On the Existance of Certain Circulant Weighing Matrices

Vassil Yorgov
Fayetteville State University
1200 Murchison Rd, Fayetteville, NC 28301
vyorgov@uncfsu.edu

Abstract

We prove nonexistence of circulant weighing matrices with parameters from seven previously open entries of the updated Strassler's table. The method of proof utilizes some modular constraints on circulant weighing matrices with multipliers.

1 Introduction

For any two positive integers n and k with $k \leq n$, a matrix W of order n with entries from the set $\{1, -1, 0\}$ satisfying

$$W \cdot W^T = kI,$$

where I is the identity matrix of order n, is called a weighing matrix of order n with weight k and is denoted by $W(n, k)$. All weighing matrices of order not exceeding 12 are completely classified. For larger orders numerous weighing matrices are known.

Circulant matrix is a square matrix in which each row (except for the first one) is a right cyclic shift of its predecessor. The ring of all circulant matrices of order n over the integers, $\mathbb{Z}$, is isomorphic to the quotient ring $R_n = \mathbb{Z}[x]/(x^n - 1)$. A natural isomorphism takes the circulant matrix W with first row $(w_0, w_1, \ldots, w_{n-1})$ into the polynomial $w(x) = w_0 + w_1 x + \ldots + w_{n-1} x^{n-1}$ and we can work with $w(x)$ instead of W. A polynomial $w(x)$ with coefficients from the set $\{1, -1, 0\}$ determines a circulant weighing matrix if and only if

$$w(x)w(x^{n-1}) = k \text{ in } R_n.$$

JCMCC **86** (2013), pp. 73-85

We denote $CW(n,k)$ the set of all circulant weighing matrices of length n and weight k. If $w(x) \in CW(n,k)$, so does $-w(x)$. In this work we assume that the number of ones in a circulant weighing matrix is greater then the number of negative ones.

Theorem 1 *(Mullin [11]) If $w(x)$ is in $CW(n,k)$, then:*
(1) $k = s^2$ for some positive integer s, and
(2) $w(x)$ has $(s^2+s)/2$ coefficients equal to one and $(s^2-s)/2$ coefficients equal to negative one.

The following theorem shows in particular that if a circulant weighing matrix of a given order n exists, then there exist circulant weighing matrices of order any multiple of n.

Theorem 2 *(Geramita and Seberry [9]) If there exist $CW(n_1,k)$ and $CW(n_2,k)$ with $\gcd(n_1,n_2)=1$, then there exist*
(1) $CW(mn_1,k)$ for all positive integers m;
(2) two inequivalent $CW(n_1n_2,k)$;
(3) $CW(n_1n_2,k^2)$.

2 Some Known Existence Results

All orders for which circulant weighing matrices of weight 4, 9, or 16 exist are given in the next three theorems.

Theorem 3 *(Eades, Hain [7]) A $CW(n,4)$ exists if and only if $n \geq 4$ is even or 7 divides n.*

Theorem 4 *(Ang et al. [1] and Strassler [13]) A $CW(n,9)$ exists 13 divides n or 24 divides n.*

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

Some infinite classes of circulant weighing matrices are provided in the next three theorems.

Theorem 6 *(Wallis and Whiteman [12]) If q is a prime power, then there exists a $CW(q^2+q+1,q^2)$.*

Theorem 7 *(Eades [6]) If q is a prime power, q odd and i even, then there exists a $CW(\frac{q^{i+1}-1}{q-1}, q^i)$.*

Theorem 8 *(Arasu et al. [2]) If $q = 2^t$ and i even, then there exists a $CW(\frac{q^{i+1}-1}{q-1}, q^i)$.*

3 Modular Constraints

We will obtain and use some modular restrictions on circulant weighing matrices having multipliers. Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ and

$$\mathbb{Z}_n^* = \{q \in \mathbb{Z}_n \mid \gcd(q, n) = 1\}.$$

Definition. An integer $t \in \mathbb{Z}_n^*$ is called a multiplier of $a(x) \in R_n$ if $a(x^t) = x^m a(x)$ for some integer $m \in \mathbb{Z}_n$.

Theorem 9 *(The Multiplier Theorem [10]) Let $a(x) \in R_n$ and $a(x)a(x^{-1}) = k$ for some positive integer k relatively prime to n. Let $k = p_1^{e_1} \cdots p_r^{e_r}$ be the prime power factorization of k. Suppose there are integers t, $f_1, \ldots, f_r$ such that*

$$t \equiv p_1^{f_1} \equiv \cdots \equiv p_r^{f_r} \pmod{n}.$$

Then t is a multiplier of $a(x)$.

Corollary 10 *Let $a(x) \in R_n$ and $a(x)a(x^{-1}) = k$ for some positive integer $k = p^e$, where p is a prime not dividing n. Then p is a multiplier of $a(x)$.*

For $a(x) \in CW(n, k)$, $u \in \mathbb{Z}_n$, and $v \in \mathbb{Z}_n^*$, the polynomial $x^u a(x^v) \in CW(n, k)$. The weighing matrix $x^u a(x^v)$ is called equivalent to $a(x)$.

Corollary 11 *[4] If $a(x)$ is in $CW(n, k)$, $\gcd(k, n) = 1$, and t is a multiplier of $a(x)$, then for some $u \in \mathbb{Z}_n$ the equivalent weighing matrix $w(x) = x^u a(x)$ is fixed by t, i.e. $w(x^t) = w(x)$.*

Let p be a prime not dividing n and

$$x^n - 1 = f_1(x) f_2(x) \cdots f_r(x)$$

be the factorization of $x^n - 1$ into irreducible factors over the field $\mathbb{Z}_p$. It is known ([8], Theorem 4.3.8) that the factor ring $\mathbb{Z}_p[x]/(x^n - 1)$ is a direct sum of minimal ideals,

$$\mathbb{Z}_p[x]/(x^n - 1) = J_1 \oplus J_2 \oplus \ldots \oplus J_r \quad (1)$$

where J_i is generated by

$$\widehat{f}_i(x) = f_1(x) \cdots f_{i-1}(x) f_{i+1}(x) \cdots f_r(x)$$

for $i = 1, 2, \ldots, r$. The unity, $e_i(x)$, of J_i is called the idempotent of J_i. In order to compute the idempotents we apply the Euclidian algorithm and find polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}_p[x]$ such that

$$u(x)\widehat{f}_i(x) + v(x) f_i(x) = 1.$$

Then $e_i(x) = u(x)\widehat{f}_i(x)$.

It is easy to check that the map in the ring $\mathbb{Z}_p[x]/(x^n - 1)$ that fixes the elements of $\mathbb{Z}_p$ and sends x to x^{n-1} is a ring automorphism. It follows that $e_i(x^{n-1}) = e_{\mu(i)}(x)$ where $\mu(i)$ is an integer, $1 \leq \mu(i) \leq r$ for $i = 1, 2, \ldots, r$. The map μ is a permutation of order two from S_r, the symmetric group of degree r.

Theorem 12 *Assume $w(x) \in CW(n, s^2)$ has a prime fixing multiplier p which divides s and does not divide n. Then*

$$w(x) = c_1 e_1(x) + c_2 e_2(x) + \cdots + c_r e_r(x)$$

in $\mathbb{Z}_p[x]/(x^n - 1)$ where $c_i \in \mathbb{Z}_p$ and $c_i c_{\mu(i)} = 0$ for $i = 1, 2, \ldots, r$. Particularly, $c_i = 0$ when $\mu(i) = i$.

Proof. The equalities $w(x^p) = w(x)$ and $w(x)w(x^{n-1}) = s^2$ hold in the ring R_n. Reducing the coefficients of the polynomials modulo p gives the natural ring homomorphism $\mathbb{Z}[x]/(x^n - 1) \to \mathbb{Z}_p[x]/(x^n - 1)$. Identifying $w(x)$ with its image we obtain the following equalities in the ring $\mathbb{Z}_p[x]/(x^n - 1)$:

$$w(x^p) = w(x) \tag{2}$$

and

$$w(x)w(x^{n-1}) = 0. \tag{3}$$

Since $\mathbb{Z}_p[x]/(x^n - 1)$ is a direct sum of minimal ideals, the idempotents of the ideals satisfy the equalities $e_i(x)e_j(x) = 0$ for $i \neq j$ and $e_i(x)^2 = e_i(x)$. The polynomial $w(x)$ is an element of $\mathbb{Z}_p[x]/(x^n - 1)$ and can be written as

$$w(x) = c_1(x)e_1(x) + \cdots + c_r(x)e_r(x),$$

where $c_1(x) \in J_1, \ldots, c_r(x) \in J_r$. Since the characteristic of the ring $\mathbb{Z}_p[x]/(x^n - 1)$ is p, equation (2) implies

$$\begin{aligned} w(x) &= w(x^p) = w(x)^p \\ &= c_1(x)^p e_1(x) + \cdots + c_r(x)^p e_r(x). \end{aligned}$$

Hence, $c_i(x)^p = c_i(x)$ for $i = 1, 2, \ldots, r$. As the minimal ideal J_i is an extension field of $\mathbb{Z}_p$, this implies $c_i(x) \in \mathbb{Z}_p$. Thus, we can replace $c_i(x)$ by $c_i \in \mathbb{Z}_p$ and write $w(x) = c_1 e_1(x) + \cdots + c_r e_r(x)$. Then

$$\begin{aligned} w(x^{n-1}) &= c_1 e_1(x^{n-1}) + \cdots + c_r e_r(x^{n-1}) \\ &= c_1 e_{\mu(1)}(x) + \cdots + c_r e_{\mu(r)}(x) \\ &= c_{\mu(1)} e_{\mu\mu(1)}(x) + \cdots + c_{\mu(r)} e_{\mu\mu(r)}(x) \\ &= c_{\mu(1)} e_1(x) + \cdots + c_{\mu(r)} e_r(x) \end{aligned}$$

because $\mu^2 = id$. Equation (3) gives

$$w(x)w(x^{n-1}) = c_1 c_{\mu(1)} e_1(x) + \cdots + c_r c_{\mu(r)} e_r(x) = 0.$$

Thus, $c_i c_{\mu(i)} = 0$ for $i = 1, 2, \ldots, r$. If $\mu(i) = i$ we have $c_i c_i = 0$ so $c_i = 0$. ∎

Let $p \in \mathbb{Z}_n^*$ and let $\langle p \rangle$ be the multiplicative subgroup of $\mathbb{Z}_n^*$ generated by p. The order of $\langle p \rangle$ is equal to the smallest positive integer d such that $p^d \equiv 1 \pmod{n}$. Lets define the action of $p^t \in \langle p \rangle$ on i from the additive group $\mathbb{Z}_n$ by $p^t i \pmod{n}$. The orbits of this action are called p-cyclotomic classes modulo n. The length of each p-cyclotomic class modulo n is a divisor of d. The number r of minimal ideals in (1) is equal to the number of p-cyclotomic classes modulo n ([8], Theorem 4.1.1).

In the next theorem we obtain some equations which a circulant weighing matrix with certain prime multipliers satisfy.

Theorem 13 *Assume $w(x) \in CW(n, s^2)$ has a prime fixing multiplier p which divides s and does not divide n. Let $C_1, \ldots, C_r$ be the p-cyclotomic classes modulo n in some order. Denote $h_i(x) = \sum_{q \in C_i} x^q$, $i = 1, 2, \ldots, r$. Then, in the notations of Theorem 12, the following equalities hold over $\mathbb{Z}_p$:*

(i) $w(x) = \sum_{i=1}^{r} d_i h_i(x)$, where each d_i is 0, 1, or -1;

(ii) $h_j(x) = \sum_{i=1}^{r} t_{ij} e_i(x)$, where $j = 1, 2, \ldots, r$ and $t_{ij} \in \mathbb{Z}_p$;

(iii) $\sum_{j=1}^{r} t_{ij} d_j = 0$ or $\sum_{j=1}^{r} t_{\mu(i)j} d_j = 0$ for $i = 1, \ldots, r$;

(iv) if $\mu(i) = i$, then $\sum_{j=1}^{r} t_{ij} d_j = 0$.

Proof. Condition (i) follows from the fact that p is a fixing multiplier of $w(x)$ and $w(x)$ defines a weighing matrix. The polynomial $w(x)$ belongs to the linear span V of $h_1(x), \ldots, h_r(x)$ over $\mathbb{Z}_p$. The idempotents $e_j(x) \in \mathbb{Z}_p[x]/(x^n - 1)$ satisfy the equalities $e_j(x^p) = e_j(x)^p = e_j(x)$ and also belong to V. Hence, $e_1(x), \ldots, e_r(x)$ and $h_1(x), \ldots, h_r(x)$ are two bases of V. The matrix $T = (t_{ij})$ defined in (ii) is the change of basis matrix. Now (iii), and (iv) follow from Theorem 12. ∎

4 Nonexistence of Certain Circulant Weighing Matrices

The Strassler [13] table contains information for existence of circulant weighing matrices, $CW(n,k)$, of order $n \leq 200$ and weight $k \leq 100$. The last update of the table is done by Arasu and Gutman [3]. The updated table still has open entries. In the following theorem we solve some of these open problems. We use software system Maple to find the matrix T from Theorem 13. The running time for each of the seven cases below is less then 10 seconds.

Theorem 14 *Circulant weighing matrices $CW(n,k)$ do not exist for*
(i) $n = 117, 133, 152, 171$ and $k = 25$;
(ii) $n = 148, 162, 198$ and $k = 49$.

Proof. (a) Assume that $CW(117,25)$ is not empty. According to Corollaries 10 and 11 there exists a $w(x) \in CW(117,25)$ for which 5 is a fixing multiplier. The number of 5-cyclotomic classes modulo 117 is 18. We order the classes by ordering their representatives as follows:

$$[1, 2, 4, 7, 14, 23, 13, 3, 6, 9, 12, 18, 21, 36, 42, 69, 39, 0].$$

Under this ordering the weights of the polynomials $h_i(x)$, $i = 1, 2, \ldots, 18$, from Theorem 13 are given in the next table

i	1	2	3	4	5	6	7	8	9	10
$wt(h_i)$	12	12	12	12	12	12	6	4	4	4

i	11	12	13	14	15	16	17	18
$wt(h_i)$	4	4	4	4	4	4	2	1

where $wt(h_i)$ is the number of nonzero coefficients of $h_i(x)$.
The table shows that $wt(h_1(x)) = 12$ and so on. Theorem 1 implies that $w(x)$ has 15 coefficients equal to 1 and 10 coefficients equal to -1. From Theorem 13 (i) $w(x) = \sum_{i=1}^{18} d_i h_i(x)$ where each d_i is 0, 1, or -1. For $j = 1, 2, \ldots, 12$, let denote p_j (n_j), the number of coefficients d_i equal to 1

(-1), and $wt(h_i(x)) = j$. Then we have the following equations in $\mathbb{Z}$:

$$\begin{aligned} 12p_{12} + 6p_6 + 4p_4 + 2p_2 + p_1 &= 15 \\ 6n_6 + 4n_4 + 2n_2 + n_1 &= 10. \end{aligned}$$

It follows that $p_{12} \in \{0,1\}$, p_1 is odd and n_1 is even. As only $h_{18}(x)$ has weight 1, $p_1 + n_1 \le 1$. It follows that $p_1 = d_{18} = 1$, $n_1 = 0$. There are six equations from Theorem 13 (iv) over $\mathbb{Z}_5$. Three of them are as follows:

$$\begin{aligned} d_1 + d_5 + 2d_{11} + 2d_{12} + 2d_{13} &\equiv 0 \pmod 5, \\ d_2 + d_6 + 3d_9 + 3d_{11} + 3d_{13} + 2d_{14} + 3d_{16} + 4d_{17} &\equiv 0 \pmod 5, \\ d_3 + d_4 + 2d_9 + 3d_{12} + 3d_{14} + 2d_{16} + 2d_{18} &\equiv 0 \pmod 5. \end{aligned}$$

Adding the congruences, we obtain

$$d_1 + d_2 + d_3 + d_4 + d_5 + d_6 + 4d_{17} + 2d_{18} \equiv 0 \pmod 5.$$

Hence, $p_{12} + 4d_{17} + 2 \equiv 0 \pmod 5$. As $p_{12} \in \{0,1\}$ and $d_{17} \in \{0,1,-1\}$, the last congruence is impossible. This shows that a $CW(117,25)$ does not exist.

(b) Assume that $CW(133,25)$ is not empty. Corollaries 10 and 11 imply the existence of $w(x) \in CW(133,25)$ for which 5 is a fixing multiplier. We select the following representatives for the 5-cyclotomic classes modulo 133:

$$[1,2,3,6,9,18,7,14,19,0].$$

Under this ordering, the weights of the polynomials $h_i(x)$, $i = 1,2,\ldots,18$, from Theorem 13 are as follows:

i	1	2	3	4	5	6	7	8	9	10
$wt(h_i)$	18	18	18	18	18	18	9	9	6	1

From Theorem 13 (i) $w(x) = \sum_{i=1}^{10} d_i h_i(x)$ where each d_i is 0, 1, or -1. Since $w(x)$ has 15 ones and 10 negative ones, $d_i = 0$ for $i = 1,2,\ldots,6$. The congruences from Theorem 13 (iv) are

$$\begin{aligned} 2d_9 &\equiv 0 \pmod 5, \\ d_7 + d_8 + 4d_{10} &\equiv 0 \pmod 5. \end{aligned}$$

Hence, $d_9 = 0$ and $w(x)$ cannot have 15 ones. This contradiction shows that $CW(133,25)$ is empty.

(c) Assume that $CW(152,25)$ is not empty. According to Corollaries 10 and 11 there exists a $w(x) \in CW(152,25)$ for which 5 is a fixing multiplier.

The number of 5-cyclotomic classes modulo 152 is 18. We order the classes by ordering their representatives as follows:

$$[1,3,7,13,2,4,6,8,12,14,16,26,19,57,0,38,76,114].$$

Under this ordering the weights of the polynomials $h_i(x)$ are

i	1	2	3	4	5	6	7	8	9	10
$wt(h_i)$	18	18	18	18	9	9	9	9	9	9

i	11	12	13	14	15	16	17	18
$wt(h_i)$	9	9	2	2	1	1	1	1

.

Now $w(x) = \sum_{i=1}^{18} d_i h_i(x)$ where each d_i is 0, 1, or -1. For $j = 1,2,\ldots,18$, let denote p_j (n_j), the number of coefficients d_i equal to 1 (-1), and $wt(h_i(x)) = j$. Then we have the following equations in $\mathbb{Z}$:

$$\begin{aligned} 9p_9 + 2p_2 + p_1 &= 15 \\ 9n_9 + 2n_2 + n_1 &= 10. \end{aligned}$$

From the table we obtain $p_2 + n_2 \leq 2$ and $p_1 + n_1 \leq 4$. Hence, $p_9 = 1$, $p_2 = 2$, $p_1 = 1$, $n_9 = 1$, $n_2 = 0$, and $n_1 = 1$. One of the congruences from Theorem 13 (iv) looks like

$$d_1 + d_2 + d_3 + d_4 + 4d_{13} + 4d_{14} \equiv 0 \pmod 5 .$$

As $wt(h_i(x)) = 18$ for $i = 1,2,3,4$, we have $d_1 = d_2 = d_3 = d_4 = 0$. Hence, $d_{13} + d_{14} \equiv 0 \pmod 5$, $p_2 - n_2 = d_{13} + d_{14} = 0$, and $p_2 = n_2$. But we have $p_2 = 2$ and $n_2 = 0$. This contradiction shows that $CW(152,25)$ is empty.

(d) Assume that $CW(171,25)$ is not empty. This case is similar to case (c). The number of 5-cyclotomic classes modulo 152 is 13. We order the representatives as follows:

$$[1,2,3,4,6,8,13,16,9,18,19,57,0].$$

The weights of the polynomials $h_i(x)$ are

i	1	2	3	4	5	6	7	8	9	10	11	12	13
$wt(h_i)$	18	18	18	18	18	18	18	18	9	9	6	2	1

and two of the of the congruences from Theorem 13 (iv) look like

$$\begin{aligned} d_1 + d_2 + d_4 + d_6 + d_7 + d_8 + 2d_{11} &\equiv 0 \pmod 5, \\ d_3 + d_5 + 4d_{12} &\equiv 0 \pmod 5. \end{aligned}$$

As $wt(h_i(x)) = 18$ for $i = 1,2,\ldots,8$, we have $d_i = 0$. The above congruences imply $d_{11} = d_{12} = 0$. Hence, $p_6 = 0$, $p_2 = 0$, and $9p_9 + p_1 = 15$. Since $p_1 \leq 1$, the last equation does not have a solution in nonnegative integers. Hence, $CW(171,25)$ is empty.

(e) Assume that $CW(148,49)$ is not empty. According to Corollaries 10 and 11, there exists a $w(x) \in CW(148,49)$ for which 7 is a fixing multiplier. The number of 7-cyclotomic classes modulo 148 is 15. We order the classes by ordering their representatives as follows:

$$[1,3,5,15,2,4,6,8,10,12,20,30,37,0,74].$$

Under this ordering, the weights of the polynomials $h_i(x)$, $i = 1,2,\ldots,15$, from Theorem 13 are

i	1	2	3	4	5	6	7	8	9	10	11	12
$wt(h_i)$	18	18	18	18	9	9	9	9	9	9	9	9

i	13	14	15
$wt(h_i)$	2	1	1

Theorem 1 implies that $w(x)$ has 28 coefficients equal to 1 and 21 coefficients equal to -1. From Theorem 13 (i), $w(x) = \sum_{i=1}^{18} d_i h_i(x)$ where each d_i is 0, 1, or -1. For $j = 1,2,\ldots,18$, let denote p_j (n_j), the number of coefficients d_i equal to 1 (-1), and $wt(h_i(x)) = j$. Then we have the following equations in $\mathbb{Z}$:

$$\begin{aligned} 18p_{18} + 9p_9 + 2p_2 + p_1 &= 28, \\ 18n_{18} + 9n_9 + 2n_2 + n_1 &= 21. \end{aligned}$$

It follows that $p_2 \in \{0,1\}$, $p_1 \in \{0,1,2\}$, $n_2 \in \{0,1\}$, and $n_1 \in \{0,1,2\}$. Reducing the above two equations modulo 9 we obtain $2p_2+p_1 \equiv 1 \pmod 9$ and $2n_2 + n_1 \equiv 3 \pmod 9$. Hence, $p_2 = 0$, $p_1 = 1$, $n_2 = 1$, and $n_1 = 1$. There are three equations from Theorem 13 (iv) over $\mathbb{Z}_7$. One of them is:

$$d_1 + d_2 + d_3 + d_4 + 4d_{13} \equiv 0 \pmod 7.$$

Since $p_2 = 0$ and $n_2 = 1$, we have $d_{13} = -1$. As $d_1+d_2+d_3+d_4 = p_{18}-n_{18}$, the congruence becomes $p_{18} - n_{18} - 4 \equiv 0 \pmod 7$. Thus $p_{18} - n_{18} \equiv 3 \pmod 7$. This is impossible because $p_{18} \in \{0,1\}$, and $n_{18} \in \{0,1\}$. Hence, $CW(148,49)$ is empty.

(f) Assume that $CW(162,49)$ is not empty. According to Corollaries 10 and 11, there exists a $w(x) \in CW(162,49)$ for which 7 is a fixing multiplier. The number of 7-cyclotomic classes modulo 162 is 18. We order the classes by ordering their representatives as follows:

$$[1,2,4,5,3,6,12,15,9,18,36,45,0,27,54,81,108,135].$$

The weights of the polynomials $h_i(x)$ are

i	1	2	3	4	5	6	7	8	9	10	11	12
$wt(h_i)$	27	27	27	27	9	9	9	9	3	3	3	3

i	13	14	15	16	17	18
$wt(h_i)$	1	1	1	1	1	1

. With notations as in the previous case, we have the following equations in $\mathbb{Z}$:

$$\begin{aligned} 27p_{27} + 9p_9 + 3p_3 + p_1 &= 28, \\ 9n_9 + 3n_3 + n_1 &= 21. \end{aligned}$$

It follows that $p_1 \equiv 1 \pmod 3$ and $n_1 \equiv 0 \pmod 3$. Since $p_1 + n_1 \leq 6$, we have

$$p_1 = 1, n_1 = 0 \text{ or } p_1 = 1, n_1 = 3 \text{ or } p_1 = 4, n_1 = 0. \tag{4}$$

Theorem 13 (iii) gives, among the others, the following equations over $\mathbb{Z}_7$:
$(d_{13} + 2d_{14} + 4d_{15} + d_{16} + 2d_{17} + 4d_{18} = 0$ or
$d_{13} + 4d_{14} + 2d_{15} + d_{16} + 4d_{17} + 2d_{18} = 0)$ and
$(d_{13} + 3d_{14} + 2d_{15} + 6d_{16} + 4d_{17} + 5d_{18} = 0$ or
$d_{13} + 5d_{14} + 4d_{15} + 6d_{16} + 2d_{17} + 3d_{18} = 0)$.
Hence at least one of the following systems must have a solution with $d_i \in \{-1, 0, 1\}$ satisfying (4):

$$\left| \begin{aligned} d_{13} + 2d_{14} + 4d_{15} + d_{16} + 2d_{17} + 4d_{18} &= 0 \\ d_{13} + 3d_{14} + 2d_{15} + 6d_{16} + 4d_{17} + 5d_{18} &= 0 \end{aligned} \right. \tag{5}$$

or

$$\left| \begin{aligned} d_{13} + 2d_{14} + 4d_{15} + d_{16} + 2d_{17} + 4d_{18} &= 0 \\ d_{13} + 5d_{14} + 4d_{15} + 6d_{16} + 2d_{17} + 3d_{18} &= 0 \end{aligned} \right. \tag{6}$$

or

$$\left| \begin{aligned} d_{13} + 4d_{14} + 2d_{15} + d_{16} + 4d_{17} + 2d_{18} &= 0 \\ d_{13} + 3d_{14} + 2d_{15} + 6d_{16} + 4d_{17} + 5d_{18} &= 0 \end{aligned} \right. \tag{7}$$

or

$$\left| \begin{aligned} d_{13} + 4d_{14} + 2d_{15} + d_{16} + 4d_{17} + 2d_{18} &= 0 \\ d_{13} + 5d_{14} + 4d_{15} + 6d_{16} + 2d_{17} + 3d_{18} &= 0 \end{aligned} \right. . \tag{8}$$

The solution space of the system (5) is the row space over $\mathbb{Z}_7$ of the matrix

$$\begin{bmatrix} -1 & 2 & 1 & 0 & 0 & 0 \\ 2 & 2 & 0 & 1 & 0 & 0 \\ 2 & -2 & 0 & 0 & 1 & 0 \\ -2 & -1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

A check shows that the row space does not have a vector with a unique nonzero entry equal to 1; does not have a vector with two entries equal to 0, three entries equal to -1, and one entry equal to 1; does not have a vector with two entries equal to 0 and four entries equal to 1. Thus, the systems (5) does not have solutions with $d_i \in \{-1,0,1\}$ satisfying (4).

We obtain similarly that the systems (6), (7), and (8) do not have solutions with $d_i \in \{-1,0,1\}$ satisfying (4).

This contradiction shows that $CW(162,49)$ is empty.

(g) Assume that $CW(198,49)$ is not empty. Corollaries 10 and 11 imply the existence of $w(x) \in CW(198,49)$ for which 7 is a fixing multiplier. The number of 7-cyclotomic classes modulo 162 is 20. We order the classes by ordering their representatives as follows:

$$[1,2,4,5,3,6,9,12,15,18,11,22,44,55,0,33,66,99,132,165].$$

The weights of the polynomials $h_i(x)$ are

i	1	2	3	4	5	6	7	8	9	10
$wt(h_i)$	30	30	30	30	10	10	10	10	10	10
i	11	12	13	14	15	16	17	18	19	20
$wt(h_i)$	3	3	3	3	1	1	1	1	1	1

Theorem 1 implies that $w(x)$ has 28 coefficients equal to 1 and 21 coefficients equal to -1. From Theorem 13 (i), $w(x) = \sum_{i=1}^{20} d_i h_i(x)$ where each d_i is 0, 1, or -1. For $j = 1,2,\ldots,30$, let denote p_j (n_j), the number of coefficients d_i equal to 1 (-1), and $wt(h_i(x)) = j$. Hence, $d_1 = d_2 = d_3 = d_4 = 0$. We have the following equations in $\mathbb{Z}$:

$$\begin{aligned} 10p_{10} + 3p_3 + p_1 &= 28, \\ 10n_{10} + 3n_3 + n_1 &= 21, \end{aligned}$$

and $10(p_{10} + n_{10}) + 3(p_3 + n_3) + p_1 + n_1 = 49$. It follows from the table above that $p_3 + n_3 \leq 4$ and $p_1 + n_1 \leq 6$. The previous equality implies $p_{10} + n_{10} \geq 4$. The congruences from Theorem 13 (iv) are

$$\begin{aligned} d_5 + d_7 + d_9 &\equiv 0 \pmod 7, \\ d_6 + d_8 + d_{10} &\equiv 0 \pmod 7, \\ d_{11} + d_{14} + 5d_{16} + 5d_{18} + 5d_{20} &\equiv 0 \pmod 7, \\ d_{12} + d_{13} + 5d_{15} + 5d_{17} + 5d_{19} &\equiv 0 \pmod 7. \end{aligned} \tag{9}$$

The first two of them imply $p_{10} = n_{10} \leq 2$. Hence, $p_{10} = n_{10} = 2$. Thus $n_3 = 0$ and $n_1 = 1$.

Clearly, $p_3 \in \{1,2\}$. If $p_3 = 1$, then $p_1 = 5$ and one of the last two congruences of (9), say, the last one, would be $d_{12} + d_{13} + 15 \equiv 0 \pmod 7$. This is impossible because $n_3 = 0$ and each of d_{12} and d_{13} is either 0 or 1. Hence, $p_3 = 2$, and $p_1 = 2$.

One of the equations of Theorem 13 (iii) is

$$\begin{aligned} & 5(d_{11}+d_{13})+6(d_{12}+d_{14}) \\ \equiv\ & -(d_5+d_6+\cdots+d_{10})-(d_{15}+d_{16}+\cdots+d_{20}) \pmod 7 . \end{aligned}$$

Its corresponding equation under the permutation μ is

$$\begin{aligned} & 6(d_{11}+d_{13})+5(d_{12}+d_{14}) \\ \equiv\ & -(d_5+d_6+\cdots+d_{10})-(d_{15}+d_{16}+\cdots+d_{20}) \pmod 7 . \end{aligned}$$

But $d_5+d_6+\cdots+d_{10}=p_{10}-n_{10}=0$, and $d_{15}+d_{16}+\cdots+d_{20}=p_1-n_1=1$. Thus,

$$\begin{aligned} 5(d_{11}+d_{13})+6(d_{12}+d_{14}) &\equiv 6 \pmod 7, \text{ or} \\ 6(d_{11}+d_{13})+5(d_{12}+d_{14}) &\equiv 6 \pmod 7 . \end{aligned}$$

Because $n_3=0$ and $p_3=2$, two of the d's are equal to 0 and the other two are are equal to 1. No combination of two zeros and two ones makes any one of the congruences true. This contradicts Theorem 13 (iii). Hence, $CW(198,49)$ is empty.

Acknowledgement This work was partially supported by a Faculty Research Mini-Grant funded by Fayetteville State University HBCU Master's Degree STEM Program.

References

[1] M. H. Ang, K. T. Arasu, S. L. Ma, Y. Strassler, Study of proper circulant weighing matrices with weight 9. Discrete Math. 308 (2008), 2902-2809.

[2] K. T. Arasu, J. F. Dillon, D. Jungnickel and A. Pott, The solution of the Waterloo problem. J. Combin. Theory (A), 17, (1995), 316-331.

[3] K. T. Arasu, A. J. Gutman, Circulant weighing matrices. Cryptogr. Commun., 2 (2010),155 -171.

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

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

[6] P. Eades, On the existence of orthogonal designs. Ph.D. thesis, Australian National University, Canberra, 1977.

[7] P. Eades, R. M. Hain, On circulant weighing matrices. Ars Comb. 2, (1976) 265-284.

[8] W. Cary Huffman and Vera Pless, Fundamentals of Error-Correcting Codes (Cambridge University Press, New York, 2003).

[9] A. V. Geramita, J. Seberry, Orthogonal designs: quadratic forms and Hadamard Matrices, Lecture Notes in Pure and Applied Mathematics, Dekker, New York (1979).

[10] R. L. McFarland, On multipliers of abelian difference sets, Ph.D. thesis, The Ohio State University, 1970.

[11] R. C. Mullin, A note on balanced weighing matrices. In: Combinatorial Mathematics III: Proceedings of the Third Australian Conference. Lecture Notes in Mathematics, vol. 452, pp. 28-41, Springer-Verlag, Berlin-Heidelberg, New York (1975).

[12] J. Seberry, A. L. Whiteman, Some results on weighing matrices, Bull Aus. Math. Soc. 12 (1975), 433-447.

[13] Y. Strassler, The classification of circulant weighing matrices with weight 9. Ph.D. thesis, Bar-Ilan University (1997).