2009

Circulant Weighing Matrices

Alex James Gutman
Wright State University

CIRCULANT WEIGHING MATRICES

A thesis submitted in partial fulfillment
of the requirements for the degree of
Masters of Science

By

ALEX JAMES GUTMAN
B.S., Wright State University, 2007

2009
Wright State University

WRIGHT STATE UNIVERSITY

SCHOOL OF GRADUATE STUDIES

June 3, 2009

I HEREBY RECOMMEND THAT THE THESIS PREPARED UNDER MY SUPERVISION BY Alex J. Gutman ENTITLED Circulant Weighing Matrices BE ACCEPTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF Master of Science.

K.T. Arasu, Ph.D.
Thesis Director

Weifu Fang, Ph.D.
Department Chair

Committee on
Final Examination

K.T. Arasu, Ph.D.

Yuqing Chen, Ph.D

Xiaoyu Liu, Ph.D.

Joseph F. Thomas, Jr., Ph.D.
Dean, School of Graduate Studies

Abstract

Gutman, Alex James. M.S., Department of Mathematics and Statistics, Wright State University, 2009. Circulant Weighing Matrices.

The existence status of previously open cases of circulant weighing matrices will be established using various techniques. The results fill in 52 missing entries in Strassler's Table of Circulant Weighing Matrices [16], which considers matrices of order 1 - 200 with weight $k \leq 100$.

Contents

List of Tables

1 Introduction

A weighing matrix $W = W(n, k)$ of order n with weight k is a square matrix W 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.

A circulant weighing matrix, denoted $CW(n, k)$ (or simply C when the parameters are clear), is a special type of weighing matrix in which every row, save for the first, is a right cyclic shift of the previous row. A trivial example of a circulant weighing matrix is I_n.

Circulant weighing matrices can also be represented in the context of abelian groups. We label the first row of $CW(n, k)$ by a cyclic group G of order n. Let g generate G.

Define

$$\begin{aligned} P &= \{g^i | C(1,i) = 1, i = 0, 1, ...n-1\} \\ &\text{and} \\ N &= \{g^i | C(1,i) = -1, i = 0, 1, ...n-1\}. \end{aligned} \tag{1}$$

It is clear that $|P| + |N| = k$.

Theorem 1.1 *For $C = CW(n, k)$,*
(i) $k = s^2$ for some integer s, and
(ii) $|P| = \frac{s^s+s}{2}$ and $|N| = \frac{s^2-s}{2}$.

The proof can be found in [14].

Example 1.2 *A nontrivial example of a circulant weighing matrix is*

$$C = CW(7,4) = \begin{pmatrix} -1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & -1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & -1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & -1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & -1 \end{pmatrix}.$$

It is easy to check $CC^T = 4I_7$ *and each row is a right cyclic shift of the previous row. Using group notation,* $P = \{g, g^2, g^4\}$ *and* $N = \{g^0 = 1\}$.

2 Preliminaries

As previously mentioned, circulant weighing matrices can be represented in the context of groups. Specifically, $CW(n,k)$ can be viewed as an element of the group ring of a multiplicatively written group G over $\mathbf{Z}$. For our purpose, we will only consider cyclic groups G, and we will denote the group ring as $\mathbf{Z}G$. For $S \subseteq G$, we let S denote the element $\sum_{x\in S} x$ of $\mathbf{Z}G$. For more on group rings, refer to [8] and [16].

Definition 2.1 *Let t be an integer and $A \in \mathbf{Z}G$. For $A = \Sigma_{g\in G} a_g g$, we define $A^{(t)} = \Sigma_{g\in G} a_g g^t$.*

Be careful not to confuse $A^{(t)}$ with A^t, which is A multiplied by itself t times. Also, with circulant weighing matrices, $a_g \in \{0, \pm 1\}$.

Theorem 2.2 *A $CW(n,k)$ exists if and only if there exist disjoint subsets P and N, as in (1), such that*

$$(P-N)(P-N)^{(-1)} = k \tag{2}$$

in $\mathbf{Z}G$. See [3] for details.

Example 2.3 *Consider $CW(7,4)$ in* Example 1.2. *$P-N = -1+g+g^2+g^4$ and $(P-N)^{(-1)} = -1+g^3+g^5+g^6$. A simple calculation verifies $(P-N)(P-N)^{(-1)} = 4$.*

Notice the group ring element $P-N$ corresponds to the first row of the matrix.

2.1 Multipliers

Definition 2.4 *Let G be a group of order n and $A \in \mathbf{Z}G$. Any integer t with $(n,t) = 1$ is called a multiplier of A if $A^{(t)} = Ag$ for some $g \in G$.*

Theorem 2.5 (The Multiplier Theorem [13]) *Let G be a finite abelian group of order n. Let A be an element of $\mathbf{Z}G$ 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 2.6 *If $A = \Sigma_g a_g g \in \mathbf{Z}G$ such that $(\Sigma_g a_g, |G|) = 1$, then $A^{(t)} = A$ for any multiplier t. Thus, the multiplier t "fixes" A. This result is from Arasu and Ray-Chaudhuri in [7]*

Referring to P and N in (1) and (2), we can apply the Multiplier Theorem 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 coefficients equal to 0 or 1. Therefore, we can create orbits by applying the action $x \mapsto tx$ to the elements of $\mathbf{Z}_n$ (which is isomorphic to G), and P and N are unions of some of these orbits. It's important to note that every element in an orbit has the same value.

Example 2.7 *Consider $CW(7, 4)$. $|G| = 7$ and $k = 2^2$, so 2 is a multiplier that fixes P and N. The orbits of $\mathbf{Z}_7$ under $x \mapsto 2x$ are $\{0\}$, $\{1, 2, 4\}$, and $\{3, 6, 5\}$. $P = \{g, g^2, g^4\}$ corresponds to orbit $\{1, 2, 4\}$ and N to $\{0\}$. The use of exponents to describe orbits will simplify the notation for future use.*

Definition 2.8 *To easily classify the orbits of $\mathbf{Z}_n$ for a given multiplier, we define the orbit spectrum as $x_1^{i_1} x_2^{i_2} x_3^{i_3} ... x_m^{i_m}$ where x_j is the size of an orbit and i_j is the number of orbits with size x_j. A orbit of size 1 will be known as a singleton.*

Example 2.9 *The orbit spectrum of $\mathbf{Z}_7$ with 2 as a multiplier is $1^1 3^2$. (See 2.7).*

2.2 Integer Circulant Weighing Matrices

We now turn our attention to a special group of circulant matrices. These "new" matrices are an integral part of this research. For more information on this topic, please see [5] and [16].

Definition 2.10 *An integer circulant weighing matrix of order* n *with weight* k*, denoted* $ICW(n,k)$*, is simply a circulant matrix* M *with integer entries such that* $MM^T = kI_n$*. A* $CW(n,k)$ *is an* $ICW(n,k)$*, but unlike a circulant weighing matrix,* $ICW(n,k)$*'s entries are not confined to* $\{0, \pm 1\}$*.*

The group ring notation and Multiplier Theorem discussed earlier apply here. Also, as with circulant weighing matrices, if $ICW(n,k)$ exists, then $k = s^2$ for some integer s. We say an $ICW(n,k)$ is *trivial* if $ICW(n,k) = sI_n$. In group ring notation, an integer circulant weighing matrix A is trivial if $A = s$.

In order to find trivial weighing matrices, we can apply a variation of Ma's Lemma from [12].

Lemma 2.11 (Ma's Lemma) *Let* G *be an abelian group and* A *belong to the group ring* $\mathbf{Z}G$ *such that* $AA^{(-1)} = s^2$ *for some integer* s*. Assume there exists a prime* p *such that*
(i) $p^{2r} | s^2$ *for some positive integer* r*, and*
(ii) $p^f \equiv -1 \pmod{|G|}$ *for some nonnegative integer* f*.*
Then $A \equiv 0 \pmod{p^r}$*.*

Another important concept for this research was that of *projecting*, as described by Strassler in [16] (He used the term "folding"). First, we note that every group homomorphism $\phi : G \to H$ can be linearly extended to a ring homomorphism of group rings, $\sigma : \mathbf{Z}G \to \mathbf{Z}H$, where $\sigma(\Sigma_{g\in G} a_g g) = \Sigma_{g\in G} a_g \sigma(g)$. Next, in order to clarify the projection of ICWs, a change of notation will take place. If an element A belongs to the group ring $\mathbf{Z}G$

with $|G| = n$, we write $A = \Sigma_{g \in G} a_g g$. However, we could also write A in polynomial notation as a function of g:

$$A(g) = \sum_{i=0}^{n-1} a_i g^i.$$

Theorem 2.12 (The Projection Theorem) *Let g generate the cyclic group G of order n. Let $A(g) = \sum_{i=0}^{n-1} a_i g^i$ be an $ICW(n,k)$. Define $m = \max_{0 \le i \le n-1} |a_i|$. If $d|n$, then*

$$B(\dot{g}) = \sum_{i=0}^{d-1} \Big(\sum_{\substack{j \equiv i \pmod d \\ 0 \le j \le n-1}} a_j \Big) \dot{g}^i \tag{3}$$

is the generating polynomial of an $ICW(d,k)$ whose coefficients $b_i = \sum_{\substack{j \equiv i \pmod d \\ 0 \le j \le n-1}} a_j$ satisfy $|b_i| \le \frac{mn}{d}$. $\dot{g}$ is the generator of a cyclic group of order d.

Remark 2.13 If $A(g) = \sum_{i=0}^{n-1} a_i g^i$ is an $ICW(n,k)$, with $k = s^2$, then $\sum_{i=0}^{n-1} a_i = s$ and $\sum_{i=0}^{n-1} {a_i}^2 = s^2$.

3 Known Existence Results

The objective of most research on circulant weighing matrices revolves around a natural question: For a given weight k, what are the possible values of n such that $CW(n,k)$ exists? For smaller weights, (1, 4, 9, and 16) the orders n have been completely determined. The case when $k = 1$ is trivial.

Theorem 3.1 (Eades and Hain [10]) *A $CW(n,4)$ exists if and only if n is even ($\neq 2$) or $7|n$.*

Theorem 3.2 (Strassler and Arasu et al. [1]) *A $CW(n,9)$ exists if and only if $13|n$ or $24|n$.*

Theorem 3.3 (Arasu et al. [5]) *A $CW(n,16)$ exists if and only if $n \geq 21$ and $14|n$, $21|n$, or $31|n$.*

Theorem 3.4 ((Seberry) Wallis and Whiteman [15]) *If q is a prime power, then there exists $CW(q^2+q+1, q^2)$.*

Theorem 3.5 (Eades [9]) *If q is a prime power, q odd and i even, then there exists $CW(\frac{q^{i+1}-1}{q-1}, q^i)$.*

Theorem 3.6 (Arasu, Dillon, Jungnickel, and Pott [3]) *If $q = 2^t$ and i is even, then there exists $CW(\frac{q^{i+1}-1}{q-1}, q^i)$.*

Theorem 3.7 (Geramita and Seberry [11]) *If there exists $CW(n_1,k)$ and $CW(n_2,k)$ with $(n_1,n_2) = 1$, then there exist*
(i) $CW(mn_1,k)$ for all positive integers m;
(ii) two inequivalent $CW(n_1n_2,k)$;
(iii) $CW(n_1n_2,k^2)$.

4 New Results

The known existence theorems could not be applied to the following matrices. These cases were previously open, so each was examined on an individual basis, employing the techniques discussed in Section 2. To clarify some techniques, the first proof will include more detail to help the reader visualize each step. The Multiplier Theorem is used throughout this section, and each proof will show the necessary conditions of the theorem are satisfied. Also, as in Example 2.7, orbits will be described by using exponents rather than the actual terms. (i.e. $P = \{g, g^2, g^4\}$ will be written as $P = \{1, 2, 4\}$). Because the natural numbers describe our orbits and $G \cong \mathbf{Z}_n$, we will use $\mathbf{Z}_n$ as our arbitrary cyclic group from this point forward. Although the actual orbits are not shown, the curious reader could easily create the orbits if desired.

The term *projecting* implies the application of natural homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_d$ when $d|n$. Thus, the Projection Theorem is taking place on the group ring elements underneath this operation. The term *lifting* implies an undoing of the projection, which brings the matrix back to its original state.

Important note to reader: All proofs being with the assumption that the $CW(n, k)$ under investigation exists.

Proposition 4.1 *There does not exist any $CW(77, 6^2)$.*

Proof

$$4 \equiv 2^2 \equiv 3^4 \pmod{77}.$$

Therefore, 4 is a multiplier of $\mathbf{Z}_{77}$ and produces 9 orbits with a spectrum $1^1 3^2 5^2 15^4$. Projecting from $\mathbf{Z}_{77}$ to $\mathbf{Z}_{11}$, and using 4 as a multiplier on $\mathbf{Z}_{11}$ gives the orbits {0}, {1,4,5,9,3}, and {2,8,10,7,6}. From Remark 2.13, we have the equations $a + 5b + 5c = 6$ and $a^2 + 5b^2 + 5c^2 = 36$, where a is the value (i.e. coefficient) of the singleton, b is the value of each term in the orbit {1,4,5,9,3}, and c is the value of each term in {2,8,10,7,6}. Since $a \equiv 1 \pmod 5$, we must have $a = 6$, $a = 1$, or $a = -4$ ($-7 \leq a \leq 7$ by the Projection Theorem.)

If $a = 1$, then $b + c = 1$ and $b^2 + c^2 = 7$. This is not possible, so $a = 6$ or $a = -4$.

In $\mathbf{Z}_{77}$, the singleton and orbits of size 3 contain all multiples of 11, so these orbits "project" into a. Thus, $a = x + 3y + 3z$ where $x, y, z \in \{0, \pm 1\}$. x is the singleton value of $\mathbf{Z}_{77}$, and $a = 6$ or -4 forces x to be 0 or -1.

Projecting from $\mathbf{Z}_{77}$ to $\mathbf{Z}_7$, using 4 as a multiplier, gives the equations $a' + 3b' + 3c' = 6$ and $a'^2 + 3b'^2 + 3c'^2 = 36$. Since $a' \equiv 0 \pmod 3$, we must have $a' = 6, 3, 0$, or -3. If $a' = 0$, then $b + c = 2$ and $b'^2 + c'^2 = 12$. This is not possible. If $a' = 3$, then $b + c = 1$ and $b'^2 + c'^2 = 9$. This is also not possible, so either $a' = 6$ or $a' = -3$.

In $\mathbf{Z}_{77}$, the singleton and orbits of size 5 contain all multiples of 7, so these orbits project into a'. Thus, $a' = x + 5u + 5v$ where $u, v \in \{0, \pm 1\}$. We know x must equal 0 or -1, but 6 or -3 $\neq 5u + 5v$ and 6 or -3 $\neq -1 + 5u + 5v$ for $u, v \in \{0, \pm 1\}$. We have a contradiction.

Thus, there cannot exist $CW(77, 6^2)$. **Q.E.D.**

Proposition 4.2 *There does not exist any* $CW(81, 7^2)$.

Proof

$$7 \equiv 7 \pmod{81}.$$

Using 7 as a multiplier, $\mathbf{Z}_{81}$ has the orbit spectrum $1^3 3^2 9^2 27^2$. By Theorem 1.1, $|P| = 28$ and $|N| = 21$. Thus, the +1's must come from an orbit of size 27 and a singleton. Let A and B be the orbits of size 27. $A = \{1, 7, 49, 19, ...\}$ and $B = \{2, 14, 17, 38, ...\}$. So, $x \equiv 1 \pmod 3$ $\forall x \in A$ and $y \equiv 2 \pmod 3$ $\forall y \in B$. Projecting from $\mathbf{Z}_{81}$ to $\mathbf{Z}_3$ gives the equations $a + b + c = 7$ and $a^2 + b^2 + c^2 = 49$, where a, b, c are constant values on the orbits $\{0\}, \{1\}, \{2\}$, respectively. But, when either A or B project to $\{1\}$ or $\{2\}$ in $\mathbf{Z}_3$, 27 is too large to satisfy the equations.

Thus, there cannot exist $CW(81, 7^2)$. **Q.E.D.**

Proposition 4.3 *There does not exist any* $CW(117, 10^2)$.

Proof We can project from $CW(117, 10^2)$ to $ICW(13, 10^2)$. Let A be the group ring element corresponding to the first row of $ICW(13, 10^2)$. Note that $5^2 \equiv -1 \pmod{13}$ and $2^6 \equiv -1 \pmod{13}$. By Ma's Lemma, $A \equiv 0 \pmod 5$ and $A \equiv 0 \pmod 2$. Thus, $A \equiv 0 \pmod{10}$. However, projecting from $\mathbf{Z}_{117}$ to $\mathbf{Z}_{13}$ only allows coefficients from $[-9, 9]$. We have a contradiction.

Thus, there cannot exist $CW(117, 10^2)$. **Q.E.D.**

Proposition 4.4 *There does not exist any* $CW(143, 10^2)$.

Proof

$$25 \equiv 5^2 \equiv 2^{18} \pmod{143}.$$

So, 25 is a multiplier of $\mathbf{Z}_{143}$ and creates the orbit spectrum $1^1 2^6 5^2 10^{12}$. Projecting from $\mathbf{Z}_{143}$ to $\mathbf{Z}_{11}$ gives equations $a+5b+5c = 10$ and $a^2+5b^2+5c^2 = 100$, where a, b, and c are constant values on the orbits. There are two solutions to these equations (WLOG on b and c): (i) $a = 0$, $b = -2$, and $c = 4$, and (ii) $a = 10$, $b = c = 0$.

Thus, the values in $\mathbf{Z}_{11}$, ($\{0\}$, $\{1,3,9,5,4\}$, and $\{2,6,7,10,8\}$), are all even. If we focus on elements $\equiv 1 \pmod{11}$ and lift from $\mathbf{Z}_{11}$ to $\mathbf{Z}_{143}$, the multiplier 25 gives 6 orbits of size 10 that contain exactly 2 elements $\equiv 1 \pmod{11}$ and 1 orbit of size 5 that contains a single element $\equiv 1 \pmod{11}$. All elements $\equiv 1 \pmod{11}$ must add to an even number (i.e. b), so the element in the orbit of size 5 is 0. An orbit holds a constant value, so the entire orbit of size 5 is empty.

Now, if we focus on elements $\equiv 2 \pmod{11}$ and lift from $\mathbf{Z}_{11}$ to $\mathbf{Z}_{143}$, a similar situation happens and the other orbit of size five is forced to be empty. This leaves the spectrum $1^1 2^6 10^{12}$ to make the 55 $+1$'s and 45 -1's needed to satisfy the weight. This is not possible.

Thus, there does not exist $CW(143, 10^2)$. **Q.E.D.**

Proposition 4.5 *There does not exist any $CW(175, 6^2)$.*

Proof

$$4 \equiv 2^2 \equiv 3^{46} \pmod{175}.$$

Thus, 4 is a multiplier of $\mathbf{Z}_{175}$ and produces the orbit spectrum $1^1 2^2 3^2 6^4 10^2 30^4$. Project from $\mathbf{Z}_{175}$ to $\mathbf{Z}_{25}$. Using 4 as a multiplier at the $\mathbf{Z}_{25}$ gives the orbit spectrum $1^1 2^2 10^2$. Also, we see that $2^{10} \equiv 3^{10} \equiv -1 (\text{mod } 25)$. From Ma's Lemma, $ICW(25, 6^2)$ is trivial.

Now, lift from $ICW(25, 6^2)$ to $CW(175, 6^2)$. The singleton and orbits of size 3 in $\mathbf{Z}_{175}$ are multiples of 25, so these orbits must add to 6. An orbit holds a constant value, so the orbits of size 3 contain $+1$, and the singleton contains 0. This leaves the spectrum $2^2 6^4 10^2 30^4$ to make the 15 remaining $+1$'s to make $|P| = 21$, which is impossible.

Thus, there cannot exist $CW(175, 6^2)$. **Q.E.D.**

Proposition 4.6 *There does not exist any $CW(182, 5^2)$.*

Proof

$$5 \equiv 5 \pmod{182}.$$

5 is a multiplier and produces the orbit spectrum $1^2 4^6 6^2 12^{12}$. Projecting from $\mathbf{Z}_{182}$ to $\mathbf{Z}_7$ gives equations $a + 6b = 5$ and $a^2 + 6b^2 = 25$, where a and b are constant values on the orbits. The only solution is $a = 5, b = 0$. Thus, the elements $\equiv 0 \pmod 7$ in $\mathbf{Z}_{182}$, which are in the orbits of size 4 and the singletons, add to 5. So, a singleton must be $+1$.

Projecting from $\mathbf{Z}_{182}$ to $\mathbf{Z}_{13}$ and using 5 as a multiplier gives equations $a' + 4b' + 4c' + 4d' = 5$ and $a'^2 + 4b'^2 + 4c'^2 + 4d'^2 = 25$, where a', b', c', and d' are constant values on the orbits at the $\mathbf{Z}_{13}$ level. There are two solutions to these equations: (i) $a' = 5$ and $b' = c' = d' = 0$, and (ii) $a' = -3$, with exactly one of b', c', or d' $=2$. So, the elements $\equiv 0$ (mod 13) in Z_{182}, which are in the orbits of size 6 and both singletons, project into a' and add to 5 or -3. We know one singleton is $+1$, so it follows that $1+x+6y+6z=5$ or -3, where $x,y,z \in \{0,\pm 1\}$. This has no solution.

Thus, there does not exist $CW(182,5^2)$. **Q.E.D.**

Proposition 4.7 *There does not exist any $CW(145,7^2)$.*

Proof

$$7 \equiv 7 \pmod{145}.$$

7 is a multiplier and produces the orbit spectrum $1^1 4^1 7^4 28^4$. Projecting from $\mathbf{Z}_{145}$ to $\mathbf{Z}_5$, we can apply Ma's Lemma since $7^2 \equiv -1 \pmod{5}$. Thus, only the trivial solution to $ICW(5,7^2)$ exists.

Now, lift from $ICW(5,7^2)$ to $CW(145,7^2)$. The singleton and orbits of size 7 in $\mathbf{Z}_{145}$ are $\equiv 0 \pmod 5$, so these orbits must add to 7. Therefore, the singleton is empty and one orbit of size 7 contains $+1$'s. This leaves the orbit spectrum $4^1 7^3 28^4$ to make the remaining 21 $+1$'s and 21 -1's needed to satisfy the weight. This is not possible.

Thus, there does not exist $CW(145,7^2)$. **Q.E.D.**

Proposition 4.8 *There does not exist any $CW(46,6^2), CW(69,6^2)$, or $CW(92,6^2)$.*

Proof

$$4 \equiv 2^2 \equiv 3^3 \pmod{23}.$$

Projecting from $\mathbf{Z}_{46}$ to $\mathbf{Z}_{23}$ with multiplier 4 gives the equations $a+11b+11c = 6$ and $a^2+11b^2+11c^2 = 36$ where a, b, and c are constant values on the orbits. It is easy to see there are only two solutions to these equations: (i) $a=6$, $b=c=0$ and (ii) $a=-5$ and either b or $c=1$, but not both. But, projecting from $\mathbf{Z}_{46}$ to $\mathbf{Z}_{23}$ only allows coefficients from $[-2,2]$.

Thus, there cannot exist $CW(46,6^2)$

It follows from similar proofs that there cannot exist $CW(69,6^2)$ or $CW(92,6^2)$ since the Projection Theorem will be violated. **Q.E.D.**

Proposition 4.9 *There does not exist any $CW(70, 8^2)$.*

Proof

$$2 \equiv 2 \pmod{35}.$$

Project from $\mathbf{Z}_{70}$ to $\mathbf{Z}_{35}$. Using 2 as a multiplier, the orbit spectrum of $\mathbf{Z}_{35}$ is $1^1 3^2 4^1 12^2$. From Ma's Lemma, $2^2 \equiv -1 \pmod 5$ implies only the trivial solution exists at the $\mathbf{Z}_5$ level with $ICW(5, 8^2)$. Thus, the multiples of 5 at the $\mathbf{Z}_{35}$ level, which are the singleton and orbits of size 3, add to 8. $x + 3y + 3z = 8 \Rightarrow x \equiv 2 \pmod 3$ where x is the singleton of $\mathbf{Z}_{35}$ and $x, y, z \in \{0, \pm 1, \pm 2\}$.

Projecting from $\mathbf{Z}_{35}$ to $\mathbf{Z}_7$ gives equations $a + 3b + 3c = 8$ and $a^2 + 3b^2 + 3c^2 = 64$, where a, b, c are constant values on the orbits (2 is still being used as the multiplier). There are four solutions to these equations (WLOG on b and c):

$(i) a = 8, b = c = 0,$

$(ii) a = 5, b = 3, c = -2,$

$(iii) a = 2, b = 4, c = -2,$

$(iv) a = -4, b = 4, c = 0.$

The multiples of 7 at the $\mathbf{Z}_{35}$ level, which are the singleton and orbit of size 4, project into a and add to 8, 5, 3, or -2. So, $a = x + 4v = 8, 5, 2,$ or -4 where x is the singleton of $\mathbf{Z}_{35}$ and $x, v \in \{0, \pm 1, \pm 2\}$. We know from above that $x \equiv 2 \pmod 3$.

If $a = 8$ or -4, then $x \equiv 0 \pmod 4$. But, $x \equiv 0 \pmod 4$ and $x \equiv 2 \pmod 3$ has no solutions for $x \in \{0, \pm 1, \pm 2\}$. Thus, $a \neq 8$ or -4.

If $a = 5$, then $x \equiv 1 \pmod 4$. But, $x \equiv 1 \pmod 4$ and $x \equiv 2 \pmod 3$ has no solutions for $x \in \{0, \pm 1, \pm 2\}$. Thus, $a \neq 5$.

If $a = 2$, then $x \equiv 0 \pmod 2$. $x \equiv 0 \pmod 2$ and $x \equiv 2 \pmod 3$ implies x, the singleton value of $\mathbf{Z}_{35}$, is 2. Thus, we know that a, the singleton value of $\mathbf{Z}_7$, must be 2.

The orbits at the $\mathbf{Z}_7$ level are $\{0\}, \{1, 2, 4\}, \{3, 6, 5\}$ and the only solution is $a = 2, b = 4, c = -2$. If we focus on elements $\equiv 1 \pmod 7$, which add to $b(=4)$ and lift from $\mathbf{Z}_7$ to $\mathbf{Z}_{35}$, the multiplier 2 gives an orbit of size 12 that contains exactly 4 elements $\equiv 1 \pmod 7$ and an orbit of size 3 that contains a single element $\equiv 1 \pmod 7$. These elements $\in \{0, \pm 1, \pm 2\}$ and add to 4. Thus, the orbit of size 12 contains $+1$'s and the orbit of size 3 is empty.

When we lift from $\mathbf{Z}_{35}$ to $\mathbf{Z}_{70}$, the orbit of size 12 with the $+1$'s will lift 12 0's and 12 $+1$'s into $CW(70, 8^2)$. This is a contradiction because $CW(70, 8^2)$ only has six 0's.

Thus, there cannot exist $CW(70, 8^2)$. **Q.E.D.**

Proposition 4.10 *There does not exist any $CW(98, 8^2)$.*

Proof

$$2 \equiv 2 \pmod{49}.$$

Project from $\mathbf{Z}_{98}$ to $\mathbf{Z}_{49}$. This ICW in $\mathbf{Z}_{49}$ can only have values $\{0, \pm 1, \pm 2\}$. Using 2 as a multiplier, the orbit spectrum of $\mathbf{Z}_{49}$ is $1^1 3^2 21^2$ with equations (i) $a + 3b + 3c + 21d + 21e = 8$ and (ii) $a^2 + 3b^2 + 3c^2 + 21d^2 + 21e^2 = 64$ where a, b, c, d, e are constant values on the orbits.

Focus on the orbits of size 21. Neither d nor e can be ± 2 because this would make equation (ii) too large. Thus, WLOG, we have three cases to consider. (1) $d = e = \pm 1$, (2) $d = \pm 1$, $e = 0$, or (3) $d = e = 0$.

If (1) is satisfied, $d^2 = e^2 = 1$, and (ii) becomes $a^2 + 3b^2 + 3c^2 + 21 + 21 = 64$. $a^2 + 3b^2 + 3c^2 = 22$ has no solutions for $a, b, c \in \{0, \pm 1, \pm 2\}$.

If (2) is satisfied, $d^2 = 1$, $e^2 = 0$, and (ii) becomes $a^2 + 3b^2 + 3c^2 + 21 = 64$. $a^2 + 3b^2 + 3c^2 = 43$ has no solutions for $a, b, c \in \{0, \pm 1, \pm 2\}$.

If (3) is satisfied, $d^2 = e^2 = 0$, and (ii) becomes $a^2 + 3b^2 + 3c^2 = 64$. $a^2 + 3b^2 + 3c^2 = 64$ has no solutions for $a, b, c \in \{0, \pm 1, \pm 2\}$.

Thus, there cannot exist $CW(98, 8^2)$. **Q.E.D.**

Proposition 4.11 *There does not exist any $CW(154, 8^2)$.*

Proof Project from $\mathbf{Z}_{154}$ to $\mathbf{Z}_{77}$. Using 2 as a multiplier, the orbit spectrum at $\mathbf{Z}_{77}$ is $1^1 3^2 10^1 30^2$ with equations (i) $a+3b+3c+10d+30e+30f=8$ and (ii) $a^2+3b^2+3c^2+10d^2+30e^2+30f^2=64$ where a,b,c,d,e,f are constant values on the orbits.

$2^5 \equiv -1 \pmod{11}$, so by Ma's Lemma, $ICW(11,8^2)$ has only the trivial solution. Thus, the elements in $\mathbf{Z}_{77} \equiv 0 \pmod{11}$, which are in the orbits of size 3 and the singleton, add to 8. $a+3b+3c=8 \Rightarrow a \equiv 2 \pmod 3$. $a \in \{0, \pm 1, \pm 2\}$, so $a=2$ or $a=-1$. We see there are three solutions to this equation (WLOG on b and c).

(i) $a=2$, $b=2, c=0$, (ii) $a=2$, $b=1, c=1$, and (iii) $a=-1, b=2, c=1$. As a result, $a^2+3b^2+3c^2=16$ or 10, and equation (ii) becomes either $10d^2+30e^2+30f^2=48$ or $10d^2+30e^2+30f^2=54$. Neither of these have solutions.

Thus, there cannot exist $CW(154,8^2)$. **Q.E.D.**

Proposition 4.12 *There does not exist any* $CW(165,9^2)$.

Proof

$$3 \equiv 3 \pmod{55}.$$

Project from $\mathbf{Z}_{165}$ to $\mathbf{Z}_{55}$. Using 3 as a multiplier, the orbit spectrum at $\mathbf{Z}_{55}$ is $1^1 4^1 5^2 20^2$ with equations (i) $a+4b+5c+5d+20e+20f=9$ and (ii) $a^2+4b^2+5c^2+5d^2+20e^2+20f^2=81$ where a,b,c,d,e,f are constant values on the orbits.

$3^2 \equiv -1 \pmod 5$, so by Ma's Lemma, $ICW(5,9^2)$ is trivial. Thus, the elements in $\mathbf{Z}_{55} \equiv 0 \pmod 5$, which are in the orbits of size 5 and the singleton, add to 9. $a+5c+5d=9 \Rightarrow a \equiv 4 \pmod 5$. $a \in \{0, \pm 1, \pm 2 \pm 3\}$, so $a=-1$.

Now, projecting from $\mathbf{Z}_{55}$ to $\mathbf{Z}_{11}$ with 3 as a multiplier gives equations $x+5y+5z=9$ and $x^2+5y^2+5z^2=81$, where x,y,z are constant values on the orbits of $\mathbf{Z}_{11}$. $x \equiv 4 \pmod 5$ and $x \in [-9,9] \Rightarrow x=-6,-1,4$, or 9.

The multiples of 11 (i.e the elements that project into x) at the $\mathbf{Z}_{55}$ level, which are the singleton and orbits of size 4, add to -6, -1, 4, or 9. We know from above that the singleton of $\mathbf{Z}_{55}$, or a, is -1. So, $x = \{-6, -1, 4, 9\} = -1 + 4b$. Since $b \in \{0, \pm 1, \pm 2, \pm 3\}$, it is easy to see that $x = -1$ is the only possibility.

Returning to the equations at the $\mathbf{Z}_{11}$ level with $x = -1$, it follows that $5y + 5z = 10$ and $5y^2 + 5z^2 = 80$. However, $y + z = 2$ and $y^2 + z^2 = 16$ has no solutions.

Thus, there cannot exist $CW(165, 9^2)$. **Q.E.D.**

Proposition 4.13 *There does not exist any* $CW(114, 10^2)$.

Proof

$$5 \equiv 5 \equiv 2^{16} \pmod{19}.$$

Projecting from $\mathbf{Z}_{114}$ to $\mathbf{Z}_{19}$ with multiplier 5 gives the equations $a+9b+9c = 10$ and $a^2+9b^2+9c^2 = 100$ where a, b, and c are constant values on the orbits. It is easy to see there are only two solutions to these equations: (i) $a = 10$, $b = c = 0$ and (ii) $a = -8$ and either b or c =2, but not both. But, projecting from $\mathbf{Z}_{114}$ to $\mathbf{Z}_{19}$ only allows entries from ± 6.

Thus, there cannot exist $CW(114, 10^2)$. **Q.E.D.**

4.1 Matrices with Trivial ICW

All matrices in this section were shown to be non-existent using similar methods. A general proof is described, and a table shows the results.

Proposition 4.14 *According to the Projection Theorem, a $CW(n,k)$ can be projected to an $ICW(d,k)$ if $n = dm$ for some $d, m \in \mathbf{Z}$. However, when $s > m$, ($s^2 = k$), it is impossible to lift from $ICW(d,k)$ to $CW(n,k)$ with final values of -1, 0, or 1 because the singleton of $ICW(d,k)$, according to the Projection Theorem, can have a maximum value of m. (Refer to Proposition 4.3 for a written example.) In each of the following cases, only a trivial ICW exists at a lower level $\mathbf{Z}_d$ when $s > \frac{n}{d}$.*

Thus, it is impossible to construct these matrices.

The Multiplier Theorem and Ma's Lemma were used extensively throughout this section to find the trivial ICWs.

The multiplier is the first number in the congruence relation.

Table 1: Matrices with Only Trivial ICW

$CW(n,s^2)$	Multiplier of trivial ICW	d,m
$(55,6^2)$	$9 \equiv 3^2 \equiv 2^6 \pmod{55}$	55,1
$(110,6^2)$	9	55,2
$(165,6^2)$	9	55,3
$(47,6^2)$	$8 \equiv 2^3 \equiv 3^5 \pmod{47}$	47,1
$(94,6^2)$	8	47,2
$(141,6^2)$	8	47,3
$(188,6^2)$	8	47,4
$(71,6^2)$	$2 \equiv 3^{11} \pmod{71}$	71,1
$(142,6^2)$	2	71,2
$(85,6^2)$	$2 \equiv 3^{14} \pmod{17}$	17,5
$(92,8^2)$	$2 \equiv 2 \pmod{23}$	23,4
$(94,8^2)$	$2 \equiv 2 \pmod{47}$	47,2
$(118,10^2)$	$5 \equiv 2^6 \pmod{59}$	59,2
$(138,8^2)$	$2 \equiv 2 \pmod{23}$	23,6
$(141,9^2)$	$3 \equiv 3 \pmod{47}$	47,3
$(142,8^2)$	$2 \equiv 2 \pmod{71}$	71,2
$(153,10^2)$	$4 \equiv 2^2 \equiv 5^{12} \pmod{17}$	17,8
$(158,8^2)$	$2 \equiv 2 \pmod{79}$	79,2
$(177,9^2)$	$3 \equiv 3 \pmod{59}$	59,3
$(178,8^2)$	$2 \equiv 2 \pmod{89}$	89,2
$(188,8^2)$	$2 \equiv 2 \pmod{47}$	47,4
$(190,6^2)$	$2 \equiv 3^7 \pmod{95}$	95,2
$(190,8^2)$	$2 \equiv 2 \pmod{95}$	95,2
$(110,8^2)$	$2 \equiv 2 \pmod{55}$	55,2
$(138,9^2)$	$3 \equiv 3 \pmod{23}$	23,6

4.2 Matrices in Violation of Theorem 1.1

The circulant weighing matrices in this section were shown to be nonexistent because their multipliers and orbit spectrum did not allocate enough room for the ± 1's needed to satisfy the weight. (i.e. Theorem 1.1 was violated.)

Proposition 4.15 *There does not exist any* $CW(95, 6^2)$.

Proof

$$3 \equiv 2^{31} \pmod{95}.$$

3 is a multiplier and gives 5 orbits with a spectrum $1^1 36^2 18^1 4^1$. By Theorem 1.1, $|P| = 21$ and $|N| = 15$. However, there is no way to get 21 +1's and 15 -1's with the given spectrum.

Thus, there cannot exist $CW(95, 6^2)$. **Q.E.D.**

Similar proofs using multipliers, orbit spectrums, and $|P|, |N|$ show the nonexistence of the following circulant weighing matrices:

Table 2: Matrices in Violation of Theorem 1.1

$CW(n, k^2)$	Multiplier	Orbit Spectrum	$\|P\|, \|N\|$
$(115, 6^2)$	$2 \equiv 3^7 \pmod{115}$	$1^1 4^1 11^2 44^2$	21, 15
$(119, 6^2)$	$2 \equiv 3^{14} \pmod{119}$	$1^1 3^2 8^2 24^4$	21, 15
$(119, 10^2)$	$2 \equiv 5^{22} \pmod{119}$	$1^1 3^2 8^2 24^4$	55, 45
$(151, 10^2)$	$2 \equiv 5^{10} \pmod{151}$	$1^1 15^{10}$	55, 45
$(161, 6^2)$	$2 \equiv 3^{62} \pmod{161}$	$1^1 3^2 11^2 33^4$	21, 15
$(167, 6^2)$	$2 \equiv 3^{64} \pmod{167}$	$1^1 83^2$	21, 15
$(199, 10^2)$	$5 \equiv 2^{48} \pmod{199}$	$1^1 33^6$	55, 45
$(187, 6^2)$	$4 \equiv 2^2 \equiv 3^{44} \pmod{187}$	$1^1 4^4 5^2 20^8$	21, 15
$(187, 10^2)$	$4 \equiv 2^2 \equiv 5^{28} \pmod{187}$	$1^1 4^4 5^2 20^8$	55, 45
$(191, 6^2)$	$2 \equiv 3^{79} \pmod{191}$	$1^1 95^2$	21, 15
$(191, 10^2)$	$5 \equiv 2^{40} \pmod{191}$	$1^1 19^{10}$	55, 45

5 Updated Strassler's Table

Strassler's Table of Circulant Weighing Matrices originally appeared in [16]. Here, the table is updated with the information from this paper, as well as information from [2], [4], and [6].

Table Key: Existence (Y), Nonexistence (.), Nonexistence shown in this paper (N), and open cases (?) for $CW(n, s^2)$.

Table 3: Strassler's Table of $CW(n, s^2)$ in 2009

s	1	2	3	4	5	6	7	8	9	10
n										
1	Y	.	.	.	.	.	.	.	.	.
2	Y	.	.	.	.	.	.	.	.	.
3	Y	.	.	.	.	.	.	.	.	.
4	Y	Y	.	.	.	.	.	.	.	.
5	Y	.	.	.	.	.	.	.	.	.
6	Y	Y	.	.	.	.	.	.	.	.
7	Y	Y	.	.	.	.	.	.	.	.
8	Y	Y	.	.	.	.	.	.	.	.
9	Y	.	.	.	.	.	.	.	.	.
10	Y	Y	.	.	.	.	.	.	.	.
11	Y	.	.	.	.	.	.	.	.	.
12	Y	Y	.	.	.	.	.	.	.	.
13	Y	.	Y	.	.	.	.	.	.	.
14	Y	Y	.	.	.	.	.	.	.	.
15	Y	.	.	.	.	.	.	.	.	.
16	Y	Y	.	.	.	.	.	.	.	.
17	Y	.	.	.	.	.	.	.	.	.
18	Y	Y	.	.	.	.	.	.	.	.
19	Y	.	.	.	.	.	.	.	.	.
20	Y	Y	.	.	.	.	.	.	.	.
21	Y	Y	.	Y	.	.	.	.	.	.
22	Y	Y	.	.	.	.	.	.	.	.
23	Y	.	.	.	.	.	.	.	.	.
24	Y	Y	Y	.	.	.	.	.	.	.
25	Y	.	.	.	.	.	.	.	.	.
26	Y	Y	Y	.	.	.	.	.	.	.
27	Y	.	.	.	.	.	.	.	.	.
28	Y	Y	.	Y	.	.	.	.	.	.

Table 3: Strassler's Table of $CW(n, s^2)$ in 2009

29	Y	.	.	.	.	.	.	.	.	.
30	Y	Y	.	.	.	.	.	.	.	.
31	Y	.	.	Y	Y	.	.	.	.	.
32	Y	Y	.	.	?	.	.	.	.	.
33	Y	.	.	.	Y	.	.	.	.	.
34	Y	Y	.	.	.	.	.	.	.	.
35	Y	Y	.	.	.	.	.	.	.	.
36	Y	Y	.	.	.	.	.	.	.	.
37	Y	.	.	.	.	.	.	.	.	.
38	Y	Y	.	.	.	.	.	.	.	.
39	Y	.	Y	.	.	.	.	.	.	.
40	Y	Y	.	.	?	.	.	.	.	.
41	Y	.	.	.	.	.	.	.	.	.
42	Y	Y	.	Y	.	.	.	.	.	.
43	Y	.	.	.	.	.	.	.	.	.
44	Y	Y	.	.	.	.	.	.	.	.
45	Y	.	.	.	.	.	.	.	.	.
46	Y	Y	.	.	.	N	.	.	.	.
47	Y	.	.	.	.	N	.	.	.	.
48	Y	Y	Y	.	?	?	.	.	.	.
49	Y	Y	.	.	.	.	.	.	.	.
50	Y	Y	.	.	.	.	.	.	.	.
51	Y	.	.	.	.	.	.	.	.	.
52	Y	Y	Y	.	.	Y	.	.	.	.
53	Y	.	.	.	.	.	.	.	.	.
54	Y	Y	.	.	.	.	?	.	.	.
55	Y	.	.	.	.	N	.	.	.	.
56	Y	Y	.	Y	.	.	.	.	.	.
57	Y	.	.	.	.	.	Y	.	.	.
58	Y	Y	.	.	.	.	.	.	.	.
59	Y	.	.	.	.	.	.	.	.	.
60	Y	Y	.	.	.	?	.	.	.	.
61	Y	.	.	.	.	.	.	.	.	.
62	Y	Y	.	Y	Y	.	.	.	.	.
63	Y	Y	.	Y	.	.	?	.	.	.
64	Y	Y	.	.	?	.	?	.	.	.
65	Y	.	Y	.	.	.	.	.	.	.
66	Y	Y	.	.	Y	.	.	.	.	.
67	Y	.	.	.	.	.	.	.	.	.
68	Y	Y	.	.	.	?	.	.	.	.
69	Y	.	.	.	.	N	.	.	.	.
70	Y	Y	.	Y	.	?	.	N	.	.

Table 3: Strassler's Table of $CW(n, s^2)$ in 2009

71	Y	.	.	.	Y	N	.	.	.	.
72	Y	Y	Y	.	.	.	?	.	.	.
73	Y	.	.	.	.	.	.	Y	.	.
74	Y	Y	.	.	.	?	.	.	.	.
75	Y	.	.	.	.	.	.	.	.	.
76	Y	Y	.	.	.	?	?	.	.	.
77	Y	Y	.	.	.	N	.	.	.	.
78	Y	Y	Y	.	.	Y	.	.	.	.
79	Y	.	.	.	.	.	.	.	.	.
80	Y	Y	.	.	?	.	?	.	.	.
81	Y	.	.	.	.	.	N	.	.	.
82	Y	Y	.	.	.	.	.	.	.	.
83	Y	.	.	.	.	.	.	.	.	.
84	Y	Y	.	Y	.	.	.	Y	.	.
85	Y	.	.	.	.	N	.	.	.	.
86	Y	Y	.	.	.	.	.	.	.	.
87	Y	.	.	.	.	.	Y	.	.	.
88	Y	Y	.	.	?	.	.	.	?	.
89	Y	.	.	.	.	.	.	.	.	.
90	Y	Y	.	.	.	.	?	?	.	.
91	Y	Y	Y	.	.	Y	.	.	Y	.
92	Y	Y	.	.	.	N	.	N	?	.
93	Y	.	.	Y	Y	.	.	.	.	.
94	Y	Y	.	.	.	N	.	N	.	.
95	Y	.	.	.	.	N	?	.	.	.
96	Y	Y	Y	.	?	?	?	?	.	.
97	Y	.	.	.	.	.	.	.	.	.
98	Y	Y	.	Y	.	.	.	N	.	.
99	Y	.	.	.	Y	.	.	.	?	.
100	Y	Y	.	.	.	.	.	.	.	.
101	Y	.	.	.	.	.	.	.	.	.
102	Y	Y	.	.	.	.	.	.	.	.
103	Y	.	.	.	.	.	.	.	.	.
104	Y	Y	Y	.	.	Y	.	.	?	.
105	Y	Y	.	Y	.	?	.	.	?	.
106	Y	Y	.	.	.	.	.	.	.	.
107	Y	.	.	.	.	.	.	.	.	.
108	Y	Y	.	.	.	.	.	.	.	.
109	Y	.	.	.	.	.	.	.	.	.
110	Y	Y	.	.	?	N	.	N	?	?
111	Y	.	.	.	.	.	.	.	.	.
112	Y	Y	.	Y	?	?	.	?	.	?

Table 3: Strassler's Table of $CW(n, s^2)$ in 2009

113	Y	.	.	.	.	.	.	.	.	.
114	Y	Y	.	.	.	.	Y	.	.	N
115	Y	.	.	.	.	N	.	.	.	.
116	Y	Y	.	.	.	.	?	.	.	.
117	Y	.	Y	.	?	?	.	.	?	N
118	Y	Y	.	.	.	.	.	.	.	N
119	Y	Y	.	.	.	N	.	.	.	N
120	Y	Y	Y	.	?	?	?	.	.	?
121	Y	.	.	.	.	.	.	.	Y	.
122	Y	Y	.	.	.	.	.	.	.	.
123	Y	.	.	.	.	.	.	.	.	.
124	Y	Y	.	Y	Y	.	.	Y	.	Y
125	Y	.	.	.	.	.	.	.	.	.
126	Y	Y	.	Y	.	.	?	?	.	.
127	Y	.	.	.	.	.	.	Y	.	.
128	Y	Y	.	.	.	.	?	?	.	.
129	Y	.	.	.	.	.	.	.	.	.
130	Y	Y	Y	.	.	Y	.	.	?	.
131	Y	.	.	.	.	.	.	.	.	.
132	Y	Y	.	.	Y	.	.	.	?	Y
133	Y	Y	.	.	?	.	.	.	.	?
134	Y	Y	.	.	.	.	.	.	.	.
135	Y	.	.	.	.	.	.	.	.	.
136	Y	Y	.	.	.	.	.	.	.	.
137	Y	.	.	.	.	.	.	.	.	.
138	Y	Y	.	.	.	?	.	N	N	.
139	Y	.	.	.	.	.	.	.	.	.
140	Y	Y	.	Y	.	?	.	?	.	.
141	Y	.	.	.	.	N	.	.	N	.
142	Y	Y	.	.	Y	N	.	N	.	Y
143	Y	.	Y	.	.	?	.	.	?	N
144	Y	Y	Y	.	?	?	?	.	.	.
145	Y	.	.	.	.	.	N	.	.	.
146	Y	Y	.	.	.	.	.	Y	.	.
147	Y	Y	.	Y	.	.	.	?	.	.
148	Y	Y	.	.	.	.	?	.	.	.
149	Y	.	.	.	.	.	.	.	.	.
150	Y	Y	.	.	.	.	.	.	.	.
151	Y	.	.	.	.	.	.	.	.	N
152	Y	Y	.	.	?	.	?	.	.	.
153	Y	.	.	.	.	.	.	.	.	N
154	Y	Y	.	Y	.	?	.	N		?

Table 3: Strassler's Table of $CW(n, s^2)$ in 2009

155	Y	.	.	Y	Y	?	.	.	.	?
156	Y	Y	Y	.	?	Y	.	.	?	?
157	Y	.	.	.	.	.	.	.	.	.
158	Y	Y		.	.	.	.	N	.	?
159	Y	.	.	.	.	.	.	.	.	.
160	Y	Y	.	.	?	.	?	.	?	?
161	Y	Y	.	.	.	N	.	.	.	.
162	Y	Y	.	.	.	.	?	.	.	.
163	Y	.	.	.	.	.	.	.	.	.
164	Y	Y	.	.	.	.	.	.	.	.
165	Y	.	.	.	Y	N	?	.	N	?
166	Y	Y	.	.	.	.	.	.	.	.
167	Y	.	.	.	.	N	.	.	.	.
168	Y	Y	Y	Y	.	Y	.	Y	.	.
169	Y	.	Y	.	.	.	.	.	.	.
170	Y	Y	.	.	.	?	.	?	.	.
171	Y	.	.	.	?	.	Y	.	.	.
172	Y	Y	.	.	.	.	.	.	.	.
173	Y	.	.	.	.	.	.	.	.	.
174	Y	Y	.	.	.	.	Y	.	.	.
175	Y	Y	.	.	.	N	.	.	.	.
176	Y	Y	.	.	.	.	.	.	.	?
177	Y	.	.	.	.	.	.	.	N	.
178	Y	Y	.	.	.	.	.	N	.	.
179	Y	.	.	.	.	.	.	.	.	.
180	Y	Y	.	.	.	?	.	?	.	.
181	Y	.	.	.	.	.	.	.	.	.
182	Y	Y	Y	Y	N	Y	.	?	Y	?
183	Y	.	.	.	.	.	.	.	.	.
184	Y	Y	.	.	.	?	.	?	?	.
185	Y	.	.	.	.	.	.	.	.	.
186	Y	Y	.	Y	Y	.	.	Y	.	Y
187	Y	.	.	.	.	N	.	.	.	N
188	Y	Y	.	.	.	N	.	N	.	.
189	Y	Y	.	Y	.	.	?	.	.	.
190	Y	Y	.	.	?	N	?	N	.	?
191	Y	.	.	.	.	N	.	.	.	N
192	Y	Y	Y	.	?	?	?	.	?	?
193	Y	.	.	.	.	.	.	.	.	.
194	Y	Y	.	.	.	.	.	.	.	.
195	Y	.	Y	.	.	?	.	.	?	?
196	Y	Y	.	.	.	.	.	?	.	.

Table 3: Strassler's Table of $CW(n, s^2)$ in 2009

197	Y	.	.	.	.	.	.	.	.	.
198	Y	Y	.	.	Y	.	?	.	?	?
199	Y	.	.	.	.	.	.	.	.	N
200	Y	Y	.	.	.	.	.	.	.	.

6 Future Work

Although 52 previously open existence case have been settled, Strassler's Table has many cases that need solved. Research can focus on solving individual cases, or it can be extended to find a general solution for the existence of $CW(n, s^2)$ for $s \geq 5$. Moreover, while this research developed matrices over cyclic groups, it would be interesting to extend the results to see how weighing matrices are developed over non-cyclic abelian groups.

7 Acknowledgements

A tremendous amount of gratitude is owed to my teacher, advisor, and friend, Dr. K.T. Arasu not only for his continuous support during the preparation of this thesis but also for his encouragement, advice, and faith throughout my many years at Wright State University. Additional thanks goes out to his former students who laid the foundation for this research. Without their work, completion of this paper would have been impossible. I am also indebted to the entire Mathematics department at Wright State for the education I was so fortunate to receive. Special recognition is owed to Dr. Yuqing Chen and Dr. Xiaoyu Liu for meticulously reviewing this work.

Finally, I would like to thank my parents, Ed and Nancy, and my best friend and fiancée, Erin. Although they may never understand the words and symbols printed on these pages, their love and encouragement during my study of mathematics made this thesis possible.

References

[1] M.H. Ang, K.T. Arasu, S.L. Ma and Y. Strassler, *Study of Proper Circulant Weighing Matrices with weight 9*, Discrete Mathematics 308, 13, (2008), 2802-2809

[2] K.T. Arasu, *A reduction theorem for circulant weighing matrices*, Australas. J. Combin., 18 (1998), 111-114

[3] K.T. Arasu, J.F. Dillon, D. Jungnickel, and A. Pott, *The Solution of the Waterloo Problem*, J. Combin. Theory Ser., 71, 2 (1995), 316 - 331

[4] K.T. Arasu, I.S. Kotsireas, C. Koukouvinos, and J. Seberry, *One two circulant weighing matrices*, (2008), preprint

[5] K.T. Arasu, K.H. Leung, S.L. Ma, A. Nabavi, and D.K. Ray-Chaudhuri, *Determination of all possible orders of weight 16 circulant weighing matrics*, Finite Fields and Their Applications, 12 (2006), 498-538

[6] K.T. Arasu and S.L. Ma, *Some new results on circulant weighing matrices*, J. Algebraic Combin., 14 (2001), 91-101

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

[8] K.T. Arasu and J. Seberry, *Circulant Weighing Designs*, J. Combin. Designs, 4 (1996), 437-439

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

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

[11] A.V. Geramita and J. Sebery, *Orthogonal designs: Quadratic forms and Hadamard matrices*, Lecture Notes in Pure and Applied Mathematics, New York: Dekker, (1979)

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

[13] R.L. McFarland, *On multipliers of abelian difference sets*, Ph.D. Thesis, The Ohio State University, (1970)

[14] R.C. Mullin, "*A Note on Balanced Weighing Matrices*," *Combinatorial Mathematics III: Proceedings of the Third Australian Conference*, in Lecture notes in mathematics, Vol. 45 Spring-Werlag, Berlin-Heidelberg-New York, (1975), 28-41

[15] J. Seberry Wallis and A.L. Whiteman, *Some Results on Weighing Matrices*, Bull. Austral. Math. Sec., 12 (1975), 433-447.

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