University of Wollongong
Research Online

Faculty of Informatics - Papers (Archive)

Faculty of Engineering and Information Sciences

1970

(v, k, lambda)-configurations and Hadamard matrices

Jennifer Seberry
University of Wollongong, jennifer_seberry@uow.edu.au

Publication Details

Jennifer Seberry Wallis, (v, k, lambda) configurations and Hadamard matrices, Journal of the Australian Mathematical Society, 11, (1970), 297-309.

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

(v, k, lambda)-configurations and Hadamard matrices

Abstract
(v, k, lambda) Configirations and Hadamard matrics

Disciplines
Physical Sciences and Mathematics

Publication Details
Jennifer Seberry Wallis, (v, k, lambda) configurations and Hadamard matrices, Journal of the Australian Mathematical Society, 11, (1970), 297-309.

This journal article is available at Research Online: http://ro.uow.edu.au/infopapers/933

(v, k, λ) CONFIGURATIONS AND HADAMARD MATRICES

BY

JENNIFER WALLIS

Reprinted from

THE JOURNAL OF THE AUSTRALIAN
MATHEMATICAL SOCIETY

Volume XI – Part 3 – p.p. 297–309
1970

(v, k, λ) CONFIGURATIONS AND HADAMARD MATRICES

JENNIFER WALLIS

(Received 28 October 1968; revised 14 January 1969)

Communicated by G. B. Preston

1. Introduction

Using the terminology in **2** (where the expression m-type is also explained) we will prove the following theorems:

THEOREM 1. *If there exist*

(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*

(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) $XX^T = aI_x + bJ_x$

$$YY^T = \left\{\frac{m+mx-mh-a}{m-1}\right\} I_x + \left\{\frac{mh-m-b}{m-1}\right\} J_x$$

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

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 mxh.

THEOREM 2. *If all the conditions of theorem* 1 *are satisfied and in addition* X *is skew-type and* Y *and* Z *are symmetric then* H *is skew-Hadamard.*

We will show theorem 2 demonstrates the existence of previously unknown skew-Hadamard matrices of orders 552 and 3304.

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

Theorem 3 is due to Williamson [8; p. 67] we include a proof because we use the matrices of the proof elsewhere.

THEOREM 4. *If there exist*

(i) *a skew-Hadamard matrix of order* h,

(ii) *four matrices* X, Y, Z, W *of order* $p \equiv 1$ (*mod* 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.

THEOREM 5. *If* $h \equiv 0$ (*mod* 4) *is the order of a skew-Hadamard matrix and* $2h+3$ *is a prime then there is an Hadamard matrix of order* $2h(h+1)$.

2. Preliminaries

An *Hadamard matrix* H is a matrix of order n, all of whose elements are $+1$ and -1 and which satisfies $HH^T = nI_n$. It is conjectured that an Hadamard matrix exists for $n = 2$ and for $n = 4t$, where t is any positive integer. Many classes of Hadamard matrices are known; most of these can be found by reference to [3], [6] and [7]. Hadamard matrices are known for all orders less than 188.

An Hadamard matrix $H = U+I$ is called a *skew-Hadamard* if $U^T = -U$. It is conjectured that whenever there exists an Hadamard matrix of order n there exists a skew-Hadamard matrix of the same order. As the existence of certain skew-Hadamard matrices is essential for my results I list the order for which skew-Hadamard matrices are known to exist.

I	$2^t \Pi k_i$	t, r_i all positive integers, $k_i = p_i^{r_i}+1 \equiv 0 \pmod 4$, p_i a prime; from [9],
II	$(p-1)^3+1$	p the order of a skew-Hadamard matrix; from [2],
III	$2^t(q+1)$	$t \geqq 1$ an integer, q (prime power) $\equiv 5 \pmod 8$; from [5],
IV	52	from [1],
V	36	unpublished result of J. M. Goethals
VI	$p^r(p^r+1)(m-1)$	m of type I, p^r(prime power) $\equiv 3 \pmod 4$, and $(m-1)(p^r+1)/m$ the order of a skew-Hadamard matrix; proved in corollary 9,
VII	$p^r(p^r-3)(m-1)$	m of type I, p^r (prime power) $\equiv 3 \pmod 4$ and $(m-1)(p^r-3)/m$ the order of a skew-Hadamard matrix; proved in corollary 9,
VIII	$h(p^r+1)$	h the order of a skew-Hadamard matrix, p^r (prime power) $\equiv 3 \pmod 4$, from [8],
IX	$2h$	h the order of a skew-Hadamard matrix.

The orders less than 1004 for which skew-Hadamard matrices are not yet known are:

92, 100, 116, 148, 156, 172, 184, 188, 196, 232, 236, 260, 268, 276, 292, 296, 324, 340, 356, 372, 376, 388, 392, 404, 412, 428, 436, 452, 472, 476, 484, 508, 516, 520, 532, 536, 580, 584, 592, 596, 604, 612, 628, 652, 668, 676, 680, 708, 712, 716, 724, 732, 756, 764, 772, 776, 784, 804, 808, 820, 836, 852, 856, 868, 872, 876, 892, 900, 904, 908, 916, 932, 940, 944, 952, 956, 964, 980, 988, and 996.

We study skew-Hadamard matrices because the construction of [2], [4], [6], [7], [9] and this paper depend heavily on the existence of these special matrices. Also theorem 14.1.3 of [3], quite powerful theorem depends on skew-Hadamard matrices.

A *skew-type matrix* $A = U+I$ has $U^T = -U$.

A (v, k, λ)-*configuration* is an arrangement of v elements $x_1, x_2, \cdots x_v$ into v sets $S_1, S_2, \cdots, S_v$ such that every set contains exactly λ elements in common. A (v, k, λ)-configuration can be characterized by its *incidence matrix* $A = (a_{ij})$ defined by $a_{ij} = 1$ if $x_j \in S_i$ and $a_{ij} = -1$ if $x_j \notin S_i$. This matrix A, of order v, consists entirely of 1's and -1's, and it can be seen that A satisfies the *incidence equation.*

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

where I is the identity matrix of order v and J is the matrix of order v with every element $+1$.

A set of elements $D = \{x_1, x_2, \cdots, x_k\}$ will be said to generate a *circulant* $(1, -1)$ matrix $A = (a_{ij})$ if $a_{ij} = a_{1, j-i+1} = 1$ when $j-1+1 \in D$ (all numbers modulo v) and -1 otherwise. A *back-circulant* matrix $A = (a_{ij})$ of order v has $a_{1i} = a_{1+j, i-j}$ where $1+j$ and $i-j$ are reduced to modulo v.

LEMMA 6. (i) *If there exists a circulant A of order v then there also exists a back circulant B of the same order.* (ii) *If A is circulant B back circulant, both of order v, then* AB^T *is symmetric.*

PROOF. (i) trivial, (ii) this is Theorem 1 of [6] restated.

Table 1 gives those known (v, k, λ) configurations, together with their incidence equations, which have a circulant, (hence back circulant) incidence matrix. All are derived from difference sets, and we use the notation of Marshall Hall [3; p. 141–2] to indicate the type of the difference set.

In the table p is a prime and p^r a prime power.

Table 2 gives those configurations from Marshall Hall [3; 291–8] which are not already covered by Table 1 and in which v is an odd prime power. Each entry in Table 2 satisfies the conditions for (v, k, λ) configurations, namely that

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

and that

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

TABLE 1

Type of Difference Set	(v, k, λ)-configuration generating A	Incidence Equation AA^T	Comment
	$(v, v, v) = J$	vJ	
	$(v, v-1, v-2) = J-2I$	$4I+(v-4)J$	
S type	$\left(\frac{q^{n+1}-1}{q-1}, \frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}\right)$	$4q^{n-1}I+\left(\frac{q^{n+1}-1}{q-1}-4q^{n-1}\right)J$	$q = p^r$
Q type	$(4t-1, 2t-1, t-1)$	$4tI-J$	$4t = p+1$
T type	$\left(pq, \frac{pq-1}{2}, \frac{pq-3}{4}\right)$	$(pq+1)I-J$	$p = q+2$, p, q prime
B type	$\left(4x^2+1, x^2, \frac{x^2-1}{4}\right)$	$(3x^2+1)I+x^2J$	$p = 4x^2+1$; x odd
B_0 type	$\left(4x^2+9, x^2+3, \frac{x^2+3}{4}\right)$	$(3x^2+9)I+x^2J$	$p = 4x^2+9$; x odd
0 type	$(64b^2+9, 8b^2+1, b^2)$	$4(7b^2+1)I+(36b^2+5)$	$p = 8a^2+1 = 64b^2+9$; a, b odd
0_0 type	$(64b^2+441, 8b^2+56, b^2+7)$	$4(7b^2+49)I+(36b^2+245)J$	$p = 8a^2+49 = 64b^2+441$; a odd, b even

should have a solution in the integers for x, y, z not all zero.

No case has yet been found where these two conditions are both satisfied and the corresponding configuration has not been found by a systematic search.

TABLE 2

(v, k, λ)-configuration	Incidence equation	Comment
(31, 10, 3)	$28I+3J$	Exists: but no circulant design exists
(71, 15, 3)	$48I+23J$	Solution Unknown
(79, 13, 2)	$44I+35J$	Exists: but no circulant design exists
(111, 11, 1)	$40I+71J$	Solution Unknown
(25, 9, 3)	$24I+J$	Exists: but no circulant design exists
(157, 13, 1)	$48I+109J$	Solution Unknown

We now define the matrices needed to prove theorem 3. With $q = p^r$ (prime power) $\equiv 3 \pmod 4$, let $a_0 = 0, a_1, \cdots, a_{q-1}$ be the elements of $GF(q)$ numbered so that $a_0 = 0$ and $a_{q-i} = -a_i$, $i = 1, \cdots, q-1$. Now put

$$S = (s_{ij}), \qquad s_{ij} = \chi(a_i - a_j),$$

where $\chi(x)$ is the character defined on $GF(q)$ by $\chi(0) = 0$, $\chi(x) = +1$ if x is a square and $\chi(x) = -1$ if x is not a square.

Here

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

and since -1 is a non-square if $q \equiv 3 \pmod 4$, $S^T = -S$. By the properties of χ it may be shown $SS^T = qI_q - J_q$.

Let $R = (r_{ij})$ $i, j = 0, \cdots, q-1$ be the matrix of order $q = p^r$ defined by

$$\begin{aligned} r_{00} &= 1 \\ r_{i,q-i} &= 1 \qquad i = 1, \cdots, q-1, \\ r_{ij} &= 0 \qquad \text{otherwise.} \end{aligned}$$

Then $R^T = R$, and if we write $RS = (c_{ij})$, then $c_{0j} = \chi(0 - a_j)$ and

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

whence in all cases $c_{ij} = \chi(-a_i - a_j)$ and so RS is symmetric.

Using $S^T = -S$, $SS^T = qI - J$, $RJ = J$, and $(RS)^T = RS$ we have $S(R+RS)^T = (R+RS)S^T$.

Choose

$$P = S+I \text{ and } D = R+RS$$

then $PD^T = DP^T$. Then if

$$(1) \qquad M = \begin{bmatrix} 1 & 1 \cdots 1 \\ -1 & \\ \vdots & P \\ -1 & \end{bmatrix} \quad \text{and} \quad N = \begin{bmatrix} 1 & 1 \cdots 1 \\ 1 & \\ \vdots & D \\ 1 & \end{bmatrix}$$

$MN^T = NM^T$. M and N are of order p^r+1 and $MM^T = NN^T = (p^r+1)I_{p^r+1}$.

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

$$K = I\times M+U\times N = I_h\times I_h+I_h\times V+U\times N.$$

It can be shown that K is a skew-Hadamard matrix of order $h(p^r+1)$.

Definition. 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 7. *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 8. *If $m = 2^t\prod(p_i^{r_i}+1)$ where t is a non-negative integer and $p_i^{r_i}$ (prime power) $\equiv 3$ (mod 4) then there are m-type matrices of order m.*

Proof. (i) $\quad M_2 = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ and $N_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

are two suitable matrices of order 2.

(ii) M and N as defined in (1) 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 m-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

$$\begin{aligned} M_{mn} N_{mn}^T &= (I_m \times M_n + W_m \times N_n)(N_m^T \times N_n^T) \\ &= N_m^T \times M_n N_n^T + W_m N_m^T \times N_n N_n^T \\ &= N_m \times N_n M_n^T + N_m W_m^T \times N_n N_n^T \qquad \text{using lemma 7} \\ &= (N_m \times N_n)(I_m \times M_n^T + W_m^T \times N_n^T) \\ &= N_{mn}^T M_{mn}^T \end{aligned}$$

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 $m > 1$. But the case $m = 1$ is trivial.

3. A construction with $v \equiv 3 \pmod 4$

Proof of theorem 1. 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 $N^T = N$ and lemma 7 shows $WN^T = NW^T$.

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

which completes the proof.

Proof of theorem 2. The Hadamard property has been proved above. To prove skew-type property let $X = R+I$ where $R^T = -R$ then

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

and

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

Which completes the proof.

We now investigate when the conditions of theorem 2 are satisfied.

COROLLARY 9. *Let p^r and $q_i^{s_i}$ be prime powers $\equiv 3$ (mod 4), t be positive integer and $m = 2^t \Pi(q_i^{s_i}+1)$ then if there is a skew-Hadamard matrix of order*

$$\text{(i)}\ \frac{(m-1)(p^r+1)}{m} \qquad \text{(ii)}\ \frac{(m-1)(p^r-3)}{m}$$

then there is a skew-Hadamard matrix of order

$$\text{(i)}\ p^r(p^r+1)(m-1), \qquad \text{(ii)}\ p^r(p^r-3)(m-1)$$

respectively.

PROOF. m as given is, from lemma 8, the order of m-type matrices. Then if P and D are as defined in (1), the proof follows with

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

in theorem 2.

With $m = 2$, $p^r = 23$ and (i) of corollary 9 we find a skew-Hadamard matrix of order 552, and with $m = 2$, $p^r = 59$ and (ii) of corollary 9 we obtain a skew-Hadamard matrix of order 3304; neither of these two matrices were previously known.

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

$$H = \begin{bmatrix} 1 & 1 \cdots 1 \\ 1 & \\ \vdots & F \\ 1 & \end{bmatrix} \tag{2}$$

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

$$E = FG \tag{3}$$

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

Then using theorem 1 we have

COROLLARY 10. *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.*

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

then there is an Hadamard matrix of order

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

PROOF. The proof follows from theorem 1 with F and E as in (2) and (3)

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) $X = K$, $Y = F$, $Z = E$ and $m = 1$.

(iii) and (iv) were given in [6].

COROLLARY 11. *If there is a skew-Hadamard matrix of order*

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

where m is the order of m-type matrices, q, y and $y+2$ are odd primes, $x = q^n+q^{n-1}+\cdots+q+1 \equiv 3$ (mod 4), and $x = y(y+2)$ then there is an Hadamard matrix of order

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

respectively.

PROOF. If P is the circulant matrix generated by an $(x, \frac{1}{2}(x+1), \frac{1}{4}(x+1))$ configuration and Q is back circulant (from table 1) then the proof follows with (i) $X = Q$, $Y = K$, $Z = P$, (ii) $X = K$, $Y = Q$, $Z = P$ in theorem 1.

With $m = 1$ and $n = 2$ we obtain corollary 5 of [6] from (ii).

The existence of a circulant incidence matrix for any of the entries with $v \equiv 3$ (mod 4) in Table 2 will give Hadamard matrices. If a circulant $(71, 15, 3)$ configuration exists then there is an Hadamard matrix of order 1704. This would be a new order.

4. A construction with $v \equiv 1$ (mod 4)

In this section $q = p^r$ (prime power) $\equiv 1$ (mod 4). Let $a_0 = 0, a_1, \cdots, a_{q-1}$ be the elements of $GF(q)$ numbered so that $a_0 = 0$ and $a_{q-i} = a_i$, $i = 1, \cdots, q-1$. Now define $F = (f_{ij})$ by

$$f_{ij} = \begin{cases} 0 & i = j \\ \chi(a_i - a_j) & i \neq j \end{cases} \tag{4}$$

Then by the properties of χ and $GF(q)$, F is a symmetric matrix satisfying

$$FF^T = p^r I - J.$$

Write p for p^r and define X and Y by

$$\begin{aligned} X &= F + I_p \\ Y &= F - I_p. \end{aligned} \tag{5}$$

Then $XY^T = (F+I_p)(F^T-I_p) = FF^T - I_p = (F-I_p)(F^T+I_p) = YX^T$ and

$$XX^T = YY^T = (FF^T+2F+I_p)+(FF^T-2F+I_p) = 2(p+1)I_p - 2J_p.$$

PROOF OF THEOREM 4. If $m = 2$ use

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

for $m = 4$ use

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

Then since ZW^T and XY^T are symmetric

$$MN^T = NM^T$$

and

$$\begin{aligned} MM^T &= \{m(p+1-h)I_p + m(h-1)J_p\} \times I_m \\ NN^T &= \{m(p+1)I_p - mJ_p\} \times I_m. \end{aligned}$$

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

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

is the required Hadamard matrix of order mph since

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

Which completes the proof.

PROOF OF THEOREM 5. Szekeres' construction for primes $\equiv 3 \pmod 4$, see [5], 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 gives the result.

We now investigate when the conditions of theorem 4 are satisfied. We note that for p prime X and Y defined by (5) are circulant symmetric matrices.

COROLLARY 12. *Let p^r be a prime power $\equiv 1$ (mod 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) $p+1-\dfrac{4q^{n-1}}{m}$; *where* $p = q^n+q^{n-1}+\cdots+q+1$, *n a positive integer*;

(iii) $p+1-4q^{n-1}+\dfrac{4q^{n-1}}{m}$, *with p as in* (ii);

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

(v) $p-3-\dfrac{4(q^{n-1}-1)}{m}$, *with p as in* (ii);

(vi) $\dfrac{5x^2+3}{2}$, *where* $p = 4x^2+1$;

(vii) $\dfrac{13x^2-5}{4}$, *where* $p = 4x^2+1$;

(viii) $\dfrac{7x^2+1}{4}$, *where* $p = 4x^2+1$;

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

(x) $2(25b^2+3)$, *where* $p = 8a^2+1 = 64b^2+9$, *b odd*;

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

(xii) $57b^2+390$, *where p and b are as in* (x);

(xiii) $43b^2+294$, *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) $[m(p+1-4q^{n-1})+4q^{n-1}]p$;

(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) $4(25b^2+172)(64b^2+441)$;

(xii) $4(57b^2+390)(64b^2+441)$;

(xiii) $4(43b^2+294)(64b^2+441)$;

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:

(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) $m = 2,\ Z = 0,\ W = J-2I$;

(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 [7].

Although the entries in table 2 give Hadamard matrices they do not yield any new orders.

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

Note added in proof (January 31st, 1970): We wish to thank R. Turyn and L. D. Baumert for pointing out some errors in the original forms of Tables 1 and 2.

References

[1] D. Blatt and G. Szekeres, 'A skew Hadamard matrix of order 52', to appear in *Can. J. Math.*

[2] Karl Goldberg, 'Hadamard matrices of order cube plus one', *Proc. Amer. Math. Soc.* 17 (3) 744–746.

[3] Marshall Hall Jr., *Combinatorial Theory*, Blaisdell, Waltham, Mass., 1967.

[4] E. C. Johnsen, '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.
[5] G. Szekeres, 'Tournaments and Hadamard matrices', *L'Enseignment Math.* T. XV (1969), 269–278.
[6] Jennifer Wallis, 'A class of Hadamard matrices', *J. of Combinatorial Th.* 6 (1969), 40–44.
[7] Jennifer Wallis, 'A note of a class of Hadamard matrices', *J. of Combinatorial Th.* 6 (1969), 222–223.
[8] J. Williamson, 'Hadamard's determinant theorem and the sum of four squares', *Duke Math. J.* 11 (1944) 65–81.
[9] J. Williamson, 'Note on Hadamard's Determinant Theorem', *Bull. Amer. Math. Soc.* 53 (1947) 608–613.

Canberra College of Advanced Education
Box 381, P.O., Canberra City, A.C.T., 2601