Circulant Weighing Designs

K. T. Arasu*
Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435

Jennifer Seberry†
Department of Computer Science, University of Wollongong, NSW 2522, Australia

ABSTRACT

Algebraic techniques are employed to obtain necessary conditions for the existence of certain families of circulant weighing designs. As an application we rule out the existence of many circulant weighing designs. In particular, we show that there does not exist a circulant weighing matrix of order 43 for any weight. We also prove two conjectures of Yosef Strassler. © **1996 John Wiley & Sons, Inc.**

1. INTRODUCTION

A weighing matrix $W(n,k) = W$ of order n with 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, written as $W = CW(n,k)$, is a weighing matrix 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.

Define

$$A = \{g^i | W(1,i) = 1, i = 0,1,\ldots,n-1\}$$

* Research partially supported by NSA Grant #904-94-H-2042 and by NSF Grant #NCR-9200265. The author thanks the Computer Security Research Centre of University of Wollongong for its hospitality during the time of this research.
† Supported by an ATERB and ARC Grant A48830241.

CCC 1063-8539/96/060439-09
Journal of Combinatorial Designs, Vol. 4, No. 6 (1996)

$$\text{and } B = \{g^i | W(1,i) = -1, i = 0,1,\ldots,n-1\} \tag{1}$$

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

It is well known that k must be a perfect square, (see [11], for instance), write $k = s^2$ for some integer s.

Strassler [14] has recently announced new results giving CW(31, 16), CW(71, 25), and CW(127, 64). CW(31, 16) and CW(127, 64) are already constructed in [6] and [1], but the CW(71, 25) of Strassler is new. For more on weighing designs and related topics refer to [6].

References [11, 12] show:

Theorem 1.

(i) $k = s^2$,

(ii) $|A| = \frac{s^2+s}{2}$ *and* $|B| = \frac{s^2-2}{2}$.

The following theorem can be found in [6].

Theorem 2. *There exists a* $W = W(n,k)$, *only if*

(i) $(n-k)^2 - (n-k) \geq n-1$;

(ii) *if equality holds in (i), then*

$$A = J - W * W$$

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 **ZG** denote the group ring of G over Z. We will consider only abelian (in fact, only cyclic) groups. A character of the group G, is therefore, a homomorphism from G to the multiplicative group of complex numbers. Extending this to the entire group ring **ZG** yields a map from **ZG** to C. For $S \subseteq G$, we let S denote the element $\sum_{x \in S} x$ of **ZG**. For $A = \sum_g a_g g$ and $t \in \mathbf{ZG}$, we define $A^{(t)} = \sum_g a_g g^t$.

Thus, if $W = W(n,k)$ is a circulant weighing matrix and A and B are as in (1), then it is easy to see that

$$(A-B) \cdot (A-B)^{(-1)} = k \tag{2}$$

in **ZG** (see [1] or [13], for details).

We exploit (2), in conjunction with a few known results on characters in group rings, to obtain necessary conditions on the order n and weight k of a possible circulant $W(n,k)$.

2. ALGEBRAIC PRELIMINARIES

In this section we quote two results:

Theorem 3 (Turyn [15]). *Let p be a prime and $G = H \times P$, an abelian group, where P is the Sylow p-subgroup of G. Assume that there exists an integer f such that $p^f \equiv -1 \pmod{exp\ H}$. Let χ be a nonprincipal character of G and let α be a positive integer. Suppose $A \in \mathbf{ZG}$ satisfies $\chi(A)\overline{\chi(A)} \equiv 0 \pmod{p^{2\alpha}}$. Then $\chi(A) \equiv 0 \pmod{p^\alpha}$.*

Theorem 4 (Ma [8]). *Let p be a prime and G an Abelian group with a cyclic Sylow p-subgroup. $A \in \mathbf{ZG}$ satisfies $\chi(A) \equiv 0 \pmod{p^\alpha}$ for all nonprincipal characters χ of G, then there exist $x_1, x_2 \in \mathbf{ZG}$ such that*

$$A = p^\alpha x_1 + Qx_2$$

where Q is the unique subgroup of order p.

3. MAIN RESULT

Theorem 5. *Suppose that a $CW(n,k)$ exists. Let p be a prime such that $p^{2t}|k$ for some positive integer t. Assume that*

(i) *m is a divisor of n. Write $m = m'p^u$, where $(p, m') = 1$;*
(ii) *there exists an $f \in Z$ such that $p^f \equiv -1 \pmod{m'}$.*

Then

(i) $\frac{2n}{m} \geq p^t$ *if* $p|m$;
(ii) $\frac{n}{m} \geq p^t$ *if* $p \not| m$.

Proof. By (2) we have:

$$(A - B)(A - B)^{(-1)} = k \text{ in } \mathbf{ZG}. \tag{3}$$

where $G = \langle g \rangle$ is a cyclic group of order n.

Let H be the unique subgroup of G of order $\frac{n}{m}$ such that G/H is cyclic group of order m and let σ denote the canonical homomorphism from $G \to G/H$. Then σ extends to a homomorphism from $\mathbf{ZG}$ to $Z_{G/H}$. Applying σ to (3), we get

$$(A^\sigma - B^\sigma)(A^\sigma - B^\sigma)^{(-1)} = k \text{ in } Z_{G/H} \tag{4}$$

Since $p^{2t}|k$ for each nonprincipal character χ of G/H, we have

$$\chi(A^\sigma - B^\sigma) \cdot \chi(A^\sigma - B^\sigma) \equiv 0 \pmod{p^{2t}}$$

from (4). This, in view of Theorem 3, yields $\chi(A^\sigma - B^\sigma) \equiv 0 \pmod{p^t}$.

Now to prove (i) we apply Theorem 4 and conclude that:

$$A^\sigma - B^\sigma = p^t x_1 + Qx_2 \tag{5}$$

for some $x_1, x_2 \in Z[G/H]$ and $Q = \langle h \rangle$ is the unique subgroup of G/H of order p.

We note that the coefficients of $A^\sigma - B^\sigma$ must lie in $[-\frac{n}{m}, \frac{n}{m}]$.

Now (5) yields

$$(A^\sigma - B^\sigma)(1 - h) \equiv 0 \pmod{p^t}, \tag{6}$$

since $Q(1-h)=0$ in $Z[G/H]$.

Since the coefficients of $(A^\sigma - B^\sigma)(1-h)$ are bounded in modulus by $\frac{2n}{m}$, by (6) we have proved part (i) of the desired result, noting that at least one coefficient of $(A^\sigma - B^\sigma)(1-h)$ is nonzero. (For otherwise, we would have $(A^\sigma - B^\sigma)(1-h)=0$. Let χ be a character of G/H such that $\chi(h)\neq 1$. Then we would have $(A^\sigma - B^\sigma)=0$, which implies $k=0$ by (4), which gives a contradiction.)

To prove (ii), since $p\not| m$ and $\chi_0(A^\sigma - B^\sigma)=k=0 \pmod{p^{2t}}$ (here χ_0 =principal character of $Z[G/H]$) the "inversion formula" (see [9]), for instance, yields $(A^\sigma - B^\sigma)\equiv 0 \pmod{p^{2t}}$. Arguing as in the proof of (i), we get $\frac{n}{m}\geq p^t$, completing the proof of Theorem 5. □

4. KNOWN EXISTENCE RESULTS

We first give the known existence results for $\mathrm{CW}(n,k)$.

Theorem 6 ((Seberry) Wallis and Whiteman [12]). *If q is a prime power, then there exists $CW(q^2+q+1,q^2)$.*

Theorem 7 (Eades [4]). *If q is a prime power, q odd and i even, then there exists $CW(\frac{q^{i+1}-1}{q-1},q^i)$.*

Theorem 8 (Arasu, Dillon, Jungnickel, and Pott [1]). *If $q=2^t$ and i even, then there exists $CW((\frac{q^{i+1}-1}{q-1},q^i)$.*

Theorem 9 (Eades and Hain [5]). *A $CW(n,4)$ exists $\leftrightarrow 2|n$ or $7|n$.*

Theorem 10. *If there exist $CW(n_1,k)$ and $CW(n_2,k)$ with $gcd(n_1,n_2)=1$ then there exist*

(i) *a $CW(mn_1,k)$ for all positive integers m;*
(ii) *two inequivalent $CW(n_1n_2,k)$;*
(iii) *a $CW(n_1n_2,k^2)$.*

Proof. If the first rows of the $\mathrm{CW}(n_1,k)$ and $\mathrm{CW}(n_2,k)$ are $\{a_1,a_2,\ldots,a_{n_1}\}$ and $\{b_1,b_2,\ldots,b_{n_2}\}$, respectively. Then the first row(s) of the

(i) $\mathrm{CW}(mn_1,k)$ is, after writing 0_{m-1} for sequences of $m-1$ zeros,

$$\{a_1,0_{m-1},a_2,0_{m-1},\ldots,a_{n_1},0_{m-1}\};$$

(ii) of the two inequivalent $\mathrm{CW}(n_1n_2,k)$s are

$$\{a_1,0_{n_2-1},a_2,0_{n_2-1},\ldots,a_{n_1},0_{n_2-1}\},\text{ and }\{b_1,0_{n_1-1},b_2,0_{n_1-1},\ldots,b_{n_2},0_{n_1-1}\};$$

(iii) $\mathrm{CW}(n_1n_2, k^2)$ is

$$\{a_1b_1, a_1b_2, \ldots, a_1b_{n_2}, a_2b_1, a_2b_2, \ldots, a_2b_{n_2}, \ldots, a_{n_1}b_1, a_{n_1}b_2, \ldots, a_{n_1}b_{n_2}\}.$$

The groups that are used to develop case (ii) have coprime order ensuring the inequivalence. □

Remark 1. This theorem is known but we do not know of a reference in the literature.

Example 1. Consider the CW(7, 4) and CW(4, 4) with first rows

$$1 - - 0 - 0\ 0 \text{ and } 1 - - - .$$

Then, writing **0** for 0_{m-3}, the matrices constructed in theorem have first rows

$$\begin{array}{l} 1\ 0\ \mathbf{0}\ 0\ -\ 0\ \mathbf{0}\ 0\ -\ 0\ \mathbf{0}\ 0\ 0\ 0\ \mathbf{0}\ -\ 0\ \mathbf{0}\ 0\ 0\ 0\ \mathbf{0}\ 0\ 0\ 0\ \mathbf{0}\ 0, \\ 1\ 0\ 0\ 0\ -\ 0\ 0\ 0\ -\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ -\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0, \\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ -\ 0\ 0\ 0\ 0\ 0\ 0\ -\ 0\ 0\ 0\ 0\ 0\ 0\ -\ 0\ 0\ 0\ 0\ 0\ 0, \end{array}$$

and

$$1\ -\ -\ 0\ -\ 0\ 0\ -\ 1\ 1\ 0\ 1\ 0\ 0\ -\ 1\ 1\ 0\ 1\ 0\ 0\ -\ 1\ 1\ 0\ 1\ 0\ 0,$$

respectively. □

5. FURTHER RESULTS USING MULTIPLIERS

The following theorem is proved in Arasu, Dillon, Jungnickel, and Pott [1].

Theorem 11 (Multiplier Theorem). *Let R be an arbitrary group ring element in* **ZG** *that satisfies $RR^{(-1)} = p^n$ where p is a prime with $(p, |G|) = 1$ and where G is an abelian group then $R^{(p)} = Rg$ for some $g \in G$.*

Remark 2. Let $R = \sum_g a_g g \in \mathbf{ZG}$. By a result in Arasu and Ray-Chaudhuri [3] if $(\sum_g a_g, |G|) = 1$, we can replace R by a suitable translate of it, if necessary, in Theorem 11 and conclude $R^{(p)} = R$, i.e., the multiplier p actually fixes R.

We now apply Theorem 11, in conjunction with the above remark for $R = A - B$ and when $k = p^n$ in (2), and obtain $(A - B)^{(p)} = A - B$ or $A^{(p)} - B^{(p)} = A - B$. But A and B have coefficients 0 or 1, hence it follows that $A^{(p)} = A$ and $B^{(p)} = B$. Thus A and B are unions of some of the orbits of G under the action $x \mapsto px$.

A. Applications

(I) $\mathrm{CW}(57, 5^2)$ does not exist. If a $\mathrm{CW}(57, 5^2)$ did exist there would exist $A, B \subseteq \mathbf{Z_{57}}$ such that $A^{(5)} = A$ and $B^{(5)} = B$, by Theorem 11 and remark 2 (since 5 is a multiplier fixing A and B). Now the orbit sizes of $\mathbf{Z_{57}}$ under $x \mapsto 5x$ are:

$$18, 18, 9, 9, 2, 1. \tag{7}$$

However $|A| = 15$ and $|B| = 10$ so we cannot form A (a set of size 15) by using orbits whose sizes are as in (7). Thus there is no $\mathrm{CW}(57, 5^2)$.

(II) CW(73, 4^2) does not exist. As in (I), 2 is a multiplier of A and $B \subseteq \mathbf{Z_{73}}$, where $|A| = 10$ and $|B| = 6$. But the orbit sizes of $\mathbf{Z_{73}}$ under $x \mapsto 2x$ are:

$$9(8 \text{ times}) \text{ and } 1(\text{once}).$$

Hence B cannot be formed from a union of those orbits and so the CW(73, 4^2) does not exist.

(III) CW(91, 4^2) does not exist. We proceed as in (II) above, noting that 2 is a multiplier and the orbit sizes of $\mathbf{Z_{91}}$ under $x \mapsto 2x$ are:

$$12(7 \text{ times}), 3(\text{twice}) \text{ and } 1(\text{once}).$$

(IV) CW(91, 5^2) does not exist. We proceed as in (I) above, noting that 5 is a multiplier and the orbit sizes of $\mathbf{Z_{91}}$ under $x \mapsto 5x$ are:

$$12(6 \text{ times}), 4(3 \text{ times}), 6(\text{once}) \text{ and } 1(\text{once}).$$

6. APPLICATIONS

Now we proceed to give some nonexistence results as applications of Theorem 5.

Example 2. If there exists a CW(31, k), then $k = 5^2$ or 4^2.

Proof. By Theorems 1 and 2, if there exists a CW(31, k), then $k = s^2, s = 2, 3, 4$ or 5.

$CW(31, 3^2)$ Take $m = n; p = 3; t = 1$ in Theorem 5 and use the fact that $3^{15} \equiv -1 (\text{mod } 31)$. Then $\dfrac{2n}{m} \geq p^t$, i.e. $2 \geq 3$, a contradiction.

$CW(31, 2^2)$ does not exist by Theorem 9.

□

Remark 3. Both CW(31, 4^2) and CW(31, 5^2) exist by Theorems 8 and 6, respectively.

Example 3. There exists a CW(57, k) only if $k = 7^2$. □

Proof. By Theorems 1 and 2, $k = s^2, s = 2, 3, \ldots, 7$. CW(57, 2^2) is resolved by Theorem 9. The CW(57, 3^2) and CW(57, 6^2) are both eliminated by Theorem 5 by choosing $p = 3, t = 1, m = n = 57$ and noting $3^9 \equiv -1$ (mod 19). For CW(57, 4^2) we apply Theorem 5 with $p = 2, t = 2, m = n = 57$, since $2^9 \equiv -1$ (mod 57). For CW(57, 5^2) we use Application (I) above. □

Remark 4. A CW(57, 7^2) exists by Theorem 6.

Example 4. There exists a CW(73, s^2) only if $s = 8$.

s	Theorem	p	t	m	n	$p^f \equiv -1 \pmod{m'}$
2	Theorem 9					
3	Theorem 5	3	1	73	73	$3^6 \equiv -1 \pmod{73}$
4	Application (II)					
5	Theorem 5	5	1	73	73	$5^{36} \equiv -1 \pmod{73}$
6	Theorem 5	3	1	73	73	$3^6 \equiv -1 \pmod{73}$
7	Theorem 5	7	1	73	73	$7^{12} \equiv -1 \pmod{73}$

□

Example 5. A CW(91, s^2) exists only if $s = 2, 3, 6$. □

Proof. Similar to example 3. □

Example 6. There does not exist a CW(43, k) for any $k > 1$.

□

Proof. $k = s^2, s = 2, 3, \ldots, 6$.

k	Theorem	p	t	m	n	$p^f \equiv -1 \pmod{m'}$
6^2	Theorem 2	No projective plane of order 6				
5^2	Theorem 5	5	1	43	43	$5^{22} \equiv -1 \pmod{43}$
4^2	Theorem 5	2	2	43	43	$2^7 \equiv -1 \pmod{43}$
3^2	Theorem 5	3	1	43	43	$3^{21} \equiv -1 \pmod{43}$
2^2	Theorem 9					

□

7. TWO CONJECTURES OF STRASSLER

In [13], Strassler made the following conjectures:

Conjecture 1. *A CW($p, 9$) for p prime exists only for $p = 13$.*

Conjecture 2. *A CW(p, k) for fixed k exists for a finite set of primes p.*

In this section, we prove the above conjectures. Our main tool to achieve this is stated in

Theorem 12 (McFarland [10]). *For every positive integer m there exists an integer $M(m)$ such that if K is a finite abelian group with order w relatively prime to $M(m)$, then the only solutions $A \in \mathbf{ZK}$ satisfying*

$$AA^{(-1)} = m^2$$

in $\mathbf{ZG}$ are $A = \pm m$. We can define $M(m)$ as follows: $M(1) = 1$; for $m > 1$, let $M(m)$ be the product of the distinct prime factors of

$$m, m\left(\frac{m^2}{p^{2e}}\right), p-1, p^2-1, \ldots, p^{u(m)-1},$$

where p is a prime dividing m such that $p^e \| m$ and where $u(2) = 3, u(3) = 5, u(4) = 7$ and $u(m) = \frac{1}{2}(m^2 - m)$ for $m \geq 5$.

To prove conjecture 1, we note that the existence of CW$(p, 9), p$ prime, in view of (2), implies

$$(A - B)(A - B)^{(-1)} = 9 = 3^2 \text{ in } \mathbf{Z}[\mathbf{Z}_p].$$

By Theorem 11,

$$M(3) = 2 \cdot 3 \cdot 5 \cdot 11 \cdot 13.$$

Hence if $p \neq 2, 3, 5, 11$ or 13,

$$A - B = \pm 3$$

which gives a contradiction. Therefore $p = 2, 3, 5, 11$, or 13. We now note that a CW$(p, 9)$ exists for only $p = 13$, among these possible values of p establishing conjecture 1.

To prove conjecture 2, we proceed in a similar fashion and obtain

$$(A - B)(A - B)^{(-1)} = k \text{ in } \mathbf{Z}[\mathbf{Z}_p].$$

We note $\gcd(p, m(k)) = 1$ implies $A - B = \pm\sqrt{k}$, which is a contradiction. Hence $p | n(k)$. Thus for a fixed k, only a finite number of primes p are possible where a CW(p, k) exists.

REFERENCES

[1] K. T. Arasu, J. F. Dillon, D. Jungnickel, and A. Pott, *The solution of the Waterloo problem,* J. Combin. Theory Ser. A, in press.

[2] K. T. Arasu, D. Jungnickel, S. L. Ma, and A. Pott, *Relative difference sets with $n = 2$,* to appear in Discrete Math.

[3] K. T. Arasu and D. K. Ray-Chaudhuri, *Multiplier theorem for a difference list,* Ars Combin., **22** (1986), 119–138.

[4] P. Eades, *On the existence of orthogonal designs,* Ph.D. Thesis, Australian National University, Canberra, 1977.

[5] P. Eades and R. M. Hain, *On circulant weighing matrices,* Ars. Combin. **2** (1976), 265–284.

[6] A. V. Geramita and J. Seberry, *Orthogonal designs: Quadratic forms and Hadamard matrices,* Marcel Dekker, New York-Basel, 1979.

[7] R. M. Hain, *Circulant weighing matrices,* Master of Science Thesis, Australian National University, Canberra, 1977.

[8] S. L. Ma, *Polynomial addition sets,* Ph.D. Thesis, University of Hong Kong, 1985.

[9] H. B. Mann, *Addition theorems,* Wiley, New York, 1965.

[10] R. L. McFarland, *On multipliers of Abelian difference sets,* Ph.D. Thesis, Ohio State University, 1970.

[11] R. C. Mullin, "A note on balanced weighing matrices," *Combinatorial Mathematics III: Proceedings of the Third Australian Conference,* in *Lecture notes in mathematics, Vol. 452,* Springer-Verlag, Berlin-Heidelberg-New York, 1975, pp. 28–41.

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

[13] Y. Strassler, "Circulant weighing matrices of prime order and weight 9 having a multiplier," talk presented at *Hadamard Centenary Conference,* Wollongong, Australia, December, 1993.

[14] ———, "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.

[15] R. J. Turyn, *Character sums and difference sets,* Pacific J. Math. **15** (1965), 319–346.

Received September 13, 1995
Accepted February 5, 1996