Construction of Williamson type matrices

Jennifer Seberry

University of Wollongong, jennie@uow.edu.au

Follow this and additional works at: https://ro.uow.edu.au/infopapers

Part of the Physical Sciences and Mathematics Commons

Recommended Citation

https://ro.uow.edu.au/infopapers/966
Construction of Williamson type matrices

Abstract
Recent advances in the construction of Hadamard matrices have depended on the existence of Baumert-Hall arrays and four (1, -1) matrices A, B, C, D of order m which are of Williamson type, that is they pair-wise satisfy

i) $MN^T = NM^T$, $M, N \in \{A, B, C, D\}$ and

ii) $AA^T + BB^T + CC^T + DD^T = 4mI_m$.

It is shown that Williamson type matrices exist for the orders $m = s(4s - 1)$, $m = s(4s + 3)$ for $s \in \{1, 3, 5, \ldots, 25\}$ and also for $m = 93$. This gives Williamson matrices for several new orders including 33, 95, 189. These results mean there are Hadamard matrices of order

i) $4s(4s - 1)t, 20s(4s - 1)t, s \in \{1, 3, 5, \ldots, 25\}$;

ii) $4s(4s + 3)t, 20s(4s + 3)t, s \in \{1, 3, 5, \ldots, 25\}$;

iii) $4.93t, 20.93t$;

for $t \in \{1, 3, 5, \ldots, 61\} \cup \{1 + 2^a10^b26^c, a, b, c \text{ nonnegative integers}\}$, which are new infinite families.

Also, it is shown by considering eight-Williamson-type matrices, that there exist Hadamard matrices of order $4(p + 1)(2p + 1)r$ and $4(p + 1)(2p + 5)r$ when $p = 1 \pmod{4}$ is a prime power, $8r$ is the order of a Plotkin array, and, in the second case $2p + 6$ is the order of a symmetric Hadamard matrix. These classes are new.

Disciplines
Physical Sciences and Mathematics

Publication Details

This journal article is available at Research Online: https://ro.uow.edu.au/infopapers/966
Construction of Williamson Type Matrices

JENNIFER SEBERRY WALLIS

Institute of Advanced Studies, Australian National University, Canberra

(Received January 3, 1974)

Recent advances in the construction of Hadamard matrices have depended on the existence of Baumert-Hall arrays and four $(1, -1)$ matrices $A$, $B$, $C$, $D$ of order $m$ which are of Williamson type, that is they pair-wise satisfy

i) $M^T = N^T$, $M, N \in \{A, B, C, D\}$ and

ii) $A^T + B^T + C^T + D^T = 4mI_m$.

It is shown that Williamson type matrices exist for the orders $m = s(4s - 1)$, $m = s(4s + 3)$ for $s \in \{1, 3, 5, \ldots, 25\}$ and also for $m = 93$. This gives Williamson matrices for several new orders including 33, 95, 189.

These results mean there are Hadamard matrices of order

i) $4s(4s - 1)t$, $20s(4s - 1)t$, $s \in \{1, 3, 5, \ldots, 25\}$;

ii) $4s(4s + 3)t$, $20s(4s + 3)t$, $s \in \{1, 3, 5, \ldots, 25\}$;

iii) 4.93t, 20.93t;

for $t \in \{1, 3, 5, \ldots, 61\} \cup \{1 + 26a + 26b, a, b \text{ nonnegative integers} \}$, which are new infinite families.

Also, it is shown by considering eight-Williamson-type matrices, that there exist Hadamard matrices of order $4(p^2 - 1)(2p^2 + 1)r$ and $4(p^2 + 1)(2p^2 + 5)r$ when $p = 1 \pmod{4}$ is a prime power, $8r$ is the order of a Plotkin array, and, in the second case $2p + 6$ is the order of a symmetric Hadamard matrix. These classes are new.

1. INTRODUCTION

We wish to form four $(1, -1)$ matrices $A$, $B$, $C$, $D$ of order $m$ which pairwise satisfy

i) $M^T = N^T$, $M, N \in \{A, B, C, D\}$,

and ii) $A^T + B^T + C^T + D^T = 4mI_m$. (1)
Williamson first used such matrices and we call them *Williamson type*. The matrices Williamson originally used were both circulant and symmetric but neither the circulant nor symmetric properties are necessary in order to satisfy (1).

Goethals and Seidel [2] found two $(1, -1)$ matrices $I + R$, $S$ of order $\frac{1}{2}(p + 1), p \equiv 1 \pmod{4}$ a prime power, which are circulant and symmetric and which satisfy

$$RR^T + SS^T = pI_{\frac{1}{4}(p + 1)}$$

where $I$ is the identity matrix.

Turyn [6] noted that $A = I + R$, $B = I - R$, $C = D = S$ satisfy the conditions (1) for $m = \frac{1}{2}(p + 1)$ and hence are Williamson matrices. White-

man [11] provided an alternate construction for $A$, $B$, $C$, $D$ of these orders.

Turyn announced [7] that he has found Williamson type matrices of order $9c$, $c$ a natural number. In [9] Williamson type matrices are constructed for orders $\frac{1}{2}p(p + 1)$, where $p \equiv 1 \pmod{4}$ is a prime power.

This means that there are Williamson type matrices of the following classes:

<table>
<thead>
<tr>
<th>Class</th>
<th>Expression</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>WI</td>
<td>$b$</td>
<td>$b \in {1, 3, 5, \ldots, 29, 37, 43}$; see [10, p. 388–389].</td>
</tr>
<tr>
<td>WII</td>
<td>$\frac{1}{2}(p + 1)$</td>
<td>$p \equiv 1 \pmod{4}$ a prime power; [6], [11].</td>
</tr>
<tr>
<td>WIII</td>
<td>$9c$</td>
<td>$c$ a natural number; [7]</td>
</tr>
<tr>
<td>WIV</td>
<td>$\frac{1}{2}p(p + 1)$</td>
<td>$p \equiv 1 \pmod{4}$ a prime power; [9].</td>
</tr>
<tr>
<td>WV</td>
<td>$s(4s - 1)$</td>
<td>$s$ the order of a good matrix; Corollary 3.</td>
</tr>
<tr>
<td>WVI</td>
<td>$s(4s + 3)$</td>
<td>$s$ the order of a good matrix, $4s + 4$ the order of a symmetric Hadamard matrix; Corollary 4.</td>
</tr>
<tr>
<td>WVII</td>
<td>$sv$</td>
<td>$s$ the order of a good matrix, $v$ the order of an abelian group $G$ on which are defined a $(v, k, \lambda)$ and a $(v, (v - 1)/2, (v - 3)/4$ difference set $v - 4(k - \lambda) = 4s - 1$; Corollary 5.</td>
</tr>
</tbody>
</table>

Good matrices (see next section for definition) are known to exist [3], [8] for orders $n \in \{1, 3, 5, \ldots, 23, 25\}$, and symmetric Hadamard matrices do exist for each of these $4n + 4$ (see [10]). So WVI gives Williamson type matrices for the new orders 1207, 1827, 2185, 2575, WV gives the new orders 33, 95, 189, 315, 473, 663, 885, 1139, 1425, 1743, 2093, 2475 and WVII gives the new order 93.

The table gives the orders less than 100 for which Williamson type matrices are known.

We use the following theorem (see Section 2 for definitions):

**Theorem 1** (Baumert and Hall, see [10]) *If there are Williamson type matrices of order $m$ and a Baumert-Hall array of order $t$ then there exists a Hadamard matrix of order $4mt$.*
Turyn has announced [7] that he has found Baumert-Hall arrays for the orders $t$ and $5t$

$$t \in \{1, 3, 5, \ldots, 59\} \cup \{1 + 2^{a}5^{b}26^{c}, a, b, c \text{ nonnegative integers}\}. \quad (3)$$

Some Baumert–Hall arrays found by Cooper, Hunt and Wallis may be found in [1], [4]. David Hunt (unpublished) has shown 61 may be added to the set in (3).

<table>
<thead>
<tr>
<th>order</th>
<th>class</th>
<th>order</th>
<th>class</th>
<th>order</th>
<th>class</th>
<th>order</th>
<th>class</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>I</td>
<td>27</td>
<td>I</td>
<td>51</td>
<td>II</td>
<td>77</td>
<td>II</td>
</tr>
<tr>
<td>3</td>
<td>I</td>
<td>29</td>
<td>I</td>
<td>53</td>
<td>II</td>
<td>79</td>
<td>II</td>
</tr>
<tr>
<td>5</td>
<td>I</td>
<td>31</td>
<td>II</td>
<td>55</td>
<td>II</td>
<td>81</td>
<td>III</td>
</tr>
<tr>
<td>7</td>
<td>I</td>
<td>33</td>
<td>V</td>
<td>57</td>
<td>II</td>
<td>83</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>I</td>
<td>35</td>
<td></td>
<td>59</td>
<td>II</td>
<td>85</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>I</td>
<td>37</td>
<td>I</td>
<td>61</td>
<td>II</td>
<td>87</td>
<td>II</td>
</tr>
<tr>
<td>13</td>
<td>I</td>
<td>39</td>
<td></td>
<td>63</td>
<td>II</td>
<td>89</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>I</td>
<td>41</td>
<td>II</td>
<td>65</td>
<td></td>
<td>91</td>
<td>II</td>
</tr>
<tr>
<td>17</td>
<td>I</td>
<td>43</td>
<td>I</td>
<td>67</td>
<td></td>
<td>93</td>
<td>VII</td>
</tr>
<tr>
<td>19</td>
<td>I</td>
<td>45</td>
<td>II</td>
<td>69</td>
<td>II</td>
<td>95</td>
<td>V</td>
</tr>
<tr>
<td>21</td>
<td>I</td>
<td>47</td>
<td></td>
<td>71</td>
<td></td>
<td>97</td>
<td>II</td>
</tr>
<tr>
<td>23</td>
<td>I</td>
<td>49</td>
<td>II</td>
<td>73</td>
<td></td>
<td>99</td>
<td>II</td>
</tr>
<tr>
<td>25</td>
<td>I</td>
<td></td>
<td></td>
<td>75</td>
<td>II</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. BASIC DEFINITIONS

A matrix with every entry $+1$ or $-1$ is called a $(1, -1)$-matrix. An Hadamard matrix $H = (h_{ij})$ is a square $(1, -1)$ matrix of order $n$ which satisfies the equation

$$HH^T = H^TH = nI_n.$$  

We use $J$ for the matrix of all 1’s.

A Baumert–Hall array of order $t$ is a $4t \times 4t$ array with entries $A, -A, B, -B, C, -C, D, -D$ and the properties that:

i) in any row there are exactly $t$ entries $\pm A$, $t$ entries $\pm B$, $t$ entries $\pm C$, and $t$ entries $\pm D$; and similarly for columns;

ii) the rows are formally orthogonal, in the sense that if $\pm A, \pm B, \pm C, \pm D$ are realized as elements of any commutative ring then the distinct rows of the array are pairwise orthogonal; and similarly for columns.

The Baumert–Hall arrays are a generalization of the following array of Williamson:

$$\begin{bmatrix}
A & B & C & D \\
-B & A & -D & C \\
-C & D & A & -B \\
-D & -C & B & A
\end{bmatrix} \quad (4)$$
Four (1, -1) matrices $A, B, C, D$ of order $m$ with the properties

i) $MN^T = NM^T$ for $M, N \in \{A, B, C, D\},$

ii) $(A - I)^T = -(A - I), \quad B^T = B, \quad C^T = C, \quad D^T = D,$ (5)

iii) $AA^T + BB^T + CC^T + DD^T = 4mI_m$

will be called good matrices. These are used in [3], [8], [10] to form skew-Hadamard matrices and exist for odd $m \leq 25.$

Let $S_1, S_2, \ldots, S_n$ be subsets of $V,$ an additive abelian group of order $v,$ containing $k_1, k_2, \ldots, k_n$ elements respectively. Write $T_i$ for the totality of all differences between elements of $S_i$ (with repetitions), and $T$ for the totality of elements of all the $T_i.$ If $T$ contains each nonzero element a fixed number of times, $\lambda$ say, then the sets $S_1, S_2, \ldots, S_n$ will be called $n$-{v; $k_1, k_2, \ldots, k_n; \lambda}$ supplementary difference sets. If $n = 1$ we have a (v, k, $\lambda$) difference set which is cyclic or abelian according as $V$ is cyclic or abelian. Henceforth we assume $V$ is always an additive abelian group of order $v$ with elements $g_1, g_2, \ldots, g_v.$

The type 1 (1, -1) incidence matrix $M = (m_{ij})$ of order $v$ of a subset $X$ of $V$ is defined by

$$m_{ij} = \begin{cases} +1 & g_j - g_i \in X, \\ -1 & \text{otherwise}; \end{cases}$$

while the type 2 (1, -1) incidence matrix $N = (n_{ij})$ of order $v$ of a subset $Y$ of $V$ is defined by

$$n_{ij} = \begin{cases} +1 & g_j + g_i \in Y, \\ -1 & \text{otherwise}. \end{cases}$$

It is shown in [10] that if $M$ is a type 1 (1, -1) incidence matrix and $N$ is a type 2 (1, -1) incidence matrix of 2-{2q - 1; q - 1, q; q - 1} supplementary difference sets then

$$MN^T = NM^T$$

and

$$MM^T + NN^T = 4qI - 2J.$$ (6)

If $N$ were type 1 (6) would still be satisfied.

In general the (1, -1) incidence matrices $A_1, \ldots, A_n$ of $n$-{v; $k_1, k_2, \ldots, k_n; \lambda$} supplementary difference sets satisfy

$$\sum_{i=1}^{n} A_i A_i^T = 4 \left( \sum_{i=1}^{n} k_i - \lambda \right) I + \left[ nv - 4 \left( \sum_{i=1}^{n} k_i - \lambda \right) \right] J.$$ (7)

3. THE MAIN CONSTRUCTION

**Theorem 2** Suppose $X, Y$ are (1, -1) matrices of order $v$ such that

i) $XY^T = YX^T,$

ii) $XX^T = (v - 4m + 1)I + (4m - 1)J,$

iii) $YY^T = (v + 1)I - J.$
Further suppose $A, B, C, D$ are good matrices of order $m$ satisfying (5). Then $A_1, B_1, C_1, D_1$, of order $mn$ given by
\[
A_1 = I \times X + (A - I) \times Y \\
B_1 = B \times Y \\
C_1 = C \times Y \\
D_1 = D \times Y
\]
are Williamson type matrices.

Proof Since $B, C, D$ are symmetric, clearly
\[
MN^T = NM^T \text{ for } M, N \in \{B_1, C_1, D_1\}.
\]
The terms $A_1B_1^T, A_1C_1^T, A_1D_1^T$ are all similar and we only prove the result for $A_1B_1^T$:
\[
A_1B_1^T = (I \times X + (A - I) \times Y)B^T \times Y^T \\
= B^T \times XY^T + (A - I)B^T \times YY^T \\
= B \times YX^T + (B4^T - B) \times YY^T \\
= (B \times Y)(I \times X^T + (A^T - I) \times Y^T) \\
= (B \times Y)(I \times X + (A - I) \times Y)^T \\
= B_1A_1^T.
\]
Now, since $A^T - I = (A - I)^T = -(A - I) = -A + I$ we have $A^T + A = 2I$, and so,
\[
A_1A_1^T + B_1B_1^T + C_1C_1^T + D_1D_1^T = I \times XX^T + (A - I) \times YX^T \\
+ (A - I)^T \times XY^T \\
+ (A - I)(A - I)^T \times YY^T \\
+ (BB^T + CC^T + DD^T) \times YY^T \\
= I \times XX^T + (-A - A^T + I) \times YY^T \\
+ 4mI \times YY^T \\
= I \times [(v - 4m + 1)I + (4m - 1)J] \\
+ (4m - 1)I \times [(v + 1)I - J] \\
= [v - 4m + 1 + (4m - 1)(v + 1)]I_{nm} \\
= 4mI_{nm}.
\]
So $A_1, B_1, C_1, D_1$ are Williamson type matrices of order $mn$.

Corollary 3 Suppose there exist good matrices of order $m$. Then there exist Williamson type matrices of order $m(4m - 1)$.

Proof The good matrices can be used in (4) to form an Hadamard matrix of order $4m$. This matrix can then be normalized to the form
\[
\begin{bmatrix}
1 & 1 & \ldots & 1 \\
1 \\
\vdots \\
\ddots \\
1
\end{bmatrix}
\]
(8)
Now put \( X = J, Y = E \) in the theorem and we have the result.

This gives new Williamson type matrices of order 33, 95, 189, 315, 473, 663, 885, 1139, 1425, 1743, 2093, 2475.

**Corollary 4** Suppose there exist good matrices of order \( m \). Further suppose \( 4m + 4 \) is the order of a symmetric Hadamard matrix. Then there exist Williamson type matrices of order \( m(4m + 3) \).

**Proof** Normalize the Hadamard matrix to the form (8) where now \( E^T = E \). Put \( X = J - 2I, Y = E, v = 4m + 3 \) in the theorem and we have the result.

This gives new Williamson type matrices of order 1207, 1827, 2185, 2575.

**Corollary 5** Suppose there exist good matrices of order \( m \). Further suppose there exist \((v, k, \lambda)\) and \((v, (v - 1)/2, (v - 3)/4)\) difference sets defined on the same abelian (or cyclic) group and that \( v - 4(k - \lambda) = 4m - 1 \). Then there exist Williamson type matrices of order \( mv \).

**Proof** The reader is referred to [10] for properties of type 1 and 2. Let \( X \) be the type 1 \((1, -1)\) incidence matrix of the \((v, k, \lambda)\) difference set and \( Y \) be the type 2 \((1, -1)\) incidence matrix of the \((v, (v - 1)/2, (v - 3)/4)\) difference set and we have the result.

**Corollary 6** There exist Williamson type matrices of order 93.

**Proof** There exist \((31, 6, 1)\) and \((31, 15, 7)\) difference sets in the cyclic group of order 31. Hence with \( v = 31, k = 6, \lambda = 1 \) and \( m = 3 \) in the previous corollary we have the result.

### 4. THREE CONSTRUCTIONS FOR EIGHT-WILLIAMSON TYPE MATRICES: THE FIRST

A Baumert–Hall like array in eight symbols will be called a *Plotkin array* of order \( 8t \).

Eight \((1, -1)\) matrices \( A_1, A_2, \ldots, A_8 \) of order \( m \) which satisfy

i) \( A_i A_j^T = A_j A_i^T \), \( i, j = 1, 2, \ldots, 8 \),

ii) \( \sum_{i=1}^{8} A_i A_i^T = 8m I_m \),

will be called *eight-Williamson type matrices*. These matrices are of most interest when there are no known Williamson type matrices for the given order and they may be used in Plotkin arrays of order \( 8t \) to find an Hadamard matrix of order \( 8mt \).
Plotkin's [5] result that if there exists an Hadamard matrix \( H \) of order \( n \) there is a Plotkin array in eight symbols of order \( 4n \) is obtained as follows:

Let
\[
S = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} H, \quad T = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} H,
\]
\[
U = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} H, \quad V = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} H
\]

then define
\[
H_n(A, B) = S \times A + T \times B
\]
\[
H_{2n}(A, B, C, D) = \begin{bmatrix} H_n(A, B) & H_n(C, D) \\ H_n(-C, D) & H_n(A, -B) \end{bmatrix}
\]
\[
B_{2n}(A, B, C, D) = \begin{bmatrix} S \times A + T \times B & U \times C + V \times D \\ U \times -C + V \times -D & S \times A + T \times B \end{bmatrix}
\]
\[
H_{4n}(A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8) = \begin{bmatrix} H_{2n}(A_1, A_2, A_3, A_4) & B_{2n}(A_5, A_6, A_7, A_8) \\ B_{2n}(-A_5, A_6, A_7, A_8) & -H_{2n}(-A_1, A_2, A_3, A_4) \end{bmatrix}
\]

In [5] Plotkin exhibits a Plotkin array of order 24 and also gives the following conjecture:

**Conjecture (Plotkin)** There exist Plotkin arrays in every order \( 8n \), \( n \) a positive integer.

**Lemma 7** Let \( p \equiv 1 (\text{mod} \ 4) \) be a prime power. Suppose there exist three \((1, -1)\) matrices \(Z, P, Q\) of order \( q\) such that

i) \( PP^T = QP^T, \quad ZP^T = PZ^T, \quad ZZ^T = QZ^T\),

ii) \( PP^T + QQ^T = 2(q - p)I + 2pJ\),

iii) \( ZZ^T = (q + 1)I - J\),

then there exist eight-Williamson type matrices of order \( \frac{1}{2}(p + 1)q\).

**Proof** As in (2) we find \( I + R, S\) of order \( \frac{1}{2}(p + 1)\). Now consider
\[
A_1 = I \times P + R \times Z
\]
\[
A_2 = S \times Z
\]
\[
A_3 = I \times -P + R \times Z
\]
\[
A_4 = S \times Z
\]
\[
A_5 = I \times Q + R \times Z
\]
\[
A_6 = S \times Z
\]
\[
A_7 = I \times -Q + R \times Z
\]
\[
A_8 = S \times Z
\]

which clearly satisfy \( A_i A_j^T = A_j A_i^T \) for \( i, j = 1, 2, \ldots, 8\). Also
\[
\sum_{i=1}^{8} A_i A_i^T = 2I \times (PP^T + QQ^T) + 4(RR^T + SS^T) \times ZZ^T
\]
\[
= I \times [4(q - p) + 4p(q + 1)]I
\]
\[
= 4(p + 1)qI \frac{1}{2}(p + 1)q
\]

and hence we have the result.
Corollary 8 Let \( p \equiv 1 \pmod{4} \) be a prime power. Then there exist eight-Williamson type matrices of order \( \frac{1}{2}(p + 1)(2p + 1) \).

Proof Since \( p \) is a prime power there exists an Hadamard matrix of order \( q = 2p + 2 \) (see [10]). Form \( E \) as in (8) and then choose \( P = -J, Q = Z = E \) in the theorem.

Corollary 9 Let \( p \equiv 1 \pmod{4} \) be a prime power. Then there are eight-Williamson type matrices of order
i) \( \frac{1}{2}(p + 1)(p + 2) \);
ii) \( \frac{1}{2}(p + 1)(2p + 5) \);
when \( p + 3 \) and \( 2p + 6 \) respectively are the orders of symmetric Hadamard matrices.

Proof In both cases form \( E \) as in (8) from the symmetric Hadamard matrix. Then with
i) \( P = J, Q = J - 2I, Z = E \) of order \( p + 2 \);
ii) \( P = J - 2I, Q = Z = E \) of order \( 2p + 5 \);
in the theorem, we have the result.

Corollary 10 Let \( p \equiv 1 \pmod{4} \) be a prime power. Suppose there exist \((v, k, \lambda)\) and \((v, (v - 1)/2, (v - 3)/4)\) difference sets defined on the same abelian (or cyclic) group. Then there exist eight-Williamson type matrices of order
i) \( \frac{1}{2}(p + 1)v \) when \( v - 2(k - \lambda) = p \);
ii) \( \frac{1}{2}(p + 1)v \) when \( v - 4(k - \lambda) - 1 = 2p \).

Proof Let \( P \) be the type 1 \((1, -1)\) incidence matrix of the \((v, k, \lambda)\) difference set and \( Z \) be the type 2 \((1, -1)\) incidence matrix of the other difference set. Now using
i) \( Q = J \);
ii) \( Q = Z \);
in the theorem we have the result.

Corollary 11 Let \( p \equiv 1 \pmod{4} \) be a prime power. Let \( 8r \) be the order of a Plotkin array. Then there exist Hadamard matrices of order
i) \( 4(p + 1)(2p + 1)r \);
ii) \( 4(p + 1)(p + 2)r \), when \( p + 3 \) is the order of a symmetric Hadamard matrix;
iii) \( 4(p + 1)(2p + 5)r \), when \( 2(p + 3) \) is the order of a symmetric Hadamard matrix.

Proof Put the eight-Williamson type matrices into the Plotkin arrays of order \( 8r \). While (ii) is covered by class \( HX \) of [10, p. 450]. The other two classes
seem to be genuinely new. Unfortunately they yield no new Hadamard matrices of order less than 4000.

**Corollary 12** Let \( p \equiv 1 \pmod{4} \) be a prime power. Let \( 8r \) be the order of a Plotkin array. Further suppose there exist \((v, k, \lambda)\) and \((v, (v - 1)/2, (v - 3)/4)\) difference sets defined on the same abelian (or cyclic) group. Then there exist Hadamard matrices of order

i) \( 4(p + 1)cr \), when \( v - 2(k - \lambda) = p \);

ii) \( 4(p + 1)cr \), when \( v - 4(k - \lambda) - 1 = 2p \).

An example of how this may be used is that there are \((31, 6, 1)\) and \((31, 15, 7)\) difference sets, so with \( p = 5 \) in (ii) we have an Hadamard matrix of order 744.

5. **THE SECOND**

**Theorem 13** Let \( p \equiv 1 \pmod{4} \) be a prime power. Suppose there exist three \((1, -1)\) matrices \( X, Y, P \) of order \( q \equiv 1 \pmod{4} \) which satisfy

i) \( XY^T = YX^T \), \( XP^T = PX^T \), \( YP^T = PY^T \),

ii) \( XX^T + YY^T = 2(q + 1)I - 2J \),

iii) \( PP^T = (q - p)I + pJ \),

then there exist eight Williamson type matrices of order \( \frac{1}{2}(p + 1)q \).

**Proof** As in (2) we find \( I + R, S \) of order \( \frac{1}{2}(p + 1) \) and consider

\[
\begin{align*}
A_1 &= I \times P + R \times X \\
A_2 &= S \times X \\
A_3 &= I \times -P + R \times X \\
A_4 &= S \times X \\
A_5 &= I \times P + R \times Y \\
A_6 &= S \times Y \\
A_7 &= I \times -P + R \times Y \\
A_8 &= S \times Y 
\end{align*}
\]

which clearly satisfy \( A_iA_j^T = A_jA_i^T \) for \( i, j = 1, 2, \ldots, 8 \). Also

\[
\sum_{i=1}^{8} A_iA_j^T = 4I \times PP^T + 2(RR^T + SS^T) \times (XX^T + YY^T) \\
= 4I \times ((q - p)I - pJ) + 2pI \times (2(q + 1)I - 2J) \\
= 4(p + 1)qI \frac{1}{2}(p + 1)q,
\]

and hence we have the result.

**Corollary 14** Let \( p \equiv 1 \pmod{4} \) be a prime power. Suppose there exist a \((v, k, \lambda)\) difference set, where \( p = v - 4(k - \lambda) \), and \( 2 - \{v; (v - 1)/2; \).
Then there exist eight-Williamson type matrices of order \( \frac{1}{2}(p + 1)v \).

Proof. The choice of \( M \) and \( N \) ensures that their type 2 \((1, -1)\) incidence matrices \( X \) and \( Y \) satisfy \( XY^T = YX^T \) and also that the type 1 \((1, -1)\) incidence matrix \( P \) of the difference set satisfies \( XP^T = PX^T \) and \( YP^T = PY^T \).

Now putting \( P, X, Y \) in the theorem we have the result.

Corollary 15. Let \( p \equiv 1 \pmod{4} \) be a prime power. Then if \( p + 4 \) is a prime power there exist eight-Williamson type matrices of order \( \frac{1}{2}(p + 1)(p + 4) \).

Proof. Use \( P = J - 2I \). The construction of \( M \) and \( N \) can be found in \([10, p. 283]\).

Corollary 16. Let \( p \equiv 1 \pmod{4} \) and \( p + 4 \) be prime powers. Let \( 8r \) be the order of a Plotkin array. Then there exists an Hadamard matrix of order \( 4(p + 1)(p + 4)r \).

This is a particular case of a theorem of Goethals and Seidel (see \([10, p. 450]\)) and is of interest for the structure of the matrix.

6. THE THIRD

Lemma 17. Let \( p \) and \( q \) both be prime powers \( \equiv 1 \pmod{4} \). Then there exist eight-Williamson type matrices of order \( \frac{1}{2}(p + 1)(q + 1) \).

Proof. Form \( I + R \) and \( S \) of order \( \frac{1}{2}(p + 1) \) as in (2), and similarly form \( I' + R' \) and \( S' \) of order \( \frac{1}{2}(q + 1) \). Now consider

\[
A_1 = I' \times (I + R) + R' \times S
A_2 = S' \times S
A_3 = I' \times (I - R) + R' \times S
A_4 = S' \times S
A_5 = I' \times -S + R' \times (I + R)
A_6 = S' \times (I + R)
A_7 = I' \times -S + R' \times (I - R)
A_8 = S' \times (I - R).
\]

Clearly \( A_i A_j^T = A_j A_i^T \), for \( i, j = 1, 2, \ldots, 8 \). Also

\[
\sum_{i=1}^{8} A_i A_i^T = (I' + (R')^2 + (S')^2) \times 2(I + R^2 + S^2)
= 2(q + 1)(p + 1)I_{(p+1)(q+1)/4},
\]

and hence we have the result.

Corollary 18. Let \( p \) and \( q \) both be prime powers \( \equiv 1 \pmod{4} \). Let \( 8r \) be the order of a Plotkin array. Then there exists an Hadamard matrix of order \( 2(q + 1)(p + 1)r \).
Proof Use the results of Lemma 17 in the Plotkin array.
This is a particular case of a theorem of Goethals and Seidel [2] which obtains Hadamard matrices of order $kn$ when $k (= 2(p + 1))$ is the order of an Hadamard matrix and $n (= q + 1)$ is the order of a symmetric conference matrix (see [10, p. 368]). The interest lies in the structure of the matrix.

References


