On Circulant Weighing Matrices

K. T. Arasu*

Department of Mathematics and Statistics
Wright State University, Dayton, Ohio–45435, U.S.A.

Jennifer Seberry†

Department of Computer Science
University of Wollongong, NSW 2522, Australia

Dedicated to the memory of Derrick Breach, 1933–1996

Abstract

Algebraic techniques are employed to obtain necessary conditions for the existence of certain circulant weighing matrices. As an application we rule out the existence of many circulant weighing matrices.
We study orders $n = s^2+s+1$, for $10 \leq s \leq 25$. These orders correspond to the number of points in a projective plane of order s.

1 Introduction

A weighing matrix $W(n, k) = W$ of order n with weight k is a square matrix of order n with entries from $\{0, -1, +1\}$ such that

$$WW^t = k \cdot I_n$$

where I_n is the $n \times n$ identity matrix and W^t is the transpose of W.

A *circulant weighing matrix*, written as $W = WC(n, k)$, is a weighing matrix in which each row (except the first row) is obtained by its preceding row by a right cyclic shift. We label the columns of W by a cyclic group G of order n, say generated by g.

Define

$$\begin{aligned} A &= \{ g^i \mid W_{1,i} = 1,\ i = 0, 1, \ldots, n-1\} \\ \text{and} \quad B &= \{ g^i \mid W_{1,i} = -1,\ i = 0, 1, \ldots, n-1\} \end{aligned} \tag{1}$$

*Research partially supported by AFOSR grant F49620-96-1-0328.

†Supported by an ARC grant. The author thanks the Department of Mathematics and Statistics and the Department of Computer Science of Wright State University for their hospitality during the time of this research.

It is easy to see that $|A| + |B| = k$.

It is well known that k must be a perfect square, (see [13], for instance); we write $k = s^2$ for some integer s.

For more on weighing designs, weighing matrices and related topics refer to [8].

It is known [8, 13, 15] that:

Theorem 1 *A $WC(n,k)$ can only exist if (i) $k = s^2$, (ii) $|A| = \frac{s^2+s}{2}$ and $|B| = \frac{s^2-s}{2}$, (iii) $(n-k)^2 - (n-k) \geq n-1$ and iv) if $(n-k)^2 - (n-k) = n-1$ then $A = J - W * W$ is the incidence matrix of a finite projective plane, (here J is the $n \times n$ matrix of all 1's and $*$ denotes the Kronecker product).*

For a multiplicatively written group G, we let **ZG** denote the group ring of G over Z. We will consider only abelian (in fact, only cyclic) groups. A character of the group G, is therefore, a homomorphism from G to the multiplicative group of complex numbers. χ_o denotes the principal character of G which sends each element of G to 1. Extending this to the entire group ring **ZG** yields a map from **ZG** to the field C of complex numbers. For $S \subseteq G$, we let S denote the element $\sum_{x \in S} x$ of **ZG**. For $A = \sum_g a_g g$ and $t \in$ **ZG**, we define $A^{(t)} = \sum_g a_g g^t$.

It is easy to see (see [1] or [16], for details):

Theorem 2 *A $WC = W(n, s^2)$ exists if and only if there exist disjoint subsets A and B of Z_n satisfying*

$$(A - B)(A - B)^{(-1)} = s^2. \tag{2}$$

We exploit (2), in conjunction with a few known results on multipliers in group rings, to obtain necessary conditions on the order n and weight k of a possible circulant $W(n,k)$.

2 Known Results

Theorem 3 (Arasu and Seberry [4]) *Suppose that a $WC(n,k)$ exists. Let p be a prime such that $p^{2t} \mid k$ for some positive integer t. Assume that*

(i) m is a divisor of n. Write $m = m'p^u$, where $(p, m') = 1$;

(ii) there exists an $f \in Z$ such that $p^f \equiv -1 \pmod{m'}$.

Then

(i) $\frac{2n}{m} \geq p^t$ if $p \mid m$;

(ii) $\frac{n}{m} \geq p^t$ if $p \nmid m$.

Lemma 1 *Let q be a prime and x an integer. If there exists an integer f such that*

$$x^f \equiv -1 \pmod{q^i}$$

for some positive integer i, then there exist an integer f' such that

$$x^{f'} \equiv -1 \pmod{q^{i+1}}.$$

Proof. By hypothesis, $x^f = -1 + \ell q^i$ for some integer ℓ. Consider

$$\begin{aligned} x^{fq} &= (-1+\ell q^i)^q \\ &= -1 + \ell^q q^{iq} + \textstyle\sum_{j=1}^{q-1} \binom{q}{j} (-1)^j (\ell q^i)^{q-j}. \end{aligned}$$

Since q is a prime, each of the $(q-1)$ binomial coefficients $\binom{q}{j}$ in the right hand sum is divisible by q and hence

$$\sum_{j=1}^{q-1} (-1)^j \binom{q}{j} (\ell q^i)^{q-j} \equiv 0 \pmod{q^{i+1}}.$$

Also $q^{qi} \equiv 0 \pmod{q^{i+1}}$ since $qi \geq i+1$. Thus $x^{fq} \equiv -1 \pmod{q^{i+1}}$, proving the lemma. $\square$

Lemma 2 *If m' is a prime power, say $m' = (p')^r$ for some prime p', hypothesis (ii) in Theorem 3 is satisfied whenever the Legendre symbol $(\frac{p}{p'}) = -1$.* $\square$

Proof. In view of Lemma 1, it suffices to prove the result for $r = 1$. (An easy induction is applied afterwards.) We first claim that p has even order, say 2α, modulo p'. For otherwise, $p^{2\beta+1} \equiv 1 \pmod{p'}$ for some integer β, hence $(p^{\beta+1})^2 \equiv p \pmod{p'}$ showing that p is a quadratic residue modulo p'; this contradicts the hypothesis $(\frac{p}{p'}) = -1$. Thus the order of p modulo p' is 2α for some positive integer α. Thus $p' \mid (p^{2\alpha} - 1)$. So $p' \mid (p^\alpha - 1)$ or $p' \mid (p^\alpha + 1)$. But p' cannot divide $p^\alpha - 1$, since the order of p modulo p' is 2α. Thus $p' \mid (p^\alpha + 1)$, proving the result for $r = 1$.
$\square$

Theorem 4 ((Seberry) Wallis and Whiteman [15]) *If q is a prime power, then there exists $WC(q^2+q+1, q^2)$.*

Theorem 5 (Eades [6]) *If q is a prime power,* q odd *and i even, then there exists $WC(\frac{q^{i+1}-1}{q-1}, q^i)$.*

Theorem 6 (Arasu, Dillon, Jungnickel and Pott [1]) *If $q = 2^t$ and i even, then there exists $WC(\frac{q^{i+1}-1}{q-1}, q^i)$.*

Theorem 7 (Eades and Hain [7]) *A $WC(n, 4)$ exists if and only if $2 \mid n$ or $7 \mid n$.*

Theorem 8 (Arasu and Seberry [4]) *If there exist $WC(n_1, k)$ and $WC(n_2, k)$ with* $\gcd(n_1, n_2) = 1$ *then there exist*

(i) a $WC(mn_1, k)$ for all positive integers m;

(ii) two inequivalent $WC(n_1n_2, k)$;

(iii) a $WC(n_1n_2, k^2)$.

Theorem 9 (Strassler [18]) *A* $WC(n,9)$ *exists if and only if* $13 \mid n$ *or* $24 \mid n$.

Theorem 10 (Arasu and Seberry [4]) *For a given integer* k *and prime* p, $WC(p,k^2)$ *exists for only a finite number of* p.

Remark 1 It is shown in [4] that a $WC(p,9)$ exists for a prime p if and only if $p=13$.

Theorem 11 is given by Seberry [14] but we give a proof here for completeness. In Theorem 11 we use the following notation. If $G = H \times N$ is a group and $A \subseteq H$ and $B \subseteq N$, then $(A,B) = \{(a,b) \in G; a \in A \text{ and } b \in B\}$. Similarly, if S and T are group ring elements of $\mathbf{ZH}$ and $\mathbf{ZN}$, the element (S,T) is the product of S' and T' in $\mathbf{ZG}$, where S' and T' are the images of S and T under the canonical embedding of $\mathbf{ZH}$ and $\mathbf{ZN}$ into $\mathbf{ZG}$.

Theorem 11 (Circulant Kronecker Product Theorem) *If there exist* $WC(n_1,k_1^2)$ *and* $WC(n_2,k_2^2)$ *with* $\gcd(n_1,n_2)=1$ *then there exists* $WC(n_1n_2,k_1^2k_2^2)$.

Proof. Since there exist $WC(n_i,k_i^2)$ for $i=1,2$, by Theorem 2, there exist subsets A_i, B_i of $\mathbf{Z_{n_i}}$, $A_i \cap B_i = \phi$, $|A_i| = \frac{1}{2}(k_i^2+k_i)$ and $|B_i| = \frac{1}{2}(k_i^2-k_i)$, satisfying $(A_i-B_i)(A_i-B_i)^{(-1)} = k_i^2$ in $\mathbf{Z_{n_i}}$, for $i=1,2$.

Define $X = A_1A_2 + B_1B_2$ and $Y = A_1B_2 + A_2B_1$. Then X, $Y \in \mathbf{ZG}$ and the coefficients of X and Y are 0 and 1.

Consider

$$\begin{aligned}(X-Y)(X-Y)^{(-1)} &= (A_1-B_1)(A_1-B_1)^{(-1)}(A_2-B_2)(A_2-B_2)^{(-1)} \\ &= k_1^2k_2^2.\end{aligned}$$

An easy computation shows that $|X| = \frac{1}{2}(k_1^2k_2^2+k_1k_2)$ and $|Y| = \frac{1}{2}(k_1^2k_2^2-k_1k_2)$. This $X-Y$ defines the first row of $WC(n_1n_2,k_1^2k_2^2)$. □

Corollary 1 *There exist:*
$WC(91,6^2)$, $WC(217,8^2)$, $WC(217,10^2)$, $WC(273,4^2)$, $WC(273,9^2)$, $WC(273,6^2)$, $WC(273,12^2)$, $WC(381,8^2)$, $WC(399,14^2)$, $WC(651,8^2)$, $WC(651,10^2)$, $WC(651,16^2)$ *and* $WC(651,20^2)$.

Proof.

$$\begin{array}{lcl}
WC(7,4) \text{ and } WC(13,9) & \Rightarrow & WC(91,6^2) \\
 & \Rightarrow & WC(273,6^2) \\
WC(7,4) \text{ and } WC(31,16) & \Rightarrow & WC(217,8^2) \\
 & \Rightarrow & WC(651,8^2) \\
WC(21,16) & \Rightarrow & WC(273,4^2) \\
WC(91,81) & \Rightarrow & WC(273,9^2) \\
WC(13,9) \text{ and } WC(21,16) & \Rightarrow & WC(273,12^2) \\
WC(7,4) \text{ and } WC(31,25) & \Rightarrow & WC(217,10^2) \\
 & \Rightarrow & WC(651,10^2) \\
WC(127,64) & \Rightarrow & WC(381,8^2) \\
WC(7,4) \text{ and } WC(57,49) & \Rightarrow & WC(399,14^2) \\
WC(21,16) \text{ and } WC(31,16) & \Rightarrow & WC(651,16^2) \\
WC(21,16) \text{ and } WC(31,25) & \Rightarrow & WC(651,20^2)
\end{array}$$

□

Remark 2 A $WC(13,9)$ exists and hence a $W(509,81) = WC(13,9) \times WC(13,9) \times I_3$ exists. However the existence of the $WC(507,81)$ remains open.

Applications

(I) $WC(n, 2^2)$ exist for n =133, 273, 343, 553 and 651. $WC(n, 2^2)$ do not exist for n =111, 157, 183, 211, 241, 307, 381, 421, 463, 507 or 601.

(II) $WC(n, 3^2)$ do not exist for n = 111, 133, 157, 183, 211, 241, 307, 343, 381, 421, 463, 553, 601 or 651.

(III) A $WC(111, 10^2)$ does not exist as its existence would imply the existence of a projective plane of order 10 which does not exist.

3 Further Results using Multipliers

Notation 1 For each positive integer n, $M(n)$ is defined as follows: $M(1) = 1$, $M(2) = 2 \cdot 7$, $M(3) = 2 \cdot 3 \cdot 11 \cdot 13$, $M(4) = 2 \cdot 3 \cdot 7 \cdot 31$, and recursively, $M(z)$ for $z \geq 5$ is the product of the distinct prime factors of the numbers z, $M(\frac{z^2}{p^{2e}})$, $p-1$, p^2-1, $\cdots p^{u(z)}-1$, where p is any prime dividing m with $p^e \mid\mid m$ and $u(z) = \frac{1}{2}(z^2 - z)$.

Theorem 12 (Multiplier Theorem, Arasu and Xiang [5]) *Let R be an arbitrary group ring element in* **ZG** *that satisfies $RR^{(-1)} = a$ for some integer a, $a \neq 0$, where G is an abelian group of order v and exponent v^*. Let t be a positive integer relatively prime to v, $k_1 \mid a$, $k_1 = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$, $a_1 = (v, k_1)$, $k_2 = \frac{k_1}{a_1}$.*

For each p_i, we define

$$q_i = \begin{cases} p_i & \text{if } p_i \not| \, v^* \\ \ell_i & \text{if } v^* = p_i^r u, \ (p_i, u) = 1, \ r \geq 1, \ \ell_i \text{ is any integer such that} \\ & (\ell_i, p_i) = 1 \text{ and } \ell_i \equiv p_i^f \pmod{u}. \end{cases}$$

Suppose that for each i, there exists an integer f_i such that either

(1) $q_i^{f_i} \equiv t \pmod{v^*}$ *or*

(2) $q_i^{f_i} \equiv -1 \pmod{v^*}$.

If $\left(v, M(\frac{a}{k_2})\right) = 1$, where $M(m)$ is as defined earlier, then t is a multiplier of R.

The following corollary is proved in Arasu, Dillon, Jungnickel and Pott [1]

Corollary 2 (Multiplier Theorem) *Let R be an arbitary group ring element in* **ZG** *that satisfies $RR^{(-1)} = p^n$ where p is a prime with $(p, |G|) = 1$ and where G is an abelian group. Then $R^{(p)} = Rg$ for some $g \in G$.*

Remark 3 Let $R = \sum_g a_g g \in \mathbf{ZG}$. By a result in Arasu and Ray-Chaudhuri [3] if $(\sum_g a_g, |G|) = 1$, we can replace R by a suitable translate of it, if necessary, in Theorem 12 and Corollary 2 and conclude $R^{(t)} = R$, i.e. the multiplier t actually fixes R.

Let t be a multiplier of $R = A - B$. Then by the above remark we obtain $(A - B)^{(t)} = A - B$ or $A^{(t)} - B^{(t)} = A - B$. But A and B have coefficients 0 or 1, hence it follows that $A^{(t)} = A$ and $B^{(t)} = B$. Thus A and B are unions of some of the orbits of G under the action $x \mapsto tx$.

Theorem 13 *A $WC(7,4)$ exists and hence a $W(49,16)$ exists. However no $WC(49,16)$ exists.*

Remark 4 The non-existence of a $WC(49,16)$ follows from Corollary 2 using the multiplier 2.

Most of the above results suffice to settle the cases in the following tables except for the cases $WC(133, 10^2)$ and $WC(133, 5^2)$ which require ad hoc methods which we now prove.

Proposition 1 *There does not exist any $WC(133, 10^2)$.*

Proof. Assume the contrary. Write $G = \mathbf{Z_{133}} = \mathbf{Z_7} \times \mathbf{Z_{19}}$. Then there exists $D \in \mathbf{ZG}$, whose coefficients are $0, \pm 1$, such that

$$DD^{(-1)} = 10^2. \tag{3}$$

Let $\sigma : \mathbf{Z_7} \times \mathbf{Z_{19}} \to \mathbf{Z_{19}}$ be the canonical homomorphism. Extend σ linearly from

$$\mathbf{Z}[\mathbf{Z_7} \times \mathbf{Z_{19}}] \to \mathbf{Z}[\mathbf{Z_{19}}].$$

Apply σ to (3), setting $E = D^\sigma$, to obtain

$$EE^{(-1)} = 10^2 \tag{4}$$

in $\mathbf{Z}[\mathbf{Z_{19}}]$. Note that the coefficients of E lie in $[-7, 7]$. Since $2^{16} \equiv 5 \pmod{19}$, by Theorem 12, 5 is a multiplier of E. We may, without lost of generality, assume that $E^{(5)} = E$. The orbits of $\mathbf{Z_{19}}$ under $x \to 5x$ are of sizes $1^1 9^2$. Hence from (4) (after applying the principal character first to E and then to both sides of (4)), we can find three integers a, b, c such that

$$a + 9b + 9c = 10 \tag{5}$$

$$a^2 + 9b^2 + 9c^2 = 100. \tag{6}$$

These integers a, b, c are merely the coefficients of E. By (5) $a \equiv 1 \pmod 9$. But $a \in [-7, 7]$. Therefore $a = 1$. But then (6) gives

$$b^2 + c^2 = 11,$$

a contradiction, which proves the Proposition. □

Proposition 2 *There does not exist any* $WC(133, 5^2)$.

Proof. Assume to the contrary that there exists a $WC(133, 5^2)$. Write $G = \mathbf{Z}_{133} = \mathbf{Z}_7 \times \mathbf{Z}_{19}$. By Theorem 2, there exist A and $B \subseteq \mathbf{Z}_{133}$, $A \cap B = \phi$, $|A| = 15$ and $|B| = 10$ such that

$$(A - B)(A - B)^{(-1)} = 5^2. \tag{7}$$

By theorem 12, 5 is a multiplier of $A - B$; hence $A^{(5)} = A$ and $B^{(5)} = B$. The orbits of $\mathbf{Z}_7$ under $x \to 5x$ are $\{0\}$ and $\{1,2,3,4,5,6\}$. The orbits of $\mathbf{Z}_{19}$ under $x \to 5x$ are $\{0\}$, C_0 and C_1 where C_0 is the set of all non-zero quadratic residues of $\mathbf{Z}_{19}$ and $C_1 = \mathbf{Z}_{19} - (C_0 \cup \{0\})$.

Then, without loss of generality, we can assume that

$$A = \{1,2,3,4,5,6\} \times \{0\} \cup \{0\} \times C_0, \quad \text{and} \quad B = \{(0,0)\} \cup \{0\} \times C_1.$$

Let χ be any nonprincipal character of G such that $\chi \mid \mathbf{Z}_{19} = \chi_0$. Then $\chi(A) = -1 + 9 = 8$ and $\chi(B) = 1 + 9 = 10$. Therefore $\chi(A - B) = 8 - 10 = -2$. But by (7), $|\chi(A - B)|^2 = 5^2$, a contradiction. Thus there cannot exist $WC(133, 5^2)$. □

4 The Projective Plane Orders

In this section we consider $WC(m^2 + m + 1, k^2)$ for $k \in \{2, \cdots, m\}$.

Case	$n = 10^2 + 10 + 1$					
k	Theorem	p	t	m	n	$p^f \equiv -1 \pmod{m'}$
10		Does not exist as there is no projective plane of order 10				
9	Theorem 3	3	2	111	111	$3^9 \equiv -1 \pmod{37}$
8	Theorem 3	2	3	37	111	$2^{18} \equiv -1 \pmod{37}$
7	7 is a multiplier; orbit sizes $1^3 9^{12}$, $\|A\| = 28$, $\|B\| = 21$; impossible					
6	Theorem 3	3	1	111	111	$3^9 \equiv -1 \pmod{37}$
5	Theorem 3	5	1	37	111	$5^{18} \equiv -1 \pmod{37}$
4	Theorem 3	2	2	37	111	$2^{18} \equiv -1 \pmod{37}$
3	Theorem 9	Does not exist				
2	Theorem 7	Does not exist.				

$WC(10^2 + 10 + 1, k^2)$ does not exist for any k.

Case	$n = 11^2 + 11 + 1$					
k	Theorem	p	t	m	n	$p^f \equiv -1 \pmod{m'}$
11	Theorem 4	Exists				
10	Proposition 1					
9	Theorem 3	3	2	19	133	$3^9 \equiv -1 \pmod{19}$
8	Theorem 3	2	3	19	133	$2^9 \equiv -1 \pmod{19}$
7	Open					
6	Theorem 3	3	1	133	133	$3^9 \equiv -1 \pmod{133}$
5	Proposition 2					
4	2 is a multiplier; orbit sizes $1^1 3^2 18^7$, $\|A\| = 10$, $\|B\| = 6$; impossible					
3	Theorem 9	Does not exist				
2	Theorem 7	Exists.				

$WC(11^2 + 11 + 1, k^2)$ exists only for k = 2,11 and possibly for 7.

Case	$n = 12^2 + 12 + 1$					
k	Theorem	p	t	m	n	$p^f \equiv -1 \pmod{m'}$
12	$3^f \equiv 4 \pmod{n} \Rightarrow 4$ is a multiplier; orbit sizes $1^1 26^6$, $\|A\| = 78$, $\|B\| = 66$; impossible					
11	11 is a multiplier; orbit sizes $1^1 39^4$, $\|A\| = 66$, $\|B\| = 55$; impossible					
10	Theorem 3	2	1	157	157	$2^{26} \equiv -1 \pmod{157}$
9	3 is a multiplier; orbit sizes $1^1 78^2$, $\|A\| = 45$, $\|B\| = 36$; impossible					
8	Theorem 3	2	3	157	157	$2^{26} \equiv -1 \pmod{157}$
7	7 is a multiplier; orbit sizes $1^1 52^3$, $\|A\| = 28$, $\|B\| = 21$; impossible					
6	Theorem 3	2	1	157	157	$2^{26} \equiv -1 \pmod{157}$
5	5 is a multiplier; orbit sizes $1^1 156^1$, $\|A\| = 15$, $\|B\| = 10$; impossible					
4	Theorem 3	2	2	157	157	$2^{26} \equiv -1 \pmod{157}$
3	Theorem 9	Does not exist				
2	Theorem 7	Does not exist.				

$WC(12^2 + 12 + 1, k^2)$ does not exist for any k.

Case	$n = 13^2 + 13 + 1$					
k	Theorem	p	t	m	n	$p^f \equiv -1 \pmod{m'}$
13	Theorem 4	Exists				
12	Theorem 3	2	2	61	183	$2^f \equiv -1 \pmod{61}$
11	Theorem 3	11	1	61	183	$11^f \equiv -1 \pmod{61}$
10	Theorem 3	5	1	61	183	$5^{15} \equiv -1 \pmod{61}$
9	Theorem 3	3	2	183	183	$3^5 \equiv -1 \pmod{61}$
8	Theorem 3	2	3	61	183	$2^f \equiv -1 \pmod{61}$
7	Theorem 3	7	1	61	183	$7^f \equiv -1 \pmod{61}$
6	Theorem 3	3	1	183	183	$3^5 \equiv -1 \pmod{61}$
5	Theorem 3	5	1	61	183	$5^{15} \equiv -1 \pmod{61}$
4	Theorem 3	2	2	61	183	$2^f \equiv -1 \pmod{61}$
3	Theorem 9	Does not exist				
2	Theorem 7	Does not exist.				

$WC(13^2 + 13 + 1, k^2)$ exists only for k = 13.

Case	$n = 14^2 + 14 + 1$					
k	Theorem	p	t	m	n	$p^f \equiv -1 \pmod{m'}$
14		Does not exist as $14 \neq$ sum of two squares				
13	13 is a multiplier; orbit sizes $1^1 35^6$, $\|A\| = 91$, $\|B\| = 78$; impossible					
12	Theorem 3	2	2	211	211	$2^f \equiv -1 \pmod{211}$
11	11 is a multiplier; orbit sizes $1^1 35^6$, $\|A\| = 66$, $\|B\| = 55$; impossible					
10	Theorem 3	2	1	211	211	$2^f \equiv -1 \pmod{211}$
9	Theorem 3	3	2	211	211	$3^f \equiv -1 \pmod{211}$
8	Theorem 3	2	3	211	211	$2^f \equiv -1 \pmod{211}$
7	Theorem 3	7	1	211	211	$7^f \equiv -1 \pmod{211}$
6	Theorem 3	2	1	211	211	$2^f \equiv -1 \pmod{211}$
5	5 is a multiplier; orbit sizes $1^1 35^6$, $\|A\| = 15$, $\|B\| = 10$; impossible					
4	Theorem 3	2	2	211	211	$2^f \equiv -1 \pmod{211}$
3	Theorem 9	Does not exist				
2	Theorem 7	Does not exist.				

$WC(14^2 + 14 + 1, k^2)$ does not exist for any k.

Case	$n = 15^2 + 15 + 1$					
k	Theorem	p	t	m	n	$p^f \equiv -1 \pmod{m'}$
15	$3^{39} \equiv 5 \pmod{241}$, so 5 is a multiplier; orbit sizes $1^1 40^6$, $\|A\| = 120$, $\|B\| = 105$; impossible					
14	Theorem 3	7	1	241	241	$7^f \equiv -1 \pmod{241}$
13	Theorem 3	13	1	241	241	$13^f \equiv -1 \pmod{241}$
12	Theorem 3	2	2	241	241	$2^{12} \equiv -1 \pmod{241}$
11	Theorem 3	11	1	241	241	$11^f \equiv -1 \pmod{241}$
10	Theorem 3	2	1	241	241	$2^{12} \equiv -1 \pmod{241}$
9	Theorem 3	3	2	241	241	$3^{60} \equiv -1 \pmod{241}$
8	Theorem 3	2	3	241	241	$2^{12} \equiv -1 \pmod{241}$
7	Theorem 3	7	1	241	241	$7^f \equiv -1 \pmod{241}$
6	Theorem 3	2	1	241	241	$2^{12} \equiv -1 \pmod{241}$
5	Theorem 3	5	1	241	241	$5^{20} \equiv -1 \pmod{241}$
4	Theorem 3	2	2	241	241	$2^{12} \equiv -1 \pmod{241}$
3	Theorem 9	Does not exist				
2	Theorem 7	Does not exist.				

$WC(15^2 + 15 + 1, k^2)$ does not exist for any k.

Case	$n = 16^2 + 16 + 1$					
k	Theorem	p	t	m	n	$p^f \equiv -1 \pmod{m'}$
16	Theorem 4	Exists.				
15	Open					
14	Theorem 3	7	1	91	273	$7^6 \equiv -1 \pmod{13}$
13	Theorem 3	13	1	91	273	$13^1 \equiv -1 \pmod{7}$
12	Corollary 1	Exists				
11	Open					
10	Open					
9	Corollary 1	Exists				
8	Open					
7	Theorem 3	7	1	91	273	$7^6 \equiv -1 \pmod{13}$
6	Corollary 1	Exists				
5	Open					
4	Corollary 1	Exists				
3	Theorem 9	Exists				
2	Theorem 7	Exists.				

$WC(16^2 + 16 + 1, k^2)$ exists for $k = 2, 3, 4, 6, 9, 12, 16$
and possibly for $k = 5, 8, 10, 11, 15$.

Case	$n = 17^2 + 17 + 1$					
k	Theorem	p	t	m	n	$p^f \equiv -1 \pmod{m'}$
17	Theorem 4	Exists				
16	Theorem 3 and Lemma 2	2	4	307	307	$(\frac{2}{307}) = -1$
15	Theorem 3 and Lemma 2	5	1	307	307	$(\frac{5}{307}) = -1$
14	Theorem 3 and Lemma 2	2	1	307	307	$(\frac{2}{307}) = -1$
13	Theorem 3 and Lemma 2	13	1	307	307	$(\frac{13}{307}) = -1$
12	Theorem 3 and Lemma 2	2	2	307	307	$(\frac{2}{307}) = -1$
11	11 is a multiplier; orbit sizes $1^1 153^2$, $\lvert A\rvert = 66$, $\lvert B\rvert = 55$; impossible					
10	Theorem 3 and Lemma 2	2	1	307	307	$(\frac{2}{307}) = -1$
9	3 is a multiplier; orbit sizes $1^1 34^9$, $\lvert A\rvert = 45$, $\lvert B\rvert = 36$; impossible					
8	Theorem 3 and Lemma 2	2	3	307	307	$(\frac{2}{307}) = -1$
7	7 is a multiplier; orbit sizes $1^1 153^2$, $\lvert A\rvert = 28$, $\lvert B\rvert = 21$; impossible					
6	Theorem 3 and Lemma 2	2	1	307	307	$(\frac{2}{307}) = -1$
5	Theorem 3 and Lemma 2	5	1	307	307	$(\frac{5}{307}) = -1$
4	Theorem 3 and Lemma 2	2	2	307	307	$(\frac{2}{307}) = -1$
3	Theorem 9	Does not exist				
2	Theorem 7	Does not exist.				

$WC(17^2 + 17 + 1, k^2)$ exists only for $k = 17$.

Case	$n = 18^2 + 18 + 1$					
k	Theorem	p	t	m	n	$p^f \equiv -1 \pmod{m'}$
18	Theorem 3, Lemma 1	3	2	343	343	$3^3 \equiv -1 \pmod 7 \Rightarrow 3^f \equiv -1 \pmod{7^3}$
17	Theorem 3, Lemma 1	17	1	343	343	$17 \equiv 3 \pmod 7 \Rightarrow 3^f \equiv -1 \pmod{7^3}$
16	2 is a multiplier; orbit sizes $1^1 3^2 21^2 147^2$, $\|A\| = 136$, $\|B\| = 120$; impossible					
15	Theorem 3, Lemma 1	3	1	343	343	$3^3 \equiv -1 \pmod 7 \Rightarrow 3^f \equiv -1 \pmod{7^3}$
14	Theorem 3	7	1	343	343	$7 \equiv -1 \pmod 1$
13	Theorem 3, Lemma 1	13	1	343	343	$13 \equiv -1 \pmod 7 \Rightarrow 13^f \equiv -1 \pmod{7^3}$
12	Theorem 3, Lemma 1	3	1	343	343	$3^3 \equiv -1 \pmod 7 \Rightarrow 3^f \equiv -1 \pmod{7^3}$
11	11 is a multiplier; orbit sizes $1^1 3^2 21^2 147^2$, $\|A\| = 66$, $\|B\| = 55$; impossible					
10	Theorem 3, Lemma 1	5	1	343	343	$5^3 \equiv -1 \pmod 7 \Rightarrow 5^f \equiv -1 \pmod{7^3}$
9	Theorem 3, Lemma 1	3	2	343	343	$3^3 \equiv -1 \pmod 7 \Rightarrow 3^f \equiv -1 \pmod{7^3}$
8	2 is a multiplier; orbit sizes $1^1 3^2 21^2 147^2$, $\|A\| = 36$, $\|B\| = 28$; impossible					
7	Theorem 3	7	1	343	343	$7 \equiv -1 \pmod 1$
6	Theorem 3, Lemma 1	3	1	343	343	$3^3 \equiv -1 \pmod 7 \Rightarrow 3^f \equiv -1 \pmod{7^3}$
5	Theorem 3, Lemma 1	5	1	343	343	$5^3 \equiv -1 \pmod 7 \Rightarrow 5^f \equiv -1 \pmod{7^3}$
4	2 is a multiplier; orbit sizes $1^1 3^2 21^2 147^2$, $\|A\| = 10$, $\|B\| = 6$; impossible					
3	Theorem 9	Does not exist				
2	Theorem 7	Exists.				

$WC(18^2 + 18 + 1, k^2)$ exists only for $k = 2$.

Case	$n = 19^2 + 19 + 1$					
k	Theorem	p	t	m	n	$p^f \equiv -1 \pmod{m'}$
19	Theorem 4	Exists				
18	Theorem 3	3	2	381	381	$3^{63} \equiv -1 \pmod{127}$
17	17 is a multiplier; orbit sizes $1^1 2^1 63^2 126^2$, $\|A\| = 153$, $\|B\| = 136$; impossible					
16	2 is a multiplier; orbit sizes $1^1 2^1 7^{18} 14^{18}$, $\|A\| = 136$, $\|B\| = 120$; impossible					
15	Theorem 3	3	1	381	381	$3^{63} \equiv -1 \pmod{127}$
14	Theorem 3 and Lemma 2	7	1	127	381	$(\frac{7}{127}) = -1$
13	13 is a multiplier; orbit sizes $1^3 63^6$, $\|A\| = 91$, $\|B\| = 78$; impossible					
12	Theorem 3	3	1	381	381	$3^{63} \equiv -1 \pmod{127}$
11	11 is a multiplier; orbit sizes $1^1 2^1 63^2 126^2$, $\|A\| = 66$, $\|B\| = 55$; impossible					
10	Theorem 3 and Lemma 2	5	1	127	381	$(\frac{5}{127}) = -1$
9	Theorem 3	3	2	381	381	$3^{63} \equiv -1 \pmod{127}$
8	Corollary 1	Exists				
7	Theorem 3 and Lemma 2	7	1	127	381	$(\frac{7}{127}) = -1$
6	Theorem 3	3	1	381	381	$3^{63} \equiv -1 \pmod{127}$
5	Theorem 3 and Lemma 2	5	1	127	381	$(\frac{5}{127}) = -1$
4	2 is a multiplier; orbit sizes $1^1 2^1 7^{18} 14^{18}$, $\|A\| = 10$, $\|B\| = 6$; impossible					
3	Theorem 9	Does not exist				
2	Theorem 7	Does not exist.				

$WC(19^2 + 19 + 1, k^2)$ exists only for $k = 8$ and 19.

Case	$n = 20^2 + 20 + 1$					
k	Theorem	p	t	m	n	$p^f \equiv -1 \pmod{m'}$
20	Theorem 3 and Lemma 2	2	2	421	421	$(\frac{2}{421}) = -1$
19	Theorem 3 and Lemma 2	19	1	421	421	$(\frac{19}{421}) = -1$
18	Theorem 3 and Lemma 2	2	1	421	421	$(\frac{2}{421}) = -1$
17	Theorem 3	17	1	421	421	$17^{105} \equiv -1 \pmod{421}$
16	Theorem 3 and Lemma 2	2	4	421	421	$(\frac{2}{421}) = -1$
15	Theorem 3	5	1	421	421	$5^{105} \equiv -1 \pmod{421}$
14	Theorem 3 and Lemma 2	2	1	421	421	$(\frac{2}{421}) = -1$
13	Theorem 3 and Lemma 2	13	1	421	421	$(\frac{13}{421}) = -1$
12	Theorem 3 and Lemma 2	2	2	421	421	$(\frac{2}{421}) = -1$
11	11 is a multiplier; orbit sizes $1^1 105^4$, $\lvert A\rvert = 66$, $\lvert B\rvert = 55$; impossible					
10	Theorem 3 and Lemma 2	2	1	421	421	$(\frac{2}{421}) = -1$
9	3 is a multiplier; orbit sizes $1^1 105^4$, $\lvert A\rvert = 45$, $\lvert B\rvert = 36$; impossible					
8	Theorem 3 and Lemma 2	2	1	421	421	$(\frac{2}{421}) = -1$
7	7 is a multiplier; orbit sizes $1^1 70^6$, $\lvert A\rvert = 28$, $\lvert B\rvert = 21$; impossible					
6	Theorem 3 and Lemma 2	2	1	421	421	$(\frac{2}{421}) = -1$
5	Theorem 3 and Lemma 2	5	1	421	421	$5^{105} \equiv -1 \pmod{421}$
4	Theorem 3 and Lemma 2	2	2	421	421	$(\frac{2}{421}) = -1$
3	Theorem 9	Does not exist				
2	Theorem 7	Does not exist.				

$WC(20^2 + 20 + 1, k^2)$ does not exist for any k.

Case	$n = 21^2 + 21 + 1$					
k	Theorem	p	t	m	n	$p^f \equiv -1 \pmod{m'}$
21	Theorem 3, Lemma 2	3	1	463	463	3 is a primitive root mod 463, so $(\frac{3}{463}) = -1$
20	Theorem 3, Lemma 2	5	1	463	463	$(\frac{5}{463}) = -1$
19	Theorem 3, Lemma 2	19	1	463	463	$(\frac{19}{463}) = -1$
18	Theorem 3, Lemma 2	3	2	463	463	3 is a primitive root mod 463, so $(\frac{3}{463}) = -1$
17	17 is a multiplier; orbit sizes $1^1 231^2$, $\lvert A\rvert = 153$, $\lvert B\rvert = 136$; impossible					
16	2 is a multiplier; orbit sizes $1^1 231^2$, $\lvert A\rvert = 136$, $\lvert B\rvert = 120$; impossible					
15	Theorem 3, Lemma 2	3	1	463	463	3 is a primitive root mod 463, so $(\frac{3}{463}) = -1$
14	Theorem 3, Lemma 2	7	1	463	463	$(\frac{7}{463}) = -1$
13	Theorem 3, Lemma 2	13	1	463	463	$(\frac{13}{463}) = -1$
12	Theorem 3, Lemma 2	3	1	463	463	3 is a primitive root mod 463, so $(\frac{3}{463}) = -1$
11	Theorem 3, Lemma 2	11	1	463	463	$(\frac{11}{463}) = -1$
10	Theorem 3, Lemma 2	5	1	463	463	$(\frac{5}{463}) = -1$
9	Theorem 3, Lemma 2	3	2	463	463	3 is a primitive root mod 463, so $(\frac{3}{463}) = -1$
8	2 is a multiplier; orbit sizes $1^1 231^2$, $\lvert A\rvert = 36$, $\lvert B\rvert = 28$; impossible					
7	Theorem 3, Lemma 2	7	1	463	463	$(\frac{7}{463}) = -1$
6	Theorem 3, Lemma 2	3	1	463	463	3 is a primitive root mod 463, so $(\frac{3}{463}) = -1$
5	Theorem 3, Lemma 2	5	1	463	463	$(\frac{5}{463}) = -1$
4	2 is a multiplier; orbit sizes $1^1 231^2$, $\lvert A\rvert = 10$, $\lvert B\rvert = 6$; impossible					
3	Theorem 9	Does not exist				
2	Theorem 7	Does not exist.				

$WC(21^2 + 21 + 1, k^2)$ does not exist for any k.

Case	$n = 22^2 + 22 + 1$					
k	Theorem	p	t	m	n	$p^f \equiv -1 \pmod{m'}$
22		Does not exist as $22 \neq$ sum of two squares				
21	Theorem 3 and Lemma 2	7	1	169	507	$(\frac{7}{13}) = -1$
20	Theorem 3 and Lemma 2	2	2	169	507	$(\frac{2}{13}) = -1$
19	Theorem 3 and Lemma 2	19	1	169	507	$(\frac{19}{13}) = -1$
18	Open					
17	17 is a multiplier; orbit sizes $1^1 2^1 6^6 78^6$, $\|A\| = 153$, $\|B\| = 136$; impossible					
16	Theorem 3 and Lemma 2	2	4	169	507	$(\frac{2}{13}) = -1$
15	Theorem 3 and Lemma 2	5	1	169	507	$(\frac{5}{13}) = -1$
14	Theorem 3 and Lemma 2	7	1	169	507	$(\frac{7}{13}) = -1$
13	Theorem 3	13	1	169	507	$13^1 \equiv -1 \pmod{1}$
12	Theorem 3 and Lemma 2	2	2	169	507	$(\frac{2}{13}) = -1$
11	Theorem 3 and Lemma 2	11	1	169	507	$(\frac{11}{13}) = -1$
10	Theorem 3 and Lemma 2	5	1	169	507	$(\frac{5}{13}) = -1$
9	Open					
8	Theorem 3 and Lemma 2	2	3	169	507	$(\frac{2}{13}) = -1$
7	Theorem 3 and Lemma 2	7	1	169	507	$(\frac{7}{13}) = -1$
6	Open					
5	Theorem 3 and Lemma 2	5	1	169	507	$(\frac{5}{13}) = -1$
4	Theorem 3 and Lemma 2	2	2	169	507	$(\frac{2}{13}) = -1$
3	Theorem 9	Exists				
2	Theorem 7	Does not exist.				

$WC(22^2 + 22 + 1, k^2)$ exists for $k = 3$ and possibly for $k = 6$, 9 and 18.

Case	$n = 23^2 + 23 + 1$					
k	Theorem	p	t	m	n	$p^f \equiv -1 \pmod{m'}$
23	Theorem 4	Exists				
22	$11^7 \equiv 4 \pmod{553} \Rightarrow 4$ is a multiplier; orbit sizes $1^1 3^2 39^{14}$, $\lvert A\rvert = 253$, $\lvert B\rvert = 231$; impossible					
21	Theorem 3 and Lemma 2	7	1	553	553	$(\frac{7}{79}) = -1$
20	$5^f \equiv 8 \pmod{553} \Rightarrow 8$ is a multiplier; orbit sizes $1^7 13^{42}$, $\lvert A\rvert = 210$, $\lvert B\rvert = 190$; impossible					
19	19 is a multiplier; orbit sizes $1^1 6^1 39^2 78^6$, $\lvert A\rvert = 190$, $\lvert B\rvert = 171$; impossible					
18	$3^f \equiv 8 \pmod{553} \Rightarrow 8$ is a multiplier; orbit sizes $1^7 13^{42}$, $\lvert A\rvert = 171$, $\lvert B\rvert = 153$; impossible					
17	17 is a multiplier; orbit sizes $1^1 6^1 26^3 78^6$, $\lvert A\rvert = 153$, $\lvert B\rvert = 136$; impossible					
16	2 is a multiplier; orbit sizes $1^1 3^2 39^{14}$, $\lvert A\rvert = 136$, $\lvert B\rvert = 120$; impossible					
15	$3^f \equiv 25 \pmod{553} \Rightarrow 25$ is a multiplier; orbit sizes $1^1 3^2 39^{14}$, $\lvert A\rvert = 120$, $\lvert B\rvert = 105$; impossible					
14	Theorem 3 and Lemma 2	7	1	553	553	$(\frac{7}{79}) = -1$
13	13 is a multiplier; orbit sizes $1^1 2^3 39^2 78^6$, $\lvert A\rvert = 91$, $\lvert B\rvert = 78$; impossible					
12	Open					
11	11 is a multiplier; orbit sizes $1^1 3^2 39^{14}$, $\lvert A\rvert = 66$, $\lvert B\rvert = 55$; impossible					
10	$5^f \equiv 8 \pmod{553} \Rightarrow 8$ is a multiplier; orbit sizes $1^7 13^{42}$, $\lvert A\rvert = 55$, $\lvert B\rvert = 45$; impossible					
9	3 is a multiplier; orbit sizes $1^1 6^1 78^7$, $\lvert A\rvert = 45$, $\lvert B\rvert = 36$; impossible					
8	2 is a multiplier; orbit sizes $1^1 3^2 39^{14}$, $\lvert A\rvert = 36$, $\lvert B\rvert = 28$; impossible					
7	Theorem 3 and Lemma 2	7	1	553	553	$(\frac{7}{79}) = -1$
6	$3^f \equiv 8 \pmod{553} \Rightarrow 8$ is a multiplier; orbit sizes $1^7 13^{42}$, $\lvert A\rvert = 21$, $\lvert B\rvert = 15$; impossible					
5	5 is a multiplier; orbit sizes $1^1 6^1 39^2 78^6$, $\lvert A\rvert = 15$, $\lvert B\rvert = 10$; impossible					
4	2 is a multiplier; orbit sizes $1^1 3^2 39^{14}$, $\lvert A\rvert = 10$, $\lvert B\rvert = 6$; impossible					
3	Theorem 9	Does not exist				
2	Theorem 7	Exists.				

$WC(23^2 + 23 + 1, k^2)$ exists only for $k = 2$, 23 and possibly $k = 12$.

Case	$n = 24^2 + 24 + 1$					
k	Theorem	p	t	m	n	$p^f \equiv -1 \pmod{m'}$
24	Open					
23	Theorem 3	23	1	601	601	$23^{150} \equiv -1 \pmod{601}$
22	Theorem 3 and Lemma 2	11	1	601	601	$(\frac{11}{601}) = -1$
21	Theorem 3 and Lemma 2	7	1	601	601	$(\frac{7}{601}) = -1$
20	Theorem 3	5	1	601	601	$5^6 \equiv -1 \pmod{601}$
19	Theorem 3 and Lemma 2	1	1	601	601	$(\frac{19}{601}) = -1$
18	$2^{16} \equiv 27 \pmod{601}$; 27 is a multiplier; orbit sizes $1^1 25^{24}$, $\|A\| = 171$, $\|B\| = 153$; impossible					
17	Theorem 3 and Lemma 2	17	1	601	601	$(\frac{17}{601}) = -1$
16	2 is a multiplier; orbit sizes $1^1 25^{24}$, $\|A\| = 136$, $\|B\| = 120$; impossible					
15	Theorem 3	5	1	601	601	$5^6 \equiv -1 \pmod{601}$
14	Theorem 3 and Lemma 2	7	1	601	601	$(\frac{7}{601}) = -1$
13	Theorem 3 and Lemma 2	13	1	601	601	$13^{10} \equiv -1 \pmod{601}$
12	$2^{16} \equiv 27 \pmod{601}$; 27 is a multiplier; orbit sizes $1^1 25^{24}$, $\|A\| = 78$, $\|B\| = 66$; impossible					
11	Theorem 3 and Lemma 2	11	1	601	601	$(\frac{11}{601}) = -1$
10	Theorem 3	5	1	601	601	$5^6 \equiv -1 \pmod{601}$
9	3 is a multiplier; orbit sizes $1^1 75^8$, $\|A\| = 45$, $\|B\| = 36$; impossible					
8	2 is a multiplier; orbit sizes $1^1 25^{24}$, $\|A\| = 36$, $\|B\| = 28$; impossible					
7	Theorem 3 and Lemma 2	7	1	601	601	$(\frac{7}{601}) = -1$
6	$2^{16} \equiv 27 \pmod{601}$; 27 is a multiplier; orbit sizes $1^1 25^{24}$, $\|A\| = 21$, $\|B\| = 15$; impossible					
5	Theorem 3	5	1	601	601	$5^6 \equiv -1 \pmod{601}$
4	2 is a multiplier; orbit sizes $1^1 25^{24}$, $\|A\| = 10$, $\|B\| = 6$; impossible					
3	Theorem 9	Does not exist				
2	Theorem 7	Does not exist.				

$WC(24^2 + 24 + 1, k^2)$ exists only possibly for $k = 24$.

Case	$n = 25^2 + 25 + 1$					
k	Theorem	p	t	m	n	$p^f \equiv -1 \pmod{m'}$
25	Theorem 4	Exists				
24	Theorem 3	3	1	651	651	$3^{15} \equiv -1 \pmod{217}$
23	Theorem 3	23	1	93	651	$23^5 \equiv -1 \pmod{93}$
22	Theorem 3	11	1	93	651	$11^{15} \equiv -1 \pmod{93}$
21	Theorem 3	3	1	651	651	$3^{15} \equiv -1 \pmod{217}$
20	Corollary 1	Exists				
19	19 is a multiplier; orbit sizes $1^3 6^3 15^6 30^{18}$, $\|A\| = 190$, $\|B\| = 171$; impossible					
18	Theorem 3	3	2	651	651	$3^{15} \equiv -1 \pmod{217}$
17	Theorem 3	17	1	651	651	$17^{15} \equiv -1 \pmod{651}$
16	Corollary 1	Exists				
15	Theorem 3	3	1	651	651	$3^{15} \equiv -1 \pmod{217}$
14	Open					
13	Theorem 3	13	1	217	651	$13^{15} \equiv -1 \pmod{217}$
12	Theorem 3	3	1	651	651	$3^{15} \equiv -1 \pmod{217}$
11	Theorem 3	11	1	93	651	$11^{15} \equiv -1 \pmod{93}$
10	Corollary 1	Exists				
9	Theorem 3	3	2	651	651	$3^{15} \equiv -1 \pmod{217}$
8	Corollary 1	Exists				
7	Open					
6	Theorem 3	3	1	651	651	$3^{15} \equiv -1 \pmod{217}$
5	Corollary 1	Exists				
4	Corollary 1	Exists				
3	Theorem 9	Does not exist				
2	Theorem 7	Exists.				

$WC(25^2 + 25 + 1, k^2)$ exists for k = 2, 4, 5, 8, 10, 16, 20, 25 and possibly for k = 7, 14.

References

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

[2] K. T. Arasu, D. Jungnickel, S. L. Ma, and A. Pott, Relative difference sets with $n = 2$, *Discr. Math.*, 147, (1995), 1-17.

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

[4] K. T. Arasu and Jennifer Seberry, Circulant weighing designs, *Journal of Combinatorial Designs,* 4 (1996), 439-447.

[5] K. T. Arasu and Qing Xiang, Multiplier theorems, *J. Combinatorial Designs,* 3, (1995), 257-268.

[6] P. Eades, *On the Existence of Orthogonal Designs*, Ph.D. Thesis, Australian National University, Canberra, (1977).

[7] P. Eades and R. M. Hain, On circulant weighing matrices, *Ars. Combinatoria* 2, (1976), 265–284.

[8] A. V. Geramita and J. Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Decker, New York-Basel, (1979).

[9] R. M. Hain, *Circulant Weighing Matrices*, Master of Science Thesis, Australian National University, Canberra, (1977).

[10] S. L. Ma, *Polynomial Addition Sets*, Ph.D. Thesis, University of Hong Kong, (1985).

[11] H. B. Mann, *Addition Theorems*, Wiley, New York, (1965).

[12] R. L. McFarland, *On Multipliers of Abelian Difference Sets*, Ph.D. Thesis, Ohio State University, (1970).

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

[14] Jennifer Seberry, Asymptotic existence of some orthogonal designs, *J. Combinatorial Theory, Ser A*, (submitted).

[15] J. Seberry Wallis and A. L. Whiteman, Some results on weighing matrices, *Bull. Austral. Math. Sec.* 12, (1975), 433–447.

[16] Y. Strassler, "Circulant weighing matrices of prime order and weight 9 having a multiplier", talk presented at *Hadamard Centenary Conference*, Wollongong, Australia, December, 1993.

[17] Y. Strassler, "New circulant weighing matrices of prime order in $CW(31,16)$, $CW(71,25)$, $CW(127,64)$", paper presented at the *R. C. Bose Memorial Conference on Statistical Design and Related Combinatorics,* Colorado State University, 7-11 June, 1995.

[18] Y. Strassler, personal communication to K.T. Arasu and Jennifer Seberry of results contained in his PhD Thesis which has yet to be published.

[19] R. J. Turyn, Character sums and difference sets, *Pac. J. Math.* 15, (1965), 319–346.

(Received 13/12/1996)