

COMBINATORIAL MATRICES

Jennifer Wallis, B.Sc.(N.S.W.), M.Sc.(La Trobe)

Submitted in complete fulfilment of the requirements for the degree of Doctor of Philosophy in the Department of Mathematics, School of Physical Sciences, La Trobe University.

March 1970

CONTENTS

INTRODUCTION.	5
CHAPTER I : Preliminaries	
1.1 Quadratic Residues	9
1.2 The Legendre Symbol $\chi(b)$	10
1.3 The Kronecker Product	10
1.4 Galois Fields $GF(p^r)$	11
CHAPTER II : Block Designs, Difference Sets, Circulant Matrices and Hadamard Matrices	
2.1 Block Designs- (b,v,r,k,λ) -configurations	14
2.2 Block Designs- (v,k,λ) -configurations	16
2.3 Difference Sets	17
2.4 Circulant Matrices	19
2.5 Table of Matrix Equations Satisfied by Known Difference Sets and (v,k,λ) -configurations	20
2.6 Hadamard Matrices	23
2.7 Skew-Hadamard Matrices and m -type Matrices	24
2.8 n - type Matrices	28
2.9 Known Classes of Symmetric Hadamard Matrices	30
2.10 Known Classes of Hadamard Matrices	32
CHAPTER III : Matrix Equivalence	
3.1 Equivalence of Hadamard Matrices over the Integers	37
CHAPTER IV : Constructions for Hadamard Matrices using skew-Hadamard Matrices	
4.1 Computer Construction of skew-Hadamard Matrices and a Similar skew-Hadamard Matrix of Order 76	47
4.2 Constructions for skew-Hadamard and n -type Matrices of Order "power plus one"	53
4.3 New Classes of Hadamard Matrices	64
4.4 New Classes of skew - Hadamard Matrices	71

**CHAPTER V : Constructions for Hadamard Matrices using
n-type Matrices**

5.1	Constructions for Symmetric Hadamard Matrices	74
5.2	Other Classes of Hadamard Matrices	76

CHAPTER VI : Hadamard Designs

6.1	The Hadamard Designs of Williamson and Marshall Hall - Baumert	84
6.2	Difference Sets Which Could be used in n-letter Hadamard Designs	85
6.3	Designs using n Different Blocks, $n > 4$	88

CHAPTER VII : Constructions for Block Designs

7.1	Some Block Designs	100
7.2	The Symmetric Block Design $(q^2(q+2), q(q+1), q)$	103
7.3	Some BIBDs	121
7.4	Numerical Results from Theorems in This Chapter	124
7.5	Revisions of the Table in M. Hall's book	126
7.6	Falsity of a Theorem of Clatworthy on the $(111, 11, 1)$ and $(110, 100, 11, 10, 1)$ - configurations	127

**CHAPTER VIII : Integer Matrices satisfying certain
Matrix Equations**

8.1	The Nature of Matrices satisfying the Equations for the Core of a Skew - Hadamard Matrix	129
8.2	Integer Solutions of $AA^T = a^2(k-\lambda)I + a^2\lambda J, AJ = akJ$ with a an Integer Constant	132
8.3	Matrices Satisfying $AA^T = pI + Q, AJ = dJ$ where p and d are Integer Constants	133

.../3.

APPENDICES : A	A Table of Orders < 4000 for which Hadamard and Skew-Hadamard Matrices are Known	139
B	The Computer Programme used in §4.1	148
C	The Proofs of Theorems 4.16 and Corollary 4.17.	154
D	A Table of n -type Matrices of Order < 4000	162
BIBLIOGRAPHY :		165

SUMMARY

We investigate the existence of matrices B satisfying the equation

$$BB^T = rI + sJ$$

where r and s are integers, I and J are the identity matrix and the matrix with every element $+1$ respectively, and certain restrictions are made on the elements of B . For example, if B is a square $(1, -1)$ - matrix of order r and $s = 0$, then we have the defining equation of an Hadamard matrix. Other restrictions yield balanced incomplete block designs and n -type matrices. Several constructions for matrices are given.

We also discuss Hadamard designs, prove the uniqueness of certain Hadamard matrices under integer equivalence, and show that certain matrix equations of the type being considered force restrictions on the entries of the matrix B under discussion.

* * * * *

This thesis contains no material published elsewhere, except where reference is made in the text. It is not and has not been used for the award of any other degree or diploma in any University.

J. Wallis

INTRODUCTION :

Hadamard matrices are historically significant in solving weighing problems. They, as have other block designs, have become more important as the study of the design and analysis of experiments has increased. In the last few years, with the advent of more sophisticated electrical micro-circuitry, all these and related matrices have received increasing attention.

We first became interested in matrices, A , satisfying equations of the type

$$AA^T = pI - J \quad (p \text{ an integer})$$

where A^T denotes A transpose, and I is the identity matrix and J the matrix with every element $+1$. These were used in the author's Master's thesis to construct new classes of Hadamard matrices. Now we continue our study of matrices, B , satisfying equations of the type

$$BB^T = rI + sJ \quad (r \text{ and } s \text{ integers}).$$

Chapter 1 consists of preliminaries.

In Chapter II we give those definitions special to Combinatorial Theory which we use later. The results of other authors are not proved but reference is given to proofs. §2.7 and later sections contain some definitions not universally used which are important in subsequent chapters. In §2.7 m -type matrices, which are not used by anyone but the author, are defined and two simple lemmas (2.25 and 2.26) are proved. The tables on page 21 and 22 have been compiled using a result in the author's M.Sc. thesis. §§2.7, 2.8, 2.9, 2.10 have been compiled by the author and at the time of writing purport to be complete lists of known classes of

skew-Hadamard matrices

n -type matrices (also called symmetric C -matrices),

symmetric Hadamard matrices,

Hadamard matrices.

Broadly speaking all the material after Chapter II is original although we give credit to other authors whenever we use their work. If credit is not given to another author then it is our work.

Goethals and Seidel [2] contains a construction for some skew - Hadamard matrices. In Chapter IV we have put more restraints onto the first lines used in their construction and studied the result. This led to theorem 4.5 and a computer investigation showed that our more restrictive conditions were satisfied in every case tried. This gave new constructions for skew - Hadamard matrices of orders

12, 20, 28, 36, 44, 52, 60 and 76.

Goethals and Seidel [1], Belavitch [1], and Goldberg [1] have found constructions for skew - Hadamard matrices and n - type matrices of the form "power plus one". We have independently found the results in the first two mentioned papers and this will be published in J. Wallis [4] and in addition have found restrictions on these methods as well as extending the results to the fifth and seventh powers. These results are in J. Wallis [5].

§4.3 appears in J. Wallis [2], [3], [7] except the main results of [2] and [7] become corollaries of the more powerful theorems 4.23 and 4.26. Theorem 4.31 and corollary 4.32 are included in J. Wallis [3].

Goethals and Seidel [1] have published some of the results in Chapter V. Our results will appear in J. Wallis [4].

A result of Goethals and Seidel [1], includes our lemmas 5.1 and 5.2. Although our results are not as powerful with regard to the number of Hadamard matrices obtained, they do yield symmetric Hadamard matrices while those of Goethals and Seidel do not necessarily do so. Lemma 5.4 was known previously. The results of the remainder of the chapter will appear in J. Wallis [4].

In §6.1 we outline the previous knowledge on Hadamard designs. §6.2 develops the concept of supplementary difference sets and shows in theorem 6.3 that this is a valid concept as a method of construction is given. Szekeres [1] has found constructions for twin difference sets and the Williamson type constructions in Hall [1] and Turyn [2] may be interpreted as supplementary difference sets. So we have shown that if n -letter Hadamard designs exist the results of §6.2 may be exploited to obtain new constructions for Hadamard matrices. §6.3 investigates the existence of n -letter designs and proves they can exist only for $n = 2, 4$ or 8 . §6.3 will appear in J. Wallis [9].

In chapter 7 the results are presented that we have discovered on block designs. §7.1 appears in J. Wallis [8] while most of the other results appear in J. Wallis [6].

The configurations in §7.1 do not appear to have been given in the form presented here by other authors. The $(45,12,3)$ configuration has been found previously by K. Takeuchi [2], Shrikhande and Singh [1], and also by Ahrens and Szekeres [1]. The $(36,15,6)$ configuration was known to K. Takeuchi [2], P. Kesava Menon [1], R. Turyn [1] and M. Hall [2]. Both the

$(45,12,3)$ and $(36,15,6)$ configurations were listed as unknown in M.Hall [1].

Theorem 7.1 is proved in a stronger form by a different method in Ahrens and Szekeres [1] and K.Takeuchi [2]. Their methods are quite different. We proved our result simultaneously with the authors of the first mentioned paper. Theorem 7.3 results from a different proof of theorem 7.1. It is not known whether the matrices S of page 116 and V of page 120 are isomorphic.

The results of theorems 7.4 and 7.6 were known. Theorem 7.7 has been proved by Van Lint and Seidel [1]. Theorem 7.5 appears to be genuinely new, and interesting, as it is a means of constructing (b,v,r,k,λ) configurations from (w,k,λ) configurations: previously only the converse was readily usable.

Most of chapter VIII will appear in J. Wallis [5].

Appendix A is a table of orders less than four thousand for which Hadamard and skew-Hadamard matrices are known. Appendix B is the computer programme used in §4.1 to find skew-Hadamard matrices. We have used Appendix C so that the proofs of theorem 4.16 and corollary 4.17 in the text could be shortened by having the tedious calculations removed. A table of n -type matrices of order less than four thousand is given in appendix D, the first page of which also indicates those orders less than one thousand which are positively excluded by theorem 2.9.

We wish to thank Professor G. Szekeres, Dr. R.J.Turyn and Dr. L.D.Baumert who have read drafts of my papers and this thesis and made many helpful suggestions.

CHAPTER I : PRELIMINARIES

In this chapter we note the results we shall need on quadratic residues, the Legendre symbol and Kronecker products.

§1.1 Quadratic Residues

Suppose p is an odd prime. If b is a non-zero residue modulo p , then b is called a *quadratic residue* if

$$x^2 \equiv b \pmod{p}$$

has solutions; otherwise b is called a quadratic non-residue.

($b = 0$ is specifically excluded from consideration). The following properties are standard (see, for example, Vinogradov [1; chapter 5]) :

(a) if b is a quadratic residue then $x^2 \equiv b$ has two solutions (of the form $x \equiv c$ and $x \equiv -c$);

(b) a reduced system modulo p consists of $\frac{p-1}{2}$ quadratic residues which are congruent to the numbers

$$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$$

There are therefore $\frac{p-1}{2}$ quadratic non-residues;

(c) if b is a quadratic residue modulo p , then

$$b^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

and if b is a quadratic non-residue modulo p , then

$$b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

§1.2 The Legendre Symbol $\chi(b) = \left(\frac{b}{p}\right)$.

If b is a ~~any~~ ^{any} residue (mod p), then the Legendre symbol

§2.1 $\chi(b) = \left(\frac{b}{p}\right)$ is defined by

$$\chi(b) = \begin{cases} 0 & \text{if } b \equiv 0 \pmod{p} \\ 1 & \text{if } b \text{ is a quadratic residue,} \\ -1 & \text{otherwise} \end{cases}$$

Then (see Vinogradov [1])

$$(a) \quad \chi(b) \equiv b^{\frac{p-1}{2}} \pmod{p}, \quad \text{see property (c) of §1.1}$$

$$(b) \quad \chi(1) = +1$$

$$(c) \quad \chi(-1) = \begin{cases} +1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}, \end{cases}$$

$$(d) \quad \chi(-c) = \begin{cases} \chi(c) & \text{if } p \equiv 1 \pmod{4}, \\ -\chi(c) & \text{if } p \equiv 3 \pmod{4}, \end{cases}$$

$$(e) \quad \chi(ab \dots k) = \chi(a)\chi(b) \dots \chi(k) \quad \text{so } \chi(ab^2) = \chi(a).$$

Lemma 1.1 : Vinogradov [1; p 192] $\sum_{x=1}^p \chi(x)\chi(x+c) = -1$

for any c satisfying $(c, p) = 1$.

§1.3 The Kronecker Product.

Definition 1.2 : If $M = (m_{ij})$ is a $m \times p$ matrix and $N = (n_{ij})$ is an $n \times q$ matrix, then the Kronecker product $M \times N$ is the $mn \times pq$ matrix given by

$$M \times N = \begin{bmatrix} m_{11}N & m_{12}N & \dots & m_{1p}N \\ m_{21}N & m_{22}N & \dots & m_{2p}N \\ \vdots & \vdots & \ddots & \vdots \\ m_{m1}N & m_{m2}N & \dots & m_{mp}N \end{bmatrix}$$

constitute the set of polynomials belonging to ~~the commutative ring~~ the commutative ring $F[x]$, the addition and the multiplication being defined in the ordinary way, viz.

$$\begin{aligned} \sum_{i=0}^n a_i x^i + \sum_{i=0}^n b_i x^i &= \sum_{i=0}^n (a_i + b_i) x^i \\ \sum_{i=0}^n a_i x^i \times \sum_{i=0}^n b_i x^i &= a_0 b_0 + (a_1 b_0 + a_0 b_1) x + \\ &+ (a_2 b_0 + a_1 b_1 + a_0 b_2) x^2 + \dots \end{aligned}$$

If in a particular F is the field $GF(p)$, $a_0, a_1, \dots$ are residue classes (mod p), and the polynomial ring ~~will~~ be denoted by $GF_p[x]$.

It is known that the number of elements contained ~~in~~ a Galois field must be of the form p^n , where p is a prime integer and n any positive integer. Conversely given a number of the form p^n , there always exists a Galois field with p^n elements in it, and any two Galois fields with the same number of elements are isomorphic. The Galois field with p^n elements is denoted $GF(p^n)$.

Every element of $GF(p^n)$ can be expressed in the standard form

$a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1}$,
 where the a_i are integers ranging from 0 to $p-1$. Any non-zero element α of $GF(p^n)$ satisfies

$$\alpha^{p^n-1} = 1.$$

For some of our methods later we will need matrices derived from finite fields. Let p be an odd prime and n a positive integer. Now let $\chi(x)$ be the character defined on $\text{GF}(p^n)$ by

$$\begin{aligned}\chi(0) &= 0, \\ \chi(x) &= \begin{cases} +1 & \text{if } x \text{ is a square,} \\ -1 & \text{if } x \text{ is not a square.} \end{cases}\end{aligned}$$

Then, from the properties of finite fields $\chi(xy) = \chi(x)\chi(y)$ in all cases.

Lemma 1.3: Hall [1,p208]. $\sum_b \chi(b)\chi(b+c) = -1$, if $c \neq 0$.

With $q = p^n$, let $a_0, a_1, \dots, a_{q-1}$ be the elements of the field numbered so that

$$a_0 = 0, \quad a_{q-i} = -a_i \quad i = 1, \dots, q-1.$$

Now put

$$A = (q_{ij}), \quad q_{ij} = \chi(a_i - a_j).$$

where A is of order q . Here

$$q_{ji} = \chi(a_j - a_i) = \chi(-1)\chi(a_i - a_j),$$

and since

$$-1 \text{ is a square for } q \equiv 1 \pmod{4},$$

$$-1 \text{ is a non-square for } q \equiv 3 \pmod{4}$$

it follows that A is

$$\text{symmetric for } q \equiv 1 \pmod{4},$$

$$\text{skew-symmetric for } q \equiv 3 \pmod{4}.$$

Lemma 1.4: Hall [1,p209]. $AA^T = qI - J$, $AJ = JA = 0$.

With q a prime, define $B = (b_{ij})$ by

$$b_{ij} = \begin{cases} 0 & i = j, \\ \chi(j-i) & i \neq j, \end{cases}$$

where χ is the Legendre symbol. Then using the results of §1.2

we have B is circulant and

$$\text{symmetric for } q \equiv 1 \pmod{4},$$

$$\text{skew-symmetric for } q \equiv 3 \pmod{4}.$$

Further

Lemma 1.5: $BB^T = qI - J$, $BJ = JB = 0$.

CHAPTER II : BLOCK DESIGNS, DIFFERENCE SETS, CIRCULANT MATRICES AND HADAMARD MATRICES

In this chapter we give those definitions special to Combinatorial Theory which will be used subsequently. No theorems are proved here but reference is given to the relevant literature. §2.7 and the later sections, containing lists of known orders have been compiled by the author.

2.1 Block Designs - (b, v, r, k, λ) - configurations

⁹
Definition 2.1 : A *balanced incomplete block design* is an arrangement of v distinct objects into b blocks such that each block contains exactly k distinct objects, each object occurs in exactly r different blocks, and every pair of distinct objects a_i, a_j occurs together in exactly λ blocks.

This is called a BIBD or a (b, v, r, k, λ) -configuration.
For example, $b = 12, v = 9, r = 4, k = 3, \lambda = 1$ gives the following blocks

1	2	3	1	4	7	1	5	9	1	6	8
4	5	6	2	5	8	2	6	7	3	5	7
7	8	9	3	6	9	3	4	8	3	4	9

Counting the number of objects in two different ways we see

$$(1) \quad r(k-1) = \lambda(v-1)$$

and counting the number of replications of an element, we see each element is replicated r times but since each block has k elements we must have

$$(2) \quad bk = vr.$$

14

Definition 2.2 : The *incidence matrix* of a (b, v, r, k, λ) - configuration is a $(0, 1)$ - matrix of size $b \times v$ with $a_{ij} = 1$ if object j is in block i and $a_{ij} = 0$ otherwise,

Notation : Throughout this thesis, I is the identity matrix and J is the matrix with every element +1. If the order is not *given* then it will be clear from the context.

Then if $A = (a_{ij})$ is the incidence matrix of a (b, v, r, k, λ) - configuration, A satisfies

$$(3) \quad AJ_{v \times v} = kJ_{b \times v},$$

$$(4) \quad A^T A = (r - \lambda)I_{v \times v} + \lambda J_{v \times v}.$$

Conversely if A is a $(0, 1)$ - matrix satisfying (3) and (4) then this ensures there is a (b, v, r, k, λ) - configuration.

¹⁰
Definition 2.3 : The *complement* of a (b, v, r, k, λ) - configuration is the configuration whose incidence matrix is obtained from the incidence matrix of a (b, v, r, k, λ) - configuration by replacing each 1 by 0 and each 0 by 1.

Clearly if b, v, r', k', λ' are the parameters of the complementary design of a (b, v, r, k, λ) - configuration then if $0 < \lambda$ and $k < v - 1$ we have

$$(5) \quad \begin{cases} r' = b - r \\ k' = v - k \\ \lambda' = b - 2r + \lambda \end{cases}$$

and since $\lambda'(v - 1) = r'(k' - 1)$ we have $\lambda'(v - 1) = (b - r)(v - k - 1)$, so $0 < \lambda'$ and $k' < v - 1$.

Lemma 2.4 : $\det[(r - \lambda)I + \lambda J] = [r + (v - 1)\lambda] (r - \lambda)^{v-1}$.

2.2 ^{Symmetric} Block Designs - (v, k, λ) - configurations

Defn " A symmetric (b, v, r, k, λ) - configuration has $b = v$ and $r = k$ this is called a (v, k, λ) - configuration.

¹⁵
Theorem 2.5 : Marshall Hall Jr., [1; p 104]. If A is the incidence matrix of a (v, k, λ) - configuration then A satisfies

$$(6) \quad AA^T = B = (k-\lambda)I + \lambda J$$

$$(7) \quad A^T A = B = (k-\lambda)I + \lambda J$$

$$(8) \quad AJ = kJ$$

$$(9) \quad JA = kJ.$$

For (v, k, λ) - configurations, (1) becomes

$$(10) \quad k(k-1) = \lambda(v-1).$$

¹²
Theorem 2.6 : Bruck - Ryser - Chowla Condition [Ryser, 1; p 111]

If v, k, λ are integers for which there is a (v, k, λ) - configuration, then

(i) if v is even $(k-\lambda)$ is a square

(ii) if v is odd, then the Diophantine equation

$$(11) \quad x^2 = (k-\lambda)y^2 + (-1)^{\frac{v-1}{2}} \lambda z^2$$

has a solution in the integers not all zero.

Equation (10) and theorem 2.6 give necessary conditions for the existence of a (v, k, λ) - configuration but it is not known if they are sufficient. No case has yet been found where these two conditions are both satisfied and the corresponding configuration has been proved not to exist.

Marshall Hall [1] shows these conditions are necessary and sufficient for a rational solution, A , of the incidence equation $AA^T = (k - \lambda)I + \lambda J$, but nothing has been proved for integer solutions.

Let $(k - \lambda)'$ and λ' respectively, denote the square free parts of $k - \lambda$ and λ and let $d = ((k - \lambda)', \lambda')$; then (11) may be written as

$$dx^2 = \frac{(k - \lambda)'}{d} y^2 + (-1)^{\frac{1}{2}(v-1)} \frac{\lambda' z^2}{d}$$

or $ax^2 + by^2 + cz^2 = 0$.

where a, b, c are square-free and $(a, b, c) = 1$.

This latter is called the *Legendre Equation* and

¹³
Theorem 2.7 : Ryser [1, p114]. The Legendre equation has solutions for x, y, z in the integers not all zero if and only if $-bo$, $-ac$, $-ab$ are quadratic residues of a, b , and c respectively.

For our later work we shall repeatedly use the following result:

¹⁷
Theorem 2.8 : J.Wallis [1, p11]. If A is the matrix obtained from the incidence matrix of a (v, k, λ) -configuration by every element 0 being replaced by -1 , then A satisfies

$$AA^T = 4(k - \lambda)I_v + (v - 4(k - \lambda))J_v.$$

§2.3 DIFFERENCE SETS

⁵¹
Definition 2.9 : A set of k residues $D = \{a_1, \dots, a_k\}$ modulo v is called a (v, k, λ) - difference set or a perfect difference set, if for every $d \neq 0 \pmod{v}$ there are exactly λ ordered pairs (a_i, a_j) , $a_i, a_j \in D$ such that $a_i - a_j \equiv d \pmod{v}$.

For example the numbers 0, 1, 3, 8, 12, 18 modulo 31 form a $(31, 5, 1)$ - difference set since

$1 - 0 \equiv 1$	$12 - 1 \equiv 11$	$8 - 18 \equiv 21$
$3 - 1 \equiv 2$	$12 - 0 \equiv 12$	$3 - 12 \equiv 22$
$3 - 0 \equiv 3$	$0 - 18 \equiv 13$	$0 - 8 \equiv 23$
$12 - 8 \equiv 4$	$1 - 18 \equiv 14$	$1 - 8 \equiv 24$
$8 - 3 \equiv 5$	$18 - 3 \equiv 15$	$12 - 18 \equiv 25$
$18 - 12 \equiv 6$	$3 - 18 \equiv 16$	$3 - 8 \equiv 26$
$8 - 1 \equiv 7$	$18 - 1 \equiv 17$	$8 - 12 \equiv 27$
$8 - 0 \equiv 8$	$18 - 0 \equiv 18$	$0 - 3 \equiv 28$
$12 - 3 \equiv 9$	$0 - 12 \equiv 19$	$1 - 3 \equiv 29$
$18 - 8 \equiv 10$	$1 - 12 \equiv 20$	$0 - 1 \equiv 30$

We now list the known difference sets given in Hall [1,p141].

Type S : (Singer difference sets). These are hyperplanes in $PG(n,q)$, $q = p^r$. The parameters are

$$v = \frac{q^{n+1} - 1}{q - 1}, \quad k = \frac{q^n - 1}{q - 1}, \quad \lambda = \frac{q^{n-1} - 1}{q - 1}.$$

Type Q : (quadratic residues in $GF(p^r)$, $p^r \equiv 3 \pmod{4}$) :

$$v = p^r = 4t - 1, \quad k = 2t - 1, \quad \lambda = t - 1.$$

Type T : (Brauer's twin primes). Suppose that p and $q = p+2$

are ~~both~~ twin primes. Of the $(p-1)(q-1)$ residues modulo pq prime to pq , let $a_1, \dots, a_m$, $m = (p-1)(q-1)/2$ be those for which $\left(\frac{a_i}{p}\right) = \left(\frac{a_i}{q}\right)$, and also let $a_{m+1}, \dots, a_{m+p}$ be $0, q, 2q, \dots, (p-1)q$. Here, $m+p = (pq-1)/2 = k$. Then $a_1, \dots, a_k$ form a difference set modulo v , $v = pq$. Here the parameters are

$$v = pq, \quad k = \frac{pq-1}{2}, \quad \lambda = \frac{pq-3}{4}.$$

Necessarily, $pq \equiv 3 \pmod{4}$, and we have $v = 4t - 1$, $k = 2t - 1$, $\lambda = t - 1$. This also holds for $GF(p^r)$ and $GF(q^s)$ if $q^s = p^r + 2$.

Type B : (biquadratic residues of primes $p = 4x^2 + 1$, x odd).

Here,

$$v = p = 4x^2 + 1, \quad k = x^2, \quad \lambda = \frac{x^2 - 1}{4}.$$

Type B₀ : (biquadratic residues and zero modulo $p = 4x^2 + 9$, x odd).

Here $v = 4x^2 + 9$, $k = x^2 + 3$, $\lambda = \frac{x^2 + 3}{4}$.

Type 0: (octic residues of primes $p = 8a^2 + 1 = 64b^2 + 9$ with a, b odd). Here

$$v = p, \quad k = a^2, \quad \lambda = b^2.$$

Type 0₀: (octic residues and zero for primes $p = 8a^2 + 49 = 64b^2 + 441$, a odd, b even). Here

$$v = p, \quad k = a^2 + 6, \quad \lambda = b^2 + 7.$$

Type W₄: (a generalization of type T, developed by Whiteman [1], which uses biquadratic rather than quadratic residues). Here p and q are two primes such that $(p-1, q-1) = 4$, and we write $d = \frac{1}{4}(p-1)(q-1)$. We take g as an appropriate number which is a primitive root of both p and q . The difference set consists of $1, g, g^2, \dots, g^{d-1}, 0, q, 2q, \dots, (p-1)q$ modulo pq , where

$$v = pq, \quad k = \frac{pq-1}{4}, \quad \lambda = \frac{pq-5}{16}.$$

We must have $q = 3p + 2$ and also $\frac{pq-1}{4}$, an odd square.

2.4 CIRCULANT MATRICES

¹⁸
Definition 2.10: A *circulant matrix* $A = (a_{ij})$ of order n is one in which $a_{ij} = a_{1, j-i+1}$ where $j-i+1$ is reduced modulo n .

For example:

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

¹⁹
Definition 2.11: A $(1, -1)$ -matrix is a matrix whose only elements are $+1$ and -1 .

²⁰
Definition 2.12: A set $D = \{x_1, x_2, \dots, x_k\}$ will be said to generate a circulant $(1, -1)$ -matrix if

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

²¹
Definition 2.13: 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

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

²²
Lemma 2.14: A back circulant matrix is symmetric.

23

Lemma 2.15 : J. Wallis [1;p 15] The product of a back - circulant matrix with a circulant matrix is symmetric. In particular if A is back - circulant and B is circulant

$$AB^T = BA^T$$

24

Lemma 2.16 : J. Wallis [1;p 16] Any two circulant (hence back - circulant) matrices of the same order commute.

Lemma 2.16 shows that any two circulant matrices A and B satisfy $AB = BA$. Lemma 2.15, on the other hand shows that any circulant matrix A and back circulant matrix B satisfy $AB^T = BA^T$. Both are useful to us but the latter is used most.

Theorem 2.17 : Ryser [1] A perfect difference set D is equivalent to a (v,k,λ) - configuration with circulant incidence matrix.

2.5

Table of Matrix Equations satisfied by known Difference Sets and (v,k,λ) - configurations.

In this section we confine our attention to the $(1,-1)$ matrices, A , obtained from the incidence matrices of difference sets and (v,k,λ) - configurations. Table 1 uses theorem 2.8 to obtain the equations satisfied by these $(1,-1)$ matrices for the difference sets in §2.3. We note that theorem 2.17 ensures all these matrices A may be taken as circulant (or back circulant).

Throughout the table p is a prime and p^r a prime power. We do not include k_4 since it has $v \equiv 1 \pmod{4}$, v non-prime and so can never be used in our construction.

Type of Difference Set	(v,k,λ)-configuration generating A	Incidence equation for A	Comments
	$(v,v,v) = J$	vJ	
	$(v,v-1,v-2) = J - 2I$	$4I + (v - 4)J$	
S type	$\frac{q^{n+1}-1}{q-1}, \frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}$	$4q^{n-1}I + \left(\frac{q^{n+1}-1}{q-1} - 4q^{n-1}\right)J$	$q = p^r$
Q type	$(4t-1, 2t-1, t-1)$	$4tI - J$	$4t = p^r + 1$
T type	$(pq, \frac{pq-1}{2}, \frac{pq-3}{4})$	$(pq + 1)I - J$	$p=q+2, \frac{pq-3}{4}$ prime
B type	$(4x^2 + 1, x^2, \frac{x^2-1}{4})$	$(3x^2 + 1)I + x^2J$	$p = 4x^2 + 1; x$ odd
B _o type	$(4x^2 + 9, x^2 + 3, \frac{x^2+3}{4})$	$(3x^2 + 9)I + x^2J$	$p = 4x^2 + 9; x$ odd
O type	$(64b^2 + 9, 8b^2 + 1, b^2)$	$4(7b^2 + 1)I + (36b^2 + 5)J$	$p=8a^2 + 1=64b^2+9; a, b$ odd
O _o type	$(64b^2 + 441, 8b^2 + 56, b^2 + 7)$	$4(7b^2 + 49)I + (36b^2 + 249)J$	$p = 8a^2 + 49 = 64b^2 + 441; a$ odd, b even

TABLE 1.

Table 2 gives those (v,k,λ) configurations from Marshall Hall [1], and Takeuchi [1] which are not already covered by Table 1 and in which v is a prime. All the entries satisfy the necessary conditions for (v,k,λ) configurations given by equation 10 and theorem 2.6.

As for Table 1 the incidence equation is calculated using the $(1,-1)$ incidence matrix of the configuration.

(v,k,λ) configuration	incidence equation	comment
(31,10,3)	$28I + 3J$	exists
(41,16,6)	$40I + J$	unknown
(61,16,4)	$48I + 13J$	unknown
(61,21,7)	$56I + 5J$	unknown
(61,25,10)	$60I + J$	unknown
(71,15,3)	$48I + 23J$	unknown
(71,21,6)	$60I + 11J$	unknown
(79,13,2)	$44I + 35J$	unknown
(157,13,1)	$48I + 109J$	unknown

TABLE 2

For our later constructions we would need the configurations of Table 2 to have circulant incidence matrices, however using the results in Turyn [1] and Baumert [3] we see that none of these configurations can have circulant incidence matrices.

§2.6 HADAMARD MATRICES

These matrices were first considered as Hadamard determinants. They were so named because the determinant of an Hadamard matrix satisfies the equality of Hadamard's determinant theorem, which states that if $X = (x_{ij})$ is a matrix of order n then

$$|\det X|^2 \leq \prod_{i=1}^n \prod_{j=1}^n |x_{ij}|^2.$$

Properties of Hadamard Matrices :

$$\begin{aligned} (a) \quad & HH^T = h I_n \\ (b) \quad & \det H = h^{n/2} \\ (c) \quad & HH^T = H^T H \end{aligned}$$

- Lemma 26.*
- (a) every element is ± 1 ;
 - (b) the scalar product of any two distinct row vectors is zero;
 - (c) an Hadamard matrix of order $4n$ has determinant $\pm (4n)^{2n}$;
 - (d) if H is an Hadamard matrix of order $4n$ then H satisfies $HH^T = 4nI_{4n}$;
 - (e) Hadamard matrices may be changed into other Hadamard matrices by permuting rows and columns and by multiplying rows and columns by -1 . We call matrices which can be obtained from one another by these methods H -equivalent. Not all Hadamard matrices of the same order are H -equivalent;
 - (f) every Hadamard matrix is H -equivalent to an Hadamard matrix which has every element of its first row and column $+1$ - matrices of this latter form are called normalized;
 - (g) if H is a normalized Hadamard matrix of order $4n$, then every row except the first has $2n$ minus ones and $2n$ plus ones in each row, further n minus ones in any row overlap with n minus ones in each other row;
 - (h) the order of an Hadamard matrix is 2 or $4n$, n integer.

2.7 SKEW - HADAMARD MATRICES AND M-TYPE MATRICES

Definition 2.18 : A skew - Hadamard matrix H of order $h \equiv 0 \pmod{4}$, has every element $+1$ or -1 , and is of the form $H = S + I$ where S is skew - symmetric.

Lemma 2.19 : If $H = S + I$ is a skew - Hadamard matrix of order h then

$$SS^T = (h-1)I.$$

Proof : Follows from property (d). ***

In Appendix A we list by class all the known skew - Hadamard matrices with order < 4000 .

We study skew - Hadamard matrices because the constructions of Goldberg [1], Johnsen [1], J.Wallis [2], [3], [7], Williamson [1] and this thesis depend heavily on the existence of these special matrices.

Definition 2.20 : A skew - type matrix $A = T + I$ has T skew - symmetric.

Definition 2.21 : The core of a skew - Hadamard matrix H of order h is that matrix W of order $h-1$ obtained from H by first multiplying the columns so that the first row has only $+1$ elements and then multiplying the rows so every element in the first column (bar the first) is -1 ; then H becomes

$$\begin{bmatrix} 0 & e \\ -e^T & W \end{bmatrix} + I$$

where $e = [1, 1, \dots, 1]$ is a $1 \times (h-1)$ matrix.

Skew - Hadamard matrices are known to exist for the

following orders :

- SI $2^{t \prod k_i}$ t, r_i are non-negative integers,
 $k_i = p_i^{r_i} + 1 \equiv 0 \pmod{4}$ p_i a prime;
 from Williamson [1; p 67],
- SII $(p-1)^3 + 1$ p the order of a skew-Hadamard matrix;
 from Goldberg [1],
- SIII $2^t(q+1)$ $t \geq 1$ an integer, q (prime power) $\equiv 5 \pmod{8}$;
 from Szekeres [1],
- SIV 52 Blatt and Szekeres [1],
- SV 36 Goethals and Seidel [1],
- SVI $p^r(p^r+1)(m-1)$ m of type SI, p^r (prime power) $\equiv 3 \pmod{4}$, and
 $m' (m'-1) (m-1)$ $\frac{(m-1)(p^r+1)m'}{m}$ the order of a skew-Hadamard
 matrix; from J.Wallis [3] and corollary 4.32,
- SVII $p^r(p^r-3)(m-1)$ m of type SI, p^r (prime power) $\equiv 3 \pmod{4}$, and
 $(m'-1)(m'-4)(m-1)$ $\frac{(m-1)(p^r-3)m'}{m}$ the order of a skew-Hadamard
 matrix; from J.Wallis [3] and corollary 4.32,
- SVIII $(p-1)^5 + 1$ p the order of a skew-Hadamard matrix;
 from J.Wallis [5] and theorem 4.15,
- SIX $(p-1)^7 + 1$ $\left. \begin{array}{l} \text{now} \\ \text{known} \\ \text{+} \\ \text{add } u \end{array} \right\}$ p the order of a skew-Hadamard matrix;
 from J.Wallis [5] and theorem 4.19,
- SX $(p-1)^u + 1$ $u = 3^a 5^b 7^c$ where p is the order of a skew-
 Hadamard matrix and a, b, c are non-negative
 integers; from J.Wallis [5] and theorem 4.22,
- SXI $4k$ $k \in \{3, 5, 7, 9, 13, 15, 19\}^{23}$; from theorem 4.4;
- SXII $q(p^r+1)$ q the order of a skew-Hadamard matrix,
 p^r (prime power) $\equiv 3 \pmod{4}$; from J.Williamson
 [1, p67] and theorem 4.30,
- SXIII $2q$ q the order of a skew-Hadamard matrix from
 theorem 4.29.
- p_{+1}^t $p \equiv 5 \pmod{8}$; $t \equiv 2 \pmod{4}$; A.L. Whiteman + G. Szekere

Lemma 2.22 : If W of order $h-1$ is the core of a skew-Hadamard matrix then W satisfies

$$WW^T = (h-1)I - J, \quad WJ = 0, \quad W^T = -W.$$

Proof : Let H be the skew-Hadamard matrix of order h of which W is the core. Then since $HH^T = hI_h$ we have (with J of order $h-1$):

$$\begin{aligned} HH^T &= \left(\begin{bmatrix} 0 & e \\ -e^T & W \end{bmatrix} + I_h \right) \left(\begin{bmatrix} 0 & -e \\ e^T & W^T \end{bmatrix} + I_h \right) \\ &= \begin{bmatrix} h-1 & eW^T \\ We^T & J+WW^T \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & W+W^T \end{bmatrix} + I_h = hI_h. \end{aligned}$$

Since H is skew-Hadamard $W^T = -W$ and so we have

$$We^T = 0 \quad \text{which gives} \quad WJ = 0,$$

$$\text{and} \quad J + WW^T + W + W^T + I_{h-1} = hI_{h-1},$$

$$\text{or} \quad WW^T = (h-1)I_{h-1} - J. \quad ***$$

Definition 2.23 : Any matrix W of order $h-1$ with zero diagonal satisfying

$$WW^T = (h-1)I - J, \quad WJ = 0$$

will be called a core.

The term core was first used to us by R. Turyn and we feel that it is particularly descriptive and apt.

Definition 2.24 : M and N will be called m-type matrices if M is a skew-Hadamard matrix, N is a symmetric Hadamard matrix and

$$MN^T = NM^T.$$

Lemma 2.25 : If $M = W + I$ and N are m -type matrices then

$$WN^T = NW^T.$$

Proof : Since $MN^T = NM^T$, we have

$$MN^T = (W+I)N^T = WN^T + N^T = WN^T + N = NM^T = N(W^T + I) = NW^T + N$$

and so

$$WN^T = NW^T.$$

Lemma 2.26 : If $s = 2^t \prod (p_i^{r_i} + 1)$ where t is a non-negative integer and $p_i^{r_i}$ (prime power) $\equiv 3 \pmod{4}$ then there are m -type matrices of order s .

Proof : (i) $M_2 = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ and $N_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ are two suitable matrices of order 2.

(ii) Let $e = (1, \dots, 1)$ be the vector of q 1's. Further let A be the matrix of order q defined in §1.4 for $h-1 = q = p^r \equiv 3 \pmod{4}$. Then the matrix

$$B = \begin{bmatrix} 0 & e \\ -e^T & A \end{bmatrix}$$

has the properties

$$B^T = -B, \quad BB^T = (h-1)I_h.$$

Here

$$M = I_h + B$$

is a matrix of +1's and -1's satisfying $MM^T = hI_h$ and so is a skew-Hadamard matrix of order h .

Let U be the matrix of order $h-1 = p^r = q$, where

$$\begin{aligned} U &= (u_{ij}), & i, j &= 0, \dots, q-1, & u_{00} &= 1, \\ u_{i, q-i} &= 1, & i &= 1, \dots, q-1, & u_{ij} &= 0, \\ & & & & & \text{otherwise.} \end{aligned}$$

Now define the matrix N by the equation

$$\begin{aligned} N &= \begin{bmatrix} 1 & 0 \\ 0 & -U \end{bmatrix} M = \begin{bmatrix} 1 & 0 \\ 0 & -U \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & -U \end{bmatrix} \begin{bmatrix} 0 & e \\ -e^T & A \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & -U \end{bmatrix} + \begin{bmatrix} 0 & e \\ e^T & -UA \end{bmatrix}. \end{aligned}$$

Since

$$A = (q_{ij}), \quad i, j = 0, \dots, q-1 \quad \text{and} \quad q_{ij} = \chi(a_i - a_j),$$

with $UA = (c_{ij})$, then $c_{0j} = \chi(0 - a_j)$ and

$$c_{ij} = \chi(a_{q-i} - a_j) = \chi(-a_i - a_j), \quad i=1, \dots, q-1,$$

whence in all cases $c_{ij} = \chi(-a_i - a_j)$ and so UA is symmetric, whence also N is symmetric: $N^T = N$.

In addition, noting $U^T = U$ and $U^2 = 1$, we find

$$NN^T = \begin{bmatrix} 1 & 0 \\ 0 & -U \end{bmatrix} MM^T \begin{bmatrix} 1 & 0 \\ 0 & -U \end{bmatrix} = hI_h.$$

So N is a symmetric Hadamard matrix. Now

$$MN^T = MM^T \begin{bmatrix} 1 & 0 \\ 0 & -U \end{bmatrix} = hI_h \begin{bmatrix} 1 & 0 \\ 0 & -U \end{bmatrix} = NM^T,$$

So M and N are two suitable matrices of order $p^r + 1 \equiv 0 \pmod{4}$, p^r a prime power.

(iii) Let $M_m = W_m + I_m$ and N_m be m -type matrices of order m and $M_n = W_n + I_n$ and N_n be n -type matrices of order n . Then

$$M_{mn} = I_m \times M_n + W_m \times N_n$$

is a skew-Hadamard matrix of order mn and

$$N_{mn} = N_m \times N_n$$

is a symmetric Hadamard matrix of order mn .

Now

$$\begin{aligned}
 M_{mn} N_{mn}^T &= (I_m \times M_n + W_m \times N_n)(N_m^T \times N_n^T) \\
 &= N_m^T \times M_n N_n^T + W_m N_m^T \times N_n N_n^T \\
 &= N_m \times N_n M_n^T + N_m W_m^T \times N_n N_n^T && \text{using lemma 2.25} \\
 &= (N_m \times N_n)(I_m \times M_n^T + W_m^T \times N_n^T) \\
 &= N_{mn}^T M^T.
 \end{aligned}$$

So M_{mn} and N_{mn} are m -type matrices of order mn .

(iv) Combining the results of (i), (ii), and (iii) we have the lemma for $s > 1$. But the case $s = 1$ is trivial.

8 n-TYPE MATRICES

Those who are familiar with the work of Belevitch and Goethals and Seidel will see that our n -type matrices to be defined below can be easily derived from symmetric C -matrices of the above writers. We have persisted in our use of n -type in order to be consistent with our own writings in J. Wallis [4], [5].

For a discussion of the electrical applications of n -type matrices see Belevitch [1].

Definition 2.27 : An n -type matrix N of order $n \equiv 2 \pmod{4}$ has every element $+1$ or -1 , and is of the form $N = R + I$ where R is symmetric, $RR^T = (n-1)I$ and $RJ = 0$.

Comparison of definitions 2.27 and 2.18 show that n -type matrices are analogous to skew - Hadamard matrices.

n -type matrices are known to exist for the following orders :

- NI $p^r + 1$ r a positive integer, p a prime, and $p^r \equiv 1 \pmod{4}$; from Paley [1; p 315]
- NII $(h-1)^2 + 1$ h the order of a skew-Hadamard matrix; from Belevitch [1] and J.Wallis [4], and theorem 4.6
- NIII $(n-1)^2 + 1$ n the order of an n -type matrix; from Belevitch [1] and J.Wallis [4], and theorem 4.6
- NIV $(n-1)^3 + 1$ n the order of an n -type matrix; from Belevitch [1] and J.Wallis [4], and theorem 4.10
- NV $(n-1)^5 + 1$ n the order of an n -type matrix; from J.Wallis [5] and theorem 4.14
- NVI $(n-1)^7 + 1$ n the order of an n -type matrix; from J.Wallis [5] and theorem 4.18
- NVII $(n-1)^u + 1$ $u = 2^a 3^b 5^c 7^d$, a, b, c, d non-negative integers, n the order of an n -type matrix; from J.Wallis [5] and theorem 4.20
now known integer u
- NVIII $(h-1)^u + 1$ $u = 2^a 3^b 5^c 7^d$, a an integer $a > 0$, b, c, d non-negative integers, h the order of a skew-Hadamard matrix; from J.Wallis [5] and theorem 4.21
now known even integer u

Analogous to definition 2.21 we now define the core of an n -type matrix.

Definition 2.28 : The *core of an n -type matrix* N of order n is that matrix W of order $n-1$ obtained from N by first multiplying the rows and columns so that the first row and column has only $+1$ elements; then N becomes

$$\begin{bmatrix} \overline{0} & \overline{e} \\ \underline{e}^T & \underline{W} \end{bmatrix} + I$$

where $\underline{e} = [1, 1, \dots, 1]$ is a $1 \times (n-1)$ matrix.

Combining the results given in Belevitch [2,p 15], Griffin [1,p 158], Hall [1,p 114 and p 175], Hardy and Wright [1,p 299], Raghavarao [1,p 883], and Shrikhande and Singh[1,p 30] we have the following theorem:

Theorem 2.29 : A necessary condition for the existence of an n -type matrix of order $n \equiv 2 \pmod{4}$ is that

- (i) $n-1 = a^2 + b^2$, where a and b are integers,
- (ii) the square free part of $n-1$ must not contain a prime factor $\equiv 3 \pmod{4}$.

Note that (i) and (ii) are equivalent.

Theorem 2.29 tells us immediately that there are no n -type matrices of orders 22,34,58,70 and 94.

Appendix D shows the orders < 1000 for which n -type matrices exist and those orders which are excluded by theorem 2.29. Also in appendix D is a list of those orders between 1000 and 4000 for which n -type matrices do exist.

2.9 KNOWN CLASSES OF SYMMETRIC HADAMARD MATRICES

We include this list as our definition of m -type requires symmetric Hadamard matrices and so does the theorem on p 213 of Marshall Hall [1], which is included in our class HVIII.

The following notation is used below

t t is a non-negative integer,

p^r $p^r \equiv 3 \pmod{4}$ is a prime power,

q^s $q^s \equiv 1 \pmod{4}$ is a prime power,

n $n \equiv 2 \pmod{4}$ is the order of an n -type matrix.

The following are orders of symmetric Hadamard matrices:

- SHI 2^t t is a non-negative integer;
- SHII p^{r+1} $p \equiv 3 \pmod{4}$ is a prime power;
- SHIII $2(q^s+1)$ $q^s \equiv 1 \pmod{4}$ is a prime power;
- SHIV $2n$ J. Wallis [4] and theorem 5.1;
- SHV $2n(n-1)$ J. Wallis [4] and theorem 5.2;
- SHVI $4s^2$ if strong graphs of order $4s^2$ exist with eigenvalues $\rho_1 = 2s + 1$, $\rho_2 = -2s + 1$; or if pseudo Latin-square graphs $L_s(2s)$ or negative-Latin-square graphs $NL_s(2s)$ exist; from Goethals and Seidel [3];
- SHVII $(n-1)^2$ if $n-2$ is the order of a skew-Hadamard matrix; from Goethals and Seidel [3];
- SHVIII h_1^2 h_1 the order of an Hadamard matrix; from Goethals and Seidel [3];
- SHIX $(2k)^2$ If there exists a $(4k^2-1, k(2k-1), 2k+1, k, 1)$ configuration: from Goethals and Seidel [3], and W.D. Wallis [2];
- SHX k k is a product of orders from the other classes SHI - SHIX.

where $n \equiv 2 \pmod{4}$ is the order of an n -type matrix.

2.10 KNOWN CLASSES OF HADAMARD MATRICES

In this section we use the following notations

$p^r, p_1^{r_1}$	prime powers $\equiv 3 \pmod{4}$;
q^s	prime power $\equiv 1 \pmod{4}$;
x^u	any prime power;
t	a non-negative integer;
h_1, h_2	$h_1 > 1, h_2 > 1$ are the orders of Hadamard matrices;
h	is the order of a skew - Hadamard matrix;
n	is the order of an n -type matrix;
K	$\{i: i \text{ an odd integer, } 3 \leq i \leq 29, \text{ or } i = 37 \text{ or } i = 43\}$

in all cases the class indexed with an A is stronger than the others classified under the same number. Thus HIIA which is $h(p^r+1)$ includes the other member of the class HII which is p^r+1 . If we say as in HIIIA that the class is proved in theorem 5.4 then it means theorem 5.4 of this thesis.

The following classes of Hadamard matrices are known :

HIA	2^t	Sylvester [1];	✓
HIIA	$h(p^r+1)$ p^r+1	(Paley [1], Williamson [1,p66]; Paley [1,p 315];	✓
HIIIA	$h n$	Goethals and Seidel [1,p 1009], J. Wallis [4,lemma 2] and theorem 5.4;	✓
	$2(q^s+1)$	Paley [1,p 315];	
	$h(q^s+1)$	Williamson [1,p 66];	
	$2n$	J. Wallis [4,lemma 1] and theorem 5.1 : the matrix obtained is symmetric;	
	$2^t(q+1)$	$g(\text{prime power}) \equiv 5 \pmod{8}$: Szekeres [1];	

HIVA	$4k$	$k \in K$;
Welch 20K	92,184	Baumert, Golomb, Hall [1];
$\left. \begin{array}{l} 28K \\ 36K \\ 44K \end{array} \right\} J. Wallis$	116	Hall [1];
HVA	172	Williamson [1];
	$12k$	$k \in K$;
	156	Baumert, Hall [1];
HVIA	$h(h-1)$	Williamson [1, p 67];
	$p(p+1)$	Scarpis [1];
	$h_1 h_2 p^r (p^r + 1)$	Williamson [2, p 611];
	$h(h-1)$	if an $(h-1, h/2, h/4)$ configuration with circulant incidence matrix exists; J. Wallis [7, corollary 6]; <i>corollary 4.24</i> ;
HVIAA	$h_1 n(n-1)$	Goethals and Seidel [1, p 1009];
	$2n(n-1)$	J. Wallis [4, theorem 3] and theorem 5.2: the matrix obtained is also symmetric;
	$h_1 h_2 n(n-1)$	J. Wallis [4, theorem 9] and theorem 5.9;
	$h_1 h_2 q^s (q^s + 1)$	Williamson [2, p 611];
	$2q^s (q^s + 1)$	J. Wallis [4, corollary 4] and corollary 5.3;
HVIII	$h(h+3)$	$h+4$ a symmetric Hadamard matrix; M. Hall [1, p 13];
	$h(h+3)$	<i>$h+4$ the order of an Hadamard matrix: cor 4.24</i> if an $(h-1, h/2, h/4)$ configuration with circulant incidence matrix exists; J. Wallis [7, corollary 7];
	$(p^r + 1)(p^r + 4)$	J. Wallis [7, corollary 7]; <i>$p+5$ the order of an Hadamard matrix, corollary 4.25.</i>
	$g(g+3)$	g and $g+4$ both of the form $2^t \prod (p_i^{r_i} + 1)$: Williamson [2, p 610];
HIXA	$h_3 n(n+3)$	$h_3 > 2$ the order of an Hadamard matrix, $n+4$ the order of an n -type matrix; Goethals and Seidel [1, p 1009];
	$h_1 h_2 (q^s + 1)(q^s + 4)$	$q^s + 5$ of the form $q^s + 1$: Williamson [1, p 613];
	$h_1 h_2 n(n+3)$	$n+4$ the order of an n -type matrix: J. Wallis [4, theorem 9] and theorem 5.9;

$$\text{HXA} \quad \begin{cases} h^2 \\ n^2 \end{cases} \\ x^u(x^u+2)+1$$

$$\text{HXIA} \quad \begin{cases} (h-2)^2 \\ (h-1)^u+1 \\ (h-1)^3+1 \end{cases}$$

$$\text{HXIIA} \quad m(m+1-4g^{(w-1)s})$$

$$\text{HXIIIA} \quad f(q^2+1)$$

$$\text{HXIVA} \quad h(b-1)$$

$$(b-2)(b-1)(b^2+b+1)$$

$$\text{HXVA} \quad 2h(h+1)$$

$$\text{HXVIA} \quad mzh$$

$$\begin{cases} h=n+2 \\ n=h+2 \end{cases} : \text{Goethals and Seidel} \\ [1, p 1008];$$

Brauer [1] and Whiteman [1];

$$q^s = h-3 : \text{Erllich [1];}$$

$c = 3^a 5^b 7^c$ a, b, c non-negative integers : J. Wallis [5; corollary 3.3] and theorem 4.22;

Goldberg [1];

$w \geq 2$ an integer, g a product of the form $2^t \prod (p_i^{r_i} + 1)$, $m = 1 + q^s + q^{2s} + \dots + q^{ws}$ is a prime $\equiv 3 \pmod{4}$ or a product of twin primes : Spence [1, p 60];

~~...~~ Turyan [2].

Welch whenever $(b-1, u, \frac{h-b}{4} + u)$ and

$(b-1, v, v - \frac{b}{4})$ configurations with circulant incidence matrices exist: J. Wallis [7, theorem 3];

$$b^2+b+1 \equiv 3 \pmod{4}, b = q^s, \\ h = (b-1)(b-2) : \text{J. Wallis [7, corollary 5];}$$

$2h+3$ a prime: J. Wallis [3, theorem 5] and theorem 4.27;

m the order of m -type matrices, and there exist three matrices X, Y, Z of order $z \equiv 3 \pmod{4}$ satisfying

(a) XY^T, YZ^T and ZX^T all symmetric, and

(b) $XX^T = aI_z + bJ_z$, a, b integers

$$YY^T = \left\{ \frac{m+mz-mh-a}{m-1} \right\} I_z + \left\{ \frac{mh-m-b}{m-1} \right\} J_z$$

$$ZZ^T = (z+1)I_z - J_z;$$

from J. Wallis [3, theorem 1] and theorem 4.23. Corollaries 4.24 and 4.25 show some cases where these conditions are satisfied.

HXVIIA

mzh

$m = 2$ or 4 , and there exist four matrices X, Y, Z, W of order $z \equiv 1 \pmod{4}$ satisfying

(a) $XY^T, XZ^T, XW^T, YZ^T, YW^T, ZW^T$ all symmetric, and

(b) $XX^T + YY^T = 2(z+1)I_z - 2J_z$

$WW^T = aI_z + bJ_z$, a, b integers

$ZZ^T = \{m(z+1-h-a)+a\} I_z +$

$\{m(h-1-b)+b\} J_z$

from J. Wallis [3, theorem 1] and theorem 4.26. Corollary 4.28 shows some cases where these conditions are satisfied;

HXVIII A

 $4nm$

D and M are symmetric matrices of order m , satisfying

$D^2 = mI_m - J_m, M^2 = (m+1-n)I_n + (n-1)J_n$,

$MD = DM$ where D has zero diagonal; from J. Wallis [4, theorem 5] and theorem 5.5 of this thesis.

J. Wallis [4, corollary 7] and corollary 5.7 show some cases where these conditions are satisfied;

 $4q^*n$

M is a back circulant matrix of order q^* satisfying

$M^2 = (q^*+1-n)I + (n-1)J$; from J. Wallis [4, corollary 6] and corollary 5.6

HXIXA

 $2nvh_1$

$v \equiv 1 \pmod{4}$ is the order of three matrices A, B and D satisfying

$DD^T = vI - J, AA^T = aI + (v-a)J$,

$BB^T = \{2(v-n+1)-a\} I + \{-v+2(n-1)+a\} J$,

where AB^T, BD^T and AD^T are all symmetric. J. Wallis [4, theorem 8] and theorem 5.8;

$4q^s n$

q^s is the order of three matrices

A, C and D satisfying $AA^T = aI + (q^s - a)J$,

$CC^T = [2q^s - 2n + 2 - a]I + [-q^s + 2n - 2 + a]J$,

$DD^T = q^s I - J$, where AC^T , CD^T and AD^T

are all symmetric and D has zero

diagonal. J. Wallis [4, theorem 10]

and theorem 5.10; J. Wallis [4,

corollary 11] and corollary 5.11

give some cases where these conditions
are satisfied;

HXX

m

m the product of orders from any
classes. ✓

CHAPTER III : MATRIX EQUIVALENCE

~~§3.1~~ ^{includes} §3.1 ~~includes~~ the results of a paper by W.D.Wallis and J.Wallis [1].

§3.1 EQUIVALENCE OF HADAMARD MATRICES OVER THE INTEGERS

Definition 3.1: If A and B are matrices over the ring Z of integers, A and B are called equivalent ($A \sim B$) if there are Z -matrices P and Q , of determinant ± 1 , such that

$$B = PAQ.$$

This is the same as saying that B can be obtained from A by performing some sequence of the following operations:

- (a) add an integer multiple of one row to another,
- (b) negate some row,
- (c) reorder the rows,

and the corresponding column operations.

The following theorem is due to Smith [1] and has been reworded from the theorems and proofs in MacDuffee [1,p41] and Marcus and Minc [1,p44].

Lemma 3.2: If A is any $n \times n$ Z -matrix of rank r , then there is a unique Z -matrix

$$D = \text{diag} (a_1, a_2, \dots, a_r, 0, \dots, 0)$$

such that $A \sim D$ and

$$a_i \mid a_{i+1}$$

where the a_i are non-negative. The greatest common divisor of the $i \times i$ subdeterminants of A is

$$a_1 a_2 a_3 \dots a_i.$$

If $A \sim E$ where

$$E = \left[\begin{array}{ccc|c} a_1 & & & \\ & a_2 & & \\ & & \dots & \\ & & & a_i \\ \hline & & & F \end{array} \right]$$

then a_{i+1} is the greatest common divisor of the non-zero elements of F .

The a_i are called the invariants of A , and D is called the Smith normal form of A .

We recall the following properties :

- (i) the determinant of an Hadamard matrix of order n is $\pm n^{\frac{1}{2}n}$,
- (ii) the determinant of the incidence matrix of a (v, k, λ) configuration is $[k + (v - 1)\lambda](k - \lambda)^{v-1}$.

Then, noting that the rank of ^{the incidence matrix of} a (v, k, λ) configuration is v , we have the following theorem:

Theorem 3.3: Marcus and Minc [1, p46]. The incidence matrix of a (v, k, λ) -configuration is equivalent to a diagonal matrix with entries

$$\left\{ \begin{array}{ll} 1 & \frac{v+1}{2} \text{ times,} \\ (k-\lambda) & \frac{v-3}{2} \text{ times,} \\ k(k-\lambda) & \text{once.} \end{array} \right.$$

where $k-\lambda$ is square-free and $(k-\lambda, k)=1$.

We recall that every Hadamard matrix is equivalent to a normalized Hadamard matrix which has every element in the first row and column ± 1 .

Lemma 3.4: If A is an Hadamard matrix of order $4m$ and $A \sim D$ where $D = [a_1, a_2, \dots, a_{4m}]$ is diagonal, then $a_1 = 1$ and $a_2 = 2$.

Proof: There is no loss of generality in assuming that A is normalized.

Since every element of A is ± 1 , a_1 must be 1. Now subtract the first row from every other row, and then the first column from every other column. The resulting matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & K \end{bmatrix}$$

is equivalent to A , and every element of K is 0 or -2 .
So

$$a_2 = 2.$$

Lemma 3.5: With A and D as in lemma 3.4 $a_{4m} = 4m$.

Proof: By definition

$$a_{4m} = \pm \frac{|A|}{a_1 a_2 \dots a_{4m-1}} ;$$

the numerator is $(4m)^{2m}$, and the denominator is the greatest common divisor of the $(4m-1)$ -subdeterminants of A .

Suppose C is any $(4m-1)$ -subdeterminant of A . Then

$$A \sim \left[\begin{array}{c|cccc} \pm 1 & \pm 1 & \dots & \pm 1 \\ \hline \pm 1 & & & \\ \vdots & & & \\ \pm 1 & & & \\ \hline & & C & \end{array} \right]$$

$$\sim \left[\begin{array}{c|cccc} 1 & 1 & \dots & 1 \\ \hline 1 & & & \\ \vdots & & & \\ 1 & & & \\ \hline & & B & \end{array} \right] = F;$$

B is obtained from C by negating rows and columns, so

$$|B| = \pm |C|.$$

F is Hadamard, so

$$FF^T = 4mI_{4m};$$

but

$$FF^T = \left[\begin{array}{c|cccc} 4m & & & 0 \\ \hline 0 & & BB^T + J_{4m-1} & \end{array} \right]$$

where J_v is the $v \times v$ matrix which has every element + 1.

So

$$BB^T = 4mI_{4m-1} - J_{4m-1}.$$

Now from Ryser [1,p99] we have

$$|(r-\lambda)I_v + \lambda J_v| = \{r + (v-1)\lambda\}(r-\lambda)^{v-1},$$

whence, putting $v = r = 4m - 1$, $\lambda = -1$,

$$|B|^2 = (4m)^{4m-2}$$

$$|C| = \pm (4m)^{2m-1}.$$

This process is valid for any $(4m-1)$ -subdeterminant, so the

greatest common divisor is $(4m)^{2m-1}$, and substituting in

$$a_{4m} = \pm \frac{|A|}{a_1 a_2 \dots a_{4m-1}}$$

we have

$$a_{4m} = 4m.$$

Theorem 3.6: If m is odd and square free, then an Hadamard matrix A of order $4m$ is equivalent over Z to a diagonal matrix with invariant factors

$$\left\{ \begin{array}{ll} 1 & \text{once,} \\ 2 & 2m-1 \text{ times,} \\ 2m & 2m-1 \text{ times,} \\ 4m & \text{once.} \end{array} \right.$$

Proof: From lemmas 3.4 and 3.5 $a_1 = 1$, $a_2 = 2$, $a_{4m} = 4m$.

Since 2 must divide every invariant but a_1 , write

$$b_i = \frac{1}{2}a_i, \quad i > 1.$$

$$|A| = \pm (4m)^{2m} = \pm 2^{4m} m^{2m};$$

but on the other hand

$$\begin{aligned} |A| &= \pm \prod_{i=1}^{4m-1} a_i \\ &= \pm 2^{4m} m \prod_{i=2}^{4m-1} b_i; \end{aligned}$$

therefore

$$\prod_{i=2}^{4m-1} b_i = m^{2m-1}.$$

If p is any prime factor of m , then p^{2m-1} is a factor of this product. p^2 does not divide a_{4m} , so p^2 cannot divide any of the b_i . Hence exactly $2m-1$ of the b_i must have a factor p .

By the property

$$a_i \mid a_{i+1},$$

these must be $b_{2m+1}, \dots, b_{4m-1}$. Hence m divides each of these b_i ; the rest must all be 1.

Corollary 3.7: Any two Hadamard matrices of order $4m$, where m is odd and square-free, are $\mathbb{Z}$ -equivalent. ***

We can partially extend theorem 3.6 to the case where m is even and square-free. If H is an Hadamard matrix of order $2m$, then

$$A = \begin{bmatrix} H & H \\ H & -H \end{bmatrix}$$

is Hadamard of order $4m$. Now

$$\begin{aligned} A &\sim \begin{bmatrix} H & 0 \\ 0 & -2H \end{bmatrix} \\ &\sim \begin{bmatrix} D & 0 \\ 0 & 2D \end{bmatrix}, \end{aligned}$$

where D is the diagonal matrix of theorem 3.6 corresponding to H . (The theorem can be applied, as $\frac{1}{2}m$ is odd). Thus A is equivalent to a diagonal matrix with elements

$$\left\{ \begin{array}{ll} 1 & \text{once,} \\ 2 & m \text{ times,} \\ m & m-1 \text{ times} \\ 2m & m \text{ times} \\ 4 & m-1 \text{ times} \\ 4m & \text{once.} \end{array} \right.$$

{ This matrix, of course, is not in the Smith normal form.

There is a $(2m)$ -subdeterminant

$$1.2^m.m^{m-1} = 2^{2m-1}k,$$

where k is odd, and another

$$1.2^m.4^{m-1} = 2^{3m-2}.$$

The greatest common divisor of these is 2^{2m-1} , so

$$a_1 a_2 \dots a_{2m} \leq 2^{2m-1}.$$

On the other hand each a_i (after a_1) is divisible by 2, so

$$a_1 a_2 \dots a_{2m} \geq 2^{2m-1};$$

equality holds, and

$$a_1 = 1, \quad a_2 = a_3 = \dots = a_{2m} = 2.$$

Now we find a_{4m-1} . From an earlier result

$$a_1 a_2 \dots a_{4m-1} = (4m)^{2m-1}.$$

One $(4m-2)$ -subdeterminant is

$$\delta = 2(4m)^{2m-2},$$

obtained by deleting the elements $4m$ and $2m$. Every other $(4m-2)$ -subdeterminant can be obtained from δ by replacing one or two of its terms by $2m$ or $4m$ (or both); every term of δ divides every other $(4m-2)$ -subdeterminant. Therefore

$$a_1 a_2 \dots a_{4m-2} = 2(4m)^{2m-2},$$

$$a_{4m-1} = 2m.$$

Since m is square-free,

$$a_{2m+1} = a_{2m+2} = \dots = a_{4m-2} = 2m.$$

Theorem 3.8: If m is even and square-free, and if there is an Hadamard matrix of order $2m$, then there is an Hadamard matrix of order $4m$ of the type in theorem 3.6.

However it is possible that there are also matrices of these orders with other invariants.

Trivial cases. In the trivial cases ($n = 1$ or 2) the invariants are of the type in theorem 3.6.

A matrix of order 16. Finally we show there is an Hadamard matrix whose invariants are not in the form of theorem 3.6.

Let H be an Hadamard matrix of order 4. The invariants of H are thus $\{1, 2, 2, 4\}$. If A is the direct product $H \times H$ then

$$A \sim \text{diag}(1, 2, 2, 4) \times \text{diag}(1, 2, 2, 4).$$

This is a diagonal matrix with elements

$$\left\{ \begin{array}{ll} 1 & \text{once} \\ 2 & \text{four times} \\ 4 & \text{six times} \\ 8 & \text{four times} \\ 16 & \text{once,} \end{array} \right.$$

and clearly these are the invariants of A .

As an example of the diagonalizing process, suppose H is the Hadamard matrix of order 12 given by

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

Then theorem 3.6 tells us that the diagonal matrix

D equivalent to H has elements

$$D = [1, 2, 2, 2, 2, 2, 2, 6, 6, 6, 6, 6, 12].$$

If ~~we want to~~

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & -1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & -1 & 0 & -2 & -1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & -1 & -1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & -1 & -1 & 1 & 0 & 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 1 & 0 & 0 & -1 & 0 & -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & -1 & 0 & 0 & 1 & -1 & 1 & 0 \\ -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 \end{bmatrix}$$

and

$$Q = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & -1 & 0 & 0 & 0 & 0 & -1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & -1 & -1 & 2 & 0 & -1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & -1 & -1 & 0 & 1 & -1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & -2 & -1 & 0 & -1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$

then

$$PHQ = D.$$

CHAPTER IV : CONSTRUCTIONS FOR HADAMARD MATRICES USING SKEW - HADAMARD MATRICES

COMPUTER CONSTRUCTION OF SKEW - HADAMARD MATRICES AND A SIMILAR SKEW - HADAMARD MATRIX OF ORDER 76

Skew - Hadamard matrices (belonging to classes SI and SIII .. see page 25) have been constructed by the methods of Paley [1] and Szekeres [1] for all orders $4m < 100$ except 36, 52 and 92, cf. the table in Johnsen [1]. Blatt and Szekeres [1] have constructed a matrix of order 52 and Goethals and Seidel [2] have found one of order 36. This section is concerned with the method in Goethals and Seidel [2] and an extension of their method.

Theorem 4.1 : Goethals and Seidel [2]. If A, B, C, D are square circulant matrices of order m , and $R = (r_{ij})$ is defined by $r_{i, m-i} = 1, i = 1, \dots, m$, then if A is skew-type, and if

$$AA^T + BB^T + CC^T + DD^T = 4mI,$$

then

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

is skew - Hadamard of order $4m$.

Proof : This is easily verified using lemmas 2.15 and 2.16. ***

Theorem 4.2 : Goethals and Seidel [2]. There exist skew - Hadamard matrices of orders 36 and 52.

Proof : Apply theorem 4.1 with the following circulant matrices of order 9, where the comma denotes the middle of the string :

$$\begin{aligned} A &= + + + - + , - + - - ; & B &= + - + + - , - + + - ; \\ C &= + + - - - , - - - + ; & D &= + + + - + , + - + + . \end{aligned}$$

By inspection the skew - type A and the symmetric B,C,D are seen to satisfy the hypotheses. Hence a skew - Hadamard matrix of order 36 is obtained. Next consider the following circulant matrices of order 13 :

$$\begin{aligned} A &= + + + + - + + , - - + - - - ; \\ B &= + - + - - + + , + + - - + - ; \\ C &= D = + + - + - - - , - - + - - - . \end{aligned}$$

Applying theorem 4.1 to A,B,C,D yields a skew - Hadamard matrix of order 52. ***

As Goethals and Seidel [2] note, this method is similar to that of Williamson [1]. We now restate theorem 4.1 slightly differently to obtain the form discussed in the remainder of this section.

Theorem 4.3 : Let A,B,C and D be square matrices of order m. Further let A be skew-type and circulant and B,C,D be back-circulant matrices whose first rows satisfy the following equations :

$$(12) \quad \left\{ \begin{array}{ll} a_{1,j} = -a_{1,m+2-j} \\ b_{1,j} = b_{1,m+2-j} \\ c_{1,j} = c_{1,m+2-j} \\ d_{1,j} = d_{1,m+2-j} \\ a_{11} = b_{11} = c_{11} = d_{11} = +1, \end{array} \right. \quad 2 \leq j \leq m.$$

where $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$, $D = (d_{ij})$ and every element is +1 or -1.

Then if

$$AA^T + BB^T + CC^T + DD^T = 4mI_m,$$

H given by

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

is skew - Hadamard of order $4m$.

Using the computer programme given in appendix B (except that the case $m = 19$ is described below) we have found the matrices generated by the following first rows satisfy equations (12) and the other conditions of theorem 4.3.

$$\begin{aligned} m = 3 : \quad A &= 1 \quad -1, \quad 1 \\ B &= 1 \quad -1, \quad -1 \\ C &= 1 \quad -1, \quad -1 \\ D &= 1 \quad 1, \quad 1 \end{aligned}$$

$$\begin{aligned} m = 5 : \quad A &= 1 \quad -1 \quad -1, \quad 1 \quad 1 \\ B &= 1 \quad -1 \quad -1, \quad -1 \quad -1 \\ C &= 1 \quad -1 \quad -1, \quad -1 \quad -1 \\ D &= 1 \quad -1 \quad 1, \quad 1 \quad -1 \end{aligned}$$

$$\begin{aligned} m = 7 : \quad A &= 1 \quad -1 \quad -1 \quad -1, \quad 1 \quad 1 \quad 1 \\ B &= 1 \quad -1 \quad -1 \quad -1, \quad -1 \quad -1 \quad -1 \\ C &= 1 \quad -1 \quad -1 \quad 1, \quad 1 \quad -1 \quad -1 \\ D &= 1 \quad -1 \quad 1 \quad -1, \quad -1 \quad 1 \quad -1 \end{aligned}$$

$$\begin{aligned} m = 9 : \quad A &= 1 \quad -1 \quad -1 \quad -1 \quad 1, \quad -1 \quad 1 \quad 1 \quad 1 \\ B &= 1 \quad -1 \quad -1 \quad -1 \quad 1, \quad 1 \quad -1 \quad -1 \quad -1 \\ C &= 1 \quad 1 \quad -1 \quad 1 \quad -1 \quad -1 \quad 1 \quad -1 \quad 1 \\ D &= 1 \quad 1 \quad 1 \quad -1 \quad 1, \quad 1 \quad -1 \quad 1 \quad 1 \end{aligned}$$

$$\begin{aligned} m = 11 : \quad A &= 1 \quad -1 \quad -1 \quad -1 \quad -1 \quad 1, \quad -1 \quad 1 \quad 1 \quad 1 \quad 1 \\ B &= 1 \quad -1 \quad -1 \quad -1 \quad -1 \quad 1, \quad 1 \quad -1 \quad -1 \quad -1 \quad -1 \\ C &= 1 \quad 1 \quad -1 \quad 1 \quad -1 \quad 1, \quad 1 \quad -1 \quad 1 \quad -1 \quad 1 \\ D &= 1 \quad 1 \quad -1 \quad 1 \quad 1 \quad -1, \quad -1 \quad 1 \quad 1 \quad -1 \quad 1 \end{aligned}$$

$m = 13$: $A = 1 \ -1 \ -1 \ -1 \ -1 \ 1 \ -1, 1 \ -1 \ 1 \ 1 \ 1 \ 1$
 $B = 1 \ -1 \ 1 \ 1 \ 1 \ -1 \ 1, 1 \ -1 \ 1 \ 1 \ 1 \ -1$
 $C = 1 \ 1 \ -1 \ -1 \ 1 \ -1 \ 1, 1 \ -1 \ 1 \ -1 \ -1 \ 1$
 $D = 1 \ 1 \ 1 \ 1 \ -1 \ -1 \ 1, 1 \ -1 \ -1 \ 1 \ 1 \ 1$

$m = 15$: $A = 1 \ -1 \ -1 \ -1 \ -1 \ -1 \ 1 \ -1, 1 \ -1 \ 1 \ 1 \ 1 \ 1 \ 1$
 $B = 1 \ -1 \ 1 \ -1 \ -1 \ 1 \ 1 \ -1, -1 \ 1 \ 1 \ -1 \ -1 \ 1 \ -1$
 $C = 1 \ 1 \ -1 \ 1 \ 1 \ 1 \ 1 \ -1, -1 \ 1 \ 1 \ 1 \ 1 \ -1 \ 1$
 $D = 1 \ 1 \ 1 \ -1 \ -1 \ 1 \ -1 \ 1, 1 \ -1 \ 1 \ -1 \ -1 \ 1 \ 1$

$m = 19$: $A = 1 \ 1 \ -1 \ -1 \ 1 \ 1 \ 1 \ 1 \ -1 \ 1, -1 \ 1 \ -1 \ -1 \ -1 \ -1 \ 1 \ 1 \ -1$
 $B = 1 \ 1 \ -1 \ -1 \ -1 \ -1 \ -1 \ 1 \ 1 \ -1, -1 \ 1 \ 1 \ -1 \ -1 \ -1 \ -1 \ -1 \ 1$
 $C = 1 \ -1 \ 1 \ 1 \ -1 \ 1 \ -1 \ -1 \ -1 \ -1, -1 \ -1 \ -1 \ -1 \ 1 \ -1 \ 1 \ 1 \ -1$
 $D = 1 \ -1 \ -1 \ -1 \ 1 \ -1 \ 1 \ -1 \ -1 \ 1, 1 \ -1 \ -1 \ 1 \ -1 \ 1 \ -1 \ -1 \ -1$

So we have the theorem :

Theorem 4.4 : There exist skew Hadamard matrices of order 12, 20, 28, 36, 44, 52, 60 and 76.

We notice that our matrices for 36, 52 and 76 are different from those of Goethals and Seidel [2], Blatt and Szekeres [1] and Szekeres [1].

The matrices A, B, C, D for $m = 19$ were obtained in the following manner : 2 is a primitive root of 19, so we find the subgroup $H_0 = \{2^{3a} : a = 1, 2, \dots, 6\}$ of index 3 in the group of powers of 2 and its cosets $H_1 = 2H_0$ and $H_2 = 2^2H_0$. Then choosing A given by the quadratic residues, B, C, D by H_0, H_1 and H_2 respectively, we have all the requirements for Theorem 4.3.

The computer was not used to generate a skew - Hadamard matrix of orders 68 or larger as the time required to find a set of solutions for 60 was more than 24 hours. The original programme was much less efficient than that in Appendix B and in an attempt to further reduce the computer time we have proceeded as in Williamson [1] to analyse the matrices under the conditions of theorem 4.3.

Let T be the $m \times m$ matrix and R be the $m \times m$ matrix

$$(13) \quad T = \begin{bmatrix} \overline{0} & 1 & 0 & \dots & \overline{0} \\ 0 & 0 & 1 & \dots & 0 \\ \cdot & \cdot & \cdot & \dots & \cdot \\ 0 & 0 & 0 & \dots & 1 \\ \underline{1} & 0 & 0 & \dots & \underline{0} \end{bmatrix}, \quad T^m = I_m, \quad R = \begin{bmatrix} \overline{0} & \dots & 0 & 0 & \overline{1} \\ 0 & \dots & 0 & 1 & 0 \\ \cdot & \dots & \cdot & \cdot & \cdot \\ 0 & \dots & 0 & 0 & 0 \\ \underline{1} & \dots & 0 & 0 & \underline{0} \end{bmatrix}$$

Polynomials in T commute with each other. So consider

$$(14) \quad \left\{ \begin{array}{l} A = a_{11}I + a_{12}T + \dots + a_{1m}T^{m-1}, \\ B = (b_{11}I + b_{12}T + \dots + b_{1m}T^{m-1})R, \\ C = (c_{11}I + c_{12}T + \dots + c_{1m}T^{m-1})R, \\ D = (d_{11}I + d_{12}T + \dots + d_{1m}T^{m-1})R, \end{array} \right.$$

where $a_{1i}, b_{1i}, c_{1i}, d_{1i}$ are given by equations (12).

Then provided

$$(15) \quad AA^T + BB^T + CC^T + DD^T = 4mI_m$$

we have all the conditions of theorem 4.3 satisfied and so

we would have a skew - Hadamard matrix of order $4m$.

Now let us consider equation (15) further .

Write

$$(16) \quad A = P_1 - N_1$$

with P_1 the sum of the terms with positive coefficient in A and

$-N_1$ the sum of the terms with negative coefficient in A , whence

$$(17) \quad P_1 = \sum_j a_{1j}T^{j-1}, \quad a_{1j} = +1, \quad -N_1 = \sum_j a_{1j}T^{j-1}, \quad a_{1j} = -1.$$

In the same way write

$$(18) \quad B = P_2 - N_2, \quad C = P_3 - N_3, \quad D = P_4 - N_4.$$

Since $a_{11} = +1$ and by (12) $a_{1j} = -a_{1,m+2-j}$, $2 \leq j \leq m$,

there are

$$(19) \quad \frac{m+1}{2} = p_1$$

positive terms in A , so the number of terms in P_1 is an odd number if $m \equiv 1(\text{mod } 4)$ and an even number if $m \equiv 3(\text{mod } 4)$.

Since by (12) $b_{11} = +1$ and $b_{1j} = b_{1,m+2-j}$, $2 \leq j \leq m$, the positive terms occur in pairs, so p_2 , the number of positive terms in P_2 , is an odd number. Similarly p_3 and p_4 are odd numbers.

We now write

$$(20) \quad J = I + T + T^2 + \dots + T^{m-1} = (I + T + T^2 + \dots + T^{m-1})R.$$

Then

$$(21) \quad P_i + N_i = J, \quad i = 1, 2, 3, 4,$$

so (15) becomes

$$AA^T + B^2 + C^2 + D^2 = 4mI_m$$

and by (16), (17), (18) this becomes

$$(2P_1 - J)(2P_1 - J)^T + (2P_2 - J)^2 + (2P_3 - J)^2 + (2P_4 - J)^2 = 4mI_m,$$

$$\text{that is } (2P_1 - J)(-2P_1 + J + 2I) + (2P_2 - J)^2 + (2P_3 - J)^2 + (2P_4 - J)^2 = 4mI_m,$$

since A is skew-symmetric. So we have since $P_i J = p_i J$ and $J^2 = mJ$

$$(22) \quad 4(-P_1^2 + P_2^2 + P_3^2 + P_4^2 + P_1) + 4(p_1 - p_2 - p_3 - p_4)J + (2m - 2)J = 4mI_m.$$

Now from (19)

$$4p_1 + 2m - 2 = 4m$$

so (22) becomes

$$(23) \quad (-P_1^2 + P_2^2 + P_3^2 + P_4^2 + P_1) = -(m - p_2 - p_3 - p_4)J + mI_m.$$

odd then since
If m is / p_2, p_3 and p_4 are all odd, we have the coefficients of J are all even.

Now we notice B, C, D are polynomials in $T^j R$ so

$$P_i = \left(\sum_j e_{1j} T^{j-1} \right) R$$

for $i = 2, 3, 4$ and $e_{1j} = b_{1j}, c_{1j}, d_{1j}$ respectively, also

$$P_i = P_i^T \text{ so}$$

$$P_i^2 = P_i P_i^T = \left(\sum_j e_{1j} T^{j-1} \right) R R^T \left(\sum_k e_{1k} T^{k-1} \right) = \sum_n f_n T^n,$$

that is $P_1^2, P_2^2, P_3^2, P_4^2$ and P_1 may all be regarded as polynomials in T .

For each $t = 1, \dots, m-1$, there is a unique s such that $(T^s)^2 = T^t$. In $P_j^2 = (\sum T^k)^2$, k in a subset of $1, 2, \dots, m$, we have

$$P_j^2 \equiv \sum T^{2k} \pmod{2}.$$

Then since the coefficient of J in (23) is always even we have shown :

Theorem 4.5 : If m is odd, T is given by (13), P_1, P_2, P_3, P_4 are the terms with positive coefficients of A, B, C, D as defined by (14), respectively, and if

$$AA^T + BB^T + CC^T + DD^T = 4mI$$

then writing $P_1 + P_1^2 = \sum_{i \neq 0} f_i T^i$ and $P_2^2 + P_3^2 + P_4^2 = \sum_{i \neq 0} g_i T^i$

we have $g_i = f_i \pmod{2}$ when $i \neq 0$.

4.2 Constructions for skew - Hadamard and n - type matrices of the form "power plus one".

The following theorem was proved independently by J. Wallis [4] and Belevitch [1] for W the core of an n - type matrix and by J. Wallis [4] and Goethals and Seidel [1, p.1008] for W the core of a skew - Hadamard matrix :

Theorem 4.6 : If h is the order of (i) an n - type matrix (ii) a skew - Hadamard matrix then there is an n - type matrix of order $(h-1)^2 + 1$.

Proof : Let W be the core of the matrix of order h .

Define A by

$$A = J \times -I + I \times J + W \times W$$

then

$$\begin{aligned} AA^T &= (n-1)J_{n-1} \times I_{n-1} + I_{n-1} \times (n-1)J_{n-1} + [(n-1)I_{n-1} - J_{n-1}] \times [(n-1)I_{n-1} - J_{n-1}] \\ &\quad - 2J_{n-1} \times J_{n-1} \\ &= (n-1)^2 I_{(n-1)^2} - J_{(n-1)^2} . \end{aligned}$$

Now $A^T = A$ if $W \times W = W^T \times W^T$, but this is true for W

from either n - type or skew Hadamard matrices and so

$$M = \begin{bmatrix} 0 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & A & \\ 1 & & & \end{bmatrix} + I_{(n-1)^2 + 1}$$

is an n - type matrix of order $(n-1)^2 + 1$.

The line of proof of lemma 4.8 and theorem 4.9 are due to W.D. Wallis; we include these theorems as they greatly simplify our proofs later in this section.

Definition 4.7 : Let $A = [a_{ij}]$ and $C = [c_{ij}]$ be two matrices of order n . The *Hadamard product* $A * C$ of A and C is given by

$$A * C = [a_{ij} c_{ij}].$$

Lemma 4.8 : When A, B, C, D are matrices of the same order,

$$(A \times B) * (C \times D) = (A * C) \times (B * D).$$

Proof : $(A \times B) * (C \times D) = [a_{ij} B] * [c_{ij} D]$

$$= [a_{ij} c_{ij} B * D]$$

$$= (A * C) \times (B * D).$$

Theorem 4.9 : Suppose I, J and W are of order h , where W is a matrix with zero diagonal and $+1$ or -1 elsewhere. Suppose A is a matrix of order $q = h^p$ which is of the form

$$A = B_1 + B_2 + \dots + B_k$$

where each B_i is a Kronecker product of p terms I, J or W in some order, such that (a) each B_i contains at least one term W ,

(b) for any two summands B_i and B_j there is a position r such that one of the summands has I in the r th position and the other has W in that position,

and suppose A satisfies

$$AA^T = qI_q - J_q,$$

Then A has zero diagonal and $+1$ or -1 in every other place.

Proof : Clearly

$$W * I = I * W = 0;$$

so, by part (b) of the hypothesis and lemma 4.8

$$B_i * B_j = B_j * B_i = 0$$

whenever $i \neq j$.

Hence no two B_i have non-zero elements in the same position, so each non-zero element of A comes from exactly one of the B_i ; since each B_i is a $(0,1,-1)$ matrix it follows that A is a

$(0,1,-1)$ matrix. But

$$AA^T = qI_q - J_q,$$

so if $A = (a_{ij})$

$$\sum_j a_{ij}^2 = q - 1$$

for any i : therefore at most one element in any row of A is zero.

W appears in each B_i , and W has zero diagonal, so each B_i - and

consequently A - has zero diagonal. So we have the result. ***

The next theorem was proved independently by J. Wallis [4] and Belevitch [1] for n - type matrices.

Theorem 4.10 : Let n be the order of an n - type matrix then there is an n - type matrix of order $(n-1)^3 + 1$.

Proof : Let W be the core of the n - type matrix of order n , then with W, J and I all of order $n-1$ we define

$$A = I \times W \times J + J \times I \times W + W \times J \times I + W \times W \times W.$$

Now $WJ = 0$, so $A(J \times J \times J) = 0$, and as $W^T = W$, $A^T = A$. If we call the terms B_1, B_2, B_3, B_4 we see

$$B_i B_j^T = 0$$

for $i \neq j$, since for every pair B_i and B_j there is an r such that J occurs in the r th place in one of the B_i, B_j and W occurs in the r th place of the other, Also

$JW^T = WJ = 0$. For example for B_1 and B_2

$$(I \times W \times J)(J \times I \times W^T) = I \times W \times JW^T = 0$$

and for B_3 and B_4

$$(W \times J \times I)(I \times W^T \times J) = W \times JW^T \times J = 0.$$

So

$$\begin{aligned} AA^T &= \sum_{i=1}^4 B_i B_i^T \\ &= I \times [(n-1)I - J] \times (n-1)J + (n-1)J \times I \times [(n-1)I - J] \\ &\quad + [(n-1)I - J] \times (n-1)J \times I + [(n-1)I - J] \times [(n-1)I - J] \times [(n-1)I - J] \\ &= (n-1)^2 I \times I \times J - (n-1) I \times J \times J + (n-1)^2 J \times I \times I - (n-1) J \times I \times J \\ &\quad + (n-1)^2 I \times J \times I - (n-1) J \times J \times I \\ &\quad + (n-1)^3 I \times I \times I - (n-1)^2 I \times I \times J - (n-1)^2 I \times J \times I + (n-1) I \times J \times J \\ &\quad - (n-1)^2 J \times I \times I + (n-1) J \times I \times J + (n-1) J \times J \times I - J \times J \times J \\ &= (n-1)^3 I \times I \times I - J \times J \times J. \end{aligned}$$

Hence A satisfies all the equations necessary for the core of an n -type matrix of order $(n-1)^3 + 1$. It remains to show that A has zero diagonal and $+1$ or -1 elsewhere.

By inspection A satisfies all the conditions of theorem 4.9 and so we have the result. ***

The following theorem of Goldberg [1] is proved in J.Wallis [4] and here in a slightly different manner, and is almost identical with the previous theorem.

Theorem 4.11 : If h is the order of a skew - Hadamard matrix then there is a skew - Hadamard matrix of order $(h-1)^3 + 1$.

Proof : Let W of order $h-1$ be the core of the skew - Hadamard matrix, then with I and J of order $h-1$ we define

$$B = I \times W \times J + W \times J \times I + J \times I \times W + W \times W \times W.$$

Since $WJ = 0$ and $W^T = -W$ we see $B(J \times J \times J) = 0$ and $B^T = -B$.

Now for each pair of terms there is an r such that J occurs in the r th place of one of the terms and W occurs in the r th place of the other term so

$$\begin{aligned} BB^T &= I \times WW^T \times J^2 + WW^T \times J^2 \times I + J^2 \times I \times WW^T + WW^T \times WW^T \times WW^T \\ &= I \times [(h-1)I - J] \times (h-1)J + [(h-1)I - J] \times (h-1)J \times I \\ &\quad + (h-1)J \times I \times [(h-1)I - J] + [(h-1)I - J] \times [(h-1)I - J] \times [(h-1)I - J] \\ &= (h-1)^3 I \times I \times I - J \times J \times J. \end{aligned}$$

as B satisfies the conditions of theorem 4.9 so we see B has zero diagonal and all other elements of B are $+1$ or -1 .

So B is the core of a skew-Hadamard matrix of order $(h-1)^3 + 1$ and we have the result. ***

Corollary 4.12 : Let W of order $h-1$ be the core of a skew - Hadamard matrix then

$$B = W \times W \times W + I \times J \times W + J \times W \times I + W \times I \times J$$

is the core of a skew - Hadamard matrix of order $(h-1)^3+1$. ***

Theorem 4.11 and corollary 4.12 show us that the construction formulae are not unique.

The next theorems are also found in J.Wallis [5] but the proofs we give here are much more complete.

Theorem 4.13 : If I, J, W are of order h and W is a core then B given by

$$B = W \times W \times W \times W \times W + \Sigma^1 I \times J \times [W \times W + I \times J] \times W,$$

where Σ^1 is defined in §1.3, is a core of order h^5 .

Proof : Since $WJ = 0$, $B(J \times J \times J \times J \times J) = 0$. We now exhibit

B in full so we may check that there is a W in every term

corresponding to a J in each other term. This ensures that in BB^T

there is no contribution from term (1) • term (2)^{transpose} as

..... WJ or JW^T always occurs.

$$B = I \times J \times W \times W \times W + I \times J \times I \times J \times W + W \times W \times W \times W \times W$$

$$J \times W \times W \times W \times I \quad J \times I \times J \times W \times I$$

$$W \times W \times W \times I \times J \quad I \times J \times W \times I \times J$$

$$W \times W \times I \times J \times W \quad J \times W \times I \times J \times I$$

$$W \times I \times J \times W \times W \quad W \times I \times J \times I \times J$$

Term Number											Formula
1	2	3	4	5	6	7	8	9	10	11	h^5 IIIII
		h^4								$-h^4$ IIIIJ	
			h^4							$-h^4$ IIIJI	
			$-h^3$							h^3 IIIJJ	
				h^4						$-h^4$ IIJII	
		$-h^3$		$-h^3$				h^3	h^3	IIJIJ	
				$-h^3$						h^3 IIJJI	
				h^2						$-h^2$ IIJJJ	
h^4										$-h^4$ IJIII	
$-h^3$		$-h^3$					h^3			h^3 IJIIJ	
$-h^3$			$-h^3$		h^3					h^3 IJJIJ	
h^2			h^2		$-h^2$					$-h^2$ IJIIJJ	
$-h^3$										h^3 IJJII	
h^2		h^2					$-h^2$			$-h^2$ IJJIJ	
h^2										$-h^2$ IJJJI	
$-h$										h IJJJJ	
	h^4									$-h^4$ JIIII	
		$-h^3$								h^3 JIIIJ	
	$-h^3$		$-h^3$					h^3		h^3 JIIJI	
			h^2							$-h^2$ JIIJJ	
	$-h^3$			$-h^3$		h^3				h^3 JIIJII	
		h^2		h^2					$-h^2$	$-h^2$ JIIJIJ	
	h^2			h^2		$-h^2$				$-h^2$ JIIJJI	
				$-h$						h JIIJJJ	
	$-h^3$									h^3 JJI III	
		h^2								$-h^2$ JJI IIJ	
	h^2		h^2					$-h^2$		$-h^2$ JJI IJI	
			$-h$							h JJI IJJ	
	h^2									$-h^2$ JJJ II	
		$-h$								h JJJ IJ	
	$-h$									h JJJ JI	
										-1 JJJ JJ	

TABLE 3

Proof : B is the sum of twenty nine separate terms : write

$$B = \sum_{i=1}^{29} B_i.$$

We write out the summands of B fully and the number after the term will be called the term number and indicates the B_i to which the term belongs. For example

$$B_6 = W \times W \times W \times I \times J \times W \times W.$$

$$\begin{aligned}
 B = & W \times W \times W \times W \times W \times W \times W^1 \\
 & + I \times J \times W \times W \times W \times W \times W^2 + I \times J \times W \times W \times I \times J \times W^9 \\
 & + J \times W \times W \times W \times W \times W \times I^3 + J \times W \times W \times I \times J \times W \times I^{10} \\
 & + W \times W \times W \times W \times W \times I \times J^4 + W \times W \times I \times J \times W \times I \times J^{11} \\
 & + W \times W \times W \times W \times I \times J \times W^5 + W \times I \times J \times W \times I \times J \times W^{12} \\
 & + W \times W \times W \times I \times J \times W \times W^6 + I \times J \times W \times I \times J \times W \times W^{13} \\
 & + W \times W \times I \times J \times W \times W \times W^7 + J \times W \times I \times J \times W \times W \times I^{14} \\
 & + W \times I \times J \times W \times W \times W \times W^8 + W \times I \times J \times W \times W \times I \times J^{15} \\
 & + I \times J \times I \times J \times W \times W \times W^{16} + I \times J \times I \times J \times I \times J \times W^{23} \\
 & + J \times I \times J \times W \times W \times W \times I^{17} + J \times I \times J \times I \times J \times W \times I^{24} \\
 & + I \times J \times W \times W \times W \times I \times J^{18} + I \times J \times I \times J \times W \times I \times J^{25} \\
 & + J \times W \times W \times W \times I \times J \times I^{19} + J \times I \times J \times W \times I \times J \times I^{26} \\
 & + W \times W \times W \times I \times J \times I \times J^{20} + I \times J \times W \times I \times J \times I \times J^{27} \\
 & + W \times W \times I \times J \times I \times J \times W^{21} + J \times W \times I \times J \times I \times J \times I^{28} \\
 & + W \times I \times J \times I \times J \times W \times W^{22} + W \times I \times J \times I \times J \times I \times J^{29}
 \end{aligned}$$

We see that each B_i has a W in its formula and so each B_i , and consequently B, has zero diagonal. By inspection we see that if there is a J in the r th position of B_i then there is a W in that position of B_j for some r, that is, since $JW^T = WJ = 0$

$$B_i B_j^T = 0 \quad \text{for every } j \neq i.$$

Hence

$$BB^T = \sum_{i=1}^{29} B_i B_i^T$$

and from $J^2 = hJ$, $WW^T = hI - J$ and the table of appendix C we have

$$BB^T = gI_g - J_g$$

where $g = h^7$. Now $B(J \times J \times J \times J \times J \times J \times J) = 0$ since each B_i contains a W in its formula and so B is a core of order h^7 . ***

Corollary 4.17: If I, J, W are of order h and W is a core then B

given by $B = W \times W \times W \times W \times W \times W \times W + \Sigma' I \times J \times [W \times W + I \times J] \times W \times W \times W$

$$+ \Sigma' J \times W \times I \times J \times [W \times I \times W + J \times I \times I]$$

is a core of order h^7 .

Proof: We proceed exactly as in theorem 4.16 except that B is now

given by

$$\begin{aligned} B = & W \times W \times W \times W \times W \times W \times W^1 \\ & + I \times J \times W \times W \times W \times W \times W^2 + I \times J \times I \times J \times W \times W \times W^{14} \\ & + J \times W \times W \times W \times W \times W \times I^3 + J \times I \times J \times W \times W \times W \times W^{15} \\ & + W \times W \times W \times W \times W \times I \times J^4 + I \times J \times W \times W \times W \times I \times J^9 \\ & + W \times W \times W \times W \times I \times J \times W^5 + J \times W \times W \times W \times I \times J \times I^{10} \\ & + W \times W \times W \times I \times J \times W \times W^6 + W \times W \times W \times I \times J \times I \times J^{11} \\ & + W \times W \times I \times J \times W \times W \times W^7 + W \times W \times I \times J \times I \times J \times W^{12} \\ & + W \times I \times J \times W \times W \times W \times W^8 + W \times I \times J \times I \times J \times W \times W^{13} \\ & + J \times W \times I \times J \times W \times I \times W^{20} + J \times W \times I \times J \times J \times I \times I^{26} \\ & + W \times I \times J \times W \times I \times W \times J^{21} + W \times I \times J \times J \times I \times I \times J^{29} \\ & + I \times J \times W \times I \times W \times J \times W^{17} + I \times J \times J \times I \times I \times J \times W^{24} \\ & + J \times W \times I \times W \times J \times W \times I^{19} + J \times J \times I \times I \times J \times W \times I^{27} \\ & + W \times I \times W \times J \times W \times I \times J^{22} + J \times I \times I \times J \times W \times I \times J^{28} \\ & + I \times W \times J \times W \times I \times J \times W^{16} + I \times I \times J \times W \times I \times J \times J^{25} \\ & + W \times J \times W \times I \times J \times W \times I^{18} + I \times J \times W \times I \times J \times J \times I^{23} \end{aligned}$$

Now proceeding as in theorem 4.16 and using the other table of appendix C we have the result. ***

We see that theorem 4.16 and corollary 4.17 imply that

$$\Sigma' I \times J \times [W \times W + I \times J] \times I \times J \times W = \Sigma' J \times W \times I \times J \times [W \times I \times W + J \times I \times I]$$

that is

$$\Sigma' J \times W \times I \times J \times [W \times W \times I + I \times J \times I] = \Sigma' J \times W \times I \times J \times [W \times I \times W + J \times I \times I].$$

This latter implies that there might possibly be more formulae with the square bracket replaced by permutations of the letters inside.

Theorem 4.16 and Corollary 4.17 show us that the formula for obtaining the core of order h^7 is not unique.

Theorem 4.18 : If n is the order of an n -type matrix then there is an n -type matrix of order $(n-1)^7 + 1$.

Proof : Using theorem 4.16 we see that if W is the core of an n -type matrix then $B^T = B$ and $BJ_{(n-1)^7} = 0$. So provided $B + I$ is a $(1, -1)$ matrix, B is the core of an n -type matrix of order $(n-1)^7 + 1$, but clearly B satisfies the conditions of theorem 4.9 and so we have the result. ***

Theorem 4.19 : If h is the order of a skew - Hadamard matrix then there is a skew - Hadamard matrix of order $(h-1)^7 + 1$.

Proof : Using theorem 4.16 we see that if W is the core of a skew - Hadamard matrix then $B^T = -B$ and $BJ_{(h-1)^7} = 0$. Now the definition of B and theorem 4.9 show $B + I$ is a $(1, -1)$ matrix, so B is the core of a skew - Hadamard matrix of order $(h-1)^7 + 1$. ***

Since the core obtained in corollary 4.17 also satisfies the conditions of theorem 4.9 we see that our n -type and skew - Hadamard matrices of theorems 4.18 and 4.19 are not unique.

Corollary 4.20 : If n is the order of an n -type matrix then there is an n -type matrix of order $(n-1)^u + 1$ where $u = 2^a 3^b 5^c 7^d$ and a, b, c, d are non-negative integers.

Proof: This result follows by combining the results of theorems 4.6, 4.10, 4.14 and 4.18. ***

Corollary 4.21 : If h is the order of a skew-Hadamard matrix then there is an n -type matrix of order $(h-1)^u + 1$ where $u = 2^a 3^b 5^c 7^d$ and b, c, d are non-negative integers while a is a positive integer.

Proof : This result follows by combining the results of theorems 4.6, 4.10, 4.14 and 4.18. ***

Corollary 4.22 : If h is the order of a skew-Hadamard matrix then there is a skew-Hadamard matrix of order $(h-1)^u + 1$ where $u = 3^b 5^c 7^d$ and b, c, d are non-negative integers.

Proof : This result follows by combining the results of theorems 4.11, 4.15 and 4.19. ***

§4.3 NEW CLASSES OF HADAMARD MATRICES.

All the work in this section is original. It also appears in J. Wallis [2], [3], [7], except that the main results of [2] and [7] become corollaries of the more powerful theorems 4.23 and 4.26. Theorems 4.23, 4.24 and 4.25 use (v, k, λ) -configurations with $v \equiv 3 \pmod{4}$ while theorems 4.26 and 4.28 use $v \equiv 1 \pmod{4}$.

Theorem 4.23 : If there exists

- (i) a skew-Hadamard matrix $H = U + I$ of order h ,
- (ii) m -type matrices $M = W + I$ and $N = N^T$ of order m , and
(1, -1)
- (iii) three matrices X, Y, Z of order $x \equiv 3 \pmod{4}$ satisfying
 - (a) XY^T, YZ^T and ZX^T all symmetric, and
 - (b) $XX^T = aI_x + bJ_x$

$$YY^T = \left\{ \frac{m+mx-mh-a}{x-1} \right\} I + \left\{ \frac{mh-m-b}{m-1} \right\} J$$

$$ZZ^T = (x+1) I_x - J_x$$

then

$$\bar{H} = U \times N \times Z + I_h \times W \times Y + I_h \times I_m \times X$$

is an Hadamard matrix of order $m \times h$.

Proof : Since H is skew - Hadamard $U^T = -U$ and $UU^T = (h-1)I_h$.

$M = W + I$ and N being m -type means $W^T = -W$, $WW^T = (m-1)I_m$,

$MN^T = NM^T$, $MM^T = NN^T = mI_m$ and $N^T = N$. Now lemma 2.25 shows $WN^T = NW^T$,

$$\begin{aligned} \bar{H}\bar{H}^T &= (U \times N \times Z + I_h \times W \times Y + I_h \times I_m \times X)(U^T \times N^T \times Z^T + I_h \times W^T \times Y^T + I_h \times I_m \times X^T) \\ &= UU^T \times NN^T \times ZZ^T + I_h \times WW^T \times YY^T + I_h \times I_m \times XX^T \\ &\quad + U^T \times WN^T \times YZ^T + U \times NW^T \times ZY^T + U^T \times N^T \times XZ^T + U \times N \times ZX^T \\ &\quad + I_h \times W^T \times XY^T + I_h \times W \times YX^T \\ &= UU^T \times NN^T \times ZZ^T + I_h \times WW^T \times YY^T + I_h \times I_m \times XX^T \\ &\quad + (U + U^T) \times WN^T \times YZ^T + (U^T + U) \times N \times ZX^T + I_h \times (W + W^T) \times XY^T \\ &= (h-1)I_h \times mI_m \times \{(x+1)I_x - J_x\} \\ &\quad + I_h \times I_m \times \{(m+mx-mh-a)I_x + (mh-m-b)J_x\} + I_h \times I_m \times \{aI_x + bJ_x\} \\ &= I_{mh} \times \{[m(h-1)(x+1) + m + mx - mh]I_x - [m(h-1)-mh + m]J_x\} \\ &= mxhI_{mxh}. \end{aligned}$$

Which completes the proof. ***

Let H of order $x+1$ be any Hadamard matrix written in the form

$$(24) \quad H = \begin{bmatrix} \overline{1} & 1 & \dots & \overline{1} \\ 1 & & & \\ \vdots & & F & \\ \overline{1} & & & \end{bmatrix}$$

Then $FF^T = (x+1)I - J$ and if

$$(25) \quad E = FG$$

where G is the back diagonal matrix, then $FE^T = FG^T F^T = FGF^T = EF^T$.

Then using theorem 4.23 we have

Corollary 4.24 : If $x + 1$ is the order of any Hadamard matrix and m is the order of m -type matrices then if there is a skew - Hadamard matrix of order

$$(i) \frac{(x+1)(m-1)}{m}, \quad (ii) \frac{(x-3)(m-1)}{m}, \quad (iii) x+1, \quad (iv) x-3.$$

then there is an Hadamard matrix of order

$$(i) x(x+1)(m-1), \quad (ii) x(x-3)(m-1), \quad (iii) x(x+1), \quad (iv) x(x-3)$$

Proof : The proof follows from theorem 4.23 with F and E as in (24) and (25) and (i) $X = F$, $Y = J$, $Z = E$; (ii) $X = F$, $Y = K$, $Z = E$; (iii) $X = J$, $Y = F$, $Z = E$ and $m = 1$; (iv) $X = J-2I$, $Y = F$, $Z = E$ and $m=1$. (iii) and (iv) were given in J.Wallis [7]. ***

Corollary 4.25 : If there is a skew - Hadamard matrix of order

$$(i) \frac{m(x-3)-4(q^{n-1}-1)}{m} \quad (ii) \frac{m(x+1-4q^{n-1})+4(q^{n-1}-1)}{m}$$

where m is the order of m -type matrices, q a prime power, and y and $y+2$ odd primes, $x = q^n + q^{n-1} + \dots + q + 1 \equiv 3 \pmod{4}$, and $x = y$ or

or $x = y(y+2)$ then there is an Hadamard matrix of order

$$(i) [m(x-3)-4(q^{n-1}-1)]x \quad (ii) [m(x+1-4q^{n-1})+4(q^{n-1}-1)]x$$

respectively.

Proof : If P is the circulant matrix generated by an

$(x, \frac{x+1}{2}, \frac{x+1}{4})$ configuration and Q is back circulant (from table 1)

then the proof follows with (i) $X = Q$, $Y = J-2I$, $Z = P$,

(ii) $X = J-2I$, $Y = Q$, $Z = P$ in theorem 4.23 ***

Until the end of this section p is a prime or prime power $\equiv 1 \pmod{4}$.

If F is a symmetric matrix of order p satisfying

$$FJ = JF = 0, \quad FF^T = pI - J$$

then writing $X = F + I_p$, $Y = F - I_p$ we have

$$\begin{aligned} XY^T &= (F + I_p)(F^T - I_p) = FF^T - I_p = (F - I_p)(F^T + I_p) = YX^T \quad \text{and} \\ XX^T + YY^T &= (FF^T + 2F + I_p) + (FF^T - 2F + I_p) = 2(p+1)I_p - 2J_p. \end{aligned}$$

For the remainder of this section if

(i) p is a prime power choose F to be the symmetric matrix A of §1.4. So

$$(26) \quad X = A + I_p, \quad Y = A - I_p;$$

(ii) p is prime, choose F to be the circulant symmetric matrix B of §1.4. So

$$(27) \quad X = B + I_p, \quad Y = B - I_p.$$

In both cases $XY^T = YX^T$ and $XX^T + YY^T = 2(p+1)I_p - 2J_p$.

Theorem 4.26 : If there exist

- (i) a skew-Hadamard matrix of order h ,
- (ii) four $(+1, -1)$ matrices X, Y, Z, W of order $p \equiv 1 \pmod{4}$, satisfying
 - (a) $XY^T, XZ^T, XW^T, YZ^T, YW^T, ZW^T$ all symmetric and
 - (b) $XX^T + YY^T = 2(p+1)I_p - 2J_p$

$$WW^T = aI_p + bJ_p$$

$$ZZ^T = \{m(p+1-h-a) + a\}I_p + \{m(h-1-b) + b\}J_p$$

where $m = 2$ or 4 , then there is an Hadamard matrix of order mph .

Proof : If $m = 2$ use

$$M = \begin{bmatrix} \overline{Z} & \overline{W} \\ -\overline{W} & \overline{Z} \end{bmatrix} \quad \text{and} \quad N = \begin{bmatrix} \overline{X} & \overline{Y} \\ \overline{Y} & -\overline{X} \end{bmatrix}$$

for $m = 4$ use

$$M = \begin{bmatrix} \overline{Z} & \overline{W} & \overline{W} & \overline{W} \\ -\overline{W} & \overline{Z} & -\overline{W} & \overline{W} \\ -\overline{W} & \overline{W} & \overline{Z} & -\overline{W} \\ -\overline{W} & -\overline{W} & \overline{W} & \overline{Z} \end{bmatrix} \quad \text{and} \quad N = \begin{bmatrix} \overline{X} & \overline{Y} & \overline{X} & \overline{Y} \\ \overline{Y} & -\overline{X} & \overline{Y} & -\overline{X} \\ \overline{X} & \overline{Y} & -\overline{X} & -\overline{Y} \\ \overline{Y} & -\overline{X} & -\overline{Y} & \overline{X} \end{bmatrix}$$

Then since ZW^T and XY^T are symmetric

$$MN^T = NM^T$$

and

$$MM^T = m(p+1-h)I_p + m(h-1)J_p \times I_m$$

$$NN^T = m(p+1)I_p - mJ_p \times I_m.$$

Now H is Hadamard so $HH^T = hI_h = UU^T + I_h$ and

$$\overline{H} = U \times N + I_h \times M$$

is the required Hadamard matrix of order mph since

$$\begin{aligned} \overline{H} \overline{H}^T &= (U \times N + I_h \times M)(U^T \times N^T + I_h \times M^T) \\ &= UU^T \times NN^T + U^T \times MN^T + U \times NM^T + I_h \times MM^T \\ &= (h-1)I_h \times \{m(p+1)I_p - mJ_p\} \times I_m \\ &\quad + I_h \times \{m(p+1-h)I_p + m(h-1)J_p\} \times I_m \\ &= mphI_{mph}. \end{aligned}$$

Which completes the proof.

Theorem 4.27 : If $h \equiv 0 \pmod{4}$ is the order of a skew-Hadamard matrix and $2h + 3$ is a prime then there is an Hadamard matrix of order $2h(h+1)$.

Proof : Szekeres' [1] construction for primes $\equiv 3 \pmod{4}$ gives two complementary difference sets of order $h+1$.

Use one of these two sets to generate a circulant matrix, X , and the other to generate a back circulant matrix, Y . Then with $Z = J$, $W = J - 2I$, $p = h+1$ and $m = 2$, theorem 4.26 gives the result. ***

We now investigate when the conditions of theorem 4.26 are satisfied. X and Y will always mean those circulant symmetric matrices defined by (27), *except for case (i) below where X and Y are given by (26).*

Corollary 4.28 : Let p^r be a prime power $\equiv 1 \pmod{4}$, q be a prime power (may be a power of 2), x and a odd, and $m = 2$ or 4 , then if there is a skew-Hadamard matrix of order

$$(i) p^r - 1; (ii) p + 1 - \frac{4q^{n-1}}{m}; \text{ where } p = q^n + q^{n-1} + \dots + q + 1,$$

$$n \text{ a positive integer; (iii) } p + 1 - 4q^{n-1} + \frac{4q^{n-1}}{m}, \text{ with } p \text{ as in (ii);}$$

$$(iv) p + 1 - 4q^{n-1} + \frac{4(q^{n-1} - 1)}{m}, \text{ with } p \text{ as in (ii);}$$

$$(v) p - 3 - \frac{4(q^{n-1} - 1)}{m}, \text{ with } p \text{ as in (ii); (vi) } \frac{5x^2 + 3}{2}, \text{ where}$$

$$p = 4x^2 + 1; (vii) \frac{13x^2 - 5}{4}, \text{ where } p = 4x^2 + 1; (viii) \frac{7x^2 + 1}{4},$$

$$\text{where } p = 4x^2 + 1; (ix) \frac{5x^2 + 11}{2}, \text{ where } p = 4x^2 + 9;$$

$$(x) 2(25b^2 + 3), \text{ where } p = 8a^2 + 1 = 64b^2 + 9, \text{ } b \text{ odd}$$

$$(xi) 2(25b^2 + 173), \text{ where } p = 8a^2 + 49 = 64b^2 + 441, \text{ } b \text{ even;}$$

$$(xii) 57b^2 + 391, \text{ where } p \text{ and } b \text{ are as in (x); (xiii) } 43b^2 + 297,$$

where p and b are as in (x); then there is an Hadamard matrix of order

$$(i) 2p^r(p^r - 1); (ii) [m(p + 1) - 4q^{n-1}]p, (iii) [m(p + 1 - 4q^{n-1})]p;$$

$$(iv) [m(p + 1 - 4q^{n-1}) + 4(q^{n-1} - 1)]p; (v) [m(p - 3) - 4(q^{n-1} - 1)]p,$$

(vi) $(5x^2 + 3)(4x^2 + 1)$; (vii) $(13x^2 - 5)(4x^2 + 1)$;
 (viii) $(7x^2 + 1)(4x^2 + 1)$; (ix) $(5x^2 + 11)(4x^2 + 9)$;
 (x) $4(25b^2 + 3)(64b^2 + 9)$; (xi) $4(25b^2 + 173)(64b^2 + 441)$;
 (xii) $4(57b^2 + 391)(64b^2 + 441)$; (xiii) $4(43b^2 + 297)(64b^2 + 441)$;
 respectively.

Proof : We use the notation of Table 1, and each matrix for Z and W if it is not J or $J-2I$ is back circulant. In cases (ii) (iii), (iv) and (v) m is not evaluated as q may be a power of 2. The corollary follows with the following substitutions in theorem 4.26 :

(i) $m = 2$, $Z = J-2I$, $W = J$; (ii) $Z = S$, $W = J$; (iii) $Z = J$, $W = S$; (iv) $Z = J-2I$, $W = S$; (v) $Z = S$, $W = J-2I$; (vi) $m = 2$, $Z = B$, $W = J$; (vii) $m = 4$, $Z = B$, $W = J-2I$; (viii) $m = 4$, $Z = J-2I$, $W = B$; (ix) $m = 2$, $Z = B_0$, $W = J$; (x) $m = 2$, $W = J-2I$, $Z = 0$; (xi) $m = 2$, $Z = 0_0$, $W = J$; (xii) $m = 4$, $Z = 0_0$, $W = J-2I$; (xiii) $m = 4$, $Z = J-2I$, $W = 0_0$.

The result in (i) comes from J. Wallis [2].

This corollary gives no new orders less than 4000 but it appears highly likely that ^{new} higher order matrices may be obtained.

§4.4 NEW CLASSES OF SKEW-HADAMARD MATRICES

For completeness we include theorems 4.29 and 4.30 but theorem 4.31 and corollary 4.32 are original and are included in J.Wallis [3].

Theorem 4.29 : If h is the order of any skew-Hadamard matrix then there is a skew-Hadamard matrix of order $2h$.

Proof : Let $H = I + R$ be the skew-Hadamard matrix of order h , then $R^T = -R$ and

$$I \times \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} + R \times \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

is the required skew-Hadamard matrix of order $2h$. ***

Theorem 4.30 : If h is the order of any skew-Hadamard matrix and p^r is a prime power $\equiv 3 \pmod{4}$ then there is a skew-Hadamard matrix of order $h(p^r + 1)$.

Proof : Write $q = p^r$. Then with M and N defined in part (ii) of the proof of lemma 2.26 we have

$$\begin{aligned} MN^T &= NM^T, \\ MM^T &= NN^T = qI_q. \end{aligned}$$

Now if $H = I + U$ is a skew-Hadamard matrix of order h then $HH^T = hI_h = I_h + UU^T$. Write $M = I_h + V$ where $V^T = -V$ and consider

$$\begin{aligned} K &= I \times M + U \times N = I_h \times I_h + I_h \times V + U \times N \\ K^T &= I_h \times I_h + I_h \times -V + -U \times N \end{aligned}$$

so K is skew-type and

$$\begin{aligned} KK^T &= (I_h \times M + U \times N)(I_h \times M^T + U^T \times N^T) \\ &= I_h \times MM^T + U \times NM^T + U^T \times MN^T + UU^T \times NN^T \\ &= I_h \times qI_q + (h-1)I_h \times qI_q \\ &= hqI_{hq}, \end{aligned}$$

where $q = p^r + 1$. This completes the proof that K is skew-Hadamard of order $h(p^r + 1)$. ***

Theorem 4.31 : If all the conditions of theorem 4.23 are satisfied and in addition X is skew-type and Y, Z are symmetric then $\bar{H}$ is skew-Hadamard.

Proof : The Hadamard property has been proved in theorem 4.23.

To prove the skew-type property let $X = R + I$ where $R^T = -R$.

Then

$$\bar{H} = U \times N \times Z + I_h \times W \times Y + I_h \times I_m \times R + I_h \times I_m \times I_x = Q + I$$

and

$$\begin{aligned} \bar{H}^T &= U^T \times N^T \times Z^T + I_h \times W^T \times Y^T + I_h \times I_m \times R^T + I_h \times I_m \times I_x \\ &= -U \times N \times Z + I_h \times -W \times Y + I_h \times I_m \times -R + I_h \times I_m \times I_x \\ &= -Q + I. \end{aligned}$$

Which completes the proof. ***

We now investigate when the conditions of theorem 4.31 are satisfied.

Let M and N be m -type matrices of order $q+1$. Then writing M and N in the form

$$(28) \quad M = \begin{bmatrix} 1 & e \\ -e^T & P \end{bmatrix} \quad \text{and} \quad N = \begin{bmatrix} 1 & e \\ e^T & D \end{bmatrix},$$

where $e = (1, \dots, 1)$ is of order $1 \times q$, we have, since $MN^T = NM^T$,

$$\begin{aligned} MN^T &= \begin{bmatrix} 1 & e \\ -e^T & P \end{bmatrix} \begin{bmatrix} 1 & e \\ e^T & D \end{bmatrix} = \begin{bmatrix} q+1 & 0 \\ 0 & PD^T - J \end{bmatrix} \\ &= \begin{bmatrix} q+1 & 0 \\ 0 & DP^T - J \end{bmatrix} \\ &= \begin{bmatrix} 1 & e \\ e^T & D \end{bmatrix} \begin{bmatrix} 1 & -e \\ e^T & P^T \end{bmatrix} = NM^T \end{aligned}$$

and so $PD^T = DP^T$.

Corollary 4.32: Let m and m' be the orders of m -type matrices then if there is a skew-Hadamard matrix of order

$$(i) \quad \frac{(m-1)m'}{m} \qquad (ii) \quad \frac{(m-1)(m'-4)}{m}$$

then there is a skew-Hadamard matrix of order

$$(i) \quad m'(m'-1)(m-1) \qquad (ii) \quad (m'-1)(m'-4)(m-1)$$

respectively.

Proof: With P and D defined in (28) of order $m'-1$ the proof follows with

$$(i) \quad X=P, Y=J \text{ and } Z=D \qquad (ii) \quad X=P, Y=K \text{ and } Z=D,$$

in theorem 4.31.

With $m=2$, $m'=24$ and (i) of corollary 4.32, we find a skew-Hadamard matrix of order 552, which was not previously known.

CHAPTER V : CONSTRUCTIONS FOR HADAMARD MATRICES USING n-TYPE MATRICES

There is some overlap between the work in this chapter and that of Goethals and Seidel [1] but our results were obtained independently. Most of the material in this chapter is to be published in J.Wallis [4].

§5.1 CONSTRUCTIONS FOR SYMMETRIC HADAMARD MATRICES

Lemma 5.1: If there is an n-type matrix of order n then there is a symmetric Hadamard matrix of order 2n.

Proof: Let $N = I + P$ be the n-type matrix of order n. Then $P^2 = (n-1)I_n$ and $P^T = P$. Now choose

$$X = \begin{bmatrix} -P-I & P-I \\ P-I & P+I \end{bmatrix}$$

then $X^T = X$ and $XX^T = 2nI_{2n}$. So X is the required symmetric Hadamard matrix. ***

Since there are skew-Hadamard matrices of orders 16, 36

and 40, we see, using class NII, that there are n -type matrices of order 226, 1226 and 1522. Then using the above lemma there are symmetric Hadamard matrices of orders 452, 2452 and 3044.

Theorem 5.2: If $N = I + R$ is an n -type matrix of order n then there is an symmetric Hadamard matrix of order $2n(n-1)$.

Proof: Let D be the core of N above then $D^T = D$ and

$$D^2 = (n-1)I_{n-1} - J_{n-1}. \text{ Further } R^T = R, R^2 = (n-1)I_n \text{ and } JD = 0.$$

So if J is of order $n-1$ let

$$X = \begin{bmatrix} J & J \\ J & -J \end{bmatrix} \text{ and } Y = \begin{bmatrix} D+I & D-I \\ D-I & -D-I \end{bmatrix}$$

then $X^T = X$, $Y^T = Y$, $XX^T = 2(n-1)J_{n-1} \times I_2$, $YY^T = (2nI_{n-1} - 2J_{n-1}) \times I_2$, and $XY^T + YX^T = 0$.

Then if

$$H = I_n \times X + R \times Y,$$

H is symmetric and since

$$\begin{aligned} HH &= I_n \times XX^T + R \times (YX^T + XY^T) + RR^T \times YY^T \\ &= I_n \times 2(n-1)J_{n-1} \times I_2 + (n-1)I_n \times (2nI_{n-1} - 2J_{n-1}) \times I_2 \\ &= 2n(n-1)I_{2n(n-1)}, \end{aligned}$$

H is Hadamard.

Corollary 5.3: If $p^r \equiv 1 \pmod{4}$ is a prime power then there is a symmetric Hadamard matrix of order $2p^r(p^r+1)$.

Proof: This follows putting n equal to orders from class NI. ***

This corollary is important as it means class VII of Marshall Hall [1,p207] may be partially rewritten. The construction gives an Hadamard matrix of order 612.

§5.2 OTHER CLASSES OF HADAMARD MATRICES

Lemma 5.4: If there is an n -type matrix of order n and an Hadamard matrix of order h then there is an Hadamard matrix of order hn .

Proof: Let H be an Hadamard matrix and define $K = HS$ where

$$(29) \quad S = \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & 1 \\ & & & & & -1 \\ & & & & & & 1 \\ & & & & & & & -1 \\ & & & & & & & & \ddots \\ & & & & & & & & & 1 \\ & & & & & & & & & & -1 \end{bmatrix}$$

is of order h then $SS^T = I_h$ and $S^T = -S$ so

$$HK^T = HS^T H^T = -HS^T H^T = -KH^T \text{ and } hI_n = HH^T = HSS^T H^T = HS(HS)^T = KK^T.$$

Then if $N = I + R$ is an n -type matrix of order n ,

$R^2 = (n-1)I_n$ and $R^T = R$ so if

$$L = I_n \times H + R \times K,$$

then

$$\begin{aligned} LL^T &= I_n \times HH^T + R \times KH^T + R^T \times HK^T + RR^T \times KK^T \\ &= I_n \times hI_h + (n-1)I_n \times hI_h \\ &= nhI_{nh}. \end{aligned}$$

So L is the required Hadamard matrix of order nh . ***

Theorem 5.5: If $N = I + R$ is an n -type matrix of order m ,

then if there are symmetric matrices D and M ^{of order n} satisfying $*$

$$D^2 = nI_n - J_n, M^2 = \overset{\text{same}}{(n+1-m)}I_n + (m-1)J_n \text{ and } MD = DM \text{ where } D$$

has zero diagonal, there is an Hadamard matrix of order $4mn$.

Proof: Choose

$$X = \begin{bmatrix} M & M & M & M \\ M & -M & -M & M \\ M & -M & M & -M \\ M & M & -M & -M \end{bmatrix} \text{ and } Y = \begin{bmatrix} D+I & -D-I & D-I & -D+I \\ -D-I & -D-I & D-I & D-I \\ -D+I & -D+I & -D-I & -D-I \\ D-I & -D+I & -D-I & D+I \end{bmatrix}$$

then $XY^T + YX^T = 0$, $XX^T = [4(n+1-m)I_n + 4(m-1)J_n] \times I_4$ and

$YY^T = [4(n+1)I_n - 4J_n] \times I_4$, so if

$$H = I_m \times X + R \times Y$$

then

$$\begin{aligned}
HH^T &= I_m \times XX^T + R \times (XY^T + YX^T) + R^2 \times YY^T \\
&= I_m \times [4(n+1-m)I_n + 4(m-1)J_n] \times I_4 \\
&\quad + (m-1)I_m \times [4(n-1)I_n - 4J_n] \times I_4 \\
&= 4nmI_{4nm}.
\end{aligned}$$

So H is an Hadamard matrix of order $4nm$.

The matrix

$$Y = \begin{bmatrix} D+I & -D-I & -D+I & D-I \\ -D-I & -D-I & D-I & D-I \\ D-I & -D+I & D+I & -D-I \\ -D+I & -D+I & -D-I & -D-I \end{bmatrix}$$

would also suffice in theorem 5.5.

For the rest of this chapter if

D is required to be of prime power order then choose D to be the symmetric matrix A defined in §1.4;

D is required to be of prime order then choose D to be the circulant symmetric matrix B defined in §1.4.

Corollary 5.6: If m is the order of an n -type matrix then if there is a back-circulant matrix M of order $p \equiv 1 \pmod{4}$, a prime, satisfying $M^2 = (p+1-m)I + (m-1)J$ then there is an Hadamard matrix of order $4pm$.

Proof: This follows with the n of theorem 5.5 of class NI and D defined to be the circulant symmetric matrix B given in §1.4.

$$D^2 = p^2 I - J.$$

By lemma 2.15 a circulant D and a back-circulant M satisfy

$MD^T = DM^T$ and since M and D are both symmetric the conditions

of the theorems are satisfied. ***

Corollary 5.7: If there is an n -type matrix of order

- (i) $p^r - 3$; (ii) $p^r - 4q^{n-1} + 1$, where $p^r = q^n + q^{n-1} + \dots + 1$, n integer;
 - (iii) $q^2 - 3q + 2$, where $p^r = q^2 + q + 1$; (iv) $x^2 + 1$, where $p = 4x^2 + 1$;
 - (v) $x^2 + 1$, where $p = 4x^2 + 9$; (vi) $36b^2 + 6$, where $p = 8a^2 + 1 = 64b^2 + 9$, b odd
 - (vii) $36b^2 + 250$, where $p = 8a^2 + 49 = 64b^2 + 441$, b even;
- with $p^r \equiv 1 \pmod{4}$, p^r and q prime powers, p prime and x and a odd,

then there are Hadamard matrices of orders

- (i) $4p^r(p^r - 3)$; (ii) $4(q^n + q^{n-1} + \dots + 1)(q^n - 3q^{n-1} + q^{n-2} + \dots + q^2 + q + 2)$;
- (iii) $4(q-1)(q-2)(q^2 + q + 1)$; (iv) $4(x^2 + 1)(4x^2 + 1)$;
- (v) $4(x^2 + 1)(4x^2 + 9)$; (vi) $24(6b^2 + 1)(64b^2 + 9)$;
- (vii) $8(18b^2 + 125)(64b^2 + 441)$;

respectively.

Proof: In each case M of the corollary is a back-circulant

matrix generated by a difference set, the notation we use for

these difference sets is that of Marshall Hall [1, p141]. The

proof follows with M given by (i) $J - 2I$; (ii) S ; (iii) S with $n=3$;

(iv) B; (v) B_0 ; (vi) 0; (vii) 0_0 ; respectively in theorem 5.5. ***

Theorem 5.8: If $h > 1$ is the order of an Hadamard matrix, n is the order of an n -type matrix and $v \equiv 1 \pmod{4}$ the order of three matrices A , B and D which satisfy $DD^T = vI - J$, $AA^T = aI + (v-a)J$, $BB^T = [2(v-n+1) - a]I + [-v + 2(n-1) + a]J$, and AB^T , BD^T , and AD^T all symmetric where D has zero diagonal then there is an Hadamard matrix of order $2nh$.

Proof: Let $I_n + R$ be the n -type matrix, H the Hadamard matrix and $K = HS$ be as defined in the proof of lemma 5.4. Now choose

$$X = \begin{bmatrix} A & B \\ B & -A \end{bmatrix} \quad \text{and} \quad Y = \begin{bmatrix} D+I & D-I \\ -D+I & D+I \end{bmatrix}$$

then $XY^T = YX^T$. So

$$W = I_n \times H \times X + R \times K \times Y$$

is the required matrix. ***

In the construction of Williamson shown in Marshall Hall [1,p214-216] m and n are defined as being of the form p^r+1 where $p^r \equiv 1 \pmod{4}$ is a prime power, if we read instead that m and n are the orders of n -type matrices then the same proofs give us the theorem

Theorem 5.9: If Hadamard matrices of orders h_1 and h_2 exist $h_1 > 1$, $h_2 > 1$ and (i) n ; (ii) n and $n+4$, are the orders of n -type matrices, then there exist Hadamard matrices of orders

$$(i) \quad h_1 h_2 n(n-1); \quad (ii) \quad h_1 h_2 n(n+3)$$

respectively.

We note that the similar theorems of Goethals and Seidel [1] are stronger than ^{our} ~~my~~ theorem 5.9.

Theorem 5.10: If there is an n -type matrix of order n and $q \equiv 1 \pmod{4}$, a prime power, the order of three matrices A , C and D satisfying $AA^T = aI + (q-a)J$, $CC^T = (2q-2n+2-a)I + (-q+2n-2+a)J$, $DD^T = qI - J$, and AC^T , CD^T and AD^T all symmetric where D has zero diagonal, then there is an Hadamard matrix of order $4qn$.

Proof: Define

$$M = \begin{bmatrix} A & A & C & C \\ A & -A & C & -C \\ C & C & -A & -A \\ C & -C & -A & A \end{bmatrix} \quad \text{and} \quad P = \begin{bmatrix} -D-I & D+I & D-I & -D+I \\ D+I & D+I & -D+I & -D+I \\ -D+I & D-I & -D-I & D+I \\ D-I & D-I & D+I & D+I \end{bmatrix}$$

then since AC^T , CD^T and AD^T are all symmetric $MP^T + PM^T = 0$.

$$\begin{aligned} \text{Also} \quad MM^T &= \{4(q-n+1)I_q + 4(n-1)J_q\} \times I_4 \\ PP^T &= \{4(q+1)I_q - 4J_q\} \times I_4. \end{aligned}$$

So if $N = I + R$ is the n -type matrix, $R^T = R$ and $R^2 = (n-1)I_n$.

Now consider

$$H = I_n \times M + R \times P,$$

then

$$\begin{aligned} HH^T &= I_n \times MM^T + R \times \{MP^T + PM^T\} + R^2 \times PP^T \\ &= I_n \times \{[4(q-n-1)+4(q+1)(n-1)]I_q \\ &\quad + [4(n-1)-4(n-1)]J_q\} \times I_4 \\ &= 4qnI_{4qn}. \end{aligned}$$

So H is the required Hadamard matrix.

Corollary 5.11: If there is an n -type matrix of order

(i) $q^n - q^{n-1} + q^{n-2} + \dots + q^2 + q + 2$, where $p^r = q^n + q^{n-1} + \dots + q + 1$, n , integer;

(ii) $q^n - q^{n-1} + q^{n-2} + \dots + q^2 + q$, p^r as in (i); (iii) $\frac{5x^2-1}{2}$, where

$p = 4x^2+1$; (iv) $\frac{5x^2+7}{2}$, where $p = 4x^2+9$; (v) $50b^2+8$, where

$p = 8a^2+1 = 64b^2+9$, b odd; (vi) $50b^2+346$, where $p = 8a^2+49 = 64b^2+441$,

b even; with $p^r \equiv 1 \pmod{4}$, p^r and q prime powers ^{p prime} and x and

a odd, then there are Hadamard matrices of orders

(i) $4(q^n + q^{n-1} + \dots + 1)(q^n - q^{n-1} + q^{n-2} + \dots + q^2 + q + 2)$;

(ii) $4(q^n + q^{n-1} + \dots + 1)(q^n - q^{n-1} + q^{n-2} + \dots + q^2 + q)$;

(iii) $2(5x^2-1)(4x^2+1)$; (iv) $2(5x^2+7)(4x^2+9)$; (v) $8(25b^2+4)(64b^2+9)$;

(vi) $8(25b^2+173)(64b^2+441)$.

Proof: In each case C of the theorem is a back-circulant matrix generated by a difference set, we again use the notation of Marshall Hall [1,p141]. The proof follows with

- (i) $A = J$, $C = S$, q powers of 2; (ii) $A = J - 2I$, $C = S$,
 $q \equiv 3 \pmod{4}$; (iii) $A = J - 2I$, $C = B$; (iv) $A = J - 2I$, $C = B_0$;
 (v) $A = J$, $C = 0$; (vi) $A = J$, $C = 0_0$. ***

CHAPTER VI : HADAMARD DESIGNS

All the material in §6.2 and §6.3 is original. §6.3 will appear in J.Wallis [9]. The result of theorem 6.11 has also been found by Jan Folkman in his paper "A nonexistence theorem for Hadamard matrices in many variables".

There are four main types of Hadamard designs, those of Williamson [1], Baumert-Hall [1], those of our previous chapters which have the blocks repeated an unequal number of times, and those of this chapter which have blocks repeated an equal number of times.

Definition 6.1 : An Hadamard design is a ^{square} array of letters such that if the letters commute in pairs then the scalar product of any two rows considered as vectors is zero.

Definition 6.2 : An Hadamard design on n letters or an n-letter design has n distinct letters.

§6.1 THE HADAMARD DESIGNS OF WILLIAMSON AND BAUMERT-HALL

Williamson's design from Williamson [1] is a four-letter design with each letter repeated once. It is

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

This design was used to generate the Hadamard matrices of orders 92, 116, and 172.

The Baumert-Hall design is a four-letter design with each letter repeated three times. It is

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	

This design has been used to generate the Hadamard matrix of order 156.

This is the total that has been published on n-letter Hadamard designs.

§6.2 DIFFERENCE SETS WHICH COULD BE USED IN n-LETTER HADAMARD DESIGNS

We have already used the twin difference sets of Szekeres [1] in chapter 4 and have noted in §4.1 that the subgroup of index 3 in the group of powers of a primitive root

of 19 is useful in finding a 4-letter skew-Hadamard design.

We now turn our attention to supplementary difference sets which yield results that could be useful in n-letter Hadamard designs.

A (v, k, λ) difference set $D = \{d_1, d_2, \dots, d_k\}$ is said to generate a circulant $(1, -1)$ -matrix $A = (a_{ij})$ if

$$a_{1j} = \begin{cases} +1 & j \in D \\ -1 & \text{otherwise} \end{cases}$$

$$a_{ij} = a_{1, j-i+1} \quad \text{where } j-i+1 \text{ is reduced modulo } v.$$

Then from theorem 2.8

$$AA^T = 4(k - \lambda)I + \{v - 4(k - \lambda)\}J$$

and hence we have

Theorem 6.3 : Let $D = \{d_1, d_2, \dots, d_k\}$ be a (v, k, λ) difference set. Further let $D_i = D - \{d_i\}$ generate the circulant $(1, -1)$ -matrix A_i (using a similar process to that outlined above). Then

$$\sum_{i=1}^k A_i A_i^T = vkI - 4\lambda(v - k + 1)J.$$

Proof : Define

$$\theta(z) = \begin{cases} +1 & z \in D \\ -1 & \text{otherwise} \end{cases}$$

then

$$\sum_{z=1}^v \theta(z)\theta(z+c) = v - 4(k - \lambda) \quad (c, v) \neq 0.$$

is the scalar product of any two distinct row vectors of A .

Now define

$$\psi_i(z) = \begin{cases} -1 & z = d_i \\ \theta(z) & \text{otherwise} \end{cases}$$

then

$$\sum_{z=1}^v \psi_i(z) \psi_i(z+c) \quad c \neq 0,$$

is the scalar product of any two distinct row vectors of A_i .

Now

$$\sum_{i=1}^k \sum_{z=1}^v \psi_i(z) \psi_i(z+c) \quad c \neq 0$$

$$= \sum_{i=1}^k \left\{ \sum_{z=1}^v \theta(z) \theta(z+c) + \psi_i(d_i) \psi_i(d_i+c) \right. \\ \left. + \psi_i(d_i-c) \psi_i(d_i) - \theta(d_i) \theta(d_i+c) \right. \\ \left. - \theta(d_i-c) \theta(d_i) \right\}$$

$$\text{if } z = d_i \text{ then } \psi_i(d_i+c) = \theta(d_i+c)$$

$$= \sum_{i=1}^k \left\{ v - 4(k - \lambda) - 2\theta(d_i+c) - 2\theta(d_i-c) \right\}$$

Now $c = d_a - d_b$ for exactly λ different pairs of d_a and d_b .

So $\theta(d_i+c) = \theta(d_i + d_a - d_b)$ for exactly λ different d_b . In

$\sum_{i=1}^k \theta(d_i+c)$ d_i runs through all the elements of D and so

$\theta(d_i+c) = +1$ exactly λ times, that is

$$\sum_{i=1}^k \theta(d_i+c) = +1(\lambda \text{ times}) + -1(k - \lambda \text{ times})$$

$$= 2\lambda - k.$$

So

$$\begin{aligned}
 \sum_{i=1}^k \sum_{z=1}^v \psi_i(z) \psi_i(z+c) & \quad c \neq 0 \\
 &= \sum_{i=1}^k \left\{ v - 4(k - \lambda) \right\} - 4(2\lambda - k) \\
 &= vk - 4k(k - \lambda) - 4(2\lambda - k) \\
 &= vk - 4\lambda(v - k + 1) \quad \text{using } \lambda(v-1) = k(k-1).
 \end{aligned}$$

Also

$$\sum_{i=1}^k \sum_{z=1}^v \psi_i(z) \psi_i(z) = vk$$

so

$$\sum_{i=1}^k A_i A_i^T = vkI - 4\lambda(v - k + 1)J. \quad ***$$

So we may call these subsets of difference sets *supplementary difference sets* *when we take all the differences in* ~~as, in their union each difference~~ *each subset and collect them, each difference occurs a fixed* ~~occurs a fixed number of times.~~ *number of times in the totality.*

Using theorem 6.3 we see we have a collection of k matrices which could be used as the block matrices replacing the letters in an n -letter design if $n \geq k$. So now we investigate n -letter designs.

§6.3 DESIGNS USING n DIFFERENT BLOCKS, $n > 4$.

We have already seen that there is an Hadamard design with four different letters each repeated once. We would like to know if there is an Hadamard design with each letter repeated once in each row and in each column with the number of distinct

letters, n , greater than four. So we shall try to construct such a design.

Suppose there is an Hadamard design on the letters $A, B, C, D, \dots$, whose first two rows are

$$\begin{array}{ccccccc} \pm A & \pm B & \pm C & \pm D & \dots \\ \pm B & \pm A & \pm D & \pm C & \dots \end{array}$$

(clearly any design can be put in this form by suitable relabelling : the signs of the elements are not important at the moment). There will be a row whose first element is $\pm C$; reorder the rows so as to make this the third row. $\pm C$ is in the $(3,1)$ position, so $\pm A$ must occur in the $(3,3)$ position. On the other hand the C element of row 3 occurs under the $\pm B$ element of row 2, so there must be a $\pm B$ in the $(3,4)$ position, and similarly the $(3,2)$ element must be $\pm D$. So the first three rows are

$$\begin{array}{ccccccc} \pm A & \pm B & \pm C & \pm D & \dots \\ \pm B & \pm A & \pm D & \pm C & \dots \\ \pm C & \pm D & \pm A & \pm B & \dots \end{array}$$

In the same way, if we move the row whose first element is $\pm D$ into the position of row 4, we find the design can be put in the form

$$\begin{array}{ccccccc}
 \pm A & \pm B & \pm C & \pm D & . & . & . \\
 \pm B & \pm A & \pm D & \pm C & . & . & . \\
 \pm C & \pm D & \pm A & \pm B & . & . & . \\
 \pm D & \pm C & \pm B & \pm A & . & . & . \\
 . & . & . & . & . & . & . \\
 . & . & . & . & . & . & . \\
 . & . & . & . & . & . & .
 \end{array}$$

by interchanging rows and columns.

Write down the four-letter design and repeat one letter of this design in the $(5,5)$ position, then the letters in the $(t,5)$ positions $1 \leq t \leq 4$ must be all different from each other and from the first mentioned four letters.

So $n = 8$ is the next smallest possible order for an Hadamard design on n letters with each repeated once.

By repeating the above method, assuming the existence of an 8-letter design we see that this implies $n = 16$ is the next possible order for an Hadamard design on n -letters each repeated once. Continuing we see

Lemma 6.4 : An Hadamard design on n letters each repeated once can exist only if $n = 2^s$, s a positive integer. ***

Now we

note, there are eight possible ways of combining two letters into an Hadamard design :

X	Y	X	Y	X	-Y	X	-Y
-Y	X	Y	-X	Y	X	-Y	-X
-X	Y	-X	Y	-X	-Y	-X	-Y
-Y	-X	Y	X	Y	-X	-Y	X

but of these only two

X	Y	X	Y
-Y	X	Y	-X

are distinct as the other six may be obtained from these two by substituting $\bar{+} X$ for $\pm X$ and $\bar{+} Y$ for $\pm Y$. We note

Proposition 6.5 : The Hadamard property of a 2-letter design is not altered by replacing any letter by its negative throughout. ***

Since any Hadamard design on n letters is an array of 2-letter Hadamard designs interwoven we have

Proposition 6.6 : The Hadamard property of a design on n letters with each letter repeated once per row and column is not altered by replacing any letter by its negative throughout. ***

Another obvious property is

Proposition 6.7 : The Hadamard property of an n -letter design is not altered by multiplying through any row or any column by -1 . ***

So a single letter may be chosen (altering rows and columns by transposition if necessary) in the diagonal positions and always with positive sign.

Every element in the first row may be chosen with a positive sign, for if $-X$ occurs it may be removed by using proposition 6.6.

Also we may choose the $(4t+1, 4t+1)$, $(4t+1, 4t+2)$, $(4t+1, 4t+3)$, $(4t+1, 4t+4)$ elements with positive sign, $t = 1, 2, \dots$. Suppose one of these, the $(4t+1, s)$ element has negative sign. Then using proposition 6.7 we may multiply the s th column by -1 and so the (s, s) element and the $(1, s)$ element, both formerly with positive sign acquire a negative sign, but our element $(4t+1, s)$ has the required sign. Proposition 6.7 is now used to multiply the s th row by -1 so the diagonal element again has a positive sign, and finally proposition 6.6 is used to replace the $(1, s)$ th element by its negative throughout.

Finally, it is clear that the rows and columns may be interchanged so that the $(4t+1, 4t+k)$ element = $(1, k)$ element for $k = 1, 2, 3, 4$.

, So we have shown

Proposition 6.8 : Any Hadamard design on n letters where each letter must occur only once in any row or column is equivalent under the operations

- (a) interchange of rows or columns,
- (b) multiplying rows and columns by -1
- (c) replacing any letter by its negative throughout the design

to an Hadamard design with the properties

- (i) every element of the first row has positive sign,
- (ii) the diagonal element is constant and has positive sign,
- (iii) the elements $(4t+1, 4t+k) = (1, k)$ for $k = 1, 2, 3, 4$;
 $0 \leq t \leq \frac{n-4}{4}$,
- (iv) the elements $(4t+1, 4t+k)$ $k=1, 2, 3, 4$, $0 \leq t \leq \frac{n-4}{4}$
 occur with positive sign.

Notation 6.9 : Call an Hadamard design satisfying conditions (i), (ii), (iii), (iv) of proposition 6.8 a normalized design.

Constructing the normalized 4-letter design on the letters A,B,C,D we have the following first row and diagonal

A B C D .

A

A

A

Then depending on whether we make the (2,3) element +D or -D we see

Proposition 6.10 : There are two normalized 4-letter Hadamard designs on the letters A,B,C,D which are

A	B	C	D	and	A	B	C	D
-B	A	D	-C		-B	A	-D	C
-C	-D	A	B		-C	D	A	-B
-D	C	-B	A		-D	-C	B	A

but these are equivalent under properties (b) and (c) of proposition 6.8.

We now use this first mentioned four-letter design to construct an 8-letter design on the letters A,B,C,D,E,F,G,H. Then using proposition 6.8 we must have

A	B	C	D	E	F	G	H	.
-B	A	D	-C					
-C	-D	A	B					
-D	C	-B	A					
				A	B	C	D	
					A			
						A		
							A	

in a normalized 8-letter design. Then immediately by considering the $(1,k)$, $(1,k+4)$ and $(5,k+4)$ elements for $k = 1,2,3,4$ we see the $(5,k)$ elements must be -E, -F, -G, -H respectively.

Now considering the $(2,k)$, $(5,k)$ and $(5,k+4)$ elements we see the $(2,k+4)$ elements must be F, -E, -H, G respectively. Similarly the $(3,k+4)$ elements must be G, H, -E, -F respectively and the $(4,k+4)$ elements must be H, -G, F, -E respectively. So we have

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	
-E	-F	-G	-H	A	B	C	D	
					A			
						A		
							A	

Consideration of the $(k,6)$, $(6,6)$ and (k,k) elements shows the $(6,k)$ elements must be $-F, E, -H, G$ respectively. Similarly the $(7,k)$ elements must be $-G, H, E, -F$ respectively and the $(8,k)$ elements $-H, -G, F, E$ respectively. The $(5,5)$, $(5,m)$ and (m,m) elements for $m = 6,7,8$ show us the $(m,5)$ elements must be $-B, -C, -D$ respectively. So now we have

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	
-E	-F	-G	-H	A	B	C	D	
-F	E	-H	G	-B	A			
-G	H	E	-F	-C		A		
-H	-G	F	E	-D			A	

Finally the $(2,s)$, $(6,s)$ and $(2,4+s)$ elements for $s = 3,4$ show the $(6,4+s)$ elements must be $-D, C$ respectively. The $(4,1)$, $(7,1)$ and $(4,6)$ elements show the $(7,6)$ element must be D ; the $(4,3)$, $(7,3)$ and $(4,8)$ elements show the $(7,8)$ element must be $-B$; and the $(4,t)$, $(8,t)$ and $(4,4+t)$ elements for $t = 2,3$ show the $(8,4+t)$ elements must be $-C, B$ respectively. So we have the 8-letter design

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	
-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	

We note that using one of the 4-letter designs to form an 8-letters design forced the other 4-lettersdesign into the 8-letter design. So, in an 8-letter design both 4-letter designs must appear.

Proposition 6.11 : There are two normalized 8-letter Hadamard designs but they are equivalent under proposition 6.8. If the 8-letter design is written in the form

$$\begin{array}{cc} X_1 & Y_1 \\ Y_2 & X_2 \end{array}$$

where X_1 is one four-letter design then X_2 must be the other 4-letter design. ***

Obviously if we start with four letters within an n-letter design in normalized form and put them into the upper left hand block using our equivalence relations, then they must form a 4-letter design within themselves.

In proving proposition 6.11, we have also shown that if A,B,C,D form a normalized 4-letter design and A,B,C,D,E,F,G,H,I,J, ... are the letters of an n-letter normalized design then we may write them in the form :

...

(30)

A	B	C	D	E	F	G	H	I	J	...	,
	A										
		A									
			A								
-E				A	B	C	D				
-F					A						
-G						A					
-H							A				
-I								A	B	...	
⋮											

but then the letters A,B,C,D,E,F,G,H in the top left hand corner of (30) form within themselves an 8-letter normalized design. Now there are only two normalized 4-letter designs, call them X_1 and X_2 respectively. If we denote the 4-letter designs in (30) on E,F,G,H by Y_1 and Y_2 we have (30) is

(31)

X_1	Y_1	Z_1	...
Y_2	X_2	U_1	...
Z_2	U_2	X_1	
⋮			

Now because (31) is an n -letter Hadamard design all the letters comprising Z_r are distinct from the letters in X_j and Y_m . Similarly the letters in U_s are distinct from the letters in Z_r , X_j , Y_m .

If (31) were rewritten as

$$(32) \quad \begin{array}{c|c|c|c} X_1 & Z_1 & Y_1 & \dots \\ \hline Z_2 & X_i & U_2 & \dots \\ \hline Y_2 & U_1 & X_2 & \\ \hline \vdots & & & \end{array}$$

by the admissible equivalence relation of interchanging rows and columns. We see (32) is still normalized and so by the above reasoning the block

$$\begin{array}{c|c} X_1 & Z_1 \\ \hline Z_2 & X_i \end{array}$$

must form an 8-letter normalized design and so $X_i = X_2$.

Now rewrite (31) as

$$(33) \quad \begin{array}{c|c|c|c} X_2 & U_1 & Y_2 & \dots \\ \hline U_2 & X_i & Z_2 & \dots \\ \hline Y_1 & Z_1 & X_1 & \\ \hline \vdots & & & \end{array}$$

by interchanging rows and columns. (33) may not be normalized as some of the letters of the first row of $U_1, Y_2, \dots$ may have negative signs, but using the equivalence relation which permits the replacing of any letter by its negative throughout the design we may normalize (33) to

$$(34) \quad \begin{array}{c|c|c|c} X_2 & U_1^* & Y_2^* & \dots \\ \hline U_2^* & X_i & Z_2 & \dots \\ \hline Y_1^* & Z_1 & X_1 & \\ \hline \vdots & & & \end{array} \quad .$$

We note that (34) is now normalized and that X_2, X_i were unaffected by the change.

Then, by the reasoning above, the block

X_2	U_1^*
U_2^*	X_i

must form an 8-letter normalized design so $X_i = X_1$. But this is a contradiction, so we have

Theorem 6.11 : There is no n -letter Hadamard design with each letter repeated only once for $n > 8$. ***

Corollary 6.12 : There are n -letter Hadamard designs with each letter repeated only once for $n = 2, 4$, and 8 , and for no other n . ***

CHAPTER VII : CONSTRUCTIONS FOR BLOCK DESIGNS

In this chapter we present the results we have found on block designs. Many of these results appear in J.Wallis [6] and §7.1 appears in J.Wallis [8].

§7.1 SOME BLOCK DESIGNS

In this section we use the following notation :

$$I = \begin{bmatrix} \overline{1} & 0 & \overline{0} \\ 0 & 1 & 0 \\ 0 & 0 & \underline{1} \end{bmatrix}, \quad L = \begin{bmatrix} \overline{0} & 1 & \overline{0} \\ 0 & 0 & 1 \\ \underline{1} & 0 & \underline{0} \end{bmatrix}, \quad M = \begin{bmatrix} \overline{0} & 0 & \overline{1} \\ 1 & 0 & 0 \\ 0 & 1 & \underline{0} \end{bmatrix}, \quad J = \begin{bmatrix} \overline{1} & 1 & \overline{1} \\ 1 & 1 & 1 \\ \underline{1} & 1 & \underline{1} \end{bmatrix},$$

$$e = [1, 1, 1] \quad \text{and} \quad \varepsilon = \begin{bmatrix} \overline{1} \\ 1 \\ \underline{1} \end{bmatrix},$$

all blank blocks contain all zeros.

The incidence matrix of a $(15, 7, 3)$ configuration may be written as

$$W = \begin{bmatrix} \overline{J} & I & I & I & \overline{I} \\ I & J & I & L & M \\ I & I & J & M & L \\ I & L & M & J & I \\ \underline{I} & M & L & I & \underline{J} \end{bmatrix}.$$

This configuration is of course well known.

Another formulation of the well known (25,9,3) configuration is

			e	e	e				
	e		e					e	
	e			e		e			
	e				e		e		
			I	I	I	J-I	J-I	J-I	
ε	ε	ε	I	I	I	I	I	I	
ε	ε	ε	I	M	L	I	M	L	
ε	ε	ε	I	L	M	I	L	M	
	I	J-I	I		J-I	J-I		I	
	I	J-I	J-I	I		I	J-I		
	I	J-I		J-I	I		I	J-I	

Although M.Hall [1] lists as unknown the (45,12,3) configuration it had in fact been found by K.Takeuchi [2], Shrikhande and Singh [1,p 28], ~~and Ahrens and Szekeres [1].~~ An incidence matrix for the (45,12,3) configuration is

J				I I I	I I I	I I I
J				L L L	M M M	I I I
J				M M M	L L L	I I I
	J			I L M	I M L	I L M
	J			L M I	M L I	I L M
	J			M I L	L I M	I L M
I L M	I M L	J				I M L
L M I	M L I	J				I M L
M I L	L I M	J				I M L
I M L	I L M	I M L	J			
M L I	L M I	I M L	J			
L I M	M I L	I M L	J			
I I I	I I I			I M L	J	
M M M	L L L			I M L	J	
L L L	M M M			I M L	J	

Also we found the following incidence matrix for the
(36,15,6) configuration

J	J	I	I	I	I	I	I	I
J	J	L	L	L	M	M	M	I
J	J	M	M	M	L	L	L	I
I	M	L	J	J	I	L	M	I
I	M	L	J	J	L	M	I	M
I	M	L	J	J	M	I	L	M
I	L	M	I	M	L	J	J	I
I	L	M	M	L	I	J	J	L
I	L	M	L	I	M	J	J	M
I	I	I	I	L	M	I	M	L
I	I	I	L	M	I	M	L	I
I	I	I	M	I	L	L	I	M

This configuration is listed as unknown in M.Hall [1], but has
been found by K.Takeuchi [2], P.Kesava Menon [1], R.Turyn [1] and
M. Hall [2].

Using

$$J = \begin{bmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{1} \end{bmatrix}, \quad I = \begin{bmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{bmatrix} \quad \text{and} \quad K = \begin{bmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{bmatrix}$$

we also found

O	O	O	J	I	I	I	I
O	O	J	O	I	K	I	K
O	J	O	O	I	I	K	K
J	O	O	O	I	K	K	I
I	I	I	I	O	O	O	J
I	K	I	K	O	O	J	O
I	I	K	K	O	J	O	O
I	K	K	I	J	O	O	O

which is the incidence matrix of a (16,6,2) configuration.

§7.2 THE SYMMETRIC BLOCK DESIGN $(q^2(q+2), q(q+1), q)$.

The theorem of this section has been proved in a stronger form by K. Takeuchi [2] and Ahrens and Szekeres [1]. *My results are found quite differently.*

Theorem 7.3 is another formulation of the class of configurations of theorem 7.1.

Firstly I show there exist $(0,1)$ matrices $R_i, 0 \leq i \leq q-1, Q$ and P of order q^2 and Q^* which is $kq \times q$, where k is an integer less than q , which satisfy the following conditions

$$(37) \left\{ \begin{array}{ll} \text{(i)} & PR_j^T = J \times J \\ \text{(ii)} & R_i R_j^T = J \times J \quad i \neq j \\ \text{(iii)} & \sum_{i=0}^{q-1} R_i R_i^T = q^2 I \times I + q(J - I) \times J \\ \text{(iv)} & P = I \times J, PP^T = qI \times J \\ \text{(v)} & QQ^T = qI \times I + (J - I) \times J \\ \text{(vi)} & Q^* Q^{*T} = qI_{kq} + (J - I) \times J_k \\ \text{(vii)} & J_{kq} Q^* = kJ^* \\ \text{(viii)} & Q^* J_{q^2} = qJ^*. \end{array} \right.$$

In formula (37) unless subscripted otherwise, I is the identity matrix of order q , J , unless subscripted otherwise, is the matrix of order q with every element +1 and J^* is the $kq \times q^2$ matrix with every element +1.

Define T to be the circulant matrix of order q given by

$$(38) \quad T = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 & 0 \\ \vdots & & & & & & \\ 0 & 0 & 0 & \dots & 0 & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 & 0 \end{bmatrix}$$

and I, J to be of order q .

THE CASE FOR q PRIME. Choose q block matrices R_i ,

$0 \leq i \leq q-1$ of order q^2 with T as in (38) above, thus

$$R_i = \begin{bmatrix} I & T^i & T^{2i} & \dots & T^{(q-1)i} \\ T^{(q-1)i} & I & T^i & \dots & T^{(q-2)i} \\ \vdots & & & & \vdots \\ T^i & T^{2i} & T^{3i} & \dots & I \end{bmatrix} = (T^{(m-r)i})_{rm}$$

and let

$$Q = \begin{bmatrix} I & I & I & \dots & I \\ I & T & T^2 & \dots & T^{q-1} \\ I & T^2 & T^{2 \cdot 2} & \dots & T^{(q-1)2} \\ \vdots & & & & \vdots \\ I & T^{q-1} & T^{2(q-1)} & \dots & T^{(q-1)(q-1)} \end{bmatrix} = (T^{(i-1)(j-1)})_{ij}$$

and

$$Q^* = \begin{bmatrix} \overline{I} & I & I & \dots & I \\ I & T & T^2 & \dots & T^{q-1} \\ I & T^2 & T^{2 \cdot 2} & \dots & T^{(q-1)2} \\ \vdots & & & & \vdots \\ I & T^k & T^{2k} & \dots & T^{(q-1)k} \end{bmatrix}$$

We now verify that these matrices satisfy the conditions (37).

Note that $JT^k = J$ for all k so (i), (vii) and (viii) are immediate.

$$\begin{aligned} \text{(ii)} \quad R_i R_j^T &= \left(\sum_{m=0}^{q-1} T^{(m-s)i} T^{(n-m)j} \right)_{s,n} \\ &= \left(\sum_{m=0}^{q-1} T^{m(i-j)+nj-si} \right)_{s,n} \end{aligned}$$

now i, j, s and n are fixed so, if J is of order q and J^* is the $(+1)$ matrix of order q^2 ,

$$= \left(\sum_{r=0}^{q-1} T^r \right)_{s,n} = (J)_{s,n} = J^* \text{ for } i \neq j.$$

$$\begin{aligned} \text{(iii)} \quad R_i R_i^T &= \left(\sum_{m=0}^{q-1} T^{(m-s)i} T^{(n-m)i} \right)_{s,n} \\ &= (kT^{(n-s)i})_{s,n} \\ &= qR_i. \end{aligned}$$

Now

$$\sum_{i=0}^{q-1} R_i = \begin{bmatrix} qI & J & \dots & J \\ J & qI & \dots & J \\ \vdots & & & \vdots \\ J & J & \dots & qI \end{bmatrix} = qI \times I + (J-I) \times J,$$

where I and J are of order q , and so the result follows.

$$\begin{aligned} (v) \quad QQ^T &= \left(\sum_{m=1}^q T^{(i-1)(m-1)} T^{q-(m-1)(j-1)} \right)_{ij} \\ &= \sum_{m=1}^q T^{(m-1)(i-j)}_{ij} \end{aligned}$$

then if $i = j$ we have $\sum_{m=1}^q I = qI_q$, and if $i \neq j$ $\sum_{m=1}^q T^{(m-1)(i-j)} = J_q$

which gives the result.

(vi) This follows since we have chosen Q^* as the first kq rows of Q .

Hence I have shown that for q a prime the $(0,1)$ matrices P, Q, Q^*, R_1 satisfying (37) exist.

THE CASE FOR q A PRIME POWER : It is known that a cyclic $(p^2+p+1, p+1, 1)$ configuration exists whenever p is a prime power. If we form the circulant incidence matrix of this configuration then we may rearrange its rows and columns until the following matrix is obtained

$$A = \begin{bmatrix} \overline{1} & e & 0 \\ e^T & 0 & I_p \times e \\ 0 & I_p \times e^T & N \end{bmatrix}$$

where $e = [1, 1, \dots, 1]$ is of size $1 \times p$, I_p is the identity matrix of size p and N is of size p^2 .

Now $AA^T = pI_r + J_r$, where $r = p^2 + p + 1$,

$$= \begin{bmatrix} p+1 & e & exe \\ e^T & pI_p + J_p & (I_p \times e)N^T \\ e^T \times e^T & N(I_p \times e^T) & I_p \times J_p + NN^T \end{bmatrix}$$

so (a) N is of order p^2 ;

$$(b) \quad NN^T = pI_p \times I_p + J_p \times J_p - I_p \times J_p = pI_p \times I_p + (J_p - I_p) \times J_p;$$

$$(c) \quad N(I_p \times e^T) = J' \quad \text{where } J' \text{ is of size } p^2 \times p.$$

This last condition implies that if N is partitioned into p^2 block matrices N_i then each block matrix N_i has exactly one non-zero element in each row and column. Now rearrange the columns of N keeping the first $p+1$ rows of A unaltered until the first row of block matrices in the partitioned N are all I_p and similarly alter the rows of N keeping the first $p+1$ columns of A unaltered until the first column of block matrices in the partitioned N are all I_p . Then this new matrix obtained from N satisfies all the conditions for the matrix Q .

We have not been able to derive enough information about the structure of this partitioned matrix N to be able to ensure the existence of the matrices R_i .

This case ensures that P, Q and Q^* exist for all prime powers but not that the R_i exist.

THE CASE FOR q CERTAIN PRIME POWERS : Our construction for q prime depended on the powers of the matrix T of size q given by (38). For q^p , a power of q , we will consider the matrices

$$S = T^a \times T^b \times \dots \times T^c.$$

where the T^i are of period (multiplicative order) q and we take the Kronecker product of p such matrices. Two matrices $T^a \times T^b \times \dots \times T^c$ and $T^d \times T^e \times \dots \times T^f$ of the same size commute since the powers of T commute and since T is of period q , S is of period q . Hence all the matrices of the form S form an abelian group

$$X = Z_q \times Z_q \times \dots \times Z_q$$

where there are p copies of Z_q . Now X has p generators and for convenience we will assume they are

$$a_1 = T \times I \times I \times \dots \times I$$

$$a_2 = I \times T \times I \times \dots \times I$$

$$\vdots$$

$$a_p = I \times I \times I \times \dots \times T$$

all of size q^p , since I and T are of size q .

We have seen how Q^* may be obtained from Q , where Q was constructed of elements of the form T^i and the process for constructing Q^* from a Q comprising elements of the form S is identical.

Now we will show that it is only necessary for us to know how to construct Q from these elements because if Q is of a suitable form the matrices R_i may be obtained from Q .

Write $Q = (q_{ij})$ where each q_{ij} is of the form S and size q^p . We need Q to have the following properties

- (39) $\left\{ \begin{array}{l} \text{(i)} \quad Q \text{ is of size } q^{2p} \\ \text{(ii)} \quad q_{i1} = q_{1j} = I \times I \times \dots \times I \text{ where each } I \text{ is of} \\ \quad \text{size } q \text{ and is repeated } p \text{ times;} \\ \text{(iii)} \quad \text{for each row (column) but the first every element} \\ \quad \text{of } X = Z_q \times Z_q \times \dots \times Z_q \text{ mentioned above is} \\ \quad \text{included once and only once;} \\ \text{(iv)} \quad QQ^T = q^p I \times I + (J-I) \times J, \text{ where } I \text{ and } J \text{ here} \\ \quad \text{mentioned have size } q^p; \\ \text{(v)} \quad q_{in}^{-1} q_{im} \neq q_{jn}^{-1} q_{jm} \text{ for all } i \neq j \neq 1, n \neq m; \end{array} \right.$

Choose R_i from Q in the following manner, where $r = q^p$,

$$(40) \quad \left\{ \begin{array}{l} R_0 = J \times I \\ R_{i-1} = \begin{bmatrix} e & q_{i2} & q_{i3} & \dots & q_{ir} \\ q_{i2}^{-1} & e & q_{i2}^{-1} q_{i3} & \dots & q_{i2}^{-1} q_{ir} \\ q_{i3}^{-1} & q_{i3}^{-1} q_{i2} & e & \dots & q_{i3}^{-1} q_{ir} \\ \vdots & \vdots & \vdots & & \vdots \\ q_{ir}^{-1} & q_{ir}^{-1} q_{i2} & q_{ir}^{-1} q_{i3} & & e \end{bmatrix} \end{array} \right.$$

e is the identity matrix of order r . We note that $(T^i)^T = (T^i)^{-1}$ so for any element of the form S (including the element q_{ij}) satisfies $S^{-1} = S^T$ that is $SS^T = e$.

So with (39,v) satisfied,

$$\sum_{i=0}^{q-1} R_i R_i^T = r^2 I \times I + r(J-I) \times J.$$

where I and J are of size r .

We now consider another property of the R_i . Let

$B_i = [e \ q_{i2} \ q_{i3} \ \dots \ q_{ir}]$ then $R_{i-1} = B_i^T B_i$ so

$$\begin{aligned} R_{i-1} R_{j-1}^T &= B_i^T B_i B_j^T B_j \\ &= B_i^T [e \ q_{i2} \ \dots \ q_{ir}] \begin{bmatrix} e \\ -1 \\ q_{j2} \\ \vdots \\ -1 \\ q_{jr} \end{bmatrix} B_j \\ &= B_i^T J B_j \quad \text{from (39,iv)} \\ &= J \times J \quad \text{by (39,iii)} \end{aligned}$$

where J is of order q^p

Defining $P = I \times J$ we now have all the conditions of (37) except (iii) satisfied and (39,v) ensures that (37,iii) is also satisfied.

THE MATRICES Q AND R_i FOR 2^2 , 2^3 , AND 2^4 : The method we outline here for finding Q and R_i does not work for 2^5 .

Let $I = \begin{bmatrix} \overline{1} & 0 \\ 0 & \underline{1} \end{bmatrix}$ and $K = \begin{bmatrix} \overline{0} & \overline{1} \\ \underline{1} & \underline{0} \end{bmatrix}$ then define for

- (a) 2^2 , $a_1 = K \times I$ and $a_2 = I \times K$;
- (b) 2^3 , $a_1 = K \times I \times I$, $a_2 = I \times K \times I$ and $a_3 = I \times I \times K$;
- (c) 2^4 , $a_1 = K \times I \times I \times I$, $a_2 = I \times K \times I \times I$, $a_3 = I \times I \times K \times I$
and $a_4 = I \times I \times I \times K$.

Then the elements a_1 are generators of $Z_2 \times Z_2 \times \dots \times Z_2$ (repeated j times) for 2^j .

Now Q is a block matrix and we choose the first row of Q to consist of 2^j block matrices $e = I \times I \times \dots \times I$ (repeated j times). Choose the second row of Q , that is $q_{21}, q_{22}, \dots, q_{2p}$ where $p = 2^j$ by

$$q_{2i} = e = q_{i1} \quad 2 \leq i \leq p$$

$$q_{22} = a_1, q_{23} = a_2, \dots, q_{2,j+1} = a_j,$$

$$q_{2,j+1} = q_{2i} q_{2,i+1}$$

$$q_{ij} = q_{i+k,j-k} \text{ where if } j-k < 2 \text{ replace } j-k \text{ by } j-k+p-1,$$

and simplifying the $q_{2,j+i}$ by using the fact that $a_i^2 = e$ and $a_i a_j = a_j a_i$ for every i and j .

For example the matrix Q for $p = 2^3$ is (replacing a_1 by a , a_2 by b and a_3 by c)

$$R_0 = \begin{pmatrix} e & e & e & e & e & e & e & e \\ e & a & b & c & ab & bc & abc & ac \\ e & b & c & ab & bc & abc & ac & a \\ e & c & ab & bc & abc & ac & a & b \\ e & ab & bc & abc & ac & a & b & c \\ e & bc & abc & ac & a & b & c & ab \\ e & abc & ac & a & b & c & ab & bc \\ e & ac & a & b & c & ab & bc & abc \end{pmatrix}$$

and the matrices R_i (using (40)) are

$$R_0 = J_8 \times I_8,$$

$$R_1 = \begin{array}{|c|c|c|c|c|c|c|c|} \hline e & a & b & c & ab & bc & abc & ac \\ \hline a & e & ab & ac & b & abc & bc & c \\ \hline b & ab & e & bc & a & c & ac & abc \\ \hline c & ac & bc & e & abc & b & ab & a \\ \hline ab & b & a & abc & e & ac & c & bc \\ \hline bc & abc & c & b & ac & e & a & ab \\ \hline abc & bc & ac & ab & c & a & e & b \\ \hline ac & c & abc & a & bc & ab & b & e \\ \hline \end{array}$$

$$R_2 = \begin{array}{|c|c|c|c|c|c|c|c|} \hline e & b & c & ab & bc & abc & ac & a \\ \hline b & e & bc & a & c & ac & abc & ab \\ \hline c & bc & e & abc & b & ab & a & ac \\ \hline ab & a & abc & e & ac & c & bc & b \\ \hline bc & c & b & ac & e & a & ab & abc \\ \hline abc & ac & ab & c & a & e & b & bc \\ \hline ac & abc & a & bc & ab & b & e & c \\ \hline a & ab & ac & b & abc & bc & c & e \\ \hline \end{array}$$

$$R_3 = \begin{array}{|c|c|c|c|c|c|c|c|} \hline e & c & ab & bc & abc & ac & a & b \\ \hline c & e & abc & b & ab & a & ac & bc \\ \hline ab & abc & e & ac & c & bc & b & a \\ \hline bc & b & ac & e & a & ab & abc & c \\ \hline abc & ab & c & a & e & b & bc & ac \\ \hline ac & a & bc & ab & b & e & c & abc \\ \hline a & ac & b & abc & bc & c & e & ab \\ \hline b & bc & a & c & ac & abc & ab & e \\ \hline \end{array}$$

$$R_4 = \begin{bmatrix} e & ab & bc & abc & ac & a & b & c \\ ab & e & ac & c & bc & b & a & abc \\ bc & ac & e & a & ab & abc & c & b \\ abc & c & a & e & b & bc & ac & ab \\ ac & bc & ab & b & e & c & abc & a \\ a & b & abc & bc & c & e & ab & ac \\ b & a & c & ac & abc & ab & e & bc \\ c & abc & b & ab & a & ac & bc & e \end{bmatrix}$$

$$R_5 = \begin{bmatrix} e & bc & abc & ac & a & b & c & ab \\ bc & e & a & ab & abc & c & b & ac \\ abc & a & e & b & bc & ac & ab & c \\ ac & ab & b & e & c & abc & a & bc \\ a & abc & bc & c & e & ab & ac & b \\ b & c & ac & abc & ab & e & bc & a \\ c & b & ab & a & ac & bc & e & abc \\ ab & ac & c & bc & b & a & abc & e \end{bmatrix}$$

$$R_6 = \begin{bmatrix} e & abc & ac & a & b & c & ab & bc \\ abc & e & b & bc & ac & ab & c & a \\ ac & b & e & c & abc & a & bc & ab \\ a & bc & c & e & ab & ac & b & abc \\ b & ac & abc & ab & e & bc & a & c \\ c & ab & a & ac & bc & e & abc & b \\ ab & c & bc & b & a & abc & e & ac \\ bc & a & ab & abc & c & b & ac & e \end{bmatrix}$$

$$R_7 = \begin{bmatrix} e & ac & a & b & c & ab & bc & abc \\ ac & e & c & abc & a & bc & ab & b \\ a & c & e & ab & ac & b & abc & bc \\ b & abc & ab & e & bc & a & c & ac \\ c & a & ac & bc & e & abc & b & ab \\ ab & bc & b & a & abc & e & ac & c \\ bc & ab & abc & c & b & ac & e & a \\ abc & b & bc & ac & ab & c & a & e \end{bmatrix}$$

It may be verified that condition (39,v) is satisfied but we are unable to prove that this is necessarily so from the definitions of Q and R_i .

THE MATRICES Q AND R_i FOR 3^2 AND 7^2 : The construction we give here does not apply to 3^3 , 5^2 or 11^2 . Let T_3 be the matrix given by (38) of size 3 and T_7 be the corresponding matrix of size 7.

Now write

$$\begin{aligned} T_a &= T_i \times I_i \\ T_b &= I_i \times T_i, \end{aligned}$$

where i is 3 or 7 respectively. The T_a and T_b are the generators of $Z_i \times Z_i$.

Now we choose $Q = (q_{mj})$, where each q_{mj} is a matrix of size i^2 , by

$$\begin{aligned} q_{1j} &= I \times I = q_{j1} & 1 \leq j \leq i^2 \\ q_{22} &= T_a, \quad q_{23} = T_b, \quad \dots \quad q_{2j} = q_{2,j-2}^{-1} q_{2,j-1} \\ q_{mj} &= q_{m+k,j-k} \quad \text{where if } j-k < 2 \text{ replace } j-k \text{ by } j-k+i^2, \end{aligned}$$

where q_{2j} is simplified by the fact that $T_a^i = T_b^i = I$, $T_a^\alpha T_b^\beta = T_b^\beta T_a^\alpha$ since $Z_i \times Z_i$ is abelian, $T_a^{-1} = T_a^{i-1}$ and $T_b^{-1} = T_b^{i-1}$.

The R_j may now be chosen using (40) and again it may be verified that the condition (39,v) is satisfied.

THE MATRICES Q AND R_i FOR 3^3 : This construction does not apply to 3^2 . Let T be the matrix given by (2) of size 3, and I be of size 3. Now write

$$T_1 = T \times I \times I, \quad T_2 = I \times T \times I, \quad T_3 = I \times I \times T.$$

Then T_1, T_2 and T_3 are the generators of $Z_3 \times Z_3 \times Z_3$.

$Q = (q_{mj})$, where q_{mj} is a matrix of size 3^3 may be chosen by

$$\begin{aligned} q_{1j} &= I \times I \times I = q_{j1} \quad 1 \leq j \leq 3^3 \\ q_{22} &= T_1, \quad q_{23} = T_2, \quad q_{24} = T_3 \quad \dots \quad q_{2j} = q_{2,j-3}^{-1} q_{2,j-2} \\ q_{mj} &= q_{m+k,j-k} \quad \text{where if } j-k < 2 \text{ replace } j-k \text{ by} \\ &\quad j-k+3^3-1, \end{aligned}$$

where q_{2j} is simplified by using $T_1^3 = T_2^3 = T_3^3 = I \times I \times I$, the commutativity of elements of $Z_3 \times Z_3 \times Z_3$, and $T_k^{-1} = T_k^2$.

The R_i may be chosen using (40) and condition (39,v) verified.

So we have shown the matrices P, Q, Q^* and R_i exist for orders $2^2, 2^3, 2^4, 3^2, 3^3$ and 7^2 .

Theorem 7.1 : There exists a $(q^2(q+2), q(q+1), q)$ configuration whenever q is a prime or $q = 2^2, 2^3, 2^4, 3^2, 3^3$ or 7^2 .

Proof : We have already shown that $(0,1)$ matrices $R_i, 0 \leq i \leq q-1$, Q and R of order q^2 , satisfying the equations (37,i,ii,iii,iv,v) exist for the required q .

Let S be the $q^2(q+2)$ block matrix given by

$$S = \begin{bmatrix} \overline{0} & P & R_0 & R_1 & \dots & R_{q-3} & R_{q-2} & R_{q-1} \\ R_{q-1} & 0 & P & R_0 & \dots & R_{q-4} & R_{q-3} & R_{q-2} \\ \vdots & & & & & & \vdots & \\ R_0 & R_1 & R_2 & R_3 & \dots & R_{q-1} & 0 & P \\ \underline{P} & R_0 & R_1 & R_2 & \dots & R_{q-2} & R_{q-1} & 0 \end{bmatrix}$$

$$\begin{aligned} \text{then } SS^T &= I_{q+2} \times \{PP^T + \sum_{i=0}^{q-1} R_i R_i^T\} + (J_{q+2} - I_{q+2}) \times qJ \times J \\ &= q^2 I_{q^2(q+2)} + qJ_{q^2(q+2)}. \end{aligned}$$

Now S is a $0,1$ matrix, and the triplet $v = q^2(q+2)$, $k = q(q+1)$, $\lambda = q$ is easily seen to satisfy the necessary condition for (v,k,λ) configurations, so S is the incidence matrix of a $(q^2(q+2), q(q+1), q)$ configuration. ***

For the rest of this section q is a prime.

We now consider the q $(0,1)$ matrices S_i , $0 \leq i \leq q-1$, of order q^2 given by

$$(41) \quad S_i = \begin{bmatrix} I & I & I & \dots & I \\ T^i & T^i & T^i & \dots & T^i \\ T^{2i} & T^{2i} & T^{2i} & \dots & T^{2i} \\ \vdots & & & & \\ T^{(k-1)i} & T^{(k-1)i} & T^{(k-1)i} & \dots & T^{(k-1)i} \end{bmatrix}$$

Lemma 7.2 : Let $B = \{1, \dots, q-1\}$ and $A = B \cup \{0\}$, I, J be of order q , I^*, J^* be of order q^2 , and P, R_i and Q be as above satisfying (37, i, ii, iii, iv, v). Then the S_i defined by (41) satisfy

$$\begin{aligned}
 (42) \quad & \left\{ \begin{aligned}
 & (i) \quad PP^T + \sum_{i=0}^{q-1} = q^2 I^* + qJ^*, \\
 & (ii) \quad PP^T + S_j^T S_j + \sum_{k=1}^{q-1} R_k R_k^T = q^2 I^* + qJ^*, \quad \text{for every } j \in A. \\
 & (iii) \quad S_0 P^T + \sum_{i=1}^{q-1} S_i R_i^T = qJ^*, \\
 & (iv) \quad PS_0 + \sum_{i=0}^{q-2} S_i R_{i+1}^T = qJ^*, \\
 & (v) \quad PR_j^T + S_{q-j} P^T + (q-2) S_i R_k^T = qJ^*, \quad \text{for every } i, j, k \\
 & \quad \quad \quad \text{such that } i \in A, k \in B. \\
 & (vi) \quad S_i^T S_j + R_1 P^T + (q-2) R_k R_m^T = qJ^*, \quad \text{for every } i, j, k, m \\
 & \quad \quad \quad \text{such that } i, j \in A, \\
 & \quad \quad \quad i \neq j; k, m \in B, m \neq k. \\
 & (vii) \quad S_i^T S_j + PR_k^T + R_m P^T + (q-3) R_n R_s^T = qJ^* \quad \text{for every } i, j, k, m, \\
 & \quad \quad \quad n, s \text{ such that } i, j \in A \\
 & \quad \quad \quad i \neq j; k, m, n, s \in B, n \neq s. \\
 & (viii) \quad S_0^T P^T + PR_1^T + (q-2) R_m R_n^T = qJ^* \quad \text{for every } m, n \in B, \\
 & \quad \quad \quad m \neq n. \\
 & (ix) \quad S_i^T P^T + R_j S_0^T + PR_k^T + (q-3) R_m R_n^T = qJ^*, \quad \text{for every } i, j, k, m, \\
 & \quad \quad \quad n \text{ such that } i \in A; \\
 & \quad \quad \quad j, k, m, n \in B, m \neq n.
 \end{aligned} \right.
 \end{aligned}$$

Proof : We first prove the following results

$$\begin{aligned}
 (a) \quad S_i^T P^T &= \begin{bmatrix} I & T^{q-i} & \dots & T^i \\ I & T^{q-i} & \dots & T^i \\ \vdots & & & \vdots \\ I & T^{q-i} & \dots & T^i \end{bmatrix} \begin{bmatrix} J & & & \\ & J & & \\ & & \ddots & \\ & & & J \end{bmatrix} \\
 &= J^*
 \end{aligned}$$

(b) Since S_0 is symmetric, we have, using (a)

$$S_0^T P^T = PS_0 = S_0 P^T = J^*.$$

(c) Clearly

$$S_j^T P^T = J^* = PS_j^T.$$

(d) From (37,i)

$$R_j P^T = J^* = PR_j^T.$$

$$(e) \quad S_j^T S_j = \begin{bmatrix} I & T^{q-j} & \dots & T^j \\ I & T^{q-j} & \dots & T^j \\ \vdots & \vdots & & \vdots \\ I & T^{q-j} & \dots & T^j \end{bmatrix} \begin{bmatrix} I & I & \dots & I \\ T^j & T^j & \dots & T^j \\ \vdots & \vdots & & \vdots \\ T^{q-j} & T^{q-j} & \dots & T^{q-j} \end{bmatrix}$$

$$= qJ \times I.$$

$$(f) \quad S_i R_j^T = \begin{bmatrix} I & I & \dots & I \\ T^i & T^i & \dots & T^i \\ \vdots & \vdots & & \vdots \\ T^{q-i} & T^{q-i} & & T^{q-i} \end{bmatrix} \begin{bmatrix} I & T^j & T^{2j} & \dots & T^{q-j} \\ T^{q-j} & I & T^j & \dots & T^{q-2j} \\ \vdots & \vdots & \vdots & & \vdots \\ T^j & T^{2j} & T^{3j} & & I \end{bmatrix}$$

$$= (T^{(k-1)i})_{k,m} (T^{(n-m)j})_{m,n}$$

$$= \left(\sum_{m=1}^q T^{(k-1)i+(n-m)j} \right)_{k,n}$$

Since i, j are fixed by the S_i and R_j , and k, n are fixed by the position in $S_i R_j^T$

$$(k-1)i + nj - mj$$

runs through the residues module q as m goes from 1 to q , so

$$\sum_{m=1}^q T^{(k-1)i+(n-m)j} = \sum_{s=0}^{q-1} T^s = J$$

and

$$S_i R_j^T = J^*$$

(g) Since S_0 is symmetric, we have, using (f)

$$S_0 R_j^T = R_j S_0 = J^*.$$

$$\begin{aligned} (h) \quad S_i S_i^T &= (T^{(k-1)i})_{k,m} (T^{q-(n-1)i})_{m,n} \\ &= \left(\sum_{m=1}^q T^{q+(k-n)i} \right)_{k,n} \\ &= q (T^{(k-n)i})_{k,n} \\ &= q R_i^T. \end{aligned}$$

Then using the fact that

$$\sum_{i=0}^{q-1} R_i = \left(\sum_{i=0}^{q-1} R_i \right)^T = qI \times I + (J-I) \times J,$$

we have

$$\sum_{i=0}^{q-1} S_i S_i^T = q \{ qI \times I + (J-I) \times J \}.$$

$$\begin{aligned} (k) \quad S_i^T S_j &= (T^{q-(n-1)i})_{m,n} (T^{(n-1)j})_{n,k} \\ &= \left(\sum_{n=1}^q T^{(n-1)(j-1)} \right)_{m,k}. \end{aligned}$$

i, j are fixed by S_i^T and S_j , so if $i \neq j$

$$(n-1)(j-i)$$

runs through the numbers $1, \dots, q$ as n runs through these numbers. Hence

$$S_i^T S_j = J^*, \quad i \neq j.$$

THE RESULTS : The formulae (42,i) to (42,ix) can now be verified as follows. For

- (i) use (37,iv) and h ;
- (ii) use (37,iv), (e) and (37,iii) ;
- (iii) use (b) and (f) ;
- (iv) use (b) and (f) ;
- (v) use (d),(c) and (f) ;
- (vi) use (k),(d) and (37,ii) ;
- (vii) use (k),(d) and (37,ii) ;
- (viii) use (b),(d),(37,ii) ;
- (ix) use (a),(g), (d) and (f).

Theorem 7.3 : Let V be the $q^2(q+2)(0,1)$ block matrix given by

$$\begin{array}{cccccccc}
 0 & P & S_0 & S_1 & S_2 & \dots & S_{q-3} & S_{q-2} & S_{q-1} \\
 S_0^T & 0 & P & R_1 & R_2 & \dots & R_{q-3} & R_{q-2} & R_{q-1} \\
 S_1^T & R_{q-1} & 0 & P & R_1 & \dots & R_{q-4} & R_{q-3} & R_{q-2} \\
 S_2^T & R_{q-2} & R_{q-1} & 0 & P & \dots & R_{q-5} & R_{q-4} & R_{q-3} \\
 \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
 S_{q-3}^T & R_3 & R_4 & R_5 & R_6 & \dots & P & R_1 & R_2 \\
 S_{q-2}^T & R_2 & R_3 & R_4 & R_5 & \dots & 0 & P & R_2 \\
 S_{q-1}^T & R_1 & R_2 & R_3 & R_4 & \dots & R_{q-1} & 0 & P \\
 P & S_0 & R_1 & R_2 & R_3 & \dots & R_{q-2} & R_{q-1} & 0
 \end{array}$$

Then V is the incidence matrix of a $(q^2(q+2), q(q+1), q)$ configuration, for q a prime.

Proof : This is easily verified using lemma 7.2.

We include the two matrices S (from theorem 7.1) and V (above) because V has S_0 in the last row fixed and not obviously in the pattern. It is possible that S and V are non-isomorphic.

§7.3 SOME BIBDS

~~_____~~
~~_____~~
~~_____~~

The result of theorem 7.4 was known ^{previously} but not expressed in the form of ^{our} theorem. Theorem 7.6 is completely superceded by the results ~~_____~~ on Steiner triples. Theorem 7.7 has been proved by Van Lint and Seidel [1, p 342].

Theorem 7.5 appears to be genuinely new, and important, as it is a means of constructing (b,v,r,k,λ) configurations from some (v,k,λ) configurations : previously only the converse was readily usable.

Q and Q^* are as defined in 7.2, and we use the style of Ryser [1].

Theorem 7.4: The following (b,v,r,k,λ) configuration exists for q a prime power

$$(q(q+1), q^2, q+1, q, 1).$$

Proof : It is easily seen that these five numbers satisfy the necessary conditions for (b,v,r,k,λ) configurations.

Now let $\varepsilon^T = (1, 1, \dots, 1)$ be a $1 \times q$ matrix and I, J of order q , then A given by

$$A^T = \begin{bmatrix} \overline{I} & \varepsilon & \overline{Q} \\ \hline I_q & & \end{bmatrix}$$

has q non-zero elements in each row and $q+1$ in each column.

Now
$$A^T A = qI \times I + J \times J$$

so A is the incidence matrix of a $(q(q+1), q^2, q+1, q, 1)$ configuration.***

If $\exists (b, q, r, k, \lambda) \Rightarrow q, (q+k+\lambda), kq, q+k+\lambda, k, \lambda$ (check back 1939)

Theorem 7.5 : Whenever a (q, k, λ) configuration exists, q a prime power, then the following (b, v, r, k, λ) configuration exists :

$$(q(k^2 + \lambda), qk, k^2 + \lambda, k, \lambda)$$

Proof: It is easily verified that these five numbers satisfy the necessary conditions for (b, v, r, k, λ) configurations.

Let V be the incidence matrix of the (q, k, λ) configuration then A given by

$$A^T = [I_k \times V, Q^*, Q^*, \dots, Q^*], \quad Q^* \text{ repeated } \lambda \text{ times}$$

has k non-zero elements in every row and $\lambda q + k = k^2 + \lambda$

(using the $\lambda(q-1) = k(k-1)$ condition) non-zero elements in each column.

$$\begin{aligned} \text{Now } A^T A &= (k - \lambda + \lambda q) I + \lambda J \\ &= k^2 I_{qk} + \lambda J_{qk} \quad (\text{using } \lambda(q-1) = k(k-1)) \end{aligned}$$

so A is the incidence matrix of the required configuration. ***

Theorem 7.6 : The (b, v, r, k, λ) configuration

$(\frac{1}{2}q(3q-1), 3q, \frac{1}{2}q(3q-1), 3, 1)$ exists for q odd, $q \neq 1$.

Proof : Let T be given by (38) and I, J be of order q . It is easily verified that the quintuple satisfies the necessary conditions for (b, v, r, k, λ) configurations.

Now choose $A_i = T^i + T^{-i}$ and $p = \frac{q-1}{2}$; then

$$\begin{aligned} \sum_{i=1}^p A_i A_i^T &= \sum_{i=1}^p (T^i + T^{-i})^2 \\ &= \sum_{i=1}^p (T^{2i} + T^{-2i}) + (q-1) I \\ &= (q-2) I + J \end{aligned}$$

and
$$\sum_{i=1}^p A_i = J - I.$$

So if B is defined by

$$B^T = \begin{bmatrix} I & A_1 A_2 & \dots & A_p & I & I & \dots & I \\ I & I & I & \dots & I & & & A_1 A_2 & \dots & A_p \\ I & & & & A_1 A_2 & \dots & A_p & I & I & \dots & I \end{bmatrix}$$

B has 3 non-zero elements in each row and $\frac{3q-1}{2}$ non-zero elements in each column and

$$B^T B = \frac{3q-3}{2} I_{3q} + J_{3q}.$$

Hence B is the incidence matrix of a $(\frac{1}{2}q(3q-1), 3q, \frac{1}{2}(3q-1), 3, 1)$ configuration .

Theorem 7.7 : Let N be any matrix of odd order $v-1$ with zero diagonal and every other element $+1$ or -1 , further let $NJ = JN = 0$ where J is the matrix with every element $+1$ and

$$NN^T = (v-1) I_{v-1} - J_{v-1}$$

then there is a $(2(v-1), v, v-1, v/2, (v-2)/2)$ configuration.

Proof : Since N has zero diagonal and every other element $+1$ or -1 C and D defined (with I and J of order $v-1$) by

$$C = \frac{1}{2} (N + I + J)$$

$$D = \frac{1}{2} (N - I + J)$$

are $(0,1)$ matrices. Now

$$CC^T + DD^T = \frac{1}{2} (NN^T + I + (v-1)J) = \frac{v}{2} I + \frac{v-2}{2} J$$

and

$$JC = v/2J = CJ$$

$$JD = (v-2)/2J = DJ.$$

We define ω_v , ω_b and e to be the vectors of v , b and $(v-1)$ 1's respectively and A^T by

$$A^T = \begin{bmatrix} D & C \\ e & 0 \end{bmatrix}.$$

So A is $2(v-1) \times v$, and

$$\omega_v A^T = \frac{1}{2} v \omega_b, \quad A^T \omega_b^T = (v-1) \omega_v^T,$$

$$\begin{aligned} A^T A &= \begin{bmatrix} D & C \\ e & 0 \end{bmatrix} \begin{bmatrix} D^T & e^T \\ C^T & 0 \end{bmatrix} \\ &= \begin{bmatrix} DD^T + CC^T & \frac{1}{2}(v-2)e^T \\ \frac{1}{2}(v-2)e & v-1 \end{bmatrix} \\ &= \frac{1}{2}vI_v + \frac{1}{2}(v-2)J_v. \end{aligned}$$

Thus A is the incidence matrix of a $(2(v-1), v, v-1, \frac{1}{2}v, \frac{1}{2}(v-2))$ configuration. ***

§7.4 NUMERICAL RESULTS FROM THEOREMS IN THIS CHAPTER.

Some of our results put into classes results which previously appeared to be 'one off' configurations. We now compare our results with the table in Marshall Hall's book [1, p.291 - 298].

We noted that our results use $(7,3,1)$ to form a $(70,21,10,3,1)$ configuration, but the complementary configuration of $(7,3,1)$, namely $(7,4,2)$, yields $(26,28,18,4,2)$ which is a multiple of $(63,28,9,4,1)$. Also we noted an $(182,169,14,13,1)$ and a $(26,14,13,7,6)$ design neither of which appear in Hall [].

The

theorems of this chapter give the following designs

with $r \leq 20$. (Marshall Hall's table assumes $r \leq 15$).

b	v	r	k	λ	M.HALL NUMBER	FISHER -YATES	RAO NUMBER	NOTE OR THEOREM
6	4	3	2	1				7.4, 7.7
12	9	4	3	1	2			7.4, 7.6
10	6	5	3	2	4			7.7
20	16	5	4	1	6			7.4
15	6	5	2	1				7.5
16	16	6	6	2	10	5		7.1
30	25	6	5	1	11			7.4
14	8	7	4	3	13			7.7
35	15	7	3	1	14	7		7.6
56	49	8	7	1	24			7.4
18	10	9	5	4	27			7.7
63	28	9	4	1	32	21		I find the multiple (126,28,18,4,2)
72	64	9	8	1	36			7.4
70	21	10	3	1	38	25		7.5, 7.6
90	81	10	9	1	45			7.4
22	12	11	6	5	49			7.7
44	12	11	3	2	47		32	7.5
45	45	12	12	3	64		49	7.1
132	121	12	11	1	68			7.4
26	14	13	7	6	not included			7.7
117	27	13	3	1	70			7.6
143	66	13	3	1	77		56	I find the multiple (429,66,39,6,3)
182	169	14	13	1	not included			7.4
30	16	15	8	7	97			7.7
176	33	16	3	1				7.6
34	18	17	9	8				7.7

b	v	r	k	λ	M.HALL NUMBER	FISHER -YATES	RAO NUMBER	NOTE OR THEOREM
221	52	17	4	1				7.5
272	256	17	16	1				7.4
126	28	18	4	2				7.5
306	289	18	17	1				7.4
38	20	19	10	9				7.7
95	20	19	4	3				7.5
247	39	19	3	1				7.6
96	96	20	20	4				7.1
380	361	20	19	1				7.4

§ 7.5 REVISIONS OF THE TABLE IN M.HALL'S BOOK

None of this section is new but for completeness we include, for reference, the errors and misprints we have found in the table in Hall [1, p 291 - 298], and some revisions. We make no claims that this is a complete list of the corrections.

M.HALL NUMBER	v	b	r	k	λ	COMMENT
5	11	11	5	5	2	1,3,4,5,9 mod 11.
13	8	14	7	4	3	k = 4.
31	25	25	9	9	3	ℓ_3 of solution: pigotswxh.
53	56	56	11	11	2	known: Hall, Lane, Wales [1].
61	33	44	12	9	3	known: Takeuchi [1].
64	45	45	12	12	3	known: see §7.1.
between 67 and 70	26	14	13	7	6	theorem 7.7.
77	66	143	13	6	1	known: Rao [1].
between 91 and 92	169	182	14	13	1	theorem 7.4.
96	16	40	15	6	5	r=15; ℓ_2 of solution: [0,8,1,9,3,11] mod 16 period 8.
99	26	65	15	6	3	r = 15.
104	36	36	15	15	6	known : see §7.1.

§7.6 FALSITY OF A THEOREM OF CLATWORTHY ON THE (111,11,1) AND
(110,100,11,10,1) - configurations

It has been reported in Clatworthy [1] that the (111,11,1) and (110,100,11,10,1) are impossible. However the proof is clearly wrong. Clatworthy's result comes from theorem 4.1 of Shrikhande, Raghavarao, and Tharthare [1], which contains a list of necessary conditions for the existence of various types of partially balanced incomplete block designs. Many of these conditions are of the form

$$x^2 + y^2 = nz^2 \text{ must be soluble in the integers.}$$

This statement (see Hardy and Wright [1,p 299]) is equivalent to

n must be expressible as a sum of integer squares

In Shrikhande, Raghavarao, and Tharthare [1] this is stated as

any prime factor of the square - free part of n must be congruent to 1 (mod 4).

Clearly this latter statement is not equivalent to the first two as

$$1^2 + 3^2 = 10$$

but 10 has two prime factors, 2 and 5, and

$$2 \not\equiv 1 \pmod{4}.$$

The latter statement should have read (see Hardy and Wright [1,p])

no prime factor of the square - free part of n can be $\equiv 3 \pmod{4}$.

For the existence of an (110,100,11,10,1) - configuration Shrikhande, Raghavarao and Tharthare require that

$$x^2 + y^2 = 10z^2$$

be soluble in the integers; we have shown this is possible.

The theorem, as originally stated would have implied that this configuration and the $(111,11,1)$ configuration did not exist. This is the result Clatworthy used. Clatworthy knows of this error.

We only include this section in order to be able to indicate that the existence or otherwise of the $(111,11,1)$ is, as yet, unresolved.

CHAPTER VIII : ON INTEGER MATRICES OBEYING CERTAIN MATRIX EQUATIONS

Most of this chapter is included in J.Wallis [5].

Some interesting theorems have been discovered on the subject of integer matrices by H.J.Ryser [2], [3], [4], K.Majindar [1] and W.G Bridges and H J,Ryser [1]. We have included the theorem of Ryser we use in the text. Other specialized integer matrices not immediately related to block designs or Hadamard matrices have been studied by E.C.Johnsen [1].

In this chapter we look at some integer matrices satisfying certain restrictive matrix equations.

§8.1 THE NATURE OF MATRICES SATISFYING THE EQUATIONS FOR THE CORE OF A SKEW-HADAMARD MATRIX

In §4.2 we showed that solutions to the equations

$$(43) \quad AA^T = vI - J, \quad AJ = O = JA \quad \text{and} \quad A^T = -A$$

exist for an infinitude of matrices A of order v . In these cases it is clear that A is a $(0,1,-1)$ matrix with zero diagonal and 1 or -1 elsewhere. We now show that it is possible to have a matrix A satisfying (43) but which is not

a $(0,1,-1)$ matrix. Consider

$$A = \begin{bmatrix} 0 & 1 & -1 & -1 & 1 & 1 & -1 \\ -1 & 0 & 2 & -1 & 0 & 0 & 0 \\ 1 & -2 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & -2 & 0 \\ -1 & 0 & -1 & 0 & 0 & 0 & 2 \\ -1 & 0 & 0 & 2 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & -2 & 1 & 0 \end{bmatrix}$$

then $AA^T = 7I - J$, $AJ = 0 = JA$ and $A^T = -A$.

However there are considerable restrictions on the elements of A as theorem 4.9 and the following theorem show.

Theorem 8.1: Let A be an integer matrix of order v , where $v \equiv 3 \pmod{4}$, satisfying

$$AA^T = vI - J, \quad AJ = 0 = JA, \quad A^T = -A.$$

Suppose $-a$ is the least element of A ; define

$$B = A + a(J - I);$$

write e for the g.c.d. of the non-zero elements of B . Then either $e = 1$ or A has zero diagonal and $+1$ or -1 elsewhere.

Proof: $A^T = -A$, so A has zero diagonal, and hence B has zero diagonal. B satisfies

$$BB^T = (v + a^2)I + [a^2(v - 2) - 1]J$$

$$BJ = a(v - 1)J.$$

Consider the matrix $C = \frac{1}{e} B$. C is an integer matrix and

$$CC^T = \frac{v + a^2}{e^2} I + \frac{a^2(v-2) - 1}{e^2} J$$

$$CJ = \frac{a(v-1)}{e} J.$$

The element $-a$ occurs in A ; and since $A^T = -A$ the element a must occur in A and must be the greatest element of A . Then $2a$ is the greatest element of B and $\frac{2a}{e}$, which is therefore an integer, the greatest element of C .

$e|2a$, so there are two possibilities:

- (i) e is odd, $e|a$;
- (ii) e is even.

If (i) is true, since $\frac{a^2(v-2) - 1}{e^2}$ is an integer we have $e^2|1$ and so $e = 1$.

Now consider (ii). $v \equiv 3 \pmod{4}$, so since $e^2|v + a^2$ and e is even we must have a odd. Since e is even, every element of B is even; all the non-diagonal elements of A differ from elements of B by a , an odd number, so they are odd.

$AA^T = vI - J$, so (evaluating the i th diagonal element)

$$\sum_{j=1}^v a_{ij}^2 = v - 1.$$

Each a_{ij} is an odd integer, unless $j = i$; so $a_{ij}^2 \geq 1$, and

$$\sum_{j=1}^v a_{ij}^2 \geq v - 1,$$

with equality only when each a_{ij} (except a_{ii}) is ± 1 . This holds for every i , so we have the result. ***

§8.2 INTEGER SOLUTIONS OF $AA^T = a^2(k-\lambda)I + a^2\lambda J$, $AJ = akJ$ WITH a AN INTEGER

Let B be the incidence matrix of a (v, k, λ) configuration then if $A = aB$ where $a > 0$ is an integer

$$(44) \quad \begin{cases} AA^T &= a^2(k-\lambda)I + a^2\lambda J \text{ and} \\ AJ &= akJ \\ \lambda(v-1) &= k(k-1). \end{cases}$$

One might conjecture, in view of the powerful theorems of Ryser [3] and Bridges and Ryser [1], that an integer matrix satisfying the equations (44) would necessarily be a times the incidence matrix of a (v, k, λ) configuration.

But we see the matrix

$$A = \begin{bmatrix} 0 & 3 & 0 & 0 & 1 & 1 & 1 \\ -1 & 0 & 2 & 1 & 2 & 1 & 1 \\ 2 & 0 & 0 & 0 & 2 & 2 & 0 \\ 2 & 1 & 2 & 0 & 1 & -1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 3 \\ 1 & 1 & 0 & 3 & 1 & 0 & 0 \\ 1 & 1 & 2 & 1 & -1 & 2 & 0 \end{bmatrix}$$

satisfies

$$AA^T = 4(2) I + 4(1) J$$

$$AJ = 2(3) J$$

which is (44) with $a = 2$, $v = 7$, $k = 3$ and $\lambda = 1$.

So we need other conditions on the matrix A before we can ensure that every element is 0 or a . In §8.3 we

consider some such conditions.

§8.3 MATRICES SATISFYING $AA^T = pI + Q$, $AJ = dJ$ WHERE p AND d
ARE CONSTANT

Theorem 8.2: If $B = (b_{ij})$ of order b is a matrix of non-negative integers such that $\sum_{j=1}^b b_{ij}^2 = p$, p a constant, for every i and $BJ = dJ$, d a non-zero constant then if every element of B is 0 or

- (i) $\geq \frac{p}{d}$; or
(ii) $\leq \frac{p}{d}$,

then every element of B is 0 or $\frac{p}{d}$.

Proof:

$$\sum_{j=1}^b b_{ij}^2 = p \text{ and } \sum_{j=1}^b b_{ij} = d, \text{ so}$$

$$d \sum_j b_{ij}^2 - p \sum_j b_{ij} = dp - dp = 0$$

that is

$$\sum_j b_{ij} (db_{ij} - p) = 0$$

then since every element of B is non-negative, every element is 0 or $\frac{p}{d}$. ***

Corollary 8.3: If $B = (b_{ij})$ of order b is a matrix of non-negative integers such that $\sum_{j=1}^b b_{ij}^2 = p$, a constant > 0 for every i and $BJ = dJ$, d a non-zero constant and if every element of B is 0 or (i) $\geq \frac{p}{d}$, (ii) $\leq \frac{p}{d}$ then $d|p$. ***

Corollary 8.4: If $B = (b_{ij})_b$ of order b is a matrix of non-negative integers such that $\sum_{j=1}^b b_{ij}^2 = p$, a constant > 0 for every i and $BJ = pJ$, then every element of B is 0 or 1. ***

Similarly we may obtain the following results for matrices with non-positive elements.

Theorem 8.5: If $B = (b_{ij})_b$ of order b is a matrix of non-positive integers such that $\sum_{j=1}^b b_{ij}^2 = p$, p a constant, for every i and $BJ = dJ$, d a non-zero constant then if every element of B is 0 or (i) $\leq \frac{p}{d}$; or (ii) $\geq \frac{p}{d}$, then every element of B is 0 or $\frac{p}{d}$.

Proof: The proof is almost identical with that of theorem 8.2. ***

Corollary 8.6: If $B = (b_{ij})_b$ of order b is a matrix of non-positive integers such that $\sum_{j=1}^b b_{ij}^2 = p$, a constant for every i and $BJ = dJ$, d a non-zero constant and if every element of B is 0 or (i) $\leq \frac{p}{d}$, (ii) $\geq \frac{p}{d}$ then $d|p$. ***

Corollary 8.7: If $B = (b_{ij})_b$ of order b is a matrix of non-positive integers such that $\sum_{j=1}^b b_{ij}^2 = p$, a constant for every i , and $BJ = pJ$, then every element of B is 0 or 1. ***

We now quote a theorem of Ryser which is very important in the study of integer matrices and which is used in theorem 8.9; the enunciation of M.Hall [1,p284] is

Theorem 8.8: Suppose $B = (b_{ij})$ is a $v \times v$ matrix of integers and

$$\begin{aligned}\lambda(v-1) &= k(k-1) \\ BB^T &= (k-\lambda)I + \lambda J \\ BJ &= kJ\end{aligned}$$

then B is the incidence matrix of a symmetric block design. ***

Theorem 8.9: Let A , of order v , be a matrix of non-negative integers which satisfies

$$\begin{aligned}AA^T &= (b^2k - b^2\lambda)I + b^2\lambda J \\ AJ &= bkJ \\ \lambda(v-1) &= k(k-1)\end{aligned}$$

then if every element is $\leq b$, then A is b times the incidence matrix of a (v, k, λ) configuration.

Proof: Since every element is $\leq \frac{p}{d} = \frac{b^2k}{bk} = b$ we have from theorem 8.2 that every element is 0 or b .

Form

$$B = \frac{1}{b} A$$

then B satisfies

$$\begin{aligned}BB^T &= (k-\lambda)I + \lambda J \\ BJ &= kJ.\end{aligned}$$

These equations together with theorem 8.8 show B is the incidence matrix of a (v, k, λ) configuration and so we have the result. ***

The next theorem is quite interesting.

Theorem 8.10: Let B be an integer matrix of order b which satisfies

$$BB^T = (p - q)I + qJ$$

$$BJ = dJ$$

where p, q and d are constants and $d > 0$. Write w and z for the greatest and least elements of B respectively, and $\omega = |w|$. If

$$z \leq \frac{d}{b} = \delta \text{ and } z \leq \frac{\omega d + p}{d + \omega b}$$

then δ is an integer, $p = d\delta = b\delta^2$, and

$$B = \delta J.$$

Proof: Clearly $p = \sum_i b_{iJ}^2$, so $p \geq 0$; and $d > 0$ implies $p > 0$. Consider the class of matrices

$$C_\alpha = B + \alpha J$$

where α is an integer and $\alpha \geq \omega$. Every element of every member of this class is non-negative and

$$C_\alpha C_\alpha^T = (p - q)I + (\alpha^2 b + 2\alpha d + q)J$$

$$C_\alpha = (d + \alpha b)J.$$

Then, using theorem 8.2, if every element of C_α is

$$0 \text{ or } \leq \beta = \alpha + \frac{\alpha d + p}{d + \alpha b},$$

then every element is 0 or β .

We show that the conditions on z imply that every element is $\leq \beta$. For

$$z \leq \frac{\omega d + p}{d + \omega b}$$

implies

$$z(d + \omega b) \leq \omega d + p;$$

since $z \leq \frac{d}{b}$ we have

$$zd + z\omega b + \gamma zb \leq \omega d + p + \gamma zb \leq \omega d + p + \gamma d$$

for any integer $\gamma \geq 0$, so

$$z \leq \frac{(\omega + \gamma)d + p}{d + (\omega + \gamma)b}.$$

This means (putting $\alpha = \omega + \gamma$) that for any admissible α ,

$$z + \alpha \leq \alpha + \frac{\alpha d + p}{d + \alpha b};$$

but $z + \alpha$ is the greatest element of C_α .

Therefore any element of C_α is 0 or $\alpha + \frac{\alpha d + p}{d + \alpha b}$,
so any element of B is $-\alpha$ or $\frac{\alpha d + p}{d + \alpha b}$.

Corollary 8.3 tells us that

$$A(\gamma) = \frac{(\omega + \gamma)d + p}{d + (\omega + \gamma)b}$$

is an integer for every $\gamma \geq 0$, so

$$A(\gamma) = \frac{d + p(\omega + \gamma)^{-1}}{d(\omega + \gamma)^{-1} + b}$$

is integral for all integers $\gamma \geq 0$. Therefore $\lim_{\gamma \rightarrow \infty} A(\gamma)$
must be an integer, so $b|d$. Write $d = b\delta$:

$$A(\gamma) = \frac{(\omega + \gamma)b\delta + p}{b\delta + (\omega + \gamma)b}$$

so $b|p$. Write $p = eb$:

$$A(\gamma) = \frac{(\omega + \gamma)\delta + e}{\delta + (\omega + \gamma)}.$$

Choose n any integer greater than $\delta + \omega$. Then

$$A(n - \delta - \omega) = \frac{(n - \delta)\delta + e}{n}$$

so $n | (\epsilon - \delta^2)$. But this is true for every large enough n ;

hence $\epsilon = \delta^2$. That is

$$d = b\delta$$

$$p = b\delta^2$$

so

$$p = d\delta = b\delta^2.$$

Then we have

$$\frac{\alpha d + p}{d + \alpha b} = \frac{b\delta(\alpha + \delta)}{b(\delta + \alpha)} = \delta$$

for any γ , so every element of B is $-\alpha$ or δ . Now the row sum of B is $d = b\delta$ and the sum of the squares of the elements is $p = b\delta^2$; together these imply

$$B = \delta J$$

where $\delta = \frac{d}{b}$.

APPENDIX A : A TABLE OF ORDERS $< 4,000$ FOR WHICH HADAMARD
AND SKEW-HADAMARD MATRICES ARE KNOWN

2 is omitted from the table, but there exists both
an Hadamard and a skew-Hadamard matrix of order 2.

The table shows one class from chapter II for each
matrix : the order of the matrix may also belong to other
classes. The numbers down the left hand side of the page give
the last two digits of the order while the number at the top
of each column gives the first two digits. The heading "type"
gives a class of Hadamard matrices to which the order belongs
while "skew" gives a class of skew-Hadamard matrices to which
the order belongs. A blank in the table indicates that no
matrix is known.

J.W

CW

NW

J.W. had 2174

Wallis White

28,36,44

52,60,68

skid - 4th order 2/2-0

.../140

~~first two digits~~ hundreds

last two digits	type	skew	type	skew	type	skew	type	skew	type	skew
	00	00	100	100	200	200	300	300	400	400
0			HIII	<i>S29 Hunt</i>	HII	SI	HIII	SIII	HII	SI
4	HI	SI	HII	SI	HIII	SIII	HII	SI		
8	HI	SI	HII	SI	HII	SI	HII	SI	HIII	SIII
12	HII	SI	HII	SI	HII	SI	HII	SI		
16	HI	SI	HIV		HII	SI	HIII	SIII	HII	SI
20	HII	SI	HII	SI	HIII	SIII	HII	SI	HII	SI
24	HII	SI	HIII	SIII	HII	SI	HX		HII	SI
28	HII	SI	HI	SI	HII	SI	HII	SI		
32	HI	SI	HII	SI	HXX		HII	SI	HII	SI
36	HIII	SV	HII	SI			HII	SI		
40	HII	SI	HII	SI	HII	SI	HIII	<i>ALW</i>	HII	SI
44	HII	SI	HII	SI	HII	SI	HII	SI	HII	SI
48	HII	SI	HIII		HIII	SIII	HII	SI	HII	SI
52	HIII	SIV	HII	SI	HII	SI	HII	SI	HIII	
56	HII	SI	HV		HI	SI			HII	SI
60	HII	SI	HII	SI	<i>Welsh</i>		HII	SI	HIII	SIII
64	HI	SI	HII	SI	HII	SI	HIII	SIII	HII	SI
68	HII	SI	HII	SI			HII	SI	HII	SI
72	HII	SI	HIV		HII	SI	HXII			
76	HIII	SIII	HII	SI	HIII				<i>28x17</i> <i>J.W</i>	
80	HII	SI	HII	SI	HII	SI	HII	SI	HII	SI
84	HII	SI	HIV		HII	SI	HII	SI	HIII	
88	HII	SI			HII	SI	HIII		HII	SI
92	HIV		HII	SI			HIII		HII	SI
96	HII	SI	HIII		HIII	<i>WW</i>	HIII	SIII	HIII	SIII

last two digits	first two digits									
	type	skew	type	skew	type	skew	type	skew	type	skew
	500	500	600	600	700	700	800	800	900	900
0	HII	SI	HII	SI	HIII	SIII	HII	SI	HIII	
4	HII	SI			HII	SI	HIII		HIII	
8			HII	SI	HIII				HII	SI
12	HI	SI	HVII				HII	SI	HII	SI
16	HIII		HII	SI			HIII	SIII	HIII	
20	HIX		HII	SI	HII	SI	HIII		HII	SI
24	HII	SI	HII	SI	HIII		HII	SI	HIII	SIII
28	HII	SI	HIII		HII	SI	HII	SI	HII	SI
32	~~HII~~ 14.38 J.W.		HII	SI	H ~~XIII~~		HII	SI		
36			HIII	SIII	HII	SI	~~44x19~~ 22x38		HII	SI
40	HIII	SIII	HII	SI	HII	SI	HII	SI		
44	HII	SI	HII	SI	HII	SI	HIII	SIII		
48	HII	SI	HII	SI	HIII	SIII	HII	SI	HII	SI
52	HIII	SVI			HII	SI	~~11x40~~		HIX	
56	HIII	SIII	HII	SI	HVI					
60	HII	SI	HII	SI	HII	SI	HII	SI	HII	SI
64	HII	SI	HII	SI			HII	SI		
68	HII	SI			HII	SI	HIII		HII	SI
72	HII	SI	HII	SI					HII	SI
76	HII	SI	HIII		HIII				HII	SI
80	HIII		HIII	~~2x30~~	HIII	SIII	HII	SI	~~Welsch~~	
84			HII	SI	HIII		HII	SI	HII	SI
88	HII	SI	HII	SI	HII	SI	HII	SI	~~C+H~~	
92	HIII	2x296	HII	SI	HIII	SIII			HII	SI
96			HII	SI	HIII	SIII	HII	SI	~~11x40~~	

first two digits

last two digits	type	skew	type	skew	type	skew	type	skew	type	skew
	1000	1000	1100	1100	1200	1200	1300	1300	1400	1400
0	HII	SI	<i>44x25</i>		HII	SI	HVII		HII	SI
4			HII	SI	IIII		HII	SI	IIII	SI
8	HII	SI					HII	SI	HII	SI
12	<i>23x44</i>		IIII	SI			HII	SI		
16			IIII	SI	HII	SI			IIII	
20	HII	SI	HII	SI	<i>Welsh</i>		HII	SI	IIII	SI
24	HI	SI	HII	SI	HII	SI	IIII	SI	HII	SI
28			HII	SI	IIII	SI	HII	SI	HII	SI
32	HII	SI			HII	SI	HII	SI		
36	<i>14x74</i> <i>J.W.</i>		HII	SI	IIII					
40	<i>23x29</i> HII	SI	IIII		HII	SI			HII	SI
44	IIII		HII	SI			HII	SI		
48	HII	SI	<i>14x82</i> <i>J.W.</i>		HII	SI	IIII		HII	SI
52	HII	SI	HII	SI	IIII		IIII		HII	SI
56	HII	SI	IIII		IIII		IIII	SI	HII	SI
60	IIII		IIII		HII	SI	IIII		HII	SI
64	HII	SI	HII	SI	HII	SI	<i>22x62</i>		IIII	
68							HII	SI	IIII	SI
72			HII	SI	IIII	SI	<i>14x98</i> <i>J.W.</i>		HII	SI
76			HII	SI	<i>44x</i> <i>29</i>		HII	SI	<i>18x82</i> <i>J.W.</i>	
80	IIII	SI			HII	SI	<i>H XII</i>		HII	SI
84	IIII	SI	IIII	<i>4x296</i>	HII	SI	HII	SI	HII	SI
88	HII	SI	HII	SI	HII	SI			HII	SI
92	HII	SI			HII	SI	HII	SI		
96	HII	SI	<i>complex</i> <i>Ca W</i>		HII	SI			IIII	SI

last two digits	first two digits									
	type	skew	type	skew	type	skew	type	skew	type	skew
	1500	1500	1600	1600	1700	1700	1800	1800	1900	1900
0	HII	SI	HII	SI	HII	SI	HIII		~~Atter~~ C&W	
4	~~HII~~	SI			HIII				HIX	
8	~~C&W~~		HII	SI	HIII	SIII	HIII		HII	SI
12	HII	SI	C&W				HII	SI		
16	HIII	SIII			HIII		HII	SI		
20	HII	SI	HII	SI	HII	SI	Welsh		HII	SI
24	HII	SI	HII	SI	HII	SI	HII	SI	HIII	
28			HII	SI	HII	SI				
32	HII	SI	HIII	SIII			HII	SI	HII	SI
36	HII	SI			HIII		^{18x} ^{19x} S.W.		HII	SI
40	HIII		HIII	W&W	HVII		HII	SI	Welsh	
44	HII	SI	HIII	SIII					HII	SI
48	HIII	SIII	HII	SI	HII	SI	HII	SI		
52	HIII								HII	SI
56			HII	SI	HIII	SIII	HII	SI	HIII	
60	HII	SI	HIII	SIII	HII	SI	HIII		HIX	
64	~~HIII~~ C&W		HII	SI	HIII					
68	HII	SI	HII	SI	HII	SI	HII	SI	HII	SI
72	HII	SI	2x836				HII	SI		
76	HII	SI			HII	SI	HIII		HIII	
80	HII	SI	HII	SI	Welsh		HII	SI	HII	SI
84	HII	SI	HIII	^{18x}	HII	SI	HIII	SIII	HII	SI
88			HIII	SIII	HII	SI			HII	SI
92	HIII	SIII	~~HXII~~		HII	SI	HVI		HIII	
96	HIII	SIII	HII	SI			HII	SI	HIII	SIII

last two digits	first two digits									
	type	skew	type	skew	type	skew	type	skew	type	skew
	2000	2000	2100	2100	2200	2200	2300	2300	2400	2400
0	HII	SI	HII	SI	HIX		Welsh		HII	SI
4	HII	SI	HII	SI	HII	SI	HII	SI	HIII	
8	~~02~~				HII	SI	HIII		HIII	WW
12	HII	SI	HII	SI	14x158 J.W.		HII	SI	HII	SI
16	HII	SI								
20	HIII		HIII		HIII	SIII	HIII		Welsh	
24	2x 1012		HIII	SIII	HIII	SIII			HII	SI
28	HII	SI	HII	SI			HII	SI	HIII	SIII
32			HII	SI	HIII	SIII			HII	SI
36					HIII	SIII			HIII	
40	HII	SI	HIII	SIII	HII	SI	HII	SI	HIX	
44	HIII	SIII	HII	SI	HII	SI	HII	SI		
48	HI	SI			HII	SI	HII	SI	HII	SI
52	18x114 ALW J.W.		98x22 ~~1012~~		HII	SI	HII	SI	HIII	
56					HII	SI			HIII	SIII
60	HIX		HIII	SIII	HIII		HIX		HII	SI
64	HII	SI					HIII	SIII	HII	SI
68	HIII		HIII	SIII	HII	SI	HIII	8x296	HII	SI
72	HIII		11x111		HII	SI	HII	SI	HIII	WW
76			HII	SI			HII	SI	HIII	SIII
80	HII	SI	HII	SI	HIII	WW	170x14 J.W.		HII	SI
84	HII	SI	HII	SI	~~1012~~		HII	SI	18x136 J.W.	
88	HII	SI	HII	SI	HII	SI	HIII			
92			HII	SI			HIII			
96	HII	SI	HIII		HIII				HII	SI

last two digits	first two digits									
	type	skew	type	skew	type	skew	type	skew	type	skew
	2500	2500	2600	2600	2700	2700	2800	2800	2900	2900
0	HIII		HVII		HII	SI	HII	SI		
4	HII	SI	HIII	SIII	HIII		HII	SI	HII	SI
8	22x114		HII	SI	HII	SI	HIII	SIII	HIII	SIII
12	HIII				HII	SI	HVII		HII	SI
16	(7)		HII	SI	14x194 J.W.		HII	SI	HX	
20	HII	SI	~~XXXX~~		HII	SI	HII	SI	HII	SI
24			HII	SI	HIII					
28	HII	SI			HIII				HII	SI
32	HII	SI			HII	SI	HIII			
36					HII	SI			HIII	SIII
40	HII	SI	HII	SI	HIII	2x11	HIII	SIII	HII	SI
44	HII	SI	HIII		HIII		HII	SI	HII	SI
48	14x181 J.W.		HII	SI	HIII	SIII	HII	SI		
52	HII	SI	HVI		HII	SI	HII	SI	HIII	
56	HIII	SIII	HII	SI			HII	SI		
60	HII	SI	HII	SI	HVII		HIII	SIII	HII	SI
64			HII	SI	HII	SI			HII	SI
68	HII	SI			HII	SI	HIII		HII	SI
72			HII	SI	HXIII				HII	SI
76	HII	SI							HII	SI
80	HII	SI	HIX		Welsh		HII	SI	HIII	
84	HII	SI	HII	SI	HII	SI				
88			HII	SI			HII	SI	HIII	SIII
92	HII	SI			HII	SI			HIII	SIII
96	HIII		HIII				HII	SI		

first two digits										
last two digits	type 3000	skew 3000	type 3100	skew 3100	type 3200	skew 3200	type 3300	skew 3300	type 3400	skew 3400
0	HII	SI	HIII	SIII	HII	SI	HII	SI	HII	SI
4			HIII		HII	SI	HVIII	SVII		
8	HII	SI	HIII				HII	SI	HII	SI
12	HII	SI					HII	SI		
16	HIX		<i>complex</i>		HII	SI	HIII		HIII	SIII
20	HII	SI	HII	SI	HIII		HII	SI	HIII	SIII
24	HII	SI			HIII		HII	SI		
28					HIII	SIII	HII	SI		
32	HIII	SIII	<i>H XII</i>				HII	SI	HIII	<i>WV</i>
36	<i>22x138</i>		HII	SI			HII	SI		
40	HII	SI			HII	SI	HIII	SIII	HII	SI
44	HIII		HII	SI	HIII	SIII	HII	SI	HIII	
48	HII	SI			HII	SI	HII	SI	HII	SI
52			HII	SI	HII	SI				
56			~~WV~~		HII	SI			HII	SI
60	HIX		HII	SI	HII	SI	HII	SI		
64	HII	SI	HII	SI	HIII	SIII	HIII	<i>AV</i>	HII	SI
68	HII	SI	HII	SI			HIII	<i>2x158</i>	HII	SI
72	HII	SI	<i>C+U</i>		HII	SI	HII	SI	HIII	<i>SXII</i>
76					HIII	SIII	HIII	SII	<i>22x158</i>	
80	HII	SI	<i>Welsh</i>		HIII	<i>SXII</i>	<i>Welsh</i>		HVII	
84	HII	SI	HIII	SIII			HIII		HIII	SIII
88	HII	SI	HII	SI	HIII	SIII	HIII	SIII		
92			HII	SI			HII	SI	HII	SI
96	HIII	SIII	HIII	SIII	HXX	SI	HIII		HII	SI

last two digits	first two digits									
	type	skew	type	skew	type	skew	type	skew	type	skew
	3500	3500	3600	3600	3700	3700	3800	3800	3900	3900
0	HII	SI	HIII	SXII	HIII		HIX		HIII	SIII
4			HIII				HII	SI	HII	SI
8	HIII		HII	SI	~~HXIII~~		HIX		HII	SI
12	HII	SI	~~HXIII~~		HII	SI			HII	SI
16	~~HIII~~		HIII				HII	SI		
20	HII	SI	~~Welch~~		HII	SI			HII	SI
24			HII	SI	HIII	SIII	HII	SI	HII	SI
28	HII	SI			HII	SI	HIII			
32			HII	SI					HII	SI
36	HII	SI			HII	SI			HII	SI
40	HII	SI	HVII		HII	SI	HII	SI	~~HIII~~	
44			HII	SI	HII	SI	Hx		HII	SI
48	HII	SI	HII	SI	HIII		HII	SI	HII	SI
52	HII	SI			HIII	WW	HII	SI	HIII	
56	HIII				HIII	SIII				
60	HII	SI	HII	SI	HII	SI			HII	SI
64	~~HXIII~~		HII	SI			HII	SI		
68	~~HII~~	SI			HII	SI	HIII	SIII	HII	SI
72	HII	SI	HII	SI			HII	SI	~~HXIII~~	
76	HII	SI					~~HIII~~		HII	SI
80	HIII	SIII	HII	SI	HII	SI	HIX		~~Welch~~	
84	HII	SI	~~HXIII~~		HXX				HXX	~~SIII~~
88							HII	SI	HIII	
92			HII	SI	HII	SI	14x278		HIII	SIII
96			HII	SI			5.W		HIII	SIII

APPENDIX B : THE COMPUTER PROGRAMME USED IN §4.1

This programme, written in Fortran-IV, was run on La Trobe University's PDP9 computer. The programme has an extremely long run time and some special devises have been built into the programme so as to be able to discontinue the run and restart it at the same point at a later time.

```

C
C      TO USE THE WILLIAMSON METHOD TO CONSTRUCT SKEW-TYPE
C      HADAMARD MATRICES.
C
      INTEGER P,A,B,C,D,E,P1,P2,P3,P4,P6,X,Y
      COMMON A(25),B(25),C(25),D(25),P1(25,25),
      1P2(25,25),P3(25,25),P4(25,25),P6(25,25)
900    READ(1,496)P
      J=(P-1)/2
C
C      WE NOW CONVERT J TO BINARY
C
      IB=1
      IA=2
      DO 100 K=2,J
      IB=IB+IA
100    IA=IA*2
      A(1)=1
      B(1)=1
      C(1)=1
      D(1)=1
      NEW=J
      IN=IB+1
      DO 500 I=1,IN
C
C      TO SET UP THE MATRIX A
C
      IA=I-1
      IC=NEW*2
      DO 101 N=1,IC
101    A(N+1)=0
      DO 102 N=1,NEW
      IQUOT=IA/2

```

```

      IREM=IA-IQUOT*2
      ISUB=NEW-N+2
      A(ISUB)=IREM
102    IA=IQUOT
103    DO 104 N=1,NEW
      IF (A(N+1).EQ.1) GO TO 104
      IX=P+1-N
      A(IX)=1
104    CONTINUE
C
C      TO SET UP THE MATRIX B
C
      DO 500 J=1,IN
      DO 105 N=1,IC
105    B(N+1)=0
      IA=J-1
      DO 106 N=1,NEW
      IQUOT=IA/2
      IREM=IA-IQUOT*2
      ISUB=NEW-N+2
      B(ISUB)=IREM
106    IA=IQUOT
107    DO 108 N=1,NEW
      IF (B(N+1).EQ.0) GO TO 108
      IX=P+1-N
      B(IX)=1
108    CONTINUE
C
C      TO SET UP THE MATRIX C
C
      DO 500 K=1,IN
      DO 109 N=1,IC
109    C(N+1)=0

```

```

      LA=K-1
DO 110 N=1,NEW
      IQUOT=LA/2
      IREM=LA-IQUOT*2
      ISUB=NEW-N+2
      C(ISUB)=IREM
110    LA=IQUOT
111    DO 112 N=1,NEW
      IF (C(N+1).EQ.0) GO TO 112
      IX=P+1-N
      C(IX)=1
112    CONTINUE
C
C      TO SET UP THE MATRIX D
C
      DO 500 L=1,IN
      DO 113 N=1,IC
113    D(N+1)=0
      LA=L-1
      DO 114 N=1,NEW
      IQUOT=LA/2
      IREM=LA-IQUOT*2
      ISUB=NEW-N+2
      D(ISUB)=IREM
114    LA=IQUOT
115    DO 116 N=1,NEW
      IF (D(N+1).EQ.0) GO TO 116
      IX=P+1-N
      D(IX)=1
116    CONTINUE
      DO 130 N=1,P
      IF (A(N).EQ.1) GO TO 131
      A(N)=-1

```

```

131     IF (B(N).EQ.1) GO TO 132
        B(N)=-1
132     IF (C(N).EQ.1) GO TO 133
        C(N)=-1
133     IF (D(N).EQ.1) GO TO 130
        D(N)=-1
130     CONTINUE
C
C     FORMING THE FULL MATRICES
C
        DO 124 N=1,P
        DO 124 M=1,P
        NZ=N-M+P+1
        NZ=NZ-(NZ/P)*P
        IF (NZ.EQ.0) NZ=P
        P1(M,N)=A(NZ)
        P2(M,N)=B(NZ)
        P3(M,N)=C(NZ)
124     P4(M,N)=D(NZ)
C
C     TEST FOR HADAMARDNESS
C
        DO 128 M=1,P
        DO 128 N=1,P
        NSUM=0
        DO 128 X=1,P
        NSUM=P1(M,X)*P1(N,X)+P2(M,X)*P2(N,X)+P3(M,X)*
1      P3(N,X)+P4(M,X)*P4(N,X)+NSUM
        P6(M,N)=NSUM
128     CONTINUE
        DO 129 N=1,P
        DO 129 M=1,P
        IF (M.EQ.N) GO TO 129

```

```
IF (P6(M,N).NE.0) GO TO 500
129 CONTINUE
DO 140 N=1,P
IF (A(N).EQ.1) GO TO 150
A(N)=0
150 IF (B(N).EQ.1) GO TO 151
B(N)=0
151 IF (C(N).EQ.1) GO TO 153
C(N)=0
153 IF (D(N).EQ.1) GO TO 152
D(N)=0
152 CONTINUE
140 CONTINUE
495 FORMAT(///1X)
496 FORMAT(25I2)
WRITE(6,495)
WRITE(6,496)(A(I),I=1,P)
WRITE(6,496)(B(I),I=1,P)
WRITE(6,496)(C(I),I=1,P)
WRITE(6,496)(D(I),I=1,P)
GO TO 502
500 CONTINUE
499 FORMAT(///1X,15HNO ANSWER FOUND)
503 WRITE(6,499)
502 CONTINUE
GO TO 900
STOP
END
```

APPENDIX C: THE PROOFS OF THEOREM 4.16 AND COROLLARY 4.17.

In theorem 4.16 the terms in BB^T must be expanded using

$$\begin{aligned} WW^T &= hI - J \\ JJ^T &= hJ \end{aligned}$$

so that each term becomes a sum of various combinations of I and J in some order. For example term 29 gives

$$h^4 IxIxJxIxJxIxJ - h^3 JxIxJxIxJxIxJ.$$

Term 29 in the table is represented by h^4 in column 29 against IJIJIJ and $-h^3$ in column 29 against JIJIJIJ.

The table may be read by noting that the column is the term number and the coefficients in that column must be multiplied onto the Kronecker product of the letters (in the same order) on the right hand side of the table.

The proof is then completed by looking across the table and noting that all the coefficients vanish except the first and last so

$$BB^T = h^7 IxIxIxIxIxIxI - JxJxJxJxJxJxJ.$$

The comment on the proof of corollary 4.17 appears after the table for the proof of theorem 4.16.

Term Number

1 2-3 4 5 6 7 8 9-10 11 12 13-14 15 16-19 20 21 22 23-28 29

1	2-3	4	5	6	7	8	9-10	11	12	13-14	15	16-19	20	21	22	23-28	29
h^7																	IIIIIIII
$-h^6$		h^6															IIIIIIJ
$-h^6$			h^6														IIIIIIJ
h^6			$-h^5$														IIIIIIJ
$-h^6$				h^6													IIIIIIJ
h^5		$-h^5$		$-h^5$									h^5				IIIIIIJ
h^5				$-h^5$													IIIIIIJ
$-h^4$				h^4													IIIIIIJ
$-h^6$					h^6												IIIIIIJ
h^5		$-h^5$			$-h^5$			h^5									IIIIIIJ
h^5			$-h^5$		$-h^5$												IIIIIIJ
$-h^4$																	IIIIIIJ
$-h^6$																	IIIIIIJ
h^5		$-h^5$			$-h^5$												IIIIIIJ
h^5			h^4		h^4												IIIIIIJ
$-h^4$					$-h^5$												IIIIIIJ
$-h^4$					h^4			$-h^4$									IIIIIIJ
$-h^4$					h^4												IIIIIIJ
h^3					$-h^3$												IIIIIIJ
$-h^6$						h^6											IIIIIIJ
h^5		$-h^5$			$-h^5$						h^5						IIIIIIJ
h^5			$-h^5$		$-h^5$												IIIIIIJ
$-h^4$			h^4		h^4												IIIIIIJ
h^5					$-h^5$												IIIIIIJ
h^5						h^4											IIIIIIJ
$-h^4$					h^4			$-h^4$									IIIIIIJ
$-h^4$					h^4												IIIIIIJ
h^3					$-h^3$												IIIIIIJ
$-h^6$						h^6											IIIIIIJ
h^5		$-h^5$			$-h^5$						h^5						IIIIIIJ
h^5			$-h^5$		$-h^5$												IIIIIIJ
$-h^4$			h^4		h^4												IIIIIIJ
h^5				$-h^5$		$-h^5$											IIIIIIJ
$-h^4$				h^4		h^4											IIIIIIJ
$-h^4$				h^4		h^4											IIIIIIJ
h^3				$-h^3$		$-h^3$											IIIIIIJ

C o e f f i c i e n t s

[illegible]

[illegible]

		Term Number																	Formula				
		1	3	4	5	6	7	8	10	11	12	14	15	17	19	20	21	22	24	26	28	29	
		h^5	$-h^5$				$-h^5$					h^5											$JIIJIII$
		$-h^4$		h^4			h^4		$-h^4$														$JIIJIIJ$
		$-h^4$	h^4	h^4	h^4		h^4				$-h^4$	$-h^4$		$-h^4$	$-h^4$	$-h^4$				h^4		$JIIJIIJ$	
		h^3			$-h^3$		$-h^3$										h^3						$JIIJIIJ$
		$-h^4$	h^4				h^4				$-h^4$												$JIIJIII$
		h^3		$-h^3$			$-h^3$		h^3														$JIIJIIJ$
		h^3	$-h^3$				$-h^3$					h^3											$JIIJJI$
		$-h^2$					h^2																$JIIJJJJ$
C		h^5	$-h^5$				$-h^5$							h^5									$JIIJIII$
e		$-h^4$		h^4			h^4					$-h^4$											$JIIJIIJ$
f		$-h^4$	h^4		h^4		h^4				$-h^4$		$-h^4$	$-h^4$	$-h^4$					h^4		$JIIJIIJ$	
f		$-h^4$	h^4		h^4		h^4				$-h^4$												$JIIJIIJ$
i		h^3			$-h^3$		$-h^3$				h^3												$JIIJIIJ$
c		$-h^4$	h^4			h^4		$-h^4$						$-h^4$									$JIIJIIJ$
i		$-h^4$	h^4			h^4		h^4	$-h^4$					$-h^4$									$JIIJIIJ$
e		h^3		$-h^3$		$-h^3$		$-h^3$			h^3												$JIIJIIJ$
n		h^3		$-h^3$		$-h^3$		$-h^3$			h^3		h^3	h^3	h^3	h^3						$JIIJIIJ$	
t		h^3	$-h^3$			$-h^3$		$-h^3$	h^3				h^3	h^3	h^3	h^3						$JIIJIIJ$	
s		$-h^2$				h^2		h^2										$-h^2$					$JIIJIIJ$
		$-h^4$	h^4					h^4						$-h^4$									$JIIJIII$
		h^3		$-h^3$			$-h^3$						h^3										$JIIJIIJ$
		h^3	$-h^3$		$-h^3$		$-h^3$				h^3			h^3	h^3	h^3				$-h^3$		$JIIJIIJ$	
		$-h^2$				h^2		h^2			$-h^2$												$JIIJIIJ$
		h^3	$-h^3$					h^2			$-h^2$			h^3	h^3	h^3						$JIIJIIJ$	
		h^3	$-h^3$		h^2			h^2						h^3	h^3	h^3						$JIIJIIJ$	
		$-h^2$						h^2					$-h^2$										$JIIJIIJ$
		$-h^2$	h^2					h^2						$-h^2$									$JIIJIIJ$
		h						$-h$															$JIIJJJJ$

	Term Number														Formula
1	2	3	4	5	6	7	10	11	14	19	20	21	28		
h^5	$-h^4$	$-h^5$	h^4											JJIIIIII	
$-h^4$	h^4	h^4	h^4	h^4										JJIIIIII	
$-h^3$	h^3	h^3	h^3	$-h^3$										JJIIIIII	
$-h^4$	h^4	h^4	h^4	h^4	h^4									JJIIIIII	
h^3	h^3	$-h^3$	$-h^3$	$-h^3$	$-h^3$	h^4	$-h^4$							JJIIIIII	
h^3	$-h^3$	h^3	h^3	h^3	$-h^3$	h^3	h^3				h^3			JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^3	h^3						JJIIIIII	
$-h^4$	h^4	h^4	h^4	h^4	h^4	h^4	h^4	h^3	$-h^4$					JJIIIIII	
h^3	h^3	$-h^3$	$-h^3$	$-h^3$	$-h^3$	$-h^3$	h^3	h^3	h^3	h^3				JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	$-h^2$	$-h^2$			h^3	$-h^3$	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3				JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2			JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	JJIIIIII	
$-h^2$	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	h^2	JJIIIIII	
h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	h^3	$h^$						

To prove corollary 4.17 we must show that if

$$C = \sum' I \times J \times W \times I \times J \times [W \times W + I \times J]$$

and

$$D = \sum' J \times W \times I \times J \times [W \times I \times W + J \times I \times I]$$

then

$$CC^T = DD^T.$$

For C we use the numbering of theorem 4.16 and let the number after D in the expression below be the term number of D. Then

$$\begin{aligned} D = & J \times W \times I \times J \times W \times I \times W \quad {}^{30} & + & J \times W \times I \times J \times J \times I \times I \quad {}^{37} \\ & + W \times I \times J \times W \times I \times W \times J \quad {}^{31} & + & W \times I \times J \times J \times I \times I \times J \quad {}^{38} \\ & + I \times J \times W \times I \times W \times J \times W \quad {}^{32} & + & I \times J \times J \times I \times I \times J \times W \quad {}^{39} \\ & + J \times W \times I \times W \times J \times W \times I \quad {}^{33} & + & J \times J \times I \times I \times J \times W \times I \quad {}^{40} \\ & + W \times I \times W \times J \times W \times I \times J \quad {}^{34} & + & J \times I \times I \times J \times W \times I \times J \quad {}^{41} \\ & + I \times W \times J \times W \times I \times J \times W \quad {}^{35} & + & I \times I \times J \times W \times I \times J \times J \quad {}^{42} \\ & + W \times J \times W \times I \times J \times W \times I \quad {}^{36} & + & I \times J \times W \times I \times J \times J \times I \quad {}^{43} \end{aligned}$$

and DD^T can be read from the table as before. Then if we compare columns 9 to 15 inclusive and 23 to 29 inclusive of the previous table with the next table we see that

$$CC^T = DD^T$$

and so we have verified corollary 4.17.

[illegible]

APPENDIX D : A TABLE OF n-TYPE MATRICES OF ORDER $< 4,000$

The first page of this appendix uses the following notation :

'NI, NII' - indicates that an n-type matrix is known and it belongs to the class NI or NII respectively.

See §2.8.

'non' - theorem 2.9 shows that an n-type matrix cannot exist for this order.

blank - an n-type matrix is not known but this order is not excluded by theorem 2.9.

As in appendix A the numbers on the left of the page are the last two digits of the order and the top of the column gives the first two digits.

On the second page of this appendix we have listed the orders between 1,000 and 4,000 for which n-type matrices are known. An asterisk after a number indicates it is from class NII otherwise all orders belong to class NI.

last two digits	first two digits									
	00	100	200	300	400	500	600	700	800	900
2	NI	NI	non	non	NI	non	NI	NI		
6	NI	non		<i>complex</i>				non	non	
10	NI	NI	non	non	NI	NI	non	NI	NI	
14	NI	NI	non	NI	non	non	NI	non	non	non
18	NI		non	NI	non	non	NI	non	non	non
22	non	NI		non	NI	NI	non	non	NI	non
26	NI	NI	NI			non	NI		non	
30	NI	non	NI	non	non	NI		NI	NI	NI
34	non	non	NI		NI		non	NI		non
38	NI	NI	non	NI	non	non		non	non	NI
42	NI	non	NI	non		NI	NI	non	NI	NI
46				non			non			non
50	NI	NI	non	NI	NI		<i>complex</i> non	non	non	
54	NI		non	NI	non	non	NI	non	NI	NI
58	non	NI	NI	non	NI	NI		NI	NI	non
62	NI	non		NI	NI	non	NI	NI	non	NI
66		non			non		non			
70	non	NI	NI		non	NI	non	NI	<i>complex</i> non	non
74	NI	NI	non	NI	non	non	NI	NI		non
78	non	non	NI		non	NI	NI	non	NI	NI
82	NI	NI	NI	non		non	non	non	NI	
86			non	non					non	
90	NI	non	NI	NI	non	non		non	non	non
94	non	NI	NI	non		NI	non		non	non
98	NI	NI	non	NI	non	non		NI	non	NI

1010	1482	1994	2478	3038	3594
1014	1490	1998	2522	3042	3614
1022	1494	2018	2550	3050	3618
1034	1522*	2030	2558	3062	3638
1050	1550	2054	2594	3090	3674
1062	1554	2070	2602*	3110	3678
1070	1598	2082	2610	3122	3698
1094	1602	2090	2618	3138 3126	3702
1098	1610	2114	2622	3170	3710
1110	1614	2130	2634	3182	3722
1118	1622	2138	2658	3210	3734
1130	1638	2142	2678	3218	3762
1154	1658	2154	2690	3222	3770
1182	1670	2162	2694	3230	3794
1194	1682	2214 2198 2210	2714	3254	3798
1202	1694	2222	2730	3258	3822
1214	1698	2238	2742	3302	3834
1218	1710	2270	2750	3314	3854
1226*	1722	2274	2778	3330	3878
1230	1734	2282	2790	3362	3882
1238	1742	2294	2798	3374	3890
1250	1754	2298	2802	3390	3918
1278	1778	2310	2810	3414	3930
1290	1790	2334	2834	3434	3970*
1298	1802	2342	2838	3450	3990
1302	1850	2358	2858	3458	
1322	1862	2378	2862	3462	
1362	1874	2382	2898	3470	
1370	1878	2390	2910	3482	
1374	1890	2394	2918	3518	
1382	1902	2402	2954	3530	
1410	1914	2418	2958	3534	
1430	1934	2438	2970	3542	
1434	1950	2442	3002	3558	
1454	1974	2474	3026*	3582	

n-type matrices are known to exist for the above orders.

BIBLIOGRAPHY :

AHRENS, R. AND G. SZEKERES,

- [1] "On a Combinatorial Generalization of 27 Lines associated with a Cubic Surface," *J. Aust. Math. Soc.* ~~(to appear)~~ 10(1969), 485-492.

BAUMERT, L.D.,

- [1] "Hadamard Matrices of Orders 116 and 232," *Bull. Amer. Math. Soc.* 72 (1966), 237.

- [2] "Hadamard Matrices of the Williamson Type," *Math. of Comp.* 19 (1965), 442 - 447.

- [3] ^{Difference Sets,} ~~Cyclic Incidence Matrices,~~ ~~(to appear)~~ Springer-Verlag, Berlin-Heidelberg-New York, 1971.

BAUMERT, L.D., S.W. GOLOMB, AND MARSHALL HALL JR.,

- [1] "Discovery of an Hadamard Matrix of order 92," *Bull. Amer. Math. Soc.*, 68 (1962), 237 - 238.

BAUMERT L.D. AND MARSHALL HALL JR.,

- [1] "A New Construction for Hadamard Matrices," *Bull. Amer. Math. Soc.* 71 (1965), 169 - 170.

BELEVITCH, V.,

- [1] "Conference Networks and Hadamard Matrices," *Ann. Soc. Scientifique Brux. T.* 82 (1968) 13 - 32.

- [2] "Theory of 2n-terminal Networks with Applications to Conferency Telephony. *Electr. Commun.*, 27,3,(1950), 231-244.

BLATT, D. AND SZEKERES, G.,

- [1] "A skew Hadamard matrix of order 52", *Can. J. Math.* ~~(to appear)~~. 22 (1970), 1319 - 1322

BOSE, R.C.,

- [1] "On the Construction of Balanced Incomplete Block Designs," *Ann. of Eugenics*, 9 (1939) p 353 - 399.

BRAVER, A.,

- [1] "On a New Class of Hadamard Determinants," *Math. Z.* 58 (1953) 219 - 225.

BRIDGES, W.G. AND RYSER, H.J.,

- [1] "Combinatorial Designs and Related Systems," *J. of Algebra* ~~(to appear)~~ 13 (1969), 432-446.

CLATWORTHY, W.H.,

- [1] "The subclass of Balanced Incomplete Block Designs with $r = 11$ Replications," *Review of the Int. Stat. Inst.*, 36 (1968) 7 - 11.

EHLICH, H.,

- [1] "Neue Hadamard - Matrizen," *Arch. Math.*, 16 (1965), 34 - 36.

FISHER, R.A., AND F. YATES,

- [1] *Statistical Tables for Biological, Agricultural, and Medical Research*, 2nd ed. London : Oliver and Boyd Ltd., 1943.

GOETHALS, J.M. AND J.J. SEIDEL,

- [1] "Orthogonal Matrices with Zero Diagonal," *Can. J. Math.* 19 (1967), 1001 - 1010.
[2] "A skew - Hadamard matrix of order 36, *J. Aust. Math. Soc.* ~~(to appear)~~. 11 (1970) 343 - 344.
[3] "Strongly Regular Graphs derived from Combinatorial Designs," *Can. J. Math.* ~~(to appear)~~. 22 (1970), 597 - 614.

GOLDBERG, K.,

- [1] "Hadamard matrices of order cube plus one," *Proc. Amer. Math. Soc.* 17, ⁽¹⁹⁶⁶⁾ ~~(3)~~ 744 - 746.

GRIFFIN, HARRIET,

- [1] *Elementary Theory of Numbers*, McGraw-Hill, New York, 1954.

HALL, MARSHALL JR.,

- [1] *Combinatorial Theory*, Blaisdell, Waltham, Mass, 1967.
- [2] "Designs with Transitive Automorphism Groups," (to appear).
- [3] "Hadamard Matrices of Order 20," *J.P.L. Technical Report* No. 32 - 761.
- [4] "A Survey of Difference Sets," *Proc. Amer. Math. Soc.*, 7 (1956), 975 - 986.

HALL, MARSHALL, JR., RICHARD LANE AND DAVID WALES,

- [1] "Designs Derived from Permutation Groups," (to appear).

HALL, MARSHALL, JR., AND H.J. RYSER,

- [1] "Normal Completions of Incidence Matrices," *Amer. J. Math.* 76 (1954) 581 - 589.
- [2] "Cyclic Incidence Matrices," *Can. J. Math.*, 3 (1951), 495-502.

HARDY, G.H. AND E.M. WRIGHT,

- [1] *An Introduction to the Theory of Numbers*. Oxford : Clarendon Press, 1938.

JOHNSON, E.C.,

- [1] "Integral solutions to the Incidence Equation for finite projective plane cases of orders $n \equiv 2 \pmod{4}$," *Pacific J. of Math.* 17 (1) 1966, 97 - 120.
- [2] "The Inverse Multiplier for Abelian Group Difference Sets," *Can. J. Math.* 16 (1964) 787 - 796.

LEHMER, D.H.,

- [1] *List of Prime Numbers from 1 to 10,006,721*, Hafner, New York, 1956.

MACDUFFEE, C.C.,

- [1] *The Theory of Matrices*, Reprint of First Ed., Chelsea, N.Y. 1964.

MAJINDAR, K.N.,

- [1] "On Integer Matrices and Incidence Matrices of Certain Combinatorial Configurations, I : Square Matrices," *Can. J. Math.* 18 (1966), 1 - 5.

MARCUS, M. AND H. MINC,

- [1] *A Survey of Matrix Theory and Matrix Inequalities*, Allyn and Bacon, Boston, 1964.

MENON, P. KESAVA,

- [1] "Difference Sets in Abelian Groups," *Proc. Amer. Math. Soc.* 11 (1960), 368 - 376.

PALEY, R.E.A.C.,

- [1] "On Orthogonal Matrices," *J. Math. Phys.* 12 (1933), 311 - 320.

RAO, C. RADHASKRISHNA,

- [1] "A Study of B I B Designs with Replications 11 to 15," *Sankhyā*, 23 (1961), 117 - 127.

RAGHAVARAO, D.,

- [1] "Some Aspects of Weighing Designs," *Ann. Math. Stat.* 31 (1960), 878 - 884.

RYSER, H.J.,

- [1] *Combinatorial Mathematics*, (Carus Monograph No. 14), Wiley, New York, 1963.
- [2] "A Note on a Combinatorial Problem," *Proc. Amer. Math. Soc.* 1 (1950), 422 - 424.
- [3] "Matrices with Integer Elements in Combinatorial Investigations," *Amer. J. Math.* 74 (1952), 769 - 773.
- [4] "An Extension of a Theorem of de Bruijn and Erdős on Combinatorial Designs," *J. of Algebra*, 10 (1968) 246 - 261.

SCARPIS, V.,

- [1] "Sui determinanti di valore massimo," *Rend. R. Inst. Lombardo Sci. e Lett.*, (2) 31 (1898), 1441 - 1446.

SHRIKHANE, S.S., D. RAGHAVARAO, AND S.K. THARTHARE,

- [1] "Non-existence of Some Partially Balanced Incomplete Block Designs," *Can. J. Math.*, 15 (1963), 686 - 701.

SHRIKHANDE, S.S. AND N.K. SINGH,

- [1] "On a Method of Constructing Symmetrical Balanced Incomplete Block Designs. *Sankhyā* Ser. A, 24 (1962), p25 - 32.

SMITH, H.J.S.,

- [1] "-----," *Proc. London Math. Soc.* 4 (1873) 236 - 253.

SPENCE, E.,

- [1] "A New Class of Hadamard Matrices," *Glasgow J.* (1967) 59 - 62.

SYLVESTER, J.J.

- [1] "Thoughts on Inverse Orthogonal Matrices, Simultaneous Sign-successions, and Tessellated Pavements in two or more Colours, with Applications to Newton's Rule, Ornamental Tile-work, and the Theory of Numbers." *Phil. Mag.* (4) 34, (1867) 461 - 475.

SZEKERES, G.,

- [1] "Tournaments and Hadamard matrices," ~~*Enseignement Math.*~~ *Enseignement Math.* 15 (1969) 269-278.

TAKEUCHI, K.,

- [1] "A Table of Difference Sets generating Balanced Incomplete Block Designs," *Review of Int. Stat. Inst.*, 30 (1962) 361 - 366.
[2] "On the Construction of a Series of B I B Designs," *Rep. Stat. Appl. Res. JUSE*, 10 (3) (1963), 48.

TURYN, R.J.,

- [1] "Character Sums and Difference Sets," Pacific J. of Math. 15 (1), (1965), 319 - 346.
- [2] "An Infinite Class of Williamson Matrices," (to appear).

J.H. VAN LINT AND J.J. SEIDEL,

- [1] "Equilateral Point Sets in Elliptic Geometry," Proceedings, Series A, 69 (3) and Indag. Math., 28, (3), (1966), 335 - 348.

VINOGRADOV, I.M.,

- [1] Elements of Number Theory, reprinted by Dover, New York, 1954.

[11] *Amicable Hadamard matrices* J. Comb Th 11 (1971) 296-298

WALLIS, JENNIFER,

- [1] "Hadamard Matrices," M.Sc. Thesis, La Trobe University, 1969.
- [2] "A Note of a Class of Hadamard Matrices," J. Combinatorial Theory, 6 (1969), 222 - 223.
- [3] " (v, k, λ) - configurations and Hadamard Matrices," J. Austral. Math. Soc. (to appear). 11 (1970) 297-309. ser B, 10 (1971), 1-11.
- [4] "Some $(1, -1)$ - matrices," J. Combinatorial Theory, (to appear).
- [5] "On Integer Matrices obeying Certain Matrix Equations," J. Combinatorial Theory (to appear). 12 (1972), 112-118. (1971) 378-384
- [6] "Some Results on Configurations," J. Austral. Math. Soc. (to appear).
- [7] "A Class of Hadamard Matrices," J. Combinatorial Theory 6, (1969), 40 - 44.
- [8] "Two New Block Designs," J. Combinatorial Theory (to appear). 7 (1969) 369-370
- [9] "Hadamard Designs," Bull. Austral. Math. Soc. (to appear). 2 (1970) 5-54
- [10] "Integer Matrices obeying generalized incidence equations" Bull Austral M.S. 4 (1971) 51-56.

WALLIS, W.D. AND JENNIFER WALLIS,

- [1] "Equivalence of Hadamard Matrices," Israel J. of Math. 7, (1969), 122 - 128.

WALLIS, W.D.,

- [1] "Certain Graphs arising from Hadamard Matrices," Bull. Aust. Math. Soc. (to appear).

WHITEMAN, A.L.,

- [1] "A Family of Difference Sets," *Illinois J. Math.*, 6
(1962), 107 - 121.

WILLIAMSON, J.,

- [1] "Hadamard's determinant theorem and the sum of four squares,"
Duke. Math. J. 11 (1944) 65 - 81.
[2] "Note on Hadamard's determinant theorem," *Bull. Amer. Math.*
Soc. 53 (1947) 608 - 613.