Available online at www.sciencedirect.com
ScienceDirect
Discrete Mathematics 308 (2008) 2802–2809
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Study of proper circulant weighing matrices with weight 9

Miin Huey Ang[a], K.T. Arasu[b,1], Siu Lun Ma[c,2], Yoseph Strassler[d]

[a]*Pusat Pengajian Sains Matematik, Universiti Sains Malaysia, Minden 11800, Penang, Malaysia*
[b]*Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435, USA*
[c]*Department of Mathematics, National University of Singapore, Kent Ridge, Singapore 119260, Republic of Singapore*
[d]*Department of Mathematics and Computer Science, Bar-Ilan University, Ramat-Gan, 52900 Israel*

Received 7 October 2003; received in revised form 8 September 2004; accepted 16 December 2004
Available online 6 June 2007

Dedicated to Professor Jennifer Seberry on the occasion of her 60th birthday

Abstract

We provide the first theoretical proof of the spectrum of orders n for which circulant weighing matrices with weight 9 exist. This spectrum consists of those positive integers n, which are multiples of 13 or 24. We actually characterize the "minimal" examples which exist for orders 13, 26, or 24.

Keywords: Weighing matrices; Characters

1. Introduction

A *weighing matrix* of order n and weight m^2 is a square matrix M of order n with entries from $\{-1, 0, +1\}$ such that

$$MM^{\mathrm{T}} = m^2 I,$$

where I is the identity matrix of order n and M^{T} is the transpose of M. In the following, we say that M is a $W(n, m^2)$ if M is a weighing matrix of order n and weight m^2.

Let $G = \{g_1, g_2, \ldots, g_n\}$ be a group of order n. Let $A = \sum_{i=1}^{n} a_i g_i$, $a_i \in \mathbf{Z}$, be an element of the group ring $\mathbf{Z}[G]$. For any integer t, we define $A^{(t)}$ to be $\sum_{i=1}^{n} a_i g_i^t$. Suppose A satisfies

(W1) $a_i \in \{0, \pm 1\}$ and
(W2) $AA^{(-1)} = m^2$.

Then the group matrix $M = (b_{ij})$, where $b_{ij} = a_k$ if $g_i g_j^{-1} = g_k$, is a $W(n, m^2)$, see [1].

For the convenience of our study of group weighing matrices using the notation of group rings, we say that $A \in \mathbf{Z}[G]$ is a $W(G, m^2)$ if it satisfies conditions (W1) and (W2) above. In particular, if G is cyclic group of order n, the group

[1] The research is partially supported by a grant from NSA.
[2] The research is supported by NUS Research Grant R-146-000-041-112.
E-mail address: karasu@math.wright.edu (K.T. Arasu).

0012-365X/$ - see front matter
doi:10.1016/j.disc.2004.12.029

matrix obtained is a circulant matrix and we say that A is a $CW(n, m^2)$. We use the prefix CW to mean "Circulant weighing matrices". For more on circulant weighing matrices, see Arasu and Seberry [4,5], and Mullin [6].

For A as defined above, the *support* of A is defined to be the set $\mathrm{supp}(A) = \{g_i | a_i \neq 0\}$. Suppose A is a $W(G, m^2)$. If the support of A is contained in a (left or right) coset of a proper subgroup H in G, we say that A is a *trivial extension* of a $W(H, m^2)$. If A is not a trivial extension of any $W(H, m^2)$ for any proper subgroup H of G, A is called a *proper* $W(G, m^2)$.

In this paper, we shall prove that proper $CW(n, 9)$ only exist for $n = 13$, 26 and 24. A machine-dependent proof of this is already contained in [7]. In this paper, we provide a theoretical proof.

Example 1. Let $G = \langle g \rangle$ where $\mathrm{o}(g) = 26$. Let

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

Then A is a proper $CW(26, 9)$. Let $\rho : G \longrightarrow G/\langle g^{13} \rangle$ be the natural epimorphism. It can be shown that $\rho(A)$ is a proper $CW(13, 9)$. Here $\mathrm{o}(g)$ denotes the order of g.

Example 2. Let $G = \langle h \rangle \times \langle g \rangle$ where $\mathrm{o}(h) = 3$ and $\mathrm{o}(g) = 8$. Let

$$A = -1 + (1 - g^4)(g + g^3) + (h + h^2)(1 + g^4).$$

Then A is a proper $CW(24, 9)$.

The following is the main theorem of this paper:

Theorem 3. *There exists a proper $CW(n, 9)$ if and only if $n = 13$, 26 or 24.*

2. Preliminaries

The following notation will be used throughout this paper. For integers n and p which are relatively prime, we shall denote $\mathrm{Ord}_n(p)$ to be the smallest positive integer e such that $p^e \equiv 1 \bmod n$ or in other words, e is the smallest positive integer such that $p^e - 1 \equiv 0 \bmod n$. For an element h of a group, $\theta(h, p)$ will be used to denote the set $\{h, h^p, h^{p^2}, \ldots\}$. If K is a normal subgroup of a group G, then τ_K is the natural epimorphism from G to G/K. Let S be a subset of G. Following the usual practice of algebraic design theory, we identify S with the group ring element $S = \sum_{g \in S} g$ in $\mathbf{Z}[G]$.

Proposition 4. *Let G be a finite group, K a normal subgroup of G and k an integer. If $A \in \mathbf{Z}[G]$ satisfies $AA^{(-1)} = k$, then $\tau_K(A)\tau_K(A)^{(-1)} = k$.*

The following two lemmas are well known, see e.g. [2].

Lemma 5. *Let A be a $W(G, m^2)$ for some finite group G. Then $A = X_1 - X_2$ for two disjoint subsets X_1 and X_2 such that $\{|X_1|, |X_2|\} = \{(m^2 + m)/2, (m^2 - m)/2\}$.*

Lemma 6. *Let G be an abelian group of order n and let p be a prime relatively prime to n. If $A \in \mathbf{Z}[G]$ is such that $AA^{(-1)} = p^{2r}$, then there exists $g \in G$ such that $(gA)^{(p)} = gA$.*

We prove a couple of useful lemmas.

Lemma 7. *Let G be a cyclic group of order n and let p be a prime relatively prime to n. Let $X_1, X_2, \ldots, X_s$ be pairwise disjoint subsets of G. Let $A = \sum_{i=1}^{s} a_i X_i \in \mathbf{Z}[G]$, where $a_1, a_2, \ldots, a_s$ are distinct nonzero integers, be such that $AA^{(-1)} = p^{2r}$ and the support of A is not contained in any coset of any proper subgroup of G, then n is a divisor of the least common multiple of $p - 1, p^2 - 1, \ldots, p^u - 1$ where $u = \max\{|X_i| | i = 1, 2, \ldots, s\}$.*

Proof. By Lemma 6, we know that there exists $g \in G$ such that $(gA)^{(p)} = gA$. Clearly $(gA)(gA)^{(-1)} = p^{2r}$ and the support of gA is not contained in any coset of any proper subgroup of G. Also $gA = \sum_{i=1}^{s} a_i g X_i$ where $gX_1, gX_2, \ldots, gX_s$

are pairwise disjoint subsets of G. By Lemma 5, WLOG we can assume that $|X_1| \geqslant |X_i|$ for all $i \geqslant 2$. Let $h \in \mathrm{supp}(gA)$. As $(gA)^{(p)} = gA$, if $h \in gX_i$, then $\theta(h, p) \subseteq gX_i$. Thus for all $h \in \mathrm{supp}(gA)$,

$$|\theta(h, p)| = \mathrm{Ord}_{\mathrm{o}(h)}\, p \leqslant |gX_i| = |X_i| \leqslant |X_1|.$$

As the support of gA is not contained in any coset of any proper subgroup of G, $G = \langle \mathrm{supp}(gA) \rangle$. Since for every $h \in \mathrm{supp}(gA)$, $\mathrm{o}(h) | p^t - 1$ where $t = \mathrm{Ord}_{\mathrm{o}(h)}\, p \leqslant |X_1|$, n is a divisor of the least common multiple of $p-1, p^2-1, \ldots, p^u - 1$. $\square$

Lemma 8. *Let G be a cyclic group of order n and let p be a prime relatively prime to n. Let $X_1, X_2, \ldots, X_s$ be pairwise disjoint subsets of G such that $|X_1| > |X_i|$ for all $i \geqslant 2$. Let $A = \sum_{i=1}^{s} a_i X_i \in \mathbf{Z}[G]$, where $a_1, a_2, \ldots, a_s$ are distinct nonzero integers, be such that $AA^{(-1)} = p^{2r}$* and *$A^{(p)} = A$. If q is a prime divisor of n such that $q^f | n$ and* $\mathrm{Ord}_{q^f}(p) > |X_i|$ *for all $i \geqslant 2$, then*

$$A = C + a_1 \sum_{i=1}^{d} \theta(h_i, p)$$

for some $h_1, h_2, \ldots, h_d \in X_1$ and $C \in \mathbf{Z}[G]$ where $\mathrm{supp}(C)$ *is contained in the proper subgroup $K = \{g \in G | q^f$ does not divide* $\mathrm{o}(g)\}$ *of G.*

Proof. For any $h \in \mathrm{supp}(A)$, if $q^f | \mathrm{o}(h)$, then $|\theta(h, p)| \geqslant \mathrm{ord}_{q^f}(p)$. This implies that $h \in \mathrm{supp}(X_1)$ and thus $\theta(h, p) \subseteq X_1$. So we can write

$$A = C + a_1 \sum_{i=1}^{d} \theta(h_i, p)$$

for some $h_1, h_2, \ldots, h_d \in \mathrm{supp}(X_1)$ and $C \in \mathbf{Z}[G]$ where $\mathrm{supp}(C) \subseteq K$. $\square$

3. The case when n is not a multiple of 3

In this section, we assume that n is not a multiple of 3. Let G be a cyclic group of order n and let $A \in \mathbf{Z}[G]$ be a proper $CW(n, 9)$. Clearly hA is a proper $CW(n, 9)$ for $h \in G$ if and only if A is a proper $CW(n, 9)$. Consider gA for the $g \in G$ such that $(gA)^{(3)} = gA$. By Lemma 5, WLOG we assume that $gA = X_1 - X_2$ where X_1, X_2 are disjoint subsets of G such that $|X_1| = 6$ and $|X_2| = 3$. By the choice of g, we know that $X_i^{(3)} = X_i$ for $i = 1, 2$. Thus if $h \in \mathrm{supp}(X_i)$, then $\theta(h, 3) \subseteq \mathrm{supp}(X_i)$ too. By Lemma 7, n is a divisor of the smallest common multiple of $3-1, 3^2-1, \ldots, 3^6-1$, i.e. $2^4 \times 5 \times 7 \times 11^2 \times 13$. Note that

$$3 - 1 = 2 \;\Rightarrow\; \mathrm{Ord}_2 3 = 1;$$

$$3^2 - 1 = 2^3 \;\Rightarrow\; \mathrm{Ord}_{2^2} 3 = \mathrm{Ord}_{2^3} 3 = 2;$$

$$3^3 - 1 = 2 \times 13 \;\Rightarrow\; \mathrm{Ord}_{13} 3 = \mathrm{Ord}_{2\times 13} 3 = 3;$$

$$3^4 - 1 = 2^4 \times 5 \;\Rightarrow\; \mathrm{Ord}_{2^4} 3 = \mathrm{Ord}_5 3 = \mathrm{Ord}_{2^4\times 5} 3 = 4;$$

$$3^5 - 1 = 2 \times 11^2 \;\Rightarrow\; \mathrm{Ord}_{11} 3 = \mathrm{Ord}_{11^2} 3 = \mathrm{Ord}_{2\times 11} 3 = \mathrm{Ord}_{2\times 11^2} 3 = 5;$$

$$\begin{aligned} 3^6 - 1 = 13 \times 7 \times 2^3 \;\Rightarrow\; \mathrm{Ord}_7 3 &= \mathrm{Ord}_{7\times 2} 3 = \mathrm{Ord}_{7\times 2^2} 3 = \mathrm{Ord}_{7\times 2^3} 3 \\ &= \mathrm{Ord}_{7\times 13} 3 = \mathrm{Ord}_{13\times 2^2} 3 = \mathrm{Ord}_{13\times 2^3} 3 \\ &= \mathrm{Ord}_{13\times 7\times 2^3} 3 = 6. \end{aligned}$$

Case 1: Assume that $n = 11a$ for some integer a.

There exists an element $h \in \mathrm{supp}(gA)$ such that $11|\mathrm{o}(h)$ as A is proper. Note that $|\theta(h,3)|=5$ and $\mathrm{o}(h)=11$, 11^2, 2×11 or 2×11^2. By Lemma 8, $gA = C + \theta(h,3)$ where $\mathrm{supp}(C) \subseteq K = \{g \in G | 11|\mathrm{o}(g)\}$. Let H be a subgroup of G such that

$$|H| = \begin{cases} 11 & \text{if } \mathrm{o}(h) = 11 \text{ or } 2\times 11, \\ 11^2 & \text{if } \mathrm{o}(h) = 11^2 \text{ or } 2\times 11^2. \end{cases}$$

Then

$$\tau_H(gA) = \tau_H(C) + 5\alpha, \tag{1}$$

where $\alpha \in G/H$, $\mathrm{o}(\alpha) = 1$ or 2 and the coefficients of $\tau_H(C)$ are 0, ± 1. By Proposition 4, the coefficient of the identity in $\tau_H(gA)\tau_H(gA)^{(-1)}$ is 9 while by Eq. (1), the coefficient of the identity in $\tau_H(gA)\tau_H(gA)^{(-1)}$ is the sum of the squares of all coefficients of $\tau_H(gA)$ which is at least $(5-1)^2 + 4 - 1 = 19$, a contradiction.

Case 2: Assume that $n = ma$, where $m \in \{2^4, 5, 7\}$, for some integer a.

There exists an element $h \in \mathrm{supp}(gA)$ such that $m|\mathrm{o}(h)$ as A is proper. Note that $|\theta(h,3)| = 4$ if $m = 2^4$ or 5; and $|\theta(h,3)| = 6$ if $m = 7$. By Lemma 8, $gA = C + \theta(h,3)$ where $\mathrm{supp}(C) \subseteq K = \{g \in G | m \text{ does not divide } \mathrm{o}(g)\}$. Let H be a subgroup of G such that

$$|H| = \begin{cases} 2^3 a & \text{if } \mathrm{o}(h) = 2^4, \\ a & \text{if } \mathrm{o}(h) = 5 \text{ or } 7. \end{cases}$$

Then

$$\tau_H(gA) = \begin{cases} -1 + 4\tau_H(h) & \text{if } \mathrm{o}(h) = 2^4, \\ -1 + \theta(\tau_H(h), 3) & \text{if } \mathrm{o}(h) = 5, \\ -3 + \theta(\tau_H(h), 3) & \text{if } \mathrm{o}(h) = 7, \end{cases} \tag{2}$$

where $\tau_H(h)$ is not the identity. This contradicts Proposition 4 as the coefficients of the identity in $\tau_H(gA)\tau_H(gA)^{(-1)}$ are, respectively, 17, 5 and 15 by Eq. (2).

Case 3: Assume that $n = 2^2 \times 13 \times a$ where $a = 1$ or 2.

Let $h \in G$. Note that

$$|\theta(h,3)| = \begin{cases} 1 & \text{if } \mathrm{o}(h) = 1 \text{ or } 2, \\ 2 & \text{if } \mathrm{o}(h) = 4 \text{ or } 8, \\ 3 & \text{if } \mathrm{o}(h) = 13 \text{ or } 26, \\ 6 & \text{if } \mathrm{o}(h) = 52 \text{ or } 104. \end{cases}$$

(a) Suppose for all $h \in X_2$, $\mathrm{o}(h) \notin \{13, 26\}$. Then $X_2 \subseteq P$ where P is the subgroup of G or order $4a$. Since A is proper,

$$\tau_P(gA) = -3 + X, \quad -3 + 2Y \quad \text{or } Z,$$

where $X, Y \subseteq G/P$ such that $|X| = 6$ and $|Y| = |Z| = 3$. The coefficient of the identity in $(-3+X)(-3+X^{(-1)})$ is 15, the coefficient of the identity in $(-3+2Y)(-3+2Y^{(-1)})$ is 21 and the coefficient of the identity in $ZZ^{(-1)}$ is 3. All these contradict $\tau_P(gA)\tau_P(gA)^{(-1)} = 9$.

(b) Suppose $X_2 = \theta(h_1, 3)$ for some $h_1 \in G$ of order 13 or 26.
If $X_1 \subseteq P$ where P is the subgroup of G of order $4a$, then $\tau_P(gA) = 6 - \theta(\tau_P(h_1))$, a contradiction. Hence there exists $h_2 \in X_1$ such that $13|\mathrm{o}(h_2)$. If $\mathrm{o}(h_2) = 52$ or 104, then

$$\tau_P(gA) = 2X - Y \quad \text{or } Z,$$

where $X, Y, Z \subseteq G/P$, $X \cap Y = \emptyset$, $|X| = |Y| = |Z| = 3$, and both cases contradict with $\tau_P(gA)\tau_P(gA)^{(-1)} = 9$. So $\mathrm{o}(h_2) = 13$ or 26. Since A is proper, $X_1 = g_1 + \theta(g_2, 3) + \theta(h_2, 3)$ where $\mathrm{o}(g_1) = 1$ or 2, $\mathrm{o}(g_2) = 4$ or 8 and

$\mathrm{o}(h_2) = 13$ or 26. Let L be a subgroup of G of order 26. Then

$$\tau_L(gA) = \begin{cases} 1 + 2\tau_L(g_2) & \text{if } \mathrm{o}(g_2) = 4, \\ 1 + \theta(\tau_L(g_2), 3) & \text{if } \mathrm{o}(g_2) = 8. \end{cases}$$

This contradicts $\tau_L(gA)\tau_L(gA)^{(-1)} = 9$.

As a conclusion of this section, we have the following theorem.

Theorem 9. *If n is not a multiple of 3, then there exists a proper $CW(n, 9)$ if and only if $n = 13$ or $n = 26$.*

4. The case when n is a multiple of 3

We shall now consider the case where n is a multiple of 3. By Theorem 3.11 of [3], we know that all $CW(n, 9)$, where $9|n$, are not proper. Thus we can assume $3\|n$.

The following lemma is a particular case of Lemma 3.5 of [3].

Lemma 10. *Let $G = P \times H$ be an abelian group where $P = \langle\alpha\rangle$, $\mathrm{o}(\alpha) = 3$, and $|H|$ is not a multiple of 3. Let $A \in \mathbf{Z}[G]$ be such that $AA^{(-1)} = 9$. Then for $t \equiv 2 \bmod 3$ and $t \equiv 1 \bmod |H|$, there exists an integer b such that*

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

for some $g, \beta \in H$ where $\mathrm{o}(\beta) = 1$ or 2 and $\varepsilon = \pm 1$.

We first consider the case when $\mathrm{o}(\beta) = 2$.

Lemma 11. *Let $G = P \times H$ be an abelian group where $P = \langle\alpha\rangle$, $\mathrm{o}(\alpha) = 3$, and $(3, |H|) = 1$. Let $A \in \mathbf{Z}[G]$ be such that for $t \equiv 2 \bmod 3$ and $t \equiv 1 \bmod |H|$*

$$A^{(t)} = \beta A + (1 - \beta)Pg \tag{3}$$

for some $g, \beta \in H$ where $\mathrm{o}(\beta) = 2$. Let $K = \langle\alpha, \beta\rangle$ and let $A = \sum_{h\in I} A_h h$ where I is the complete set of coset representatives of K, $g \in I$ and $A_h \in \mathbf{Z}[K]$. Then

$$A_h = a_h(1 + \beta) + a_{h\alpha}(\alpha + \alpha^2) + a_{h\alpha^2}(\alpha^2 + \alpha\beta) \quad \text{for } Kh \neq Kg \tag{4}$$

and

$$A_g = a_g + (a_g - 1)\beta + a_{g\alpha}\alpha + (a_{g\alpha} - 1)\alpha^2\beta + a_{g\alpha^2}\alpha^2 + (a_{g\alpha^2} - 1)\alpha\beta. \tag{5}$$

In particular, if the coefficients of A are $0, \pm 1$, then $a_g, a_{g\alpha}, a_{g\alpha^2} \in \{0, 1\}$ and $|\mathrm{supp}(A_g)| = 3$.

Proof. First, we consider A_h where $Kh \neq Kg$. In this case $A_h^{(t)} = \beta A_h$. Note that if $A_h = a_h + a_{h\beta}\beta + a_{h\alpha}\alpha + a_{h\alpha^2}\alpha^2 + a_{h\beta\alpha}\beta\alpha + a_{h\beta\alpha^2}\beta\alpha^2$, then

$$\beta A_h = a_{h\beta} + a_h\beta + a_{h\alpha\beta}\alpha + a_{h\alpha}\alpha\beta + a_{h\alpha^2\beta}\alpha^2 + a_{h\alpha^2}\alpha^2\beta, \tag{6}$$

$$A_h^{(t)} = a_h + a_{h\beta}\beta + a_{h\alpha^2}\alpha + a_{h\alpha^2\beta}\alpha\beta + a_{h\alpha}\alpha^2 + a_{h\alpha\beta}\alpha^2\beta. \tag{7}$$

By comparing the coefficients of Eqs. (6) and (7), we know that $a_h = a_{h\beta}$, $a_{h\alpha^2} = a_{h\beta\alpha}$ and $a_{h\alpha} = a_{h\beta\alpha^2}$. Thus

$$A_h = a_h(1 + \beta) + a_{h\alpha}(\alpha + \alpha^2) + a_{h\alpha^2}(\alpha^2 + \alpha\beta).$$

Now, let us consider A_g. By Eq. (3),

$$A_g^{(t)} = \beta A_g + (1 - \beta)P.$$

This implies that $a_g = a_{g\beta} + 1$, $a_{g\alpha^2} = a_{g\beta\alpha} + 1$ and $a_{g\alpha} = a_{g\beta\alpha^2} + 1$. Hence

$$A_g = a_g + (a_g - 1)\beta + a_{g\alpha}\alpha + (a_{g\alpha} - 1)\alpha^2\beta + a_{g\alpha^2}\alpha^2 + (a_{g\alpha^2} - 1)\alpha\beta.$$

If the coefficients of A are $0, \pm 1$, it is obvious that $a_g, a_{g\alpha}, a_{g\alpha^2}$ cannot be -1 and hence $|\mathrm{supp}(A_g)| = 3$. □

Lemma 12. *Let $G = P \times H$ be a cyclic group where $P = \langle\alpha\rangle$, $\mathrm{o}(\alpha) = 3$, and $|H|$ is not a multiple of 3. If $A \in \mathbf{Z}[G]$ is a proper $CW(n, 9)$, then there exists an integer b such that*

$$\alpha^b A = B + (P - 1)C + (P - 2)D + PE$$

for some $B, C, D, E \in \mathbf{Z}[H]$ where coefficients of B, C, D, E are $0, \pm 1$, and the supports of B, C, D, E are pairwise disjoint.

Proof. By Lemma 10, for $t \equiv 2 \bmod 3$ and $t \equiv 1 \bmod |H|$, there exists an integer b such that

$$(\alpha^b A)^{(t)} = \beta(\alpha^b A) + \varepsilon(1 - \beta)Pg,$$

where $g, \beta \in H$, $\mathrm{o}(\beta) = 1$ or 2 and $\varepsilon = \pm 1$. By replacing A with $\alpha^b A$ and, if $\varepsilon = -1$, replacing g with $g\beta$ (note that $\mathrm{o}(\beta) = 1$ or 2 and hence $\beta^{-1} = \beta$), we can assume

$$A^{(t)} = \beta A + (1 - \beta)Pg. \tag{8}$$

Suppose $\mathrm{o}(\beta) = 2$. Then Lemma 11 can be applied. By using the notation of Lemma 11, we have the following four cases.

Case 1: All the elements in the support of A_g have coefficient 1.

Case 2: There are two elements in the support of A_g that have coefficient -1 and one element in the support of A_g that has coefficient 1.

Case 3: All the elements in the support of A_g have coefficient -1.

Case 4: There are two elements in the support of A_g that have coefficient 1 and one element in the support of A_g that has coefficient -1.

WLOG we can assume that $gA = X_1 - X_2$ where X_1, X_2 are disjoint subsets of G such that $|X_1| = 6$ and $|X_2| = 3$. Since all elements in A_h with coefficients $+1$ and -1 for $Kh \neq Kg$ come in pairs as in Eq. (4), either one or three of the coefficients of A_g are -1 in order to have $|X_2| = 3$. Hence cases 1 and 2 are impossible.

If all the elements in the support of A_g have coefficient -1, then we have $\tau_K(A) = -3g + X$, where $X = \tau_K(X_1)$ and $g \notin \mathrm{supp}(X)$. By comparing the coefficient of the identity in the equation $\tau_K(A)\tau_K(A)^{(-1)} = 9$, we have $X = 0$, a contradiction.

If there are two elements in the support of A_g that have coefficient 1 and one element in the support of A_g that has coefficient -1, then

$$\tau_K(A) = g(1 + 2h_1 + 2h_2 - 2h_3),$$

where h_1, h_2, h_3 are nonidentity elements in G/K. Note that contradiction occurs as the coefficient of the identity in the equation $\tau_K(A)\tau_K(A)^{(-1)}$ is 13 if h_1, h_2 and h_3 are all distinct; 21 if $h_1 = h_2 \neq h_3$; and 5 if $h_3 = h_1$ or h_2.

So $\beta = 1$ in Eq. (8) and $A^{(t)} = A$. Hence,

$$A = Y_0 + PY_1, \tag{9}$$

where $Y_0, Y_1 \in \mathbf{Z}[G]$. Let $A = \sum_{h \in J} B_h h$ where J is the complete set of coset representatives of P and $B_h \in \mathbf{Z}[P]$. For $h \in J$, $B_h = \delta + \eta(\alpha + \alpha^2)$ by Eq. (9) where $\delta, \eta = 0, \pm 1$. We shall now sort each coset into a different category such that A can be written in the following form:

$$A = B + (P - 1)C + (P - 2)D + PE,$$

where if $\delta = \pm 1$ and $\eta = 0$, then $h \in \mathrm{supp}(B)$; if $\delta = 0$ and $\eta = \pm 1$, then $h \in \mathrm{supp}(C)$; if $\delta = -\eta = \pm 1$, then $h \in \mathrm{supp}(D)$; and if $\delta = \eta = \pm 1$, then $h \in \mathrm{supp}(E)$. □

Theorem 13. *If n is a multiple of 3, then there exists a proper $CW(n, 9)$ if and only if $n = 24$.*

Proof. Let $G = P \times H$ be a cyclic group where $P = \langle\alpha\rangle$, $\mathrm{o}(\alpha) = 3$, $|H| = w$ and $(3, w) = 1$. If $A \in \mathbf{Z}[G]$ is a proper $CW(n, 9)$, by Lemma 12, WLOG, we can assume

$$A = B + (P-1)C + (P-2)D + PE, \tag{10}$$

where $B, C, D, E \in \mathbf{Z}[H]$, coefficients of B, C, D, E are $0, \pm 1$ and the supports of B, C, D, E are pairwise disjoint. By comparing the coefficients of α in $AA^{(-1)} = 9$, we obtain

$$|\mathrm{supp}(C)| - |\mathrm{supp}(D)| + 3|\mathrm{supp}(E)| = 0. \tag{11}$$

By Eq. (10), $\tau_P(A) = \tau_P(B) + 2\tau_P(C) + \tau_P(D) + 3\tau_P(E)$. If $|\mathrm{supp}(E)| \geqslant 1$, then the coefficient of the identity in $\tau_P(A)\tau_P(A)^{(-1)} > 9$ as $|\mathrm{supp}(D)|$ is not 0 in this case by Eq. (11). Hence $|\mathrm{supp}(\tau_P(E))| = 0$ and hence $|\mathrm{supp}(E)| = 0$ too. Now by Eq. (11), $|\mathrm{supp}(\tau_P(C))| = |\mathrm{supp}(\tau_P(D))|$ and thus by comparing the coefficients of the identity in $\tau_P(A)\tau_P(A)^{(-1)} = 9$,

$$|\mathrm{supp}(\tau_P(B))| + 5|\mathrm{supp}(\tau_P(C))| = 9.$$

Since A is proper, $|\mathrm{supp}(\tau_P(C))| \neq 0$. We have $|\mathrm{supp}(\tau_P(B))| = 4$ and $|\mathrm{supp}(\tau_P(C))| = |\mathrm{supp}(\tau_P(D))| = 1$. Hence,

$$\tau_P(A) = \tau_P(B) + 2\gamma h_1 + \varepsilon h_2, \tag{12}$$

where $\gamma, \varepsilon = \pm 1$ and h_1, h_2 are distinct elements in $(G/P) - \mathrm{supp}(\tau_P(B))$. By Lemma 6, there exists $g \in G/P$ such that

$$(g\tau_P(A))^{(3)} = g\tau_P(A).$$

Let us write

$$X = \gamma g \tau_P(A) = 2x + X_1 - X_2,$$

where $x = gh_1$, X_1 and X_2 are disjoint subsets of G/P and $x \notin X_1 \cup X_2$. Note that

$$X^{(3)} = X \quad \text{and} \quad XX^{(-1)} = 9.$$

By $X^{(3)} = X$, we get $\mathrm{o}(x) = 1$ or 2. By $XX^{(-1)} = 9$, we get

$$4 + |X_1| + |X_2| = 9 \quad \text{and} \quad 2 + |X_1| - |X_2| = \pm 3. \tag{13}$$

By solving Eq. (13), we get either $|X_1| = 0$ and $|X_2| = 5$ or $|X_1| = 3$ and $|X_2| = 2$. By Lemma 7, w is a divisor of the smallest common multiple of $3-1, 3^2-1, \ldots, 3^5-1$, i.e. $2^4 \times 5 \times 11^2 \times 13$.

Case 1: Assume $w = 11a$ for some integer a.

There exists an element $h \in \mathrm{supp}(X)$ such that $11|\mathrm{o}(h)$ as A is proper. Since $|\theta(h, 3)| = 5$, we have $|X_1| = 0$ and $|X_2| = 5$. WLOG, in Eq. (12), we can assume $h = gh_2$ and hence by Eq. (10),

$$\gamma g' A = -\sum_{i=1}^{4} h'^{3^i} + (P-1)x' + (P-2)h',$$

where $g', h', x' \in H$ such that $\tau_P(g') = g$, $\tau_P(h') = h$ and $\tau_P(x') = x$. Note that $11|\mathrm{o}(h')$ and $\mathrm{o}(x') = 1$ or 2. Let $H = \langle h'\rangle$. Then $\tau_H(\gamma g' A) = -6 + P + (P-1)\tau_H(x')$ if $\mathrm{o}(x') = 2$ and $\mathrm{o}(h')$ is odd, otherwise $\tau_H(\gamma g' A) = -7 + 2P$. Note that in both situations, the coefficient of $\tau_H(1)$ in $\tau_H(AA^{(-1)}) > 9$.

Case 2: Assume $w = ma$, where $m = 2^4$ or 5, for some integer a.

There exists an element $h \in \mathrm{supp}(X)$ such that $m|\mathrm{o}(h)$ as A is proper. Since $\theta(h, 3) = 4$, we have $|X_1| = 0$ and $|X_2| = 5$. Then $X = 2x - \theta(h, 3) - y$ where $y \in G/P$, $\mathrm{o}(y) = 1$ or 2 and $y \neq x$. Let K be a subgroup of G/P such that

$$|K| = \begin{cases} 2^3 a & \text{if } m = 2^4, \\ a & \text{if } m = 5. \end{cases}$$

Clearly $x, y \in K$. Then

$$\eta(X) = \begin{cases} 1 - 4\eta(h) & \text{if } m = 2^4, \\ 1 - \theta(\eta(h), 3) & \text{if } m = 5, \end{cases}$$

where $\eta : G/P \to (G/P)/K$ is the natural epimorphism. Note that $\eta(h)$ is not the identity. There is a contradiction as the coefficient of $\eta(1)$ in $\eta(X)\eta((X)^{(-1)})$ are, respectively, 17 and 5.

Case 3: Assume that $n = 13a$ for some positive integer a.

There exists an element $h \in \mathrm{supp}(X)$ such that $13|\mathrm{o}(h)$ as A is proper. As $|\theta(h, 3)|$ cannot be 6, $\mathrm{o}(h) = 13$ or 26. Since $|\theta(h, 3)| = 3$ and there are at most two elements f in G/P such that $f^3 = f$, we have

$$X = 2x - y - y^3 \pm \theta(h, 3),$$

where $y \in G/P$ and $\mathrm{o}(y) = 4$ or 8. Let $\chi \in G^*$ such that $\chi(y) = -1$ and $\chi(h) = 1$. Thus, $\chi(x) = 1$. Then we have $\chi(X) = \chi(X^{(-1)}) = 4 \pm 3$. Hence $XX^{(-1)} \neq 9$.

Thus $w = 2^3 = 8$. $\square$

By Theorems 9 and 13, we have proved Theorem 3.

Acknowledgment

M.H. Ang wants to thank Universiti Sains Malaysia for the financial support under the Academic Staff Training Scheme that gives her the opportunity to pursue a Ph.D. degree from National University of Singapore.

References

[1] M.H. Ang, Group weighing matrices, Ph.D. Thesis, National University of Singapore, Singapore, 2003.
[2] K.T. Arasu, J.F. Dillon, in: Perfect Ternary Arrays: Different Sets, Sequences and their Correlation Properties, NATO Advanced Science Institute Series C Mathematical and Physical Sciences, vol. 542, Kluwer Academic Publishers, Dordrecht, 1999, pp. 1–15.
[3] K.T. Arasu, S.L. Ma, Some new results on circulant weighing matrices, J. Algebraic Combin. 14 (2001) 91–101.
[4] K.T. Arasu, J. Seberry, Circulant weighing designs, J. Combin. Designs 4 (1996) 439–447.
[5] K.T. Arasu, J. Seberry, On circulant weighing matrices, Australasian J. Combin. 17 (1998) 21–37.
[6] R.C. Mullin, A note on balanced weighing matrices, in 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.
[7] Y. Strassler, The classification of circulant weighing matrices of weight 9, Ph.D. Thesis, Bar-Ilan University, Israel, 1998.