www.combinatorics.ir

Transactions on Combinatorics
ISSN (print): 2251-8657, ISSN (on-line): 2251-8665
Vol. 4 No. 3 (2015), pp. 43-52.
© 2015 University of Isfahan
www.ui.ac.ir

NONEXISTENCE OF TWO CIRCULANT WEIGHING MATRICES OF WEIGHT 81[1]

K. T. ARASU*, KYLE BAYES[2] AND ALI NABAVI

Communicated by Behruz Tayfeh Rezaie

Dedicated to Professor G. B. Khosroshahi on the occasion of his 75th Birthday.

Abstract. In this paper, we prove the nonexistence of two weighing matrices of weight 81, namely $CW(88, 81)$ and $CW(99, 81)$. We will apply two very different methods to do so; for the case of $CW(88, 81)$, we will use almost purely counting methods, while for $CW(99, 81)$, we will use algebraic methods.

1. Introduction

A square matrix $\mathbf{W}$ of order n with entries from $\{-1, 0, +1\}$ satisfying

$$\mathbf{W} \cdot \mathbf{W^T} = k\mathbf{I}_n$$

is said to be a *weighing matrix* of order n with *weight* k. We denote such a matrix by $W(n, k)$.

A *circulant weighing matrix*, written as $CW(n, k)$, is a weighing matrix where each row (except the first) is obtained from its preceding row by a right cyclic shift. We label the columns of $\mathbf{W}$, a $CW(n, k)$, by a cyclic group G of order n, generated by g. By using zero-based indexing, we define

$$P = \{g^i \,|W_{0,i} = 1, i = 0, 1 \ldots, n-1\}$$

and

$$N = \{g^i \,|W_{0,i} = -1, i = 0, 1 \ldots, n-1\},$$

MSC(2010): Primary: 05C15; Secondary: 20D60.

Keywords: circulant weighing matrices.

Received: 28 April 2014, Accepted: 8 September 2014.

* Corresponding Author.

[1] Research partially supported by grants from the AFOSR and the NSF.

[2] Author's work is supported by a REU grant from the NSF.

hence,

$$|P| + |N| = k. \tag{1.1}$$

It is well known that k is a perfect square (See [6] or [7] for instance). It can be shown that $\{|P|, |N|\} = \{\frac{s^2+s}{2}, \frac{s^2-s}{2}\}$ where $s^2 = k$. (See [2], [6] or [7]). We can always assume that $|P| = \frac{s^2+s}{2}$. (If $\mathbf{W}$ doesn't satisfy this condition consider $-\mathbf{W}$. Two weighing matrices are equivalent if one is obtained by the other by negating or by interchanging the rows or columns.)

In [1] there were two nonexistence theorems claimed, but no proofs were given. This paper provides those proofs, but since the publication of [1], there has been other results. In particular, some nonexistence results can be found in [10]. These results are given in the following theorem.

Theorem 1.1. *Circulant weighing matrices $CW(n, k)$ do not exist for the following n and k.*

(1) *When $n = 112, 117, 133, 152$ and 171, where $k = 25$.*
(2) *When $n = 148, 162, 165, 190$ and 198, where $k = 49$.*

Other recent results can be found in [8] and [9]. For convenience, the results are summarized here.

Theorem 1.2. *Circulant weighing matrices $CW(n, k)$ do not exist for the following (n, k) pairs: $(158, 100)$, $(138, 36)$, $(184, 36)$, $(184, 64)$, $(184, 81)$, $(190, 100)$, $(154, 100)$, $(63, 49)$, $(128, 49)$, $(189, 49)$, $(147, 64)$, $(117, 81)$, $(160, 100)$, $(176, 100)$, $(192, 100)$, $(60, 36)$ and $(120, 36)$.*

2. **Preliminaries**

Let G be a multiplicatively written group and let $\mathbb{Z}[G]$ be the group ring of G over $\mathbb{Z}$. (We will consider only cyclic groups in this article.) For each subset S of G, we let S also denote the group ring element $S = \sum_{x \in S} x$ of $\mathbb{Z}[G]$. For $A = \sum_g \alpha_g g \in \mathbb{Z}[G]$ and for any integer t, we define $A^{(t)} = \sum_g \alpha_g g^t$ and we call the α_g's the *coefficients* of A. Let $A \in \mathbb{Z}[G]$, then any integer t relatively prime to the order of G is called a *multiplier* of A if $A^{(t)} = Ag$ for some $g \in G$.

Theorem 2.1 (Multiplier Theorem [5])**.** *Let G be a finite abelian group of order n. Let A be an element of $\mathbb{Z}[G]$ such that $AA^{(-1)} = k$ for some integer k relatively prime to n. Let*

$$k = p_1^{e_1} \dots p_s^{e_s}$$

where the $p_i's$ are distinct primes. Suppose there are integers $t, f_1, \dots, f_s$ such that

$$t \equiv p_1^{f_1} \equiv \dots \equiv p_s^{f_s} \pmod{n}.$$

Then t is a multiplier of A.

Remark 2.2. *If $A = \sum_g a_g g \in \mathbb{Z}[G]$ such that $\sum_g a_g$ and $|G|$ are relatively prime, then $A^{(t)} = A$ for any multiplier t. Thus, the multiplier t "fixes" A. This result is from Arasu and Ray-Chaudhuri in* [4]*. Referring to P and N in (1.1), we can apply Theorem 2.1 when $k = s^2$ since $(P - N)(P - N)^{(-1)} = k$. For multiplier t, we have $(P - N)^{(t)} = P - N$, i.e., $P^{(t)} - N^{(t)} = P - N$, which implies $P^{(t)} = P$ and $N^{(t)} = N$, as P and N have coefficient equal to 0 or 1.*

Let $\mathfrak{S}_E$ be the group of permutations of the set E. Then, the identity automorphism from $\mathfrak{S}_E$ onto $\mathfrak{S}_E$ is a group action on the set E. Let $\overline{\sigma}$ be the subgroup generated by $\sigma \in \mathfrak{S}_E$, then the inclusion map from $\overline{\sigma}$ to $\mathfrak{S}_E$ is also a group action on E. When $E = \mathbb{Z}_n$ (the cyclic group of order n), from Remark 2.2, we can create orbits by applying the action of the group generated by the permutation $x \mapsto tx$ to the elements of $\mathbb{Z}_n$, where t is a multiplier. P and N are unions of some of these orbits and every element in an orbit has the same coefficient.

3. **Nonexistence of** $CW(88, 81)$

Let $\mathbb{Z}[G]$ be the group ring over the group G and let $A = \sum_{g\in G} a_g g$ be an arbitrary element of $\mathbb{Z}[G]$. We define $S(A) = \sum_{g\in G} a_g$. (This is a finite sum as A has finite support.) If ϕ is a group homomorphism, then ϕ can be *linearly extended* to be a ring homomoprhism on $\mathbb{Z}[G]$. This is to say $\phi(A) = \sum_{g\in G} a_g \phi(g)$.

Lemma 3.1. *If $\phi : \mathbb{Z}[G] \to \mathbb{Z}[G]$ is a linearly-extended ring homomorphism then $S(\phi(A)) = S(A)$.*

Proof. $S(\phi(A)) = S(\phi(\sum_{g\in G} a_g g)) = S(\sum_{g\in G} a_g \phi(g)) = \sum_{g\in G} a_g = S(A)$ □

An *integer circulant weighing matrix* of order n of weight k, written as $ICW(n, k)$, is defined similarly as a $CW(n, k)$ except that the matrix entries can be arbitrary integers. If the entries are restricted to be in the set $\{0, \pm1, \pm2, \ldots, \pm a\}$ we write $ICW_{\{0,\pm1,\pm2,\ldots,\pm a\}}$ or simply ICW_a.

Remark 3.2. *Naturally, the group ring notions can be extended to include ICW matrices. The Multiplier Theorem can also be applied. We observe that if $\sum_g a_g g$ is an $ICW(n, k)$, then $\sum_g a_g = \sqrt{k}$ and $\sum_g a_g^2 = k$.*

Lemma 3.3. *$9I_4$ is the only $ICW(4, 81)$ up to equivalence.*

Proof. The orbits of $\mathbb{Z}_4$ under the action of 3 are:

$$O_1 = \{0\}$$
$$O_2 = \{1, 3\}$$
$$O_3 = \{2\}.$$

Since 4 and 81 are relatively prime, Remark 2.2 applies, i.e., if A is an $ICW(4, 81)$, then

$$\begin{aligned} A &= aO_1 + bO_2 + cO_3 \\ &= ag^0 + b(g^1 + g^3) + cg^2 \\ &= ae + bg + bg^3 + cg^2 \text{ where } a, b, c \in \mathbb{Z}. \end{aligned}$$

Since A is an ICW of weight 81 we have

$$\begin{cases} a + b + b + c = a + 2b + c = 9 \\ a^2 + b^2 + b^2 + c^2 = a^2 + 2b^2 + c^2 = 81. \end{cases}$$

What are the possible values for b? Since $a^2 + 2b^2 + c^2 = 81$ we get $2b^2 \leq 81$ so $b^2 \leq 40$, then the possible values for b are $0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6$.

Hence

$$\begin{aligned}
&\text{if } b = 0 \text{ then we have } a^2 + c^2 = 81\\
&\text{if } b = \pm 1 \text{ then we have } a^2 + c^2 = 79\\
&\text{if } b = \pm 2 \text{ then we have } a^2 + c^2 = 73\\
&\text{if } b = \pm 3 \text{ then we have } a^2 + c^2 = 63\\
&\text{if } b = \pm 4 \text{ then we have: } a^2 + c^2 = 49\\
&\text{if } b = \pm 5 \text{ then we have } a^2 + c^2 = 31\\
&\text{if } b = \pm 6 \text{ then we have } a^2 + c^2 = 9.
\end{aligned}$$

The integers 79, 63 and 31 are not the sum of two perfect squares, leaving 81, 73, 49 and 9 as the only possibilities for $a^2 + c^2$.

Case $b = 0$: We have $a^2 + c^2 = 81$, hence $\{a, c\} = \{0, \pm 9\}$. This leads to the solution $9e$ which is the group ring representation of $9I_4$.

Case $b = \pm 2$: We have: $a^2 + c^2 = 73$, hence $\{a, c\} = \{\pm 3, \pm 8\}$. We need $a + 2b + c = 9$, which is $\pm 3 \pm 4 \pm 8 = 9$. The only possibility is $-3 + 4 + 8 = 9$, meaning without loss of generality, $a = -3$, $b = 2$ and $c = 8$. This leads to a contradiction as $B = -3e + 2g + 2g^3 + 8g^2$ is not a solution, since $BB^{-1} \neq 81e$.

Case $b = \pm 4$: We have: $a^2 + c^2 = 49$, hence $\{a, c\} = \{0, \pm 7\}$. We need $a \pm 2b + c = 9$ which is $0 \pm 8 \pm 7 = 9$. This is impossible.

Case $b = \pm 6$: We have: $a^2 + c^2 = 9$ and $\{a, c\} = \{0, \pm 3\}$. We need $a \pm 2b + c = 9$ which is $0 \pm 12 \pm 3 = 9$. The only possibility is $0 + 12 - 3 = 9$, meaning without loss of generality $a = -3$, $b = 6$ and $c = 0$. This leads to a contradiction as $B = -3e + 6g + 6g^3 + 0g^2$ is not a solution because $BB^{-1} \neq 81e$.

This proves that the only $ICW(4, 81)$ is the trivial one, i.e., $9I_4$.

□

Theorem 3.4. *There does not exist a* $CW(88, 81)$.

Proof. Assume that there is one which we will call A. Consider the homomorphism $\phi_2 : g \to g^2$, then

$$\phi_2(CW(88, 81)) = ICW_2(44, 81) = B.$$

Let n_1 denote the number of ± 1 coefficients in B and let n_2 denote the number of ± 2 coefficients in B. We have

$$n_1 + 4n_2 = 81. \tag{3.1}$$

The coefficients of $B = \phi_2(A)$ are of the form $a_i + a_{i+44}$. Therefore a ± 1 appears as a coefficient in B only if a 0 of A is added with a ± 1 of A. We get four cases from the seven zeros of A.

Case 1: All zeros are combined with a ± 1, we have seven ± 1's in B, i.e., $n_1 = 7$. Hence by (3.1), $4n_2 = 74$ but n_2 being an integer this case is impossible.

Case 2: Only one pair of zeros are combined with each other, we have five which are combined with ± 1's, hence we have five ± 1's in B, i.e., $n_1 = 5$. Hence by (3.1), $4n_2 = 76$, so $n_2 = 19$.

Case 3: Two pairs of zeros are combined with each other, we have three which are combined with ± 1's, hence we have three ± 1's in B, i.e., $n_1 = 3$. Hence by (3.1), $4n_2 = 78$ but n_2 being an integer this case is impossible.

Case 4: Three pairs of zeros are combined with each other, we have one which is combined with a ± 1, hence we have only one ± 1 in B, i.e., $n_1 = 1$. Hence by (3.1), $4n_2 = 80$, so $n_2 = 20$.

Let us first look at Case 4, i.e., $n_1 = 1$ and $n_2 = 20$. For $i = 1$ and 2, let n_i^+ denote the number of $+i$ coefficients in B and let n_i^- denote the number of $-i$ coefficients in B. By Lemma 3.1, we have

$$S(B) = S(\phi_2(A)) = S(A) = +\sqrt{81} = 9. \tag{3.2}$$

Thus we have the two equations

$$n_2^+ + n_2^- = 20 \text{ and } 2n_2^+ - 2n_2^- \pm 1 = 9,$$

from which we obtain

$$4n_2^+ \pm 1 = 49.$$

Because n_2^+ must be an integer, we conclude that $n_2^+ = 12$, $n_2^- = 8$, $n_1^+ = 1$ and $n_1^- = 0$.

Since 44 and 81 are relatively prime, Remark 2.2 applies to B. There are 9 orbits of $\mathbb{Z}_{44}$ under the action $g \mapsto 3g$. They are

$$\begin{aligned}
O_1 &= \{0\},\\
O_2 &= \{1, 3, 9, 27, 37, 23, 25, 31, 5, 15\},\\
O_3 &= \{2, 6, 18, 10, 30\},\\
O_4 &= \{4, 12, 36, 20, 16\},\\
O_5 &= \{7, 21, 19, 13, 39, 29, 43, 41, 35, 17\},\\
O_6 &= \{8, 24, 28, 40, 32\},\\
O_7 &= \{11, 33\},\\
O_8 &= \{14, 42, 38, 26, 34\} \text{ and}\\
O_9 &= \{22\},
\end{aligned}$$

and the orbit lengths are

$$1, 1, 2, 5, 5, 5, 5, 10 \text{ and } 10. \tag{3.3}$$

The only way to cover the eight -2 coefficients is one orbit of length 5, one orbit of length 2 and one orbit of length 1. We also need one orbit of length 1 to cover the 1 coefficient, so there is no orbit of length 1 or 2 left. Hence, it is impossible to cover the twelve $+2$ coefficients. This case leads to a contradiction.

Now, let us look at Case 2, i.e., $n_1 = 5, n_2 = 19$. The five ± 1 must all be 1 or all -1, because from (3.3) only an orbit of length 5 can cover n_1. Thus, by (3.2) we have

$$n_2^+ + n_2^- = 19 \text{ and } 2n_2^+ - 2n_2^- \pm 5 = 9,$$

and we obtain $4n_2^+ \pm 5 = 47$. Because n_2^+ must be an integer, we conclude that $n_2^+ = 13$, $n_2^- = 6$, $n_1^+ = 0$ and $n_1^- = 5$.

The only way to cover n_2^- is one orbit of length 1 and one orbit of length 5. There are two ways to cover n_2^+. One way is one orbit of length 10, one orbit of length 2 and one orbit of length 1. The other way is two orbits of length 5, one orbit of length 2 and one of length 1. n_1^- is covered by one orbit of length 5. Hence, both orbits of length one are used to cover either a $+2$ or a -2. This means that the coefficient of $e = g^0$ in B is either $+2$ or -2.

Consider the homomorphism generated by $\phi_{11} : g \to g^{11}$. This will send B to an $ICW(4, 81)$. But by Lemma 3.3 the only possibility for this latter ICW is $9e$. The preimage of e has 11 elements, namely $\{g^i : i \in O_1 \cup O_4 \cup O_6\}$. Writing $B = \pm 2e + xO_4 + yO_6 + R$ where $e \notin \phi_{11}(R)$, then

$$\begin{aligned}\phi_{11}(B) &= \phi_{11}(\pm 2e + xO_4 + yO_6 + R)\\ &= \pm 2\phi_{11}(e) + x\phi_{11}(O_4) + y\phi_{11}(O_6) + \phi_{11}(R).\end{aligned}$$

Observe that

$$\phi_{11}(O_4) = \phi_{11}(O_6) = 5e \text{ and } \phi_{11}(e) = e.$$

Hence,

$$\pm 2\phi_{11}(e) + x\phi_{11}(O_4) + y\phi_{11}(O_6) + \phi_{11}(R) = \pm 2e + 5xe + 5ye + \phi_{11}(R).$$

Therefore the coefficient of e in the image of $\phi_{11}(B)$ is $\pm 2 + 5x + 5y$ which must equal 9 (as $\phi_{11}(B) = 9e$), but there are no integer solutions, as 5 does not divide 11 or 8. Hence, this case too, leads to a contradiction. □

4. Nonexistence of $CW(99, 81)$

In this section we prove the nonexistence of $CW(99, 81)$ using purely algebraic methods. First we need two lemmas. The first one is an easy combinatorial one while the second one, which is stated and proven in [3], is of a more advanced nature.

Lemma 4.1. *Let $y = g(\beta) + G$ be an element of the group ring $\mathbb{Z}[G]$ where $G = \langle\alpha\rangle \oplus \langle\beta\rangle$, let a be the order of α and b be the order of β, then $|supp(y)| \geq b(a-1)$.*

Proof. The group G has $ab - b$ elements which are not contained in $\langle\beta\rangle$, namely all the elements of $G - \langle\beta\rangle$. Regardless of how $g(\beta)$ is defined, $g(\beta) + G$ will contain all these elements. Hence $|\text{supp}(y)| \geq b(a-1)$. □

A *character* χ of the group G is a homomorphism from G to the multiplicative group of the nonzero complex numbers. We can extend χ linearly to $\mathbb{Z}[G]$. This extension will also be denoted by χ. Then, χ is a ring homomorphism of $\mathbb{Z}[G]$ into the field $\mathbb{C}$ of complex numbers.

Given two primes p and q, we remind the reader that the *multiplicative order* of p modulo q is the smallest positive integer n such that $p^n \equiv 1 \mod q$. The notation is usually written as $n = ord_q(p)$.

Lemma 4.2. *Let $G = \langle\alpha\rangle \oplus \langle\beta\rangle$ be a cyclic group of order $v = p^t q$ where p, q are odd primes, $gcd(p(p-1), q) = 1$, $ord_q(p) = \frac{(q-1)}{2}$, the order of α is p^t and the order of β is q. If $y \in \mathbb{Z}[G]$ satisfies $\chi(y)\overline{\chi(y)} = p^{2r}$ for all nonprincipal characters χ of G, then either*

$$y = p\alpha^c f(\beta) + \langle\alpha^{p^{t-1}}\rangle x,$$

where $x \in \mathbb{Z}[G]$, $f(X) \in \mathbb{Z}[X]$ (the polynomial ring with integer coefficients) and $f(\beta)f(\beta^{-1}) = p^{2(r-1)}$ or

$$y = \alpha^c g(\beta) + \mu G,$$

where μ is an integer, $g(X) \in \mathbb{Z}[X]$ and $g(\beta)g(\beta^{-1}) = p^{2r}$.

Theorem 4.3. *Let p and q be odd primes, satisfying:*

(1) $gcd(p(p-1), q) = 1$,
(2) $ord_q(p) = \frac{(q-1)}{2}$,
(3) $q \leq p^{2r} \leq q(p^t - 1)$,

Note that r and t both must be strictly positive integers. If these three items are satisfied, then there does not exist a matrix of the form $CW(p^t q, p^{2r})$.

Proof. Assume the contrary, let y be a $CW(p^t q, p^{2r})$ with p and q satisfying all the conditions stated in the theorem. We have $yy^{-1} = p^{2r}$, hence for any character χ of G we have: $\chi(y)\overline{\chi(y)} = p^{2r}$. Lemma 4.2 can be applied and therefore there are two possibilities for y.

Case 1: $y = p\alpha^c f(\beta) + \langle\alpha^{p^{t-1}}\rangle x$, where $x \in \mathbb{Z}[G]$, $f(X) \in \mathbb{Z}[X]$ and $f(\beta)f(\beta^{-1}) = p^{2(r-1)}$

Since $f(\beta)f(\beta^{-1}) = p^{2(r-1)}$, $f(\beta)$ cannot be zero. Hence $f(\beta)$ contains a $\lambda\beta^{n_1}$ with $\lambda \neq 0$ for some n_1.

Then, $\beta^{-n_1}\alpha^{-c}y = pf_1(\beta) + \langle\alpha^{p^{t-1}}\rangle x_1$, with the coefficient of e in f_1 being nonzero. So without loss of generality, we can assume that $y = pf(\beta) + \langle\alpha^{p^{t-1}}\rangle x$ without the coefficient of e in f being nonzero.

Denote $\langle\alpha^{p^{t-1}}\rangle$ by P. Therefore, we have $Px = P\sum_{g\in G} x_g g = \sum_{g\in G} x_g Pg$.

(Let $G = P_1 \cup P_2 \cup \cdots \cup P_n$ be the coset decomposition of G with respect to P. We have $\sum_{g\in G} x_g Pg$, since the coset decomposition implies $\sum_{g\in G} x_g Pg = \sum_{i=1}^{n}\sum_{g\in P_i} x_g Pg$)

Therefore, $\sum_{i=1}^{n}\sum_{g\in P_i} x_g Pg = \sum_{i=1}^{n}\sum_{g\in P_i} x_g P_i$ (since $g \in P_i$ implies $Pg = P_i$) (So, $Px = \sum_{i=1}^{n}\sum_{g\in P_i} x_g P_i = \sum_{i=1}^{n}(\sum_{g\in P_i} x_g)P_i$.)

Let $\omega_i = \sum_{g \in P_i} x_g$, then $Px = \sum_{i=1}^{n} \omega_i P_i$.

We have $e \in P$. Hence, the coefficient of e in Px is ω_1, but ω_1 is also the coefficient of (any) $\alpha \in P$. $f(\beta)$ is a sum of powers of β, so it cannot contain α. Therefore, the coefficient of α in $y = pf(\beta) + \langle \alpha^{p^{t-1}} \rangle x = pf(\beta) + Px$ is the same as the coefficient of α in Px which is ω_1.

The coefficient of e in $y = pf(\beta) + Px$ is $p\lambda + \omega_1$. y is a ± 1 element of $\mathbb{Z}[G_{p^t q}]$. Hence, both of these coefficients are in $\{0, \pm 1\}$. Therefore,

$$\begin{cases} -1 \leq p\lambda + \omega_1 \leq 1 \\ -1 \leq \omega_1 \leq 1 \end{cases}$$

Multiplying the second inequality by -1 and adding the two $-2 \leq p\lambda \leq 2$, which is impossible since λ is a nonzero integer (hence of absolute value larger or equal to 1). and p is a (prime) number strictly larger than 2. Therefore, the first possibility for y does not occur.

Case 2: $y = \alpha^c g(\beta) + \mu G$, where μ is an integer, $g(X) \in \mathbb{Z}[X]$ and $g(\beta)g(\beta^{-1}) = p^{2r}$. If $\mu = 0$, then $y = \alpha^c g(\beta)$. Hence, y is a $CW(q, p^{2r})$, but by the assumption y is a $CW(p^t q, p^{2r})$. Therefore μ must be nonzero. Multiplying y by α^{-c}, we have $y = g(\beta) + \mu G$, $\mu \neq 0$.

Because $G = \langle \alpha \rangle \oplus \langle \beta \rangle$, $\alpha \notin g(\beta)$, and coefficients other than $\{-1, 0, 1\}$ cannot be in y, μ must be ± 1. Without loss of generality, it can be assumed that $y = g(\beta) + G$ (multiply by -1 if necessary).

By applying Lemma 4.1, with $b = q$ and $a = p^{2t}$ we have the inequality

$$|\mathrm{supp}(y)| \geq q(p^{2t} - 1). \tag{4.1}$$

Since y is a CW of weight p^{2r}, $|\mathrm{supp}(y)| = p^{2r}$. Therefore, by (4.1),

$$p^{2r} \geq q(p^{2t} - 1).$$

This contradicts the third condition of the assumption. Therefore, the second possibility cannot occur.

□

We leave the second part of our main result as a corollary.

Corollary 4.4. *There is no matrix of the form $CW(99, 81)$.*

Proof. We have $CW(99, 81) = CW(3^2 \cdot 11, 3^4)$, let's apply Theorem 4.3.

We have $p = 3$ and $q = 11$, let's check the three conditions of Theorem 4.3:

(1) $(p(p-1), q) = 1$ which is $(3 \cdot 2, 11) = 1$,
(2) $ord_q(p) = \frac{(q-1)}{2}$ which is $3^5 = 243 \equiv 1 \pmod{11}$ so $ord_{11}(3) = \frac{11-1)}{2} = 5$,
(3) $q \leq p^{2r} \leq q(p^t - 1)$ which is $11 \leq 81 \leq 11(3^2 - 1) = 88$.

All the conditions of Theorem 4.3 are verified. Hence there is no $CW(3^2 \cdot 11, 3^4) = CW(99, 81)$. □

Acknowledgments

The authors would like to thank the referee of this paper for providing helpful comments and for noticing the nonexistence of all other CW matrices of order less than or equal to 500 that follow from Theorem 4.3. A table of these matrices follows below along with the parameter values that would satisfy the hypothesis of Theorem 4.3.

CW	p	q	r	t
$CW(99,81)$	3	11	2	2
$CW(297,81)$	3	11	2	3
$CW(207,81)$	3	23	2	2
$CW(333,81)$	3	37	2	2
$CW(141,81)$	3	47	2	1
$CW(423,81)$	3	47	2	2
$CW(177,81)$	3	59	2	1
$CW(213,81)$	3	71	2	1
$CW(55,25)$	5	11	1	1
$CW(275,25)$	5	11	1	2
$CW(95,25)$	5	19	1	1
$CW(475,25)$	5	19	1	2
$CW(217,49)$	7	31	1	1
$CW(329,49)$	7	47	1	1
$CW(299,169)$	13	23	1	1
$CW(377,169)$	13	29	1	1
$CW(323,289)$	17	19	1	1

References

[1] K. T. Arasu and A. J. Gutman, Circulant weighing matrices, *Cryptogr. Commun.*, **2** (2010) 155–171.

[2] K. T. Arasu, J. F. Dillon, D. Jungnickel and A. Pott, The solution of the waterloo problem, *J. Combin. Theory Ser. A*, **71** (1995) 316–331.

[3] K. T. Arasu and S. L. Ma, Abelian difference sets without self-conjugacy, *Des. Codes Cryptogr.*, **15** (1998) 223–230.

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

[5] R. L. McFarland, *On Multipliers of Abelian Difference Sets*, PhD thesis, The Ohio State University, 1970.

[6] R. C. Mullin, *A Note On Balanced Weighing Matrices*, **452** of Lecture Notes in Mathematics, Springer-Verlag, Berlin-Heidelberg-New York, 1975.

[7] Y. Strassler, *The classification of circulant weighing matrices with weight 9*, PhD thesis, Bar-Ilan University, 1997.

[8] M. M. Tan, *Circulant weighing matrices and multipliers*, Preprint, 2014.

[9] M. M. Tan, *Nonexistence of circulant weighing matrices of weight 36 and orders 60*, Preprint, (2014).

[10] V. Yorgov, *On the existence of certain circulant weighing matrices*, J. Combin. Math. Combin. Comput., **86** (2013) 73–85.

K. T. Arasu
Department of Mathematics and Statistics, Wright State University, Dayton, OH, USA
Email: k.arasu@wright.edu

Kyle Bayes
Department of Mathematical Sciences, SUNY-Binghamton, P. O. Box 6000, Binghamton, NY, USA
Email: bayes@math.binghamton.edu

Ali Nabavi
Institute for Research in Fundamental Sciences (IPM), Tehran, Iran
Email: ali_nabavi2000@yahoo.com