New Nonexistence Results on Circulant Weighing Matrices

K. T. Arasu[1], Daniel M. Gordon[2], and Yiran Zhang*[3]

[1]Riverside Research
2640 Hibiscus Way
Beavercreek, OH 45431
karasu@riversideresearch.org

[2]Center for Communications Research
4320 Westerra Court
San Diego, CA 92121
gordon@ccrwest.org

[3]Loyola University
Chicago, IL 60660
yzhang45@luc.edu

July 21, 2019

Abstract

A circulant weighing matrix $W = (w_{i,j}) \in CW(n, k)$ is a square matrix of order n and entries $w_{i,j}$ in {-1, 0, +1} such that $WW^T = kI_n$. In his thesis [7], Strassler gave tables of known results on such matrices with $n \leq 200$ and $k \leq 100$.

In the latest version of Strassler's tables given by Tan [8], there are 34 open cases remaining. In this paper we resolve six of these cases, showing that there are no weight 81 CW matrices for $n = 110$, 130, 143 or 154, and also no $CW(116, 49)$ or $CW(143, 36)$.

1 Introduction

A weighing matrix $W = W(n, k)$ with weight k is a square matrix of order n and entries $w_{i,j}$ in {-1, 0, +1} such that $WW^T = kI_n$ where W^T is the transpose of W and I_n is the $n \times n$ identity matrix.

*REU research supported by an NSF grant and presented at the Young Mathematicians' Conference at OSU August 2015

A circulant weighing matrix $CW(n,k)$ is a special type of weighing matrix in which every row except for the first is a right cyclic shift of the previous row. Let P be the set of locations with a $+1$ in the first row, and N be the locations with a -1. Then $|P|+|N|=k$.

The following facts are well known [1, 2, 3].

i. $k = s^2$ for some positive integer s

ii. $|P| = \frac{s^2+s}{2}$

iii. $|N| = \frac{s^2-s}{2}$

It must be noted that within a weighing matrix, interchanging the $(+)$s and $(-)$s will not change any properties of the matrix. We choose $|P|$ and $|N|$ by convention. For further information on weighing matrices, we refer the reader to [1, 2, 3].

To illustrate these ideas, $\mathbb{Z}_7$ gives $CW(7,4)$, which is shown in matrix form below:

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

We see that $|P|=3$ and $|N|=1$; their sum is 4, a square.

In his 1997 thesis [7], Strassler gave tables of known results on such matrices with $n \leq 200$ and $k \leq 100$. Over the years many open cases in his tables have been resolved. In Tan's 2018 version of the tables there are 34 open cases remaining. In this paper we will show that no $CW(n,k)$ exists for six of those cases.

2 Preliminaries

We will use standard results from the literature on group rings and multipliers for our proofs.

Let R be a commutative ring with identity i_R and G be a finite multiplicatively written group of order n. Let $R[G] = \{\sum_{g\in G} a_g g \mid a_g \in R\}$ denote the group ring of G over R.

In this paper, we will be working with $\mathbb{Z}[G]$, the group ring of G over the ring $\mathbb{Z}$ of integers. Furthermore, for an element A of $\mathbb{Z}[G]$ and integer t, $A^{(t)}$ denotes the image of A under the group homomorphism $x \to x^t$, extended linearly to all of $\mathbb{Z}[G]$.

A $CW(n,k)$ is equivalent to an element X of the group ring $\mathbb{Z}[\mathbb{Z}_n]$ with coefficients in $\{-1,0,1\}$ such that

$$XX^{(-1)} = k. \tag{1}$$

The following result, given in this form for group rings in [5], will be used below. A prime p is called *self-conjugate* modulo n if there is an integer i with

$$p^i \equiv -1 \bmod v(n),$$

where $v(n)$ is the largest divisor of n relatively prime to p.

Theorem 1. *For an abelian group G of order n, if $X \in \mathbb{Z}[G]$ satisfies*

$$XX^{(-1)} \equiv 0 \bmod p^{2a},$$

for a positive integer a and prime p, and p is self-conjugate mod n then,

$$X \equiv 0 \bmod p^a.$$

Next, we will discuss multipliers.

Definition 2.1. *Let G be a finite abelian group of order n and D be a subset of G. Let t be an integer relatively prime to n. If $D^{(t)} = Dg$ for some g in G, then t is called a multiplier of D.*

For example, in $\mathbb{Z}_{11}$, 3 is a multiplier of $D = \{2, 4, 5, 6, 10\}$.

$$D = \{2, 4, 5, 6, 10\}$$
$$D^{(3)} = \{6, 1, 4, 7, 8\} = D + 2$$

The following theorem is well-known; see, for example, [3]:

Theorem 2. *Let A be a $CW(n, k)$ circulant weighing matrix, where $k = p^{2r}$ is a prime power, and $\gcd(n, k) = 1$. Then p is a multiplier of A. Furthermore, p fixes some translate of A.*

We will frequently use this theorem. When a $CW(n, k)$ has a multiplier p, then some translate of it is fixed by the group generated by p mod n, and so P and N must both be unions of orbits of $\mathbb{Z}_n$ under the action of multiplying by p. Needing to exhaust unions of orbits instead of arbitrary subsets will often transform an infeasible search into a feasible one, and allow us to handle the cases in this paper by hand.

Let $\sigma : G \to H$ be some homomorphism between the groups G and H. Then σ can be extended linearly as a ring homomorphism from $\mathbb{Z}[G] \to \mathbb{Z}[H]$. The linearly extended form of σ between the rings $\mathbb{Z}[G] \to \mathbb{Z}[G/H]$ is called folding.

For a $CW(n, k)$ in $G = \mathbb{Z}_n$ corresponding to the group ring element

$$A = \sum_{g \in G} a_g g$$

we will let $i_h = \sum_{\sigma(g)=h} a_g$ denote the *intersection numbers*, so that

$$\sigma(A) = \sum_{g \in G} a_g \sigma(g) = \sum_{h \in H} i_h h.$$

As is common practice with difference sets, we may use these intersection numbers to investigate the existence of circulant weighing matrices, using:

Lemma 2.1. *For a $CW(n,k)$ circulant weighing matrix A and H a subgroup of $\mathbb{Z}_n$, we have*

$$\sum_{h\in H} i_h = s, \tag{2}$$

$$\sum_{h\in H} i_h^2 = s^2 = k. \tag{3}$$

In all of the proofs in this paper, we will consider possible circulant weighing matrices in $\mathbb{Z}_n = \mathbb{Z}_h \times \mathbb{Z}_w$, where h and w are relatively prime. If p is a multiplier for a $CW(n,k)$ matrix A, then we may assume that a translate of A is fixed by the group $\langle p \rangle \pmod n$, and so P and N must each be the union of orbits of the multiplier group. This applies to the folded versions in $\mathbb{Z}_h$ and $\mathbb{Z}_w$ as well, so we may use Lemma 2.1 to get information about what orbits are in P and N in the two subgroups, and from that limit the possibilities for orbits in the full group.

3 Circulant Weighing Matrices of Weight 81

Proposition 3.1. *A $CW(110,81)$ does not exist.*

Proof. Suppose a $CW(110,81)$ exists. Then $WW^{(-1)} = 81$, $(P-N)(P-N)^{(-1)} = 81$, $|P| = 45, |N| = 36$ and 3 is its multiplier. Note that $\mathbb{Z}_{110} = \mathbb{Z}_{11} \times \mathbb{Z}_{10}$. Let σ and τ be projections from $\mathbb{Z}_{110}$ to $\mathbb{Z}_{10}$ and $\mathbb{Z}_{11}$, respectively. The $\mathbb{Z}_{11}$ orbits under the multiplier action $x \to 3x$ are:

$$\{0\}$$

$$\{1,3,9,5,4\}$$

$$\{2,6,7,10,8\}$$

The $\mathbb{Z}_{10}$ orbits under the multiplier action $x \to 3x$ are:

$$\{0\}$$

$$\{5\}$$

$$\{1,3,9,7\}$$

$$\{2,6,8,4\}$$

Table 1 shows the structure of orbits of 3 in $\mathbb{Z}_{110}$ relative to $\mathbb{Z}_{10}$ and $\mathbb{Z}_{11}$. In the table, $\langle x \rangle_m$ denotes the orbit of 3 with representative x and size m. The top row and left column indicate orbits in $\mathbb{Z}_{11}$ and $\mathbb{Z}_{10}$, respectively, and the numbers on the right and bottom indicate the value of $|P| - |N|$ for orbits in that row or column. Each $\mathbb{Z}_{110}$ orbit is in the row and column of the orbits it projects to modulo 10 and 11.

Since 3 is self-conjugate mod 10, by Theorem 1 we have $\sigma(P-N) \equiv 0 \pmod 9$, and so $\sigma(P-N) = 9$. This means that the sum of the first row is 9, and the other row sums are all zero. The only way to do that is for $\langle 0 \rangle_1$ to be in N, and $\langle 20 \rangle_5$ and $\langle 10 \rangle_5$ to be in P.

	$\mathbb{Z}_{11}$			
$\mathbb{Z}_{10}$	$\langle 0\rangle_1$	$\langle 1\rangle_5$	$\langle 2\rangle_5$	
$\langle 0\rangle_1$	$\langle 0\rangle_1$	$\langle 20\rangle_5$	$\langle 10\rangle_5$	9
$\langle 5\rangle_1$	$\langle 55\rangle_1$	$\langle 5\rangle_5$	$\langle 35\rangle_5$	0
$\langle 1\rangle_4$	$\langle 11\rangle_4$	$\langle 3\rangle_{20}$	$\langle 7\rangle_{20}$	0
$\langle 2\rangle_4$	$\langle 22\rangle_4$	$\langle 4\rangle_{20}$	$\langle 2\rangle_{20}$	0
	a	$5b$	$5c$	

Table 1: Orbit information for $CW(110, 81)$

	$\mathbb{Z}_{11}$			
$\mathbb{Z}_{14}$	$\langle 0\rangle_1$	$\langle 1\rangle_5$	$\langle 2\rangle_5$	
$\langle 0\rangle_1$	$\langle 0\rangle_1$	$\langle 14\rangle_5$	$\langle 28\rangle_5$	9
$\langle 7\rangle_1$	$\langle 77\rangle_1$	$\langle 49\rangle_5$	$\langle 7\rangle_5$	0
$\langle 1\rangle_6$	$\langle 11\rangle_4$	$\langle 3\rangle_{30}$	$\langle 13\rangle_{30}$	0
$\langle 2\rangle_6$	$\langle 22\rangle_4$	$\langle 4\rangle_{30}$	$\langle 2\rangle_{30}$	0
	a	$5b$	$5c$	

Table 2: Orbit information for $CW(154, 81)$

Applying Lemma 2.1, we get equations

$$a + 5(b + c) = 9 \tag{4}$$

and

$$a^2 + 5(b^2 + c^2) = 81 \tag{5}$$

for $\mathbb{Z}_{11}$. Since, for the rows after the first, the size of the first column orbit is different from the other two, the row sums being zero means that in each row one of the orbits in the second and third columns must be in P, and the other in N, and the first row orbit in neither. So we must have $a = -1$. But equations (4) and (5) have no integer solutions with $a = -1$.

□

Proposition 3.2. *A $CW(154, 81)$ does not exist.*

Proof. The proof for this is nearly identical to the above Proposition 2. The orbit information is given in Table 2, and 3 is self-conjugate modulo 14.

□

Proposition 3.3. *A $CW(130, 81)$ does not exist.*

	$\mathbb{Z}_{13}$					
$\mathbb{Z}_{10}$	$\langle 0\rangle_1$	$\langle 1\rangle_3$	$\langle 2\rangle_3$	$\langle 4\rangle_3$	$\langle 7\rangle_3$	
$\langle 0\rangle_1$	$\langle 0\rangle_1$	$\langle 40\rangle_3$	$\langle 70\rangle_3$	$\langle 10\rangle_3$	$\langle 20\rangle_3$	9
$\langle 5\rangle_1$	$\langle 65\rangle_1$	$\langle 35\rangle_3$	$\langle 5\rangle_3$	$\langle 25\rangle_3$	$\langle 85\rangle_3$	0
$\langle 1\rangle_4$	$\langle 13\rangle_4$	$\langle 3\rangle_{12}$	$\langle 19\rangle_{12}$	$\langle 17\rangle_{12}$	$\langle 7\rangle_{12}$	0
$\langle 2\rangle_4$	$\langle 26\rangle_4$	$\langle 14\rangle_{12}$	$\langle 2\rangle_{12}$	$\langle 4\rangle_{12}$	$\langle 8\rangle_{12}$	0
	x	$3y_0$	$3y_1$	$3y_2$	$3y_3$	

Table 3: Orbit information for $CW(130, 81)$

Proof. The orbit information is given in Table 3. While 3 is still self-conjugate modulo 10, the orbit structure is different, so the argument is not quite as straightforward.

The first row sum is 9, so three of the four size-3 orbits must be in P. The other row sums are 0, so the first column can never be included, and the other four columns for each row must have the same number of orbits in N and P.

Since $|P| = 45$ and $|N| = 36$, the parts of these sets in the last three rows must consist of three size-12 orbits each, or two size-12 sets and all four remaining size-3 orbits. But there is no way to satisfy this while having zero row sums.

□

Proposition 3.4. *A $CW(143, 81)$ does not exist.*

Proof. Suppose a $CW(143, 81)$ exists; $WW^{(-1)} = 81$, $(P - N)(P - N)^{(-1)} = 81$, $|P| = 45, |N| = 36$ and 3 is its multiplier. Note that $\mathbb{Z}_{143} = \mathbb{Z}_{11} \times \mathbb{Z}_{13}$. The $\mathbb{Z}_{11}$ orbits under the multiplier action $x \to 3x$ are:

$$\{0\}$$

$$\{1, 3, 9, 5, 4\}$$

$$\{2, 6, 7, 10, 8\}$$

The $\mathbb{Z}_{13}$ orbits under the multiplier action $x \to 3x$ are:

$$\{0\}$$

$$\{1, 3, 9\}$$

$$\{2, 6, 5\}$$

$$\{4, 12, 10\}$$

$$\{7, 8, 11\}$$

Table 4 gives the orbit information.

Unfortunately, 3 is not self-conjugate modulo 11 or 13, so we need to work a bit harder.

				$\mathbb{Z}_{13}$			
$\mathbb{Z}_{11}$	$\langle 0\rangle_1$	$\langle 1\rangle_3$	$\langle 2\rangle_3$	$\langle 4\rangle_3$	$\langle 7\rangle_3$	
$\langle 0\rangle_1$	$\langle 0\rangle_1$	$\langle 22\rangle_3$	$\langle 44\rangle_3$	$\langle 77\rangle_3$	$\langle 11\rangle_3$	a
$\langle 1\rangle_5$	$\langle 26\rangle_5$	$\langle 1\rangle_{15}$	$\langle 5\rangle_{15}$	$\langle 4\rangle_{15}$	$\langle 20\rangle_{15}$	$5b$
$\langle 2\rangle_5$	$\langle 13\rangle_5$	$\langle 29\rangle_{15}$	$\langle 2\rangle_{15}$	$\langle 10\rangle_{15}$	$\langle 7\rangle_{15}$	$5c$
	x	$3y_0$	$3y_1$	$3y_2$	$3y_3$	

Table 4: Orbit information for $CW(143, 81)$

Applying Lemma 2.1, we get equations

$$x + 3(y_0 + y_1 + y_2 + y_3) = 9$$
$$x^2 + 3(y_0^2 + y_1^2 + y_2^2 + y_3^2) = 81$$

for $\mathbb{Z}_{13}$, and

$$a + 5(b + c) = 9$$
$$a^2 + 5(b^2 + c^2) = 81$$

for $\mathbb{Z}_{11}$.

For $\mathbb{Z}_{11}$ the integer solutions are $(9, 0, 0)$, $(4, 3, -2)$, and $(-6, 3, 0)$ (together with swapping the second and third coordinates).

The first one is impossible, since it forces three size-3 orbits in the first row to be in P, leaving 36 remaining elements, but the orbits in the other rows all have size a multiple of 5. Similarly for the second solution, the first row sum being 4 means that we either have orbits in the first row contributing 4 (the size-1 and a size-3 orbit in P, and none in N) or 7 (the size-1 and two size-3 orbits in P, and the remaining orbit in N), but again the number of remaining elements is not a multiple of 5.

Finally for $(a, b, c) = (-6, 3, 0)$, the first row is forced to have two size-3 orbits in N, and none in P. This leaves 45 elements of P and 30 of N for the other rows, and so one row must have two size-15 orbits in P and one in N, while the other has one of each. The size-5 orbits cannot be used, so x must be 0.

There are three solutions to the $\mathbb{Z}_{13}$ equations with $x = 0$:
$(0, 3, 3, 0, -3)$,
$(0, 4, 1, 1, -3)$, and
$(0, 5, 0, -1, -1)$,
as well as permutations of the last four coordinates.

The first two may be quickly eliminated; in both cases we need a column sum equal to -9, and it is not possible to achieve this. However, the third solution can be satisfied. Table 5 shows a selection satisfying all the equations, although the orbits do not form a $CW(143, 81)$.

		$\mathbb{Z}_{13}$				
$\mathbb{Z}_{11}$	$\langle 0\rangle_1$	$\langle 1\rangle_3$	$\langle 2\rangle_3$	$\langle 4\rangle_3$	$\langle 7\rangle_3$	
$\langle 0\rangle_1$			$\langle 44\rangle_3$	$\langle 77\rangle_3$		-6
$\langle 1\rangle_5$		$\langle 1\rangle_{15}$	$\langle 5\rangle_{15}$	$\langle 4\rangle_{15}$		15
$\langle 2\rangle_5$			$\langle 2\rangle_{15}$	$\langle 10\rangle_{15}$		15
	0	15	-3	-3	0	

Table 5: A choice of orbits satisfying the equations (*not* a $CW(143, 81)$). Black orbits are in P, red in N.

To finish the proof, consider the orbits in $\mathbb{Z}_{13}$. There are six ways to pick two of the four columns with column sum -3, and then two ways to pick which of the other columns has sum 15. For each of these 12 choices, we can check that (1) is not satisfied. For example, the choices in Table 5 give

$$X = 5\langle 1\rangle - \langle 2\rangle - \langle 4\rangle,$$

and we find

$$XX^{(-1)} = 81 - 18\left(\langle 1\rangle + \langle 2\rangle - \langle 4\rangle + \langle 7\rangle\right).$$

□

4 Circulant Weighing Matrices of Other Weights

Proposition 4.1. *A $CW(143, 36)$ does not exist.*

Proof. The one difficulty here is that Theorem 2 does not apply, since k is not a prime power. However, a more general multiplier theorem ([4], Theorem 2.4) shows that 3 is still a multiplier, and so the table is exactly the same as Table 4.

The difference is that now $|P| = 21$ and $|N| = 15$, so the argument is easier. Because $|P| \equiv 1 \pmod 5$, the only way to make P as a union of orbits is to have $\langle 0\rangle_1$, the upper left orbit, in P, and nothing else in the top row. But all of the solutions in $\mathbb{Z}_{11}$, $(9, 0, 0)$, $(4, 3, -2)$, and $(-6, 3, 0)$, are incompatible with that, so no $CW(143, 36)$ exists.

□

Proposition 4.2. *A $CW(116, 49)$ does not exist.*

Proof. The equations mod 29 are

$$x + 7(y_0 + y_1 + y_2 + y_3) = 9$$
$$x^2 + 7(y_0^2 + y_1^2 + y_2^2 + y_3^2) = 81$$

There are two integer solutions:
$(9, 0, 0, 0, 0)$, and

				$\mathbb{Z}_{29}$			
$\mathbb{Z}_4$	$\langle 0\rangle_1$	$\langle 1\rangle_7$	$\langle 2\rangle_7$	$\langle 4\rangle_7$	$\langle 8\rangle_7$	
$\langle 0\rangle_1$	$\langle 0\rangle_1$	$\langle 16\rangle_7$	$\langle 32\rangle_7$	$\langle 4\rangle_7$	$\langle 8\rangle_7$	a_0
$\langle 2\rangle_1$	$\langle 58\rangle_1$	$\langle 30\rangle_7$	$\langle 2\rangle_7$	$\langle 6\rangle_7$	$\langle 10\rangle_7$	a_1
$\langle 1\rangle_2$	$\langle 29\rangle_2$	$\langle 7\rangle_{14}$	$\langle 3\rangle_{14}$	$\langle 5\rangle_{14}$	$\langle 15\rangle_{14}$	b
	x	$7y_0$	$7y_1$	$7y_2$	$7y_3$	

Table 6: Orbit information for $CW(116, 49)$

$(2, 3, 0, -1, -1)$
and the permutations of the last four coordinates.

The first one is clearly impossible because there are only four elements in the orbits in the first column. The second is impossible because $|P| = 28$ and $|N| = 21$. Since the orbits not in the first column all have size a multiple of 7, that solution forces P to have size equal to $2 \pmod 7$.

□

References

[1] K.T. Arasu, J.R. Hollon: Group Developed Weighing Matrices. *Australas. J. Combin.* 55 (2013), 205-233.

[2] K.T. Arasu, J. Seberry: On Circulant Weighing Matrices. *Australas. J. Combin.* 17 (1998), 21-37.

[3] K.T. Arasu, J. Seberry: Circulant Weighing Designs. *J. Combin. Des.* 4 (1996), 439-447.

[4] K.T. Arasu, Q. Xiang: Multiplier Theorems. *J. Combin. Des.* 3 (1995), 257-268.

[5] D. Jungnickel: On Lander's Multiplier Theorem for Difference Lists. *J. Comb. Info. and Syst. Sci.* 17 (1992), 123-129.

[6] A. Pott: *Finite geometry and character theory.* Springer Lecture Notes **1601**, Springer 1995.

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

[8] M.M. Tan: Group Invariant Weighing Matrices. *Designs, Codes and Cryptography*, 86 (2018), 2677-2702.

[9] R.J. Turyn: Character Sums and Difference Sets. *Pac. J. Math*, 15 (1965), 319-346.