Anticirculant Structured block weighing matrices from Williamson matrices

M.K.Singh[1], S.N. Topno[2], T. Paswan[3]

[1] *Ranchi University, Ranchi, Jharkhand, India,*
[2] *Research Scholar, Ranchi University, Ranchi,India,*
[3] *Netarhat Residential School, Jharkhand,*

Abstract: Recent advances in optical quantum computing created an interest in Hankel block Weighing matrices. This paper forwards a partial answer to a open problem posed by Arasu and his coworkers by constructing some infinite families of anticirculant block weighing matrices with additional structures.

Keywords: Williamson matrices, Weighing matrices, block matrices, Hadamard matrices.
Mathematical Subject Class: 05B20.

1 INTRODUCTION

Hankel block weighing matrices have gained importance due to their applications in optical quantum computing [2,5,8,9]. Recently Arasu et.al. [1] suggested a problem i.e., to construct a family of Hankel block weighing matrices by a method different from theirs. In this paper we construct a family of anticirculant structured block weighing matrices. This family has additional properties: (a) each block is a weighing matrix (b) The whole matrix is a weighing matrix. In a special case we have obtained three infinite classes of anticirculant block matrices, with the additional properties (a) and (b).

2 PRELIMINARY

Following definitions are keys for the main construction presented in the next sections:

2.1 Basic symmetric circulant matrix: Let α=circ(0 1 0 ...0) be a circulant matrix of order n whose first row is (0 1 0 ...0) and other rows are obtained by right cyclic shift. $\Gamma_i = \alpha^i+\alpha^{n-i}, \quad i = 1, 2, ...r = \frac{n-1}{2}$ will be called basic symmetric circulant matrices, as symmetric circulant matrix of order n is a linear combination of $\Gamma_i^{'s}$. $\Gamma_i^{'s}$have following properties [3,6,7]:

$$\Gamma_i = \Gamma_{n-i}, {\Gamma_i}^2 = 2I_n + \Gamma_{2i}, \Gamma_i\Gamma_j = \Gamma_{i+j} +\Gamma_{i-j}, for i \neq j, \ \ \Gamma_{-i} = \Gamma_i. \Gamma_i * \Gamma_j = 0 , for\ i \neq j$$

(* denote the Hadamard product)

2.2 Orthogonal designs: An orthogonal design of order m and type (t_1, t_2,....t_k) where t_i are positive integers is an m×m matrix a with entries from commutative indeterminates 0, $\pm x_1$, $\pm x_2$,....,$\pm x_k$ such that $XX^T=(\sum_{i=1}^{k} t_i^2 x_i^2)I_n$. Each row (or column) of X has t_i entries of type $\pm x_i$ and the two rows (or columns) are orthogonal. In this paper our construction depends on OD of order 4t and type (t,t,t,t) which is called a Baumert-Hall array. Such arrays exist for many even values of t and all odd values of t≤73. It is conjectured that it exists for every positive integer t. (Vide Craigen and Kharaghani [4])

2.3 Williamson matrices: Four symmetric, circulant, commuting (1,-1)-matrices A, B, C, D of order n are said to be Williamson matrices if $A^2+B^2+C^2+D^2=4nI_n$. [3]

3 MAIN CONSTRUCTION

Our construction depends upon the following theorems and their corollaries:

3.1 Theorem

Existence of symmetric circulant (0, 1, -1) matrices A_1, A_2, ...A_k of order n satisfying $\sum_{i=1}^{k} A_i^2 = rtI_n$, $k \leq n$ **(1)** *and orthogonal design OD(rt;t, t,...,t) implies the existence of an anticirculant structured block weighing (ASBW) matrix.*

Proof: If Γ_i (i=1,2,..., m=$\frac{n-1}{2}$) be basic symmetric and circulant matrices, then A_i'c can be expressed as $[A_1\ A_2\ ...\ A_k]=\bar{a}_0\times I+\bar{a}_1\times\Gamma_1+\bar{a}_2\times\Gamma_2+...+\bar{a}_m\times\Gamma_m$ **(2)** where $\bar{a}_i=[a_{1i}\ a_{2i}\ ...\ a_{ki}]$ is a vector with entries 1, -1, 0, for i=1, 2,....k.

In view of (1) $\sum A_i^2=(\bar{a_0}^2+2\sum_{i=1}^{m} a_i^2)I$

and

$$\sum_{i=1}^{m} \bar{a}_i^2\Gamma_{2i}+\sum_{i=1}^{m} \bar{a}_0.\bar{a}_k\Gamma_k + \sum_{i,j:a_i=\rho a_j,i,j\neq 0,\rho\in\{-1,1\}} \rho\bar{a}_i^2(\Gamma_{i+j}+\Gamma_{i-j}) + \sum_{i,j:a_1\neq\rho a_j,i,j\neq 0,\rho\in\{-1,1\}} \bar{a}_i.\bar{a}_j(\Gamma_{i+j}+\Gamma_{i-j})=0. \quad \textbf{(3)}$$

($\bar{a}_i.\bar{a}_j, \bar{a}_i^2=\bar{a}_i.\bar{a}_i$ are Euclidean inner product of vectors in R^k.)

Define a linear mapping $R^k \rightarrow R_{rt}$= vector space of real rt×rt matrices by $f(\bar{a}) = f([a_1\ a_2...a_k]) = M(a_1\ a_2...a_k)$ where M is an OD(rt;t, t,...,t). Then $f(\bar{a})$ can be expressed as $f(\bar{a})=\sum_{i=1}^{k} a_iW_i$ where W_i are weighing matrices satisfying
$W_iW_i^T=tI_{rt}, W_iW_j^T+W_jW_i^T=0$ **(4)**
(Vide Geramita and Seberry [6].)

Now for $0\leq i,j\leq m$ we have
$f(\bar{a}_i)f(\bar{a}_j)^T=(\sum_{p=1}^{k} a_{ki}W_p)(\sum_{q=1}^{k} a_{qi}W_q^T)$.

Hence, using (4),
$f(\bar{a}_i)f(\bar{a}_j)^T+f(\bar{a}_j)f(\bar{a}_j)^T=2t(\sum a_{pi}a_{pj})I_{rt}$
$=2t(\bar{a}_i.\bar{a}_j)I_{rt}$ **(5)**.

Since f is linear, equation (2) turns to $W=f([A_1\ A_2\ ...\ A_k])=f(\bar{a}_0)\times I+f(\bar{a}_1)\times\Gamma_1+f(\bar{a}_2)\times\Gamma_2+...+f(\bar{a}_m)\times\Gamma_m$ **(6)** and

$$WW^T=f(\bar{a}_0)f(\bar{a}_0)^T+2\sum_{i=1}^{m} f(\bar{a}_i)f(\bar{a}_i)^T\times I_n$$

$$+[\sum_{i=1}^{m} f(\bar{a}_i)f(\bar{a}_i)^T\times\Gamma_{2i}$$

$$+\sum_{k=1}^{m}\{f(\bar{a}_0)f(\bar{a}_k)^T+f(\bar{a}_k)f(\bar{a}_0)^T\}\times\Gamma_k$$

$$+\sum_{i,j:a_i=\rho a_j,i,j\neq 0,\rho\in\{-1,1\}} \rho f(\bar{a}_i).f(\bar{a}_j)^T\times(\Gamma_{i+j}+\Gamma_{i-j})$$

$$+\sum_{i,j:a_1\neq\rho a_j,i,j\neq 0,\rho\in\{-1,1\}} \{f(\bar{a}_i).f(\bar{a}_j)^Tf(\bar{a}_j)f(\bar{a}_i)^T\}\times(\Gamma_{i+j}+\Gamma_{i-j})].$$

But the expression in the large bracket vanishes in view of (3) and (5), implying that W is a weighing matrix.

At last the matrix $\bar{W}=\bar{f}([A_1A_2...A_k])=I\times f(\bar{a}_0)+\Gamma_1\times f(\bar{a}_1)+...+\Gamma_m\times f(\bar{a}_m)$ **(7)** is clearly a weighing matrix. Also since Γ_i are circulant and $\Gamma_i*\Gamma_j=0$ it is also block circutant weighing matrix whose blocks $f(\bar{a})$ are weighing matrices. Finally $\bar{W}R$ where R=

$$\begin{bmatrix} 0 & & I_{rt} \\ & \iddots & \\ I_{rt} & & 0 \end{bmatrix}$$

is an anticirculant block weighing matrix which will be abbreviated as ASBW matrix. We introduce following definition which renders $\sum_{i,j\ satisfying\ a_1\neq\rho a_j,i,j\neq 0,\rho\in\{-1,1\}} \bar{a}_i.\bar{a}_j(\Gamma_{i+j}+\Gamma_{i-j})=0$ in equation (3).

Basic set of vectors: If the vectors $\bar{a}_i$ (i=1,2,...,m) defined in (2) belong to the set $\mathcal{B}=\{\underline{0}, \pm\underline{i}, i=1, 2, ...l\}$ $l\leq k$ then the set of blocks in $\mathcal{B}$ will be called the basic set of vectors, if $\underline{i}.\underline{j}=0$ for i≠j. $\underline{1},\underline{2},...,\underline{l}$ can be taken as the rows of a weighing matrix. The size of the basic set

counts the number of blocks in $\bar{W}$R given in theorem I. Two basic sets $\mathcal{B}$ and $\mathcal{B}'$ will be called proportional if (i)there is a bijection $\mathcal{B} \mapsto \mathcal{B}'$ by $\underline{i} \mapsto \underline{i}'(ii)\frac{0.i}{i^2}=\frac{0'.i'}{i'^2}$ **(8)**

We note that when k=4, (2) gives Williamson matrices if the basic set is $\mathcal{B} \subset \{\underline{0}, \underline{i}, i = 1, 2, 3, 4\}$ where $\underline{i}$ is a 4-vector in which i^{th} entry is -1 and the remaining entries are +1, and if the condition $\sum_{i=1}^{m} \bar{a}_i^2\Gamma_{2i}+\sum_{i=1}^{m} \bar{a}_0.\bar{a}_k\Gamma_k$ $+ \sum_{i,j:a_i=\rho a_j,i,j\neq 0,\rho\in\{-1,1\}} \rho\bar{a}_i^2(\Gamma_{i+j} + \Gamma_{i-j})=0$ **(9)** is satisfied. $\mathcal{B}$ must contain at least two $\underline{i}'^s$,$\underline{i} \in \underline{1}, \underline{2}, \underline{3}, \underline{4}$

The Williamson matrices A_i (i=1, 2, 3, 4) will be called

of type I if $\mathcal{B} = \{\underline{0}, \underline{1}, \underline{2}\}$

of type II if $\mathcal{B} = \{\underline{0}, \underline{1}, \underline{2}, \underline{3}\}$

of type III, if $\mathcal{B} = \{\underline{0}, \underline{i}, i = 1, 2, 3, 4\}$.

3.1.1 Construction of block Hadamard matrix:

As soon as Williamson matrices in (2) satisfying (9) is obtained, $\bar{W}$ given in (7) becomes an anticirculant block Hadamard matrix and $\bar{W}$R is an ASBW of order 4nt, block weight n, block size 4t and weight 4nt. A similar result has been obtained in [10] when t=1. When n=$\frac{q+1}{2}$ where q is an odd prime power Turyn has obtained an infinite family of Williamson matrices [11] when the basic set is $\mathcal{B} = \{\underline{0}, \underline{1}, \underline{2}\}$. Hence we can obtain infinite family of ASBW matrices with H-blocks of order 2(q+1)t for every t for which OD (4t; t, t, t, t) exists. In the next theorem we construct ASBW matrices whose blocks are weighing matrices which are not Hadamard.

3.2 Theorem

Let the Williamson matrices A, B, C, D be expressed as [A B C D]=$\sum_{i=0}^{m} \bar{a}_i \times \Gamma_i$*,where* Γ_0=*I and* Γ_i *are basic symmetric and circulant (0,1) matrices,*$\bar{a}_i$ *are 4-vectors, with co-ordinates +1,-1, belonging to a basic set* $\mathcal{B}$ *of vectors. If* $\bar{a}_i'$ *are vectors with co-ordinates 0, +1, -1 belonging to a basic set B' proportional to B then* $[A_1A_2A_3A_4]=$ $\sum_{i=0}^{m} \bar{a}_i \times \Gamma_i$ *satisfy* $\sum_{i=1}^{4} A_i^2$=*4kI, k*≤*n.*

Proof: Since the vector in basic sets are proportional, (8) holds. Hence $\frac{\bar{a}_0.\bar{a}_i}{\bar{a}_0'.\bar{a}_i'}=\frac{\bar{a}_i^2}{\bar{a}_i'^2}$. Thus if $\bar{a}_0$, $\bar{a}_i$ (i=1,2,...,m) satisfy (9) , $\bar{a}_0'$, $\bar{a}_i'$ also satisfy (9). Hence $\sum_{i=1}^{4} A_i^2$=4kI, k≤n.

3.2.1 Corollary

For Williamson matrices basic set $B' = \{\underline{0}', \underline{1}', \underline{2}', \underline{3}', \underline{4}'\}$ is proportional to $B = \{\underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}\}$ in the following cases:

Case I:
(a)$\underline{0}'$=[0 0 - 0],$\underline{1}'$=[0 0 + -], $\underline{2}'$=[0 0 + +]
(b)$\underline{0}'$=[0 + - 0],$\underline{1}'$=[0 0 + -], $\underline{2}'$=[0 0 + +]
(c)$\underline{0}'$=[+ + - 0], $\underline{1}'$=[0 0 + -], $\underline{2}'$=[0 0 + +]

Case II:
(a)$\underline{0}'$=[- - 0 0], $\underline{1}'$=[+ 0 0 -], $\underline{2}'$=[0 + + 0], $\underline{3}'$=[0 + - 0]
(b)$\underline{0}'$=[0 - 0 +], $\underline{1}'$=[+ 0 0 -],$\underline{2}'$=[0 + + 0], $\underline{3}'$=[0 + - 0]

Case III:
$\underline{0}'$=[- - 0 0], $\underline{1}'$=[+ 0 0 -], $\underline{2}'$=[+ 0 0 +], $\underline{3}'$=[0 + + 0], $\underline{4}'$=[0 + - 0]
(+ denotes +1 and - denotes -1)

By theorem I we have an infinite family of ASBW's in each subcase (a), (b) and (c) of case I.

In Case I blocks of ASBW belong to the set $\{f(\underline{0}'), \pm f(\underline{1}'), \pm f(\underline{2}')\}$. These Are essentially 3 blocks.

In case II blocks of ASBW belong to the set $\{f(\underline{0}'), \pm f(\underline{1}'), \pm f(\underline{2}'), \pm f(\underline{3}')\}$. These are essentially 4 blocks.

In case III blocks of ASBW belong to the set $\{f(\underline{0}'), \pm f(\underline{i}'), i = 1, 2, 3, 4\}$. These are essentially 5 blocks.

4 EXAMPLES

1(a).Using $\underline{0}', \underline{1}', \underline{2}'$ in case I (a)and OD(4;1,1,1,1)

$\bar{W}(12,5)$=circ(f($\underline{0}'$) f($\underline{1}'$) f($\underline{1}'$))R=

$$\begin{bmatrix}
-+00 & -+00 & 0-00 \\
++00 & ++00 & -000 \\
00-- & 00-- & 000+ \\
00-+ & 00-+ & 00+0 \\
\\
-+00 & 0-00 & -+00 \\
++00 & -000 & ++00 \\
00-- & 000+ & 00-- \\
00-+ & 00+0 & 00-+ \\
\\
0-00 & -+00 & -+00 \\
-000 & ++00 & ++00 \\
000+ & 00-- & 00-- \\
00+0 & 00-+ & 00-+
\end{bmatrix}$$

1(b).Using $\underline{0}', \underline{1}', \underline{2}'$ in case I (b)and OD(4;1,1,1,1)

$\bar{W}(12,6)$=circ(f($\underline{0}'$) f($\underline{1}'$) f($\underline{1}'$))R=

$$\begin{bmatrix}
-+00 & -+00 & 0-+0 \\
--00 & --00 & +00- \\
00+- & 00+- & +00+ \\
00++ & 00++ & 0--0 \\
\\
-+00 & 0-+0 & -+00 \\
--00 & +00- & --00 \\
00+- & +00+ & 00+- \\
00++ & 0--0 & 00++ \\
\\
0-+0 & -+00 & -+00 \\
+00- & --00 & --00 \\
+00+ & 00+- & 00+- \\
0--0 & 00++ & 00++
\end{bmatrix}$$

1(c).Using $\underline{0}', \underline{1}', \underline{2}'$ in case I (c)and OD(4;1,1,1,1)

$\bar{W}(12,7)$=circ(f($\underline{0}'$) f($\underline{1}'$) f($\underline{1}'$))R=

$$\begin{bmatrix}
-+00 & -+00 & 0-++ \\
--00 & --00 & +0+- \\
00+- & 00+- & ++0+ \\
00++ & 00++ & +--0 \\
\\
-+00 & 0-++ & -+00 \\
--00 & +0+- & --00 \\
00+- & ++0+ & 00+- \\
00++ & +--0 & 00++ \\
\\
0-++ & -+00 & -+00 \\
+0+- & --00 & --00 \\
++0+ & 00+- & 00+- \\
+--0 & 00++ & 00++
\end{bmatrix}$$

2(a).Using $\underline{0}', \underline{1}', \underline{2}'$ in case I (a) and OD(4;1,1,1,1) $\bar{W}(20,9)$=circ(f($\underline{0}'$)f($\underline{1}'$)f($\underline{2}'$)f($\underline{2}'$)f($\underline{1}'$))R=

$$\begin{bmatrix}
-+00 & ++00 & ++00 & -+00 & 0-00 \\
++00 & +-00 & +-00 & ++00 & -000 \\
00-- & 00+- & 00+- & 00-- & 000+ \\
00-+ & 00-- & 00-- & 00-+ & 00+0 \\
\\
++00 & ++00 & -+00 & 0-00 & -+00 \\
+-00 & +-00 & ++00 & -000 & ++00 \\
00+- & 00+- & 00-- & 000+ & 00-- \\
00-- & 00-- & 00-+ & 00+0 & 00-+ \\
\\
++00 & -+00 & 0-00 & -+00 & ++00 \\
+-00 & ++00 & -000 & ++00 & +-00 \\
00+- & 00-- & 000+ & 00-- & 00+- \\
00-- & 00-+ & 00+0 & 00-+ & 00-- \\
\\
-+00 & 0-00 & -+00 & ++00 & ++00 \\
++00 & -000 & ++00 & +-00 & +-00 \\
00-- & 000+ & 00-- & 00+- & 00+- \\
00-+ & 00+0 & 00-+ & 00-- & 00-- \\
\\
0-00 & -+00 & ++00 & ++00 & -+00 \\
-000 & ++00 & +-00 & +-00 & ++00 \\
000+ & 00-- & 00+- & 00+- & 00-- \\
00+0 & 00-+ & 00-- & 00-- & 00-+
\end{bmatrix}$$

(+ denotes +1 and - denotes -1)

Likewise 3.Using $\underline{0}', \underline{1}', \underline{2}', \underline{3}', \underline{4}$ in case II(a) and OD(4;1,1,1,1)
$\bar{W}(28,14)$=circ(f($\underline{0}'$)f($\underline{1}'$)f($\underline{2}'$)f($\underline{3}'$)f($\underline{3}'$)f($\underline{2}'$)f($\underline{1}'$))

and 4.Using $\underline{0}', \underline{1}', \underline{2}', \underline{3}', \underline{4}$ in case III and OD(12;3,3,3,3)
$\bar{W}$(36,18)=circ(f($\bar{0}'$) f($\bar{1}'$) f($\bar{1}'$))

5 CONCLUSION

Our method clearly differs from that of Arasu et al. The anticirculant block weighing matrix depends upon Williamson matrices and OD(4t;t,t,t,t) both of which are available abundantly. We have obtained three infinite series of such weighing matrices. However more such series can be obtained from (1) new infinite series of Williamson matrices (2) new infinite series of certain symmetric circulant (0,1,-1)-matrices $A_1, A_2,...,A_k$ of order n satisfying $\sum_{i=1}^{k} A_i$=rtI$_n$, k≤n. Also resulting matrices are structured in the sense that the whole matrix is a weighing matrix as well as the blocks. There is an open problem: Can the method be modified to include Hankel block weighing matrices which are not anticirculant block weighing matrices?

REFERENCES

[1] K.T. Arasu, S. Severini, E. Velten, Block Weighing Matrices, *Cryptogr. Commun.* (2013) 5: 201. doi:10.1007/s12095-013-0083-0

[2] H.J. Briegel, R. Raussendorf, Persistent entanglement in arrays of interacting particles, *Phys. Rev. Lett.* **86** 910 (2001).

[3] R. Craigen and H. Kharaghani , Hadamard Matrices and Hadamard Designs in Handbook of Combinatorial designs (*eds. C.J.Colbourn and J.H. Dinitz)2nd edition,Chapman and Hall/CRC, Boca Raton* (2007).

[4] R. Craigen , and H. Kharaghani , Orthogonal Designs in Handbook of Combinatorial designs *(eds. C.J.Colbourn and J.H. Dinitz)2nd edition,Chapman and Hall/CRC, Boca Raton* (2007).

[5] S. T.Flammia, S. Severini ,Weighing matrices and optical quantum computing, *J. Phys. A: Math. Theor.* **42**(2009)065302

[6] A.V. Geramita, J. Seberry, : Orthogonal Designs: Quadratic Forms and Hadamard Matrices. *Marcel Decker, New York-Basel* (1979).

[7] M. Hall, Jr., Combinatorial Theory , *Wiley, New York 2nd edition*,(1986).

[8] N. C. Menicucci, S. T. Flammia, and O. Pfister, One-way quantum computing in the optical frequency comb, *Phys. Rev. Lett.* **101** 130501 (2008).

[9] R. Raussendorf and H. J. Briegel, A one-way quantum computer, *Phys. Rev. Lett.* **86** 5188 (2001).

[10] M.K.Singh and S.N. Topno, On the construction of Hadamard matrices of order 4n(n odd,n≥ 3) with Hadamard blocks of order 4, *Acta Ciencia Indica*,vol XL M,No.3.309(2014).

[11] R. J. Turyn, An infinite class of Williamson Matrices , *J.Combin. Theo. Ser. A*. 1972.