AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **48** (2010), Pages 43–51

On circulant and two-circulant weighing matrices

K. T. Arasu*

Department of Mathematics and Statistics
Wright State University, Dayton, Ohio 45435
U.S.A.

I. S. Kotsireas†

Wilfrid Laurier University
Department of Physics and Computer Science
75 University Avenue West, Waterloo, ON N2L 3C5
Canada

C. Koukouvinos

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

Jennifer Seberry‡

Centre for Computer and Information Security Research
School of Computer Science and Software Engineering
University of Wollongong, Wollongong, NSW 2522
Australia

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.

* Research partially supported by grants from NSF and AFOSR. The author thanks the Centre for Computer and Information Security Research, University of Wollongong, for its hospitality during the time of this sabbatical research.

† Supported by grants from NSERC and SHARCnet

‡ Supported by an ARC grant.

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 $\{-1, 0, +1\}$ 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; see [10].
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.
For any circulant weighing matrix $W = CW(n, k)$, define

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

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 [9], for instance); write $k = s^2$ for some integer s.
For more on weighing designs, weighing matrices and related topics, refer to [7]. It is known [7, 11] 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 $\mathbf{Z}G$. For $A = \sum_g a_g g$ and $t \in \mathbf{Z}$, we define $A^{(t)} = \sum_g a_g g^t$. (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*

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

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*

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

For the results of this paper, the definition of the periodic autocorrelation function is needed.

Definition 2 *Let* $A = [a_1, a_2, \ldots, a_n]$ *be a sequence of length* n. *The* periodic autocorrelation function, PAF, $P_A(s)$ *is defined as:*

$$P_A(s) = \sum_{i=1}^{n} a_i a_{i+s}, \quad s = 0, 1, \ldots, n-1,$$

where we consider $i+s$ *modulo* n.

Definition 3 *Two sequences,* $A = [a_1, \ldots, a_n]$ *and* $B = [b_1, \ldots, b_n]$, *of length* n, *are said to have* zero PAF *if* $P_A(s) + P_B(s) = 0$, *where we consider* $i+s$ *modulo* n *for* $s = 1, \ldots, n-1$.

In this paper we use the following notation:

1. $DC(n,k)$ denotes two $\{0, \pm 1\}$ sequences of order n each and (total) weight k, that have PAF zero;

2. 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* $W(G/\langle\alpha\rangle, k)$, *where* $\eta : G \longrightarrow G/\langle\alpha\rangle$ *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 1 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 4 *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 $CW(2n,4k)$.*

Definition 5 *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 4 of disjoint support for circulant matrices.

Theorem 6 *If A and B are two $W(n,k)$ with disjoint support then*

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

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 $G = \langle x \rangle$ 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:

```
--00-0+0--+-0+0-+++0++++----000++-++-
+-000-+-+-++-0+-++0-0+-+-0+0+00++0+-0
0+0+0----0+0-+++0--++++++000++++---+0
00-+-++-+-0-+--0+0---+0-0+00-+0
```

Remark 1 The existence of a $CW(142,100)$ was previously open; see Strassler [13].

Remark 2 The first example of a $CW(71,25)$ was given by Strassler [12].

3 Two-Circulants or Double Circulant Constructions

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

Definition 6 *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 [9].

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 $\langle t\rangle = \mathbf{Z}_2$ where $t^2 = 1$. Define $H = G \times \langle t\rangle$ and*

$$C = (1+t)A + (1-t)B \quad and \quad D = (1-t)A + (1+t)B.$$

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

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

$$\begin{aligned} CC^{(-1)} &= 2(1+t)AA^{(-1)} + 2(1-t)BB^{(-1)} \quad \text{and} \\ DD^{(-1)} &= 2(1-t)AA^{(-1)} + 2(1+t)BB^{(-1)}. \end{aligned}$$

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 $DC(78,144)$, and 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 [9]:

```
A = ++--0-0-++0+00++0+0+00-+0+000-0+00000
B = 0000-0+000+0--00-0-0+-00+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 [8]:

```
A = 000000000000000-0+0--+-+--0-+++++-0+0-
B = +-+---+0--+----0+0+000000000000000-0-0
```

   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 [8]:

```
A = 00000000000000--+-+----+0++00+0-0+0-0++
B = --0+++--+--+-00000000000000+-0-0-0-0-00
```

   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 [9]:

```
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 = 0000000-0-00000-0++0000+000-0--
B = 0--+0000-000-+00000-0000-+00000
```

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. □

4 Infinite classes of weighing matrices from ternary complementary pairs

We now give a construction for weighing matrices related to ternary complementary pairs. A ternary complementary pair TCP(n, w) is made up of two $\{-1, 0, +1\}$ sequences A and B both of length n, containing w non-zero elements in total, with the property that they have NPAF zero. See [5] for more on TCPs.
Our first theorem allows one to construct a $W(4n, 4w)$, starting from a TCP(n, w).
Our second theorem allows one to construct an infinite class of $W(4n + 2k, 4w)$, for any integer $k \geq 1$.

Theorem 9 *Given any* TCP(n, w)*, there is an* n' *such that* $n' \geq n$ *and a weighing matrix* $W(4n', 4w)$ *constructed from two circulants.*

Proof. Suppose $A; B$ is a disjoint TCP(n, w) for a specific length n and weight w. This TCP(n, w) is equivalent to a disjoint pair $C; D$, TCP(n', w) (shifting alone is sufficient and $n' \geq n$), see [5]. Since $C; D$ is a disjoint pair, by Lemma 11 of [5], $F = (C + D)/2; G = (C - D)/2$ is a $TCP(n', 2w)$. We can double this pair, by another common construction ([5]) to $F' = [F, G]; G' = [F, -G]$. This pair of $F'; G'$ is a TCP$(2n', 4w)$ and hence a weighing matrix $W(2 \cdot 2n', 4w) = W(4n', 4w)$ can be constructed by two circulants. □

In Theorem 9, note that the original $TCP(n, w)$ is not required to have the disjoint support property.

Theorem 10 *Given any* TCP(n, w)*, there is a an* n' *such that* $n' \geq n$ *and a weighing matrix* $W(4n' + 2k, 4w)$ *constructed from two circulants, for any integer* $k \geq 1$.

Proof. Suppose that a TCP(n, w) is given, for a specific length n and a specific weight w and, as before, let C and D be the sequences of the corresponding equivalent TCP(n', w) with disjoint support. For any integer $k \geq 1$, we can add k zeros at the end of each sequence F' and G' constructed in Theorem 9. The resulting sequences will have length $2n' + k$ each and will have NPAF zero, i.e. they form a TCP$(2n' + k, 4w)$, and hence we can construct a $W(2 \cdot (2n' + k), 4w) = W(4n' + 2k, 4w)$. □

4.1 Applications

An updated table of all currently known TCPs appears in [6]. We illustrate the application of Theorem 9 with the following proposition.

Proposition 2 *There exists an infinite class of weighing matrices* $W(108 + 2k, 64)$ *for all integers* $k \geq 0$.

Proof. Consider the following TCP$(21, 16)$, made up of two sequences of length 21 not with disjoint support:

```
+ 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 + -
```

By adding six zeros to each of these two sequences, we obtain a TCP$(27, 16)$ with disjoint support:

```
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
```

Using Theorem 9 we obtain a $W(108, 64)$ constructed from two circulants. Using Theorem 10 we obtain an infinite class $W(108 + 2k, 64)$ for all integers $k \geq 1$. □

5 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 two anonymous reviewers for their useful suggestions and comments.

References

[1] K. T. Arasu and J. F. Dillon, Perfect ternary arrays, in *Difference sets, sequences and their correlation properties*, (Eds. A. Pott, P. V. Kumar, T. Helleseth and D. Jungnickel), *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.,* 542, Kluwer Acad. Publ., Dordrecht, 1999, pp. 1–15.

[2] K. T. Arasu, K. H. Leung, S. L. Ma, A. Nabavi and D. K Ray-Chaudhuri, Circulant weighing matrices of weight 2^{2t}, *Des. Codes Cryptogr.* 41 (2006), 111–123.

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

[4] R. Craigen and H. Kharaghani, Orthogonal designs, in *Handbook of Combinatorial Designs*, (Eds. C.J. Colbourn and J.H. Dinitz), 2nd ed. CRC Press, Boca Raton, Fla., 2006, pp. 290–306.

[5] R. Craigen and C. Koukouvinos, A theory of ternary complementary pairs, *J. Combin. Theory Ser. A* 96 (2001), 358–375.

[6] R. Craigen, S. Georgiou, W. Gibson and C. Koukouvinos, Further explorations into ternary complementary pairs. *J. Combin. Theory Ser. A* 113 (2006), 952–965.

[7] 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.

[8] I. S. Kotsireas, C. Koukouvinos and J. Seberry, Weighing matrices and string sorting, *Ann. Combin.* 13 (2009), 305–313.

[9] C. Koukouvinos and J. Seberry, New weighing matrices and orthogonal designs constructed using two sequences with zero autocorrelation function — a review, *J. Statist. Plann. Inference* 81 (1999), 153–182.

[10] J. Seberry Wallis, Orthogonal $(0, 1, -1)$ matrices, *Proc. First Australian Conf. Combin. Math.*, TUNRA, Newcastle, (1972), 61–84.

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

[12] Y. Strassler, New circulant weighing matrices of prime order in $CW(31, 16)$, $CW(71, 25)$, $CW(127, 64)$, *J. Statist. Plann. Inference* 73 (1998), 317–330.

[13] Y. Strassler, The Classification of Circulant Weighing Matrices of Weight 9, Ph.D. Thesis, *Bar-Ilan University*, Ramat-Gan, Israel, 1997.

(Received 24 Apr 2009; revised 27 Apr 2010)