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

November 2, 2020

Abstract

A circulant weighing matrix $W = (w_{i,j})$ is a square matrix of order n and entries $w_{i,j}$ in $\{0, \pm 1\}$ such that $WW^T = kI_n$. In his thesis [21], Strassler gave a table of existence results for such matrices with $n \leq 200$ and $k \leq 100$.

In the latest version of Strassler's table given by Tan [22] there are 34 open cases remaining. In this paper we give nonexistence proofs for 12 of these cases, report on preliminary searches outside Strassler's table, and characterize the known proper circulant weighing matrices.

1 Introduction

A *weighing matrix* $W = W(n, k)$ with weight k is a square matrix of order n with 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 $C = CW(n,k)$ is a 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 ([2], [3], [4]):

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

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

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

$|P|$ and $|N|$ are chosen by convention, since $-C$ is also a circulant weighing matrix. For further information on weighing matrices, we refer the reader to [2], [3], [4].

In his 1997 thesis [21], Strassler gave a table of known results on such matrices with $n \le 200$ and $k \le 100$. Over the years many open cases in his table have been resolved. In Tan's 2018 version of the table there are 34 open cases remaining. In this paper we will show that no $CW(n,k)$ exists for six of those cases.

2 Group Rings and Multipliers

It is more convenient to think of circulant weighing matrices $CW(n,k)$ as elements of a group ring. 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 $\mathbb{Z}[\mathbb{Z}_n]$, the group ring of the cyclic group of order n $\mathbb{Z}_n$ over the ring $\mathbb{Z}$ of integers. A $CW(n,k)$ A is an element of $\mathbb{Z}[\mathbb{Z}_n]$ such that

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

with all coefficients in $\{0, \pm 1\}$. If the coefficients of A are in $\{0, \pm 1, \pm 2, \ldots, \pm m\}$, then we will call it an *integer circulant weighing matrix*, denoted $ICW_m(n,k)$.

Representing elements of $\mathbb{Z}_n$ as $\{1, X, X^2, \ldots, X^{n-1}\}$ modulo $(X^n - 1)$, we may think of $CW(n,k)$ as a polynomial in $\mathbb{Z}[X]/(X^n - 1)$. For example, the $CW(7,4)$ is

$$A(X) = -1 + X + X^2 + X^4.$$

We will generally leave the $\bmod (X^n - 1)$ implicit. For any integer s, $X^s A(X)$ is an equivalent CW, a cyclic shift of A. For an integer t, $A^{(t)} = A(X^t)$ denotes the image of A under the group homomorphism $x \to x^t$, extended linearly to all of $\mathbb{Z}[\mathbb{Z}_n]$. If $\gcd(t,n) = 1$, then this map is an automorphism. If $\gcd(t,n) = d$, then $A^{(t)}$ is an $ICW_d(n/d, k)$.

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. The following result, given in this form for group rings in [13], will be used below.

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

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

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

$$A \equiv 0 \bmod p^{a}.$$

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.*

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

Theorem 2. *Let A be a $CW(n,k)$, 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 $p \bmod n$, and so P and N must both be unions of orbits of $\mathbb{Z}_n$ under the action of multiplying by p. For example, 2 is a multiplier of $CW(7,4)$, and the presentation given above is fixed by it:

$$A^{(2)} = A(X^2) = -1 + X^2 + X^4 + X^8 \equiv A \pmod{X^7 - 1}.$$

The orbits of 2 mod 7 are $\{0\}$, $\{1,2,4\}$ and $\{3,5,6\}$, so the only possibilities are $N = \{0\}$ and P being one of the other orbits, both of which give (equivalent) $CW(7,4)$s. 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 $n = dm$, with $d, m > 1$. We may reduce $A = \sum_{i=0}^{n-1} a_i X^i$ modulo $X^m - 1$ to get

$$B = \sum_{i=0}^{m-1} \left(\sum_{j=0}^{d-1} a_{i+jm} \right) X^i = \sum_{i=0}^{m-1} b_i X^i.$$

The b_i's are called the *intersection numbers*. As is common practice with difference sets, we may use these intersection numbers to investigate the existence of circulant weighing matrices:

Lemma 2.1. *For an $ICW(n,k)$ circulant weighing matrix A as above,*

$$\sum_{i=0}^{m-1} b_i = s, \tag{2}$$

$$\sum_{i=0}^{m-1} b_i^2 = s^2 = k. \tag{3}$$

$B(X)$ is an $ICW_d(m, w)$. If $A(X)$ is equivalent to $B(X^d)$ for any $d > 1$, then A is called a *multiple* of $B(X)$. If $A(X)$ is not a multiple of any CW, then it is called *proper*.

In this paper we will consider possible circulant weighing matrices in $\mathbb{Z}_n = \mathbb{Z}_d \times \mathbb{Z}_m$, where d and m 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 $\mathbb{Z}_d$ and $\mathbb{Z}_m$ 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.

For any of the cases in Strassler's table, Equations (2) and (3) will be small enough that we can solve them either by hand or with a short computer exhaust. The bulk of each proof will be showing that none of those pairs of solutions corresponds to a circulant weighing matrix.

3 Nonexistence Results

In this section we present proofs of nonexistence for several of the open cases in Strassler's table. All these proofs may be done by hand, without computer assistance. In later sections we will look at more difficult parameters, where more substantial computation is needed.

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, $\langle x \rangle_s$ denotes the orbit of 3 with representative x and size s. 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.

$\mathbb{Z}_{10}$ \ $\mathbb{Z}_{11}$	$\langle 0\rangle_1$	$\langle 1\rangle_5$	$\langle 2\rangle_5$	
$\langle 0\rangle_1$	$\langle 0\rangle_1$	$\langle 20\rangle_5$	$\langle 10\rangle_5$	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 $CW(110, 81)$

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.

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 the first column orbit cannot be in P or N, so we must have $a = -1$. But equations (4) and (5) have no integer solutions with $a = -1$.

□

Proposition 3.2. *Suppose m is an integer for which $\gcd(33, m) = 1$, and 3 is self-conjugate modulo m. Then no $CW(11 \cdot m, 81)$ exists.*

Proof. For any $n = 11 \cdot m$, we may make a table of orbits similar to Table 1. Since $\gcd(3, m) = 1$, 3 is a multiplier. The orbits mod 11 will be the same, and since 3 is self-conjugate mod m the sum of the first row must still be 9, so that again the $\langle 0\rangle_1$ orbit must be in N. All the other row sums are 0, and since each row has orbits of size o, $5o$ and $5o$, that means that the orbit in the first column cannot be in P or N. Therefore a in equations (4) and (5) would need to be -1, and those equations still have no such integer solutions.

□

This rules out many such parameters, one of which is in Strassler's table and was open:

Corollary 3.1. *A $CW(154, 81)$ does not exist.*

The same method, with different orbits, may be used for other parameters.

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

$\mathbb{Z}_{10}$ \ $\mathbb{Z}_{13}$	$\langle 0\rangle_1$	$\langle 1\rangle_3$	$\langle 2\rangle_3$	$\langle 4\rangle_3$	$\langle 7\rangle_3$	
$\langle 0\rangle_1$	$\langle 0\rangle_1$	$\langle 40\rangle_3$	$\langle 70\rangle_3$	$\langle 10\rangle_3$	$\langle 20\rangle_3$	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 2: Orbit information for $CW(130, 81)$

Proof. The orbit information is given in Table 2. 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 3 gives the orbit information.

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

$\mathbb{Z}_{11}$	$\mathbb{Z}_{13}$: $\langle 0\rangle_1$	$\langle 1\rangle_3$	$\langle 2\rangle_3$	$\langle 4\rangle_3$	$\langle 7\rangle_3$	
$\langle 0\rangle_1$	$\langle 0\rangle_1$	$\langle 22\rangle_3$	$\langle 44\rangle_3$	$\langle 77\rangle_3$	$\langle 11\rangle_3$	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 3: 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 4 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
$\langle 1\rangle_5$		$\boldsymbol{\langle 1\rangle_{15}}$	$\langle 5\rangle_{15}$	$\boldsymbol{\langle 4\rangle_{15}}$		15
$\langle 2\rangle_5$			$\boldsymbol{\langle 2\rangle_{15}}$	$\langle 10\rangle_{15}$		0
	0	15	-3	-3	0	

Table 4: A choice of orbits satisfying the equations (*not* a $CW(143, 81)$). P orbits are in **bold**

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 4 give

$$A(X) \equiv 5X^{\langle 1\rangle} - X^{\langle 2\rangle} - X^{\langle 4\rangle} \pmod{X^{13} - 1},$$

where $X^{\langle a\rangle} = \sum_{b\in\langle a\rangle} X^b$ for the orbit $\langle a\rangle$ in $\mathbb{Z}_{13}$, and we find

$$A(X)A(X^{-1}) \equiv 81 + 18\left(X^{\langle 1\rangle} + X^{\langle 2\rangle} - X^{\langle 4\rangle} + X^{\langle 7\rangle}\right) \pmod{X^{13} - 1} \neq 81.$$

$\square$

Finally, we have:

Proposition 3.5. *A $CW(143, 36)$ does not exist.*

Proof. Since k is not a prime power, Theorem 2 does not apply. However, a more general multiplier theorem ([5], Theorem 2.4) shows that 3 is still a multiplier, and so the orbit information is exactly the same as in Table 3.

The table is the same, but the equations are

$$\begin{aligned} x + 3(y_0 + y_1 + y_2 + y_3) &= 6 \\ x^2 + 3(y_0^2 + y_1^2 + y_2^2 + y_3^2) &= 36 \end{aligned}$$

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

$$\begin{aligned} a + 5(b + c) &= 6 \\ a^2 + 5(b^2 + c^2) &= 36 \end{aligned}$$

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

The solutions to the $\mathbb{Z}_{11}$ equations are $(6, 0, 0)$, $(-4, 2, 0)$ and $(-4, 0, 2)$. The solutions to the $\mathbb{Z}_{13}$ equations are $(6, 0, 0, 0, 0)$ and $(0, 2, 2, -2, 0)$ and permutations of the last four coordinates.

$\mathbb{Z}_4$	$\langle 0\rangle_1$	$\langle 1\rangle_5$	$\langle 2\rangle_5$	
$\langle 0\rangle_1$	$\langle 0\rangle_1$	$\langle 4\rangle_5$	$\langle 8\rangle_5$	9
$\langle 2\rangle_1$	$\langle 22\rangle_1$	$\langle 14\rangle_5$	$\langle 2\rangle_5$	0
$\langle 1\rangle_2$	$\langle 11\rangle_2$	$\langle 1\rangle_{10}$	$\langle 7\rangle_{10}$	0
	a	$5b$	$5c$	

(Column header group: $\mathbb{Z}_{11}$)

Table 5: Orbit information for $ICW_3(44, 81)$

But none of the $\mathbb{Z}_{11}$ and $\mathbb{Z}_{13}$ are compatible; $(6, 0, 0)$ would force two or more of the size-3 orbits in the first row to be in P. The corresponding columns would then have weight 3 (mod 15), which does not fit with any of the $\mathbb{Z}_{13}$ solutions. Similarly, $(-4, 2, 0)$ or $(-4, 0, 2)$ would force the $\langle 0\rangle_1$ orbit to be in N, so that the first column would have weight $4 \pmod 5$, which is not compatible with any of the $\mathbb{Z}_{13}$ solutions. □

4 Contracted Circulant Weighing Matrices

For most of the remaining open cases in Strassler's table, we do not have any multipliers from Theorem 2, either because k is composite or not relatively prime to n.

The following theorem, due to McFarland [18], will sometimes allow us to obtain multipliers in these cases:

Theorem 3. *Let M be an $ICW(m, k)$ with $\gcd(m, k) = 1$. Let k have prime factorization $p_1^{e_1} \cdots p_s^{e_s}$. If t is an integer for which there are f_i for $i = 1, 2, \ldots, s$ with*

$$t \equiv p_i^{f_i} \pmod m, \tag{6}$$

then t is a multiplier of M.

Thus for a putative $CW(n, k)$ A, we may apply this theorem to $A^{(d)}$ for $d = \gcd(n, k)$. If such a t exists, we will call it a d-multiplier for A if we can find a t satisfying (6), and we may apply the methods of the previous section.

Proposition 4.1. *A $CW(132, 81)$ does not exist.*

Proof. By Theorem 3, 3 is a multiplier for an $ICW_3(44, 81)$. Table 5 gives the orbit information. Since this is an ICW, any of the orbits may occur with a coefficient up to 3 in absolute value.

Since 3 is self-conjugate modulo 4, the row sums must be $(9, 0, 0)$. This means that $\langle 0\rangle_1$ has a coefficient of -1, with the other orbits in the first row having coefficients $(1, 1)$, $(2, 0)$, or $(3, -1)$ in either order.

The solutions to the $\mathbb{Z}_{11}$ equations are $(9, 0, 0)$, $(4, 3, -2)$, $(-6, 0, 3)$, and permutations of the last two columns. But since the second and third row sums are zero, and the other

n	k	m	t	$\|M\|$	$\# \, ICW_d(m,k)$
105	36	35	4	6	1
112	36	7	2	3	2
117	36	13	3	3	3
140	36	35	4	6	1
195	36	65	16	3	4
140	64	35	2	12	3
180	64	45	2	12	1
182	64	91	2	12	0
196	64	49	2	21	3
132	81	44	3	10	0
156	81	52	3	6	100
195	81	65	3	12	2
198	81	22	3	5	13
156	100	39	5	4	6
165	100	33	4	5	8
195	100	39	5	4	6

Table 6: ICWs for Open Cases

orbits all have order $0 \pmod 5$, the coefficient of the orbits in those rows in the first column must be zero. None of the solutions has first coefficient -1, so no $ICW_3(44, 81)$ exists, and so no $CW(132, 81)$ exists.

□

Table 6 gives the other open cases where we can apply Theorem 3 with a reasonably large m. Except for $CW(132, 81)$, all of them require computer assistance. Since there is no $ICW_2(91, 81)$, we have:

Proposition 4.2. *A* $CW(182, 64)$ *does not exist.*

For the other cases there are ICWs that could potentially be lifted to the corresponding CW. It is likely that further computations could eliminate some of these, similar to how [9] showed that there was no lift of an $ICW_2(77, 36)$ to a $CW(154, 36)$, or of an $ICW_2(85, 64)$ to a $CW(170, 64)$.

5 Strassler's Table and Beyond

There has been a large amount of work on entries in Strassler's table in the past few years. In particular, Tan [22] showed nonexistence for 19 cases, and gave an updated version of the table with 34 open cases remaining ($CW(126, 64)$ and $CW(198, 100)$ were listed as open in Tan's thesis, although it was already known that they could be constructed using Theorem 2.2 of [6]; this was corrected in the published paper). The seven cases resolved above leave 27 open cases.

n	k	n	k	n	k	n	k	n	k
105	36	116	49	140	64	156	81	112	100
112	36	120	49	180	64	195	81	120	100
117	36	192	49	196	64	198	81	155	100
140	36							156	100
180	36							165	100
195	36							182	100
								195	100

Table 7: Remaining Open Cases with $n \leq 200$, $k \leq 100$

Of the remaining cases, while the above methods do not yield hand-checkable proofs, when there is a sufficiently large multiplier group a computer exhaust becomes quite feasible. We were able to eliminate $CW(144, 49)$, $CW(152, 49)$, $CW(160, 49)$ $CW(104, 81)$, and $CW(160, 81)$. The longest of these, $CW(144, 49)$, had 27 solutions to equations (4) and (5) modulo 9, and 252 solutions modulo 16. The computation took 15 days on a workstation, and required testing 2.4 billion putative circulant weighing matrices.

The remaining cases either have no known multipliers or a very small multiplier group, so the methods of this paper will not work to eliminate them. Hopefully some new ideas will soon allow Strassler's table to be fully settled, as Lander's table of difference set cases were twenty years ago [12].

As with Lander's table for difference sets, the parameters for Strassler's table, $n \leq 200$ and $s \leq 10$, were a convenient focus on approachable problems, not a hard limit never to be exceeded. The code written for the above searches can handle larger numbers, so we have started exploring further. The second author has set up an online database [11], which contains a current version of the table, along with known circulant weighing matrices for parameters in Strassler's table. It also has partial results for for $n \leq 1000$ and $k \leq 19^2$. Out of the 15982 such parameters, 1175 have CWs, 12017 do not, and 2790 remain open.

6 Proper $CW(n, k)$

Recall that a $CW(n, k)$ is called proper if it is not a multiple of any smaller CW, i.e. its group ring representation $A(X)$ is not equal to $B(X^d)$ for any $n = dm$ for $B(X)$ a $CW(m, k)$.

Leung and Schmidt [16] showed that there are only a finite number of $CW(n, k)$ for a fixed k. For which k can we give a complete list of proper $CW(n, k)$? This has been solved for $k = 4$ [10] and $k = 9$ [1]. For $k = 25$ Leung and Ma [15] show that none exist with $n \equiv 0 \pmod 5$, and in a 2011 preprint [14] deal with the other cases, although this has not appeared in print.

For $k = 16$ this question was not completely answered. In [8], it is shown that all proper $CW(n, 16)$ have either $n = 21, 31, 63$ or are of "Type II", meaning that they are constructed using Theorem 2.3 of that paper:

Theorem 4. *If B is a $CW(2n,k)$, and C is a $CW(n,k)$. If the supports of $B(X)$, $X^nB(X)$,$C(X^2)$, $X^nC(X^2)$ are pairwise disjoint, then*

$$(1-X^n)B(X)+(1+X^n)C(X^2)$$

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

With this we can classify the proper $CW(n,16)$ of even order:

Theorem 5. *The proper $CW(n,16)$ have order 21,31,63, and $14m$ for all $m \geq 2$.*

Proof. The odd orders were taken care of in [8]. Let $C=-1+X+X^2+X^4$ denote the $CW(7,4)$, and

$$A=(1-X^{7m})C(X^{2m})+(1+X^{7m})XC(X^m).$$

The coefficients of A are disjoint for $m>1$, so by Theorem 4 A is a $CW(14m,16)$. Since the coefficients of X^0, X^1, X^{2m} and X^{7m} are nonzero, no equivalent difference set has all terms divisible by 2, 7 or m, so it is a proper one.

The only other way to construct a Type II CW would be to use one of the $CW(2m,4)$. Proper ones are equivalent to $-1+X+X^m+X^{m+1}$ and so in Theorem 4 the supports would not be disjoint. Improper ones are either a multiple of $CW(7,4)$, or also have nonzero coefficients for X^0 and X^m, and so also fail the requirements of the theorem. □

For larger k not much is known. Table 8 gives a list of known proper $CW(n,k)$ for $k \leq 19^2$. Aside from small cases, they all come from Theorems 6 and 9 below. Leung and Schmidt [17] showed that there are only a finite number of proper $CW(n,k)$ for any odd prime power k.

The Kronecker product construction of Arasu and Seberry [4] accounts for almost all of the proper $CW(n,s^2)$ for s not prime, and all the infinite classes except for $CW(2m,2^2)$ [10] and $CW(48m,6^2)$ [20]:

Theorem 6. *If a proper $CW(n_1,k_1)$ and proper $CW(n_2,k_2)$ exist with $\gcd(n_1,n_2)=1$, then they may be used to construct a proper $CW(n_1n_2,k_1k_2)$*

For k a prime power, most $CW(n,k)$ come from relative difference sets. A (m,n,k,λ) *cyclic relative difference set (RDS) D* is a k-element subset of $\mathbb{Z}_{mn}$ such that

$$DD^{-1}=k+\lambda(\mathbb{Z}_{mn}-\mathbb{Z}_n).$$

See [19] for more information on relative difference sets. It is well known (e.g. Theorem 2.1 of [8]):

Theorem 7. *If a cyclic $(m,2n,k,\lambda)$-RDS exists, then there is a $CW(mn,k)$.*

In [7] it is shown:

Theorem 8. *For q a prime power, a cyclic $\left(\frac{q^d-1}{q-1},n,q^{d-1},q^{d-2}(q-1)/n\right)$-RDS exists if and only if n is a divisor of $q-1$ when q is odd or d is even, and if and only if n is a divisor of $2(q-1)$ if q is even and d is odd.*

k	Known Proper $CW(n,k)$
2^2	$\underline{2m}$, **7**
3^2	**13**, $\underline{24}$, $\underline{26}$
4^2	$14m$, **21**, $\underline{31}$, **63**
5^2	**31**, $\underline{33}$, **62**, $\underline{71}$, $\underline{124}$, $\underline{142}$
6^2	$26m$, $\underline{48m}$, 91, 168
7^2	**57**, $\underline{87}$, **114**, **171**
8^2	$42m$, $62m$, **73**, $\underline{127}$, 217, **511**
9^2	**91**, $\underline{121}$, **182**, **364**
10^2	$62m$, $66m$, $142m$, 217, 231, 497, 994
11^2	**133**, **665**
12^2	$182m$, $336m$, 273, 403, 744
13^2	**183**, **366**, **549**, **732**
14^2	$114m$, $174m$, $342m$, 399, 609
15^2	403, 429, 744, 806, 923
16^2	$146m$, $254m$, $434m$, **273**, 511, 651, **819**, 868, 889
17^2	**307**, **614**
18^2	$182m$, $242m$, $624m$, 847
19^2	**381**, **762**

Table 8: Known Proper $CW(n,k)$. Numbers in **bold** come from Theorem 9. Underlined entries are sporadic CWs that do not come from Theorems 6 or 9. Entries cm are for all m such that $cm \geq k$.

Taking $d = 3$, we have:

Theorem 9. *A proper $CW((q^3-1)/n, q^2)$ exists for all divisors n of $(q-1)$ for even prime powers, and all divisors $n > 1$ of $(q-1)$ for odd prime powers.*

All the proper $CW(n,k)$ in Table 8 coming from this theorem are in bold. This theorem shows that there are proper $CW(q^3-1, q^2)$ when q is an even prime power. They also exist for $q = 3$ and 5, and it is tempting to conjecture that this is true for all prime powers, but larger cases are currently out of reach.

References

[1] M.H. Ang, K.T. Arasu, S.L. Ma, and Y. Strassler. Study of proper circulant weighing matrices with weight 9. *Disc. Math.*, 308:2802–2809, 2008.

[2] K. T. Arasu and J. R. Hollon. Group developed weighing matrices. *Australas. J. Combin.*, 55:205–233, 2013.

[3] K. T. Arasu and J. Seberry. Circulant weighing designs. *J. Combin. Des.*, 4:439–447, 1996.

[4] K. T. Arasu and J. Seberry. On circulant weighing matrices. *Australas. J. Combin.*, 17:21–37, 1998.

[5] K. T. Arasu and Q. Xiang. Multiplier theorems. *J. Combin. Des.*, 3:257–268, 1995.

[6] K.T. Arasu and J.F. Dillon. Perfect ternary arrays. In *Difference Sets, Sequences and their Correlation Properties*, pages 1–15. Kluwer, 1999.

[7] K.T. Arasu, J.F. Dillon, K.H. Leung, and S.L. Ma. Cyclic relative difference sets with classical parameters. *JCT A*, 94:118–126, 2002.

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

[9] K.T. Arasu and A. Nabavi. Nonexistence of CW(154,36) and CW(170,64). *Disc. Math.*, 311:769–779, 2011.

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

[11] D. M. Gordon. La Jolla Combinatorics Repository. `https://www.dmgordon.org/`, 2020.

[12] J. Iiams. Lander's tables are complete! In *Difference Sets, Sequences and their Correlation Properties*, pages 239–257. Kluwer, 1999.

[13] D. Jungnickel. On Lander's multiplier theorem for difference lists. *J. Comb. Info. and Syst. Sci.*, 17:123–129, 1992.

[14] K.H. Leung and S.L. Ma. Proper circulant weighing matrices of weight 25. preprint, 2011.

[15] K.H. Leung and S.L. Ma. Proper circulant weighing matrices of weight p^2. *Designs, Codes and Cryptography*, 72:539–550, 2014.

[16] K.H. Leung and B. Schmidt. Finiteness of circulant weighing matrices of fixed weight. *JCT A*, 118:908–919, 2011.

[17] K.H. Leung and B. Schmidt. Structure of group invariant weighing matrices of small weight. *JCT A*, 154:114–128, 2018.

[18] R.L. McFarland. *On multipliers of abelian difference sets.* PhD thesis, The Ohio State University, 1970.

[19] A. Pott. *Finite Geometry and Character Theory*, volume 1601 of *Lecture Notes in Mathematics*. Springer, 1995.

[20] B. Schmidt and K.W. Smith. Circulant weighing matrices whose order and weight are products of powers of 2 and 3. *JCT A*, 120:275–287, 2013.

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

[22] M.M. Tan. Group invariant weighing matrices. *Designs, Codes and Cryptography*, 86:2677–2702, 2018.