Cryptography and Communications (2021) 13:775–789
https://doi.org/10.1007/s12095-021-00492-0

New nonexistence results on circulant weighing matrices

K. T. Arasu[1] · Daniel M. Gordon[2] · Yiran Zhang[3]

Received: 29 October 2020 / Accepted: 3 May 2021 / Published online: 7 July 2021

Abstract

A 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, Strassler gave a table of existence results for circulant weighing matrices with $n \leq 200$ and $k \leq 100$. In the latest version of Strassler's table given by Tan, 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.

Keywords Weighing matrices · Circulant matrices · Multipliers

Mathematics Subject Classification (2010) MSC 05B20 · MSC 05B10

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.

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 $|P| + |N| = k$.

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

✉ Daniel M. Gordon
gordon@ccrwest.org

K. T. Arasu
karasu@riversideresearch.org

Yiran Zhang
yzhang45@luc.edu

[1] Riverside Research, 2640 Hibiscus Way, Beavercreek, OH 45431, USA

[2] Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121, USA

[3] Loyola University, Chicago, IL 60660, USA

The following facts are well known:

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 [1–3].

In his 1997 thesis [4], Strassler gave a table of known results on such matrices with $n \leq 200$ and $k \leq 100$. Over the years, many open cases in his table have been resolved. In Tan's 2018 version of the table [5], there are 34 open cases remaining. In this paper, we will show that no $CW(n, k)$ exists for twelve of those cases.

2 Group rings and multipliers

It is 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.

Definition 2.1 For an integer t and $A = \sum_{g\in G} a_g g$, define $A^{(t)} = \sum_{g\in G} a_g g^t$.

In this paper, we will be working with $\mathbb{Z}[\mathbb{Z}_n]$, the group ring of the cyclic group $\mathbb{Z}_n$ of order n over $\mathbb{Z}$, the ring of integers. A $CW(n, k)$ is an element A of $\mathbb{Z}[\mathbb{Z}_n]$ with all coefficients in $\{0, \pm 1\}$ such that

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

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, a circulant weighing matrix $CW(7, 4)$

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

is equivalent to

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

The group ring element is given by the first row of the matrix, and (1) applies both the the matrix and group ring element.

We will generally leave the mod$(X^n - 1)$ 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 of Lander, given in this form for group rings in [6], will be used below.

Theorem 2.2 *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 2.3 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, [2]:

Theorem 2.4 *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 mod 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*. They have been extensively used for studying the existence of difference sets, circulant weighing matrices ([4] called it *folding*), and supplementary difference sets [7].

Lemma 2.5 *For an $ICW(n, k)$ circulant weighing matrix A as above,*

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

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

where $|b_i| \leq d$.

Note that if $d \leq s$, then for any $0 \leq i < m$, these equations have a trivial solution $b_i = s$ and $b_j = 0$ for $i \neq j$. If Theorem 2.2 applies with $p^a = s$, then the trivial solutions are the only ones.

$B(X)$ 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 2.5 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 show that none of those pairs of solutions corresponds to a circulant weighing matrix.

Since this method will be used repeatedly, we will formalize it here. Let σ and τ be projections from $\mathbb{Z}_n$ to $\mathbb{Z}_d$ and $\mathbb{Z}_m$, respectively. Let the orbits of $\mathbb{Z}_n$ be

$$\mathcal{N}_1, \mathcal{N}_2, \ldots \mathcal{N}_w,$$

the orbits of $\mathbb{Z}_d$ be

$$\mathcal{D}_1, \mathcal{D}_2, \ldots \mathcal{D}_u,$$

and the orbits of $\mathbb{Z}_m$ be

$$\mathcal{M}_1, \mathcal{M}_2, \ldots \mathcal{M}_v.$$

$\mathcal{B}_{ij} = \{\mathcal{B}_{ij}^1, \mathcal{B}_{ij}^2, \ldots, \mathcal{B}_{ij}^l\}$ will denote the set of orbits $\mathcal{N}$ which map to orbits $\mathcal{D}_i$ and $\mathcal{M}_j$ under σ and τ. This information may be represented as a matrix shown in Table 1, where the row and column sums $\mathbf{r} = (r_1, \ldots, r_u)$ and $\mathbf{c} = (c_1, \ldots, c_v)$ are the sum of the orders of the orbits in that line in P minus the sums of the orders in N. The intersection numbers of Lemma 2.5 are $r_i/|\mathcal{D}_i|$ and $c_j/|\mathcal{M}|$.

To illustrate the method that will be used throughout this paper, consider a $CW(63, 16)$. By Theorem 2.4 2 is a multiplier, and the orbits of $\mathbb{Z}_{63}$ are shown in Table 2, where each orbit is represented by its generator in the appropriate group, and the subscript gives the size of the orbit. A $CW(63, 16)$ is given in Table 3 where the sets in P are in bold. Note that the intersection numbers $(4, 0, 0)$ and $(1, 2, -1)$ satisfy Lemma 2.5. Also, by Theorem 2.2 with $n = 9$ and $p = 2$ we have the intersection numbers mod 9 must be trivial. There is one other inequivalent solution, which has the same intersection numbers.

In the next section we will use this framework to demonstrate that various $CW(n, k)$ do not exist. For small cases this can be done by hand. A computer search dealing with larger cases will be discussed in Section 5.

Table 1 Orbit table for $CW(n, k)$

		$\mathbb{Z}_m$			
$\mathbb{Z}_d$	$\mathcal{M}_1$	$\mathcal{M}_2$	$\ldots$	$\mathcal{M}_v$	
$\mathcal{D}_1$	$\mathcal{B}_{1,1}$	$\mathcal{B}_{1,2}$		$\mathcal{B}_{1,v}$	r_1
$\mathcal{D}_2$	$\mathcal{B}_{2,1}$	$\mathcal{B}_{2,2}$		$\mathcal{B}_{2,v}$	r_2
$\vdots$			$\ddots$		
$\mathcal{D}_u$	$\mathcal{B}_{u,1}$	$\mathcal{B}_{u,2}$		$\mathcal{B}_{u,v}$	r_u
	c_1	c_2		c_v	

Table 2 $CW(63, 4^2)$ orbits

		$\mathbb{Z}_7$	
$\mathbb{Z}_9$	$\langle 0\rangle_1$	$\langle 1\rangle_3$	$\langle 3\rangle_3$
$\langle 0\rangle_1$	$\langle 0\rangle_1$	$\langle 9\rangle_3$	$\langle 27\rangle_3$
$\langle 1\rangle_6$	$\langle 7\rangle_6$	$\langle 1\rangle_6$ $\langle 11\rangle_6$ $\langle 23\rangle_6$	$\langle 5\rangle_6$ $\langle 13\rangle_6$ $\langle 31\rangle_6$
$\langle 3\rangle_2$	$\langle 21\rangle_2$	$\langle 15\rangle_6$	$\langle 3\rangle_6$

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 $|P| = 45, |N| = 36$ and 3 is its multiplier. Note that $\mathbb{Z}_{110} = \mathbb{Z}_{11} \times \mathbb{Z}_{10}$. 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:

$$\{0\}$$

$$\{5\}$$

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

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

Since 3 is self-conjugate mod 10, by Theorem 2.2 the intersection numbers mod 10 are trivial. Without loss of generality we may take the first row sum to be 9, and the others zero (there is no way to get the last two rows to sum to zero, and if the second row sum was 9 we can shift each element of P and N by 55). The only way for the first row to sum to 9 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 2.5, we get equations

$$y_1 + 5(y_2 + y_3) = 9 \tag{4}$$

Table 3 Solution representing a $CW(63, 4^2)$

		$\mathbb{Z}_7$		
$\mathbb{Z}_9$	$\langle 0\rangle_1$	$\langle 1\rangle_3$	$\langle 3\rangle_3$	
$\langle 0\rangle_1$	$\boldsymbol{\langle 0\rangle_1}$		$\boldsymbol{\langle 27\rangle_3}$	4
$\langle 1\rangle_6$		$\boldsymbol{\langle 11\rangle_6}$	$\langle 31\rangle_6$	0
$\langle 3\rangle_2$				0
	1	$3 \cdot (2)$	$3 \cdot (-1)$	

and

$$y_1^2 + 5(y_2^2 + y_3^2) = 81 \tag{5}$$

for $\mathbb{Z}_{11}$. Since for each row the size of the first column orbit is different from the other two, the other row sums being zero means that their first column orbit cannot be in P or N, so we must have $y_1 = -1$. But (4) and (5) have no integer solutions with $y_1 = -1$.

□

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 4. 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, by Theorem 2.2 the intersection numbers mod m must be trivial. As before the first row sum must 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 y_1 in (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 3.3 *A* $CW(154, 81)$ *does not exist.*

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

Proposition 3.4 *A* $CW(130, 81)$ *does not exist.*

Proof The orbit information is given in Table 5. While 3 is self-conjugate modulo 10, the orbit structure is different, so the argument is not quite as straightforward.

Without loss of generality, by Theorem 2.2 we take the first row sum to be 9, so three of the four 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. No orbits can come from the second row, since N has order $36 \equiv 0 \pmod{12}$, and all the other orbits are 12-orbits.

The $\mathbb{Z}_{13}$ equations from Lemma 2.5 are:

$$y_1 + 3y_2 + 3y_3 + 3y_4 + 3y_5 = 9 \tag{6}$$

Table 4 Orbit information for $CW(110, 81)$

	$\mathbb{Z}_{11}$			
$\mathbb{Z}_{10}$	$\langle 0\rangle_1$	$\langle 1\rangle_5$	$\langle 2\rangle_5$	
$\langle 0\rangle_1$	$\langle 0\rangle_1$	$\langle 20\rangle_5$	$\langle 10\rangle_5$	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
	y_1	$5y_2$	$5y_3$	

Table 5 Orbit information for $CW(130, 81)$

	$\mathbb{Z}_{13}$					
$\mathbb{Z}_{10}$	$\langle 0\rangle_1$	$\langle 1\rangle_3$	$\langle 2\rangle_3$	$\langle 4\rangle_3$	$\langle 7\rangle_3$	
$\langle 0\rangle_1$	$\langle 0\rangle_1$	$\langle 40\rangle_3$	$\langle 70\rangle_3$	$\langle 10\rangle_3$	$\langle 20\rangle_3$	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
	y_1	$3y_2$	$3y_3$	$3y_4$	$3y_5$	

and

$$y_1^2 + 3y_2^2 + 3y_3^2 + 3y_4^2 + 3y_5^2 = 81. \tag{7}$$

The only solutions with $y_1 = 0$ are permutations of $(0, 3, 3, -3, 0)$. But there is no way to get a column sum of -3 with zero or one 3-orbits from the first row in P and some number of 12-orbits in P or N.

□

Proposition 3.5 *A $CW(143, 81)$ does not exist.*

Proof Suppose a $CW(143, 81)$ exists; $|P| = 45$, $|N| = 36$ 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 6 gives the orbit information.

Table 6 Orbit information for $CW(143, 81)$

	$\mathbb{Z}_{13}$					
$\mathbb{Z}_{11}$	$\langle 0\rangle_1$	$\langle 1\rangle_3$	$\langle 2\rangle_3$	$\langle 4\rangle_3$	$\langle 7\rangle_3$	
$\langle 0\rangle_1$	$\langle 0\rangle_1$	$\langle 22\rangle_3$	$\langle 44\rangle_3$	$\langle 77\rangle_3$	$\langle 11\rangle_3$	x_1
$\langle 1\rangle_5$	$\langle 26\rangle_5$	$\langle 1\rangle_{15}$	$\langle 5\rangle_{15}$	$\langle 4\rangle_{15}$	$\langle 20\rangle_{15}$	$5x_2$
$\langle 2\rangle_5$	$\langle 13\rangle_5$	$\langle 29\rangle_{15}$	$\langle 2\rangle_{15}$	$\langle 10\rangle_{15}$	$\langle 7\rangle_{15}$	$5x_3$
	x	$3y_0$	$3y_1$	$3y_2$	$3y_3$	

Unfortunately, 3 is not self-conjugate modulo 11 or 13, so we need to work a bit harder. Applying Lemma 2.5, we get equations

$$\begin{aligned} y_1 + 3(y_2 + y_3 + y_4 + y_5) &= 9 \\ y_1^2 + 3(y_2^2 + y_3^2 + y_4^2 + y_5^2) &= 81 \end{aligned}$$

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

$$\begin{aligned} x_1 + 5(x_2 + x_3) &= 9 \\ x_1^2 + 5(x_2^2 + x_3^2) &= 81 \end{aligned}$$

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 $(x_1, x_2, x_3) = (-6, 3, 0)$, the first row is forced to have two size-3 orbits in N and none in P, or three in N and one in P. The latter is impossible, since it would leave 42 elements in P and 27 in N to be covered by the orbits in the other rows, all of which have size a multiple of 5. The former 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 $y_1 = 0$: $(0, 3, 3, 0, -3)$, $(0, 4, 1, 1, -3)$, 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 7 shows a selection satisfying all the equations, although the orbits do not form a $CW(143, 81)$.

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

Table 7 A choice of orbits satisfying the equations (*not* a $CW(143, 81)$). P orbits are in **bold**

		$\mathbb{Z}_{13}$				
$\mathbb{Z}_{11}$	$\langle 0\rangle_1$	$\langle 1\rangle_3$	$\langle 2\rangle_3$	$\langle 4\rangle_3$	$\langle 7\rangle_3$	
$\langle 0\rangle_1$			$\langle 44\rangle_3$	$\langle 77\rangle_3$		-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	

sum 15. For each of these 12 choices, we can check that (1) is not satisfied. For example, the choices in Table 7 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

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

□

Finally, we have:

Proposition 3.6 *A* $CW(143, 36)$ *does not exist.*

Proof Since k is not a prime power, Theorem 2.4 does not apply. However, a more general multiplier theorem ([8], Theorem 2.4) shows that 3 is still a multiplier, and so the orbit information is exactly the same as in Table 6.

The table is the same, but the equations are

$$\begin{aligned} y_1 + 3(y_2 + y_3 + y_4 + y_5) &= 6 \\ y_1^2 + 3(y_2^2 + y_3^2 + y_4^2 + y_5^2) &= 36 \end{aligned}$$

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

$$\begin{aligned} x_1 + 5(x_2 + x_3) &= 6 \\ x_1^2 + 5(x_2^2 + x_3^2) &= 36 \end{aligned}$$

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.

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 $3 \pmod{15}$, 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 2.4, either because k is composite or not relatively prime to n.

The following theorem, due to McFarland [9], will sometimes allow us to obtain multipliers in these cases:

Theorem 4.1 *Let M be an $ICW_d(m,k)$ 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*

$$t \equiv p_i^{f_i} \pmod{m}, \tag{8}$$

then t is a multiplier of M.

Thus for A a putative $CW(n,k)$, 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 (8), and we may apply the methods of the previous section.

Proposition 4.2 *A $CW(132,81)$ does not exist.*

Proof By Theorem 4.1, 3 is a multiplier for an $ICW_3(44,81)$. Table 8 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, by Theorem 2.2 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 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. □

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 [5] 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 [10]; this was corrected in the published paper). The seven cases resolved above leave 27 open cases.

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. The search begins in the upper right corner of Table 1, and scans the boxes right to left, doing each from from the bottom to the top. For each orbit it in turn skips it, adds it to P,

Table 8 Orbit information for $ICW_3(44,81)$

		$\mathbb{Z}_{11}$		
$\mathbb{Z}_4$	$\langle 0\rangle_1$	$\langle 1\rangle_5$	$\langle 2\rangle_5$	
$\langle 0\rangle_1$	$\langle 0\rangle_1$	$\langle 4\rangle_5$	$\langle 8\rangle_5$	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
	y_1	$5y_2$	$5y_3$	

and adds it to N, updating the row and column sums and recursing. For every possible set of row and column sums $(\mathbf{r}, \mathbf{c})$, we call Exhaust$(u, v, |\mathcal{B}_{uv}|, \emptyset, \emptyset, \mathbf{r}, \mathbf{c})$.

Algorithm 1 Exhaustive search for $CW(n, k)$.

```
Exhaust (i, j, l, P, N, r, c)
if i = j = l = 0 then                          // finished, test if we succeeded
    if r = c = 0 and {P, N} forms a CW(n, k) then
        report {P, N}
    return
if l > 0 then                                  // do orbits in this box
    Exhaust (i, j, l − 1, P, N, r, c)   // recurse without lth orbit
    Exhaust (i, j, l − 1, P ∪ B^l_{i,j}, N, (r_1, ... r_i − |B^l_{i,j}|, ..., r_u), (c_1, ... c_j −
    |B^l_{i,j}|, ..., c_v))                    // lth orbit in P
    Exhaust (i, j, l − 1, P, N ∪ B^l_{i,j}, (r_1, ... r_i + |B^l_{i,j}|, ..., r_u), (c_1, ... c_j +
    |B^l_{i,j}|, ..., c_v))                    // lth orbit in N
    else if i > 0 then
        Exhaust (i − 1, j, |B_{i−1,j}|, P, N, r, c)   // do next box in row
        else if r_j = 0 then      // row done, stop if row sum nonzero
            Exhaust (u, j − 1, |B_{u,j−1}|, P, N, r, c) // start next row up
```

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 (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.

As stated, Algorithm 1 will find all $CW(n, k)$, or show that none exist. To find $ICW_m(n, k)$, the same algorithm works, allowing up to m copies of each orbit to be added to P or N. Table 9 gives open cases where we can apply Theorem 4.1 with a reasonably large m.

Since there is no $ICW_2(91, 81)$, we have:

Proposition 5.1 *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 [11] 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 $CW(170, 64)$.

The remaining cases, given in Table 10 either have no 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 [13], which contains a current version of the table, along with known circulant weighing matrices for

Table 9 ICWs for open cases

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

parameters in Strassler's table. It also has partial results for for $n \le 1000$ and $k \le 19^2$. 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 $CW(m,k)$. For example,

$$A = X + X^2 + X^3 + X^6 + X^9 + X^{18} - X^4 - X^{12} - X^{10}$$

is a proper $CW(26, 3^2)$ (i.e. no $X^a A(X^b)$ for b relatively prime to 26 has all its coefficients with a common factor), while

$$A = X^2 + X^8 + X^{10} + X^{12} + X^{14} + X^{20} - 1 - X^4 - X^{16}$$

Table 10 Remaining open cases with $n \le 200$, $k \le 100$

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

is a multiple of the proper $CW(13, 3^2)$

$$A = X + X^4 + X^5 + X^6 + X^7 + X^{10} - 1 - X^2 - X^8.$$

Clearly it suffices to study proper CWs, and restricting our attention to those lets us present the state of knowledge about circulant weighing matrices in a form far more compact than Strassler's table. In this section we give the known results, which almost entirely come from two constructions.

Leung and Schmidt [14] showed that when k is an odd prime power there are only a finite number of proper $CW(n, k)$. For which k can we give a complete list of proper $CW(n, k)$? This has been solved for $k = 4$ [15] and $k = 9$ [16].

For $k = 25$ Leung and Ma [17] show that none exist with $n \equiv 0 \pmod 5$, and in a 2011 preprint [18] deal with the other cases, although this has not appeared in print.

For $k = 16$ this question was not completely answered. In [19], 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 6.1 *If B is a $CW(2n, k)$, and C is a $CW(n, k)$. If the supports of $B(X)$, $X^n B(X)$, $C(X^2)$, $X^n C(X^2)$ 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 6.2 *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 [19]. 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 6.1 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 6.1 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 11 gives a list of known proper $CW(n, k)$ for $k \leq 19^2$. Aside from small cases, they all come from Theorems 6.3 and 6.6 below.

The Kronecker product construction of Arasu and Seberry [3] accounts for almost all of the proper $CW(n, s^2)$ for s not prime, and all the infinite classes except for $CW(2m, 2^2)$ [15] and $CW(48m, 6^2)$ [20]:

Theorem 6.3 *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 $CW(n_1 n_2, k_1 k_2)$*

Table 11 Known Proper $CW(n, k)$

k	Known Proper $CW(n, k)$
2^2	$2m$, **7**
3^2	**13**, 24, 26
4^2	$14m$, **21**, 31, **63**
5^2	**31**, 33, **62**, 71, 124, 142
6^2	$26m$, $48m$, 91, 168
7^2	**57**, 87, **114**, **171**
8^2	$42m$, $62m$, **73**, 127, 217, **511**
9^2	**91**, 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**

Numbers in **bold** come from Theorem 6.6. Underlined entries are sporadic CWs that do not come from Theorems 6.3 or 6.6. Entries cm are for all m such that $cm \geq k$

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

Theorem 6.4 *If a cyclic $(m, 2n, k, \lambda)$-RDS exists, then there is a $CW(mn, k)$.*

In [22] it is shown:

Theorem 6.5 *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.*

Taking $d = 3$, we have:

Theorem 6.6 *Let q be a prime power. Then a proper $CW((q^3-1)/n, q^2)$ exists for all divisors n of $(q-1)$ if q is even, and all divisors $n > 1$ of $(q-1)$ if q is odd.*

All the proper $CW(n, k)$ in Table 11 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. Arasu, K.T., Hollon, J.R.: Group developed weighing matrices. Australas. J. Combin. **55**, 205–233 (2013)
2. Arasu, K.T., Seberry, J.: Circulant weighing designs. J. Combin. Des. **4**, 439–447 (1996)
3. Arasu, K.T., Seberry, J.: On circulant weighing matrices. Australas. J. Combin. **17**, 21–37 (1998)
4. Strassler, Y.: The classification of circulant weighing matrices of weight 9. Ph.D. Thesis, Bar-Ilan University (1997)
5. Tan, M.M.: Group invariant weighing matrices. Des. Codes Crypt. **86**, 2677–2702 (2018)
6. Jungnickel, D.: On Lander's multiplier theorem for difference lists. J. Comb. Info. and Syst. Sci. **17**, 123–129 (1992)
7. Đoković, D.Z., Kotsireas, I.S.: Compression of periodic complementary sequences and applications. Des. Codes Crypt. **74**, 365–377 (2015)
8. Arasu, K.T., Xiang, Q.: Multiplier theorems. J. Combin. Des. **3**, 257–268 (1995)
9. McFarland, R.L.: On multipliers of abelian difference sets. Ph.D. Thesis, The Ohio State University (1970)
10. Arasu, K.T., Dillon, J.F.: Perfect ternary arrays. In: Difference Sets, Sequences and their Correlation Properties, pp. 1–15. Kluwer (1999)
11. Arasu, K.T., Nabavi, A.: Nonexistence of CW(154,36) and CW(170,64). Disc. Math. **311**, 769–779 (2011)
12. Iiams, J.: Lander's tables are complete! In: Difference Sets, Sequences and their Correlation Properties, pp. 239–257. Kluwer (1999)
13. Gordon, D.M.: La Jolla Combinatorics Repository. https://www.dmgordon.org/ (2021)
14. Leung, K.H., Schmidt, B.: Finiteness of circulant weighing matrices of fixed weight. JCT A **118**, 908–919 (2011)
15. Eades, P., Hain, R.M.: On circulant weighing matrices. Ars Combin. **2**, 265–284 (1976)
16. Ang, M.H., Arasu, K.T., Ma, S.L., Strassler, Y.: Study of proper circulant weighing matrices with weight 9. Disc. Math. **308**, 2802–2809 (2008)
17. Leung, K.H., Ma, S.L.: Proper circulant weighing matrices of weight p^2. Des. Codes Crypt. **72**, 539–550 (2014)
18. Leung, K.H., Ma, S.L.: Proper circulant weighing matrices of weight 25. preprint (2011)
19. Arasu, K.T., Leung, K.H., Ma, S.L., Nabavi, A., Ray-Chaudhuri, D.K.: Circulant weighing matrices of weight 2^{2t}. Des. Codes Crypt. **41**, 111–123 (2006)
20. Schmidt, B., Smith, K.W.: Circulant weighing matrices whose order and weight are products of powers of 2 and 3. JCT A **120**, 275–287 (2013)
21. Pott, A.: Finite geometry and character theory, Lecture Notes in Mathematics, vol. 1601. Springer (1995)
22. Arasu, K.T., Dillon, J.F., Leung, K.H., Ma, S.L.: Cyclic relative difference sets with classical parameters. JCT A **94**, 118–126 (2002)