Bulletin of the Institute of Mathematics
Academia Sinica (New Series)
Vol. **6** (2011), No. 1, pp. 27-39

ON EXISTENCE OF WILLIAMSON SYMMETRIC CIRCULANT MATRICES

HRISHIKESH MAHATO

Center for Applied Mathematics, Central University of Jharkhand, Brambe, Ranchi-835205, India.
E-mail: hrishikesh.mahato@gmail.com

Abstract

In this paper we consider a particular type of partition of $\mathbb{Z}_n$, called H-partition and obtain a necessary and sufficient condition for existence of a set of four symmetric circulant matrices for a Hadamard matrix of order $4n$ in terms of such partitions when n odd.

1. Introduction

A $(1,-1)$ matrix H of order n is called a Hadamard matrix if $HH' = nI$, where H' is the transpose of H. If H is a Hadamard matrix of order n then $n = 2$ or $n \equiv 0(\mathrm{mod}\, 4)$. The converse of this seems to be true and is known as Hadamard conjecture.

Many exciting results have stemmed from the following basic idea put forward by Williamson . Consider the array

$$H = \begin{pmatrix} W & X & Y & Z \\ -X & W & -Z & Y \\ -Y & Z & W & -X \\ -Z & -Y & X & W \end{pmatrix}$$

If W, X, Y, and Z are replaced by square matrices A, B, C, and D of order n, respectively, then H becomes a square matrix of order $4n$. Williamson proved that a sufficient condition for H to be a Hadamard matrix is that

Received Received January 12, 2009 and in revised form October 5, 2010.

AMS Subject Classification: 05B20.

Key words and phrases: Shift matrix, match matrix, mis-match matrix, circulant matrix, Williamson matrix, Hadamard matrix.

A, B, C, and D are $(1, -1)$ matrices of order n with

$$AA' + BB' + CC' + DD' = 4nI \tag{1}$$

and for every pair X, Y of matrices chosen from A, B, C, D

$$XY' = YX' \tag{2}$$

If A, B, C, and D are symmetric and circulant then condition (2) is satisfied trivially and condition(1) becomes

$$A^2 + B^2 + C^2 + D^2 = 4nI \tag{3}$$

The basic difficulty lies in finding the matrices A, B, C, and D which satisfy the condition (3). In this article we give a necessary and sufficient condition for the existence of such symmetric circulant matrices A, B, C, and D. Our result also gives a method for finding a set of such matrices.

2. Definitions

Definition 2.1. For any odd integer n, let $\mathbb{Z}_n$ be the cyclic group of integers modulo n under addition. Let A be a proper subset of $\mathbb{Z}_n$ such that $0 \in A$ and $A = -A$. Then $A, B = \mathbb{Z}_n - A$ is clearly a partition of $\mathbb{Z}_n$ such that $B = -B$. We call such a partition of $\mathbb{Z}_n$ to be an *H-partition* of $\mathbb{Z}_n$.

For an H-partition (A, B) of $\mathbb{Z}_n$, let $A + B = \{a + b (\operatorname{mod} n) \mid a \in A, b \in B\}$. Let C denote the set of distinct elements of $A + B$. For any $c \in C$ we denote n_c the frequency of occurrence of c in $A + B$. Clearly $0 \notin C$ for any H-partition (A, B) of $\mathbb{Z}_n$.

Definition 2.2. A set of 4 symmetric circulant matrices A, B, C, and D satisfying the condition $A^2 + B^2 + C^2 + D^2 = 4nI$ is called a *set of Williamson circulant matrices.*

Definition 2.3. The *shift matrix* T of order n is a $(0, 1)$-square matrix defined as $T = [u_{ij}]$, where

$$u_{ij} = \begin{cases} 1, & \text{if } j - i \equiv 1 \operatorname{mod} n; \\ 0, & \text{otherwise.} \end{cases}$$

Definition 2.4. For any matrix A, the *Match matrix* $A^{(m)}$ of A is defined as $A^{(m)} = [n_{ij}]$, where n_{ij} = number of places in which the i^{th} row and j^{th} row of A have same non-zero entry at corresponding places.

Definition 2.5. For any matrix A with nonzero entries, the *Mis-match matrix* $A^{(mm)}$ of A is defined to be $A^{(mm)} = [\acute{n}_{ij}]$, where $\acute{n}_{ij}$ = number of places in which the i^{th} row and j^{th} row of A have different entries at corresponding places.

Definition 2.6. Let $a_0, a_1, \ldots, a_{n-1}$ be a sequence of n elements then a matrix $C = [c_{ij}]$ is called a *Circulant matrix* with entries $a_0, a_1, \ldots, a_{n-1}$ if $c_{ij} = a_{(j-i) \bmod n}$; for $1 \leq i, j \leq n$.

Clearly C is a circulant matrix if and only if $C = \sum_{i=0}^{n-1} a_i T^i$.

We now have the following result.

3. Result

Theorem 3.1. *There exists a set of four Williamson symmetric circulant matrices of order n if and only if there exists four H-partitions (A_i, B_i), $i = 1, 2, 3, 4$, of $\mathbb{Z}_n$, not necessarily distinct, such that $\bigcup_{i=1}^{4} C_i = \mathbb{Z}_n - \{0\}$ and $\sum_{i=1}^{4} n_c^i = n$ for each $c \in \mathbb{Z}_n - \{0\}$ where n_c^i denotes the occurrence number of c in $A_i + B_i$.*

Proof. Let T be the shift matrix of order n. For any set of four H-partitions (A_i, B_i), $i = 1, 2, 3, 4$ of $\mathbb{Z}_n$ of the stated type, let $P_i = \sum_{a_i \in A_i} T^{a_i}$ and $N_i = \sum_{b_i \in B_i} T^{b_i}$. Then P_i and N_i are symmetric circulant $(0, 1)$ matrices and

$$P_i N_i = \sum_{c \in C_i} n_c^i T^c$$

$$\Rightarrow \sum_{i=1}^{4} P_i N_i = n \sum_{c \in \mathbb{Z}_n - \{0\}} T^c = n(J - I) \tag{1}$$

Now let $X_i = P_i - N_i$ for $i = 1,2,3,4$; then $X_i's$ are symmetric circulant matrices with entries 1 and -1 and hence X_i, X_j commutes for $i, j \in \{1,2,3,4\}$. From Definition 2.4 it is clear that for a symmetric $(0,1)$-matrix A the match matrix $A^{(m)} = A^2$. Since P_i's and N_i's are symmetric $(0,1)$-matrices, $P_i^{(m)} = P_i^2$ and $N_i^{(m)} = N_i^2$, and $X_i^{(m)} = P_i^{(m)} + N_i^{(m)}$ for $i = 1,2,3,4$; since (A_i, B_i) is a partition of $\mathbb{Z}_n$. So

$$X_i^{(m)} = P_i^2 + N_i^2; i = 1,2,3,4; \tag{2}$$

From Definition 2.5 it is clear that, for a $(1,-1)$-matrix A of order n, the mis-match matrix $A^{(mm)} = [\acute{n}_{ij}] = [n - n_{ij}]$, where n_{ij} is the $(i,j)^{\text{th}}$ entry of $A^{(m)}$.

Therefore $A^{(mm)} = nJ - A^{(m)}$, where J is the square matrix with entry 1. Since X_i is a $(1,-1)$-matrix,

$$\begin{aligned} X_i^{(mm)} &= nJ - X_i^{(m)} \\ \Rightarrow X_i^{(mm)} &= nJ - (P_i^2 + N_i^2);\ i = 1,2,3,4 \end{aligned} \tag{3}$$

Also, since X_i is a symmetric $(1,-1)$-matrix $X_i^2 = [x_{kl}]$, where x_{kl} = inner product of the k^{th} row and l^{th} row of X_i = (number of places in which the k^{th} row and l^{th} row of X_i have the same entries) - (number of places in which the k^{th} row and l^{th} row of X_i have different entries).

Thus

$$\begin{aligned} X_i^2 &= X_i^{(m)} - X_i^{(mm)} \\ \Rightarrow \quad X_i^2 &= 2(P_i^2 + N_i^2) - nJ; i = 1,2,3,4 \\ \Rightarrow \sum_{i=1}^{4} X_i^2 &= 2(\sum_{i=1}^{4} P_i^2 + \sum_{i=1}^{4} N_i^2) - 4nJ \end{aligned} \tag{4}$$

Again

$$\begin{aligned} \sum_{i=1}^{4} X_i^2 &= \sum_{i=1}^{4} (P_i - N_i)^2 \\ &= \sum_{i=1}^{4} P_i^2 + \sum_{i=1}^{4} N_i^2 - 2\sum_{i=1}^{4} P_i N_i \end{aligned}$$

$$\Rightarrow \sum_{i=1}^{4} P_i^2 + \sum_{i=1}^{4} N_i^2 \;=\; \sum_{i=1}^{4} X_i^2 + 2\sum_{i=1}^{4} P_i N_i \tag{5}$$

From equations (4) and (5)

$$\begin{aligned} \sum_{i=1}^{4} X_i^2 &= 2(\sum_{i=1}^{4} X_i^2 + 2\sum_{i=1}^{4} P_i N_i) - 4nJ \\ \Rightarrow \sum_{i=1}^{4} X_i^2 &= 4nJ - 4\sum_{i=1}^{4} P_i N_i \end{aligned} \tag{6}$$

So equations (1) and (6) imply

$$\begin{aligned} \sum_{i=1}^{4} X_i^2 &= 4nJ - 4n(J-I) \\ &= 4nI \end{aligned}$$

Thus X_i, $i = 1,2,3,4$ form a set of four Williamson circulant matrices for a Hadamard matrix of order $4n$.

Conversely, let X_i, $i = 1,2,3,4$ be a set of four Williamson symmetric circulant matrices of order n. Then

$$\sum_{i=1}^{4} X_i^2 \;=\; 4nI \tag{7}$$

and

$$X_i X_j \;=\; X_j X_i, \tag{8}$$

for $i, j = \{1,2,3,4\}$.

Since X_i is a $(1,-1)$ circulant matrix, it can be written as

$$X_i = \sum_{k=0}^{n-1} a_k T^k;\; a_i = \pm 1\;; i = 1,2,3,4 \tag{9}$$

Let $A_i = \{k, k \in \mathbb{Z}_n \mid a_k = +1\}$ and $B_i = \{k, k \in \mathbb{Z}_n \mid a_k = -1\}$, then clearly (A_i, B_i), $i = 1,2,3,4$ are four partitions of $\mathbb{Z}_n$ and exactly one of A_i and B_i contains 0. Since equation (7) remains valid if X_i is replaced by $-X_i$, replacing X_i by $-X_i$, if necessary, we can assume that A_i contains 0, for $i = 1,2,3,4$. As $\pm X_i$ is a symmetric circulant matrix $k \in A_i \Rightarrow n-k \in A_i$

and so (A_i,B_i), $i = 1, 2, 3, 4$ are four H-partitions of $\mathbb{Z}_n$. Let $P_i = \sum_{k\in A_i} T^k$ and $N_i = \sum_{k\in B_i} T^k$. Then $X_i = P_i - N_i$; $i = 1, 2, 3, 4$ and P_i and N_i are symmetric matrices with entries $(0, 1)$. Thus $P_i^{(m)} = P_i^2$ and $N_i^{(m)} = N_i^2$, and $X_i^{(m)} = P_i^{(m)} + N_i^{(m)}$ for $i = 1, 2, 3, 4$. So

$$X_i^{(m)} = P_i^2 + N_i^2;\ i = 1, 2, 3, 4. \tag{10}$$

Since X_i is a $(1, -1)$-matrix from Definition 2.5

$$X_i^{(mm)} = nJ - X_i^{(m)}. \tag{11}$$

Using equations (7), (10) and (11) we get

$$\sum_{i=1}^{4} P_i N_i = n(J - I) \tag{12}$$

Now, if possible, let us assume that for some element $k \in \mathbb{Z}_n - \{0\}$, $\sum_{i=1}^{4} n_k^i = n_k \neq n$. As $P_i N_i = \sum_{c\in C_i} n_c^i T^c$; $i = 1, 2, 3$ and 4, where C_i is the set determined by $A_i + B_i$.

$$\begin{aligned}
\sum_{i=1}^{4} P_i N_i &= \sum_{i=1}^{4} (\sum_{c\in C_i} n_c^i T^c) = \sum_{c\in C} (\sum_{i=1}^{4} n_c^i) T^c, \quad \text{where} \quad C = \bigcup_{i=1}^{4} C_i \\
&= \sum_{c\in C-\{k\}} (\sum_{i=1}^{4} n_c^i) T^c + \sum_{i=1}^{4} n_k^i T^k = \sum_{c\in C-\{k\}} (\sum_{i=1}^{4} n_c^i) T^c + n_k T^k
\end{aligned}$$

But this contradicts

$$\sum_{i=1}^{4} P_i N_i = n(J - I), \quad as\ n_k \neq n.$$

So $C = \bigcup_{i=1}^{4} C_i = \mathbb{Z}_n - \{0\}$ and $\sum_{i=1}^{4} n_c^i = n$ for each $c \in \mathbb{Z}_n - \{0\}$. Hence the theorem. $\square$

4. Examples

Example 4.1. For $n = 5$; let $A_1 = \{0\}, B_1 = \{1,2,3,4\}$; $A_2 = \{0\}, B_2 = \{1,2,3,4\}$; $A_3 = \{0,1,4\}, B_3 = \{2,3\}$; $A_4 = \{0,2,3\}, B_4 = \{1,4\}$. Then $A_1+B_1 = \{1,2,3,4\}$ $A_2+B_2 = \{1,2,3,4\}$ $A_3+B_3 = \{1,2,2,3,3,4\}$ and $A_4+B_4 = \{1,1,2,3,4,4\}$. These four H-partitions clearly satisfy the condition of the theorem and yield a set of four Williamson symmetric circulant matrices whose first rows are given by

$$\begin{array}{ccccc}
+1 & -1 & -1 & -1 & -1 \\
+1 & -1 & -1 & -1 & -1 \\
+1 & +1 & -1 & -1 & +1 \\
+1 & -1 & +1 & +1 & -1
\end{array}$$

Example 4.2. For $n = 9$; (i) $A_1 = \{0,1,8\}, B_1 = \{2,3,4,5,6,7\}$; $A_2 = \{0,2,7\}, B_2 = \{1,3,4,5,6,8\}$; $A_3 = \{0,3,6\}, B_3 = \{1,2,4,5,7,8\}$; $A_4 = \{0,4,5\}, B_4 = \{1,2,3,6,7,8\}$. Then $A_1+B_1 = \{1,2,2,3,3,3,4,4,4,5,5,5,6,6,6,7,7,8\}$
$A_2 + B_2 = \{1,1,1,2,3,3,3,4,4,5,5,6,6,6,7,8,8,8\}$
$A_3 + B_3 = \{1,1,1,2,2,2,4,4,4,5,5,5,7,7,7,8,8,8\}$
and $A_4 + B_4 = \{1,1,2,2,2,3,3,3,4,5,6,6,6,7,7,7,8,8\}$. These four H-partitions clearly satisfy the condition of the theorem and yield a set of four Williamson symmetric circulant matrices whose first rows are given by

$$\begin{array}{ccccccccc}
+1 & +1 & -1 & -1 & -1 & -1 & -1 & -1 & +1 \\
+1 & -1 & +1 & -1 & -1 & -1 & -1 & +1 & -1 \\
+1 & -1 & -1 & +1 & -1 & -1 & +1 & -1 & -1 \\
+1 & -1 & -1 & -1 & +1 & +1 & -1 & -1 & -1
\end{array}$$

as listed in [2]. Some other sets of such matrices are obtained dy considering the partitions,
(ii) $A_1 = \{0,1,8\}, B_1 = \{2,3,4,5,6,7\}$; $A_2 = \{0,1,3,6,8\}, B_2 = \{2,4,5,7\}$; $A_3 = \{0,2,3,6,7\}, B_3 = \{1,4,5,8\}$; $A_4 = \{0,1,3,4,5,6,8\}, B_4 = \{2,7\}$.
(iii) $A_1 = \{0,2,7\}, B_1 = \{1,3,4,5,6,8\}$; $A_2 = \{0,2,3,6,7\}, B_2 = \{1,4,5,8\}$; $A_3 = \{0,3,4,5,6\}, B_3 = \{1,2,7,8\}$; $A_4 = \{0,1,2,3,6,7,8\}, B_4 = \{4,5\}$.
(iv) $A_1 = \{0,4,5\}, B_1 = \{1,2,3,6,7,8\}$; $A_2 = \{0,3,4,5,6\}, B_2 = \{1,2,7,8\}$; $A_3 = \{0,1,3,6,8\}, B_3 = \{2,4,5,7\}$; $A_4 = \{0,2,3,4,5,6,7\}, B_4 = \{1,8\}$.
The first row of the respective sets of Williamson matrices are,
(ii)

$$\begin{array}{ccccccccc}
+1 & +1 & -1 & -1 & -1 & -1 & -1 & -1 & +1 \\
+1 & +1 & -1 & +1 & -1 & -1 & +1 & -1 & +1 \\
+1 & -1 & +1 & +1 & -1 & -1 & +1 & +1 & -1 \\
+1 & +1 & -1 & +1 & +1 & +1 & +1 & -1 & +1
\end{array}$$

(iii)

$$\begin{array}{ccccccccc}
+1 & -1 & +1 & -1 & -1 & -1 & -1 & +1 & -1 \\
+1 & -1 & +1 & +1 & -1 & -1 & +1 & +1 & -1 \\
+1 & -1 & -1 & +1 & +1 & +1 & +1 & -1 & -1 \\
+1 & +1 & +1 & +1 & -1 & -1 & +1 & +1 & +1
\end{array}$$

(iv)

$$\begin{array}{ccccccccc}
+1 & -1 & -1 & -1 & +1 & +1 & -1 & -1 & -1 \\
+1 & -1 & -1 & +1 & +1 & +1 & +1 & -1 & -1 \\
+1 & +1 & -1 & +1 & -1 & -1 & +1 & -1 & +1 \\
+1 & -1 & +1 & +1 & +1 & +1 & +1 & +1 & -1
\end{array}$$

5. Possible size of partitions for Williamson matrices

Theorem 5.1. *Let $(A_i, B_i), i = 1, 2, 3, 4$ be a set of H-partitions of $\mathbb{Z}_n$, which gives rise to a set of Williamson matrices. Then $\sum_{i=1}^{4} k_i(n-k_i) = n(n-1)$, where $k_i = |A_i|; i = 1, 2, 3, 4$.*

Proof. Let (A_i, B_i); $i = 1, 2, 3, 4$ be a set of H-partitions of $\mathbb{Z}_n$, which constructs a Hadamard matrix. Then $\sum_{i=1}^{4} n_c^i = n$ for all $c \in \mathbb{Z}_n - \{0\}$. Let $k_i = |A_i|; i = 1, 2, 3, 4$.

Without loss of generality we can assume that $0 \in A_i; i = 1, 2, 3, 4$. As $A_i = -A_i; i = 1, 2, 3, 4$, k_i is an odd positive integer and consequently $|B_i| = n - k_i$ is an even integer for all $i = 1, 2, 3, 4$. Since $A_i + B_i$ is a $k_i \times (n - k_i)$ sub-matrix of the matrix corresponding to the composition table of $\mathbb{Z}_n$, for $i = 1, 2, 3, 4$; we have.

$$\sum_{c \in \mathbb{Z}_n} n_c^i \;=\; k_i(n-k_i); i = 1, 2, 3, 4.$$

$$\Rightarrow \sum_{i=1}^{4}(\sum_{c\in\mathbb{Z}_n} n_c^i) \;=\; \sum_{i=1}^{4} k_i(n-k_i) \tag{13}$$

Again

$$\begin{aligned}
\sum_{i=1}^{4}(\sum_{c\in\mathbb{Z}_n} n_c^i) \;&=\; \sum_{i=1}^{4}(\sum_{c\in\mathbb{Z}_n-\{0\}} n_c^i) \quad \text{as} \quad n_0^i = 0; i = 1,2,3,4 \\
&= \sum_{c\in\mathbb{Z}_n-\{0\}}(\sum_{i=1}^{4} n_c^i) \\
\Rightarrow \sum_{i=1}^{4}(\sum_{c\in\mathbb{Z}_n} n_c^i) \;&=\; \sum_{c\in\mathbb{Z}_n-\{0\}} n = n(n-1) \qquad (14)
\end{aligned}$$

From (13) and (14) we have

$$\sum_{i=1}^{4} k_i(n-k_i) = n(n-1). \qquad \square$$

So the possible size of A_i; $i = 1,2,3,4$ are k_1, k_2, k_3 and k_4 respectively which is a set of odd integer solution of the equation

$$w(n-w) + x(n-x) + y(n-y) + z(n-z) = n(n-1)$$

Theorem 5.2. *The equation*

$$w(n-w) + x(n-x) + y(n-y) + z(n-z) = n(n-1)$$

has an integer solution if and only if there exists an integer solution of the equation

$$X_1 + X_2 + X_3 + X_4 = n-1$$

in $\{m(m-1)\}_{m=0}^{\infty}$.

Proof. Let $\{k_1, k_2, k_3, k_4\}$ be an integer solution of the equation

$$w(n-w) + x(n-x) + y(n-y) + z(n-z) = n(n-1). \tag{15}$$

Thus

$$\sum_{i=1}^{4} k_i(n-k_i) = n(n-1).$$

Let $X_i = (\frac{n-1}{2})(\frac{n+1}{2}) - k_i(n-k_i), i = 1,2,3,4.$
Since $k_i + (n-k_i) = n; i = 1,2,3,4,$ so $(\frac{n-1}{2})(\frac{n+1}{2}) \geq k_i(n-k_i); i = 1,2,3,4$
$\Rightarrow X_i = (\frac{n-1}{2})(\frac{n+1}{2}) - k_i(n-k_i) \geq 0; i = 1,2,3,4$ Then

$$\begin{aligned}
\sum_{i=1}^{4} X_i &= \sum_{i=1}^{4}\{(\frac{n-1}{2})(\frac{n+1}{2}) - k_i(n-k_i)\} \\
&= (n-1)(n+1) - \sum_{i=1}^{4} k_i(n-k_i) \\
&= (n-1)(n+1) - n(n-1) \quad [from(15)] \\
&= n-1
\end{aligned}$$

Now we have to show that $X_i \in \{m(m-1)\}_{m=0}^{\infty}$ for $i = 1,2,3,4.$
For $i = 1,2,3,4$ we have

$$\begin{aligned}
X_i &= (\frac{n-1}{2})(\frac{n+1}{2}) - k_i(n-k_i) \\
&= (\frac{n-1}{2})(\frac{n+1}{2}) - k_i(\frac{n+1}{2}) + k_i(\frac{n+1}{2}) - k_i(n-k_i) \\
&= (\frac{n+1}{2})(\frac{n-1}{2} - k_i) - k_i(\frac{n-1}{2} - k_i) \\
&= (\frac{n+1}{2} - k_i)(\frac{n-1}{2} - k_i) \\
&= m_i(m_i - 1) \quad [say \quad m_i = \frac{n+1}{2} - k_i]
\end{aligned}$$

If $\frac{n+1}{2} > k_i \Rightarrow m_i > 0 \Rightarrow m_i(m_i-1) \geq 0 \Rightarrow X_i \geq 0.$
If $\frac{n+1}{2} \leq k_i \Rightarrow m_i \leq 0 \Rightarrow m_i(m_i-1) \geq 0 \Rightarrow X_i \geq 0.$
Thus for $i = 1,2,3,4;$ $X_i \in \{m(m-1)\}_{m=1}^{\infty}.$
Conversely, let $m_i(m_i-1); i = 1,2,3,4$ be an integer solution of

$$X_1 + X_2 + X_3 + X_4 = n-1 \tag{16}$$

Then $\sum_{i=1}^{4} m_i(m_i-1) = n-1.$ We claim that for $i = 1,2,3,4;$ $m_i \leq \frac{n-1}{2}.$ If

not, suppose for some $i = 1, 2, 3, 4$; $m_i > \frac{n-1}{2} \Rightarrow m_i(m_i - 1) > \frac{n-1}{2}\frac{n+1}{2}$for $n \geq 3$. For $n = 1$, $X_1 = X_2 = X_3 = X_4 = 0$ is a solution of (16) and the corresponding solution of (15) is $w = x = y = z = 1$.
Now consider $k_i = \frac{n+1}{2} - m_i : i = 1, 2, 3, 4$.
Then

$$\begin{aligned}
\sum_{i=1}^{4} k_i(n - k_i) &= \sum_{i=1}^{4}(\frac{n+1}{2} - m_i)\{n - (\frac{n+1}{2} - m_i)\} \\
&= \sum_{i=1}^{4}(\frac{n+1}{2} - m_i)(\frac{n-1}{2} + m_i) \\
&= \sum_{i=1}^{4}\{(\frac{n+1}{2})(\frac{n-1}{2}) + m_i(\frac{n+1}{2} - \frac{n-1}{2}) - m_i^2\} \\
&= 4(\frac{n+1}{2})(\frac{n-1}{2}) - \sum_{i=1}^{4} m_i(m_i - 1) \\
&= (n+1)(n-1) - (n-1) \\
&= n(n-1).
\end{aligned}$$

So $k_i(n - k_i); i = 1, 2, 3, 4$ is a solution set of equation (15).

Example. For $n = 31$; the solutions of the equation

$$X_1 + X_2 + X_3 + X_4 = n - 1,$$

in $\{m(m+1)\}_{m=0}^{\infty}$ are given by
(i) $(12, 12, 6, 0)$, (ii) $(12, 6, 6, 6)$, (iii) $(30, 0, 0, 0)$ and (iv)$(20, 6, 2, 2)$. Using theorem (5.2) the corresponding solutions of

$$w(n - w) + x(n - x) + y(n - y) + z(n - z) = n(n - 1)$$

are (a) $(19, 19, 13, 15)$, (b) $(19, 13, 13, 13)$, (c) $(21, 15, 15, 15)$ and (d) $(11, 13, 17, 17)$ [taking all odd solutions] respectively. So possible size of part A_i of the H-partitions $(A_i, B_i); i = 1, 2, 3, 4$ are given by one of the solutions (a), (b), (c) and (d) only. Using these concepts the exhaustive search becomes quite easy as other sizes of H-partitions are disposed off.

Let us consider the solution (a) (19,19,13,15). By hit and trial we obtain

$$\begin{aligned} A_1 &= \{0,1,2,4,7,10,11,12,14,15,16,17,19,20,21,24,27,29,30\}, \\ A_2 &= \{0,4,5,8,9,10,11,12,14,15,16,17,19,20,21,22,23,26,27\}, \\ A_3 &= \{0,2,6,9,12,14,15,16,17,19,22,25,29\} \end{aligned}$$

and

$$A_4 = \{0,2,3,4,9,10,11,13,18,20,21,22,27,28,29\};$$

such that the frequencies $n_j^i; j = 1,2,\ldots,15; i = 1,2,3,4$ are as follows:

$$\begin{aligned} n_j^1 &= \{8,8,6,8,7,9,10,8,8,7,8,7,7,6,7\}, \\ n_j^2 &= \{6,9,8,5,5,7,8,8,8,8,8,7,10,9,8\}, \\ n_j^3 &= \{10,7,6,8,9,7,8,7,9,7,9,8,8,7,7\}, \\ n_j^4 &= \{7,7,11,10,10,8,5,8,6,9,6,9,6,9,9\}. \end{aligned}$$

Since $\sum_{i=1}^{4} n_j^i = 31$ for $j = 1,2,\ldots,15$, the conditions of the theorem (3.1) are satisfied by this set of four H-partitions and we have a set of four Williamson matrices giving rise to a Hadamard matrix of order 4×31.

If we consider the solution (a) $(19,13,13,13)$. By hit and trial we obtain

$$\begin{aligned} A_1 &= \{0,4,5,6,8,10,11,12,13,15,16,18,19,20,21,23,25,26,27\}, \\ A_2 &= \{0,1,2,3,7,9,14,17,22,24,28,29,30\}, \\ A_3 &= \{0,2,3,9,11,12,15,16,19,20,22,28,29\} \end{aligned}$$

and

$$A_4 = \{0,2,3,9,11,12,15,16,19,20,22,28,29\};$$

such that the frequencies $n_j^i; j = 1,2,\ldots,15; i = 1,2,3,4$ are as follows:

$$\begin{aligned} n_j^1 &= \{8,7,9,7,6,7,8,6,10,6,8,8,9,9,6\}, \\ n_j^2 &= \{7,6,8,8,7,8,7,7,9,7,9,9,10,8,7\}, \\ n_j^3 &= \{8,9,7,8,9,8,8,9,6,9,7,7,6,7,9\}, \\ n_j^4 &= \{8,9,7,8,9,8,8,9,6,9,7,7,6,7,9\}. \end{aligned}$$

Since $\sum_{i=1}^{4} n_j^i = 31$ for all $j = 1, 2, \ldots, 15$, the conditions of the theorem (3.1) are satisfied by this set of four H-partitions and we have a set of four Williamson matrices giving rise to a Hadamard matrix of order 4×31. Both of these are listed in [3].

Remark. It can be observed that the set of H-partitions which construct Williamson matrices also yields Supplementary Difference Sets [7, 8].

Acknowledgment

I am thankful to Dr. B.B.Bhattacharya, Department of Mathematics, Ranchi University, Ranchi for his valuable suggestions and comments which helped improve the presentation of the paper.

References

1. M. Hall, Jr., *Combinatorial Theory*, John Wiley and Sons, New York, 1986.

2. A. S. Hedayat, N. J. A. Sloane and J. Stufken, *Orthogonal Array, Theory and Application*, Springer Verlag, New York, 1999.

3. W. H. Holzmann, H. Kharaghani and B. Tayfeh-Rezaie, Williamson Matrices up to Order 59, *Design, Codes and Cryptography*, **46**(2008), No. 3, 343-352.

4. K. J. Horadam, *Hadamard Matrices and Their Application*, Princeton University Press, Princeton and Oxford, 2006.

5. B. Schmidt, Williamson Matrices and a conjecture of Ito's, *Des. Codes Crypto.*, **17** (1999), 61-68.

6. J. Williamson, Hadamard determinant theorem and the sum of four squares, *Duke Math. J.*, **11**(1944), 65-81.

7. J. S. Wallis, On supplementary difference sets, *Aequationes Math.*, **8** (1972), 242-257.

8. J. S. Wallis, *Some remarks on supplementary difference sets*, *Colloquia Mathematica Societatis janos Bolyai* 10*, Infinite and Finite Sets, Keszthely* (Hungury) (1973), 1503-1526.