ | $t$, $r_i$, all positive integers $k_i = p_i^{r_i} + 1 \equiv 0 \pmod 4$, $p_i$ a prime. |
| $SII$ | $(p-1)^u + 1$ | $p$ the order of a skew-Hadamard matrix, $u > 0$ an odd integer. |
| $SIII$ | $2(q+1)$ | $q \equiv 5 \pmod 8$ a prime power. |
| $SIV$ | $2^s(q+1)$ | $q = p^t$ is a prime power such that $p \equiv 5 \pmod 8$, $t \equiv 2 \pmod 4$, $s \geq 1$ an integer. |
| $SV$ | $4m$ | $m \in \{$odd integers between 3 and 39 inclusive$\}$ |
| $SVI$ | $m'(m'-1)(m-1)$ | $m$ and $m'$ the orders of amicable Hadamard matrices, where $(m-1)\frac{m'}{m}$ is the order of a skew-Hadamard matrix. |
| $SVII$ | $4(q+1)$ | $q = 8f+1$ $f$ odd is a prime power. |
| $SVIII$ | $(\lvert t\rvert+1)(q+1)$ | $q = s^2 + 4t^2 \equiv 5 \pmod 8$ is a prime power, and $\lvert t\rvert+1$ is the order of a skew-Hadamard matrix (Wallis [234]). |
| $SIX$ | $4(1+q+q^2)$ | where $q$ is a prime power and $\begin{cases} 1+q+q^2 & \text{is a prime } \equiv 3,5, \text{ or } 7 \pmod 8; \text{ or} \\ 3+2q+2q^2 & \text{is a prime power ( [197]).} \end{cases}$ |
| $SX$ | $hm$ | $h$ the order of a skew-Hadamard matrix, $m$ the order of amicable Hadamard matrices. |

## 4.6 The Goethals-Seidel Array and other constructions using circulant matrices – constraints on constructions using circulant matrices

In studying skew-Hadamard matrices (orthogonal designs $OD(n;1,n-1)$), Szekeres realized that none were known for quite small orders, including 36. To find this matrix Goethals and Seidel gave an array (described in this section) which uses circulant matrices. This and its generalization by Wallis and Whiteman have proved invaluable in the construction of Hadamard matrices, and we will see that they play a major role in constructing orthogonal designs. Here we have another example of a method devised to give a single case having far-reaching uses.

We now consider the use of circulant matrices in constructing orthogonal designs. All the constructions using circulants require that we find circulants $A_1, \ldots, A_s$ of order $n$ satisfying the additive property:

**Table 4.5** Existence of skew-Hadamard matrices [a]

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 69(3) | 89(4) | | | | | | |
| 101(10) | 107(10) | 119(4) | 149(4) | | | | |
| 153(3) | 167(4) | 177(12) | 179(8) | 191(.) | 193(3) | | |
| 201(3) | 205(3) | 209(4) | 213(4) | 223(3) | 225(4) | 229(3) | 233(4) |
| 235(3) | 239(4) | 245(4) | 249(4) | 251(6) | 253(4) | 257(4) | 259(5) |
| 261(3) | 265(4) | 269(8) | 275(4) | 277(5) | 283(11) | 285(3) | 287(4) |
| 289(3) | 295(5) | 299(4) | | | | | |
| 301(3) | 303(3) | 305(4) | 309(3) | 311(26) | 317(6) | 319(3) | 325(5) |
| 329(6) | 331(3) | 335(7) | 337(18) | 341(4) | 343(6) | 345(4) | 347(18) |
| 349(3) | 353(4) | 359(4) | 361(3) | 369(4) | 373(7) | 377(6) | 385(3) |
| 389(15) | 391(4) | 397(5) | | | | | |
| 401(10) | 403(5) | 409(3) | 413(4) | 419(4) | 423(4) | 429(3) | 433(3) |
| 435(4) | 441(3) | 443(6) | 445(3) | 449(.) | 451(3) | 455(4) | 457(9) |
| 459(3) | 461(17) | 465(3) | 469(3) | 473(5) | 475(4) | 479(12) | 481(3) |
| 485(4) | 487(5) | 489(3) | 491(46) | 493(3) | | | |

[a] Koukouvinos and Stylianou [138, p2728] © Elsevier

**Table 4.6** Hadamard matrix orders which are unresolved

| | | | | | | |
|---|---|---|---|---|---|---|
| 107(10) | 167(3) | 179(3) | 191(3) | | | |
| 213(4) | 223(3) | 239(4) | 249(3) | 251(3) | 269(8) | 283(3) |
| 303(3) | 311(26) | 335(7) | 347(3) | 359(4) | 373(7) | |
| 419(4) | 443(6) | 445(3) | 479(12) | 487(3) | 491(46) | |

$$\sum_{i=1}^{s} A_i A_i^{\top} = fI, \text{ where } f = \sum_{j=1}^{r} s_j x_j^2 .$$

One question we shall explore in this section is the restrictions that must be placed on $(s_1, \ldots, s_r)$ in order that such circulant matrices exist.

This problem is analogous to the problems we discussed in Chapter 3 when we discovered algebraic limitations on orthogonal designs.

Conditions imposed on $(s_1, \ldots, s_r)$ in order to construct orthogonal designs from circulants is closer to the combinatorial spirit of the subject. Although there is no reason to believe that all the orthogonal designs we look for in orders $4n$ or $8n$, $n$ odd, can be expected to come from circulants (or negacyclics), we will find they usually do. In cases where they do not, especially in orders divisible by 8, negacyclic matrices have proved invaluable. See [67, 68, 78, 101, 105,108,126] among others. Thus circulant matrices are important constructive tools, and we should decide what limitations there are on their use. We also note that circulant matrices are amenable to algebraic assault because of their

relationship to roots of unity. This aspect to circulants will become more apparent when we discuss Griffin' s work on Golay sequences in Section 7.2.

We first give constructions using circulants and then consider restrictions on their use.

**Proposition 4.1.** *Suppose there exist two circulant matrices $B$ of order $n$ satisfying*

$$AA^\top + BB^\top = fI_n\,.$$

*Further suppose that $R$ is the back diagonal matrix; then*

$$H = \begin{bmatrix} A & B \\ -B^\top & A^\top \end{bmatrix} \text{ or } G = \begin{bmatrix} A & BR \\ -BR & A \end{bmatrix} \text{ is a } W(2n, f)\,,$$

*when $A$, $B$ are $(0,1,-1)$ matrices, and an orthogonal design $OD(2n; u_1, u_2, \ldots, u_s)$ on $x_1, \ldots, x_s$ when $f = \sum_{i=1}^{s} u_i x_i^2$.*

*Further, $H$ and $G$ are skew or skew-type if $A$ is skew or skew-type.*

*Proof.* A straightforward verification. □

*Remark 4.7.* We note here that these properties remain true if $A$ and $B$ are type 1 matrices and $R$ is the appropriately chosen matrix (see Lemmas 4.4 to 4.7).

**Definition 4.9.** We say that an orthogonal design is *constructed from two circulant matrices $M$, $N$* of order $n$ if

$$W = \begin{bmatrix} M & N \\ -N^\top & M^\top \end{bmatrix} \quad \text{or} \quad W = \begin{bmatrix} M & NR \\ -NR & M \end{bmatrix}.$$

*Example 4.12.*

$$A = \begin{bmatrix} x_l & x_2 & -x_2 \\ -x_2 & x_1 & x_2 \\ x_2 & -x_2 & x_1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & x_2 & x_2 \\ x_2 & 0 & x_2 \\ x_2 & x_2 & 0 \end{bmatrix}$$

of order 3 satisfy

$$AA^\top + BB^\top = (x_1^2 + 4x_2^2)I\,.$$

Thus

$$H = \begin{bmatrix} A & B \\ -B^\top & A^\top \end{bmatrix} = \left[\begin{array}{ccc|ccc} x_1 & x_2 & -x_2 & 0 & x_2 & x_2 \\ -x_2 & x_1 & x_2 & x_2 & 0 & x_2 \\ x_2 & -x_2 & x_1 & x_2 & x_2 & 0 \\ \hline 0 & -x_2 & -x_2 & x_1 & -x_2 & x_2 \\ -x_2 & 0 & -x_2 & x_2 & x_1 & -x_2 \\ -x_2 & -x_2 & 0 & -x_2 & x_2 & x_1 \end{array}\right]$$

and

$$G = \begin{bmatrix} A & BR \\ -BR & A \end{bmatrix} = \left[\begin{array}{ccc|ccc} x_1 & x_2 & -x_2 & 0 & x_2 & x_2 \\ -x_2 & x_1 & x_2 & x_2 & x_2 & 0 \\ x_2 & -x_2 & x_1 & x_2 & 0 & x_2 \\ \hline 0 & -x_2 & -x_2 & x_1 & x_2 & -x_2 \\ -x_2 & -x_2 & 0 & -x_2 & x_1 & x_2 \\ -x_2 & 0 & -x_2 & x_2 & -x_2 & x_1 \end{array}\right]$$

are orthogonal designs $OD(6;1,4)$ on $x_1, x_2$. $H$ and $G$ are constructed from two circulants.

**Theorem 4.8 (Goethals-Seidel [89]).** *Suppose there exist four circulant matrices $A$, $B$, $C$, $D$ of order $n$ satisfying*

$$AA^\top + BB^\top + CC^\top + DD^\top = fI_n\,.$$

*Let $R$ be the back diagonal matrix. Then $GS$, henceforth called the Goethals-Seidel array,*

$$GS = \begin{bmatrix} A & BR & CR & DR \\ -BR & A & D^\top R & -C^\top R \\ -CR & -D^\top R & A & B^\top R \\ -DR & C^\top R & -B^\top R & A \end{bmatrix}$$

*is a $W(4n,f)$ when $A$, $B$, $C$, $D$ are $(0,1,-1)$ matrices, and an orthogonal design $OD(4n;u_1,u_2,\ldots,u_s)$ on the variables $(x_1,x_2,\ldots,x_s)$ when $A$, $B$, $C$, $D$ have entries from $\{0,\pm x_1,\ldots,\pm x_s\}$ and*

$$f = \sum_{j=1}^{s} u_j x_j^2\,.$$

*Further, $GS$ is skew or skew-type if $A$ is skew or skew-type.*

This theorem was modified by Wallis and Whiteman to allow the circulant matrices to be generalized to types 1 and 2.

**Lemma 4.13 (Wallis-Whiteman [242]).** *Let $A$, $B$, $D$ be type 1 matrices and $C$ a type 2 matrix defined on the same abelian group of order $n$. Then if*

$$AA^\top + BB^\top + CC^\top + DD^\top = fI_n\,,$$
$$H = \begin{bmatrix} A & B & C & D \\ -B^\top & A^\top & -D & C \\ -C & D^\top & A & -B^\top \\ -D^\top & -C & B & A^\top \end{bmatrix}$$

*is a $W(4n,f)$ when $A$, $B$, $C$, $D$ are $(0,1,-1)$ matrices, and an orthogonal design $OD(4n;u_1,u_2,\ldots,u_s)$ on the commuting variables $(x_1,x_2,\ldots,x_s)$ when $A$, $B$, $C$, $D$ have entries from $0,\pm x_1,\ldots,\pm x_s$ and*

$$f = \sum_{j=1}^{s} u_j x_j^2 .$$

*Further, $H$ is skew or skew-type if $A$ is skew or skew-type.*

*Example 4.13.* We construct an orthogonal design $OD(12;3,3,3,3)$ in order 12 by using the circulant matrices with first rows, respectively,

$$abc, \qquad \bar{b}ad, \qquad \bar{c}\bar{d}a, \qquad \bar{d}c\bar{b},$$

in the Goethals-Seidel array (Theorem 4.8). This is illustrated in Table 4.15. See also Example 4.21. □

To illustrate the use of Lemma 4.13 recall that in Example 4.3 we gave a type 1 matrix $A$ and a type 2 matrix $B$ defined on the additive group $G$ of $GF(3^2)$ ($G = Z_3 \times Z_3$). Let $R$ be the matrix defined on $G$ by Lemma 4.7. Notice that by Lemma 4.7 $AR = B$ and $BR = A$. Also, $R$ is a type 2 matrix.

Let $W = \begin{bmatrix} 0 & I_3 & 0 \\ 0 & 0 & I_3 \\ I_3 & 0 & 0 \end{bmatrix}$; then $W$ is the type 1 $(1,0)$ incidence matrix generated by $\{2x\}$ (we are using the notation of Example 4.3).

Let $L = \begin{bmatrix} J_3 & 0 & 0 \\ 0 & J_3 & 0 \\ 0 & 0 & J_3 \end{bmatrix}$; then $L$ is the type 1 $(1,0)$ incidence matrix generated by the subgroup $\{0,1,2\}$ of $G$. Since the identity matrix is always a type 1 matrix for a group $G$ (for which the identity element of the group is the first element of $G$), we obtain that $U = L - I + W$ and $V = I + W^\top$ are type 1 matrices on $G$. (See Lemma 4.5.)

Set $X_1 = aI + bA$, $X_2 = b(U+V)$, $X_4 = b(U-V)$ and $X_3 = bB - aR$. Then $X_1$, $X_2$ and $X_4$ are type 1 matrices and $X_3$ is a type 2 matrix. By inspection, all entries are from $0, \pm a, \pm b$. Also

$$\sum_{i=1}^{4} X_i X_i^\top = (2a^2 + 26b^2) I_9 .$$

Thus these matrices may be used in place of $A$, $B$, $C$, $D$ in Lemma 4.13 to give an $OD(36;2,26)$.

The most general theorem we can give on using circulant matrices in the construction of orthogonal designs is

**Theorem 4.9.** *Suppose there is an orthogonal design $OD(m;u_1,u_2,\ldots,u_s)$ on the variables $x_1,x_2,\ldots,x_s$. Let $X_1,X_2,\ldots,X_s$, where $s \le \rho(n)$, be circulant (type 1) matrices of order $n$ with entries from $\{0,\pm y_1,\ldots,\pm y_r\}$ which satisfy*

$$u_1 X_1 X_1^\top + u_2 X_2 X_2^\top + \cdots + u_s X_s X_s^\top = f I_n$$

*(the additive property). Further suppose*

1. *all $X_i$ are symmetric, or*

*2. at most one is not symmetric, or*
*3. $X_1,\ldots,X_{j-1}$ are symmetric and $X_j,\ldots,X_s$ are skew-symmetric.*

*Then if $f = v_1y_1^2 + v_2y_2^2 + \cdots + v_ry_r^2$, there is an $OD(mn;v_1,v_2,\ldots,v_r)$ on the commuting variables $(y_l,y_2,\ldots,y_r)$.*

*Proof.* The main difficulty arises because the variables of the orthogonal design are commutative. When we replace commuting variables by matrices $y_i$, $i = 1,\ldots,s$, we have to ensure that the matrices pairwise satisfy

$$Y_iY_j^\top = Y_jY_i^\top \tag{4.4}$$

We established in Section 2 that if the $Y_i$ are circulant and symmetric, equation (4.4) is satisfied. Also if $Y_iR$ is back circulant (type 2) and $Y$ is circulant (type 1), then equation (4.4) is satisfied. We also note that if $Y_i$ and $Y_j$ are skew-symmetric, the back circulant matrices $Y_iR$ and $Y_jR$ satisfy equation (4.4) since

$$(Y_iR)(Y_jR)^\top = Y_iRR^\top Y_j^\top = -Y_iY_j = Y_jY_i^\top = (Y_jR)(Y_iR)^\top.$$

Thus the result can be obtained in the first case by replacing each variable $x_i$, $i \neq j$, in the orthogonal design of order $m$ by the circulant symmetric matrix $X_i$; in the second case the variable $x_i$ is replaced by the back circulant matrix $X_jR$. The third result is obtained by replacing $x_i$, $i \neq j$, $j+1,\ldots,s$, by $X_i$, and $x_j,\ldots,x_s$ by $X_jR,\ldots,X_sR$. □

*Example 4.14.* There is an orthogonal design $OD(16;1,1,1,1,3,3,3,3)$ (we will see this in Chapter 5, Example 6.4(c)). Consider the circulant matrices $X_i$, with first rows

$$\begin{array}{llll} y_1y_2y_2\bar{y}_2\bar{y}_2 & y_2\bar{y}_2y_2y_2\bar{y}_2 & \bar{y}_2y_2y_2y_2y_2 & \bar{y}_2y_2y_2y_2y_2 \\ y_3y_4\bar{y}_4\bar{y}_4y_4 & \bar{y}_4y_3\bar{y}_3\bar{y}_3y_3 & \bar{y}_3y_3y_3y_3y_3 & \bar{y}_4y_4y_4y_4y_4 \end{array}$$

and call them respectively $X_1,\ldots,X_8$. Then

$$X_1X_1^\top + X_2X_2^\top + X_3X_3^\top + X_4X_4^\top + 3X_5X_5^\top + 3X_6X_6^\top + 3X_7X_7^\top + 3X_8X_8^\top = (y_1^2 + 19y_2^2 + 30y_3^2 + 30y_4^2)I_5.$$

We use part 2 of Theorem 4.9 to assert the existence of an orthogonal design $OD(80;1,19,30,30)$; the matrix $X_1R$ is used to replace the first variable, and the circulant symmetric matrices $X_2,\ldots,X_8$ are used to replace the other variables.

We have noted that in Theorem 4.8 the only requirement was to have circulant matrices, but in Theorem 4.9 the internal structure of the circulant matrices was restricted severely. If the matrices are circulant and symmetric, we will loosely call this *Williamson criteria*, and if merely circulant, we will

call this *Goethals-Seidel criteria*. Thus in Theorem 4.8 we only had Goethals-Seidel criteria operating, but in Theorem 4.9 we were almost entirely limited to Williamson criteria.

## 4.7 Constraints on construction using circulant matrices

Of course we would like to use these constructions to form orthogonal designs, but first we must consider some combinatorial limitations on these methods (algebraic limitations on the types of orthogonal designs were discussed earlier).

**Lemma 4.14.** *Let $A_i$, $i = 1, 2, 3, \ldots, m$, be circulant matrices of order $n$ where*

$$\sum_{i=1}^{m} A_i A_i^\top = \left( \sum_{j=1}^{r} s_j x_j^2 \right) I_n \,.$$

*Suppose $A_i = \sum_{j=1}^{r} x_j A_{ij}$ and that $A_{ij} J = y_{ij} J$. Then*

$$s_j = \sum_{j=1}^{m} y_{ij}^2 \,.$$

*Proof.* By definition

$$\sum_{i=1}^{m} (x_1 A_{i1} + x_2 A_{i2} + \ldots) \left( x_1 A_{i1}^\top + x_2 A_{i2}^\top + \ldots \right) = \left( s_1 x_1^2 + s_2 x_2^2 + \ldots \right) I \,.$$

So

$$\sum_{i=1}^{m} x_1^2 \left( A_{i1} \right) A_{i1}^\top + \sum_{i=1}^{m} x_2^2 \left( A_{i2} A_{i2}^\top \right) + \cdots = \left( s_1 x_1^2 + s_2 x_2^2 + \ldots \right) I \,,$$

and setting $x_j = 1$, $x_i = 0$, for $i \neq j$ we have

$$\sum_{i=1}^{m} A_{ij} A_{ij}^\top = s_j \,.$$

Post-multiplying by $J$ gives

$$\sum_{i=1}^{m} y_{ij}^2 J = s_j J \,,$$

and equating coefficients gives the results. □

*Remark 4.8.* If $m = 4$ and we have four circulants $A_1, A_2, A_3, A_4$ such that

$$\sum_{i=1}^{4} A_i A_i^\top = \left(x_1^2 + s x_2^2\right) I_n \,,$$

$n$ odd, then $s$ must be the sum of three squares. For we may assume $A_1 = x_1 I + x_2 A_{12}$, $A_2 = x_2 A_{22}$, $A_3 = x_2 A_{32}$ and $A_4 = x_2 A_{42}$. Then by the lemma we have

$$y_{12}^2 + y_{22}^2 + y_{32}^2 + y_{42}^2 = s \,.$$

But $A_{12} = -A_{l2}^\top$, and the order of $A_{12}$ is $n$(odd). So $y_{12} = 0$, and consequently $s$ is the sum of three squares. This should be compared with Proposition 3.21.

## 4.8 Eades' Technique for Constructing Orthogonal Designs Using Circulant Matrices

The method outlined in this section has been used successfully to compute four variable orthogonal designs of order 20 and many but not all orthogonal designs of order 28, 36 and 44. Some success has been achieved with orthogonal designs of orders 18, 22, 26, 30, 44 and 52. The results of this computation are included in the the Appendices. The method can be extended to construct orthogonal designs in orders 24, 48, 56 and 72.

The method is presented as it applies to the Goethals-Seidel construction (Theorem 4.8), but there are no difficulties in extending the results for more general circulant constructions, such as those mentioned in orders 48 and 56 (see appendices).

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

$$\sum_{i=1}^{4} X_i X_i^\top = \left(\sum_{i=1}^{u} s_i x_i^2\right) I \,. \tag{4.5}$$

The existence of an orthogonal design $OD(4v; s_1, s_2, \ldots, s_u)$ follows from the Goethals-Seidel construction (Theorem 4.8).

*Remark 4.9.* The restriction that $v$ is odd is not necessary for most of the results which follow. However, the restriction is made because we are principally interested here in constructing orthogonal designs of order not divisible by 8. Orthogonal designs of order divisible by a large power of 2 can often be constructed using other methods (see Chapter 9).

Equation (4.5) has $v^2$ components, but since $X_i X_i^\top$ is circulant and symmetric, at most $\frac{1}{2}(v+1)$ of these components are independent. The next two definitions are made to isolate the independent components.

**Definition 4.10.** If $A_1, A_2, A_3, A_4$ are $v \times v$ circulant matrices with entries from $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ and the first row of $A_j$ has $m_{ij}$ entries of the kind $\pm x_i$, then the $u \times 4$ matrix $M = (m_{ij})$ is called the *entry matrix* of $(A_1, A_2, A_3, A_4)$.

**Definition 4.11.** Suppose that $A$ is a $v \times v$ circulant matrix with rows $r_1, r_2, \ldots r_v$, and denote $\frac{1}{2}(v-1)$ by $w$. Then the *IPV (Inner Product Vector) of* $A$ is $[r_1 r_2^\top, r_1 r_3^\top, \ldots, r_1 r_w^\top]$. Note that if $(d_1, d_2, \ldots, d_v)$ is the first row of $AA^\top$, then the IPV of $A$ is $(d_2, d_3, \ldots, d_w)$.

It is clear that $(X_1, X_2, X_3, X_4) = (A_1, A_2, A_3, A_4)$ is a solution of equation (4.5) if and only if

$$\sum_{j=1}^{4} m_{ij} = s_i \quad \text{for } 1 \le i \le u\,, \tag{4.6}$$

and

$$\sum_{j=1}^{4} b_j = 0, \quad \text{where } b_j \text{ is the IPV of } A_j\,. \tag{4.7}$$

In other words, to find a solution of equation (4.5) we need four circulant matrices with entries from $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ whose entry matrix has $i^{\text{th}}$ row adding to $s_i$ for $1 \le i \le u$ and whose IPV's add to zero.

*Remark 4.10.* The IPV is not the most efficient way in time or space to construct Hadamard matrices, but is valuable for orthogonal designs.

**Definition 4.12.** The *content* of a circulant matrix $A$ with entries from $\{0, \pm x_1, \pm x_2, \ldots, x_u\}$ is the set of pairs $(\epsilon x_i, m)$ where $\epsilon x_i (\epsilon = \pm 1)$ occurs a non-zero number $m$ times in the first row of $A$. Our next task is to show how the contents of solutions of equation (4.5) may be determined from the knowledge of the parameters $v, s_1, s_2, \ldots, s_u$.

**Definition 4.13.** Suppose that the rowsum of $A_j$ is $\sum_{i=1}^{u} p_{ij} x_j$ for $1 \le j \le 4$. Then the $u \times 4$ integral matrix $P = (p_{ij})$ is called the *sum matrix* of $(A_1, A_2, A_3, A_4)$. The *fill matrix* of $(A_1, A_2, A_3, A_4)$ is $M - abs(P)$. The content of $A_i$ is determined by the $i$-th columns of the sum and fill matrices.

The following theorem may be used to find the sum matrix of a solution of equation (4.5).

**Theorem 4.10 (Eades Sum Matrix Theorem [52]).** *The sum matrix $P$ of a solution of equation* (4.5) *satisfies*

$$PP^\top = diag(s_1, s_2, \ldots, s_u). \tag{4.8}$$

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

$$(JA)(A^\top J^\top) = a^2 JJ^\top = a^2 vJ\,.$$

But also

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

Hence $a^2 = b+2c$. Thus if $(p_{ij})$ and $(m_{ij})$ are the sum and entry matrices of a solution of equation (4.5), then since the sum of the sums of the entries of the IPV's is zero, it follows that

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

Expanding this equation and equating coefficients of $x_i x_j$ gives equation (4.8). □

*Remark 4.11.* (a) Note that the Sum Matrix Theorem 4.10 implies that a necessary condition for the existence of $OD(4v; s_l, s_2, \ldots, s_u)$ constructed by using the Goethals-Seidel array is the existence of a $u \times 4$ integral matrix $P$ satisfying equation (4.8). In fact this theorem says that the only time we can hope to construct an orthogonal design $OD(n; s_1, s_2, s_3, s_4)$ using the Goethals-Seidel array in order $n \equiv 0 \pmod 4$ is when there is a $4 \times 4$ integer matrix $p$ such that $PP^\top = diag(s_1, s_2, s_3, s_4)$. This is analogous to Proposition 3.23 of Chapter 3, which says that in orders $n \equiv 4 \pmod 8$ a rational family of type $[s_1, s_2, s_3, s_4]$ exists in order $n$ if and only if there is a $4 \times 4$ *rational* matrix $Q$ with $QQ^\top = diag(s_1, s_2, s_3, s_4)$. This also shows that, for four variable designs, the Goethals-Seidel approach will be less useful in orders divisible by a large power of 2.

(b) Suppose that $P$ and $Q$ are the sum and fill matrices of a solution $(X_1, X_2, X_3, X_4) = (A_1, A_2, A_3, A_4)$ of (4.5). If $B$ and $C$ are permutation matrices of orders $u$ and 4, respectively, then $BPC$ and $BQC$ are the sum and fill matrices of another solution of (4.5) formed by permuting the indices of $A_i$ and $X_j$. Hence $BPC$ and $BQC$ are regarded as essentially the same as $P$ and $Q$. Similarly, if $P'$ is formed from $P$ by multiplying some rows and columns by $-1$, then $P'$ is regarded as essentially the same as $P$.

We state the first step of the method.

*Step 1.* Use the Sum Matrix Theorem to find a sum matrix of a solution of (4.5).

If the algebraic necessary conditions (Proposition 3.23) for the existence of $OD(4v; s_1, s_2, \ldots, s_u)$ hold, then the existence of a solution to (4.8) is guaranteed by a result of Pall (see Eades [53]).

In most cases, if the $s_i$ are small (for instance, $s_1 + \cdots + s_u \leq 28$), then the solution of (4.8) is essentially unique and can be found easily by hand.

It is clear that if $Q$ is the fill matrix of a solution of (4.5), then

$$\text{the entries of } Q \text{ are even non-negative integers}, \tag{4.9}$$

and if $M = (m_{ij}) = abs(P) + Q$, then $M$ satisfies (4.6) and

$$\text{the sum of a column of } M \text{ is at most } v. \tag{4.10}$$

There may be a large number of matrices which satisfy (4.6), (4.9) and (4.10) (see Example 4.15), but the next two lemmata may be used to reduce the number of possibilities.

**Lemma 4.15 (Eades).** *Suppose that $A$ is a circulant matrix of odd order $v$, with entries from $\{0,1,-1\}$ and with $k$ non-zero entries in each row.*

*(i) If $k \geq v-1$, then each entry of the IPV of $A$ is odd.*
*(ii) If each entry of the IPV of $A$ is even, then $v \geq k + \sqrt{k} + 1$.*

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

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

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

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

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

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

and so

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

Completing the square gives

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

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

**Lemma 4.16 (Eades).** *Suppose that the entry matrix of a solution $(X_1, X_2, X_3, X_4) = (A_1, A_2, A_3, A_4)$ of equation (4.5) is $\begin{bmatrix} V \\ W \end{bmatrix}$ where $V$ is $\ell \times r$ and $W$ is $(u-\ell) \times (4-r)$. Then*

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

*and*

$$\sum_{j=r+1}^{4} A_j A_j^\top = \left( \sum_{i=\ell+1}^{u} s_i x_i^2 \right) I\,.$$

The proof of this lemma is straightforward and thus omitted. □

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

*Step 2.* Using (3.2), (3.7), (3.8) and Lemmas 4.15 and 4.16, find all possible fill matrices which could accompany the sum matrix found in Step 1.

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

*Example 4.15.* The existence of an orthogonal design $OD(20;1,5,5,9)$ is listed in Geramita and Wallis [81] as being undetermined. To construct such an orthogonal design, we require four $5 \times 5$ circulant matrices $B_1$, $B_2$, $B_3$, $B_4$, with entries from $\{0, \pm x_1, \pm x_2, \pm x_3, \pm x_4\}$ such that

$$\sum_{i=1}^{4} B_i B_i^\top = (x_1^2 + 5x_2^2 + 5x_3^2 + 9x_4^2)\, I. \tag{4.11}$$

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

$$P = \begin{bmatrix} 1 & & & \\ & 1 & 2 & \\ & -2 & 1 & \\ & & & 3 \end{bmatrix}. \tag{4.12}$$

(See Remark (b) after Theorem 4.10.)

Now there are eight $4 \times 4$ integral matrices which, on the basis of equations (4.6), (4.9), and (4.10) could be fill matrices.

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

$$(d)\begin{bmatrix} 2 & & & \\ & & & 2 \\ 2\,2\,2 & & & \end{bmatrix}, \quad (e)\begin{bmatrix} & 2 & & \\ & & 2 & \\ 4 & & & 2 \end{bmatrix}, \quad (f)\begin{bmatrix} & & 2 & \\ & 2 & & \\ 4 & & & 2 \end{bmatrix}, \tag{4.13}$$

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

However, four of these matrices can be discounted as possible fill matrices by using Lemmas 4.15 and 4.16.

Suppose that $(B_1, B_2, B_3, B_4)$ has sum matrix $P$ above (4.12) and fill matrix (4.13) (b). Then the entry matrix is

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

which satisfies equations (4.6) and (4.10). But the $(3,2)$-th entry of this entry matrix indicates by Lemma 4.15 that every entry of the IPV of $B_2$ has a term in $x_3^2$ with odd coefficient. But $x_3$ occurs at most once in each row of each of the other circulant matrices, and it follows that the IPV's of the other circulant matrices have no terms in $x_3^2$. Hence it is impossible for the IPV's of the $B_i$ to add to zero; so (4.13)(b) is not the fill matrix of the $B_i$.

Suppose that (4.13)(f) is the fill matrix of $(B_1, B_2, B_3, B_4)$; this gives entry matrix

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

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

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

is the entry matrix of another solution $(C_1, C_2, C_3, C_4)$ of (4.12) (see Remark (b) after Theorem 4.10). It follows by Lemma 4.15 that

$$C_1C_1^\top + C_2C_2^\top = (x_1^2 + 9x_2^2)I_5\,,$$

and thus, using the two-circulant construction, there is an $OD(10;1,9)$. This is impossible, as it implies the existence of an Hadamard matrix of order 10, and so (4.13)(f) is not the fill matrix of $(B_1, B_2, B_3, B_4)$.

Similarly it can be shown that (4.13)(h) and (4.13)(e) are not possible.

Each of the possible fill matrices (4.13)(a), (c), (d), (g) could specify the contents of a solution of (4.11). For each of these possibilities, we need to search through the circulant matrices whose contents are thus specified until we find a combination whose IPV's add to zero. For instance, for (4.13)(a) we need to find four $5 \times 5$ permutation matrices $M_1, M_2, M_3, M_4$ such that

$$\begin{aligned}
&(x_1, x_2, -x_2, x_3, -x_3)M_1\\
&(x_2, -x_3, -x_3, x_4, -x_4)M_2\\
&(x_2, x_2, x_3, x_4, -x_4)M_3\\
&(x_4, x_4, x_4, x_4, -x_4)M_4
\end{aligned}$$

are the first rows of circulant matrices whose IPV's add to zero. If this search fails, then we consider circulant matrices with contents specified by (4.13)(c), and so on. Note that there are a large number (about $2 \times 10^8$) of 4-tuples $M_1, M_2, M_3, M_4$ of $5 \times 5$ permutation matrices; however, only a small proportion of these need be considered, as we shall presently see.

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

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

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

**Definition 4.14.** Two circulant matrices with the same content are *isometric* if they have the same IPV.

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

The problem of executing the fourth step is considered next. Given two circulant matrices with the same content, how do we determine whether they are isometric (without the time-consuming calculation of IPV's)? How large are the lists $L_i$? Useful necessary and sufficient conditions for isometry are, in general, unknown, but one obvious sufficient condition can be described as follows.

Denote by $S_v$ the group of $v \times v$ permutation matrices, and suppose that $T \in S_v$ represents the $v$-cycle $(12\ldots v)$. Let $R$ denote the $v \times v$ back diagonal matrix (see Section 4.5). The subgroup of $S_v$ generated by $T$ and $R$ is denoted by $\langle T, R\rangle$. If $A$ and $B$ are $v \times v$ circulant matrices with first rows $a$ and $aK$ for some $K \in \langle T, R\rangle$, then it can be seen immediately that $A$ and $B$ are isometric.

It follows that the number of non-isometric circulant matrices with the same content is at most the index of $\langle T, R\rangle$ in $S_v$, that is, $\frac{(v-1)!}{2}$. Thus the lists $L_i$ in Step 4 contain at most $\frac{(v-1)!}{2}$ entries. A complete set of distinct coset representatives of $\langle T, R\rangle$ in $S_v$ is easily seen to be $E = \{M \in S_v \colon M$ represents a permutation $\theta$ on $\{1, 2, \ldots, v\}$ which satisfies $v\theta = v$ and $1\theta \leq \frac{1}{2}(v-1)\}$. Thus to compute the list $L_i$ in Step 4, we first write out the elements of $S = \{B \colon B$ is a circulant matrix with first row $a_i M$ for some $M \in E\}$, where $a_i$ denotes the first row of the circulant matrix $A_i$ chosen at Step 3. This can be done easily either automatically or by hand.

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

**Lemma 4.17.** *If $a_i = (x_1, x_2, \ldots, , x_v)$ and $B_1$ and $B_2$ are elements of $S$ with first rows $a_i M_1$ and $a_i M_2$ where $M_1$ and $M_2$ are $v \times v$ permutation matrices, then $B_1$ and $B_2$ are isometric if and only if they are equal.*

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

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

Symmetrising gives

$$a_i M_1 \left(T + T^{-1}\right) M_1^{-1} a_i^\top = a_i M_2 \left(T + T^{-1}\right) M_2^{-1} a_i^\top .$$

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

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

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

The converse is immediate. □

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

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

of $S_v$ has order

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

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

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

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

In the implementations for orthogonal designs of orders 20 and 28, there was no difficulty in using a naive algorithm for the search at Step 5 because the lists $L_i$ were relatively small. However, to extend the method to higher orders, a more sophisticated search algorithm needed to be employed (see Koukouvinos et.al. [59, 66–69, 71, 73, 102, 104, 105, 135]).

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

Firstly, suppose that $C_1, C_2, C_3, C_4$ are circulant matrices whose sum and fill matrices satisfy equations (4.6), (4.8), (4.9) and (4.10). Then the sum of the sums of the entries of the IPV's of the $C_i$ is zero (see proof of Theorem 4.10). That is, if $(c_{i1}, c_{i2}, \ldots, c_{iw})$ is the IPV of $C_i$ $(1 \le i \le 4)$, then

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

Hence if

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

then

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

Hence only $\frac{1}{2}(v-3)$ of the $\frac{1}{2}(v-1)$ components of the IPV's need to add to zero for equation (4.5) to hold. This saves time and space in computer implementation and provides a simple error-checking device for hand calculations.

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

$$\theta:\ i \rightarrowtail \begin{cases} (id)^* & \text{if } 1 \le (id)^* \le w, \\ v-(id)^* & \text{otherwise.} \end{cases} \tag{4.14}$$

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

For automatic computation this means that one of the lists, say $L_1$, may consist of elements $S' = \{B : B$ is a circulant matrix with first row $a_1 M$ for some $M \in E'\}$. This produces a considerably shorter list, and the search (Step 5) may be proportionally shorter in time.

The use of the normalizer of $\langle T\rangle$ in hand calculations is illustrated in the completion of Example 4.16 below. First, however, we show how the facts above may be used to construct a certain four variable orthogonal design of order 28.

*Example 4.16.* An orthogonal design $OD(28;1,1,1,25)$ can be constructed as follows. We want four $7 \times 7$ circulant matrices $V_1, V_2, V_3, V_4$ with entries from $\{0, \pm x_1, \pm x_2, \pm x_3, \pm x_4\}$ such that

$$\sum_{i=1}^{4} V_i V_i^{\top} = (x_1^2 + x_2^2 + x_3^2 + 25x_4^2) I\,. \tag{4.15}$$

The conditions (4.6), (4.8), (4.9), (4.10) imply that the sum and fill matrices of $(V_1, V_2, V_3, V_4)$ must be $diag(1,1,1,5)$ and

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

respectively. Hence $V_4$ must be $(J - 2I)x_4$ up to isometry (see (4.7)); thus $V_4$ has IPV $(3x_4^2, 3x_4^2, 3x_4^2)$. Choose a skew-symmetric $7 \times 7$ matrix $C_1$ with entries from $\{0,1,-1\}$ and precisely one zero in each row; denote its IPV by $(d_1, d_2, d_3)$. Now the normalizer of $\langle T\rangle$ in $S_7$ acts cyclically on $(d_1, d_2, d_3)$ by (4.14), and further, it preserves skew-symmetry. Hence there are skew-symmetric circulant matrices $C_2$ and $C_3$ with IPV's $(d_2, d_3, d_1)$ and $(d_3, d_1, d_2)$, respectively. For $1 \le i \le 3$, denote $x_i I + x_4 C_i$ by $V_i$. It is clear that the IPV's of the $V_i$, $1 \le i \le 4$, add to $(f, f, f)$, where $f = (d_1 + d_2 + d_3 + 3)x_4^2$. But since the sum and fill matrices of $(V_1, V_2, V_3, V_4)$ satisfy (4.6), (4.8), (4.9), (4.10), it follows that $f + f + f = 0$; that is, $f = 0$. Hence the IPV' s of the $V_i$ add to zero, and thus the $V_i$ satisfy (4.15).

Example 4.16 completed: The index of the normalizer of $\langle T\rangle$ in $S_5$ is 6, and so there are at most six circulants of order 5 with the same contents whose

IPV's differ by more than just a permutation. A complete set of distinct coset representatives of this subgroup is

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

Suppose that a solution $(B_1, B_2, B_3, B_4)$ of equation (4.11) has sum matrix $P$ (4.12) and fill matrix (4.13)(a). Using the set $F$, a list $L_i$ of circulants with contents thus specified and essentially different IPV's can be made for each $i \in \{1,2,3,4\}$. A short search reveals that if $B_1, B_2, B_3, B_4$ have first rows

$$\begin{aligned}
&(x_1, x_2, -x_3, x_3, -x_2),\\
&(x_2, x_4, -x_3, -x_3, -x_4),\\
&(x_3, x_2, x_4, -x_4, x_2),\\
&(-x_4, x_4, x_4, x_4, x_4),
\end{aligned}$$

respectively, then the $B_i$ satisfy equation (4.11).

Using similar methods it is possible to show that it is impossible to construct a $(1,3,6,8)$, $(2,2,5,5)$, or $(3,7,8)$ in order 20 by using four circulants. It can also be shown that, while a $(4,9)$ exists in order 14, it is impossible to construct it from two circulants.

For ease of reference we summarize these results as:

**Lemma 4.18 (Eades [52] ).** *It is not possible to find four circulant matrices $A_1, A_2, A_3, A_4$ of order 5 with entries the commuting variables $x_1, x_2, x_3, x_4$, and 0 which satisfy*

$$\sum_{i=1}^{4} A_i A_i^{\top} = \sum_{j=1}^{4} \left(s_j x_j^2\right) I_5,$$

*where $(s_1, s_2, s_3, s_4)$ is $(1,4,4,9)$, $(1,3,6,8)$, $(2,2,5,5)$ or $(3,7,8)$. Equivalently, it is not possible to use four circulant matrices in the Goethals-Seidel array to construct orthogonal designs of these types in order 20.*

**Lemma 4.19 (Eades).** *It is not possible to construct the orthogonal design $OD(14;4,9)$ using two circulant matrices.*

Horton and Seberry [107] have undertaken a full search for $OD(n;4,9)$ for small $n$ showing that, often, the necessary conditions for these orthogonal designs are not sufficient. The theoretical reasons for this strange result is undetermined.

*Remark 4.12.* It would be interesting to know if orthogonal designs of types $(1,4,4,9)$, $(1,3,6,8)$, $(2,2,5,5)$ or $(3,7,8)$ are impossible to construct by any method in order 20. If that were so, it would make the construction method by circulants assume even greater importance. We shall not even hazard a guess here, although experience should indicate that some of these designs will be impossible to construct by any method. This question is still unresolved after 30 years.

*Remark 4.13.* Since there is a strong relationship between circulant and negacyclic matrices with additive properties, it might appear fruitful to consider the "sum" and "fill" approach to finding desirable negacyclic matrices. However this IPV vector seems harder to constrain.

## 4.9 Some Arrays for Eight Circulants

Unfortunately, in trying to find designs of order $n \equiv 0 \pmod 8$ constructed using eight circulant matrices, we will not be as restricted as in Theorem 4.9 but have other problems. The difficulty of finding matrices to replace the variables has led to the following lemma using part Williamson and part Goethals-Seidel criteria. In §4.10 we will see that the Kharaghani array, which uses amicable sets and circulant and/or negacyclic matrices to greatly increase our ability to construct orthogonal designs in orders $\equiv 0 \pmod 8$.

The Kharaghani array has proved the most powerful in finding orthogonal designs of order 8. To understand why we first consider the proliferation of arrays and conditions needed to find orthogonal designs of order divisible by 8 when the Kharaghani array is not used.

**Lemma 4.20.** *Suppose $X_1, X_2, \ldots, X_8$ are eight circulant (type 1) matrices of order $n$ satisfying*

*(1) $X_i$, $1 \le i \le 8$, have entries from $\{0, \pm x_1, \ldots, \pm x_s\}$, and*
*(2) $\sum_{i=1}^{8} X_i X_i^\top = fI$.*

*Further suppose*

*(i) $X_1, X_2, \ldots, X_8$ are all symmetric or all skew, or*
*(ii) $X_1 = X_2 = \cdots = X_i$ and $X_{i+1}, \ldots, X_8$ are all symmetric or all skew, $1 \le i \le 8$, or*
*(iii) $X_2 = X_3 = X_4$ and $X_5$, $X_6$, $X_7$, $X_8$ are all symmetric (skew), or*
*(iv) $X_1 X_2^\top = X_2 X_1^\top$, $X_3 = X_4$ and $X_5$, $X_6$, $X_7$, $X_8$ are all symmetric, or*
*(v) $X_1, \ldots, X_i$ are all skew and $X_{i+1}, \ldots, X_8$ all symmetric, or*
*(vi) $X_2$, $X_3$, $X_4$ are all skew and $X_5$, $X_6$, $X_7$, $X_8$ all symmetric, or*
*(vii) $X_i X_{i+4}^\top = X_{i+4} X_i^\top$, $i = 1, 2, 3, 4$.*

*Then, with*

$$f = \sum_{i=1}^{s} u_i x_i^2 I,$$

*there exists an orthogonal design $OD(8n; u_1, u_2, \ldots, u_s)$.*

*Proof.* As in the proof of Theorem 4.9 the main difficulty is ensuring the matrices $Y_1, \ldots, Y_8$ used to replace the commuting variables of the basic design pairwise satisfy

$$Y_i Y_j^\top = Y_j Y_i^\top.$$

The results of the lemma may be obtained, recalling the results of Section 4.5, by using the following constructions:

(i) Use the circulant matrices to replace the variables in design 1.
(ii) Use a back circulant matrix $X_1R = X_iR$ to replace the first $i$ variables in design 1.
(iii) Use design 2 which needs $A, B, E, F, G, H$ all circulant, $B$ repeated three times, and $E, F, G, H$ all symmetric.
(iv) Use design 4 for which $X, A, B, C, D, E, F$ must all be circulant, $B$ repeated twice, $C, D, E, F$ symmetric, and $XA^\top = AX^\top$.
(v) Use $X_1R, \ldots$ the back circulant matrices $X_1R, \ldots, X_iR$ to replace the first $i$ variables of design 1 and $X_{i+1}, \ldots, X_8$ to replace the last 8-$i$ variables.
(vi) Use design 5 with $B = X_2$, $C = X_3$, $D = X_4$, $E = X_5$, $F = X_6$, $G = X_7$, $H = X_8$, there is no symmetry restriction on $A = X_1$.
(vii) Use design 6. □

**Table 4.7** Design 1

$$\left[\begin{array}{cccc|cccc} A & B & C & D & E & F & G & H \\ -B & A & D & -C & F & -E & -H & G \\ -C & -D & A & B & G & H & -E & -F \\ -D & C & -B & A & H & -G & F & -E \\ \hline -E & -F & -G & -H & A & B & C & D \\ -F & E & -H & G & -B & A & -D & C \\ -G & H & E & -F & -C & D & A & -B \\ -H & -G & F & E & -D & -C & B & A \end{array}\right]$$

**Table 4.8** Design 2

$$\left[\begin{array}{cccc|cccc} AR & B & B & B & E & F & G & H \\ -B & AR & B & -B & F & -E & -H & G \\ -B & -B & AR & B & G & H & -E & -F \\ -B & B & -B & AR & H & -G & F & -E \\ \hline -E & -F & -G & -H & AR & -B^\top & -B^\top & -B^\top \\ -F & E & -H & G & B^\top & AR & B^\top & -B^\top \\ -G & H & E & -F & B^\top & -B^\top & AR & B^\top \\ H & -G & F & E & B^\top & B^\top & -B^\top & AR \end{array}\right]$$

*Example 4.17.* The following orthogonal designs in order 24 are constructed by using this lemma. The reader may refer to the Table of the Appendix of Orthogonal Designs in order 24 to find the first rows of the circulant matrices which should be used as indicated:

**Table 4.9** Design 3

$$\left[\begin{array}{cccc|cccc} AR & B & B & B & E & F & G & H \\ -B & AR & B & -B & -F & -E & -H & G \\ -B & -B & AR & B & G & H & -E & -F \\ -B & B & -B & AR & H & -G & F & -E \\ \hline -E & -F & -G & -H & AR & B^\top & B^\top & B^\top \\ -F & E & -H & G & -B^\top & AR & -B^\top & B^\top \\ -G & H & E & -F & -B^\top & B^\top & AR & -B^\top \\ -H & -G & F & E & -B^\top & -B^\top & B^\top & AR \end{array}\right]$$

**Table 4.10** Design 4

$$\left[\begin{array}{cccc|cccc} XR & AR & B & B & C & D & E & F \\ -AR & XR & B & -B & D & -C & -F & E \\ -B & -B & XR & AR & E & F & -C & -D \\ -B & B & -AR & XR & F & -E & D & -C \\ \hline -C & -D & -E & -F & XR & AR & B^\top & B^\top \\ -D & C & -F & E & -AR & XR & -B^\top & B^\top \\ -E & F & C & -D & -B^\top & B^\top & XR & -AR \\ -F & -E & D & C & -B^\top & -B^\top & AR & XR \end{array}\right]$$

**Table 4.11** Design 5

$$\left[\begin{array}{cccc|cccc} AR & B & C & D & E & F & G & H \\ -B & AR & D & -C & F & -E & -H & G \\ -C & -D & AR & B & G & H & -E & -F \\ -D & C & -B & AR & H & -G & F & -E \\ \hline -E & -F & -G & -H & AR & B^\top & C^\top & D^\top \\ -F & E & -H & G & -B^\top & AR & -D^\top & C^\top \\ -G & H & E & -F & -C^\top & D^\top & AR & -B^\top \\ -H & -G & F & E & -D^\top & -C^\top & B^\top & AR \end{array}\right]$$

**Table 4.12** Design 6

$$\left[\begin{array}{cccc|cccc} A & BR & CR & DR & E & FR & GR & HR \\ -BR & A & D^\top R & -C^\top R & FR & -E & -H^\top R & G^\top R \\ -CR & -D^\top R & A & B^\top R & GR & H^\top R & -E & -F^\top R \\ -DR & C^\top R & -B^\top R & A & HR & -G^\top R & F^\top R & -E \\ \hline -E & -FR & -GR & -HR & A & BR & CR & DR \\ -FR & E & -H^\top R & G^\top R & -BR & A & -D^\top R & C^\top R \\ -GR & H^\top R & E & -F^\top R & -CR & D^\top R & A & -B^\top R \\ -HR & -G^\top R & F^\top R & E & -DR & -C^\top R & B^\top R & A \end{array}\right]$$

for $OD(24;1,1,1,1,6,6)$ use part (i);
for $OD(24;1,1,1,1,2,10)$ use part (ii);
for $OD(24;1,1,2,2,5,8)$ use part (iii);
for $OD(24;1,1,1,3,4,9)$ use part (iv);
for $OD(24;1,2,2,8,11)$ use part (v);
for $OD(24;1,1,4,4,5)$ use part (vi);
for $OD(24;1,2,5,5,8)$ use part (vii);
for $OD(24;1,2,2,4,13)$ use part (viii).

*Remark 4.14.* The conditions of Lemma 4.20 are still quite difficult to satisfy. We first consider some constraints on using circulant matrices.

## 4.10 Amicable Sets and Kharaghani Arrays

Kharaghani [120] has given a most useful array to be used to give orthogonal designs constructed from circulant and most excitingly nega-cyclic matrices in orders divisible by 8.

Following Kharaghani, a set $\{A_1, A_2, \ldots, A_{2n}\}$ of square real matrices is said to be *amicable* if

$$\sum_{i=1}^{n} \left( A_{\sigma(2i-1)} A_{\sigma(2i)}^{\top} - A_{\sigma(2i)} A_{\sigma(2i-1)}^{\top} \right) = 0 \tag{4.16}$$

for some permutation $\sigma$ of the set $\{1, 2, \ldots, 2n\}$. For simplicity, we will always take $\sigma(i) = i$ unless otherwise specified. So

$$\sum_{i=1}^{n} \left( A_{2i-1} A_{2i}^{\top} - A_{2i} A_{2i-1}^{\top} \right) = 0\,. \tag{4.17}$$

Clearly a set of mutually amicable matrices is amicable, but the converse is not true in general. Throughout this section $R_k$ denotes the back diagonal identity matrix of order $k$.

A set of matrices $\{B_1, B_2, \ldots, B_n\}$ of order $m$ with entries in $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ is said to satisfy an additive property of type $(s_1, s_2, \ldots, s_u)$ if

$$\sum_{i=1}^{n} B_i B_i^{\top} = \sum_{i=1}^{u} \left( s_i x_i^2 \right) I_m. \tag{4.18}$$

Let $\{A_i\}_{i=1}^{8}$ be an amicable set of circulant matrices (or group developed or type 1) of type $(s_1, s_2, \ldots, s_u)$ and order $t$. We denote these by $8-AS(t; s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8; Z_t)$ (or $8-AS(t; s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8; G)$ for group developed or type 1). In all cases, the group $G$ of the matrix is such that the extension by Seberry and Whiteman [187] of the group from circulant to type 1 allows the same extension to $R$. Then the Kharaghani array [120]

$$H = \begin{pmatrix} A_1 & A_2 & A_4R_n & A_3R_n & A_6R_n & A_5R_n & A_8R_n & A_7R_n \\ -A_2 & A_1 & A_3R_n & -A_4R_n & A_5R_n & -A_6R_n & A_7R_n & -A_8R_n \\ -A_4R_n & -A_3R_n & A_1 & A_2 & -A_8^\top R_n & A_7^\top R_n & A_6^\top R_n & -A_5^\top R_n \\ -A_3R_n & A_4R_n & -A_2 & A_1 & A_7^\top R_n & A_8^\top R_n & -A_5^\top R_n & -A_6^\top R_n \\ -A_6R_n & -A_5R_n & A_8^\top R_n & -A_7^\top R_n & A_1 & A_2 & -A_4^\top R_n & A_3^\top R_n \\ -A_5R_n & A_6R_n & -A_7^\top R_n & -A_8^\top R_n & -A_2 & A_1 & A_3^\top R_n & A_4^\top R_n \\ -A_8R_n & -A_7R_n & -A_6^\top R_n & A_5^\top R_n & A_4^\top R_n & -A_3^\top R_n & A_1 & A_2 \\ -A_7R_n & A_8R_n & A_5^\top R_n & A_6^\top R_n & -A_3^\top R_n & -A_4^\top R_n & -A_2 & A_1 \end{pmatrix}$$

is an $OD(8t; s_1, s_2, \ldots, s_u)$.

The Kharaghani array has been used in a number of papers [67, 68, 72, 100, 105, 108, 120, 126] among others to obtain infinitely many families of orthogonal designs. Research has yet to be initiated to explore the algebraic restrictions imposed an amicable set by the required constraints.

Koukouvinos and Seberry [137] have extended the construction of Holzmann and Kharaghani [101] to find infinite families of Kharaghani type orthogonal designs, and in [136] orthogonal designs $OD(8t; k, k, k, k, k, k)$ in 6 variables for odd $t$.

## 4.11 Construction using 8 Disjoint Matrices

First we give the following definition.

**Definition 4.15.** Define $L$-matrices, $L_1, L_2, \ldots, L_n$ to be $n$ circulant (or type 1) $(0, \pm 1)$ matrices of order $\ell$ satisfying

(i) $L_i * L_j = 0$, $i \neq j$,

(ii) $\sum_{i=1}^{n} L_i L_i^\top = kI_\ell$,

where $*$ denotes the Hadamard product. We say $k$ is the weight of these $L$-matrices.

From Definition 4.15 we observe that $T$-matrices of order $t$ (see Seberry and Yamada [188] for more details) are $L$-matrices with $\ell = k = t$ and $n = 4$.

Then we have.

**Theorem 4.11.** *Suppose $L_1, L_2, \ldots, L_n$ are $n$ circulant (or type 1) $L$-matrices of order $s$ and weight $k$. Some of the $L$-matrices may be zero.*

*Further suppose $A = (a_{ij})$, $B = (b_{ij})$ are amicable orthogonal designs of type $AOD(n; p_1, p_2, \ldots, p_u; q_1, q_2, \ldots, q_v)$ on the variables $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$, and $\{0, \pm y_1, \pm y_2, \ldots, \pm y_v\}$, respectively. Then there exists an amicable set of matrices $\{A_{i=1}^{2n}\}$ which satisfy*

$$\sum_{i=1}^{2n} A_i A_i^\top = \left(\sum_{i=1}^{u} p_i x_i^2 + \sum_{i=1}^{v} q_i y_j^2\right) \sum_{i=1}^{n} L_i L_i^\top = \left(\sum_{i=1}^{u} p_i x_i^2 + \sum_{i=1}^{v} q_i y_j^2\right) kI_s, \tag{4.19}$$

*and also* (4.16).

*Hence these* $\{A_i\}_{i=1}^{2n}$ *of order* $s$ *are an amicable set satisfying the additive property for* $(kp_1, kp_2, \ldots, kp_u, kq_1, kq_2, \ldots, kq_v)$.

*Proof.* Use

$$\begin{array}{ll}
A_1 = a_{11}L_1 + a_{12}L_2 + \cdots + a_{1n}L_n, & A_2 = b_{11}L_1 + b_{12}L_2 + \cdots + b_{1n}L_n \\
A_3 = a_{21}L_1 + a_{22}L_2 + \cdots + a_{2n}L_n, & A_4 = b_{21}L_1 + b_{22}L_2 + \cdots + b_{2n}L_n \\
A_5 = a_{31}L_1 + a_{32}L_2 + \cdots + a_{3n}L_n, & A_6 = b_{31}L_1 + b_{32}L_2 + \cdots + b_{3n}L_n \\
\vdots & \vdots \\
A_{2n-1} = a_{n1}L_1 + a_{n2}L_2 + \cdots + a_{nn}L_n, & A_{2n} = b_{n1}L_1 + b_{n2}L_2 + \cdots + b_{nn}L_n
\end{array}$$

First we note that $A$ and $B$ being amicable ensures that the $(x, y)$ entry $c_{xy}$ of $C = AB^\top$ is

$$c_{xy} = \sum_{j=1}^{n} a_{xj} b_{yj} = \sum_{j=1}^{n} a_{yj} b_{xj} = c_{yx}. \tag{4.20}$$

We also note that if $A$ and $B$ are amicable then $A^\top$ and $B^\top$ are also amicable so the $(x, y)$ entry $d_{xy}$ of $D = A^\top B$ is

$$d_{xy} = \sum_{j=1}^{n} a_{jx} b_{jy} = \sum_{j=1}^{n} a_{jy} b_{jx} = d_{yx}. \tag{4.21}$$

First let us first multiply out $A_1 A_2^\top$, where we will use $(\cdots L_\ell L_m^\top)_{\ell m}$ to denote the term in $L_\ell L_m^\top$. Then

$$A_1 A_2^\top = \sum_{j=1}^{n} a_{1j} b_{1j} L_j L_j^\top + \cdots + ((a_{1\ell} b_{1m}) L_\ell L_m^\top)_{\ell m} + \cdots. \tag{4.22}$$

Similarly

$$A_2 A_1^\top = \sum_{j=1}^{n} a_{1j} b_{1j} L_j L_j^\top + \cdots + ((b_{1\ell} a_{1m}) L_\ell L_m^\top)_{\ell m} + \cdots. \tag{4.23}$$

Hence $A_1 A_2^\top - A_2 A_1^\top$ will have no terms in $L_j L_j^\top$, $j = 1, 2, \cdots, 2n$. Thus the typical term is given by

$$A_1 A_2^\top - A_2 A_1^\top = \cdots + ((a_{1\ell} b_{1m} - b_{1\ell} a_{1m}) L_\ell L_m^\top)_{\ell m} + \cdots. \tag{4.24}$$

We now formally multiply out the expression on the left hand side of (4.16), which gives the following terms in $L_\ell L_m^\top$

$$\sum_{i=1}^{n}\left(A_{2i-1}A_{2i}^\top - A_{2i}A_{2i-1}^\top\right) =$$

$$= \cdots + \left( (\sum_{j=1}^{n} a_{j\ell}b_{jm} - \sum_{i=1}^{n} b_{i\ell}a_{im}) L_\ell L_m^\top \right)_{\ell m} + \cdots$$

$$= \cdots + \left( (\sum_{j=1}^{n} a_{jm}b_{j\ell} - \sum_{i=1}^{n} a_{im}b_{i\ell}) L_\ell L_m^\top \right)_{\ell m} + \cdots$$

$$\cdots + \cdots \text{ using (4.21)}$$

$$= 0.$$

This is formally zero and we have (4.17). These matrices also satisfy (4.18) and (4.19) by virtue of $A$ and $B$ being (amicable) orthogonal designs. □

*Remark 4.15.* Although the theorem is true for any pair of amicable orthogonal designs the arrays needed to exploit the full generality of the theorem are only known, at present, to exist for $n = 2$ or 4.

The maximum number of variables in amicable orthogonal designs of orders 2 and 4 are given in Tables 5.8 and 5.9. A detailed study of amicable orthogonal designs in order 8 is given by Deborah Street in [202, p125–134] and [203, p26–29]. Thus we have:

**Corollary 4.13.** *Suppose there exist* $AOD(2\ell; p_1, p_2; q_1, q_2)$. *Further suppose there exist two circulant (or type 1)* $L$*-matrices of order* $\ell$ *and weight* $k$. *Then there exists an* $OD(4\ell; kp_1, kp_2, kq_1, kq_2)$.

*Proof.* We use the $L$-matrices in the theorem to form an amicable set satisfying the required additive property which is then used in the Goethals-Seidel array to obtain the result. □

**Corollary 4.14.** *Suppose there exist* $AOD(4\ell; p_1, p_2, p_3; q_1, q_2, q_3)$. *Further suppose there exist four circulant (or type 1)* $L$*-matrices of order* $\ell$ *and weight* $k$. *Then there exists an* $OD(8\ell; kp_1, kp_2, kp_3, kq_1, kq_2, kq_3)$.

*Proof.* We use the $L$-matrices in the theorem to form an amicable set satisfying the additive property for $(kp_1, kp_2, kp_3, kq_1, kq_2, kq_3)$. These are then used in the Kharaghani array to obtain the result. □

*Example 4.18 (**n = 2**).* Let $A$ and $B$ be the $AOD(2; 1, 1; 1, 1)$ given by

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ d & -c \end{bmatrix}.$$

Let $L_1$ and $L_2$ be two circulant (or type 1) $L$-matrices of order $\ell$ and weight $k$. Construct

$$\begin{array}{ll} A_1 = aL_1 + bL_2\,, & A_2 = cL_1 + dL_2 \\ A_3 = -bL_1 + aL_2\,, & A_4 = dL_1 - cL_2\,. \end{array} \tag{4.25}$$

Then

$$\sum_{i=1}^{4} A_i A_i^\top = (a^2+b^2+c^2+d^2)\sum_{i=1}^{2} L_i L_i^\top = k(a^2+b^2+c^2+d^2)I_\ell \tag{4.26}$$

and

$$A_1 A_2^\top - A_2 A_1^\top + A_3 A_4^\top - A_4 A_3^\top = 0\,. \tag{4.27}$$

Hence this set of matrices $\{A_1, A_2, \ldots, A_4\}$ of order $\ell$ with entries in $\{0, \pm a, \pm b, \pm c, \pm d\}$ is an *amicable set* satisfying the additive property for $(1,1,1,1)$.

These can be used in a variant of the Goethals-Seidel array

$$G = \begin{pmatrix} A_1 & A_2 & A_3R & A_4R \\ -A_2 & A_1 & -A_4R & A_3R \\ -A_3R & A_4R & A_1 & -A_2 \\ -A_4R & -A_3R & A_2 & A_1 \end{pmatrix}$$

where $R$ is the back-diagonal identity matrix, to obtain an $OD(4\ell; k, k, k, k)$. □

*Example 4.19 ($\boldsymbol{n = 4}$).* Let $A$ and $B$ be the $AOD(4; 1,1,1; 1,1,1)$ given by

$$\begin{bmatrix} a & b & c & 0 \\ -b & a & 0 & -c \\ -c & 0 & a & b \\ 0 & c & -b & a \end{bmatrix} \begin{bmatrix} d & e & f & 0 \\ e & -d & 0 & -f \\ f & 0 & -d & e \\ 0 & -f & e & d \end{bmatrix}.$$

Let $L_1,\ L_2, \cdots, L_4$ be four circulant (or type 1) $L$-matrices of order $\ell$ and weight $k$. Construct

$$\begin{array}{llll} A_1 = aL_1 & +bL_2 & +cL_3\,, & \\ A_3 = -bL_1 & +aL_2 & -cL_4\,, & \\ A_5 = -cL_1 & +aL_3 & +bL_4\,, & \\ A_7 = & +cL_2 & -bL_3 & +aL_4\,, \end{array} \qquad \begin{array}{llll} A_2 = dL_1 & +eL_2 & +fL_3\,, & \\ A_4 = eL_1 & -dL_2 & -fL_4\,, & \\ A_6 = fL_1 & -dL_3 & +eL_4\,, & \\ A_8 = & -fL_2 & +eL_3 & +dL_4\,. \end{array} \tag{4.28}$$

Then

$$\begin{aligned} \sum_{i=1}^{8} A_i A_i^\top &= \left(a^2+b^2+c^2+d^2+e^2+f^2\right)\sum_{i=1}^{4} L_i L_i^\top \\ &= k\left(a^2+b^2+c^2+d^2+e^2+f^2\right) I_\ell, \end{aligned} \tag{4.29}$$

and

$$A_1A_2^\top - A_2A_1^\top + A_3A_4^\top - A_4A_3^\top + A_5A_6^\top - A_6A_5^\top + A_7A_8^\top - A_8A_7^\top = 0. \tag{4.30}$$

Hence this set of matrices $\{A_1, A_2, \ldots, A_8\}$ of order $\ell$ with entries in $\{0, \pm a, \pm b, \pm c, \pm d, \pm e, \pm f\}$ is an *amicable set* satisfying the additive property for $(1,1,1,1,1,1)$.

They can be used in the Kharaghani array to obtain $OD(8\ell; k, k, k, k, k, k)$.

*Example 4.20 ($\boldsymbol{n = 4}$).* Let $A$ and $B$ be the $AOD(4; 1, 1, 2; 1, 1, 2)$ given by

$$\begin{bmatrix} a & b & c & c \\ -b & a & c & -c \\ c & c & -a & -b \\ c & -c & b & -a \end{bmatrix} \begin{bmatrix} d & e & f & f \\ e & -d & f & -f \\ -f & -f & e & d \\ -f & f & d & -e \end{bmatrix}.$$

Let $L_1,\ L_2, \cdots, L_4$ four circulant (or type 1) $L$-matrices of order $\ell$ and weight $k$. Construct

$$\begin{array}{llll} A_1 = aL_1 & +bL_2 & +cL_3 & +cL_4, \\ A_3 = -bL_1 & +aL_2 & +cL_3 & -cL_4, \\ A_5 = cL_1 & +cL_2 & -aL_3 & -bL_4, \\ A_7 = cL_1 & -cL_2 & +bL_3 & -aL_4, \end{array} \quad \begin{array}{llll} A_2 = dL_1 & +eL_2 & +fL_3 & +fL_4, \\ A_4 = eL_1 & -dL_2 & +fL_3 & -fL_4, \\ A_6 = -fL_1 & -fL_2 & +eL_3 & +dL_4, \\ A_8 = -fL_1 & +fL_2 & +dL_3 & -eL_4. \end{array} \tag{4.31}$$

Then

$$\begin{aligned} \sum_{i=1}^{8} A_iA_i^\top &= (a^2 + b^2 + 2c^2 + d^2 + e^2 + 2f^2) \sum_{i=1}^{4} L_iL_i^\top \\ &= k(a^2 + b^2 + 2c^2 + d^2 + e^2 + 2f^2) I_\ell, \end{aligned} \tag{4.32}$$

and

$$A_1A_2^\top - A_2A_1^\top + A_3A_4^\top - A_4A_3^\top + A_5A_6^\top - A_6A_5^\top + A_7A_8^\top - A_8A_7^\top = 0. \tag{4.33}$$

Hence this set of matrices $\{A_1, A_2, \ldots, A_8\}$ of order $\ell$ with entries in $\{0, \pm a, \pm b, \pm c, \pm d, \pm e, \pm f\}$ is an *amicable set* satisfying the additive property for $(1,1,2,1,1,2)$. These can be used in the Kharaghani array to obtain an $OD(8\ell; k, k, k, k, 2k, 2k)$.

### *4.11.1 Hadamard Matrices*

Before going to our next result, we first note:

**Lemma 4.21.** *If there is $AOD(m\colon (1, m-1); (m))$ and $OD(h; 1, h-1)$, then by Wolfe's theorem (7.9) there is an $OD(mh; 1, m-1, m(h-1))$.*

Then Theorem 8.7 of Wallis [231, p.368] can be restated as:

**Theorem 4.12 (Wallis).** *Suppose there exists* $OD(mh; 1, m-1, m(h-1))$. *Suppose there exist "suitable" matrices of order* $n$ *to replace the variables of this design. Then there exists an Hadamard matrix of order* $mhn$.

*Proof.* Obvious. □

**Corollary 4.15.** *Let* $n$ *be the order of any Hadamard matrix* $H$. *Suppose there exists an orthogonal design* $D$ *of type* $OD(n(m-1): (1, m-1, nm-n-m))$. *Then there exists an Hadamard matrix of order* $n(n-1)(m-1)$.

*Proof.* We write $H$ as

$$\begin{bmatrix} 1 & e \\ -e^\top & P \end{bmatrix}$$

where $e$ is the $1 \times (n-1)$ matrix of 1's. Then

$$PJ = J, \qquad PP^\top = nI - J.$$

The result is obtained by replacing the variables of $D$ by $P$, $J$, $P$, respectively. □

Many corollaries can be made by finding "suitable" matrices, but we will not proceed further with this here.

We will show in Chapter 9 that $OD(2^t: (1, m-1, nm-n-m))$ exist in every power of 2, $2^t = (m-1)n$. Hence we have a new result.

**Corollary 4.16.** *With* $t$, $s$ *any non-negative integers, there exists a Hadamard matrix of order* $2^s(2^s-1)(2^t-1)$.

We note the following result:

**Theorem 4.13.** *Let* $k > 1$ *be the order of an Hadamard matrix* $H$, *and* $n$ *be the order of a symmetric conference matrix* $C$. *Further, suppose there exist amicable orthogonal designs* $M$, $N$ *of types* $AOD(m: (1, m-1); (\frac{m}{2}, \frac{m}{2}))$. *Then there exists an* $OD(nmk: k, (m-1)k, (n-1)\frac{mk}{2}, (n-1)\frac{nk}{2})$.

*Proof.* let $P = \left[\begin{smallmatrix} 0 & - \\ 1 & 0 \end{smallmatrix}\right] \times I_{\frac{k}{2}}$. Then

$$R = C \times H \times N + I \times PH \times M$$

is the required orthogonal design. □

Hence we have generalized a theorem of Wallis [231, p.375, Theorem 8.24]:

**Corollary 4.17.** *Suppose* $H$, $C$, $M$, $N$ *are as in the theorem, and suppose there are "suitable" matrices of order* $p$. *Then there exists an Hadamard matrix of order* $nmkp$.

Now we note that if $m$ is of the form $\prod_i 2^t(p_i^{r_i}+1)$, where $p_i^{r_i} \equiv 3 \pmod 4$ is a prime power, then $AOD(m: (1, m-1); (\frac{m}{2}, \frac{m}{2}))$ exist. Thus we have:

**Corollary 4.18.** *Suppose $k>1$ is the order of an Hadamard matrix and $n$ the order of a symmetric conference matrix. Then there exists $OD(k,(2m-1)k,(n-1)mk,(n-1)mk)$ where $m=2_i^t\prod(p_i^{r_i}+1), p_i^{r_i}\equiv 3 \pmod 4$ is a prime power, and $t>0$ is an integer.*

## 4.12 Baumert-Hall Arrays

In 1933 Paley wrote a most important paper on the construction of Hadamard matrices which he called 'orthogonal matrices' [160]. At the same time J.A. Todd [211] realised that these matrices gave symmetric balanced incomplete block designs–of great interest in the design and analysis of experiments for agriculture and medicine.

Thus Paley opened the way for R.C. Bose's [26] fundamental and path-finding use of Galois fields in the construction of balanced incomplete block designs–a most valuable contribution to applied statistics.

Yet it was not until Williamson's 1944 [244] and 1947 [245] papers that more Hadamard matrices were found. Williamson used what we would now call orthogonal designs $OD(n;1,n-1)$ and $OD(n;2,n-2)$.

Paley listed the orders less than 200 for which Hadamard matrices were not known, viz., 92, 116, 148, 156, 172, 184, and 188. Williamson suggested using what we will call the Williamson Array

$$\begin{bmatrix} A & B & C & D \\ -B & A & D & -C \\ -C & -D & A & B \\ -D & C & -B & A \end{bmatrix}$$

to find Hadamard matrices and in fact obtained the matrices of orders 148 and 172 by finding suitable matrices (using the theory we now call cyclotomy; see Storer [200]) to replace the variables of the array. Thus we define

**Definition 4.16.** Eight circulant $(1,-1)$ matrices $X_1,\ldots,X_8$ of order $n$ which satisfy

$$\sum_{i=1}^{8} X_i X_i^\top = 8nI, \quad X_i X_j^\top = X_j X_i^\top$$

will be called *eight Williamson matrices* (cf Williamson matrices: Theorem 4.4 and proof). *Williamson matrices* are four circulant symmetric matrices $x_1,\ldots,x_u$ satisfying

$$\sum_{i=1}^{4} X_i X_i^\top = 4nI\,.$$

Baumert, Golomb and Hall [17] found Williamson matrices of order 23 giving the Hadamard matrices of orders 92 and 184. We can appreciate their excitement when on the night of September 27, 1961, after an hour of computer calculation, the output arrived. In fact, there turned out to be one and only one example of Williamson matrices of order 23.

Later, Baumert [15, 18] was to find Williamson matrices giving the Hadamard matrix of order 116. We shall give the Hadamard matrix of order 188 in Proposition 7.2.

The remainder of this section is devoted to the exciting results that have come from Baumert and Hall's search for the Hadamard matrix of order 156. But first a definition.

**Definition 4.17.** An orthogonal design $OD(4t;t,t,t,t)$ will be called a *Baumert-Hall array of order t*.

Now Baumert and Hall realised that since Williamson matrices of order 13 were known, if a Baumert-Hall array of order 3 could be found, then the Hadamard matrix of order 156 would be found. In fact, they realised:

**Theorem 4.14.** *If a Baumert-Hall array of order t and Williamson matrices of order n exist, then there exists an Hadamard matrix of order* $4nt$*; equivalently, if there exists an orthogonal design* $OD(4nt;t,t,t,t)$ *and Williamson matrices of order n, then there exists an Hadamard matrix of order* $4nt$.

*Proof.* Replace the variables of the Baumert-Hall array by the Williamson matrices. □

In 1965 Baumert and Hall [14] published the first Baumert-Hall array of order 3 (Table 4.13):

**Table 4.13** Baumert-Hall array–order 3

$$\begin{bmatrix}
A & A & A & B & -B & C & -C & -D & B & C & -D & -D \\
A & -A & B & -A & -B & -D & D & -C & -B & -D & -C & -C \\
A & -B & -A & A & -D & D & -B & B & -C & -D & C & -C \\
B & A & -A & -A & D & D & D & C & C & -B & -B & -C \\
B & -D & D & D & A & A & A & C & -C & B & -C & B \\
B & C & -D & D & A & -A & C & -A & -D & C & B & -B \\
D & -C & B & -B & A & -C & -A & A & B & C & D & -D \\
-C & -D & -C & -D & C & A & -A & -A & -D & B & -B & -B \\
D & -C & -B & -B & -B & C & C & -D & A & A & A & D \\
-D & -B & C & C & C & B & B & -D & A & -A & D & -A \\
C & -B & -C & C & D & -B & -D & -B & A & -D & -A & A \\
-C & -D & -D & C & -C & -B & B & B & D & A & -A & -A
\end{bmatrix}$$

Many attempts were made to generalise this array, but none were successful until in 1971 L.R. Welch [243] found a Baumert-Hall array of order 5 (Table 4.14):

**Table 4.14** Baumert-Hall array–order 5 constructed entirely of circulant blocks

$$
\left[\begin{array}{ccccc|ccccc|ccccc|ccccc}
-D & B & -C & -C & -B & C & A & -D & -D & -A & -B & -A & C & -C & -A & A & -B & -D & D & -B \\
-B & -D & B & -C & -C & -A & C & A & -D & -D & -A & -B & -A & C & -C & -B & A & -B & -D & D \\
-C & -B & -D & B & -C & -D & -A & C & A & -D & -C & -A & -B & -A & C & D & -B & A & -B & -D \\
-C & -C & -B & -D & B & -D & -D & -A & C & A & C & -C & -A & -B & -A & -D & D & -B & A & -B \\
B & -C & -C & -B & -D & A & -D & -D & -A & C & -A & C & -C & -A & -B & -B & -D & D & -B & A \\
\hline
-C & A & D & D & -A & -D & -B & -C & -C & B & -A & B & -D & D & B & -B & -A & -C & C & -A \\
-A & -C & A & D & D & B & -D & -B & -C & -C & B & -A & B & -D & D & -A & -B & -A & -C & C \\
D & -A & -C & A & D & -C & B & -D & -B & -C & D & B & -A & B & -D & C & -A & -B & -A & -C \\
D & D & -A & -C & A & -C & -C & B & -D & -B & -D & D & B & -A & B & -C & C & -A & -B & -A \\
A & D & D & -A & -C & -B & -C & -C & B & -D & B & -D & D & B & -A & -A & -C & C & -A & -B \\
\hline
B & -A & -C & C & -A & A & B & -D & D & B & -D & -B & C & C & B & -C & A & -D & -D & -A \\
-A & B & -A & -C & C & B & A & B & -D & D & B & -D & -B & C & C & -A & -C & A & -D & -D \\
C & -A & B & -A & -C & D & B & A & B & -D & C & B & -D & -B & C & -D & -A & -C & A & -D \\
-C & C & -A & B & -A & -D & D & B & A & B & C & C & B & -D & -B & -D & -D & -A & -C & A \\
-A & -C & C & -A & B & B & -D & D & B & A & -B & C & C & B & -D & A & -D & -D & -A & -C \\
\hline
-A & -B & -D & D & -B & B & -A & C & -C & -A & C & A & D & D & -A & -D & B & C & C & -B \\
-B & -A & -B & -D & D & -A & B & -A & C & -C & -A & C & A & D & D & -B & -D & B & C & C \\
D & -B & -A & -B & -D & -C & -A & B & -A & C & D & -A & C & A & D & C & -B & -D & B & C \\
-D & D & -B & -A & -B & C & -C & -A & B & -A & D & D & -A & C & A & C & C & -B & -D & B \\
-B & -D & D & -B & -A & -A & C & -C & -A & B & A & D & D & -A & C & B & C & C & -B & -D
\end{array}\right]
$$

For future reference we define:

**Definition 4.18.** *A Baumert-Hall-Welch array of order $t$* is a Baumert-Hall array of order $t$ constructed from sixteen circulant or type 1 matrices.

The circulant structure of Welch's array gave the clue to generalising Baumert-Hall arrays. First we consider:

**Definition 4.19.** Four circulant (type 1) $(0,1,-1)$ matrices $X_i$, $i=1,2,3,4$, of order $n$ which are non-zero for each of the $n^2$ entries for exactly one $i$, i.e., $X_i * X_j = 0$ for $i \neq j$, and which satisfy

$$\sum_{i=1}^{4} X_i X_i^\top = nI$$

will be called *$T$-matrices of order $n$*. These were first used by Cooper-Wallis [32].

A type 1 matrix has constant row (and column) sum; so:

**Lemma 4.22.** *Let $X_i$, $i=1,\ldots,4$, be $T$-matrices with row sum (and column sum) $x_i$, respectively. Then*

$$\sum_{i=1}^{4} x_i^2 = n\,.$$

*Proof.* $X_i J = x_i J$; so considering $\sum_{i=1}^{4} X_i X_i^\top J = nJ$ gives the result. □

The following result, in a slightly different form, was independently discovered by R.J. Turyn. Turyn use what are called $T$-sequences later in this chapter. $T$-sequences are the aperiodic counter part of $T$-matrices. The existence of $T$-sequences implies the existence of $T$-matrices.

**Theorem 4.15 (Cooper-Wallis [32]).** *Suppose there exist $T$-matrices $X_i$, $i=1,\ldots,4$, of order $n$. Let $a$, $b$, $c$, $d$ be commuting variables. Then*

$$\begin{aligned}
A &= aX_1 + bX_2 + cX_3 + dX_4\\
B &= -bX_1 + aX_2 + dX_3 - cX_4\\
C &= -cX_1 - dX_2 + aX_3 + bX_4\\
D &= -dX_1 + cX - bX_3 + aX_4
\end{aligned}$$

*can be used in the Goethals-Seidel (or Wallis-Whiteman [241]) array to obtain a Baumert-Hall array of order $n$; equivalently, if there exist $T$-matrices of order $n$, there exists an orthogonal design $OD(4n;n,n,n,n)$.*

*Proof.* By straightforward verification. □

*Example 4.21.* Let

$$X_1 = \begin{bmatrix} 1&0&0\\ 0&1&0\\ 0&0&1 \end{bmatrix}, \quad X_2 = \begin{bmatrix} 0&1&0\\ 0&0&1\\ 1&0&0 \end{bmatrix}, \quad X_3 = \begin{bmatrix} 0&0&1\\ 1&0&0\\ 0&1&0 \end{bmatrix}, \quad X_4 = 0.$$

Then $X_1, X_2, X_3, X_4$ are $T$-matrices of order 3, and the Baumert-Hall array of order 3 is in Table 4.15.

**Table 4.15** Baumert-Hall array–order 3

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $a$ | $b$ | $c$ | $-b$ | $a$ | $d$ | $-c$ | $-d$ | $a$ | $-d$ | $c$ | $-b$ |
| $c$ | $a$ | $b$ | $a$ | $d$ | $-b$ | $-d$ | $a$ | $-c$ | $c$ | $-b$ | $-d$ |
| $b$ | $c$ | $a$ | $d$ | $-b$ | $a$ | $a$ | $-c$ | $-d$ | $-b$ | $-d$ | $c$ |
| $b$ | $-a$ | $-d$ | $a$ | $b$ | $c$ | $-d$ | $-b$ | $c$ | $c$ | $-a$ | $d$ |
| $-a$ | $-d$ | $b$ | $c$ | $a$ | $b$ | $-b$ | $c$ | $-d$ | $-a$ | $d$ | $c$ |
| $-d$ | $b$ | $-a$ | $b$ | $c$ | $a$ | $c$ | $-d$ | $-b$ | $d$ | $c$ | $-a$ |
| $c$ | $d$ | $-a$ | $d$ | $b$ | $-c$ | $a$ | $b$ | $c$ | $-b$ | $d$ | $a$ |
| $d$ | $-a$ | $c$ | $b$ | $-c$ | $d$ | $c$ | $a$ | $b$ | $d$ | $a$ | $-b$ |
| $-a$ | $c$ | $d$ | $-c$ | $d$ | $b$ | $b$ | $c$ | $a$ | $a$ | $-b$ | $d$ |
| $d$ | $-c$ | $b$ | $-c$ | $a$ | $-d$ | $b$ | $-d$ | $-a$ | $a$ | $b$ | $c$ |
| $-c$ | $b$ | $d$ | $a$ | $-d$ | $-c$ | $-d$ | $-a$ | $b$ | $c$ | $a$ | $b$ |
| $b$ | $d$ | $-c$ | $-d$ | $-c$ | $a$ | $-a$ | $b$ | $-d$ | $b$ | $c$ | $a$ |

We will not give the proofs here which can be found in Wallis [231, p. 360] and Hunt and Wallis [110] but will just quote the results given there. More results on Baumert-Hall arrays are given in Section 7.1 after some new concepts have been introduced. In Section 7.1 we show how cyclotomy may be used in constructing these arrays, including the previously unpublished array of Hunt of order 61.

**Lemma 4.23.** *There exist Baumert-Hall arrays of order $t$, $t \in X$, $X = \{x : x$ is an odd integer, $0 \le x \le 25, 31, 37, 41, 61\}$.*

**Corollary 4.19.** *There exist Hadamard matrices of order $4tq$ where $t \in X$, $X$ given in the previous lemma, and $q$ is the order of Williamson matrices. In particular, there exist Hadamard matrices of order $4tq$, $q = \frac{1}{2}(p+1)$ or $\frac{1}{2}p(p+1)$ where $p \equiv 1 \pmod 4$ is a prime power.*

*Proof.* The required matrices are given in Corollaries 4.11 and 4.12. □

The long held conjecture that the Williamson method would give results for all orders of Hadamard matrices was first disproved for order 35 by Đoković in 1993 [42]. Schmidt's review [176] of Holzmann, Kharaghani and Tayfeh-Rezaie [106] points out that there are no Williamson matrices of order 47, 53

or 59. In their startling paper, Holzmann, Kharaghani and Tayfeh-Rezaie [106] indicate there are no Williamson matrices for four small orders. Table 4.16 summarizes the number of Williamson matrices of order 1–59.

**Table 4.16** Number of Williamson Matrices of Order 1–59 [a]

| Order: | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 | 21 | 23 | 25 | 27 | 29 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Number: | 1 | 1 | 1 | 2 | 3 | 1 | 4 | 4 | 4 | 6 | 7 | 1 | 10 | 6 | 1 |
| Order: | 31 | 33 | 35 | 37 | 39 | 41 | 43 | 45 | 47 | 49 | 51 | 53 | 55 | 57 | 59 |
| Number: | 2 | 5 | 0 | 4 | 1 | 1 | 2 | 1 | 0 | 1 | 2 | 0 | 1 | 1 | 0 |

[a] Holzmann, Kharaghani and Tayfeh-Rezaie [106, p347] © Springer

A most important theorem which shows how Baumert-Hall-Welch arrays can be used is now given. To date, the only such arrays known are of orders 5 and 9. We note that in these BHW theorems circulant or type 1 can be replaced by negacyclic matrices.

**Theorem 4.16 (Turyn [220]).** *Suppose there is a Baumert-Hall-Welch array $BHW$ of order $s$ constructed of sixteen circulant (or type 1) $s \times s$ blocks. Further suppose there are $T$-matrices of order $t$. Then there is a Baumert-Hall array of order $st$.*

*Proof.* Since $BHW$ is constructed of sixteen circulant (or type 1) blocks, we may write $BHW = (N_{ij})$, $i, j = 1, 2, 3, 4$, where each $N_{ij}$ is circulant (or type 1).

Since $(BHW)(BHW)^\top = s(a^2 + b^2 + c^2 + d^2)I_{4s}$ where $a, b, c, d$ are the commuting variables, we have

$$N_{i1}N_{j1}^\top + N_{i2}N_{j2}^\top + N_{i3}N_{j3}^\top + N_{i4}N_{j4}^\top = \begin{cases} s(a^2+b^2+c^2+d^2)I_s\,, & i = j\,, \\ & i = 1,2,3,4 \\ 0\,, & i \neq j\,. \end{cases}$$

Suppose the $T$-matrices are $T_1, T_2, T_3, T_4$. Then form the matrices

$$\begin{aligned} A &= T_1 \times N_{11} + T_2 \times N_{21} + T_3 \times N_{31} + T_4 \times N_{41} \\ B &= T_1 \times N_{12} + T_2 \times N_{22} + T_3 \times N_{32} + T_4 \times N_{42} \\ C &= T_1 \times N_{13} + T_2 \times N_{23} + T_3 \times N_{33} + T_4 \times N_{43} \\ D &= T_1 \times N_{14} + T_2 \times N_{24} + T_3 \times N_{34} + T_4 \times N_{44}\,, \end{aligned}$$

Now

$$AA^\top + BB^\top + CC^\top + DD^\top = st(a^2 + b^2 + c^2 + d^2)I_{st}\,,$$

and since $A, B, C, D$ are type 1, they can be used in the Wallis-Whiteman generalisation of the Goethals-Seidel array to obtain the desired result. (See also Lemma 4.7) □

Since the Baumert-Hall array of order 5 given by Welch is constructed of sixteen circulant blocks, as is the Ono-Sawade-Yamamoto array of order 9 given to us by K. Yamamoto [188, p. 449].

**Corollary 4.20.** *Suppose there are $T$-matrices of order $t$. Then there is a Baumert-Hall array of order $5t$ and $9t$; equivalently, there is an orthogonal design $OD(20t;5t,5t,5t,5t)$ and $OD(36t;9t,9t,9t,9t)$. As we have seen, Baumert and Hall's array of order 3, discovered to obtain the Hadamard matrix of order 156, has led to one of the most powerful constructions for Hadamard matrices. In fact, to prove the Hadamard conjecture it would be sufficient to prove:*

*Conjecture 4.3.* There exists a Baumert-Hall array of order $t$ for every positive integer $t$, or equivalently, there exists an orthogonal design $OD(4t;t,t,t,t)$ for every positive integer $t$.

## 4.13 Plotkin Arrays

Following the exciting results on Baumert-Hall arrays, which if they all exist, would answer the Hadamard conjecture in the affirmative, it became clear that similar designs in order $8n$ would give results of great import. Alas, as we shall now see, such designs of order $8n$, $n$ odd, are very hard to find.

These classes of orthogonal designs are of great interest and worthy of further study.

**Definition 4.20.** An orthogonal design $OD(8t;t,t,t,t,t,t,t,t)$ will be called a *Plotkin array.*

**Remark**. Matrices with elements $\{1,-1\}$ which can be used in Plotkin arrays to give Hadamard matrices (eight Williamson matrices) have been found by J. Wallis [236], and of course Williamson matrices (each used twice) will also suffice. Still the problem of finding suitable matrices to replace the variables in designs to give Hadamard matrices or weighing matrices is largely untouched but displaced by the use of the Kharaghani array [120] and amicable sets.

We first see that if an Hadamard matrix exists, then Plotkin arrays exist in four times the order.

**Theorem 4.17 (Plotkin [161]).** *Suppose there exists an Hadamard matrix of order $2t$. Then there exists an orthogonal design $OD(8t;t,t,t,t,t,t,t,t)$.*

*Proof.* Let $H$ be an Hadamard matrix of order 2t. Let

$$S=\frac{1}{2}\begin{pmatrix} I & -I \\ I & I \end{pmatrix} H, \qquad T=\frac{1}{2}\begin{pmatrix} I & I \\ -I & I \end{pmatrix} H,$$

$$U=\frac{1}{2}\begin{pmatrix} I & -I \\ -I & -I \end{pmatrix} H, \qquad V=\frac{1}{2}\begin{pmatrix} I & I \\ I & -I \end{pmatrix} H.$$

Then define

$$H_{2t}(a,b) = (S \times a) + (T \times b),$$
$$H_{4t}(a,b,c,d) = \begin{bmatrix} H_{2t}(a,b) & H_{2t}(c,d) \\ H_{2t}(-c,d) & H_{2t}(a,-b) \end{bmatrix},$$

and

$$B_{4t}(a,b,c,d) = \begin{bmatrix} S \times a + T \times b & U \times c + V \times d \\ U \times (-c) + V \times (-d) & S \times a + T \times b \end{bmatrix}.$$

Then

$$H_{8t}(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) = \begin{bmatrix} H_{4t}(x_1,x_2,x_3,x_4) & B_{4t}(x_5,x_6,x_7,x_8) \\ B_{4t}(x_5,x_6,x_7,x_8) & -H_{4t}(-x_1,x_2,x_3,x_4) \end{bmatrix}$$

is the required Plotkin array. □

The $8 \times 8$ matrix of Theorem 4.1, which is unique under the equivalence operations,

(i) multiply any row or column by -1,
(ii) interchange any pair of rows or columns,
(iii) replace any variable by its negative throughout,

is a design of type (1,1,1,1,1,1,1,1). Plotkin found that the following matrix is equivalent under (i), (ii) and (iii) to the Baumert-Hall array of the previous section.

$$A(x,y,z,w) = \begin{bmatrix} y & x & x & x & -z & z & w & y & -w & w & z & -y \\ -x & y & x & -x & w & -w & z & -y & -z & z & -w & -y \\ -x & -x & y & x & w & -y & -y & w & z & z & w & -z \\ -x & x & -x & y & -w & -w & -z & w & -z & -y & -y & -z \\ -y & -y & -z & -w & z & x & x & x & -w & -w & z & -y \\ -w & -w & -z & y & -x & z & x & -x & y & y & -z & -w \\ w & -w & w & -y & -x & -x & z & x & y & -z & -y & -z \\ -w & -z & w & -z & -x & x & -x & z & -y & y & -y & w \\ -y & y & -z & -w & -z & -z & w & y & w & x & x & x \\ z & -z & -y & -w & -y & -y & -w & -z & -x & w & x & -x \\ -z & -z & y & z & -y & -w & y & -w & -x & -x & w & x \\ z & -w & -w & z & y & -y & y & z & -x & x & -x & w \end{bmatrix} \tag{4.34}$$

Also, the next matrix is a Baumert-Hall array of order 12, but is not equivalent to (4.34).

$$B(x,y,z,w) = \begin{bmatrix} y & x & x & x & -w & w & z & y & -z & z & w & -y \\ -x & y & x & -x & -z & z & -w & -y & w & -w & z & -y \\ -x & -x & y & x & -y & -w & y & -w & -z & -z & w & z \\ -x & x & -x & y & w & w & -z & -w & -y & z & y & z \\ -w & -w & -z & -y & z & x & x & x & -y & -y & z & -w \\ y & y & -z & -w & -x & z & x & -x & -w & -w & -z & y \\ -w & w & -w & -y & -x & -x & z & x & z & y & y & z \\ z & -w & -w & z & -x & x & -x & z & y & -y & y & w \\ z & -z & y & -w & y & y & w & -z & w & x & x & x \\ y & -y & -z & -w & -z & -z & -w & -y & -x & w & x & -x \\ z & z & y & -z & w & -y & -y & w & -x & -x & w & x \\ -w & -z & w & -z & -v & v & -v & z & -x & x & -x & w \end{bmatrix} \tag{4.35}$$

Then we have

**Lemma 4.24.** *There is a Plotkin array of order 24, i.e. , an orthogonal design* $OD(24;3,3,3,3,3,3,3,3)$.

*Proof.*

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

is the required design. □

These results lead to:

*Conjecture 4.4 (Plotkin [161]).* There exist Plotkin arrays in every order $8n$, $n$ a positive integer.

### *4.13.1 Kharaghani's Plotkin arrays*

Until recently, only the original for $n = 3$ had been constructed in the ensuing twenty eight years. Holzmann and Kharaghani [101] using a new method constructed many new Plotkin $OD$s of order 24 and two new Plotkin $OD$s of order 40 and 56.

## 4.14 More Specific Constructions using Circulant Matrices

The constructions of this section will be used extensively later to discuss existence of orthogonal designs.

In any of the following constructions, similar results may be obtained by replacing the words circulant and back circulant by type 1 and type 2, respectively (see Section 4.2).

**Construction 4.1.** *Suppose there is a $W(n,k)$ constructed from two circulant matrices $M$, $N$ of order $\frac{n}{2}$ with the property that $M*N=0$ ($*$ denotes Hadamard product). Then $A=x_1M+x_2N$, $B=x_1N-x_2M$ may be used in $\left[\begin{smallmatrix} A & BR \\ -BR & A \end{smallmatrix}\right]$ to obtain an $OD(n;k,k)$ on $x_1$, $x_2$.*

*Proof.* A straightforward verification. One need only observe that since $M$, $N$ are circulant, $MR$, $NR$ are back circulant, and if $X$ is circulant and $Y$ is back circulant, then $XY^\top = YX^\top$. □

*Example 4.22.* Write $T$ for the circulant matrix of order $n$ whose first row is nonzero only in the second column, the entry there being 1. Now

$$M=T+T^2 \quad \text{and} \quad N=T^3-T^4$$

may be used to give a $W(2n,4)$ constructed from two circulants, $(M*N=0)$. Then, using the construction $A=x_1M+x_2N$, $B=x_1N-x_2M$ gives an $OD(2n;4,4)$ constructed from circulants.

**Construction 4.2.** *Suppose there exist $W(n,k_i)$, $i=1,2$, constructed from circulant matrices $M_i$, $N_i$, $i=1,2$, of order $\frac{n}{2}$ where $M_1*M_2=N_1*N_2=0$ and $M_1M_2^\top+M_2M_1^\top=N_1N_2^\top+N_2N_1^\top=0$; then*

$$A=x_1M_1+x_2M_2, \qquad B=x_1N_1+x_2N_2$$

*may be used as two circulants to give an $OD(n;k_1,k_2)$ on the variables $x_1$, $x_2$.*

*Example 4.23.* With $T$ as in the previous example and $n=2k+1$, let

$$M_1=T^{k-1}-T^{k+2} \qquad N_1=T^{k-1}+T^{k+2}$$
$$M_2=T^k+T^{k+1} \qquad N_2=T^k-T^{k+1}$$

which satisfy the conditions of the construction. Then

$$A=x_1M_1+x_2M_2 \qquad B=x_1N_1+x_2N_2$$

give an $OD(n;4,4)$.

**Construction 4.3.** *Suppose there exist orthogonal designs $X_1$, $X_2$ of type $OD(2n;u_{i1},u_{i2},\ldots,u_{im_i})$ on the variables $x_{i1},x_{i2},\ldots,x_{im}$, $i=1,2$, each of which is constructed using two circulants.*

*Then there exists an $OD(4n;u_{11},u_{12},\ldots u_{1m_1},\ u_{21},u_{22},\ldots,u_{2m_2})$ on the variables $x_{11},x_{12},x_{1m_1},x_{21},x_{22},\ldots,x_{2m_2}$.*

*Proof.* Let $A_i$, $B_i$ be the matrices used to form the orthogonal design $X_i$. Then use $A_1$, $B_1$, $A_2$, $B_2$ in the Goethals-Seidel array to get the result. □

**Corollary 4.21.** *Suppose there exist $W(n,k_i)$, $i=1,2$, constructed from circulant matrices $M_i$, $N_i$, $i=1,2$, of order $\frac{n}{2}$. Then there exists an $OD(2n;k_1,k_2)$, and a $W(2n,k_1+k_2)$.*

*Proof.* Set $A=x_1M_1$, $B=x_1N_1$, $C=x_2M_2$, $D=x_2N_2$ in the Goethals-Seidel array. □

*Example 4.24.* The circulant matrices $A(a)$, $B(a)$ ,with first rows

$$a\ \ a\ \ a\ \ \bar{a}\ \ 0_{n-4}, \qquad a\ \ a\ \ \bar{a}\ \ a\ \ 0_{n-4}, \qquad \text{respectively,}$$

give a $W(2n,8)$ constructed from circulants for every $r \geq 4$, and the circulant matrices $C(c,d)$, $D(d)$ with first rows

$$d\ \ c\ \ \bar{d}\ \ 0_{m-3}, \qquad d\ \ 0\ \ d\ \ 0_{m-3}, \qquad \text{respectively,}$$

give an $OD(2m;1,4)$ in every order, $m \geq 3$, where $0_t$ is a sequence of $t$ zeros.

Hence

$$\{A(a),\ B(a),\ A(b),\ B(b)\}$$
$$\{C(c,d),\ D(d),\ C(a,b),\ D(b)\}$$
$$\{A(a),\ B(a),\ C(c,d),\ D(d)\}$$

can be used as four circulant matrices in the Goethals-Seidel array to give $OD(4s;8,8)$, $OD(4s;1,1,4,4)$ and $OD(4s;1,4,8)$, $s \geq 4$ respectively.

The next theorem indicates that we may be able to prove theorems of the type, "If $(s_1,\ldots,s_r)$ satisfies all the existence criteria for an orthogonal design, then $(s_1,\ldots,s_r)$ is the type of an orthogonal design in some large enough order $tn$ and every order $un$, $u \geq t$." We will give, in a later chapter, the results that Eades and others have found in this direction.

**Theorem 4.18.** *Suppose $(s_1,s_2,s_3,s_4)$ satisfies Wolfe's necessary conditions for the existence of orthogonal designs in order $n=4 \pmod 8$ given by Proposition 3.23:*

*(i) If $s_1+s_2+s_3+s_4 \geq 12$, there is an $OD(4t;\ s_1,s_2,s_3,s_4)$ for all $t \geq 3$.*
*(ii) If $s_1+s_2+s_3+s_4 \geq 16$, there is an $OD(4t;\ s_1,s_2,s_3,s_4)$ for all $t \geq 4$, with the possible exception of $(2,2,5,5)$ which exists in order $4t$, $t \geq 4$, $t \neq 5$.*
*(iii) If $16 < s_1+s_2+s_3+s_4 \leq 28$, the Table 4.17 gives the smallest $N$ such that $(s_1,s_2,s_3,s_4)$ is the type of an orthogonal design which exists for all $4t > N$.*

*Proof.* See pages 168–170 of *Orthogonal Designs* (1st edition, 1979). □

**Table 4.17** $N$ is the order such that the indicated designs exist in every order $4t > N$

| Group $12 \le 16$ [a] | N | Group $16 \le 20$ [b] | N | Group $20 \le 24$ [c] | N | Group $24 \le 28$ [d] | N |
|---|---|---|---|---|---|---|---|
| (1,1,4,9) | 16 | (1,1,1,16) | 24 | (1,1,2,18) | 48 | (1,1,1,25) | 56 |
| (1,2,2,9) | 16 | (1,1,8,8) | 20 | (1,1,4,16) | 24 | (1,1,5,20) | 144 |
| (1,2,4,8) | 16 | (1,1,9,9) | 20 | (1,1,10,10) | 40 | (1,1,8,18) | 56 |
| (1,4,4,4) | 16 | (1,2,8,9) | 40 | (1,2,2,16) | 48 | (1,1,9,16) | 312 |
| (1,4,5,5) | 16 | (1,3,6,8) | 48 | (1,2,6,12) | 24 | (1,1,13,13) | 48 |
| (2,2,2,8) | 16 | (1,4,4,9) | 48 | (1,4,8,8) | 32 | (1,2,4,18) | 80 |
| (2,2,5,5) | 24 | (1,5,5,9) | 40 | (1,4,9,9) | 72 | (1,3,6,18) | 468 |
| (2,3,4,6) | 16 | (2,2,4,9) | 40 | (2,2,2,18) | 48 | (1,4,4,16) | 40 |
| (4,4,4,4) | 16 | (2,2,8,8) | 20 | (2,2,4,16) | 24 | (1,4,10,10) | 40 |
| | | (2,3,6,9) | 40 | (2,2,9,9) | 24 | (1,8,8,9) | 80 |
| | | (2,4,4,8) | 20 | (2,2,10,10) | 24 | (1,9,9,9) | 80 |
| | | (2,5,5,8) | 20 | (2,4,6,12) | 24 | (2,4,4,18) | 80 |
| | | (3,3,6,6) | 20 | (2,4,8,9) | 160 | (2,8,8,8) | 28 |
| | | (4,4,5,5) | 20 | (3,3,3,12) | 48 | (2,8,9,9) | 80 |
| | | (5,5,5,5) | 20 | (3,4,6,8) | 56 | (3,6,8,9) | 952 |
| | | | | (4,4,4,9) | 112 | (4,4,4,16) | 28 |
| | | | | (4,4,8,8) | 24 | (4,4,9,9) | 48 |
| | | | | (4,5,5,9) | 168 | (4,4,10,10) | 28 |
| | | | | (6,6,6,6) | 24 | (5,5,8,8) | 32 |
| | | | | | | (5,5,9,9) | 80 |
| | | | | | | (7,7,7,7) | 28 |

*a.* $12 < s_1 + s_2 + s_3 + s_4 \le 16$ *b.* $16 < s_1 + s_2 + s_3 + s_4 \le 20$ *c.* $20 < s_1 + s_2 + s_3 + s_4 \le 24$ *d.* $24 < s_1 + s_2 + s_3 + s_4 \le 28$

## 4.15 Generalized Goethals-Seidel Arrays

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

**Definition 4.21.** If $H$ is an abelian subgroup of $U_v$ and there is an element $R$ of $U_v$ such that $R^2 = I$ and $R^{-1}AR = A^{-1}$ for all $A \in H$, then we shall call $KH$ a *GC-ring* (generalized circulant ring).

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

$$\sum_{i=1}^{4} A_i A_i^\top = mI\,. \tag{4.36}$$

then the rows of

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

are mutually orthogonal.

Wallis and Whiteman [241] showed essentially that if $H$ is an abelian group of permutation matrices, then $KH$ is a $GC$-ring. The elements of $KH$ are called type 1 matrices on $H$ (see §4.3).

Delsarte, Goethals and Seidel [39] introduced another $GC$-ring. If $D$ denotes the $v \times v$ matrix $\mathrm{diag}(1,1,\ldots,1,-1)$, then $DT$ generates a cyclic subgroup $L$ of $U_v$ of order $2v$. The group ring $KL$ is a $GC$-ring.

**Remarks**

(a) Mullin and Stanton [155] use the term group matrix rather than type 1 matrix,

(b) The definition of type 1 matrix by Wallis and Whiteman in fact only includes the case where $H$ represents a transitive permutation group. However, the extension to the intransitive case is not difficult,

(c) Suppose that $b$ is odd and $N$ denotes the $b \times b$ matrix $\mathrm{diag}(1,-1,1,-1,\ldots,-1,1)$. Then a $b \times b$ matrix $A$ is circulant if and only if $N^{-1}AN$ is negacyclic (see Section 4.17). Hence an equation of the form (4.36) has a solution consisting of negacyclic matrices of order $b$ if and only if it has a solution consisting of circulant matrices of order $b$.

The Goethals-Seidel array itself may be generalized as follows.

**Definition 4.22.** Let $G$ denote the group

$$\langle r, x_1, x_1^\top, x_2, x_2^\top, \ldots, | x_i x_j = x_j x_i, x_i x_j^\top = x_j^\top x_i \quad \text{for } i,j \in \{1,2,\ldots\},\ r^2 = 1,\ r x_i r = x_i^\top \rangle$$

Denote by $S$ the subset

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

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

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

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

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

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

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

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

$$\sum_{i=1}^{u} s_i X_i X_i^\top = \left(\sum_{j=1}^{\ell} m_j y_j^2\right) I\,.$$

Then replacing the entries of $A$ with the appropriate matrices yields an $OD(nv; m_1, m_2, \ldots, m_\ell)$. Examples of orthogonal designs constructed in this way are given later in this section.

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

**Theorem 4.19 (Eades).** *Suppose that there is a GGS array of type $(s_1, s_2, \ldots, s_u)$ and order $n$, and the $v \times v$ matrices $A_1, A_2, \ldots, A_u$ are from some GC-ring and have entries from $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$. If*

$$\sum_{i=1}^{u} s_i A_i A_i^\top = \left(\sum_{j=1}^{\ell} m_j x_j x_j^\top\right) I\,.$$

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

*Proof.* Suppose that $A$ is a GGS array of type $(s_1, s_2, \ldots, s_u)$ and order $v$, and the following replacements are made:

$$\begin{aligned} 0 &\mapsto \text{zero matrix of order } v; \\ \pm x_i &\mapsto \pm A_i\,; \\ \pm x_i^\top &\mapsto \pm A_i^\top\,; \\ \pm r x_i &\mapsto \pm r R A_i\,; \\ \pm r x_i^\top &\mapsto \pm r R A_i^\top\,. \end{aligned}$$

Then the resulting matrix $B$ has entries from $S$ and

$$\begin{aligned} BB^* &= \left(\sum_{i=1}^{u} s_i A_i A_i^\top\right) \times I_n \\ &= \left(\sum_{j=1}^{\ell} m_j x_j x_j^\top\right) I_{nv}\,. \end{aligned}$$ □

To illustrate this theorem, a GGS array of type $(2,2)$ and order 6 is constructed. The 2-circulant construction (see Example 4.12) gives a GGS array of type $(1,1)$ and order 2:

$$\begin{bmatrix} x_1 & rx_2^\top \\ -rx_2^\top & x_1 \end{bmatrix}.$$

The circulant matrices

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

satisfy $A_1 A_1^\top + A_2 A_2^\top = 2(x_1 x_1^\top + x_2 x_2^\top)I$. Following the replacements in the proof of Theorem 4.19, a GGS array of type (2, 2) and order 6 is obtained:

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

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

The existence of a GGS array clearly implies the existence of an orthogonal design of the same type and order, but the converse is false (see Remark 4.16). In many cases, however, the converse is true. An important fact is that every orthogonal design on 2-variables can be made into a GGS array by replacing the second variable $x_2$ by $rx_2^\top$. The following proposition gives some infinite families of GGS arrays with 4-variables.

**Proposition 4.2 (Eades).** *Suppose that $a$ is a positive integer and $I$ is a product of at least $a$ positive integers; that is, $\ell = \ell_1 \ell_2 \ldots \ell_j$ where $j \geq a$.*

*(a) If $\ell_1 \geq > 2$ for $1 \leq i \leq j$, then there is a GGS array of type $(2^a, 2^a, 2^a, 2^a)$ and order $4\ell$.*

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

*Proof.* For $\ell_1 \geq 2$ consider the sequences $a_l = (x_1, x_2, 0_{\ell_1-2})$, $a_2 = (x_1, -x_2, 0_{\ell_1-2})$, $a_3 = (x_3, -x_4, 0_{\ell_1-2})$, $a_4 = (x_3, x_4, 0_{\ell_1-2})$, where $0_{\ell_1-2}$ denotes a sequence of $0_{\ell_1-2}$ zeros. These sequences are complementary, and, further, if $A_i$ is the circulant matrix with first row $a_i$, then

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

Using Theorem 4.19 and the Goethals-Seidel array, a GGS array of type $(2,2,2,2)$ and order $4\ell_1$ may be obtained. Repeating this procedure $a$ times gives (a), For (b) the following complementary sequences may be used in a similar fashion:

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

$$(4,4,4,4) : (x_1,-x_2,-x_3,-x_4),(x_1,x_2,-x_3,x_4),(x_1,x_2,x_3,-x_4),$$
$$(x_1,-x_2,x_3,x_4)\,.\square$$

A numerical investigation of GGS arrays of order 12 has been made, and the results are listed in Eades [52], These GGS arrays have been used to construct orthogonal designs of orders 36 and 60.

GGS arrays with 2-variables have been used successfully for constructing orthogonal designs of highly composite orders congruent to 2 modulo 4. Examples are given later.

It seems that GGS arrays are the most powerful method for constructing orthogonal designs from circulants in orders not divisible by 8.

### *4.15.1 Some Infinite Families of Orthogonal Designs*

The Goethals-Seidel array and its generalizations have been used to construct many infinite families of orthogonal designs. The theorems below illustrate some of the techniques involved.

**Theorem 4.20 (Eades).** *If there is a GGS array of type $(s_1, s_2, \ldots, s_u)$ and order $n$, then there is an $OD(2n; s_1, s_1, s_2, s_2, \ldots, s_u, s_u)$.*

*Proof.* The negacyclic matrix

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

is an $OD(1,1)$. Hence

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

The combination of Theorem 4.20 and Proposition 4.2 gives a large collection of orthogonal designs. For example, for each $a > 0$ there is an $OD(8.5^a; 4^a, 4^a, 4^a, 4^a, 4^a, 4^a, 4^a, 4^a)$. □

**Theorem 4.21 (Eades).** *Suppose that $q$ is a prime power of the form $3m+1$. Then there is a skew symmetric weighing matrix of weight $q^2$ and order $\frac{4(q^2+q+1)}{3}$.*

This proof and additional theorems illustrating more of the techniques involved and their proofs appear explicitly in *Orthogonal Designs* (Ed. 1) p186-190.

### *4.15.2 Limitations*

*Remark 4.16.* There are two ways in which the use of GGS arrays for constructing orthogonal designs is limited.

First, little is known about the existence of GGS arrays. A numerical investigation of GGS arrays of order 12 shows that existence of a GGS array is harder to establish than existence of the corresponding orthogonal design. Further, it can be deduced from Theorem 4.20 that the number of variables of a GGS array of order $n$ is at most $[\frac{1}{2}\rho(2n)]$. If 8 divides $n$, then $[\frac{1}{2}\rho(2n)] < \rho(n)$, and so there are many orthogonal designs for which a corresponding GGS array does not exist. Note also that if 16 divides $n$, then $[\frac{1}{2}\rho(2n)] > 4$, but no GGS array with more than four variables is known.

Second, it can be proved that not all orthogonal designs can be constructed using GGS arrays. There is an orthogonal design of type (4,9) and order 14 (see Chapter 8). However, using the methods of Section 4.3, it can be shown that there is no $OD(14; 4, 9)$ constructed by using two $7 \times 7$ circulant matrices in the two-circulant construction.

## 4.16 Balanced Weighing Matrices

A most important concept in the design and analysis of experiments is that of a $(v, k, \lambda)$ configuration. This is equivalent to a $(0,1)$ matrix $A$ (the incidence matrix of the configuration) of order $v$ satisfying

$$AA^\top = (k-\lambda)I + \lambda J\,, \qquad AJ = JA = kJ, \tag{4.37}$$

where

$$\lambda(v-1) = k(k-1) \tag{4.38}$$

It is natural, then, to ask when such a matrix can be signed in order to produce a weighing matrix $M = W(v,k)$. The work of this section is due to Mullin [152, 153], and Mullin and Stanton [154, 155].

**Definition 4.23.** A *balanced weighing matrix* $M$ is a square $(0,1,-1)$ matrix such that squaring all its entries gives the incidence matrix of a $(v,k,\lambda)$ configuration. That is,

$$MM^{\top} = kI_v$$

and $A = M * M$ satisfies Equation (4.37) with $\lambda(v-1) = k(k-1)$. We write $M$ is a $BW(v,k)$.

**Remark** Although we will not study it here, balanced weighing matrices have proved most useful in providing previously unknown balanced incomplete block designs (see Mullin and Stanton [154, 155].

### *4.16.1 Necessary Conditions for the Existence of Balanced Weighing Matrices*

Since a $BW(v,k)$ implies the existence of a $(v,k,\lambda)$ configuration, the following conditions are known to be necessary:

(i) if $v$ is even, then $(k-\lambda)$ must be a perfect square;
(ii) if $v$ is odd, then the equation

$$x^2 = (k-\lambda)y^2 + (-1)[\frac{v-1}{2}]\lambda z^2 \tag{4.39}$$

must have a solution in integers other than $x = y = z = 0$. (See Ryser [171, p.111])

It is also trivial that for a $BW(v,k)$ to exist,

(iii) $\lambda = k\frac{(k-1)}{(v-1)}$ must be even.

Further we saw in Section 4.15 that for a $W(v,k)$ to exist,

(iv) if $v$ is odd, then $k$ must be a perfect square, and
(v) if $v$ is odd, then $(v-k)^2 - (v-k) + 2 > v$;

and in Chapter 2,

(vi) if $v = 2 \pmod 4$, then $k$ must be the sum of two squares.

In the event that $v \equiv 1 \pmod 4$, we note that (iv) is stronger than (ii) since if $k = \alpha^2$, then $x = \alpha$, $y = z = 1$, is a solution of equation (4.39), while for the parameters $v = 27$, $k = 13$, $\lambda = 6$ (4.39) has a solution, but $k$ is not a perfect square. (Just note that $\langle 7,6\rangle = \langle 1,42\rangle$, and so (4.39) has a rational, hence integral, solution.) For $v \equiv 3 \pmod 4$, (iv) implies that (v) has a solution if and only if $k-\lambda$ is the sum of two squares.

### 4.16.2 Construction Method for Balanced Weighing Designs

The direct sum of two matrices $W(n_1,k)$ and $W(n_2,k)$ is a $W(n_1+n_2,k)$, and the Kronecker product of matrices $W(n_1,k_1)$ and $W(n_2,k_2)$ is a $W(n_1n_2,k_1k_2)$, but this is not true for balanced weighing designs since in general the property of balance is lost under these operations. This fact alone makes the construction of balanced designs difficult. This is further emphasized by the fact that the conditions (i), (ii), and the condition that $(v-1)|k(k-1)$ need not hold in general for an unbalanced design. Here we discuss the generation of balanced weighing designs from group difference sets.

Let $G$ be a finite Abelian group of order $v$. If $G$ admits a difference set $D=\{d_1,d_2,\ldots,d_k\}$ then choose $M(\chi)$ (or $M$) to be a type 1 incidence matrix of $D$ obtained from the map $\chi$.

Strictly speaking, $M(\chi)$ is determined only up to a permutation of rows and columns, but this is in no way relevant to the present discussion. Type 1 matrices have an interesting property, which we now discuss.

**Definition 4.24.** Let $r_g$ denote the $g^{\text{th}}$ row of a type 1 incidence matrix $M$ defined on an Abelian group $G$. We say $M$ has the *invariant scalar product property* (ISP property) if for all $g$, $h$, $\theta \in G$,

$$r_g \cdot r_h = r_{g+\theta} \cdot r_{h+\theta}\,,$$

where $\cdot$ denotes the usual scalar product of vectors.

**Lemma 4.25.** *Any type 1 matrix defined by $\chi$ on $G$ has the ISP property.*

*Proof.* Note that

$$\begin{aligned} r_g \cdot r_h &= \sum_{k\in G} \chi^{(k-g)}\chi^{(k-h)} \\ &= \sum_{k\in G} \chi^{((k-\theta)-g)}\chi^{((k-\theta)-h)} \\ &= \sum_{k\in G} \chi^{(k-(g+\theta))}\chi^{((k-\theta)-h)} \\ &= r_{g+\theta} \cdot r_{h+\theta} \end{aligned}$$

as required. □

A similar result holds for column scalar products.

**Lemma 4.26.** *A type 1 $(0,1,-1)$ incidence matrix is a $W(v,k)$ matrix if and only if the following equation holds for all $g \in G$:*

$$\sum_{\theta \in G} \chi^{(\theta)} \chi^{(\theta+g)} = k\delta_{0,g}\,, \tag{4.40}$$

*where $\delta_{0,g}$ is the Kronecker delta.*

*Proof.* This is clear because of the ISP property

$$r_0 \cdot r_g = \sum_{\theta \in G} \chi^{(\theta)} \chi^{\theta - g)} = \sum_{\theta \in G} \chi^{\theta+g)} \chi^{(\theta)}\,. \qquad \square$$

The equality of these two summations is of practical importance since it saves calculation in verifying equation (4.39). In particular, if $v$ is odd, one need only check $\frac{(v-1)}{2}$ equations since the nonzero elements of $G$ can be partitioned into inverse pairs.

**Lemma 4.27.** *Let $D$ be a difference set in $G$. Let $M = M(\chi)$ be a type 1 $(0,1,-1)$ incidence matrix. Then $M * M$ is the incidence matrix of a $(v,k,\lambda)$ configuration if $\chi(g) = 0$ if and only if $g \in G - D$.*

*Proof.* This is evident. $\square$

**Definition 4.25.** We refer to a function $\chi$ satisfying the condition of Lemma 4.27 as a $D$-function. If the image of $\chi$ is $\{0,1,-1\}$, we call $\chi$ a restricted function. Putting these results together, we obtain:

**Theorem 4.22 (Mullin).** *There is a matrix $BW(v,k)$ if there is a $D$-function $\chi$ on an Abelian group of order $v$ such that*

$$\sum_{\theta \in G} \chi^{(\theta)} \chi^{(\theta+g)} = k\delta_{0,g}\,.$$

*This theorem can be used as a basis for a computer algorithm.*

For notational convenience, given a restricted function $\chi$ on an Abelian group $G$, we denote $\sum_{\theta \in G} \chi^{(\theta)} \chi^{(\theta+g)}$ by $F(\chi, g)$. We demonstrate a limitation of the construction of Theorem 4.22 in the next theorem. (This can also be obtained from Lemma 4.28.)

**Theorem 4.23 (Mullin).** *If there is a $D$-function $\chi$ in an Abelian group $G$ of order $v$ such that $F(\chi,g) = k\delta_{0,g}$ for all $g \in G$ and $v$ is even, then $\lambda = k\frac{(k-1)}{(v-1)}$ satisfies $\lambda \equiv 0 \pmod 4$.*

*Proof.* Since $v$ is even, there exists an element $\bar{g} \neq 0$ in $G$ such that $\bar{g} = -\bar{g}$. Let $(a_1,b_1)(a_2,b_2),\ldots,(a_t,b_t)$ be the pairs of elements of $D$ whose difference is $g$. Here $t = \frac{\lambda}{2}$, since if $a_i - b_i = \bar{g}$, then $b_i - a_i = \bar{g}$. Now consider

$$F(\chi, \bar{g}) = \sum_{\theta \in G} \chi^{(\theta)} \chi^{(\theta+\bar{g})}\,.$$

The only nonzero terms in this expression arise when both $\theta$ and $\theta + \bar{g}$ belong to $D$, since $\chi$ is a $D$-function. Thus

$$F(\chi, \bar{g}) = \sum_{i=1}^{t} [\chi(a_i)\chi(b_i) + \chi(b_i)\chi(a_i)]$$
$$= 2\sum_{i=1}^{t} \chi(a_i)\chi(b_i) = 0\,.$$

Since each of the $t$ terms in the latter sum is either 1 or -1, this expression must have $\frac{t}{2}$ terms of each value, and $t$ must be even. This shows that $\lambda \equiv 0 \mod 4$ as required. □

There is a $(4,3,2)$ configuration $C$ which is derivable from a difference set in the group of integers $\mod 4$; however, there is no $D$-function for any difference set which will produce a $BW(4,3)$. It is possible to sign the matrix of $C$ to produce an orthogonal matrix nonetheless. More generally, there is a cyclic $\left(\frac{(3^{2n}-1)}{2}, 3^{2n-1}, 2.3^{2n-2}\right)$ configuration (since this is the complementary configuration of the set of hyperplanes in $PG(2n-1,3)$), but there is no way of signing these matrices cyclically to make them orthogonal in view of Theorem 4.23. The results of Mullin show that all of these can be signed to produce orthogonal matrices. Not all incidence matrices of $(v,k,\lambda)$ configurations with $v$ even can be signed to produce orthogonal matrices. It can be shown that the matrix of the self-dual $(16,6,2)$ configuration cannot be signed (Schellenberg [175]).

We introduce new concepts which provide a labour-saving device in the calculation associated with Theorem 4.22 in some applications.

**Definition 4.26.** Let $R$ be a finite ring with unit. A restricted function $\chi$ on the additive group of $R$ with the property that $\chi^{(1)} = 1$ is called a *normal function*. Let $U(R)$ denote the group of units of $R$. Let $N(R,\chi) = N(\chi)$ be defined by $N(\chi) = \{g :\ g \in U(R) | \chi(g,\theta) = \chi(g)\chi(\theta),\ \forall \theta \in R\}$.

Because of the importance of $N(\chi)$ in the next theorem, we demonstrate a structural property of this set.

**Proposition 4.3.** *$N(\chi)$ is a subgroup of $U(R)$.*

*Proof.* Let $g$ and $h$ be members of $M(\chi)$. Then for every $\theta \in R$, $\chi(g^{h\theta}) = \chi^{(g)}\chi^{(h\theta)} = \chi^{(g)}\chi^{(h)}\chi^{(\theta)}$. Since $R$ is finite, the result follows. □

It is clear that $\chi$ is a linear representation of $N(\chi)$ under these circumstances.

**Theorem 4.24 (Mullin).** *Let $R$ be a finite ring with unit and $\chi$ a normal function on $R$. Let $M(\chi)$ be defined as above.*

*If $g \in N(\chi)$, then $F(\chi, g) = F(x, 1)$.*

*Proof.* $F(\chi,g)=\sum_{\theta\in R}\chi(\theta)\chi(\theta+g)$.

Let $\tau=g^{-1}\theta$ or equivalently $\theta=g\tau$. Then, since this mapping is $1-1$, we have

$$\begin{aligned}F(\chi,g)&=\sum_{\tau\in R}\chi^{(g\tau)}\chi^{(g\tau+g)}\\&=\sum_{\tau\in R}\chi^{(g\tau)}\chi^{(g(\tau+1))}\\&=\sum_{\tau\in R}(\chi^{(g)})^2\chi^{(\tau)}\chi^{(\tau+1)}\end{aligned}$$

Since $\chi^{(g)}\chi^{(g-1)}=\chi^{(1)}=1$, $\chi^{(g)}\neq 0$ and $(\chi^{(g)})^2=1$. This yields

$$F(\chi,g)=\sum_{\tau\in R}\chi^{(\tau)}\chi^{(\tau+1)}=F(\chi,1)\,.\square$$

As an application of this result, let us consider $G=GF(7)$. Let $\chi^{(0)}=-1$, $\chi^{(1)}=\chi^{(2)}=\chi^{(4)}=1$ and $\chi^{(3)}=\chi^{(5)}=\chi^{(6)}=0$. Since the field marks 1, 2 and 4 are the quadratic residues and since $7=3 \pmod 4$, $N(\chi)=(1,2,4)$. Now $F(\chi,2)=F(\chi,4)=F(\chi,1)=\chi^{(0)}\chi^{(1)}+\chi^{(1)}\chi^{(2)}=0$, and since $G=\{0\}\cup N(\chi)\cup -N(\chi)$, we have

$$F(\chi,g)=4\delta_{0,g}\,,\qquad g\in G\,.$$

Thus $M$ is a $W(7,4)$ matrix, But $\{0,1,2,4\}$ is a difference set, and therefore $M$ is also a $BW(7,4)$ matrix. Thus the vector

$$(\,\bar{1}\;1\;1\;0\;1\;0\;0\,)$$

when developed cyclically $\mod 7$, generates a $BW(7,4)$.

### *4.16.3 Regular Balanced Weighing Matrices*

**Definition 4.27.** If a $BW(v,k)$ matrix is such that the number of $-1$'s per row is constant, we say that it is *regular*.

In a $BW$ matrix we denote the number of $-1$'s per row by $a(-1)$ and the number of 1's per row by $a(1)$. Since if $M$ is regular, then $-M$ is also regular, we may assume that we are dealing with matrices for which $a(1)\geq\frac{k}{2}$. Clearly, every group-generated $BW(v,k)$ is regular, as is its transpose. Using this fact, Mullin [153] proved, using a somewhat different method, a generalization of a result of Schellenberg [175] which applies these to matrices $BW(v,k)$.

**Lemma 4.28 (Mullin).** *If a $W(v,k)$ matrix is a regular type 1 matrix, then $a(1)=(k\pm\sqrt{k})/2$ and $a(-1)=(k\pm\sqrt{k})/2$.*

*Proof.* The proof is a slight generalization of a result in Ryser [171, p.134]. Let $e = a(1) - a(-1)$, and $J$ denote the $v \times v$ matrix all of whose entries are 1. Clearly, we have

$$HJ = eJ = H^\top J\,,$$

and hence

$$HH^\top J = e^2 J = kJ\,.$$

Thus

$$\begin{aligned} &e^2 = k\,,\\ &a(1) + a(-l) = k\,,\\ &a(1) - a(-1) = \pm\sqrt{k}\,, \end{aligned}$$

and the result follows. □

**Corollary 4.22.** *If a $W(v,k)$ matrix is a regular type 1 matrix, then $k$ is a perfect square.*

**Corollary 4.23.** *If a $BW(v,k)$ matrix is a type 1 matrix, then $a(-1) \geq \frac{\lambda}{4}$ with equality if and only if $v = k = 4$.*

*Proof.* Let us first note that in any $BW(v,k)$ matrix, if $v = k$, then $k = \lambda$.

Now in any $BW(v,k)$ matrix, we observe that $4(v-k-1)+\lambda \geq 0$, with equality only for $v = k = \lambda = 4$. This is immediate from the fact that in any $(v,k,\lambda)$ configuration, as defined earlier, we have $v \geq k$ with equality only for $v = k = \lambda$.

The above inequality implies that the inequality

$$4(\lambda v - \lambda + k) - 4k\lambda + \lambda^2 \geq 4k$$

is also valid, with equality only for $v = k = \lambda = 4$. But by the definition of $\lambda$, we have

$$k^2 = \lambda v - \lambda + k\,,$$

and therefore

$$(2k - \lambda)^2 \geq 4k\,,$$

with equality as above.

Now let us assume that $a(-1) < \frac{\lambda}{4}$. Since

$$k + \frac{\lambda k}{2} > \frac{k}{2} \geq \frac{\lambda}{2}\,,$$

the corollary is true unless

$$a(-1) = \frac{(k - \sqrt{k})}{2}.$$

Let us assume that $\frac{(k-\sqrt{k})}{2} < \frac{\lambda}{4}$. Then

$$(2k - \lambda)^2 \leq 4k,$$

which is impossible unless equality holds in which case $v = k = \lambda$ as required.

The design generated by

$$(-1, 1, 1, 1) \bmod 4$$

satisfies the corollary with equality. □

### *4.16.4 Application of the Frobenius Group Determinant Theorem to Balanced Weighing Matrices*

For the theory of group characters, the reader is referred to Speiser [196]. For Abelian groups, the Frobenius group determinant theorem (Speiser [196, p.178]), in the notation employed here, becomes the following:

**Theorem 4.25 (Frobenius Group Determinant Theorem).** *Let $M$ be a type 1 matrix over an Abelian group $G$ of order $v$. Then*

$$\det M(\chi) = \prod_{j=1}^{v} \sum_{g \in G} \alpha^{(j)}(g)\chi(g),$$

*where $\alpha^{(j)}$ denotes the $j^{th}$ irreducible character of $G$.*

For the cyclic group of order $v$ (written as the residues modulo $v$), this becomes

$$\det M(\chi) = \prod_{j=0}^{v-1} \sum_{k=0}^{v-1} \omega^{jk}\chi(k),$$

where $\omega$ is a primitive $v^{\text{th}}$ root of unity.

Any group $G$ of order $v$ admits the main character

$$a^{(1)}(g) = 1, \quad g \in G.$$

Every group determinant can be factored into forms in the indeterminates $\chi(g)$, which are irreducible over the integers, since it is clear that the expansion of the group determinant is a form with integer coefficients.

To illustrate the use of this theorem, we tackle the problem of finding a cyclic $BW(10, 9)$ matrix $M$. Using the integers mod 10, we can, without loss

of generality, assume that $\chi(g) = 0$ if and only if $g = 0$. Without any further theory, except for Lemma 4.28, there are $\binom{9}{3} = 84$ functions $\chi$ to consider. By the Frobenius group determinant theorem,

$$G(\chi) = \sum_{j=1}^{9} (-1)^j \chi(j),$$

corresponding to the character $\alpha$ defined by $\alpha(j) = (-1)^j$, is a divisor of $\det M = 3^{10}$.

Now let $c$ denote the number of even residues $j$ such that $\chi(j) = -1$. Then $G(\chi)$ can be determined in terms of $c$ as follows:

| $c$ | $G(\chi)$ |
|---|---|
| 0 | 6 |
| 1 | 1 |
| 2 | −3 |
| 3 | −7. |

There are 40 functions with $c = 1$ and 30 with $c = 2$; therefore, the number of functions to be investigated has been reduced. Moreover, we have some structural information. As we shall see, the structural information is extremely important. In the following, if $\chi(g) = x$, we say that $x$ appears in position $g$.

We note now that the inner product of absolute values of any pair of distinct rows is 8, since $\lambda = 8$ in the associated symmetric design. Thus the number of terms with value $-1$ in $r_0 \cdot r_j$ must be 4 for $j = 1, 2, \ldots, 9$.

In particular, this means that in $r_0$ and $r_j$ the number of times 0 opposes $-1$ must be even, that is, 0 or 2. Hence if translation (of row 0) by $j$ units moves 0 to a position containing $-1$, then there must be a $-1$ in position $-j$ which is translated to column zero. Thus $-1$'s occur in pairs of inverse positions.

Now let us consider the case of $c = 2$. There is exactly one $-1$ on an odd residue. But since the parity of inverse pairs is equal, this $-1$ must be in position 5; that is, $\chi(5) = 1$. Now it is easily verified (considering row 1) that the three $-1$'s cannot be consecutive in any event, and thus the remaining $-1$'s occur in inverse pairs of positions $\chi(4) = \chi(6) = 1$. Also since $c = 2$, $\chi(1) = \chi(3) = \chi(7) = \chi(9) = 1$, and $\chi(2) = \chi(8) = -1$. We have determined the only possible function $\chi$ with $c = 2$. However, for this function $r_0 \cdot r_1 = -4$, and the matrix is not orthogonal.

Let us now consider the case $c = 1$. Clearly, no solution exists in this case since there is only one self-inverse element 5, which is odd. Hence there is no cyclic $BW(10, 9)$ matrix.

### 4.16.5 Balanced Weighing Matrices with $v \leq 25$

**Comment 4.1.** In Table 4.18 we give a list of all triples $v$, $k$, $\lambda$ with $k > \lambda > 0$ which satisfy $\lambda(v-1) = k(k-1)$ and $\lambda \equiv 0 \bmod 2$. We also list a function $E(v,k) = E$ where $E(v,k) = 1$ if a matrix $B(v,k)$ exists, and $E(v,k) = 0$ otherwise. In this regard it is useful to note that the matrices $BW(4n, 4n-1)$ are coexistent with skew Hadamard matrices of order $4n$ and that matrices $BW(4n+2, 4n+1)$ are coexistent with symmetric Hadamard matrices. The list of values for which such designs are known to exist are listed in Wallis [231].

**Table 4.18** triples $v, k, \lambda$ with $k > \lambda > 0$ satisfying $\lambda(v-1) = k(k-1)$ and $\lambda \equiv 0 \mod 2$.

| | $v$ | $k$ | $\lambda$ | E | Reason or Reference |
|---|---|---|---|---|---|
| 1) | 4 | 3 | 2 | yes | Mullin |
| 2) | 6 | 5 | 4 | yes | *, Complement $PG(1,5)$ |
| 3) | 7 | 4 | 2 | yes | Circulant with first row [−110100]. |
| 4) | 8 | 7 | 6 | yes | *, Complement $PG(1,7)$. |
| 5) | 10 | 9 | 8 | yes | *, Complement $PG(1,9)$. |
| 6) | 11 | 5 | 2 | no | Condition (iv). |
| 7) | 12 | 11 | 10 | yes | *, Complement $PG(1,11)$. |
| 8) | 13 | 9 | 4 | yes | Condition (v). |
| 9) | 14 | 13 | 12 | no | *, Complement $PG(1,13)$. |
| 10) | 15 | 8 | 4 | no | Condition (iv). |
| 11) | 16 | 6 | 2 | no | Schellenberg |
| 12) | 16 | 10 | 6 | | |
| 13) | 16 | 15 | 14 | yes | * |
| 14) | 18 | 17 | 16 | yes | *, Complement $PG(1,17)$, |
| 15) | 19 | 9 | 4 | | |
| 16) | 20 | 19 | 18 | yes | *, Complement $PG(1,19)$. |
| 17) | 21 | 16 | 12 | yes | *, Complement $PG(2,4)$. |
| 18) | 22 | 7 | 2 | no | Condition (i). |
| 19) | 22 | 15 | 10 | no | Condition (i). |
| 20) | 22 | 21 | 20 | no | Condition (vi). |
| 21) | 23 | 12 | 6 | no | Condition (iv). |
| 22) | 24 | 23 | 22 | yes | *, Complement $PG(1,23)$. |
| 23) | 25 | 16 | 10 | | |

*see Comment 4.1

In view of our earlier remarks about the usefulness of $BW(v,k)$'s it would be of interest to establish the existence of more of these matrices. This will now be discussed.

### 4.16.6 There are No Circulant Balanced Weighing Matrices $BW(v,v-1)$ Based on $(v,v-1,v-2)$ Configurations

Without loss of generality we assume that in such matrices the element 0 occurs down the main diagonal.

**Lemma 4.29.** *In any circulant orthogonal matrix based on a $(v,k,\lambda)$ configuration, the parameter $k$ is a perfect square.*

*Proof.* Suppose that the first row of the orthogonal matrix contains a entries of 1 and $b$ entries of $-1$. By the circulant property, every row and column has sum $a-b$. If the matrix is denoted by $N$, we have

$$NJ = N^\top J = (a-b)J\,.$$

But

$$NN^\top = kI\,.$$

Hence

$$NN^\top J = kIJ = kJ\,.$$

But

$$NN^\top J = N(a-b)J = (a-b)^2 J\,.$$

Thus

$$k = (a-b)^2\,. \qquad \square$$

In the following we assume without loss of generality that $a > b$; otherwise we multiply the entire matrix by $-1$. For convenience we set $a-b=t$.

**Lemma 4.30.** *If $a$ denotes the number of 1's in the first row of an orthogonal circulant matrix, and $b$ the number of $-1$'s, then*

$$a = \tfrac{1}{2}\left(t^2+t\right) \text{ and } b = \tfrac{1}{2}\left(t^2-t\right)\,.$$

*Proof.* This is immediate since

$$\begin{aligned} a+b &= k = t^2 \\ a-b &= t\,. \end{aligned}$$

Thus in looking for circulant orthogonal matrices based on trivial designs, we need only consider $(t^2+1, t^2, t^2-1)$ configurations where $t$ is odd. □

**Definition 4.28.** An orthogonal circulant based on a $(t^2+1, t^2, t^2-1)$ configuration will henceforth be called a *trivial circulant*.

Let $x_{\alpha\beta}$ $(\alpha, \beta = 0, 1, 2)$ represent the number of times that $\alpha$ in row $i$ is in the same column as $\beta$ in row $j$ (we use 2 to represent the entry $-1$). We require

**Lemma 4.31.** *Either* $x_{01} = x_{10} = 1$, $x_{02} = x_{20} = 0$, *or vice versa.*

*Proof.* We actually determine all $x_{\alpha\beta}$. It is clear that

$$\text{i)} \qquad \sum x_{\alpha\beta} = t^2 + 1,$$

$$\text{ii)} \qquad \sum x_{0j} = \sum x_{i0} = 1,$$

$$\text{iii)} \qquad \sum x_{1j} = \sum x_{i1} = \frac{1}{2}(t^2 + t)$$

$$\text{iv)} \qquad \sum x_{2j} = \sum x_{i2} = \frac{1}{2}(t^2 - t)$$

Finally, orthogonality gives

$$\text{v)} \qquad x_{11} + x_{22} = x_{12} + x_{21}.$$

But $x_{11} + x_{22} + x_{12} + x_{21} = \lambda$, and thus each expression in v) equals $\frac{1}{2}(t^2-1)$. From iii) and iv), addition gives

$$x_{10} + x_{20} = 1 = x_{01} + x_{02}\,; x_{00} = 0\,.$$

Also

$$x_{10} - x_{01} = x_{02} - x_{20} = x_{21} - x_{12} = \text{ an even number.}$$

This proves that $x_{10} = x_{01}$, $x_{02} = x_{20}$, as required. It is useful to record the table of values following. □

| | Case $A$ | Case $B$ |
|---|---|---|
| $x_{00}$ | 0 | 0 |
| $x_{01} = X_{10}$ | 1 | 0 |
| $x_{02} = X_{20}$ | 0 | 1 |
| $x_{12} = X_{21}$ | $\frac{1}{4}t^2 - 1$ | $\frac{1}{4}t^2 - 1$ |
| $x_{11}$ | $\frac{1}{4}(t+3)(t-1)$ | $\frac{1}{4}(t-1)^2$ |
| $x_{22}$ | $\frac{1}{4}(t+1)^2$ | $\frac{1}{4}(t-3)(t+1)$ |

In the light of Lemma 4.31, we note that we can write $v = 4m+2$, $k = 4m+1 = t$, $\lambda = 4m$, and the typical circulant has the following form (illustration for $m = 6$).

$$\text{Row 1:} \quad 0a_1a_2 \ldots a_{11}a_{12}\theta a_{12}a_{11} \ldots a_3a_2a_1$$

(The symmetry of the sequence is guaranteed by the fact that $0x_{0i} = x_{i0}$ for $i = 1, 2$.)

Row $j$ is obtained by a cyclic shift through $j-1$ places to the right.

We now prove:

**Lemma 4.32.** $\theta = 1$ *if* $t \equiv 1 \pmod 4$; $\theta = -1$ *if* $t \equiv 3 \pmod 4$. *Also*

$$\sum_{j=1}^{m} a_{2j} = 0, \qquad \sum_{i=0}^{m-1} a_{2i+1} = \frac{t-\theta}{2}$$

*Proof.* Take the scalar products of row 1 with rows $2, 4, 6, \ldots 2m+2$; add, and re-arrange. We have

$$2(a_1 + a_3 + \cdots + a_{2m-1})(a_2 + a_4 + \cdots + a_{2m}) + \theta(a_2 + a_4 + \cdots + a_{2m}) = 0.$$

Thus

$$(2a_1 + \cdots + 2a_{2m-1} + \theta)(a_2 + a_4 + \cdots + a_{2m}) = 0;$$

Thus since only the second integer is even, we get $\sum a_{2j} = 0$. Also, since $2\sum a_{2n} + 2\sum a_{2j} + \theta = t$, we find that $\sum a_{2i} = \frac{t-\theta}{2}$.

Finally, note that the sum $\sum a_{2i}$ is an even integer ($m$ terms); thus $t - \theta$ is divisible by 4, and $\theta = 1$ for $t \equiv 1 \pmod 4$, $\theta = -1$ for $t \equiv 3 \pmod 4$. This completes the proof. □

Actually, if one takes scalar products of row 1 with rows $3, 5, \ldots, 2m+1$, and adds, one gets the identity

$$\left(\sum a_{2i}\right)\left(\sum a_{2i} + \theta\right) + \left(\sum a_{2j}\right)^2 = m,$$

which also produces the desired results.

*Example 4.25.* At this stage, it is most instructive to look at the example for $m = 6$, The scalar products for rows $2, 4, 6, 8, 10, 12$ are written down as follows.

1) $\displaystyle\sum_{i=1}^{12} a_i a_{i+1} = 0 \, (a_{13} = \theta)$.

In the sequence $a_l, a_2, a_3, \ldots, a_{13}$ there must be exactly six sign changes to produce a zero sum in 1). Hence $a_1$ has the same sign as $a_{13}$; that is,

2) $a_1a_2 + \sum_1^{10} a_i a_{i+3} + a_{11}a_{12} = 0\,.$

Write the sequence

$$a_3, a_6, a_9, a_{12}, a_{11}, a_8, a_5, a_2, a_1, a_4, a_7, a_{10}, a_{13}\,.$$

By the same argument, $a_3 = 0$.

3) $a_1a_4 + a_2a_3 + \sum_1^{8} a_i a_{i+5} + a_9a_{12} + a_{10}a_{11} = 0\,.$

Consider the sequence

$$a_5, a_{10}, a_{11}, a_6, a_1, a_4, a_9, a_{12}, a_7, a_2, a_3, a_8, \theta\,,$$

and we get $a_5 = 0$.

4) $a_1a_6 + a_2a_5 + a_3a_5 + \sum_1^{6} a_i a_{i+7} + a_7a_{12} + a_9a_{10} = 0\,.$

The relevant sequence is

$$a_7, a_{12}, a_5, a_2, a_9, a_{10}, a_3, a_4, a_{11}, a_8, a_1, a_6, \theta\,,$$

and the result is $a_7 = 0$.

5) $a_1a_8 + a_2a_7 + a_3a_6 + a_4a_5 + \sum_1^{4} a_i a_{i+9} + a_5a_{12} + a_6a_{11} + a_7a_{10} + a_8a_9 = 0\,.$

Hence, the sequence

$$a_9, a_8, a_1, a_{10}, a_7, a_2, a_{11}, a_6, a_3, a_{12}, a_5, a_4, \theta \quad \text{proves } a_9 = 0\,.$$

Similarly, $a_{11} = \theta$, and $\sum a_{2i+1} = 6\theta = 6$ (a contradiction of Lemma 4.32).

The method outlined is completely general and gives:

**Lemma 4.33.** *In an orthogonal circulant of the type we have been considering, with one zero per row, we have*

$$a_1 = a_3 = \cdots = a_{2m-1} = \theta\,.$$

*Thus*

$$\sum a_{2i+1} = m\theta = \tfrac{1}{2}\,(t - \theta)\,.$$

It is easy to deduce, from Lemma 4.33, that

$$t = \theta(2m+1)\,.$$

But $t^2 = 4m+1$, and so $4m+1 = (2m+1)^2$.

We conclude that $m = 0$ and state:

**Theorem 4.26.** *An orthogonal circulant with one zero per row only exists for $m = 0$; in this case, it is the identity matrix of order 2 or, equivalently, the transposition matrix of order 2.*

## 4.17 Negacyclic Matrices

A type of weighing matrix, of weight $n$ and weight $n-1$, called a $C$-matrix or conference matrix, was previously studied by Delsarte-Goethals-Seidel [39]. These can be based on circulant or on negacyclic matrices. We consider these negacyclic based matrices with weight $k \leq n$.

**Definition 4.29.** Let $P$, called the "negacyclic shift matrix" be the square matrix of order $n$, whose elements $p_{ij}$ are defined as follows:

$$\begin{aligned} p_{i,i+1} &= 1, \quad i = 0,1,\ldots,n-2, \\ p_{n-1,0} &= -1, \\ p_{ij} &= 0, \quad \text{otherwise.} \end{aligned}$$

Any matrix of the form $\sum a_i P^i$, with $a_i$ commuting coefficients, will be called *negacyclic*.

We see there are similarities but not necessarily sameness between the properties of circulant/cyclic matrices and negacyclic matrices.

**Lemma 4.34.** *Let $P = (p_{ij})$ of order $n$ be a negacyclic matrix. Then*

*(i) The inner product of the first row of $P$ with the $i^{th}$ row of $P$ equals the negative of the inner product of the first row of $P$ with the $(-i+2)^{nd}$ row. That is*

$$\sum_{j=1}^{n} p_{1j}p_{ij} = -\sum_{j=1}^{n} p_{1j}p_{n-i+2,j} \tag{4.41}$$

*(This is the negative of the result for circulant/cyclic matrices).*

*(ii) The inner product of the first row of $P$ with the $i^{th}$ row of $P$ equals the inner product of the $k^{th}$ row of $P$ with the $(i+k-1)^{st}$ row of $P$. That is*

$$\sum_{j=1}^{n} p_{1j}p_{ij} = \sum_{j=1}^{n} p_{jk}p_{i+k-1,j} \tag{4.42}$$

*(This is the same result as for circulant/cyclic matrices).*

*(iii) Then $P$ of order $n$ satisfies*

$$P^n = -1, \quad P^\top = -P^{n-1}, \quad PP^\top = I.$$

*If $A = \sum a_i P^i$, $B = \sum b_j P^j$ and $R$ is the back diagonal matrix, then*

$$AB = BA \ \text{ and } \ A(BR)^\top = BRA^\top.$$

$A$ and $BR$ are amicable matrices.

We now note some other properties of negacyclic matrices which were shown by L.G. Kovacs and Peter Eades [52]. The second result appears in Geramita and Seberry [80, p.206–207]. We give the proof here to emphasize a result which appears to have been forgotten.

**Lemma 4.35.** *If $A = \sum a_i P^i$ is a negacyclic matrix of odd order $n$, then $XAX$, where $X = diag(1,-1,1,-1,\ldots,1)$, is a circulant matrix.*

**Lemma 4.36.** *Suppose $n \equiv 0 \pmod 2$. The existence of a negacyclic $C = W(n,n-1)$ is equivalent to the existence of a $W(n,n-1)$ of the form*

$$\begin{bmatrix} A & B \\ B^\top & -A^\top \end{bmatrix} \tag{4.43}$$

*where $A$ and $B$ are negacyclic, $A^\top = (-1)A^{n/2}A$. That is the 2-block suitable matrix gives a weighing matrix which is equivalent to a 1-block matrix.*

*Proof.* First we suppose there is a negacyclic matrix $N = W(2n,2n-1)$ of order 2 which is used to form two negacyclic matrices $A$ and $B$ of order $n$ which satisfy

$$AA^\top + BB^\top = (2n-1)I. \tag{4.44}$$

Let the first row of the negacyclic matrix $N$ be

$$0x_1y_1x_2y_2\ldots y_{n-1}x_n$$

We choose $A$ and $B$ to be negacyclic matrices with first rows

$$0y_1y_2\ldots y_{n-1}, \text{ and } x_1x_2\ldots x_n,$$

respectively. If the order $n = 2t+1$ is odd and the first rows of $A$ and $B$ are

$$0a_1\ldots a_t\,(\epsilon_t a_t)\ldots(\epsilon_1 a_1) \text{ and } 1b_1b_2\ldots b_t\,(\delta_t b_t)\ldots(\delta_1 b_1),$$

with $\epsilon_i = \pm 1$, $\delta_j = \pm 1$, then taking the dot product of the first and $(i+1)^{\text{th}}$ rows, $i \le t$ (reducing using $xy \equiv x+y-1 \pmod 4$), we obtain

$$2t-2i+\epsilon_i \pmod 4 \text{ and } 2t-2i+1 \pmod 4,$$

respectively. Hence using equation (4.44),

$$\epsilon_i + 1 \equiv 0 \pmod 4,$$

we have $\epsilon_i = -1$.

If the order $n$ is even and the first rows of $A$ and $B$ are

$$0a_1 \dots a_{t-1} a_t (\epsilon_{t-1} a_{t-1}) \dots (\epsilon_1 a_1)$$

and

$$1b_1 b_2 \dots b_t (\delta_{t-1} b_{t-1}) \dots (\delta_1 b_1),$$

with $\epsilon_i = \pm 1$, $\delta_j = \pm 1$, then taking the dot product of the first and $(\mathrm{i}+1)^{\mathrm{th}}$ rows, $i \le t-1$ (reducing modulo 4), we obtain

$$2t - 2t - 1 + \epsilon_i \pmod 4 \text{ and } 2t - 2i + 2b_i - 2 \pmod 4,$$

respectively. Hence, using equation (4.44),

$$\epsilon_i + 2b_i - 3 \equiv 0 \pmod 4,$$

and since $b_i \neq 0$, we have $\epsilon_i = 1$.

This means the first row of the original negacyclic matrix of order $2n$ can be written as

$$0x_1 a_1 x_2 a_2 \dots x_t a_t 1 \bar{a}_t (\delta_t x_t) \bar{a}_{t-1} \dots \bar{a}_2 (\delta_2 x_2) \bar{a}_1 (\delta_1 x_1) \text{ for } n \text{ odd}$$

and

$$0x_1 a_1 x_2 a_2 \dots a_{t-1} x_t a_t (\delta_t x_t) a_{t-1} \dots a_2 (\delta_2 x_2) a_1 (\delta_1 x_1) \text{ for } n \text{ even}$$

with $\delta_j \neq \pm 1$ and $\bar{a}_i = -a_i$.

The inner product of the first and $(2i-1)^{\mathrm{th}}$ rows, $i \le t$ and $t-1$ respectively, is

$$-\delta_i + 1 \equiv 0 \pmod 4 \text{ and } \delta_i + 1 \equiv 0 \pmod 4.$$

So we have the first rows of $A$ and $B$

$$0a_1 \dots a_t \bar{a}_t \dots \bar{a}_1 \text{ and } b_1 b_2, \dots b_t 1 b_t \dots b_2 b_1 \text{ for } n \text{ odd} \tag{4.45}$$

and

$$0a_1 \dots a_{t-1} a_t a_{t-1} \dots a_1 \text{ and } b_1 b_2 \dots b_t \bar{b}_t \dots \bar{b}_2 \bar{b}_1 \text{ for } n \text{ even} \tag{4.46}$$

as required.

It is straightforward to check that negacyclic matrices $A$ and $B$, which satisfy $AA^\top + BB^\top = (2n-1)I_n$ and are of the form (4.45) and (4.46), give a negacyclic matrix $W(2n, 2n-1)$ when formed into first rows

$$0b_1 a_1 b_2 \dots b_t a_t 1 \bar{a}_t b_t \dots \bar{a}_l b_1, \text{ for } n \text{ odd},$$

or

$$0b_1a_1b_2\ldots b_ta_t\bar{b}_t\ldots a_1\bar{b}_1 \text{ for } n \text{ even.}\square$$

*Example 4.26.* The first rows of negacyclic matrices $(n, n-1)$ of orders 4, 6, 8, and 10, respectively;

$$\begin{array}{l} 0\,1\,1\,-, \\ 0\,1\,-\,1\,1\,1 \\ 0\,1\,1\,-\,1\,1\,1\,- \\ 0\,1\,1\,-\,1\,-\,-\,-\,-\,1. \end{array}$$

are equivalent to the existence of

$$\begin{bmatrix} 0 & 1 \\ - & 0 \end{bmatrix}, \begin{bmatrix} 1 & - \\ 1 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & - & 1 \\ - & 0 & - \\ 1 & - & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ - & 1 & 1 \\ - & - & 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ - & 0 & 1 & 1 \\ - & - & 0 & 1 \\ - & - & - & 0 \end{bmatrix}, \begin{bmatrix} 1 & - & 1 & - \\ 1 & 1 & - & 1 \\ - & 1 & 1 & - \\ 1 & - & 1 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 1 & 1 & - & - \\ 1 & 0 & 1 & 1 & - \\ 1 & 1 & 0 & 1 & 1 \\ - & 1 & 1 & 0 & 1 \\ - & - & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & - & - & - & 1 \\ - & 1 & - & - & - \\ 1 & - & 1 & - & - \\ 1 & 1 & - & 1 & - \\ 1 & 1 & 1 & - & 1 \end{bmatrix}$$

**Comment**. Peter Eades [52] and Delsarte-Goethals-Seidel [39] have determined that the only negacyclic $W(v, v-1)$ of order $v < 1000$ have $v = p^r + 1$ where $p^r$ is an odd prime power. On the positive side we know (we omit the proof):

**Theorem 4.27 (Delsarte-Goethals-Seidel [39]).** *There is a negacyclic $W(p^r+1, p^r)$ whenever $p^r$ is an odd prime power.*

G. Berman [21] has led us to believe that many results of a similar type to those found for circulant matrices can be obtained using negacyclic matrices. Negacyclic matrices are curiosities because of their properties and potential exhibited in Lemma 4.36 and Example 4.27.

*Example 4.27.* The four negacyclic matrices

$$A_1 = \begin{bmatrix} 1 & - & 0 & 0 & 0 \\ 0 & 1 & - & 0 & 0 \\ 0 & 0 & 1 & - & 0 \\ 0 & 0 & 0 & 1 & - \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix} \quad A_2 = \begin{bmatrix} 1 & 1 & - & - & 0 \\ 0 & 1 & 1 & - & - \\ 1 & 0 & 1 & 1 & - \\ 1 & 1 & 0 & 1 & 1 \\ - & 1 & 1 & 0 & 1 \end{bmatrix}$$

$$A_3 = \begin{bmatrix} 0 & - & 0 & 0 & 1 \\ - & 0 & - & 0 & 0 \\ 0 & - & 0 & - & 0 \\ 0 & 0 & - & 0 & - \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad A_4 = \begin{bmatrix} 0 & - & 0 & 0 & 0 \\ 0 & 0 & - & 0 & 0 \\ 0 & 0 & 0 & - & 0 \\ 0 & 0 & 0 & 0 & - \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

satisfy

$$A_1A_1^\top + A_2A_2^\top + A_3A_3^\top + A_4A_4^\top = 9I\,.$$

They can be merged to form two negacyclic matrices

$$B_1 = \begin{bmatrix} 1\ 0\ -\ -\ 0\ 0\ 0\ 0\ 0\ 1 \\ -\ 1\ 0\ -\ -\ 0\ 0\ 0\ 0\ 0 \\ \text{etc.} \end{bmatrix}$$

$$B_2 = \begin{bmatrix} 1\ 0\ 1\ -\ -\ 0\ -\ 0\ 0\ 0 \\ 0\ 1\ 0\ 1\ -\ -\ 0\ -\ 0\ 0 \\ \text{etc.} \end{bmatrix}$$

which satisfy

$$B_1B_1^\top + B_2B_2^\top = 9I\,.$$

These can be further merged to obtain the first row of a negacyclic $W(20,9)$:

$$1\ \ 1\ \ 0\ \ 0\ \ -\ \ 1\ \ -\ \ -\ \ 0\ \ -\ \ 0\ \ 0\ \ 0\ \ -\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0.$$

Negacyclic matrices are worthy of further existence searches. The question of when negacyclic matrices can be decomposed as in Example 4.27 is open for further research.

### *4.17.1 Constructions*

We recall suitable (plug-in) matrices $X_1, X_2, X_3, X_4, \cdots X_t$ are $t$ matrices of order $n$, with elements $\pm 1$ which satisfy the additive property, $\sum_{i=1}^{t} X_i X_i^\top =$ constant times the identity matrix. They are suitable if they satisfy other equations which enable them to be substituted into a plug-into array to make an orthogonal matrix (see Definition 4.4). Xia, Xia and Seberry [251] show 4-suitable plug-in negacyclic matrices of odd order exist if and only if 4-suitable plug-in circulant matrices exist for the same odd order. 4-suitable negacyclic matrices of order $n$, may be used instead of 4-suitable circulant matrices, in the Goethals-Seidel plug-into array [88], to construct Hadamard matrices and orthogonal designs of order $4n$. Other useful plug-into arrays are due to Kharaghani, Ito, Spence, Seberry-Balonin and Wallis-Whiteman [114, 115, 120, 182, 198, 241].

In computer searches, for some even orders, 2-suitable or 4-suitable negacyclic matrices have proved easier to find. This experimental fact has been used extensively by Holzmann, Kharaghani and Tayfeh-Rezaie [66, 67, 104, 105, 122] to complete searches for $OD$'s in orders 24, 46, 48, 56, and 80. We note that if there are 2-suitable negacyclic matrices of order $n$ and Golay sequences of order $m$, there are 2-suitable matrices of order $mn$.

This means a negacyclic matrix may give 2-suitable and 4-suitable plug-in matrices to use in plug-into arrays to make larger orthogonal matrices.

From Table 4.19 there exist $W(12,k)$ constructed using two negacyclic matrices of order 6 for $k = 1,2,\ldots,12$. From Delsarte-Goethals-Seidel [39], there exists $0,\pm 1$ negacyclic $W(12,11)$. Results for 7, 9, and 11 are due to Gene Awyzio [13] and Tianbing Xia [250].

**Table 4.19** First rows of $W(12,k)$ constructed from two negacyclic matrices of order 6 [a]

| $k$ | First Rows | $k$ | First Rows |
|---|---|---|---|
| 1 | $1\,0\,0\,0\,0\,0\,;\,0_6$ | 7 | $0\,1\,1\,1\,-\,1\,;\,1\,0\,0\,1\,0\,0$ |
| 2 | $1\,0_5\,;\,1\,0_5$ | 8 | $1\,1\,-\,1\,0_2\,;\,1\,1\,1\,-\,0_2$ |
| 3 | $1\,0\,0\,1\,0\,;\,1\,0_5$ | 9 | $0\,1\,1\,-\,1\,1\,;\,1\,0\,1\,-\,0\,-$ |
| 4 | $1\,1\,0_4\,;\,1\,-\,0_4$ | 10 | $0\,1\,1\,1\,-\,1\,;\,0\,1\,1\,1\,-\,1$ |
| 5 | $1\,1\,-\,0_3\,;\,1\,0\,1\,0_3$ | 11 | $0\,1\,1\,-\,1\,1\,;\,1\,-\,1\,1\,1\,1$ |
| 6 | $0\,1\,1\,1\,-\,1\,;\,1\,0_5$ | 12 | $1\,1\,1\,1\,-\,1\,;\,-\,1\,1\,1\,-\,1$ |

[a] G. Awyzio [13] and T. Xia [250]

*Remark 4.17.* The question of which $W(4n,k)$ can be constructed using two negacyclic $0,\pm 1$ matrices of order $2n$ has yet to be resolved.

It is easy to see that there exist $W(2n,k)$ constructed from 2 negacyclic matrices of order $n$ whenever there exist two 0, $\pm 1$ sequences of length $n$ and weight $k$ with NPAF zero.

Using results obtained by Awyzio (private communication) and Tianbing Xia (private communication) we conjecture:

*Conjecture 4.5.* Suppose $n$, $n \equiv 2 \pmod 4$ and $k$, the sum of two squares, are integers. Then there exists a $W(2n,k)$ constructed via two negacyclic $(0,1,-1)$ matrices.

## *4.17.2 Applications*

In Ang et al [8], 4-suitable negacyclic matrices are used to construct new orthogonal bipolar spreading sequences for any length 4 (mod 8) where the resultant sets of sequences possess very good autocorrelation properties that make them amenable to synchronization requirements. In particular, their aperiodic autocorrelation characteristics are very good.

It is well known, e.g. [222, 249], that if the sequences have good aperiodic cross-correlation properties, the transmission performance can be improved for those CDMA systems where different propagation delays exist.

Orthogonal bipolar sequences are of a great practical interest for the current and future direct sequence (DS) code-division multiple-access (CDMA) systems where the orthogonality principle can be used for channels separation, e.g. [8]. The most commonly used sets of bipolar sequences are Walsh-Hadamard sequences [222], as they are easy to generate and simple to implement. However, they exist only for sequence lengths which are an integer power of 2, which can be a limiting factor in some applications. The overall autocorrelation properties of the modified sequence sets are still significantly better than those of Walsh-Hadamard sequences of comparable lengths.

### *4.17.3 Combinatorial Applications*

For combinatorial applications see [21, 22, 89, 117, 121].

We also see from papers [100, 102, 104, 105] that OD's in orders 24, 40, 48, 56, 80, that had proved difficult to constructed using circulant matrices were found using negacyclic matrices.