Journal of Algebraic Combinatorics **14** (2001), 91–101
© 2001 Kluwer Academic Publishers. Manufactured in The Netherlands.

Some New Results on Circulant Weighing Matrices

K. T. ARASU* karasu@math.wright.edu
Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435, USA

SIU LUN MA† matmasl@nus.edu.sg
Department of Mathematics, National University of Singapore, Kent Ridge, Singapore 119260, Republic of Singapore

Received May 28, 1999; Revised April 2, 2001

Abstract. We obtain a few structural theorems for circulant weighing matrices whose weight is the square of a prime number. Our results provide new schemes to search for these objects. We also establish the existence status of several previously open cases of circulant weighing matrices. More specifically we show their nonexistence for the parameter pairs (n, k) (here n is the order of the matrix and k its weight) = (147, 49), (125, 25), (200, 25), (55, 25), (95, 25), (133, 49), (195, 25), $(11w, 121)$ for $w < 62$.

Keywords: weighing matrices, circulant, group rings, characters

1. Introduction

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

$$WW^t = kI_n$$

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

A circulant weighing matrix, denoted by $CW(n, k)$, is a weighing matrix $W(n, k)$ in which each row (except the first one) is obtained from its preceding row by a right cyclic shift. We refer the reader to Geramita and Seberry [8] for more on weighing matrices and related topics and to Arasu and Dillon [2] for circulant weighing matrices and a more general configuration called perfect ternary array. The paper by Arasu and Dillon had quoted results from the old version of this paper, but unfortunately we had found a mistake in the proof of some results, [2, Theorems 4.6 and 4.7]. The corrected version of the results are stated in this paper as Theorem 3.8 and Proposition 3.9.

We label the columns of W by a cyclic group G of order n, generated by g (say). Define

$$P = \{g^i \mid W_{1,i} = 1, \quad i = 0, 1, \ldots, n-1\}$$

*Research supported by NSA Grant MDA 904-01-1-0041 and NSF Grant CCR-9814106.

†This research was done when the author visited Wright State University and Ohio State University.

and

$$N = \{g^i \mid W_{1,i} - 1, \quad i = 0, 1, \dots, n-1\}.$$

Clearly $|P| + |N| = k$. It is well known that k must be a square (see Mullin [9] for instance), say $k = s^2$ for some integer s.

The following is easy to show (see Mullin [9], for instance).

Proposition 1.1 *With notations above, for a $CW(n, s^2)$,*

$$\{|P|, |N|\} = \left\{\frac{s^2 + s}{2}, \frac{s^2 - s}{2}\right\}$$

The following composition theorem is well known (see Arasu and Seberry [6], for instance).

Theorem 1.2 *Suppose that there exist $CW(n_1, k)$ and $CW(n_2, l)$ with* $\gcd(n_1, n_2) = 1$. *Then there exists*

(i) *a $CW(mn_1, k)$, for all positive integers m, and*
(ii) *a $CW(n_1 n_2, kl)$.*

The orders n for circulant weighing matrices have been determined completely for weights 4 and 9.

Theorem 1.3 (Eades and Hain [7]) *A $CW(n, 4)$ exists if and only if* $2 \mid n$ *or* $7 \mid n$.

Theorem 1.4 (Strassler [11] and Arasu et al. [5]) *A $CW(n, 9)$ exists if and only if* $13 \mid n$ *or* $24 \mid n$.

Recently, Arasu [1] has proved a reduction theorem for circulant weighing matrices based on the “self-conjugacy” assumption. In this paper we prove some reduction theorems for $CW(n, p^{2r})$ and $CW(n, p^2)$ without the ”self-conjugacy” assumption. Also we prove a few structural theorems for $CW(n, p^2)$ where p is a prime. Our results provide some new strategies to construct new circulant weighing matrices. As consequences of our theorems we establish the nonexistence of several previously open $CW(n, k)$ for a number of parameter pairs (n, k).

2. Algebraic preliminaries

For a multiplicatively written group G we let $\mathbb{Z}[G]$ denote the group ring of G over $\mathbb{Z}$. We will consider only abelian (in fact, only cyclic) groups. A character χ of G is a homomorphism from G to the multiplicative group of complex numbers. We extend this linearly to $\mathbb{Z}[G]$ obtaining a ring homomorphism from $\mathbb{Z}[G]$ to $\mathbb{C}$.

For $S \subset G$ we also let S denote the element $\sum_{g\in S} g$ of $\mathbb{Z}[G]$. For $A = \sum_{g\in G} a_g g \in \mathbb{Z}[G]$ and $t \in \mathbb{Z}$, we define $A^{(t)} = \sum_{g\in G} a_g g^t$. Also, for a subgroup H of G, we say that $A \in \mathbb{Z}[H]$ if the support of A is contained in H.

If $W = W(n,k)$ is a circulant weighing matrix and P and N are as in Section 1, then it is easy to see that in $\mathbb{Z}[G]$,

$$(P-N)(P-N)^{(-1)} = k.$$

We close this section by quoting a few results from Arasu and Ma ([3] and [4]). In the following, we use ζ_v to denote the complex vth root of unity $e^{2\pi\sqrt{-1}/v}$.

Proposition 2.1 *Let $G = \langle\alpha\rangle \times H$ be an abelian group of exponent $v = uw$ where $o(\alpha) = u$, $\exp(H) = w$ and $(u,w) = 1$. Suppose $A \in \mathbb{Z}[G]$ and $\sigma \in \mathrm{Gal}\,(\mathbb{Q}(\zeta_v)/\mathbb{Q})$ such that*

(i) *$\chi(A)\overline{\chi(A)} = n$ for all character χ of G such that $\chi(\alpha) = \zeta_u$, where n is an integer relatively prime to w; and*

(ii) *σ fixes every prime ideal divisor of $n\mathbb{Z}[\zeta_v]$.*

If $\sigma(\zeta_v) = \zeta_v^t$ then

$$A^{(t)} = \pm\beta A + \sum_{i=1}^{r} \langle\alpha^{u/p_i}\rangle X_i$$

where $\beta \in G$, $X_1, X_2, \ldots, X_r \in \mathbb{Z}[G]$ and $p_1, p_2, \ldots, p_r$ are all prime divisors of u.

Proposition 2.2 *Let $G = \langle\alpha\rangle \times H$ be an abelian group of exponent $v = p^s w$ where p is an odd prime, $(p(p-1), w) = 1$, $o(\alpha) = p^s$ and $\exp(H) = w$. Suppose $A \in \mathbb{Z}[G]$ satisfies $\chi(A)\overline{\chi(A)} = p^{2r}$ for all characters χ of G which are nonprincipal on $\langle\alpha^{p^{s-1}}\rangle$. Then $A = \alpha^c X_0 + \langle\alpha^{p^{s-1}}\rangle X_1$ where $X_1 \in \mathbb{Z}[G]$, $X_0 \in \mathbb{Z}[H]$ and $X_0 X_0^{(-1)} = p^{2r}$.*

Proposition 2.3 *Let $G = \langle\alpha\rangle \times H$ be an abelian group of exponent $v = p^s w$ where p is an odd prime, $o(\alpha) = p^s$, $\exp(H) = w$, $s \geq 2$ and $p \nmid w$. Let t be an integer such that $t \equiv 1 + p^{s-1} \bmod p^s$ and $t \equiv 1 \bmod w$. If $A \in \mathbb{Z}[G]$ satisfies*

(i) *$\chi(A)\overline{\chi(A)} = n$ for all characters χ of G which are nonprincipal on $P = \langle\alpha^{p^{s-1}}\rangle$, where n is relatively prime to w; and*

(ii) *$\sigma : \zeta_v \mapsto \zeta_v^t$ fixes every prime ideal divisor of $n\mathbb{Z}\,[\zeta_v]$,*

then

$$A = \alpha^c(X_0 + PX_1)$$

where $X_0 \in \mathbb{Z}[\langle\alpha^p\rangle \times H]$ and the support of X_1 is contained in $G \backslash (\langle\alpha^p\rangle \times H)$, and hence

$$(\alpha^{-c}A)^{(t)} = \alpha^{-c}A.$$

3. Main results

Theorem 3.1 *Let $G = \langle\alpha\rangle \times H$ where $o(\alpha) = p^s$, $\exp(H) = w$, $(p(p-1), w) = 1$ and p is a prime greater than* 3. *If $A \in \mathbb{Z}[G]$ satisfies $AA^{(-1)} = p^{2r}$ and the coefficients of A are* $0, \pm 1$, *then there exists an integer b such that $\alpha^b A \in \mathbb{Z}[H]$.*

Proof: By Proposition 2.2, there exists an integer b such that $\alpha^b A = X_0 + \langle\alpha^{p^{s-1}}\rangle X_1$ where $X_0 \in \mathbb{Z}[H]$ and $X_1 \in \mathbb{Z}[G]$. Since A has $0, \pm 1$ coefficients, we can rewrite $\alpha^b A$ as

$$\alpha^b A = B + \big(\langle\alpha^{p^{s-1}}\rangle - 1\big)C + \big(\langle\alpha^{p^{s-1}}\rangle - 2\big)D + \langle\alpha^{p^{s-1}}\rangle E$$

where the elements of the supports of B, C, D, E are in different cosets of $\langle\alpha^{p^{s-1}}\rangle$. The coefficient of $\alpha^{p^{s-1}}$ in $AA^{(-1)}$ is equal to

$$(p-2)\,|\text{support }(C)| + (p-4)\,|\text{support }(D)| + p\,|\text{support }(E)|$$

which can never be zero unless $C = D = E = 0$. □

Application of Theorem 3.1 $CW(n, k)$ does not exist for the pairs $(n, k) = (55, 25), (95, 25), (133, 49), (195, 25)$.

Lemma 3.2 *Let $G = \langle\alpha\rangle \times H$ be an abelian group of exponent $v = p^s w$ where p is an odd prime, $o(\alpha) = p^s$, $\exp(H) = w$ and $(p, w) = 1$. Suppose $A \in \mathbb{Z}[G]$ such that $\chi(A)\overline{\chi(A)} = p^{2r}$ for all characters χ of G such that $\chi(\alpha) = \zeta_{p^s}$. Let t be a primitive root modulo p^s and $t \equiv 1$ mod w. Then there exists an integer b such that*

$$(\alpha^b A)^{(t)} = \beta\alpha^b A + \langle\alpha^{p^{s-1}}\rangle X$$

where $\beta \in H$, and $o(\beta) \mid (p-1, w)$ and $X \in \mathbb{Z}[G]$.

Proof: Let $\rho : \mathbb{Z}[G] \to \mathbb{Z}[\zeta_{p^s}][H]$ be a ring homomorphism such that $\rho(\alpha) = \zeta_{p^s}$ and $\rho(h) = h$ for all $h \in H$. Let $\sigma \in \text{Gal}\,(\mathbb{Q}(\zeta_{p^s w})/\mathbb{Q})$ such that $\sigma(\zeta_{p^s w}) = \zeta_{p^s w}^t$. Note that σ fixes every prime ideal divisor of $p\mathbb{Z}[\zeta_{p^s w}]$ (see [10, Result 1.2.7]). By Proposition 2.1 we have

$$\rho(A)^\sigma = \pm\beta\zeta_{p^s}^a \rho(A) \tag{1}$$

for some $\beta \in H$. Since $\rho(A) = \rho(A)^{\sigma^{p^{s-1}(p-1)}} = \beta^{p^{s-1}(p-1)}\rho(A)$, we have $o(\beta) \mid (p-1, w)$. Let χ_0 be the principal character of H. Then $\chi_0(\rho(A)) = \varepsilon\zeta_{p^s}^c p$ where $\varepsilon = \pm 1$. Applying χ_0 to (1), we obtain $\zeta_p^{tc} = \pm\zeta_p^{a+c}$. Thus (1) can be rewritten as

$$\big[\zeta_{p^s}^b \rho(A)\big]^\sigma = \beta\zeta_{p^s}^b \rho(A)$$

where $b = -c$. This implies that $(\alpha^b A)^{(t)} = \beta\alpha^b A + \langle\alpha^{p^{s-1}}\rangle\, X$ for some $X \in \mathbb{Z}[G]$. □

Lemma 3.3 *Let $G = \langle\alpha\rangle \times H$ where $o(\alpha) = p$, $\exp(H) = w$, $(p, w) = 1$ and p is an odd prime. Let t be a primitive root modulo p and $t \equiv 1 \bmod w$. Suppose $A \in \mathbb{Z}[G]$ such that $A^{(t)} = \beta A$ for some $\beta \in H$. Let $m = o(\beta)$, $\{h_1, h_2, \ldots, h_v\}$ be a complete set of coset representatives of $\langle\beta\rangle$ in H and $Q_j = \{\alpha^{t^i}\beta^{j-i} \mid i = 0, 1, \ldots, p-2\}$ for $j = 0, 1, \ldots, m-1$. Then*

$$A = \langle\beta\rangle \sum_{k=1}^{v} a_k h_k + \sum_{j=0}^{m-1} \sum_{k=1}^{v} b_{jk} Q_j h_k$$

where a_k and b_{jk} are integers.

Proof: In A, the coefficient of $\beta^j h_k$ is the same as $\beta^{j+1}h_k$; and the coefficient of $\alpha^{t^i}\beta^j h_k$ is the same as $\alpha^{t^{i-1}}\beta^{j+1}h_k$ for all i, j, k. □

Lemma 3.4 *Let $G = \langle\alpha\rangle \times H$ where $o(\alpha) = p$, $\exp(H) = w$, $(p, w) = 1$ and p is an odd prime. Then there does not exist any element $A \in \mathbb{Z}[G]$ such that $AA^{(-1)} = p^2 - p\langle\alpha\rangle$ and the coefficients of A are $0, \pm 1$.*

Proof: Assume there exits $A \in \mathbb{Z}[G]$ such that $AA^{(-1)} = p^2 - p\langle\alpha\rangle$ and the coefficients of A are $0, \pm 1$. Let t be a primitive root modulo p and $t \equiv 1 \bmod w$. By Lemma 3.2, there exists an integer b such that

$$(\alpha^b A)^{(t)} = \alpha^b \beta A + \langle\alpha\rangle X \tag{2}$$

for some $\beta \in H$ and $X \in \mathbb{Z}[G]$ where $m = o(\beta)$ is a divisor of $p - 1$. Since $\chi(A) = 0$ for all characters χ of G which are principal on $\langle\alpha\rangle$, we have $\langle\alpha\rangle A = 0$. By multiplying both sides of (2) by $\langle\alpha\rangle$, we have $\langle\alpha\rangle X = 0$ and hence $(\alpha^b A)^{(t)} = \alpha^b \beta A$.

Let $\{h_1, h_2, \ldots, h_v\}$ be a complete set of coset representatives of $\langle\beta\rangle$ in H and $Q_j = \{\alpha^{t^i}\beta^{j-i} \mid i = 0, 1, \ldots, p-2\}$ for $j = 0, 1, \ldots, m-1$. By Lemma 3.3,

$$\alpha^b A = \langle\beta\rangle \sum_{k=1}^{v} a_k h_k + \sum_{j=0}^{m-1} \sum_{k=1}^{v} b_{jk} Q_j h_k \tag{3}$$

where $a_k, b_{jk} = 0, \pm 1$. Since $\langle\alpha\rangle Q_j = [(p-1)/m]\langle\alpha\rangle\langle\beta\rangle$, by multiplying both sides of (3) by $\langle\alpha\rangle$, we get

$$\frac{p-1}{m} \sum_{j=0}^{m-1} b_{jk} = -a_k$$

for all k. So either $m = p - 1$ or $a_k = 0$ for all k. Note that $\langle\beta\rangle Q_j = \langle\beta\rangle(\langle\alpha\rangle - 1)$. If $a_k = 0$ for all k, then

$$\langle\beta\rangle\alpha^b A = m\langle\beta\rangle \sum_{k=1}^{v} a_k h_k + \langle\beta\rangle(\langle\alpha\rangle - 1) \sum_{k=1}^{v} \sum_{j=0}^{m-1} b_{jk} h_k = 0$$

which violates the assumption $AA^{(-1)} = p^2 - p\langle\alpha\rangle$. So we have $m = p - 1$.

Let x_1 be the number of $+1$ coefficients in A and x_2 be the number of -1 coefficients in A. By $AA^{(-1)} = p^2 - p\langle\alpha\rangle$, we have $x_1 + x_2 = p^2 - p$ and by $\langle\alpha\rangle A = 0$, we have $x_1 - x_2 = 0$. Hence $x_1 = x_2 = p(p-1)/2$. By (3), since $o(\beta) = m = p - 1$ and $|Q_j| = p - 1$, x_1 and x_2 must be divisible by $p - 1$ which is impossible. □

Lemma 3.5 *Let $G = \langle\alpha\rangle \times H$ where $o(\alpha) = p$, $\exp(H) = w$, $(p, w) = 1$ and p is an odd prime. Let t be a primitive root modulo p such that $t \equiv 1 \bmod w$. If $A \in \mathbb{Z}[G]$ satisfies $AA^{(-1)} = p^2$, then there exist an integer b such that*

$$(\alpha^b A)^{(t)} = \beta\alpha^b A + \varepsilon(1 - \beta)\langle\alpha\rangle g$$

where $\varepsilon = \pm 1$, $g, \beta \in H$ and $o(\beta) \mid (p - 1, w)$.

Proof: By Lemma 3.2,

$$(\alpha^b A)^{(t)} = \beta\alpha^b A + \langle\alpha\rangle X \tag{4}$$

for some $X \in \mathbb{Z}[G]$. Let $\tau : G \to G/\langle\alpha\rangle$ be the natural epimorphism. Then $\tau(A^{(t)}) = \tau(A)$ and hence by (4),

$$(1 - \bar{\beta})\tau(A) = p\tau(X)$$

where $\bar{\beta} = \tau(\beta)$. Since $\tau(A)\tau(A)^{(-1)} = p^2$, we have $\tau(X)\tau(X)^{(-1)} = 2 - \bar{\beta} - \bar{\beta}^{-1}$. If $\beta = 1$, then $\tau(X) = 0$ and hence $\langle\alpha\rangle X = 0$. Assume $\beta \neq 1$, then the coefficient of the identity element of $\tau(X)\tau(X)^{(-1)}$ is 2 which implies the support of $\tau(X)$ has exactly two elements. Hence it is not hard to see that $\tau(X) = \varepsilon(1 - \bar{\beta})g'$, where $\varepsilon = \pm 1$, for some $g' \in G/\langle\alpha\rangle$. Thus $\langle\alpha\rangle X = \varepsilon(1 - \beta)\langle\alpha\rangle g$ where $\tau(g) = g'$. □

Lemma 3.6 *Use the notation in Lemma* 3.5. *In addition, assume the coefficients of A are* $0, \pm 1$. *Let $m = o(\beta)$ and let y_0 be the coefficient of the identity element in $\tau(\varepsilon g^{-1}\alpha^b A)$ where $\tau : G \to G/\langle\alpha\rangle$ is the natural epimorphism. Then*

(i) $\frac{p(m-2)}{m} \le y_0 < p$; *and*
(ii) *if $m > 2$, then $y_0 \equiv 1$ mod m and $m^2 \le 2(p - 1)$.*

Proof: Let $A' = \varepsilon g^{-1}\alpha^b A$ and $\{h_1 = 1, h_2, \ldots, h_v\}$ be a complete set of coset representatives of $\langle\beta\rangle$ in H. From Lemma 3.5, $(A' - \langle\alpha\rangle)^{(t)} = \beta(A' - \langle\alpha\rangle)$. So by Lemma 3.3,

$$A' - \langle\alpha\rangle = \langle\beta\rangle \sum_{k=1}^{v} a_k h_k + \sum_{j=0}^{m-1}\sum_{k=1}^{v} b_{jk} Q_j h_k \tag{5}$$

where $a_k, b_{jk} = 0, \pm 1$ (by comparing the coefficients of βh_k and $\alpha^{t^{j-1}}\beta h_k$ in both sides of (5)). Let x_1 be the number of $+1$ coefficients in A' and x_2 be the number of -1 coefficients in A'. By Proposition 1.1, $\{x_1, x_2\} = \{(p^2 - p)/2, (p^2 + p)/2\}$. On the other hand, by comparing the coefficients of h_1 and $\alpha^{t^j} h_1$ in both sides of (5), we find that the coefficients of α^i, $0 \le i < p-1$, in A' can only be 0 or 1. Thus y_0 is equal to the number of i, $0 \le i < p-1$, such that the coefficient of α^i in A' is 1. By (5), $x_1 - y_0 \equiv 0 \bmod m$ and $x_2 + p - y_0 \equiv 0 \bmod m$. Since $p \equiv 1 \bmod m$, if $m > 2$, then $x_1 = (p^2 + p)/2$, $x_2 = (p^2 - p)/2$ and $y_0 \equiv 1 \bmod m$.

Let $\bar{\beta} = \tau(\beta)$, $\bar{h}_k = \tau(h_k)$. Since $\tau(Q_j) = [(p-1)/m]\langle\bar{\beta}\rangle$,

$$\tau(A') = p + \langle\bar{\beta}\rangle \sum_{k=1}^{v} y_k \bar{h}_k$$

where $y_k = a_k + \sum_{j=0}^{m} b_{jk}$. Since $\tau(A')\tau(A')^{(-1)} = p^2$, we have

$$m \sum_{k=1}^{v} y_k^2 = -2py_1.$$

So we must have $my_1^2 \le -2py_1$ which implies $-2p/m \le y_1 \le 0$. Suppose $y_1 = 0$. Then $y_k = 0$ for all k. Hence $\tau(A') = p$ and it means $\langle\alpha\rangle A' = p\langle\alpha\rangle$. But this implies $(A' - \langle\alpha\rangle)(A' - \langle\alpha\rangle)^{(-1)} = p^2 - p\langle\alpha\rangle$ which is impossible by Lemma 3.4. So (i) follows because $y_0 = p + y_1$.

If $m > 2$, then by $-2p/m \le y_1 < 0$ and $y_1 = y_0 - p \equiv 0 \bmod m$, we have $m^2 \le 2p$. Since $p \equiv 1 \bmod, m$, $m^2 \ne 2p,\ 2p - 1$. □

Lemma 3.7 *Let $G = \langle\alpha\rangle \times H$ where $o(\alpha) = p^s$, $\exp(H) = w$, $(p, w) = 1$ and p is a prime greater than* 3. *Let t be a primitive root modulo p^s such that $t \equiv 1 \bmod w$. If $A \in \mathbb{Z}[G]$ satisfies $A^{(t)} = A$, $AA^{(-1)} = n$, for some integer n, and the coefficients of A are chosen from* $\{0, \pm1, \ldots, \pm1(p-3)/2\}$, *then $A \in \mathbb{Z}[H]$.*

Proof: The condition $A^{(t)} = A$ implies $A = X_0 + \langle\alpha\rangle X_1$ for some $X_0 \in \mathbb{Z}[H]$ and $X_1 \in \mathbb{Z}[G]$. The Lemma follows by a similar argument used in the proof of Theorem 3.1. □

Theorem 3.8 *Let $G = \langle\alpha\rangle \times H$ where $o(\alpha) = p$, $\exp(H) = w$, $(p, w) = 1$ and p is a prime greater than* 7. *If $A \in \mathbb{Z}[G]$ satisfies $AA^{(-1)} = p^2$ and the coefficients of A are* 0, ±1, *then either there exists an integer b such that $\alpha^b A \in \mathbb{Z}[H]$ or*

$$\varepsilon h A = \left[1 + (1-\beta)\sum_{i=0}^{\frac{p-1}{2}-1} \alpha^{t^{2i}}\right] + (1+\beta)E + (1-\beta)\sum_{i=0}^{p-2}(-1)^i \alpha^{t^i} F \tag{6}$$

where $\varepsilon = \pm1$, $h \in G$, $\beta \in H$, $o(\beta) = 2$, $E, F \in \mathbb{Z}[H]$ and t is a primitive root modulo p.

Proof: Let t be a primitive root modulo p such that $t \equiv 1 \bmod w$. By Lemma 3.5, there exists an integer b such that

$$(\alpha^b A)^{(t)} = \beta\alpha^b A + \varepsilon(1-\beta)\langle\alpha\rangle g$$

where $\beta, g \in H$, $o(\beta) \mid (p-1, w)$ and $\varepsilon = \pm1$. If $\beta = 1$, then by Lemma 3.7, $\alpha^b A \in \mathbb{Z}[H]$.

Assume $\beta \neq 1$. Let $m = o(\beta)$ and let $\{h_1 = 1, h_2, \ldots, h_v\}$ be a complete set of coset representatives of $\langle\beta\rangle$ in H. By Lemma 3.3, there exists an integer b such that

$$\varepsilon g^{-1}\alpha^b A - \langle\alpha\rangle = \langle\beta\rangle \sum_{k=1}^{u} a_k h_k + \sum_{j=0}^{m-1}\sum_{k=1}^{v} b_{jk} Q_j h_k$$

where $a_k, b_{jk} = 0, \pm 1$. Let $\kappa : G \to G/\langle\beta\rangle$ be the natural epimorphism and $B = \kappa(\varepsilon g^{-1}\alpha^b A)$. Note that $B^{(t)} = B$ and

$$B = \langle\alpha\rangle + m \sum_{k=1}^{u} a_k \bar{h}_k + +(\langle\bar{\alpha}\rangle - 1) \sum_{k=1}^{v} \left(\sum_{j=0}^{m-1} b_{jk} \right) \bar{h}_k$$

where $\bar{\alpha} = \kappa(\alpha)$ and $\bar{h}_k = \kappa(h_k)$. Since $p > 7$, by Lemma 3.6,

$$m < \frac{p-1}{2}. \tag{7}$$

By Lemma 3.7, $B \in \mathbb{Z}[H/\langle\beta\rangle]$. So we have $\sum_{j=0}^{m-1} b_{j1} = -1$ and $\sum_{j=0}^{m-1} b_{jk} = 0$ for all $k \geq 2$.

Suppose $m = 2$. Then

$$\begin{aligned} \langle\alpha\rangle + \sum_{j=0}^{m-1} b_{j1} Q_j &= \langle\alpha\rangle - Q_1 + b_{01}(Q_0 - Q_1) \\ &= \left[1 + (1-\beta) \sum_{i=0}^{\frac{p-1}{2}-1} \alpha^{t^{2i}} \right] + b_{01}(1-\beta) \sum_{i=0}^{p-2} (-1)^i \alpha^{t^i} \end{aligned}$$

and

$$\sum_{j=0}^{m-1} b_{jk} Q_j = b_{0k}(Q_0 - Q_1) = b_{0k}(1-\beta) \sum_{i=0}^{p-2} (-1)^i \alpha^{t^i}$$

for $k \geq 2$. So (6) follows with $E = \sum_{i=1}^{v} a_k h_k$ and $F = \sum_{i=1}^{v} b_{0k} h_k$.

Assume $m > 2$. We can write B as $B = 1 + mC$ where $C = \sum_{k=1}^{v} a_k \bar{h}_k$. Since $BB^{(-1)} = p^2$, we have

$$mCC^{(-1)} + (C + C^{(-1)}) = \frac{p^2 - 1}{m}$$

and $C + C^{(-1)} \equiv (p^2 - 1)/m \bmod m$. Note that the coefficients of $C + C^{(-1)}$ can only be $0, \pm 1, \pm 2$. Thus either

$$C + C^{(-1)} = 0 \quad \text{and} \quad CC^{(-1)} = (p^2 - 1)/m^2$$

or

$$C + C^{(-1)} = \pm 2 \quad \text{and} \quad CC^{(-1)} = (p^2 \mp 2m - 1)/m^2.$$

Let χ_0 be the principal character of $H/\langle\beta\rangle$. Then either

$$\chi_0(C) = 0 \quad \text{and} \quad \chi_0(C)^2 = (p^2 - 1)/m^2$$

or

$$\chi_0(C) = \pm 1 \quad \text{and} \quad \chi_0(C)^2 = (p^2 \mp 2m - 1)/m^2.$$

The first case is impossible. The only possible solution for the second case is $m = p \mp 1$ which violates (7). □

The following proposition is immediate from Theorem 3.8.

Proposition 3.9 *A in Eq.* (6) *satisfies* $AA^{(-1)} = p^2$ *if and only if*

(a) $(1 + 2\kappa(E))(1 + 2\kappa(E)^{(-1)}) = p^2$ *where* $\kappa : H \to H/\langle\beta\rangle$ *is the natural epimorphism*; *and*
(b) $(1 + 2\chi(F))\,\overline{(1 + 2\chi(F))} = p$ *for all characters* χ *of H which are non-principal on* $\langle\beta\rangle$.

Proof: The proposition follows by computing the values of $\chi'(A)$ for all characters χ' of G and the fact that

$$\chi'\left(\sum_{i=0}^{\frac{p-1}{2}-1} \alpha^{t^{2i}}\right) = \begin{cases} (-1 \pm \sqrt{p*})/2 & \text{if } \chi' \text{ is nonprincipal on } \langle\alpha\rangle \\ (p-1)/2 & \text{if } \chi' \text{ is principal on } \langle\alpha\rangle \end{cases}$$

and

$$\chi'\left(\sum_{i=0}^{p-2} (-1)^i \alpha^{t^i}\right) = \begin{cases} \pm\sqrt{p*} & \text{if } \chi' \text{ is nonprincipal on } \langle\alpha\rangle \\ 0 & \text{if } \chi' \text{ is principal on } \langle\alpha\rangle \end{cases}$$

where

$$p* = (-1)^{(p-1)/2} p.$$ □

Note the coefficients of $\kappa(E)$ and F are 0, ±1 and the elements of the support of F are in different cosets of $\langle\beta\rangle$. Also, the coefficient of the identity element in $1 + 2\kappa(E)$ is ±1.

Corollary 3.10 *Let* G, H, α *and* A *be as in Theorem* 3.8. *If* w *is odd or* w *is strictly divisible by 2 or* $w \leq (p^2 + 1)/2$, *then there exists an integer b such that* $\alpha^b A \in \mathbb{Z}[H]$.

Proof: The case w is odd follows by Theorem 3.8. If $w \leq (p^2+1)/2$, then $(1+2\kappa(E))\,(1+2\kappa(E)^{(-1)}) = p^2$ is impossible because the coefficient of the identity element in the left-hand-side is at most $1 + 4[(w/2) - 1]$. If $w = 2m$ for some odd number m, then $(1 + 2\chi(F))\overline{(1 + 2\chi(F))}$ cannot be p if χ is a character of order 2. □

Application of Corollary 3.10 $CW(n, k)$ does not exist for the pairs $(n, k) = (11w, 121)$ for all $w < 62$.

Theorem 3.11 *Let $G = \langle\alpha\rangle \times H$ where $o(\alpha) = p^s$, p is an odd prime,* $\exp(H) = w$, $s > 1$ *and p, w are relatively prime. If $A \in \mathbb{Z}[G]$ satisfies $AA^{(-1)} = p^2$ and the coefficients of A are* $0, \pm 1$, *then there exists an integer b such that $\alpha^b A$ is in* $\mathbb{Z}[\langle\alpha^{p^{s-1}}\rangle \times H]$.

Proof: Let $P = \langle\alpha^{p^{s-1}}\rangle$. Applying Proposition 2.3 repeatedly, there exists an integer b such that

$$\alpha^b A = B + PC$$

where B in $\mathbb{Z}[P \times H]$ and the support of C is contained in $G \backslash (P \times H)$. Let $\tau : G \to G/P$ be the natural epimorphism. Then

$$\tau(\alpha^b A) = \tau(B) + p\tau(C).$$

Since the coefficients of $\tau(\alpha^b A)\ \tau(\alpha^b A)^{(-1)} = p^2$, either $\tau(C) = 0$ or $\tau(B) = 0$ and $\tau(C) = \pm g$ for some g in G/P.

If $\tau(C) = 0$, then $PC = 0$ and hence $\alpha^b A = B$ is in $\mathbb{Z}[P \times H]$.

For the second case, $PB = 0$ and $\alpha^b A = B \pm Ph$ where $h \in G\backslash(P \times H)$. Hence $BB^{(-1)} = p^2 - pP$ but this is impossible by Lemma 3.4. □

Application of Theorem 3.11 $CW(n, k)$ does not exist for the pairs $(n, k) = (147, 49)$, $(125, 25)$, $(200, 25)$. Note that the existence of $CW(200, 25)$ impies that of $CW(40, 25)$, which has been shown not to exist by Arasu and Linthicum (unpublished computer search).

References

1. K.T. Arasu, "A reduction theorem for circulant weighing matrices," *Australas. J. Combin.* **18** (1998), 111–114.
2. K.T. Arasu and J.F. Dillon, *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.* Vol. 542, Kluwer Academic Publisher, Dordrecht, 1999, pp. 1–15.
3. K.T. Arasu and S.L. Ma, "Abelian difference sets without self-conjugacy," *Designs, Codes & Cryptography* **15** (1998), 223–230.
4. K.T. Arasu and S.L. Ma, "A nonexistence result on difference sets, partial difference sets and divisible difference sets," *J. Stat. Planning and Inference*, to appear.
5. K.T. Arasu, S.L. Ma, and Y. Strassler, "Possible orders of a circulant weighing matrix of weight 9," in preparation.
6. K.T. Arasu and J. Seberry, "Circulant weighing designs," *J. Comb. Designs* **4**(6) (1996), 439–447.
7. P. Eades and R.M. Hain, "On circulant weighing matrices," *Ars Combin.* **2** (1976), 265–284.

8. A.V. Geramita and J. Seberry, *Orthogonal Designs: Quadratic Forms* and Hadamard Matrices, Marcel Dekker, New York-Basel, 1979.

9. R.C. Mullin, "A note on balanced weighing matrices, Combinatorial Mathematics III," in *Proceedings of the Third Australian Conference*, Lecture Notes in Mathematics, Vol. 452, Springer, Berlin-Heidelberg-New York, 1975, pp. 28–41.

10. A. Pott, *Finite Geometry and Character Theory*, Lecture Notes in Mathematics, Vol. 1601, Springer, Berlin-Heidelberg-New York, 1991.

11. Y. Strassler, "The classification of circulant weighing matrices of weight 9," Ph.D. Thesis, Bar-Ilan University, 1997.