Study of proper circulant weighing matrices with weight 9

Miin Huey Ang\textsuperscript{a}, K.T. Arasu\textsuperscript{b,1}, Siu Lun Ma\textsuperscript{c,2}, Yoseph Strassler\textsuperscript{d}

\textsuperscript{a}Pusat Pengajian Sains Matematik, Universiti Sains Malaysia, Minden 11800, Penang, Malaysia
\textsuperscript{b}Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435, USA
\textsuperscript{c}Department of Mathematics, National University of Singapore, Kent Ridge, Singapore 119260, Republic of Singapore
\textsuperscript{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.

© 2007 Elsevier B.V. All rights reserved.

Keywords: Weighing matrices; Characters

1. Introduction

A \textit{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

\[ MM^T = m^2 I, \]

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 \( A = \sum_{i=1}^{n} a_i g_i, a_i \in \mathbb{Z} \), be an element of the group ring \( \mathbb{Z}[G] \). 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 \( A \in \mathbb{Z}[G] \) 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

\[ 0012-365X/S - see front matter © 2007 Elsevier B.V. All rights reserved. \
\textit{doi}:10.1016/j.disc.2004.12.029 \]
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 $\text{supp}(A) = \{g_i | a_i \neq 0\}$. 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 $o(g) = 26$. 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 $\rho : G \rightarrow G/\langle g^{13} \rangle$ be the natural epimorphism. It can be shown that $\rho(A)$ is a proper $CW(13, 9)$. Here $o(g)$ denotes the order of $g$.

**Example 2.** Let $G = \langle h \rangle \times \langle g \rangle$ where $o(h) = 3$ and $o(g) = 8$. 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 $\text{Ord}_p(n)$ to be the smallest positive integer $e$ such that $p^e \equiv 1 \mod n$ or in other words, $e$ is the smallest positive integer such that $p^e - 1 \equiv 0 \mod n$. For an element $h$ of a group, $\text{Ord}(h, p)$ 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 $\tau_K$ 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 $Z[G]$.

**Proposition 4.** Let $G$ be a finite group, $K$ a normal subgroup of $G$ and $k$ an integer. If $A \in Z[G]$ 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 $A \in Z[G]$ is such that $AA^{(-1)} = p^{2u}$, 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 $A = \sum_{i=1}^s a_i X_i \in Z[G]$, where $a_1, a_2, \ldots, a_s$ are distinct non-zero integers, be such that $AA^{(-1)} = p^{2u}$ 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 $p - 1, p^2 - 1, \ldots, p^n - 1$ 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 $(gA)(gA)^{(-1)} = p^{2u}$ and the support of $gA$ is not contained in any coset of any proper subgroup of $G$. Also $A = \sum_{i=1}^s a_i g X_i$ where $g X_1, g X_2, \ldots, g X_s$
are pairwise disjoint subsets of $G$. By Lemma 5, WLOG we can assume that $|X_1| \geq |X_i|$ for all $i \geq 2$. Let $h \in \text{supp}(gA)$. As $(gA)^{(p)} = gA$, if $h \in gX_i$, then $\theta(h, p) \subseteq gX_i$. Thus for all $h \in \text{supp}(gA)$,

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

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

**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 $i \geq 2$. Let $A = \sum_{i=1}^{s} a_i X_i \in \mathbb{Z}[G]$, where $a_1, a_2, \ldots, a_s$ are distinct nonzero integers, be such that $\text{A}(\text{A}^{-1}) = p^{2r}$ and $A^{(p)} = A$. If $q$ is a prime divisor of $n$ such that $q^f | n$ and $\text{Ord}_{q^f}(p) > |X_i|$ for all $i \geq 2$, 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 $C \in \mathbb{Z}[G]$ where $\text{supp}(C)$ is contained in the proper subgroup $K = \{ g \in G | q^f \text{ does not divide } o(g) \}$ of $G$.

**Proof.** For any $h \in \text{supp}(A)$, if $q^f | o(h)$, then $|\theta(h, p)| \geq \text{Ord}_{q^f}(p)$. This implies that $h \in \text{supp}(X_1)$ 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 $h_1, h_2, \ldots, h_d \in \text{supp}(X_1)$ and $C \in \mathbb{Z}[G]$ where $\text{supp}(C) \subseteq K$. □

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 $A \in \mathbb{Z}[G]$ 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 $h \in \text{supp}(X_i)$, then $\theta(h, 3) \subseteq \text{supp}(X_i)$ 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

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

$$3^2 - 1 = 2^3 \quad \Rightarrow \quad \text{Ord}_2 3 = \text{Ord}_2 3 = 2;$$

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

$$3^4 - 1 = 2^4 \times 5 \quad \Rightarrow \quad \text{Ord}_{24} 3 = \text{Ord}_5 3 = \text{Ord}_{2^4 \times 5} 3 = 4;$$

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

$$3^6 - 1 = 13 \times 7 \times 2^3 \quad \Rightarrow \quad \text{Ord}_7 3 = \text{Ord}_{7 \times 2^3} 3 = \text{Ord}_{7 \times 2^3} 3 = \text{Ord}_{7 \times 2^3} 3 = \text{Ord}_{7 \times 2^3} 3 = 6.$$
Case 1: Assume that \( n = 11a \) for some integer \( a \).

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

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

Then

\[
\tau_H(gA) = \tau_H(C) + 5x,
\]

where \( x \in G/H, \text{o}(x) = 1 \) or 2 and the coefficients of \( \tau_H(C) \) are 0, \pm 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 \( h \in \text{supp}(gA) \) such that \( m | \text{o}(h) \) 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 \( \text{supp}(C) \subseteq K = \{ g \in G | m \text{ does not divide } \text{o}(g) \} \). Let \( H \) be a subgroup of \( G \) such that

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

Then

\[
\tau_H(gA) = \begin{cases} 
-1 + 4\tau_H(h) & \text{if } \text{o}(h) = 2^4, \\
-1 + 0(\tau_H(h), 3) & \text{if } \text{o}(h) = 5, \\
-3 + 0(\tau_H(h), 3) & \text{if } \text{o}(h) = 7,
\end{cases}
\]

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

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

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

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

where \( X, Y \subseteq G/P \) such that \( |X| = 6 \text{ and } |Y| = |Z| = 3 \). 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 \( 13 | \text{o}(h_2) \). If \( \text{o}(h_2) = 52 \) or 104, then

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

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 \( \text{o}(h_2) = 13 \) or 26. Since \( A \) is proper, \( X_1 = g_1 + \theta(g_2, 3) + \theta(h_2, 3) \) where \( \text{o}(g_1) = 1 \text{ or } 2, \theta(g_2) = 4 \text{ or } 8 \) and
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 \( P = \langle z \rangle, o(z) = 3, \) and \( |H| \) is not a multiple of 3. Let \( A \in \mathbb{Z}[G] \) be such that \( AA^{(-1)} = 9 \). Then for \( t \equiv 2 \) mod 3 and \( t \equiv 1 \) mod \( |H| \), there exists an integer \( b \) such that

\[
(x^b A)^{(t)} = \beta(x^b A) + \varepsilon(1 - \beta)Pg
\]

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

We first consider the case when \( o(\beta) = 2 \).

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

\[
A^{(t)} = \beta A + (1 - \beta)Pg
\]

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

\[
A_h = a_h(1 + \beta) + a_{h_2}(x + x^2) + a_{h_2^2}(x^2 + \beta x) \quad \text{for } Kh \neq Kg
\]

and

\[
A_g = a_g + (a_{g_1} - 1)\beta + a_{g_2}x + (a_{g_2} - 1)x^2\beta + a_{g_2^2}x^2 + (a_{g_2^2} - 1)\beta x.
\]

In particular, if the coefficients of \( A \) are 0, 1, then \( a_g, a_{g_1}, a_{g_2} \in \{0, 1\} \) and \( |\text{supp}(A_g)| = 3 \).

Proof. First, we consider \( A_h \) where \( Kh \neq Kg \). In this case \( A_h^{(t)} = \beta A_h \). Note that if \( A_h = a_h + a_h\beta x + a_{h_2}x^2 + a_{h_2^2}x^2\beta + a_{h_2^2}\beta x + a_{h_2^2}\beta x^2 \), then

\[
\beta A_h = a_h\beta + a_h\beta x + a_{h_2}\beta x^2 + a_{h_2^2}\beta x^2 + a_{h_2^2}\beta x^2\beta,
\]

\[
A_h^{(t)} = a_h + a_h\beta x + a_{h^2}\beta x^2 + a_{h_2^2}\beta x^2 + a_{h_2^2}\beta x^2\beta.
\]

By comparing the coefficients of Eqs. (6) and (7), we know that \( a_h, a_{h_2}, a_{h_2^2} = a_{h_2^2} \) and \( a_{h_2}, a_{h_2^2} = a_{h_2^2} \). Thus

\[
A_h = a_h(1 + \beta) + a_{h_2}(x + x^2) + a_{h_2^2}(x^2 + \beta x).
\]

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

\[
A_g^{(t)} = \beta A_g + (1 - \beta)P.
\]
This implies that \( a_g = a_g \beta + 1, a_g x^2 = a_g \beta x + 1 \) and \( a_g x = a_g x^2 + 1 \). Hence

\[
A_g = a_g + (a_g - 1) \beta + a_g x + (a_g - 1) x^2 \beta + a_g x^2 + (a_g x^2 - 1) x \beta.
\]

If the coefficients of \( A \) are 0, ±1, it is obvious that \( a_g, a_g x, a_g x^2 \) cannot be -1 and hence \(|\text{supp}(A_g)| = 3\). □

**Lemma 12.** Let \( G = P \times H \) be a cyclic group where \( P = \langle \alpha \rangle, \) \( \alpha(\alpha) = 3, \) and \( |H| \) is not a multiple of 3. If \( A \in \mathbb{Z}[G] \) is a proper CW\((n, 9)\) where coefficients of \( B, C, D, E \) are 0, ±1, and the supports of \( B, C, D, E \) are pairwise disjoint.

**Proof.** By Lemma 10, for \( t \equiv 2 \mod 3 \) and \( t \equiv 1 \mod |H| \), there exists an integer \( b \) such that

\[
(\alpha^b A)^{(t)} = \beta(\alpha^b A) + \varepsilon(1 - \beta) P g,
\]

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

\[
A^{(t)} = \beta A + (1 - \beta) P g.
\]

Suppose \( \alpha(\beta) = 2 \). 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 \( g A = X_1 - X_2 \) where \( X_1, X_2 \) are disjoint subsets of \( G \) such that \(|X_1| = 6\) and \(|X_2| = 3\). Since all elements in \( A_g \) with coefficients +1 and -1 for \( K h \neq K g \) 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 \( g \notin \text{supp}(X) \). 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 \( \tau_K(A) \tau_K(A)^{(-1)} = 13 \) 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,

\[
A = Y_0 + P Y_1,
\]

where \( Y_0, Y_1 \in \mathbb{Z}[G] \). Let \( A = \sum_{h \in J} B_h h \) where \( J \) is the complete set of coset representatives of \( P \) and \( B_h \in \mathbb{Z}[P] \). For \( h \in J, B_h = \delta + \eta(\alpha + x^2) \) 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 \( h \in \text{supp}(B) \); if \( \delta = 0 \) and \( \eta = \pm 1 \), then \( h \in \text{supp}(C) \); if \( \delta = -\eta = \pm 1 \), then \( h \in \text{supp}(D) \); and if \( \delta = \eta = \pm 1 \), then \( h \in \text{supp}(E) \). □
Theorem 13. If n is a multiple of 3, then there exists a proper $\text{CW}(n, 9)$ if and only if $n = 24$.

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

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

where $B, C, D, E \in \mathbb{Z}[H]$, 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 $x$ in $AA(\langle -1 \rangle) = 9$, we obtain

$$|\text{supp}(C)| - |\text{supp}(D)| + 3|\text{supp}(E)| = 0.$$  \hspace{1cm} (11)

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

$$|\text{supp}(\tau_P(B))| + 5|\text{supp}(\tau_P(C))| = 9.$$  \hspace{1cm} (12)

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

$$\tau_P(A) = \tau_P(B) + 2\gamma h_1 + \varepsilon h_2,$$  \hspace{1cm} (12)

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

$$(g\tau_P(A))(\langle 3 \rangle) = g\tau_P(A).$$

Let us write

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

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

$$X(\langle 3 \rangle) = X \text{ and } XX(\langle -1 \rangle) = 9.$$  \hspace{1cm} (13)

By $X(\langle 3 \rangle) = X$, we get $o(x) = 1$ or 2. By $XX(\langle -1 \rangle) = 9$, we get

$$4 + |X_1| + |X_2| = 9 \quad \text{and} \quad 2 + |X_1| - |X_2| = \pm 3.$$  \hspace{1cm} (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 $h \in \text{supp}(X)$ such that $11|o(h)$ 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),

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

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

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

There exists an element $h \in \text{supp}(X)$ such that $m|o(h)$ 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 $y \in G/P$, $o(y) = 1$ 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

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

where \( \eta : G/P \rightarrow (G/P)/K \) 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 \( h \in \text{supp}(X) \) such that \( 13|o(h) \) as \( A \) is proper. As \( |\theta(h, 3)| \) cannot be 6, \( o(h) = 13 \) 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 \( o(y) = 4 \) 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