Global Journal of Computer Science and Technology
Volume 11 Issue 8 Version 1.0 May 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
ISSN: 0975-4172 & Print ISSN: 0975-4350

Prolific Generation of Williamson Type Matrices

By M.K.Singh, Sandip Dutta, N C Mahanti

Abstract- A new method of generating Williamson type Matrices A, B, C, D is described such that
(i) A, B, C, D are symmetric.
(ii) A, B, C are circulant matrices and D is a back circulant matrix.
All such Williamsom type matrices of order n = 7, 9, 11, 13, 15, 17 are obtained by exhaustive computer search. The number of Williamson type Matrices constructed here is much greater than that of Williamson Matrices of same order. For example there are only 4 Williamson Matrices of order 17 but by our method we have obtained 504 Williamson type Matrices of order 17.

Keywords: Hadamard Matrices, Williamson & Williamson type Matrices, circulant and back circulant matrices, turnpike or partial digest problem.

GJCST Classification: *F.2.1, G.1.3*

Strictly as per the compliance and regulations of:

Prolific Generation of Williamson Type Matrices

M.K.Singh, Sandip Dutta, N C Mahanti

Abstract- A new method of generating Williamson type Matrices A, B, C, D is described such that
(i) A, B, C, D are symmetric.
(ii) A, B, C are circulant matrices and D is a back circulant matrix.
All such Williamsom type matrices of order n = 7, 9, 11, 13, 15, 17 are obtained by exhaustive computer search. The number of Williamson type Matrices constructed here is much greater than that of Williamson Matrices of same order. For example there are only 4 Williamson Matrices of order 17 but by our method we have obtained 504 Williamson type Matrices of order 17.

Index Terms- Hadamard Matrices, Williamson & Williamson type Matrices, circulant and back circulant matrices, turnpike or partial digest problem.

I. Introduction

We recall the following definitions from Craigen and Kharaghani [1].

1.1 Hadamard Matrix [or H-Matrix] : An n x n (+1, -1) matrix H is a Hadamard matrix if $HH^T = nI_n$.

It is conjectured that an H-matrix exists for every order n = 4t where t is a positive integer.

1.2 Amicable matrices : Two matrices X and Y are called amicable, if $XY^T = YX^T$.

1.3 Circulant matrix : circ(a_1, a_2, ...a_n) is the matrix

$$\begin{bmatrix} a_1 & a_2 & .. & a_{n-1} & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \cdots & a_{n-2} \\ .. & .. & .. & .. & .. \\ a_2 & a_3 & .. & .. & a_1 \end{bmatrix}$$

called circulant matrix.

1.4 Back circulant matrix : bcirc(a_1, a_2, ...a_n) is the matrix

$$\begin{bmatrix} a_1 & a_2 & .. & a_{n-1} & a_n \\ a_2 & a_3 & .. & a_n & a_1 \\ a_3 & a_4 & .. & a_1 & a_2 \\ .. & .. & .. & .. & .. \\ a_n & a_1 & .. & .. & a_{n-1} \end{bmatrix}$$

called back circulant matrix.

Back circulant bcirc (0 0 .... 0 1) is called back diagonal matrix.

1.5 Matrics used in the construction of H-Matrices : n x n (+1, -1) matrices A, B, C, D satisfying

$$AA^T + BB^T + CC^T + DD^T = 4nI_n \quad (1)$$

Are

(i) Williamson Matrices if they are symmetric and circulant.

(ii) Goethals Seidel type matrices if they are circulant but not necessarily symmetric.

(iii) Williamson type matrices if they are pairwise amicable. vide [1]

1.5 Matrics used in the construction of H-Matrices : n x n (+1, -1) matrices A, B, C, D satisfying

$$AA^T + BB^T + CC^T + DD^T = 4nI_n \quad (1)$$

are

(i) Williamson Matrices if they are symmetric and circulant.

(ii) Goethals Seidel type matrices if they are circulant but not necessarily symmetric.

(iii) Williamson type matrices if they are pairwise amicable.

vide [1]

1.6 Orthogonal Design OD (4t, t, t, t, t): OD (4t, t, t, t, t) is an orthogonal design of order 4t and type (t, t, t, t), t is a +ve integer, which is defined as an 4t x 4t matrix with entries ±A, ±B, ±C, ±D (A,B,C,D are commuting indeterminates) satisfying

$$XX^T = t(A^2+B^2+C^2+D^2)I_{4t}$$

For details vide Geramita and Seberry [2]

II. Previous Work

If A,B,C,D are Williamson or Williamson type Matrices then the H-matrix, H can be constructed as

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

Originally Williamson[3] constructed Williamson matrices for m ≤ 21, m=25, 37, 43. Baumert, Golomb and Hall[4] constructed Williamson matrix for m = 23. Baumert and Hall[5] found all solutions for 3 ≤ m ≤ 23 and some solutions

for m =25, 27, 37, 43. For details of the solutions vide Hall[6]. Baumert[7] gave one solution for m = 29. Koukouvinos and Kounians[8] made exhaustive search for all Williamson atrices of order 33.

Williamson type martrices have been constructed by Seberry [9], [10] & Whiteman [11].

If A, B, C, D are circulant matrices satisfying equation (1) then H-matrix G can be obtained as the Goethals & Seidel array [12]

$$G = \begin{bmatrix} A & -BR & -CR & -DR \\ BR & A & -D^TR & C^TR \\ CR & DR & A & -BR \\ DR & -CR & BR & A \end{bmatrix}$$

Where R is a (0,1) –back diagonal matrix.

A Quadruple of Williamson type matrices A,B,C,D has advantage over other Quadruples used to construct H-matrices. The following lemma of Baumert and Hall [vide Colbourn & Dimtz[13] shows that from a quadruple(A,B,C,D) of Williamson type matrices. Several Hadamard matrices can be constructed.

Lemma 1: The existence of orthogonal design OD(4t; t,t,t,t) and four Williamson type matrices of order n implies the existence of H-matrices of order 4nt. Though it is generally conjectured that the above OD exists for all t, the existence is known for $t \leq 73$ (vide Colbourn and Dinitz ([14] p295).

III. Methodology

3.1 Some basic facts: We will begin with the following (new) definitions: (we assume that n is an odd positive integer)

(i) Input Set

A set $S_k=\{n_1, n_2, \ldots\ldots n_k\}$ of inergers where $0 < n_i < n$, k is even, will be called an input set. The input set S_k will be called symmetric if $n_i \epsilon S_k \rightarrow n - n_i \epsilon S_k$

(ii) Output Vector

Let m = (n-1)/2. Let S_k be an input set defined above

Let $S_k + j = \{ n_{1+j}, n_{2+j}, \ldots\ldots n_{k+j}\}$, where + stands for addition mod n.

Let $r_j = |S_{k+j} - S_k|$ the order of the set $(S_{k+j}) - S_k$ ——— (1)

and $e_j= n - 4r_j$, j = 1, 2, 3 ....m ———— (2)

Binary reprentation of S_k:

row vector $b_k = (a_1, a_2, \ldots \ldots a_n\text{-}1)$ will be called binary representation vector ((BR)-vector) of S_k if a_i= -1 if $i \epsilon S_k$ & a_i= +1, otherwise

3.2 Method of Construction

Step-I Generation of size vector

First construct 4-vector $(k_1, k_2, k_3; k_4)$ which consists of feasible sizes of the four input sets as follows

Express 4n as $4n = n_1^2 + n_2^2 + n_3^2 + n_4^2$

where n_i are odd integers. [This is always possible]

let $m_i = (n - n_i)/2$ and $k_i= m_i$ or $n - m_i$ according as m_i is even or odd i = 1, 2, 3

Let $k_4= (n - n_4)/2$ or $(n + n_4)/2$

The vector $(k_1, k_2, k_3; k_4)$ will be called size vector for an input set.

Step-II Generation of input sets

(a) Three symmetric input sets S_{k1}, S_{k2}, S_{k3} of size k_1, k_2, k_3 respectively.

Let $k \epsilon \{k_1, k_2, k_3\}$. Generate all (k/2) - subsets of the set {1,2,3,........m}. From each (k/2)-subset $S_{k/2}= (n_1, n_2, \ldots\ldots n_{k/2})$ obtain a k-subset S_k by adjoining k/2 new elements $n - n_i$, i = 1, 2, ... k/2

(b) One input set S_{k4} of size k_4 obtain all k_4 - subsets of the set (1, 2, ... (n-1))

Step-III Generation of binary vectors and output vectors

Let $k \epsilon \{k_1, k_2, k_3, k_4\}$

For each input set Sk obtained in Step-II form its binary vector bk and the output vector vk and record all correspondences $S_k \rightarrow b_k \rightarrow v_k$

Step-IV Sum of output vectors corresponding to three symmetric input sets

Form the set $S = \{s=(s_1, s_2, s_3, \ldots\ldots s_m) : s$ is the sum of triplets of output vectors corresponding to symmetric input sets S_{k1}, S_{k2}, S_{k3} obtained in Step II (a) Omit all vectors ϵ S

for which $|si| \geq n - 2$. Let S' be the resulting set. Also record

the correspondences $(S_{k1}, S_{k2}, S_{k3}) \rightarrow s \epsilon S'$.

Step-V Set of output vectors corresponding to S_{k4}

Form the set T of output vectors $t = (t_1, t_2, t_3, \ldots\ldots t_m)$ of S_{k4} obtained in Step II (b)

Let $T' = \{-t = (-t_1, -t_2, -t_3, \ldots\ldots -t_m)\}$

Record all correspondences $S_{k4} \rightarrow -t$

Step-VI Construction of four Williamson type matrices A, B, C, D

Corresponding to each vector $\in S' \cap T'$, there is a set of four Williamson type matrices (A, B, C, D) which can be obtained as follows:

Find $s = -t \in S \cap T'$ .... (4)

Find the corresponding (S_{k1}, S_{k2}, S_{k3}) & S_{k4} through the correspondences in Step IV & Step V

Next find the binary vectors b_{k1}, b_{k2}, b_{k3}, b_{k4} corresponding to input sets S_{k1}, S_{k2}, S_{k3} & S_{k4} obtained in step VI by means of the correspondences in Step-III. Form circulant matrices A, B, C whose 1st rows are b_{k1}, b_{k2}, b_{k3} respectively and back circulant one D whose 1st row is bk4 . Then A, B, C, D are required Williamson type matrics.

Step-VII Exhaustive search for A, B, C, D For exhaustive search repeat the preceding process for all possible size vector (k_1, k_2 , k_3; k_4).

Remark: We can get rid of Step II(b), Step-V and Step-VI by replacing them by the following single step to obtain S_{k4}.

Step Use of Turnpike problem Form the set T consisting of t = ($-s_1$, $-s_2$. . . $-s_m$) satisfying (s_1, s_2, ...s_m) ∈ S' (constructed in Step IV)

Record the correspondences t → s → {A, B, C} using the correspondences s → {A, B, C}

For the vector $t = (-s_1, -s_2, \ldots\ldots -s_m) \in T$

(i) Find $k_4 = (n - \sqrt{n - 2(s_1 + s_2 + \ldots\ldots + s_m)}) / 2$

(ii) Find $f_i = (4k_4 - n - s_i) / 4$ where i = 1, 2, ... m

(iii) Form a set $D_1 = \{d_1, d_2, \ldots\ldots d_k\}$, $d_i \in \{1, 2, \ldots. m\}$ and a multiset M of differences dj - di (mod n) of every pair of distinct elements of D_1 such that

(a) Differences are between 0 and m, (if a difference is <- m, then replace it by n - m).

(b) In the multiset M of differences obtained in (a) i appears f_i times i = 1, 2, 3, ... m, where f_i are numbers defined in (ii)

t ∈ T will be called feasible vector, if the set D_1 defined in (iii) exists. Each feasible t ∈ T will give Williamson type matrices A, B, C, D which can be obtained as follows

Circulant A, B, C can be obtained through the correspondence : feasible t →s → {A, B, C} using the correspondence in Step-IV.

The back circulant matrix D can be obtained as follows :

(iv) if $D_1 = (d_1, d_2, \ldots\ldots d_k)$ is the set corresponding to t, then form a back circulant matrix D where first row contains -1 at d_1^{th}, d_2^{th}, ... d_k^{th} place and +1 elsewhere.

Remark : Step-(iii) is equivalent to turnpike or partial digest problem (vide [15], [16], [17], [18]). Using the method described above, we have obtained all Williamson type matrices of order 9,11,13,15 & 17 by exhaustive computing search.

IV. RESULTS

Williamson type matrices of order 9

Type - I ($4 \times 9 = 1^2 + 1^2 + 3^2 + 5^2$) Subtype - I (Size Vector (4, 2, 6; 4))

Sl.no	Input Set		Set of Williamson type Matrices	Output Vector
1	{3,6}	A	circ (1 1 1 -1 1 1 -1 1 1)	1 1 5 1
	{1,4,5,8}	B	circ (1 -1 1 1 -1 -1 1 1 -1)	-3 -3 1 1
	{2,3,4,5,6,7}	C	circ (1 1 -1 -1 -1 -1 -1 -1 1)	5 1 -3 -3
	{3,5,7,8}	D	circ (1 1 1 -1 1 -1 1 -1 -1)	-3 1 -3 1
2	{3,6}	A	circ (1 1 1 -1 1 1 -1 1 1)	1 1 5 1
	{1,2,7,8}	B	circ (1 -1 -1 1 1 1 1 -1 -1)	1 -3 1 -3
	{1,3,4,5,6,8}	C	circ (1 -1 1 -1 -1 -1 -1 1 -1)	-3 5 -3 1
	{3,6,7,8}	D	circ (1 1 1 -1 1 1 -1 -1 -1)	1 -3 -3 1
3	{3,6}	A	circ (1 1 1 -1 1 1 -1 1 1)	1 1 5 1
	{2,4,5,7}	B	circ (1 1 -1 1 -1 -1 1 -1 1 1)	-3 1 1 -3
	{1,2,3,6,7,8}	C	circ (1 -1 -1 -1 1 1 -1 -1 -1)	1 -3 -3 5
	{4,6,7,8}	D	circ (1 1 1 1 -1 1 -1 -1 -1)	1 1 -3 -3

Subtype- II (Size Vector (2, 4, 4; 3))

Sl.no	Input Set		Set of Williamson type Matrices	Output Vector
1	{2,7}	A	circ (1 1 -1 1 1 1 1 -1 1)	1 1 1 5
	{1,4,5,8}	B	circ (1 -1 1 1 -1 -1 1 1 -1)	-3 -3 1 1
	{3,4,5,6}	C	circ (1 1 1 -1 -1 -1 -1 1 1)	5 1 -3 -7
	{3,6,8}	D	circ (1 1 1 -1 1 1 -1 1 -1)	-3 1 1 1
2	{4,5}	A	circ (1 1 1 1 -1 -1 1 1 1)	5 1 1 1
	{1,3,6,8}	B	circ (1 -1 1 -1 1 1 -1 1 -1)	-7 5 -3 1
	{1,2,7,8}	C	circ (1 -1 -1 1 1 1 1 -1 -1)	1 -3 1 -3
	{4,7,8}	D	circ (1 1 1 1 -1 1 1 -1 -1)	1 -3 1 1
3	{1,8}	A	circ (1 -1 1 1 1 1 1 1 -1)	1 5 1 1
	{2,4,5,7}	B	circ (1 1 -1 1 -1 -1 1 -1 1)	-3 1 1 -3
	{2,3,6,7}	C	circ (1 1 -1 -1 1 1 -1 -1 1)	1 -7 -3 5
	{5,7,8}	D	circ (1 1 1 1 1 -1 1 -1 1)	1 1 1 -3

Global Journal of Computer Science and Technology Volume XI Issue VIII Version I May 2011

Table II WILLIMASON TYPE MATRICE OF ORDER 11

Type - I ($4 \times 11 = 1^2 + 3^2 + 3^2 + 5^2$)
Subtype-1 (Size Vector (4, 6, 8; 4)

Sl.no	Input Set		Set of Williamson type Matrices	Output Vector
1	{3,5,6,8}	A	circ (1 1 1 -1 1 -1 -1 1 -1 1 1)	-1 3 3 -5 -1
	{1,2,3,8,9,10}	B	circ (1 -1 -1 -1 1 1 1 1 -1 -1 -1)	3 -1 -5 -1 -1
	{1,2,3,5,6,8,9,10}	C	circ (1 -1 -1 -1 1 -1 -1 1 -1 -1 -1)	-1 -1 3 7 -1
	{4,6,9,10}	D	circ (1 1 1 1 -1 1 -1 1 1 -1 -1)	-1 -1 -1 -1 3
2	{2,4,7,9}	A	circ (1 1 -1 1 -1 1 1 -1 1 -1 1)	-5 3 -1 -1 3
	{2,3,5,6,8,9}	B	circ (1 1 -1 -1 1 -1 -1 1 -1 -1 1)	-1 -5 3 -1 -1
	{2,3,4,5,6,7,8,9}	C	circ (1 1 -1 -1 -1 -1 -1 -1 -1 -1 1)	7 3 -1 -1 -1
	{3,7,9,10}	D	circ (1 1 1 -1 1 1 1 -1 1 -1 -1)	-1 -1 -1 3 -1
3	{3,4,7,8}	A	circ (1 1 1 -1 -1 1 1 -1 -1 1 1)	3 -5 -1 3 -1
	{1,4,5,6,7,10}	B	circ (1 -1 1 1 -1 -1 -1 -1 1 1 -1)	-1 -1 -1 -5 -3
	{1,3,4,5,6,7,8,10}	C	circ (1 -1 1 -1 -1 -1 -1 -1 -1 1 -1)	-1 7 -1 3 -1
	{4,7,8,10}	D	circ (1 1 1 1 -1 1 1 -1 -1 1 -1)	-1 -1 3 -1 -1
4	{1,2,9,10}	A	circ (1 -1 -1 1 1 1 1 1 1 -1 -1)	3 -1 3 -1 -5
	{1,3,4,7,8,10}	B	circ (1 -1 1 -1 -1 1 1 -1 -1 1 -1)	-5 -1 -1 3 -1
	{1,2,3,4,7,8,9,10}	C	circ (1 -1 -1 -1 -1 1 1 -1 -1 -1 -1)	3 -1 -1 -1 7
	{5,7,9,10}	D	circ (1 1 1 1 1 -1 1 -1 1 -1 -1)	-1 3 -1 -1 -1
5	{1,5,6,10}	A	circ (1 -1 1 1 1 -1 -1 1 1 1 -1)	-1 -1 -5 3 3
	{2,4,5,6,7,9}	B	circ (1 1 -1 1 -1 -1 -1 -1 1 -1 1)	-1 3 -1 -1 -5
	{1,2,4,5,6,7,9,10}	C	circ (1 -1 -1 1 -1 -1 -1 -1 1 -1 -1)	-1 -1 7 -1 3
	{5,8,9,10}	D	circ (1 1 1 1 1 -1 1 1 -1 -1 -1)	3 -1 -1 -1 -1

Table III WILLIMASON TYPE MATRICES OF ORDER 11

Subtype- II (Size Vector (4, 4, 8; 5))

Sl.no	Input Set		Set of Williamson type Matrices	Output Vector
1	{1,5,6,10}	A	circ (1 -1 1 1 1 -1 -1 1 1 1 -1)	-1 -1 -5 3 3
	{4,5,6,7}	B	circ (1 1 1 1 -1 -1 -1 -1 1 1 1)	7 3 -1 -5 -5
	{1,2,3,5,6,8,9,10}	C	circ (1 -1 -1 -1 1 -1 -1 1 -1 -1 -1)	-1 -1 3 7 -1
	{2,4,7,9,10}	D	circ (1 1 -1 1 -1 1 1 -1 1 -1 -1)	-5 -1 3 -5 3
2	{2,4,7,9}	A	circ (1 1 -1 1 -1 1 1 -1 1 -1 1)	-5 3 -1 -1 3
	{3,4,7,8}	B	circ (1 1 1 -1 -1 1 1 -1 -1 1 1)	3 -5 -1 3 -1
	{2,3,4,5,6,7,8,9}	C	circ (1 1 -1 -1 -1 -1 -1 -1 -1 -1 1)	7 3 -1 -1 -1
	{3,6,8,9,10}	D	circ (1 1 1 -1 1 1 -1 1 -1 -1 -1)	-5 -1 3 -1 -1
3	{2,3,8,9}	A	circ (1 1 -1 -1 1 1 1 1 -1 -1 1)	3 -5 -5 -1 7
	{1,2,9,10}	B	circ (1 -1 -1 1 1 1 1 1 1 -1 -1)	3 -1 3 -1 -5
	{1,3,4,5,6,7,8,10}	C	circ (1 -1 1 -1 -1 -1 -1 -1 -1 1 -1)	-1 7 -1 3 -1
	{3,6,8,9,10}	D	circ (1 1 1 -1 1 1 -1 1 -1 -1 -1)	-5 -1 3 -1 -1
4	{1,4,7,10}	A	circ (1 -1 1 1 -1 1 1 -1 1 1 -1)	-5 -1 7 -5 3
	{3,4,7,8}	B	circ (1 1 1 -1 -1 1 1 -1 -1 1 1)	3 -5 -1 3 -1
	{2,3,4,5,6,7,8,9}	C	circ (1 1 -1 -1 -1 -1 -1 -1 -1 -1 1)	7 3 -1 -1 -1
	{3,5,7,9,10}	D	circ (1 1 1 -1 1 -1 1 -1 1 -1 -1)	-5 3 -5 3 -1
5	{2,4,7,9}	A	circ (1 1 -1 1 -1 1 1 -1 1 -1 1)	-5 3 -1 -1 3
	{4,5,6,7}	B	circ (1 1 1 1 -1 -1 -1 -1 1 1 1)	7 3 -1 -5 -5
	{1,2,3,5,6,8,9,10}	C	circ (1 -1 -1 -1 1 -1 -1 1 -1 -1 -1)	-1 -1 3 7 -1
	{3,4,7,9,10}	D	circ (1 1 1 -1 -1 1 1 -1 1 -1 -1)	-1 -5 -1 -1 3

6	{3,5,6,8)	A	circ (1 1 1 -1 1 -1 -1 1 -1 1 1)	-1 3 3 -5 -1
	{3,4,7,8}	B	circ (1 1 1 -1 -1 1 1 -1 -1 1 1)	3 5 -1 3 -1
	{1,3,4,5,6,7,8,10}	C	circ (1 -1 1 -1 -1 -1 -1 -1 -1 1 -1)	-1 7 -1 3 -1
	{3,4,7,9,10}	D	circ (1 1 1 -1 -1 1 1 -1 1 -1 -1)	-1 -5 -1 -1 3
7	{3,5,6,8}	A	circ (1 1 1 -1 1 -1 -1 1 -1 1 1)	-1 3 3 -5 -1
	{2,3,8,9}	B	circ (1 1 -1 -1 1 1 1 1 -1 -1 1)	3 -5 -5 -1 7
	{1,3,4,5,6,7,8,10}	C	circ (1 -1 1 -1 -1 -1 -1 -1 -1 1 -1)	-1 7 -1 3 -1
	{3,6,7,9,10}	D	circ (1 1 1 -1 1 1 -1 -1 1 -1 -1)	-1 -5 3 3 -5
8	{1,4,7,10}	A	circ (1 -1 1 1 -1 1 1 -1 1 1 -1)	-5 -1 7 -5 3
	{1,5,6,10}	B	circ (1 -1 1 1 1 -1 -1 1 1 1 -1)	-1 -1 -5 3 3
	{2,3,4,5,6,7,8,9}	C	circ (1 1 -1 -1 -1 -1 -1 -1 -1 -1 1)	7 3 -1 -1 -1
	{3,6,7,8,10}	D	circ (1 1 1 -1 1 1 -1 -1 -1 1 -1)	-1 -1 -1 3 -5
9	{2,4,7,9}	A	circ (1 1 -1 1 -1 1 1 -1 1 -1 1)	-5 3 -1 -1 3
	{1,2,9,10}	B	circ (1 -1 -1 1 1 1 1 1 1 -1 -1)	3 -1 3 -1 -5
	{1,2,3,4,7,8,9,10}	C	circ (1 -1 -1 -1 -1 1 1 -1 -1 -1 -1)	3 -1 -1 -1 7
	{3,6,7,8,10}	D	circ (1 1 1 -1 1 1 -1 -1 -1 1 -1)	-1 -1 -1 3 -5
10	{2,5,6,9}	A	circ (1 1 -1 1 1 -1 -1 1 1 -1 1)	-1 -5 3 7 -5
	{3,5,6,8}	B	circ (1 1 1 -1 1 -1 -1 1 -1 1 1)	-1 3 3 -5 -1
	{1,2,3,4,7,8,9,10}	C	circ (1 -1 -1 -1 -1 1 1 -1 -1 -1 -1)	3 -1 -1 -1 7
	{4,6,8,9,10}	D	circ (1 1 1 1 -1 1 -1 1 -1 -1 -1)	-1 3 -5 -1 -1
11	{1,5,6,10}	A	circ (1 -1 1 1 1 -1 -1 1 1 1 -1)	-1 -1 -5 3 3
	{1,2,9,10}	B	circ (1 -1 -1 1 1 1 1 1 1 -1 -1)	3 -1 3 -1 -5
	{1,2,4,5,6,7,9,10}	C	circ (1 -1 -1 1 -1 -1 -1 -1 1 -1 -1)	-1 -1 7 -1 3
	{4,6,8,9,10}	D	circ (1 1 1 1 -1 1 -1 1 -1 -1 -1)	-1 3 -5 -1 -1
12	{1,3,8,10}	A	circ (1 -1 1 -1 1 1 1 1 -1 1 -1)	-5 7 -5 3 -1
	{1,2,9,10}	B	circ (1 -1 -1 1 1 1 1 1 1 1 -1 -1)	3 -1 3 -1 -5
	{1,2,4,5,6,7,9,10}	C	circ (1 -1 -1 1 -1 -1 -1 -1 1 -1 -1)	-1 -1 7 -1 3
	{4,5,8,9,10}	D	circ (1 1 1 1 -1 -1 1 1 -1 -1 -1)	3 -5 -5 -1 3
13	{1,3,8,10}	A	circ (1 -1 1 -1 1 1 1 1 -1 1 -1)	-5 7 -5 3 -1
	{3,4,7,8}	B	circ (1 1 1 -1 -1 1 1 -1 -1 1 1)	3 -5 -1 3 -1
	{1,2,4,5,6,7,9,10}	C	circ (1 -1 -1 1 -1 -1 -1 -1 1 -1 -1)	-1 -1 7 -1 3
	{4,7,8,9,10}	D	circ (1 1 1 1 -1 1 1 -1 -1 -1 -1)	3 -1 -1 -5 -1
14	{1,5,6,10}	A	circ (1 -1 1 1 1 -1 -1 1 1 1 -1)	-1 -1 -5 3 3
	{3,5,6,8}	B	circ (1 1 1 -1 1 -1 -1 1 -1 1 1)	-1 3 3 -5 -1
	{1,2,3,5,6,8,9,10}	C	circ (1 -1 -1 -1 1 -1 -1 1 -1 -1 -1)	-1 -1 3 7 -1
	{4,7,8,9,10}	D	circ (1 1 1 1 -1 1 1 -1 -1 -1 -1)	3 -1 -1 -5 -1
15	{2,4,7,9}	A	circ (1 1 -1 1 -1 1 1 -1 1 -1 1)	-5 3 -1 -1 3
	{2,5,6,9}	B	circ (1 1 -1 1 1 -1 -1 1 1 -1 1)	-1 -5 3 7 -5
	{1,2,3,4,7,8,9,10}	C	circ (1 -1 -1 -1 -1 1 1 -1 -1 -1 -1)	3 -1 -1 -1 7
	{5,7,8,9,10}	D	circ (1 1 1 1 1 -1 1 -1 -1 -1 -1)	3 3 -1 -5 -5

Table IV WILLIAMSON TYPE MATRICES OF ORDER 13

Type - I (4 x 13 = $1^2 + 1^2 + 1^2 + 7^2$)
Subtype- I (Size Vector (6, 6, 10; 6))

Sl.no	Input Set		Set of Williamson type Matrices	Output Vector
1	{1,2,6,7,11,12}	A	circ (1 -1 -1 1 1 1 -1 -1 1 1 1 -1 -1)	1 -7 -3 1 5 -3
	{3,5,6,7,8,10}	B	circ (1 1 1 -1 1 -1 -1 -1 -1 1 -1 1 1)	1 5 1 -3 -3 -7
	{1,2,3,4,5,8,9,10,11,12}	C	circ (1 -1 -1 -1 -1 -1 1 1 -1 -1 -1 -1 -1)	5 1 1 1 1 9
	{2,5,7,9,11,12}	D	circ (1 1 -1 1 1 -1 1 -1 1 -1 1 -1 -1)	-7 1 1 1 -3 1

Global Journal of Computer Science and Technology Volume XI Issue VIII Version I May 2011

Type - II (4 x 13 = $1^2 + 1^2 + 5^2 + 5^2$)
Subtype- I (Size Vector (4, 4, 6; 6))

Sl.no	Input Set		Set of Williamson type Matrices	Output Vector
1	{1,5,8,12}	A	circ (1 -1 1 1 1 -1 1 1 -1 1 1 1 -1)	-3 1 1 5 -3 5
	{5,6,7,8}	B	circ (1 1 1 1 1 -1 -1 -1 -1 1 1 1 1)	9 5 1 -3 -3 -3
	{1,2,6,7,11,12}	C	circ (1 -1 -1 1 1 1 -1 -1 1 1 1 -1 -1)	1 -7 -3 1 5 -3
	{2,4,6,9,11,12}	D	circ (1 1 -1 1 -1 1 -1 1 1 -1 1 -1 -1)	-7 1 1 -3 1 1

Type - III (4 x 13 = $3^2 + 3^2 + 3^2 + 5^2$)
Subtype- I (Size Vector (8, 8, 8; 4))

Sl.no	Input Set		Set of Williamson type Matrices	Output Vector
1	{1,3,4,6,7,9,10,12}	A	circ(1 -1 1 -1 -1 1 -1 -1 1 -1 -1 1 -1)	-7 1 5 -3 1 1
	{2,3,4,6,7,9,10,11}	B	circ(1 1 -1 -1 -1 1 -1 -1 1 -1 -1 -1 1)	1 -3 -3 1 1 1
	{2,3,4,6,7,9,10,11}	C	circ(1 1 -1 -1 -1 1 -1 -1 1 -1 -1 -1 1)	1 -3 -3 1 1 1
	(8,10,11,12}	D	circ(1 1 1 1 1 1 1 -1 1 -1 -1 -1)	5 5 1 1 -3 -3

Table V WILLIAMSON TYPE MATRICES OF ORDER 15

Type - I (4 x 15 = $1^2 + 3^2 + 5^2 + 5^2$)
Subtype- I (Size Vector (6, 10, 10; 7))

Sl.no	Input Set		Set of Williamson type Matrices	Output Vector
1	{1,2,5,10,13,14}	A	circ (1 -1 -1 1 1 -1 1 1 1 1 -1 1 1 -1 -1)	-1 -5 7 3 -5 -1 -1
	{2,3,4,6,7,8,9,11,12,13}	B	circ (1 1 -1 -1 -1 1 -1 -1 -1 -1 1 -1 -1 -1 1)	1 -7 -3 1 5 -3
	{1,2,3,4,5,10,11,12,13,14}	C	circ (1 -1 -1 -1 -1 -1 1 1 1 1 -1 -1 -1 -1 -1)	7 3 -1 -5 -5 3 3
	{2,4,6,9,11,13,14}	D	circ (1 1 -1 1 -1 1 -1 1 1 -1 1 -1 1 -1 -1)	-9 3 -1 -1 3 -5 3

Type - II (4 x 15 = $1^2 + 1^2 + 3^2 + 7^2$)
Subtype- I (Size Vector (6, 8, 8; 4))

Sl.no	Input Set		Set of Williamson type Matrices	Output Vector
1	{2,4,7,8,11,13}	A	circ (1 1 -1 1 -1 1 1 -1 -1 1 1 -1 1 -1 1)	-5 -1 -1 3 -1 7 -5
	{1,2,6,7,8,9,13,14}	B	circ (1 -1 -1 1 1 1 -1 -1 -1 -1 1 1 1 -1 -1)	3 -5 -5 -5 -1 -1 7
	{3,4,6,7,8,9,11,12	C	circ (1 1 1 -1 -1 1 -1 -1 -1 -1 1 -1 -1 1 1)	3 -1 3 -1 -1 -5 -5
	{7,10,12,14}	D	circ (1 1 1 1 1 1 1 -1 1 1 -1 1 -1 1 -1)	-1 7 3 3 3 -1 3

Table VI WILLIAMSON TYPE MATRICES OF ORDER 17

Type - I (4 x 17 = $1^2 + 3^2 + 3^2 + 7^2$)
Subtype- I (Size Vector (8, 10, 10; 5))

Sl. no	Input Set		Set of Williamson type Matrices	Output Vector
1	{1,5,7,8,9,10,12,16}	A	circ(1 -1 1 1 1 -1 1 -1 -1 -1 -1 1 -1 1 1 1 -1)	-3 5 -3 1 -7 1 -3 1
	{1,2,3,6,8,9,11,14,15,16}	B	circ (1 -1 -1 -1 1 1 -1 1 -1 -1 1 -1 1 1 -1 -1 -1)	-3 -3 1 -3 5 -3 1 1
	{1,2 ,4,5,6,11,12,13,15,6}	C	circ(1 -1 -1 1 -1 -1 -1 1 1 1 1 -1 -1 -1 1 -1 -1)	1 -3 1 -3 -3 1 5 -3
	{2,6,7,8,11}	D	circ(1 1 -1 1 1 1 -1 -1 -1 1 1 -1 1 1 1 1 1)	5 1 1 5 5 1 -3 1

Type - II (4 x 17 = $3^2 + 3^2 + 5^2 + 5^2$)
Subtype- I (Size Vector (6, 10, 10; 11))

Sl. no	Input Set		Set of Williamson type Matrices	Output Vector

1	{2,6,8,9,11,15}	A	circ(1 1 -1 1 1 1 -1 1 -1 -1 1 -1 1 1 1 -1 1)	-3 1 1 5 -3 1 1 1
	{1,3,4,7,8,9,10,13,14,16}	B	circ (1 -1 1 -1 -1 1 1 -1 -1 -1 -1 1 1 -1 -1 1 -1)	-3 -3 -3 1 1 5 1 -3
	{1,2,3,6,8,9,11,14,15,16}	C	circ(1 -1 -1 -1 1 1 -1 1 -1 -1 1 -1 1 1 -1 -1 -1)	-3 -3 1 -3 5 -3 1 1
	{2,3,4,5,7,8,9,10,11,12,13}	D	circ(1 1 -1 -1 -1 -1 1 -1 -1 -1 -1 -1 -1 -1 1 1 1)	9 5 1 -3 -3 -3 -3 1

Subtype- II (Size Vector (6, 6, 10; 7))

Sl. no	Input Set		Set of Williamson type Matrices	Output Vector
1	{1,4,8,9,13,16}	A	circ (1 -1 1 1 -1 1 1 1 -1 -1 1 1 1 -1 1 1 -1)	-3 -3 1 1 9 -7 1 5
	{1,3,8,9,14,16}	B	circ(1 -1 1 -1 1 1 1 1 -1 -1 1 1 1 1 -1 1 -1)	-3 5 -7 1 1 5 1 1
	{1,2,3,4,5,12,13,14,15,16}	C	circ(1 -1 -1 -1 -1 -1 1 1 1 1 1 1 -1 -1 -1 -1 -1)	9 5 1 -3 -7 -3 -3 -3
	{2,6,7,10,12,13,16}	D	circ(1 1 -1 1 1 1 -1 -1 1 1 -1 1 -1 -1 1 1 -1)	-3 -7 5 1 -3 5 1 -3

Subtype- III (Size Vector (6, 10,10; 6))

Sl.no	Input Set		Set of Williamson type Matrices	Output Vector
1	{3,5,8,9,12,14}	A	circ(1 1 1 -1 1 -1 1 1 -1 -1 1 1 -1 1 -1 1 1)	-3 1 1 1 1 5 -3 1
	{1,2,3,6,8,9,11,14,15,16}	B	circ(1 -1 -1 -1 1 1 -1 1 -1 -1 1 -1 1 1 -1 -1 -1)	-3 -3 1 -3 5 -3 1 1
	{1,5,6,7,8,9,10,11,12,16}	C	circ(1 -1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1)	5 5 -3 1 -3 1 -3 -7
	{2,6,7,9,15,16}	D	circ(1 1 -1 1 1 1 -1 -1 1 -1 1 1 1 1 1 -1 -1)	1 -3 1 1 -3 -3 5 5

Subtype- IV (Size Vector (10,10, 12; 8))

Sl. no	Input Set		Set of Williamson type Matrices	Output Vector
1	{1,3,4,7,8,9,10,13,14,16}	A	circ (1 -1 1 -1 -1 1 1 -1 -1 -1 -1 1 1 -1 -1 1 -1)	-3 -3 -3 1 1 5 1 -3
	{3,4,5,6,8,9,11,12,13,14}	B	circ(1 1 1 -1 -1 -1 -1 1 -1 -1 1 -1 -1 -1 -1 1 1)	5 1 1 -7 -3 -3 -3 5
	{2,3,5,6,7,8,9,10,11,12,14,15}	C	circ(1 1 -1 -1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 -1 -1 1)	5 1 5 5 5 -3 -3 1
	{3,4,6,8,10,13,14,16}	D	circ(1 1 1 -1 -1 1 -1 1 -1 1 -1 1 1 -1 -1 1 -1)	-7 1 -3 1 -3 1 5 -3

Table VII WILLIAMSON TYPE MATRICES OF ORDER 19

Type - I ($4 \times 19 = 1^2 + 5^2 + 5^2 + 5^2$)
Subtype- I (Size Vector (8, 8, 8; 6))

Sl. no	Input Set		Set of Williamson type Matrices	Output Vector
1	{1,4,8,9,10,11,15,18}	A	circ (1 -1 1 1 -1 1 1 1 -1 -1 -1 -1 1 1 1 -1 1 1 -1)	-1 -1 -1 -5 3 -5 3 -1 3
	{1,6,7,9,10,12,13,18}	B	circ(1 -1 1 1 1 1 -1 -1 1 -1 -1 1 -1 -1 1 1 1 1 -1)	-1 -1 3 -5 -1 3 -1 3 -5
	{3,5,6,7,10,11,12,14}	C	circ(1 1 1 1 -1 1 -1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 1)	3 3 -1 3 -1 -5 -1 -1 -5
	{4,5,8,12,14,18}	D	circ(1 1 1 1 -1 -1 1 1 -1 1 1 1 -1 1 -1 1 1 1 -1)	1 1 1 -7 1 -7 1 1 -7

V. REMARK

Remark-1 In the above tables A, B, C are circulant matrices and D is a back circulant matrix whose 1st row is shown.

Remark-2 Table 7 shows that there exists a Williamson type matrix corresponding to the expression $4x19 = 1^2 + 5^2 + 5^2 + 5^2$, whereas there is no Williamson matrix to the above expression. This indicates that one can find Williamson type matrices by our method, where Williamson's method fails.

The following Table 8 shows that the number of Williamson type matrices of small order obtained by our method is much greater than that of Williamson matices of the same order.

May 2011

Global Journal of Computer Science and Technology Volume XI Issue VIII Version I

Table VIII COMPARISON WITH WILLIAMSON MATRICES

Order	Number of Williamson matrices	Number of Williamson type matrices constructed by our method
Order 9	3	6
Order 11	1	20
Order 13	4	57
Order 15	4	196
Order 17	4	504

VI. Justification

Justification for the method of construction: The following theorm justifies the construction of Williamsion type matrices.

Theorm: The matrices A, B, C, D constructed above are Williamsion type matrices

Proof : The method consists in finding four circulants matrices A, B, C & D_1 of order n (odd) such that

(i) A, B, C are symmetric

(ii) $AA^T + BB^T + CC^T + D_1D_1^T = 4nI_n$

Let A=circ (a_0, a_1, a_2 , a_3, ... $a_{(n-1))}$ = the circulant where 1st row is (a_0, a1, a2 , a3, ... a(n−1))

B=circ (b_0, b_1, b_2 , b_3, ... $b_{(n-1)}$)

C=circ (c_0, c_1, c_2 , c_3, ... $c_{(n-1)}$)

D=circ (d_0, d_1, d_2 , d_3, ... $d_{(n-1)}$)

We assume without any loss of generality that $a_0 = b_0 = c_0 = d_0 = 1$

Represent A by the input set

S_{k1}= (m_1, m_2, ... m_{k1})

where $m_i \in S_{k1}$ if and only if $a_{mi} < 0$.

Parallely represent A, B, C, D_1 by input sets S_{k2} , S_{k3} & S_{k4} respectively, since A, B, C are symmetric , k_1, k_2 , k_3 are even integers

We claim that

(i) If (e_1, e_2,...... e_{n-1}) (m=(n-1)/2) be the output vector of S_{k1} then

AA^T =circ (n,e_1, e_2,...... e_m, e_m,e_{m-1}, ----------- e_1)

& similar expression for B & C.

Also $D_1D_1^T$ = circ (n, f_1, f_2, ... f_{n-1}) if (f_1, f_2,...... f_{n-1}) is the output vector of S_{k4}

(ii) $(n - 2k_1)^2 + (n - 2k_2)^2 + (n - 2k_3)^2 + (n - 2k_4)^2 + (k_4)^2 = 4n$

where $\bar{k_4}$ = k4 if k4 is odd

Proof (i) In AA^T

e_j= scalar product of 1st row R1 of A with (j + 1)th row R_{j+1} of A .

Let S_{k1}be the input set corresponding to 1st row R1of A and j+S_{k1} be that corresponding to (j+1) throw R_{j+1} of A (where + stands for addition mod n). Let the order of the set (j + S_{k1}) - S_{k1} be r_j. The rows R_1 and R_{j+1} of A differ at $2r_j$ places. Hence the scalar product R_1R_2 is ($n - 2r_2$) - $2r_2$= n - 4rj= e_j by definition. By the same argument we get expressions for BB^T, CC^T & $D_1D_1^T$. Since from (4) the sum of output vectors for A, B, C, D_1 is 0, it follows that

$\sum AA^T$ = circ (4n, 0, 0, ---------- 0)

A, B, C, D_1= $4nI_n$

Proof (ii)

Consider all $k_1(k_1- 1)$ differences (mod n) of the set S_{k1} .

Suppose in the multiset of differences j appears g_j times j = 1,2 , ------- (n-1).

Then $\sum_{j=1}^{n-1} g_j = k_1(k_1 - 1)$ ------------------------- (5)

Also j + S_{k1} and S_{k1} has g_j common elements.

Hence $|(j + S_{k1}) - S_{k1}| = k_1 - g_j = r_j$

Also e_j= n - $4r_j$ [from (1) & (2)] in 3.1

Therefore e_j= n - 4(k_1- g_j)

$=> \sum_{j=1}^{n-1} e_j = (n - 1)\, n - 4((n - 1)\, k_1 - \sum_{j=1}^{n-1} g_j) = (n - 2k_1)^2 - n$ [using (5)]

There are similar expressions corresponding to the sets S_{k2} , S_{k3} , & S_{k4}

Summing all the four expressions we get $\sum_{i=1}^{4}(n\text{-}2k_i)^2 - 4n = 0$ [Since the sum of output vectors for A, B, C, D_1 is zero.

This proves (ii) and justices Step I through Step VI. Replace D_1 by D, a back circulant matrix with same 1st row as that of D_1. Since a symmetric back circulant commutes with symmetric circulant matrices the Step VI is justified.

VII. Future Work

Like Williamson's method, the present method requires great computational effort. However using genetic algorithm or some other heuristic method one can find some Williamson type matrices of higer order.

References Références Referencias

1. R.Cragen and H. Kharaghani, Hadamard Matrices and Hadamard Design in Handbook of Combinatorial Designs (Edts C.J.Colbourn and J.H.Dinitz), 2nd Edition, Chapman & Hall, Boca Raton, London, 2006
2. A.V. Geramita and Jennifer Seberry, Orthogonal Designs: Quadratic forms and Hadamard matrices, Marcel Dekker, New York-Basel, 1979, viii, 460 pages.
3. J.Williamson, Hadamard's determinant theorem and the sum of four squares, Duke Math. J. 11(1944) 65-81.
4. L.D. Baumert, S.W. Golomb and M. Hall Jr, Discovery of an Hadamard matrix of order 92, Bull, Amer, Math. Soc. 68 (1962) 237-238.

5. L.D. Baumert and M. Hall Jr, Hadamard Matrices of the Williamson Type, Math. Comp. 19(1965) 442-447.
6. M. Hall Jr., Combinatorial Theory (Blasisdell, Waltham, MA, 1967).
7. L.D. Baumert, Hadamard matrices of orders 116 and 232, Bull. Amer. Math. Soc. 72 (1966) 237.
8. C. Koukouvinos and S. Kounias Discrete Mathematics, Elsevier Science Publisher, North-Holland, 68(1988) 45-57.
9. J. Seberry Wallis, Construction of Williamson type matrices, Linear and Multilinear Algebra 3 (1975) 197-207.
10. J. Seberry Wallis, On Hadamard matrices, J. Combin. Theory Ser. A 18(1975) 149-164.
11. A.L.Whiteman, An infinite family of Hadamard matrices of Williamson type, J. Combin, Theory ser. A. 14 (1973) 334-340.
12. J. M. Goethals & J.J.Seidel Orthogonal matrices with zero diagonal canad. J. Math 19(1967) 1001-1010.
13. C.J.Colbourn & J.H.Dinitz(editors) Handbook of combinatorial designs, Second edition, Chapter V Chapman and Hall, CRC Boea Raton(2007).
14. C.J.Colbourn & J.H.Dinitz(editors). The CRC Handbook of Combinational Design IV Chapter 24 and 31 CRC Press USA(1996).
15. T. Dakie, On the Turnpike problem, PhD thesis, Simon Fraser University, 2000.
16. P. Pevzner, Computational Molecular Biology: An Algorithmic Approach, MIT Press, 2000.
17. Z. Zhang, An Exponential Example for a Partial Digest Mapping Algorithm, Journal of Computional Biology, 1(3):235-239,1994.
18. S. Skiena, G. Sundaram, A Partial Digest Approach to Restriction Site Mapping, Bulletin of Mathematical Biology, 56:275-294, 1994.

This page is intentionally left blank