On Circulant and Two-Circulant Weighing Matrices

K. T. Arasu [*][†]
Department of Mathematics and Statistics
Wright State University
Dayton, Ohio–45435
USA

Ilias S. Kotsireas[‡]
Department of Physics and Computer Science
Wilfrid Laurier University
Waterloo, Ontario N2L 3C5
Canada

Christos Koukouvinos
Department of Mathematics
National Technical University of Athens
Zografou 15773, Athens
Greece

Jennifer Seberry [§]
Centre for Computer and Information Security Research
University of Wollongong
NSW 2522
Australia

December 6, 2009

Abstract

We employ theoretical and computational techniques to construct new weighing matrices constructed from two circulants. In particular, we construct $W(148, 144)$, $W(152, 144)$, $W(156, 144)$ which are listed as open in the second edition of the Handbook of Combinatorial Designs. We also fill a missing entry in Strassler's table with answer "YES", by constructing a circulant weighing matrix of order 142 with weight 100.

1 Introduction

A *weighing matrix* $W = W(n, k)$ of order n and weight k is a square matrix of order n with entries from $\{0, \ -1, \ +1\}$ such that

$$WW^T \ = \ k \cdot I_n$$

where I_n is the $n \times n$ identity matrix and W^T is the transpose of W.

A *circulant weighing matrix*, $W = CW(n, k)$, is a weighing matrix of order n and weight k in which each row (except the first row) is obtained from its preceding row by a right cyclic shift. We label the columns of W by a cyclic group G of order n, say generated by g.

[*]Research partially supported by grants from NSF and AFOSR.
[†]The author thanks the Centre for Computer and Information Security Research, Univ of Wollongong for its hospitality during the time of this sabbatical research.
[‡]Supported by grants from NSERC and SHARCnet
[§]Supported by an ARC grant.

For any circulant weighing matrix $W = CW(n,k)$ define

$$\begin{array}{rrcl} & A & = & \{ g^i \mid W(1,g^i) = 1 \;,\; i = 0,1,\ldots,n-1\} \\ \text{and} & B & = & \{ g^i \mid W(1,g^i) = -1 \;,\; i = 0,1,\ldots,n-1\} \end{array} \qquad (1)$$

It is easy to see that $\mid A \mid + \mid B \mid = k$.

For a circulant weighing matrix, $W = CW(n,k)$ it is well known that k must be a perfect square, (see [7], for instance), write $k = s^2$ for some integer s.

For more on weighing designs, weighing matrices and related topics refer to [5].

It is known [5, 8] that:

Theorem 1 *A $CW(n,k)$ can only exist if (i) $k = s^2$, (ii) $\mid A \mid = \frac{s^2+s}{2}$ and $\mid B \mid = \frac{s^2-s}{2}$, (iii) $(n-k)^2 - (n-k) \geq n-1$ and (iv) if $(n-k)^2 - (n-k) = n-1$ then $M = J - W * W$ is the incidence matrix of a finite projective plane, (here J is the $n \times n$ matrix of all 1's and $*$ denotes the Kronecker product).*

For a multiplicatively written group G, we let $\mathbf{Z}G$ denote the group ring of G over Z. We will consider only abelian (in fact, only cyclic) groups. For $S \subseteq G$, we let S denote the element $\sum_{x \in S} x$ of $\mathbf{ZG}$. For $A = \sum_g a_g g$ and $t \in \mathbf{Z}$, we define $A^{(t)} = \sum_g a_g g^t$.

It is easy to see (see [1], [2] or [3] for details):

Theorem 2 *A $CW = W(n, s^2)$ exists if and only if there exist disjoint subsets A and B of Z_n satisfying*

$$(A - B)(A - B)^{(-1)} = s^2. \qquad (2)$$

We shall identify a $W = CW(n,k)$ with its first row of the group ring element $\sum_i W(1,g^i) g^i$ in $\mathbf{Z}G$.

Definition 1 *The support of a circulant matrix C of order n is defined as the set*

$$\textit{support } C = \{i \,|\, C(1,i) \neq 0, 1 \leq i \leq n\}$$

In this paper we use the following notations:

1. a $W(n,k)$ denotes a weighing matrix of order n and weight k;
2. a $CW(n,k)$ denotes a circulant weighing matrix of order n and weight k;
3. $DC(n,k)$ denotes two $\{0, \pm 1\}$ sequences of order n each and (total) weight k, that have PAF zero; (see [7] for the definition of PAF)
4. a $2 - CW(2n,k)$ denotes a $W(2n,k)$ constructed from two circulants whose first rows are given by $DC(n,k)$.

2 New Results

We obtain an extension of the following theorem of Arasu and Dillon [1].

Theorem 3 *If there exists a* $CW(n,k)$ *with* n *odd, then there exists a* $CW(2tn,4k)$ *for each positive integer* $t>1$.

An extension of Theorem 3 is Theorem 2.3 in Arasu, Leung, Ma, Nabavi, Ray-Chaudhuri [2]

Theorem 4 *Let* G *be a group such that the center of* G *contains an element* α *of order* 2. *Let* B *be a* $W(G,k)$ *and let* $C \in \mathbf{Z}[G]$ *such that* C *has coefficients* $0, \pm 1$ *and* $\eta(C)$ *is a* $W(G/<\alpha>, k)$ *where* $\eta: G \longrightarrow G/<\alpha>$ *is the natural epimorphism. If* B, αB, C, αC *are pairwise disjoint, then*

$$A = (1-\alpha)B + (1+\alpha)C \tag{3}$$

is a $W(G,4k)$.

Remark The notation $W(G,k)$ used in theorem 4 above refers to a weighing matrix that is developed using the group G; we avoid giving its definition for the sake of brevity and refer the interested reader to [2] for further details. We only wish to stress that if G is a cyclic group, then the $W(G,k)$ is indeed a $CW(n,k)$ where n is the order of G.

For convenience we provide an extension of Theorem 3 to cover the case $t=1$; although a more general version is contained in Theorem 4.

Definition 2 *Two circulant matrices* A *and* B *of the same order are said to have disjoint support, if (support* A*)* $\cap$ *(support* B*)* $= \emptyset$.

Theorem 5 *Let* n *be an odd positive integer. If there exist two* $CW(n,k)$ *with disjoint supports then there exists a* $CW(2n,4k)$.

Proof. Let A and B be two $CW(n,k)$ with (support A) $\cap$ (support B) $=\emptyset$. Then $AA^{(-1)} = BB^{(-1)} = k$ in $\mathbf{Z}[G]$, where G is "the" unique multiplicatively written group of order n. Let $<t>=\mathbf{Z}_2$ where $t^2=1$. Then $H = G\times <t>$ is a cyclic group of order $2n$.

We define

$$W = (1+t)A + (1-t)B.$$

Then

$$WW^{(-1)} = 2(1+t)AA^{(-1)} + 2(1-t)BB^{(-1)} = 2(1+t)k + 2(1-t)k = 4k.$$

Since A and B have disjoint supports with coefficients $0,\pm1$, it follows that W has coefficients $0,\pm1$. Hence, W defines the required $CW(2n,4k)$. □

Definition 3 *Two matrices* A *and* B *of the same order are said to have disjoint support, if* $A \star B = 0$, *where* $\star$ *denotes the Hadamard product (element-wise product) of the two matrices.*

The above definition of disjoint support for arbitrary matrices (i.e. not necessarily circulant) boils down to the definition 2 of disjoint support for circulant matrices.

Theorem 6 *If A and B are two $W(n,k)$ with disjoint support then, since $AA^T = BB^T = kI$*

$$\begin{bmatrix} A+B & A-B \\ A-B & A+B \end{bmatrix}$$

is a $W(2n, 4k)$.

Note that theorem 6 is important since it does not require any structural assumptions (like circulant on A or B) - any random weighing matrices with disjoint support will work.

2.1 Applications

Let $G =< x >$ where $x^{71} = 1$. Then

$$A(x) = x^7 + x^{35} + x^{33} + x^{23} + x^{44} + x^9 + x^{45} + x^{12} + x^{60} + x^{16} + x^{22} + x^{39} + x^{53} + x^{52} + x^{47}$$
$$-x - x^5 - x^{25} - x^{54} - x^{57} - x^6 - x^{30} - x^8 - x^{40} - x^{58}$$

and

$$B(x) = x^{11} + x^{55} + x^{62} + x^{26} + x^{59} + x^{18} + x^{19} + x^{24} + x^{49} + x^{32} + x^{27} + x^{64} + x^{36} + x^{38} + x^{48}$$
$$-x^{13} - x^{65} - x^{41} - x^{63} - x^{31} - x^{14} - x^{70} - x^{66} - x^{46} - x^{17}$$

define two $CW(71, 25)$ with disjoint supports. Following the construction of Theorem 5, we define $W = (1 + x^{71})A(x^2) + (1 - x^{71})B(x^2)$ where we reduce modulo $2 \cdot 71$ the exponents of the polynomial W. Therefore, according to Theorem 5, W defines a $CW(142, 100)$. In order to provide an independent verification of this result, we give explicitly the first row of this $CW(142, 100)$ constructed using Theorem 5:

```
- - 0 0 - 0 + 0 - - + - 0 + 0 - + + + 0 + + + + - - - - 0 0 0 + + - +
+ - + - 0 0 0 - + - + - + + - 0 + - + + 0 - 0 + - + - 0 + 0 + 0 0 + +
0 + - 0 0 + 0 + 0 - - - - 0 + 0 - + + + 0 - - + + + + + + 0 0 0 + + +
+ - - - + 0 0 0 - + - + + - + - 0 - + - - 0 + 0 - - - + 0 - 0 + 0 0 -
+ 0
```

Remark 1 The existence of a $CW(142, 100)$ was previously open, see Strassler [10].

Remark 2 The first example of a $CW(71, 25)$ was given by Strassler [9].

3 Two-Circulants or Double Circulant Constructions

We now extend the ideas of Section 2 to the "two-circulants" case.

Definition 4 *Two elements A and B of the group ring $\mathbf{Z}G$, where G is a cyclic group of order n, are said to define two-circulants, or double-circulants, of order n with weight k, written $DC(n,k)$, if (i) the coefficients of A and B are in $\{0,1,-1\}$ and (ii) $AA^{(-1)} + BB^{(-1)} = k$.*

The following theorem is taken from [7].

Theorem 7 *Let A and B define a $DC(n,k)$. Let $circ(A)$ and $circ(B)$ be the circulant matrices whose first rows are A and B respectively. Then $\begin{bmatrix} circ(A) & circ(B) \\ circ(B)^T & -circ(A)^T \end{bmatrix}$ gives a $2-CW(2n,k) = W(2n,k)$.*

For a double circulant weighing matrix, $2-CW(2n,k)$ it is well known that k must be a sum of two squares.

Theorem 8 *Let G be a cyclic group of order n. Let A and B be $DC(n,k)$.*

Suppose that A and B have "disjoint" supports and $|G|$ is odd. Let $<t>= \mathbf{Z}_2$ where $t^2 = 1$. Define $H = G\times <t>$ and

$$C = (1+t)A + (1-t)B \text{ and } D = (1-t)A + (1+t)B.$$

Then C and D define a $DC(2n,4k)$.

Proof. Note the coefficients of C and D are $0, \pm 1$. Now

$CC^{(-1)} = 2(1+t)AA^{(-1)} + 2(1-t)BB^{(-1)}$ and $DD^{(-1)} = 2(1-t)AA^{(-1)} + 2(1+t)BB^{(-1)}$.

Hence $CC^{(-1)} + DD^{(-1)} = 4(AA^{(-1)} + BB^{(-1)}) = 4k$, as desired. □

3.1 Applications

We now apply theorem 8 to construct three new double circulant weighing matrices $DC(74,144)$, $DC(76,144)$, $DC(78,144)$. We note that the existence of the corresponding $W(148,144)$, $W(152,144)$ was previously open, see Craigen's table [4]. We also note that there exist symmetric and skew-symmetric $W(156,144)$. We are also grateful to R. Craigen for pointing out that $W(156,144)$ can be constructed by the method of weaving. However the existence of a $DC(78,144)$, hence a $W(156,144)$ constructed from two circulants, was open.

Proposition 1 *There exists a*

1. *$DC(37,36)$ hence a $DC(74,144)$ and hence a $W(148,144)$;*
2. *$DC(38,36)$ hence a $DC(76,144)$ and hence a $W(152,144)$;*
3. *$DC(39,36)$ hence a $DC(78,144)$ and hence a $W(156,144)$;*
4. *$DC(19,18)$ hence a $DC(38,72)$ and hence a $W(76,72)$;*
5. *$DC(31,18)$ hence a $DC(62,72)$ and hence a $W(124,72)$.*

Proof.

1. Consider the following $DC(37,36)$ taken from [7]:

```
A = + + - - 0 - 0 - + + 0 + 0 0 + + 0 + 0 + 0 0 - + 0 + 0 0 0 - 0 + 0 0 0 0 0
B = 0 0 0 0 - 0 + 0 0 0 + 0 - - 0 0 - 0 - 0 + - 0 0 + 0 + + - 0 - 0 + + - + 0
```

   Since A and B have disjoint supports, C and D as defined in theorem 8 define a $DC(74,144)$. Now we apply theorem 7 to this double-circulant pair (C,D), thereby obtaining a weighing matrix of order 148 and weight 144 from two-circulants.

2. Consider the following $DC(38,36)$ with disjoint support, computed via string sorting [6]

```
A = 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 - 0 + 0 - - + - + - - 0 - + + + + + - 0 + 0 -
B = + - + - - - + 0 - - + - - - - 0 + 0 + 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 - 0 - 0
```

   Since A and B have disjoint supports, C and D as defined in Theorem 8 define a $DC(76,144)$. Now we apply theorem 7 to this double-circulant pair (C,D), thereby obtaining a weighing matrix of order 152 and weight 144 from two-circulants.

3. Consider the following $DC(39,36)$ with disjoint support, computed via string sorting [6]

```
A = 0 0 0 0 0 0 0 0 0 0 0 0 0 0 - - + - + - - - - + 0 + + 0 0 + 0 - 0 + 0 - 0 + +
B = - - 0 + + + - - + - - + - 0 0 0 0 0 0 0 0 0 0 0 0 0 0 + - 0 - 0 - 0 - 0 - 0 0
```

   Since A and B have disjoint supports, C and D as defined in Theorem 8 define a $DC(78,144)$. Now we apply theorem 7 to this double-circulant pair (C,D), thereby obtaining a weighing matrix of order 156 and weight 144 from two-circulants.

   Remark. We also note that there exist known but unpublished $W(156,144)$.

4. Consider the following $DC(19,18)$ taken from [7]:

```
A = 0 0 - 0 0 0 + + - 0 0 0 0 + + + 0 - +
B = 0 0 - 0 0 0 - - - 0 0 0 0 + - + 0 - +
```

   If we reverse the second sequence we see that the resulting sequences have disjoint supports. The corresponding polynomials are:

$$A(x) = x^{19} - x^{18} + x^{16} + x^{15} + x^{14} - x^9 + x^8 + x^7 - x^3,$$

$$B(x) = -x^{17} - x^{13} - x^{12} - x^{11} + x^6 - x^5 + x^4 - x^2 + x.$$

   Following the construction of Theorem 8, we define $C = (1+x^{19})A(x^2)+(1-x^{19})B(x^2)$, $D = (1-x^{19})A(x^2)+(1+x^{19})B(x^2)$ where we reduce modulo $2 \cdot 19$ the exponents of the polynomials C, D. Therefore, according to Theorem 8, C, D define a $DC(38,72)$, i.e. a $2-CW(76,72)$ constructed from two circulants. In order to provide an independent verification of this result, we give explicitly the first rows of C, D (note that they have identical supports)

```
0 + + - + - + + + - + + + + + + - - + 0 - - + - - - - + + + - + + - + - - +
0 + - - - - - + - - - + - + - + + - - 0 + - - - + - + + - + + + - - - - + +
```

5. Consider the following $DC(31, 18)$

```
A = 0 0 0 0 0 0 0 - 0 - 0 0 0 0 0 - 0 + + 0 0 0 0 + 0 0 0 - 0 - -
B = 0 - - + 0 0 0 0 - 0 0 0 - + 0 0 0 0 0 - 0 0 0 0 - + 0 0 0 0 0
```

and use it as in 4. to obtain a $DC(62, 36)$ and hence a $2 - CW(124, 72)$

Note that the first rows of the circulant matrices C and D have identical supports. □

Remark. We note that *circulant* and *double circulant* weighing matrices have structure that is amenable to Signal Processing [11] for wireless communications.

4 Acknowledgments

We wish to thank R. Craigen for pointing out some important implications of the method of weaving, for the construction of weighing matrices. We also wish to thank an anonymous reviewer for pointing out that circulant and two-circulant weighing matrices where $n >> k$ are used in acoustic engineering.

References

[1] K. T. Arasu and J. F. Dillon Perfect ternary arrays. Difference sets, sequences and their correlation properties (Bad Windsheim, 1998), 1–15, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 542, Kluwer Acad. Publ., Dordrecht, 1999.

[2] K. T. Arasu, K. H. Leung, S. L. Ma, A. Nabavi, D. K. Ray-Chaudhuri Circulant weighing matrices of weight 2^{2t}, *Des. Codes and Cryptography*, (2006), 111–123.

[3] K. T. Arasu, J. F. Dillon, D. Jungnickel and A. Pott, The solution of the Waterloo problem, *J. Comb. Th.(A)*, 17, (1995), 316–331.

[4] R. Craigen, H. Kharaghani, Orthogonal designs, in Handbook of Combinatorial Designs. Edited by C. J. Colbourn and J. H. Dinitz. Second edition. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2007. pp. 280–295.

[5] A. V. Geramita and J. Seberry, *Orthogonal designs. Quadratic forms and Hadamard matrices*, Lecture Notes in Pure and Applied Mathematics, 45, Marcel Dekker Inc. New York, 1979.

[6] I. S. Kotsireas, C. Koukouvinos, J. Seberry, Weighing matrices and string sorting. *Annals of Combinatorics*, 13, (2009), 305-313

[7] C. Koukouvinos, J. Seberry. New weighing matrices and orthogonal designs constructed using two sequences with zero autocorrelation function—a review. *J. Statist. Plann. Inference* 81 (1999), no. 1, 153–182.

[8] J. Seberry Wallis and A. L. Whiteman, Some results on weighing matrices, *Bull. Austral. Math. Sec.* 12, (1975), 433–447.

[9] Y. Strassler, New circulant weighing matrices of prime order in $CW(31, 16)$, $CW(71, 25)$, $CW(127, 64)$, paper presented at the *R. C. Bose Memorial Conference on Statistical Design and Related Combinatorics,* Colorado State University, 7-11 June, 1995.

[10] Y. Strassler, *The Classification of Circulant Weighing Matrices of Weight* 9, PhD thesis, Bar-Ilan University, Ramat-Gan, Israel 1997.

[11] L.C. Tran, T.A. Wysocki, A. Mertins, J. Seberry, Complex Orthogonal Space-Time Processing in Wireless Communications, Springer-Verlag, Norwell, USA, 2006.