Chapter 1

Introduction to Group Weighing Matrices

In this chapter, we shall first study the history of group weighing matrices followed by some of their basic properties. Then we shall discuss an application of group weighting matrices, namely, perfect ternary sequences and arrays. Lastly, some results regarding character theory that will be used heavily throughout our discussion will be introduced.

1.1 Weighing Matrices

Let M be a square matrix of order n. Let I_n be the $n \times n$ identity matrix. A *weighing matrix* of order n and weight w, denoted by $W(n, w)$, is a square matrix M of order n with entries from $\{-1, 0, 1\}$ such that

$$MM^T = wI_n$$

where M^T is the transpose of M.

Weighing matrices can be regarded as a generalization of the well-known Hadamard matrices $H(w)$, where Hadamard matrices have only ± 1 entries and $n = w$. Let $M = (m_{ij})$ be a $W(n, w)$. If $m_{ij} = m_{1,j-i+1}$ for all i and j where $j-i+1$ is reduced modulo n, then M is called a *circulant weighing matrix*.

Example 1.1.1 *Let* $M_1 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ *and* $M_2 = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}$. *Then it can be checked that* $M = \begin{pmatrix} M_1 & M_2 \\ M_2 & -M_1 \end{pmatrix}$ *is a* $W(6,5)$.

Example 1.1.2 *Let* M *be the following matrix:*

$$\begin{pmatrix} -1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & -1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & -1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & -1 \end{pmatrix}.$$

It is a circulant weighing matrix with $MM^T = 4I_7$.

In 1960, Statisticians were the first to become interested in weighing matrices due to its application in finding optimal solutions to the problem of weighing objects. You may refer to [47] and [48] for further details and insights on why these matrices have been termed weighing matrices. Later in 1975, Sloane and Harwitt in [50] further indicated that weighing designs are also applicable to other problems of measurements such as length, voltages, resistances, concentrations of chemical etc.. In section 1.3, we shall learn that certain types of weighing matrices, are equivalent to perfect sequences and arrays that are used in the area of digital communication.

1.2 Group Weighing Matrices

Recently, a group ring approach has been introduced to study weighing matrices, see [2, 5, 7, 29]. As a consequence, finite group representation theory has become an important tool in studying weighing matrices under this new approach.

Let G be a finite group and let $\boldsymbol{R} = \mathbb{Z}$ or $\mathbb{C}$ (in more general situations, $\boldsymbol{R}$ is a commutative ring with 1). Let $\boldsymbol{R}[G]$ be the set of all the formal sums $\sum_{g \in G} \alpha_g g$ where $\alpha_g \in \boldsymbol{R}$ with the addition and multiplication defined as follows:

For all $\sum_{g\in G}\alpha_g g$, $\sum_{g\in G}\beta_g g \in \boldsymbol{R}[G]$,

$$\sum_{g\in G}\alpha_g g + \sum_{g\in G}\beta_g g = \sum_{g\in G}(\alpha_g+\beta_g)g,$$
$$\left(\sum_{g\in G}\alpha_g g\right)\left(\sum_{g\in G}\beta_g g\right) = \sum_{g\in G}\left(\sum_{h\in G}\alpha_{gh^{-1}}\beta_h\right)g.$$

Then $\boldsymbol{R}[G]$ is called a *group ring*. For any $t \in \mathbb{Z}$ and $A = \sum_{g\in G} a_g g \in \boldsymbol{R}[G]$, we define $A^{(t)} = \sum_{g\in G} a_g g^t$. Also, we use $\mathrm{supp}(A) = \{g \in G \mid a_g \neq 0\}$ for $A = \sum_{g\in G} a_g g \in \boldsymbol{R}[G]$ to denote the support of A.

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 $\boldsymbol{R}[G]$. Let $\bar{G}$ be a finite group too. For any group homomorphism ϕ from G to $\bar{G}$, we shall extend it to a ring homomorphism from $\boldsymbol{R}[G]$ to $\boldsymbol{R}[\bar{G}]$ such that for $A = \sum_{g\in G} a_g g \in \boldsymbol{R}[G]$, $\phi(A) = \sum_{g\in G} a_g \phi(g) \in \boldsymbol{R}[\bar{G}]$.

Lemma 1.2.1 *Let $G = \{g_1, g_2, \ldots, g_n\}$ be a group of order n. Let $\Phi : G \longrightarrow GL(n, \mathbb{C})$ be the regular representation of G such that for $g \in G, \Phi(g) = (\Phi(g)_{ij})$ where*

$$\Phi(g)_{ij} = \begin{cases} 1 & \text{if } g_i g_j^{-1} = g, \\ 0 & \text{otherwise.} \end{cases}$$

Then Φ is a one to one function with $\Phi(g^{(-1)}) = \Phi(g)^T$.

The proof of the above lemma can be found in [22].

Proposition 1.2.2 *Let $G = \{g_1, g_2, \ldots, g_n\}$ be a group of order n. Suppose $A = \sum_{i=1}^{n} a_i g_i \in \mathbb{Z}[G]$ satisfies*

(W1) *A has $0, \pm 1$ coefficients and*

(W2) *$AA^{(-1)} = w$.*

Then the group matrix $M = (m_{ij})$, where $m_{ij} = a_k$ if $g_i {g_j}^{-1} = g_k$, is a $W(n, w)$.

Proof Let $\Phi : G \longrightarrow GL(n, \mathbb{C})$ be the regular representation of G such that for $g \in G, \Phi(g) = (\Phi(g)_{ij})$ where

$$\Phi(g)_{ij} = \begin{cases} 1 & \text{if } g_i g_j^{-1} = g, \\ 0 & \text{otherwise.} \end{cases}$$

Clearly $M = \Phi(A)$. Thus by Lemma 1.2.1,

$$\begin{aligned} MM^T &= \Phi(A)\Phi(A)^T \\ &= \Phi(A)\Phi(A^{(-1)}) \\ &= \Phi(AA^{(-1)}) \\ &= \Phi(w) \\ &= wI_n. \end{aligned}$$ □

A weighing matrix constructed in Proposition 1.2.2 is called a *group weighing matrix* and shall be denoted as $W(G, w)$. If $G = \{g_1, \cdots, g_n\}$ is a cyclic group such that $g_i = g_2^{i-1}$, then M is a circulant weighing matrix. There are quite a number of work recently done on circulant weighing matrices [5, 7, 8, 29, 30].

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 $W(G, w)$ if it satisfies conditions (W1) and (W2) given in Proposition 1.2.2. In particular, if A has only ± 1 coefficients, M is a group Hadamard matrix and we say that A is an $H(G, w)$. When G is cyclic, then A is called a $CW(n, w)$.

Remark 1.2.3 *Let G be a finite group having H as a subgroup.*

1. *If $A \in \mathbb{Z}[H]$ is a $W(H, w)$, then A is also a $W(G, w)$.*

2. *If A is a $W(G, w)$, then it is clear that both Ag and gA are also $W(G, w)$ for any $g \in G$.*

Let $A \in \mathbb{Z}[G]$ be a $W(G,w)$. If the support of A is contained in a coset of a proper subgroup H in G, we say that A is a *trivial extension* of a $W(H,w)$. If A is not a trivial extension of any $W(H,w)$ for $H \lneqq G$, A is called a *proper* $W(G,w)$. Note that $Hg = g(g^{-1}Hg)$. Thus a right coset Hg of H in G is a left coset of $g^{-1}Hg$ in G. So we only need to check left cosets.

Throughout this thesis, we shall use C_n to denote a cyclic group of order n.

Example 1.2.4 *Let $G = \langle a \rangle \cong C_7$. Let $A = -1 + a + a^2 + a^4 \in \mathbb{Z}[G]$. Clearly $AA^{(-1)} = 4$. Thus, A is a proper $CW(7,4)$ with the weighing matrix as given in Example 1.1.2*

Example 1.2.5 *Let $G = \langle b \rangle \times \langle c \rangle \cong C_3 \times C_6$ where $o(b) = 3$ and $o(c) = 6$. Let $A = -1 + c + c^2 + c^4 + c^5 + bc^2 + b^2c^4 - b^2c - bc^5 \in \mathbb{Z}[G]$. It can be shown that A is a proper $W(G,9)$ and with a suitable arrangement of the elements of G, the corresponding weighing matrix has the form $\begin{pmatrix} \Gamma_1 & \Gamma_2 & \Gamma_3 \\ \Gamma_3 & \Gamma_1 & \Gamma_2 \\ \Gamma_2 & \Gamma_3 & \Gamma_1 \end{pmatrix}$ where*

$$\Gamma_1 = \begin{pmatrix} -1 & 1 & 1 & 0 & 1 & 1 \\ 1 & -1 & 1 & 1 & 0 & 1 \\ 1 & 1 & -1 & 1 & 1 & 0 \\ 0 & 1 & 1 & -1 & 1 & 1 \\ 1 & 0 & 1 & 1 & -1 & 1 \\ 1 & 1 & 0 & 1 & 1 & -1 \end{pmatrix}, \Gamma_2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & -1 \\ -1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 \end{pmatrix}, \Gamma_3 = {\Gamma_2}^T.$$

Note that Γ_i are circulant matrices for all i.

Remark 1.2.6 *In general, the group weighing matrix of abelian group $G \cong C_n \times C_m$ can be arranged in the form of $\begin{pmatrix} \Gamma_1 & \Gamma_2 & \cdots & \Gamma_n \\ \Gamma_n & \Gamma_1 & \cdots & \Gamma_{n-1} \\ \vdots & \vdots & & \vdots \\ \Gamma_2 & \Gamma_3 & \cdots & \Gamma_1 \end{pmatrix}$ where Γ_i are $m \times m$ circulant matrices for all i. This family of matrices is called block circulant matrix. Particularly if $n = 2$, then the group weighing matrixes are called double circulant matrix.*

We shall now prove an important basic property of group weighing matrices.

Proposition 1.2.7 *Let G be a finite group of order n and A be a $W(G, w)$. Then $w = \nu^2$ for some positive integer ν. Furthermore, the number of $+1$ coefficients of A is equal to $(\nu^2 \pm \nu)/2$ and the number of -1 coefficients of A is equal to $(\nu^2 \mp \nu)/2$.*

Proof Define

$$\Psi_1 : G \longrightarrow \mathbb{C}$$

as the principal representation of G, i.e. $\Psi_1(g) = 1$ for every $g \in G$.

Let $A = \sum_{g \in G} a_g g \in \mathbb{C}[G]$. Then

$$w = \Psi_1(AA^{(-1)}) = \Psi_1(A)\Psi_1(A^{(-1)}) = \Psi_1(A)^2 = \Psi_1(A^{(-1)})^2$$

implies that $w = \nu^2$ for some $\pm\nu = \Psi_1(A) \in \mathbb{Z}$.

Let $A^+ = \{g \in G \mid a_g = 1\}$ and $A^- = \{g \in G \mid a_g = -1\}$. Then

$$\pm\nu = \Psi_1(A) = \Psi_1(A^{(-1)}) = \sum_{g \in G} a_g = |A^+| - |A^-|. \tag{1.1}$$

Comparing the coefficient of identity in $AA^{(-1)} = w$. Obviously,

$$|A^+| + |A^-| = \sum_{g \in G} {a_g}^2 = \nu^2. \tag{1.2}$$

By solving the equations (1.1) and (1.2), we will get

$$|A^+| = \frac{\nu^2 \pm \nu}{2} \text{ and } |A^-| = \frac{\nu^2 \mp \nu}{2}.$$

□

1.3 Perfect Ternary Sequences and Arrays

Let $\mathbf{a} = (a_0, a_1, \cdots, a_{n-1})$ be an $0, \pm 1$ sequence, then $\mathbf{a}$ is called a *ternary sequence*. Let s be any nonnegative integer. The value

$$Aut_{\mathbf{a}}(s) = \sum_{i=0}^{n-1} a_i a_{i+s \bmod n}$$

is called a *periodic autocorrelation coefficient* of $\mathbf{a}$. If $s \not\equiv 0 \mod n$, then the coefficient is called *out of phase*. In a lot of engineering applications, such as signal processing, synchronizing and measuring distances by radar, sequences with small out of phase autocorrelation coefficients (in absolute values) are required. The ideal situation is that $Aut_{\mathbf{a}}(s) = 0$ for all $s \not\equiv 0 \bmod n$. Such a sequence is called a *perfect ternary sequence*.

Example 1.3.1 *Let* $\mathbf{a} = \begin{pmatrix} -1 & 1 & 1 & 1 \end{pmatrix}$ *and* $\mathbf{b} = \begin{pmatrix} -1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$. *Each is a ternary sequence. Both* $\mathbf{a}$ *and* $\mathbf{b}$ *are perfect ternary sequences as*

$$Aut_{\mathbf{a}}(s) = \sum_{i=0}^{4-1} a_i a_{i+s \bmod 4} = \begin{cases} 4 & \text{if } s \equiv 0 \bmod 4, \\ 0 & \text{if } s \not\equiv 0 \bmod 4. \end{cases}$$

and

$$Aut_{\mathbf{b}}(s) = \sum_{i=0}^{7-1} a_i a_{i+s \bmod 7} = \begin{cases} 4 & \text{if } s \equiv 0 \bmod 7, \\ 0 & \text{if } s \not\equiv 0 \bmod 7. \end{cases}$$

Let $\mathbf{a} = \begin{pmatrix} a_0 & a_1 & \cdots & a_n \end{pmatrix}$ and $A = \sum_{i=0}^{n-1} a_i g^i \in \mathbb{Z}[G]$ where $G = \langle g \rangle$ is a cyclic group of order n. Then it is clear that each $Aut_{\mathbf{a}}(s)$ is the coefficient of g^s in $AA^{(-1)}$. Hence the existence of a perfect ternary sequence is equivalent to the existence of a circulant weighing matrix.

At first, engineers were looking for binary sequences (i.e. ± 1 sequences) with perfect periodic correlation. Unfortunately, the only example we know so far is the sequence $\mathbf{a}$ in Example 1.3.1, see [52]. Later, they started to look for ternary sequences. Perfect ternary sequences were known in the literature since 1967 [15]. In 70's-80's, a lot of example of perfect ternary sequences were constructed [23, 25, 32, 42].

Let $\Pi = (\pi_{(j_1, j_2, \cdots, j_r)})_{0 \le j_i < s_i, 1 \le i \le r}$ be an r dimensional $s_1 \times s_2 \times \cdots \times s_r$ array. If each entry of Π takes the value of 0 and ± 1 only, then Π is called a ternary array. Let $u_1, u_2, \cdots, u_r$ be nonnegative integers. A periodic autocorrelation coefficient

of Π is defined as

$$Aut_{\Pi}(u_1, u_2, \cdots, u_r) = \sum_{j_1=0}^{s_1-1} \cdots \sum_{j_r=0}^{s_r-1} \pi_{(j_1,j_2,\cdots,j_r)}\pi_{(j_1+u_1 \bmod s_1, j_2+u_2 \bmod s_2, \cdots, j_r+u_r \bmod s_r)}.$$

Let $\Upsilon = \{(u_1, u_2, \cdots, u_r) \mid \text{there exists an } i \text{ such that } u_i \not\equiv 0 \mod s_i\}$. If $Aut_{\Pi}(u_1, u_2, \cdots, u_r) = 0$ for all $\mathbf{u} = (u_1, u_2, \cdots, u_r) \in \Upsilon$, then Π is called a *perfect ternary array* denoted as PTA. The number of nonzero entries in Π are called the *energy* of Π, denoted by $e(\Pi)$.

Let $A = \sum_{j_1=0}^{s_1-1} \cdots \sum_{j_r=0}^{s_r-1} \pi_{(j_1,j_2,\cdots,j_r)} {g_1}^{j_1} \cdots {g_r}^{j_r} \in \mathbb{Z}[G]$ where $G = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \langle g_r \rangle$ is an abelian group isomorphic to $C_{s_1} \times C_{s_2} \times \cdots \times C_{s_r}$. Note that each $Aut_{\Pi}(u_1, u_2, \cdots, u_r)$ is the coefficient of ${g_1}^{u_1} \cdots {g_r}^{u_r}$ in $AA^{(-1)}$. The readers may refer to [2] for the detail of the following result.

Proposition 1.3.2 *The existence of an r dimensional $s_1 \times s_2 \times \cdots \times s_r$ PTA with $e(\Pi) = w$ is equivalent to the existence of a $W(G, w)$ where G is isomorphic to $C_{s_1} \times C_{s_2} \times \cdots \times C_{s_r}$.*

Note that the perfect ternary sequence $\mathbf{b}$ given in Example 1.3.1 is a one dimensional ternary array that is equivalent to the circulant weighing matrix given in Example 1.2.4.

Example 1.3.3 *Let* $\Pi = \begin{pmatrix} -1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & -1 & 0 & 0 & 1 & 0 \end{pmatrix}$ *be a 2 dimensional ternary array that is equivalent to the group weighing matrix given in Example 1.2.5. Note that* Π *is a perfect ternary sequence with*

$$Aut_{\Pi}(u_1, u_2) = \sum_{j_1=0}^{2} \sum_{j_2=0}^{5} \pi_{(j_1,j_2)}\pi_{(j_1+u_1 \bmod 3, j_2+u_2 \bmod 6)} \begin{cases} 9 & \text{if } (u_1, u_2) \notin \Upsilon, \\ 0 & \text{if } (u_1, u_2) \in \Upsilon. \end{cases}$$

Arrays with perfect periodic correlation function are also found to have applications in higher dimensional engineering problems [32, 33, 37]. Similar to sequences, at first binary case is of special interest due to some technical and

theoretical aspects. However perfect binary arrays only exist in small numbers [12, 13, 14, 27, 34, 55]. In 1990, Antweiler, Bömer and Lüke started to consider perfect arrays with $0, \pm 1$ entries and they found that the number of perfect arrays increase if the arrays are allowed to have more degrees of freedom [1, 2]. For more details on ternary arrays, the readers may refer to [2].

1.4 Character Theory

In this thesis, most of the discussions will be on abelian group. It is well known that all irreducible representations of an abelian group are essentially the characters of the group. Thus, characters will play an important role throughout our discussion. In this section, we shall discuss in brief those results of character theory that will be heavily used throughout our discussion.

Let G be an abelian group and G^* be the set of all characters of G. Then G^* is a group with respect to the multiplication defined as follows: for any $\chi_1, \chi_2 \in G^*$, $\chi_1\chi_2$ is a character of G that maps g to $\chi_1(g)\chi_2(g)$ for all $g \in G$. The *principal character* of G denoted by χ_0 is the identity of G^* that maps all g in G to 1. Any character of G is called *nonprincipal* if it is not the principal character. Furthermore, it can be shown that $G \cong G^*$.

Theorem 1.4.1 ***(Fourier Inversion Formula)*** *Let G be a finite abelian group and G^* be the group of all characters of G. Let $A = \sum_{g \in G} \alpha_g g \in \mathbb{C}[G]$. Then*

$$\alpha_g = \frac{1}{|G|} \sum_{\chi \in G^*} \chi(A)\chi(g^{-1}).$$

Corollary 1.4.2 *Let G be an abelian group and $A, B \in \mathbb{Z}[G]$. Then $A = B$ if and only if $\chi(A) = \chi(B)$ for all $\chi \in G^*$.*

The proof of Theorem 1.4.1 can be found in [11]. Corollary 1.4.2 links between the characters of an abelian group G and its group weighing matrices $W(G, w)$.

Proposition 1.4.3 *Let G be a finite abelian group. For any $A \in \mathbb{Z}[G]$ with $0, \pm 1$ coefficients, A is a $W(G, w)$ if and only if $\chi(A)\overline{\chi(A)} = w$ for all $\chi \in G^*$.*

The *finite Fourier transform* is a mapping from $\mathbb{C}[G]$ to $\mathbb{C}[G^*]$ such that it maps $A \in \mathbb{C}[G]$ to

$$\widehat{A} = \sum_{\chi \in G^*} \chi(A)\chi \in \mathbb{C}[G^*].$$

Define $\tau_g(\chi) = \chi(g)\ \forall g \in G$. It can be shown that $\{\tau_g \mid g \in G\} = G^{**}$. By identifying the element τ_g in G^{**} with $g \in G$, we can regard G as the group of characters of G^*. The following result on finite Fourier transform will be used while we discuss symmetric group weighing matrices in chapter 5.

Proposition 1.4.4 *Let G be a finite abelian group and $A \in \mathbb{C}[G]$. Then $\widehat{\widehat{A}} = |G|A^{(-1)}$.*

Below are other important results on character theory that will be frequently used throughout our discussion. We refer to [11] for the proof of the next lemma.

Lemma 1.4.5 ***(Ma's Lemma)*** *Let p be a prime, and let G be a finite abelian group with a cyclic Sylow p-subgroup. If $A \in \mathbb{Z}[G]$ satisfies $\chi(A) \equiv 0 \bmod p^t$ for all characters χ of G, then there exist $X_1, X_2 \in \mathbb{Z}[G]$ such that*

$$A = p^t X_1 + P X_2$$

where P is the unique subgroup of G of order p.

For any positive integer v, we use ζ_v to denote the complex vth root of unity $e^{2\pi\sqrt{-1}/v}$.

Lemma 1.4.6 *Let G be an abelian group and $A \in \mathbb{Z}[G]$ such that $\chi(A)$ are rational for all $\chi \in G^*$, then $A^{(t)} = A$ for all integers t relatively prime to $|G|$.*

Proof Let v be the exponent of G and let t be an integer relatively prime to v. The mapping $\sigma : \zeta_v \mapsto \zeta_v^t$ is an element of $Gal(\mathbb{Q}(\zeta_v)/\mathbb{Q})$. Let χ be any character of G. We have $\chi(A^{(t)}) = \sigma(\chi(A)) = \chi(A)$. So $A^{(t)} = A$. □

Let G be an abelian group of order n and let t be an integer with $(t, n) = 1$. Let $A \in \mathbb{Z}[G]$. We say that t is a *multiplier* of A if $A^{(t)} = hA$ for some $h \in G$. Furthermore, we say that t is a multiplier that fixes A if $A^{(t)} = A$. By [10], we can always replace A with gA for some $g \in G$ such that $A^{(t)} = A$. Hence one may assume that t fixes A if t is a multiplier of A.

Let H be a subgroup of G. A character χ of G is called *principal on* H if $\chi(h) = 1$ for all $h \in H$; otherwise χ is called *nonprincipal on* H. The set $H^{\perp} = \{\chi \in G^* \mid \chi \text{ is principal on } H\}$ is a subgroup of G^* with $|H^{\perp}| = |G|/|H|$.

Chapter 2

Constructions of Group Weighing Matrices

In this chapter, we shall mainly study the constructions of group weighing matrices. Some of the constructions are new. Generally, the constructions will be divided into five categories.

2.1 Some Inductive Constructions of Group Weighing Matrices

The first example is a well known construction given in [2].

Construction 2.1.1 *Let H, G be finite groups. If there exists a $W(H, k_1)$ A and a $W(G, k_2)$ B, then AB is a $W(H \times G, k_1 k_2)$.*

Throughout the whole thesis, we shall denote (n_1, n_2) as the greatest common divisor of n_1 and n_2 and η_H be the natural epimorphism from G to G/H where G is a group having H as its subgroup.

The next construction is important as it provides most of the proper circulant weighing matrices of even weight.

Construction 2.1.2 *Let $G = \langle \alpha \rangle \times H$ be a group where $o(\alpha) = 2^s$. Suppose there exist $B \in \mathbb{Z}[H]$ and $C \in \mathbb{Z}[G/\langle \alpha^{2^{s-1}} \rangle]$ such that B is a $W(H, w)$ and C is*

a $W(G/\langle\alpha^{2^{s-1}}\rangle, w)$. *Let* $C_1 \in \mathbb{Z}[G]$ *such that* $\eta_{\langle\alpha^{2^{s-1}}\rangle}(C_1) = C$. *If there exists a* $g \in G$ *such that the supports of* B, $\alpha^{2^{s-1}}B$, gC_1 *and* $g\alpha^{2^{s-1}}C_1$ *are disjoint, then*

$$X = h[(1 - \alpha^{2^{s-1}})B + g(1 + \alpha^{2^{s-1}})C_1],$$

for any $h \in G$, *is a* $W(G, 4w)$.

For further details of the proof, please refer to [29].

Example 2.1.3 *Let* $G = \langle\alpha\rangle \times \langle\beta\rangle \cong C_{28}$ *where* $o(\alpha) = 4$ *and* $o(\beta) = 7$. *Choose* $B = -1 + \beta + \beta^2 + \beta^4$ *which is the* $CW(7, 4)$ *given in Example 1.2.4,* $g = \alpha$, $h = 1$ *and* $C_1 = \alpha^2\beta B$. *Clearly the supports of* B, $\alpha^2 B$, αC_1 *and* $\alpha^3 C_1$ *are disjoint. Thus by Construction 2.1.2,* X *is a proper* $CW(28, 16)$ *as* B *is proper and* $\alpha \in supp(X)$. *Inductively, we can construct proper* $CW(2^{2(r-1)} \cdot 7, 2^{2r})$ *for all* r.

2.2 Constructions Using Difference Sets

By [42], we know that some of the earliest examples of cyclic group weighing matrices are from difference sets. In fact in this section we shall show that a lot of proper group weighing matrices can be constructed from difference sets. Before we go deeper into the discussion, we need the following basic properties of difference sets. For the proofs of the properties of difference sets, please refer to [11].

Let G be a finite group of order n. Let $D \in \mathbb{Z}[G]$, $|D| = k$ and D has only coefficients 0 and 1. Then D is an (n, k, λ)-*difference set* if and only if D satisfies the group ring equation

$$DD^{(-1)} = k - \lambda + \lambda G. \tag{2.1}$$

Lemma 2.2.1 *If* D *is an* (n, k, λ)-*difference set, then*

$$k(k - 1) = \lambda(n - 1)$$

Corollary 2.2.2 *If D is an (n, k, λ)-difference set with $0 < k < n$ and $k - \lambda \leq \lambda$, then $k > \frac{n}{2}$.*

First, we have a well-known construction of group Hadamard matrices by using difference sets.

Construction 2.2.3 *Let D be a $(4m^2, 2m^2 - m, m^2 - m)$-difference set in a group G. Then $A = D - (G - D) = 2D - G$ is a proper $W(G, 4m^2)$.*

Remark 2.2.4 *In Construction 2.2.3, A has only ± 1 coefficients and hence A is an $H(G, 4m^2)$.*

Example 2.2.5 *Let $G = K \times \mathbb{Z}_{m_1}^2 \times \cdots \times \mathbb{Z}_{m_r}^2 \times \mathbb{Z}_{p_1}^4 \cdots \times \mathbb{Z}_{p_s}^4$ where K is an abelian group of order 2^{2d+2} and exponent at most 2^{d+2}, $d, m_1, \cdots, m_r$ are nonnegative integers such that $m_i = 3^{i_j}$ for some nonnegative integer i_j and $p_1, \ldots, p_s$ are odd primes. By Theorem 12.15 in Chapter VI of [11], we know that difference sets required by Construction 2.2.3 exist in G. Hence there exists a proper $W(G, 4m^2)$ where $m = 2^d 3^{i_1 + \cdots + i_r} p_1^2 \cdots p_s^2$.*

Construction 2.2.6 *Let $G = \langle \theta \rangle \times G'$ be a finite group where $o(\theta) = 2$. Suppose that G admits a $(|G|, k, \lambda)$-difference set $X \cup \theta Y$ where $X, Y \subseteq G'$. Then $X - Y$ is a $W(G', k - \lambda)$.*

Proof As the coefficient of each g in X and Y is either 0 or 1, $X - Y$ has coefficients 0, 1 and -1 only. Note that by Equation (2.1),

$$\begin{aligned}(X + \theta Y)(X + \theta Y)^{(-1)} &= XX^{(-1)} + YY^{(-1)} + \theta YX^{(-1)} + \theta XY^{(-1)} \\ &= k - \lambda + \lambda G' + \theta \lambda G'.\end{aligned}$$

Thus, by comparing coefficients, we get

$$XX^{(-1)} + YY^{(-1)} = k - \lambda + \lambda G' \quad \text{and} \quad YX^{(-1)} + XY^{(-1)} = \lambda G'.$$

Thus, we get $(X-Y)(X-Y)^{(-1)} = k-\lambda$ and the result follows. □

Theorem 2.2.7 *In Construction 2.2.6, suppose G is abelian, $k-\lambda > 1$ and let $A = X - Y$.*

1. *If $(n,k,\lambda) \neq (4m^2,\, 2m^2-m,\, m^2-m)$ for any even integer m, then A is a proper $W(G', k-\lambda)$.*

2. *If $(n,k,\lambda) = (4m^2,\, 2m^2-m,\, m^2-m)$ for some even integer m, then either A is a proper $W(G', m^2)$ or an $H(K, m^2)$ for a subgroup K of G' of index 2.*

Proof Assume that A, constructed in Construction 2.2.6, is not a proper $W(G', k-\lambda)$. Then there exists a proper subgroup K in G' such that

$$hD = S + \theta T + \langle\theta\rangle U$$

for some $h \in G'$, $S, T \subset K$, $U \subset G'$ and S, T, U are pairwise disjoint. Since $A = h^{-1}(S-T)$ is a $W(G', k-\lambda)$,

$$|S| + |T| = k - \lambda \;\text{ and }\; |U| = \frac{1}{2}(k - |S| - |T|) = \frac{\lambda}{2}.$$

Without the loss of generality, we can choose K to be a maximal subgroup of G' and thus $|K| = |G'|/p = n/(2p)$ for some prime divisor p of $n/2$. Note that $n = 2p|K| \geq 2p(|S| + |T|) = 2p(k-\lambda)$. Since

$$h(G \backslash D) = T + \theta S + \langle\theta\rangle(G \backslash (S \cup T \cup U)),$$

we can always assume that $k = |D| \leq n/2$ and hence $k - \lambda > \lambda$ by Corollary 2.2.2.

Let $U = \sum_{i=0}^{p-1} g_i W_i$ where $W_i \subset K$ and $\{g_0 = 1, g_1, \ldots, g_{p-1}\}$ is a complete set of coset representatives of K in G'. By comparing the sum of coefficients of elements in $G \backslash (\langle\theta\rangle \times K)$ in both sides of Equation (2.1), we have

$$4(|S| + |T|)(|U| - |W_0|) + 4\left(|U|^2 - \sum_{i=0}^{p-1} |W_i|^2\right) = \lambda\left(n - \frac{n}{p}\right).$$

This implies

$$\lambda^2 + 2\lambda(k-\lambda) - 4\left(\sum_{i=0}^{p-1}|W_i|^2 + (k-\lambda)|W_0|\right) = \lambda\left(n - \frac{n}{p}\right).$$

Thus $n/p > n - \lambda - 2(k-\lambda) = n - k - (k-\lambda)$. Since $n \geq 2p(k-\lambda)$ and $k \leq n/2$, we obtain $n/p > n(p-1)/(2p)$ and hence $p = 2$.

Now, let $x = |S| + |T| + 2|W_0| \geq |S| + |T| = k - \lambda$ and $y = 2|W_1| \leq 2(|W_0| + |W_1|) = 2|U| = \lambda$. Then

$$x + y = k \text{ and } 2xy = \lambda\left(n - \frac{n}{2}\right) = \frac{\lambda n}{2}$$

and hence $x, y = (k \pm \sqrt{k^2 - \lambda n})/2 = (k \pm \sqrt{k-\lambda})/2$ by Lemma 2.2.1. Since $x \geq k - \lambda > \lambda \geq y$, we have

$$x = \frac{k + \sqrt{k-\lambda}}{2}.$$

By $x \geq k - \lambda$ and $k^2 = \lambda n - \lambda + k$, we obtain $n \leq 4(k-\lambda)$. However, we know that $n \geq 2p(k-\lambda) = 4(k-\lambda)$. Hence $n = 4(k-\lambda)$ and by a well-known result of Menon [41], $(n, k, \lambda) = (4m^2,\ 2m^2 - m,\ m^2 - m)$ for some integer m. Note that for this case, $|\mathrm{supp}(A)| = m^2 = |K|$. So A is an $H(K, m^2)$ and m must be even. □

Example 2.2.8 *Let D be a $(q^{d+1}(1 + \frac{q^{d+1}-1}{q-1}), q^d(\frac{q^{d+1}-1}{q-1}), q^d(\frac{q^d-1}{q-1}))$ McFarland difference set [40] in $G = E \times K$, where q is a prime power, E is an elementary abelian group of order q^{d+1}, and K is any group of order $(1 + \frac{q^{d+1}-1}{q-1})$.*

If q is odd and d is even, then $1 + \frac{q^{d+1}-1}{q-1}$ is even and we can choose K such that $K = \langle\theta\rangle \times K'$ where $o(\theta) = 2$ and $|K'| = \frac{1}{2}(1 + \frac{q^{d+1}-1}{q-1})$. Thus, by Construction 2.2.6, there exist proper $W(E \times K', q^{2d})$.

If $q = 2^r$ with $r \geq 2$, then E can be written as $E = \langle\theta\rangle \times E'$, where θ is any nonzero element of E. Thus, by Construction 2.2.6, there exist proper $W(E' \times K, q^{2d})$.

If $q = 2$, then $(n, k, \lambda) = (4m^2, 2m^2 - m, m^2 - m)$, where $m = 2^d$. For this case, the group weighing matrices constructed by Construction 2.2.6 may not be proper.

Example 2.2.9 *Let D be a $(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1})$ Singer difference set [49] in a cyclic group G. Note that if $q \equiv 1 \bmod 4$ and $d \equiv 1 \bmod 4$, then $2||\frac{q^{d+1}-1}{q-1}$ and by Construction 2.2.6, there exist proper $CW(\frac{q^{d+1}-1}{2(q-1)}, q^{d-1})$.*

Example 2.2.10 *Let $G' = \mathbb{Z}_2 \times \mathbb{Z}_{m_1}^2 \times \cdots \times \mathbb{Z}_{m_r}^2 \times \mathbb{Z}_{p_1}^4 \times \cdots \times \mathbb{Z}_{p_s}^4$ and $G = \mathbb{Z}_2 \times G'$ where $m_1, \cdots, m_r$ are nonnegative integers such that $m_i = 3^{i_j}$ for some nonnegative integer i_j and $p_1, \ldots, p_s$ are odd primes. By Theorem 12.15 in Chapter VI of [11], we know that $(4m^2, 2m^2 - m, m^2 - m)$-difference sets exist in G with $m = 3^{i_1+\cdots+i_r} p_1^2 \cdots p_s^2$. Since m is odd, by Construction 2.2.6, there exists proper $W(G', m^2)$.*

2.3 Constructions Using Divisible Difference Sets

In this section, we shall give a construction of group weighing matrices from divisible difference sets. However, more attention will be given to relative difference sets, which is a special type of divisible difference sets.

Let G be a finite group of order n and N be a subgroup of G with order n'. Let $D \in \mathbb{Z}[G]$, $|D| = k$ and D has only coefficients 0 and 1. Then D is a $(\frac{n}{n'}, n', k, \lambda_1, \lambda_2)$-*divisible difference set* if and only if D satisfies the group ring equation

$$DD^{(-1)} = k - \lambda_1 + (\lambda_1 - \lambda_2)N + \lambda_2 G. \tag{2.2}$$

If $\lambda_1 = 0$, then D is a $(\frac{n}{n'}, n', k, \lambda_2)$-*relative difference set*. The following is a basic property of relative difference sets. The details of the proof can be found in [19].

Proposition 2.3.1 *Let D be a $(\frac{n}{n'}, n', k, \lambda)$-relative difference set in G relative to N. Then $|D \cap Ng| \leq 1$ for all $g \in G$.*

The next result tells us that the existence of a relative difference set implies the existence of a "series" of relative difference sets via projections. For further details, refer to [19].

Proposition 2.3.2 *Let D be a $(\frac{n}{n'}, n', k, \lambda)$-relative difference set in G relative to N. If U is a normal subgroup of G contained in N and η_U is the natural epimorphism from G to G/U, then $\eta_U(D)$ is a $(\frac{n}{n'}, \frac{n'}{u}, k, \lambda u)$-relative difference set in G/U relative to N/U, where $u = |U|$.*

Construction 2.3.3 *Let $G = \langle\theta\rangle \times G'$ be a finite group where $o(\theta) = 2$. Let $N = \langle\theta\rangle \times N'$ be a subgroup of G where N' is a subgroup of G'. Suppose G admits a $(|G|/|N|, |N|, k, \lambda_1, \lambda_2)$-divisible difference set $X \cup \theta Y$ where $X, Y \subset G'$, then $X - Y$ is a $W(G', k - \lambda_1)$.*

Proof Clearly, the coefficients of $X - Y$ are 0 , 1 and -1 only. Let $X + \theta Y$ be a divisible difference set. Then by Equation (2.2), we get

$$\begin{aligned}(X + \theta Y)(X + \theta Y)^{(-1)} &= XX^{(-1)} + YY^{(-1)} + \theta YX^{(-1)} + \theta XY^{(-1)} \\ &= k - \lambda_1 + \lambda_1 N' - \lambda_2 N' + \lambda_2 G' + \theta(\lambda_1 N' - \lambda_2 N' + \lambda_2 G')\end{aligned}$$

By comparing coefficients, we get,

$$XX^{(-1)} + YY^{(-1)} = k - \lambda_1 + \lambda_1 N' - \lambda_2 N' + \lambda_2 G', \tag{2.3}$$

$$YX^{(-1)} + XY^{(-1)} = \lambda_1 N' - \lambda_2 N' + \lambda_2 G'. \tag{2.4}$$

Hence, we get $(X - Y)(X - Y)^{(-1)} = k - \lambda_1$. □

Corollary 2.3.4 *In Construction 2.3.3, if $X + \theta Y$ is a relative difference set, then $X - Y$ is a $W(G', k)$.*

Theorem 2.3.5 *In Construction 2.3.3, if $X + \theta Y$ is a relative difference set and $k > 1$, then the $W(G', k)$ constructed is always proper.*

Proof Since $k > 1$, $\lambda_2 \neq 0$. Then by Equation (2.3) and Equation (2.4), we have $\langle X, Y \rangle = G'$. Also by Proposition 2.3.1, we know that $X \cap Y = \emptyset$. Hence $X - Y$ cannot be contained in a coset of a proper subgroup of G'. □

Note that by Proposition 2.3.2, we can always get a proper $W(G', k)$ from Construction 2.3.3, if there exists a $(\frac{n}{n'}, n', k, \lambda_2)$-relative difference sets G where $\frac{n}{n'}$ is odd and $2 \| n'$. Below are some examples of this case.

Example 2.3.6 *Let q be a power of prime such that $q \equiv 3 \bmod 4$ and d is odd. Then $2 \| q - 1$. Let $n' = 2a$ such that $n' \mid q - 1$. Thus, by [3], there exists a cyclic relative difference set of parameters $(\frac{q^d-1}{q-1}, n', q^{d-1}, \frac{q^{d-2}(q-1)}{n'})$. Thus by Construction 2.3.3, we have a proper $CW(\frac{(q^d-1)n'}{2(q-1)}, q^{d-1})$.*

Example 2.3.7 *Let $q = 2^r$ for some positive integer r and d is odd. Then $2 \| 2(q - 1)$ and $\frac{q^d-1}{q-1}$ is odd. Let $n' = 2a$ such that $a \mid q - 1$. Thus, by Theorem 1.2 in [3], there exists a cyclic relative difference set of parameters $(\frac{q^d-1}{q-1}, n', q^{d-1}, \frac{q^{d-2}(q-1)}{n'})$. Thus by Construction 2.3.3, we have a proper $CW(\frac{(q^d-1)n'}{2(q-1)}, q^{d-1})$ for all possible a.*

The problem of finding relative difference sets with the parameters given in the examples above are known as the Waterloo Problem. The details of this problem can be found in [46].

Remark 2.3.8 *The problem of determining whether $X - Y$ is proper, if we use divisible different sets with $\lambda_1 \neq 0$ in Construction 2.3.3, is still open. So we do not go into the details for this case.*

2.4 Construction Using Hyperplane

The following Proposition is a generalization of Theorem 2.4 of [2].

Proposition 2.4.1 *Let H be a subgroup contained in the center of a finite group G. Let $D_i \in \mathbb{Z}[H]$ with $0, \pm 1$ coefficients for $i = 0, 1, \cdots, r$. If*

1. *$\sum_{i=0}^{r} D_i D_i^{(-1)} = w$, where w is an integer, and*
2. *$D_i D_j^{(-1)} = 0$ for all $i \neq j$,*

then $A = \sum_{i=0}^{r} g_i D_i$ is a $W(G, w)$, where $g_1, \ldots, g_r$ are elements of G such that for any pair of $i, j \in \{0, 1, \ldots, r\}$, if $supp(D_i) \cap supp(D_j) \neq \emptyset$, then g_i and g_j are contained in two different cosets of H.

Proof Since H is contained in the center of G, we have $gD_i = D_i g$ for all $g \in G$ and $i = 1, 2, \ldots, r$. So

$$\begin{aligned} AA^{(-1)} &= \sum_{i=0}^{r} \sum_{j=0}^{r} g_i D_i D_j^{(-1)} g_j^{-1} \\ &= \sum_{i=0}^{r} D_i D_i^{(-1)} + \sum_{i \neq j} g_i D_i D_j^{(-1)} g_j^{-1} \\ &= w \end{aligned}$$

Obviously, the coefficients of A are $0, \pm 1$ and thus, A is a $W(G, w)$. □

Inspired by the construction of McFarland difference sets [40], we have a new construction of group weighing matrices using Proposition 2.4.1. First, we need the following lemma for checking whether a group weighing matrix is proper.

Lemma 2.4.2 *Let G be an abelian group and $S \subset G$. Then S is contained in a coset of a proper subgroup in G if and only if there exists a nonprincipal character χ of G such that $|\chi(S)| = |S|$.*

Proof If $|\chi(S)| = |S|$, then S is contained in a coset of $\ker(\chi)$. On the other hand, if S is contained in a coset of a subgroup H of G, then $|\chi(S)| = |S|$ for all characters χ that are principal on H. □

Let q be a prime power. We also need some basic properties of vector spaces over $GF(q)$, the finite field of order q.

Let L be an $(s+1)$-dimensional vector space over $GF(q)$, where $s \geq 1$. A s-dimensional subspace of L is called a *hyperplane* of L. It can be shown that there are totally $r = \frac{q^{s+1}-1}{q-1} = \sum_{i=0}^{s} q^i$ hyperplanes in L. Let $H_0, H_1, \ldots, H_{r-1}$ be all the hyperplanes in L. Then

$$|H_i \cap H_j| = \frac{|H_i||H_j|}{|H_i H_j|} = \begin{cases} q^{s-1} & \text{if } i \neq j, \\ q^s & \text{if } i = j. \end{cases}$$

Thus

$$H_i H_j = \begin{cases} q^{s-1} L & \text{if } i \neq j, \\ q^s H_i & \text{if } i = j. \end{cases} \tag{2.5}$$

Also it can be proved that

$$\sum_{i=0}^{r-1} H_i = q^{-1}(r-1)L + q^s \tag{2.6}$$

For further details, please refer to [11].

Construction 2.4.3 *Let q be a prime power and let L be an $(s+1)$-dimensional vector space over $GF(q)$ where $s \geq 1$ and if q is odd, then s must be even. Let $H_0, H_1, \ldots, H_{r-1}$, $r = 1 + q + \cdots + q^s$, be all hyperplanes in L. Let G be any finite group such that L, as an additive group, is contained in the center of G and let $g_0, g_1, \ldots, g_{(r-1)/2}$ be elements of G. If $s > 1$, then each of $g_0, g_1, \ldots, g_{(r-1)/2}$ must be contained in different cosets of L in G and hence $|G/L| \geq (r+1)/2$. Define*

$$A = \pm g_0 H_0 + \sum_{i=1}^{(r-1)/2} g_i (H_{2i} - H_{2i-1}).$$

Then A is a $W(G, q^{2s})$.

Proof Let $D_0 = H_0$ and $D_i = H_{2i} - H_{2i-1}$ for $i = 1, 2, \cdots, \frac{r-1}{2}$. By Equation (2.5), we have $D_i D_j^{(-1)} = 0$ for all $i \neq j$. By Equation (2.6), we have

$$\sum_{i=0}^{(r-1)/2} D_i D_i^{(-1)} = \sum_{i=0}^{(r-1)/2} D_i^2 = q^s \sum_{i=0}^{r-1} H_i - (r-1)q^{s-1}L = q^{2s}.$$

Hence by Proposition 2.4.1, A is a $W(G, q^{2s})$. □

Theorem 2.4.4 *In Construction 2.4.3, let η_L be the natural epimorphism from G to G/L. If G is abelian and $q > 2$, then A is proper if and only if $\{\eta_L(g_0), \eta_L(g_1), \ldots, \eta_L(g_{(r-1)/2})\}$ is not contained in any coset of any proper subgroup in G/L.*

Proof Let $S = \mathrm{supp}(A)$. Then

$$S = g_0 H_0 + \sum_{i=1}^{(r-1)/2} g_i \left[H_{2i} + H_{2i+1} - 2(H_{2i} \cap H_{2i-1})\right]$$

and $|S| = rq^s - (r-1)q^{s-1}$. Let χ be a nonprincipal character of G. Suppose χ is nonprincipal on L. Since χ is principal on exactly one H_i,

$$|\chi(S)| \leq q^s + (r-1)q^{s-1} < |S|$$

if $q > 2$. Now assume χ is principal on L. Then $\chi = \chi' \circ \eta_L$ for some character χ' of G/L. Thus

$$\chi(S) = q^s \chi(g_0) + 2(q^s - q^{s-1}) \left[\chi(g_1) + \cdots + \chi(g_{(r-1)/2})\right].$$

Thus, $|\chi(S)| = |S|$ if and only if $\chi'(\eta_L(g_0)) = \chi'(\eta_L(g_1)) = \cdots = \chi'(\eta_L(g_{(r-1)/2}))$. This is equivalent to $\{\eta_L(g_0), \eta_L(g_1), \ldots, \eta_L(g_{(r-1)/2})\}$ is contained in a coset of a proper subgroup in G/L. Thus, the theorem follows by Lemma 2.4.2. □

Example 2.4.5 *In Construction 2.4.3, let η_L be the natural epimorphism from G to G/L. Suppose $q > 2$ and G is abelian such that $G/L = \langle\theta_1\rangle \times \cdots \times \langle\theta_f\rangle$ where $o(\theta_j) = n_j$ for some positive integer n_j for all j and $f \leq (r-1)/2$. If we choose $J = \{g_0, g_1, \ldots, g_{(r-1)/2}\}$ such that $1, \theta_1, \ldots, \theta_f \in \eta_L(J)$, then by Theorem 2.4.4, A is a proper $W(G, q^{2s})$.*

2.5 Construction Using Finite Local Ring

We shall now give another construction of group weighing matrices using Proposition 2.4.1. This time, we need to use a principal local ring (or a chain ring). Let R be a finite local ring of characteristic a power of 2 with its maximal ideal I generated by a prime element π. Note that R is a finite evaluation ring such that every element in R can be written as $\pi^r u$ for some unit u in R. The following are some properties of R.

1. $R/I \cong GF(2^d)$ for some integer d.
2. $|I^{s-1}| = 2^d$ where s is the smallest positive integer such that $I^s = (\pi^s) = 0$.
3. if $2 = \pi^t u_1$ and $s = qt + s'$, where u_1 is a unit in R and $0 \leq s' < t$, then $R \cong \mathbb{Z}_{2^{q+1}}^{ds'} \times \mathbb{Z}_{2^q}^{d(t-s')}$ is an additive group.

For further details, please see [24, 39].

Define φ to be a mapping from R to R such that $\varphi(\pi^r u) = \pi^r u^{-1}$ for all units u in R and $r \in \{0, 1, \ldots, s\}$.

Construction 2.5.1 *Use the notation above. Let $\{S_1, S_2, \ldots, S_{2^d}\}$ be a partition of R such that for any coset $a + I^{s-1}$ in R, $|S_i \cap a + I^{s-1}| = 1$ for all i. Define*

$$E_i = \{(a, b) \in R \times R \mid \varphi(a)b \in S_i\}$$

for $i = 1, 2, \ldots, 2^{d-1}$. Let G be any finite group such that $R \times R$, as an additive group, is contained in the center of G and let $g_1, g_2, \ldots, g_{2^{d-1}}$ be elements (not necessarily distinct) of G. Then

$$A = \sum_{i=1}^{2^{d-1}} g_i(E_{2i-1} - E_{2i})$$

is a $W(G, 2^{2sd})$.

Proof Clearly, A has only $0, \pm 1$ coefficients because $\{E_1, E_2, \ldots, E_{2^d}\}$ is a partition of $R \times R$. Let $D_i = E_{2i-1} - E_{2i}$ and χ be any character of the additive group of $R \times R$. By the results in [28], $D_i = D_i^{(-1)}$ for all i; $\chi(D_i) = \pm 2^{sd}$ for one $i \in \{1, 2, \ldots, 2^{d-1}\}$; and $\chi(D_i) = 0$ for all other i. Thus by Corollary 1.4.2, we have

$$\sum_{i=1}^{2^{d-1}} D_i^2 = 2^{2sd} \quad \text{and} \quad D_i D_j = 0$$

for $i \neq j$. Thus $A = \sum_{i=1}^{2^{d-1}} g_i(E_{2i-1} - E_{2i})$ is a $W(G, 2^{2sd})$. □

Below are two examples of local rings.

Example 2.5.2 *Let $R = \mathbb{Z}_8$. Then $I = (2)$, $R/I \cong \mathbb{F}_2$ and $I^3 = (0)$ i.e., $d = 1$ and $s = 3$. As $I^2 = (4) = \{4, 0\}$, $S_1 = \{0, 1, 2, 3\}$ and $S_2 = \{4, 5, 6, 7\}$ satisfy the requirement of Construction 2.5.1. Note that*

$$0 = 2^3 \cdot 1 \quad 1 = 2^0 \cdot 1 \quad 2 = 2 \cdot 1 \quad 3 = 2^0 \cdot 3 \quad 4 = 2^2 \cdot 1 \quad 5 = 2^0 \cdot 5 \quad 6 = 2 \cdot 3 \quad 7 = 2^0 \cdot 7,$$

and $\varphi(i) = i$ for all i in R. Thus

$$\begin{aligned} E_1 = \{&(0,0),(0,1),(0,2),(0,3),(0,4),(0,5),(0,6),(0,7),(1,0),(2,0),(3,0),(4,0),\\ &(5,0),(6,0),(7,0),(1,1),(1,2),(1,3),(2,1),(2,4),(2,5),(3,1),(3,3),(3,6),\\ &(4,2),(4,4),(4,6),(5,2),(5,5),(5,7),(6,3),(6,4),(6,7),(7,5),(7,6),(7,7)\};\\ E_2 = \{&(1,4),(1,5),(1,6),(1,7),(2,2),(2,3),(2,6),(2,7),(3,2),(3,4),(3,5),\\ &(3,7),(4,1),(4,3),(4,5),(4,7),(5,1),(5,3),(5,4),(5,6),(6,1),(6,2),\\ &(6,5),(6,6),(7,1),(7,2),(7,3),(7,4)\}. \end{aligned}$$

Example 2.5.3 *Let $R = \mathbb{Z}_4[\xi] = \{0, 1, 2, 3, \xi, 2\xi, 3\xi, 1+\xi, 1+2\xi, 1+3\xi, 2+\xi, 2+2\xi, 2+3\xi, 3+\xi, 3+2\xi, 3+3\xi\}$ where $\xi^2 = 3+\xi$. Then $I = (2\xi) = \{0, 2, 2\xi, 2+2\xi\}$, $R/I \cong GF(2^2)$ and $I^2 = (0)$ i.e., $d = 2$ and $s = 2$. Then $S_1 = \{0, 1, 1+\xi, 2+\xi\}$, $S_2 = \{2, 3, 3+\xi, \xi\}$, $S_3 = \{2\xi, 1+2\xi, 1+3\xi, 2+3\xi\}$ and $S_4 = \{2(1+\xi), 3+2\xi, 3(1+\xi), 3\xi\}$ satisfy the requirement of Construction 2.5.1. Note that $\xi^3 = 3$ and*

$\mathbf{a}$		$\phi(\mathbf{a})$
0	$2\xi^2 \cdot 1$	0
1	$2\xi^0 \cdot 1$	1
2	$2\xi^1 \cdot 1 + 3\xi$	$2\xi^1 \cdot \xi = 2 + 2\xi$
3	$2\xi^0 \cdot 3$	3
ξ	$2\xi^0 \cdot \xi$	$1 + 3\xi$
2ξ	$2\xi^1 \cdot 1$	2ξ
3ξ	$2\xi^0 \cdot 3\xi$	$3 + \xi$
$1 + \xi$	$2\xi^0 \cdot 1 + \xi$	$2 + \xi$
$1 + 2\xi$	$2\xi^0 \cdot 1 + 2\xi$	$1 + 2\xi$
$1 + 3\xi$	$2\xi^0 \cdot 1 + 3\xi$	ξ
$2 + \xi$	$2\xi^0 \cdot 2 + \xi$	$1 + \xi$
$2 + 2\xi$	$2\xi^1 \cdot \xi$	$2\xi^1 \cdot 1 + 3\xi = 2$
$2 + 3\xi$	$2\xi^0 \cdot 2 + 3\xi$	$3 + 3\xi$
$3 + \xi$	$2\xi^0 \cdot 3 + \xi$	3ξ
$3 + 2\xi$	$2\xi^0 \cdot 3 + 2\xi$	$3 + 2\xi$
$3 + 3\xi$	$2\xi^0 \cdot 3 + 3\xi$	$2 + 3\xi$

We will not list out each E_i for $i = 1, 2, 3, 4$ as the size of $R \times R$ is quite large.

Theorem 2.5.4 *In Construction 2.5.1, let $\eta_{R\times R}$ be the natural epimorphism from G to $G/(R\times R)$. If G is abelian, then A is proper if and only if $\{\eta_{R\times R}(g_1), \eta_{R\times R}(g_2), \ldots, \eta_{R\times R}(g_{2^{d-1}})\}$ is not contained in any coset of any proper subgroup in $G/(R\times R)$.*

Proof Let $S = \mathrm{supp}(A)$. Then

$$S = \sum_{i=1}^{2^{d-1}} g_i(E_{2i-1} + E_{2i})$$

and $|S| = \sum_{i=1}^{2^d} |E_i| = |R \times R| = 2^{2sd}$. Let χ be any nonprincipal character of G. Suppose χ is nonprincipal on $R \times R$. By the results in [28], $\chi(E_i) = 2^{sd} - 2^{(s-1)d}$ for one $i \in \{1, 2, \ldots, 2^d\}$; and $\chi(E_i) = -2^{(s-1)d}$ for all other i. So

$$|\chi(S)| \leq 2^{sd} - 2^{(s-1)d} + (2^d - 1)2^{(s-1)d} < |S|.$$

Now assume χ is principal on $R \times R$. Then $\chi = \chi' \circ \eta_{R\times R}$ for some character χ' of $G/(R \times R)$. Thus

$$\chi(S) = \sum_{i=1}^{2^{d-1}} \chi(g_i)(|E_{2i-1}| + |E_{2i}|).$$

Thus, $|\chi(S)| = |S|$ if and only if $\chi'(\eta_{R\times R}(g_1)) = \chi'(\eta_{R\times R}(g_2)) = \cdots = \chi'(\eta_{R\times R}(g_{2^{d-1}}))$. This is equivalent to $\{\eta_{R\times R}(g_1), \eta_{R\times R}(g_2), \ldots, \eta_{R\times R}(g_{2^{d-1}})\}$ is contained in a coset of a proper subgroup in G/L. The theorem follows by Lemma 2.4.2. □

Example 2.5.5 *In Construction 2.5.1, let $\eta_{R\times R}$ be the natural epimorphism from G to $G/(R \times R)$. Suppose G is abelian such that $G/(R \times R) = \langle\theta_1\rangle \times \cdots \times \langle\theta_f\rangle$ where $o(\theta_j) = n_j$ for some positive integer n_j for all j and $f \leq 2^{d-1} - 1$. If we choose $J = \{g_1, g_2, \ldots, g_{2^{d-1}}\}$ such that $1, \theta_1, \ldots, \theta_f \in \eta_{R\times R}(J)$, then by Theorem 2.5.4, A is a proper $W(G, q^{2sd})$.*

Chapter 3

Some Results on Abelian Group Weighing Matrices

In this chapter, we study mainly abelian group weighing matrices. First, we study some structures of $W(G, p^{2t})$ where p is an odd prime and G is an abelian group having cyclic Sylow p-subgroup. Section 3.1 gives some results of these $W(G, p^{2t})$ in [5]. Some useful lemmas in [5] that will be needed in our later discussion are also given. Section 3.2 is the discussion of our main results which is a continuation of the work given in Section 3.1. Apart from the first two sections, the last section that is section 3.3 is a thorough study of the existent of proper circulant weighing matrices with weight 9.

3.1 Some Known Results on Abelian Groups Weighing Matrices with Odd Prime Power Weight

Let G be an abelian group having cyclic Sylow p-subgroup where p is an odd prime. Below are some results of $W(G, p^{2t})$ in [5]. The proof of these results can be found in [5].

Theorem 3.1.1 *Let $G = \langle \alpha \rangle \times H$ where $o(\alpha) = p^s$, $exp(H) = e$, $(p(p-1), e) = 1$ and p is a prime greater than 3. Then, a proper $W(G, p^{2r})$ for all $r \geq 1$ does not exist.*

Theorem 3.1.2 *Let $G = \langle\alpha\rangle \times H$ where $o(\alpha) = p$, $exp(H) = e$, $(p, e) = 1$ and p is a prime greater than 7. If e is odd or e is strictly divisible by 2 or $e \leq (p^2 + 1/2)$, then a proper $W(G, p^2)$ does not exist.*

Theorem 3.1.3 *Let $G = \langle\alpha\rangle \times H$ where $o(\alpha) = p^s$, p is an odd prime, $exp(H) = e$, $s > 1$, and $(p, e) = 1$. Then, a proper $W(G, p^2)$ does not exist .*

The following are some useful lemmas in [5] that will be needed to prove our main results in the next section.

Lemma 3.1.4 *Let $G = \langle\alpha\rangle \times H$ be an abelian group of exponent $v = p^s e$ where p is an odd prime, $o(\alpha) = p^s$, $exp(H) = e$, $s \geq 2$ and $p \nmid e$. Let t be an integer such that $t \equiv 1 + p^{s-1}$ mod p^s and $t \equiv 1$ mod e. If $A \in \mathbb{Z}[G]$ satisfies*

1. *$\chi(A)\overline{\chi(A)} = w$ for all characters χ of G which are nonprincipal on P_1 where $P_1 = \langle\alpha^{p^{s-1}}\rangle$ is the subgroup of G of order p and $(w, e) = 1$; and*

2. *$\sigma : \zeta_v \mapsto \zeta_v^t$ fixes every prime ideal divisor of $w\mathbb{Z}[\zeta_v]$,*

then

$$A = \alpha^c(X_0 + P_1X_1)$$

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

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

Lemma 3.1.5 *Let $G = \langle\alpha\rangle \times H$ be an abelian group of exponent $v = p^s e$ where p is an odd prime, $o(\alpha) = p^s$, $exp(H) = e$ and $(p, e) = 1$. 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 e. Then there exists an integer b such that*

$$(\alpha^b A)^{(t)} = \beta\alpha^b A + P_1X$$

where $\beta \in H$, $o(\beta) \mid (p-1, e)$, $P_1 = \langle \alpha^{p^{s-1}} \rangle$ *is the subgroup of* G *of order* p, *and* $X \in \mathbb{Z}[G]$.

Lemma 3.1.6 *Let* $G = \langle \alpha \rangle \times H$ *where* $o(\alpha) = p$, $exp(H) = e$, $(p, e) = 1$ *and* p *is an odd prime. Let* t *be a primitive root modulo* p *and* $t \equiv 1 \bmod e$. *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.*

Lemma 3.1.7 *Let* $G = \langle \alpha \rangle \times H$ *where* $o(\alpha) = p$, $exp(H) = e$, $(p, e) = 1$ *and* p *is an odd prime. Then there is no element* $A \in \mathbb{Z}[G]$ *such that* $AA^{(-1)} = p^2 - p\langle \alpha \rangle$ *and the coefficients of* A *are* $0, \pm 1$.

3.2 Some New Results on Abelian Group Weighing Matrices with Odd Prime Power Weight

Our main results in this section is a continuation of the work done in Section 3.1 The following lemma is a slightly generalized version of Lemma 3.1.7.

Lemma 3.2.1 *Let* $G = \langle \alpha \rangle \times H$ *where* $o(\alpha) = p$, $exp(H) = e$, $(p, e) = 1$ *and* p *is an odd prime. Then there is no element* $A \in \mathbb{Z}[G]$ *such that* $AA^{(-1)} = p^u - p^{u-1}\langle \alpha \rangle$, $u \in \mathbb{Z} \backslash \{1\}$ *and the coefficients of* A *are* $0, \pm 1$.

Proof It is obvious that our claim is true for $u < 1$. Assume that there exists $A \in \mathbb{Z}[G]$ such that $AA^{(-1)} = p^u - p^{u-1}\langle \alpha \rangle$, $u > 1$ and the coefficients of A are

$0, \pm 1$. Let t be a primitive root modulo p and $t \equiv 1 \bmod e$. By Lemma 3.1.5, there exists an integer b such that

$$(\alpha^b A)^{(t)} = \beta \alpha^b A + \langle \alpha \rangle X \tag{3.1}$$

for some $\beta \in H$, and $X \in \mathbb{Z}[G]$ where $m = o(\beta)$ is a divisor of $p-1$. As $\chi(A) = 0$ for $\chi \in \langle \alpha \rangle^{\perp}$ and $\chi(\langle \alpha \rangle) = 0$ for $\chi \in G^* \backslash \langle \alpha \rangle^{\perp}$, we have $\langle \alpha \rangle A = 0$ by Corollary 1.4.2. By multiplying equation (3.1) with $\langle \alpha \rangle$, we get $\langle \alpha \rangle X = 0$. Hence $(\alpha^b A)^{(t)} = \beta \alpha^b A$.

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 3.1.6,

$$\alpha^b A = \langle \beta \rangle \sum_{k=1}^{v} a_k h_k + \sum_{j=0}^{m-1} \sum_{k=1}^{v} b_{jk} Q_j h_k \tag{3.2}$$

where $a_k, b_{jk} = 0, \pm 1$. Note that $\langle \alpha \rangle Q_j = [\frac{p-1}{m}] \langle \alpha \rangle \langle \beta \rangle$. By multiplying both sides of Equation (3.2) by $\langle \alpha \rangle$, we get $a_k + \frac{p-1}{m} \sum_{j=0}^{m-1} b_{jk} = 0$ and thus

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

for all k. So it is either $m = p-1$ or $a_k = 0$ for all k.

Now we multiply equation (3.2) by $\langle \beta \rangle$. Note that $\langle \beta \rangle Q_j = \langle \beta \rangle (\langle \alpha \rangle - 1)$. If $a_k = 0$ for all k, then $\sum_{j=0}^{m-1} b_{jk} = 0$ for all k. Hence $\langle \beta \rangle \alpha^b A = 0$, which is a contradiction, as $\langle \beta \rangle A A^{(-1)} \neq 0$.

Assume that $m = p-1$. Let x_1 and x_2 be respectively the number of $+1$ and -1 coefficients in A. By $AA^{(-1)} = p^u - p^{u-1} \langle \alpha \rangle$, we have $x_1 + x_2 = p^u - p^{u-1}$ and by $\langle \alpha \rangle A = 0$, we have $x_1 - x_2 = 0$. Hence $x_1 = x_2 = \frac{p^u - p^{u-1}}{2} = \frac{p^{u-1}(p-1)}{2}$. By equation (3.2), 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 3.2.2 *Let $G = \langle \alpha \rangle \times H$ where $o(\alpha) = p^s$, $exp(H) = e$, $(p, e) = 1$ and p is an odd prime. Let $A \in \mathbb{Z}[G]$ satisfy $\chi(A)\overline{\chi(A)} = p^{2r}$ for all characters nonprincipal*

on P_1 where $P_1 = \langle \alpha^{p^{s-1}} \rangle$ is the subgroup of G of order p. Then

$$A = \alpha^c (X_0 + P_1 X_1)$$

for some integer c and $X_0 \in \mathbb{Z}[P_1 \times H]$ and $X_1 \in \mathbb{Z}[G \setminus (P_1 \times H)]$.

Proof By Lemma 3.1.4, we get

$$A = \alpha^{c_1} (X_{0,1} + P_1 X_{1,1})$$

for $c_1 \in \mathbb{Z}$, $X_{0,1} \in \mathbb{Z}[\langle \alpha^p \rangle \times H]$ and the support of $X_{1,1}$ is contained in $G \setminus (\langle \alpha^p \rangle \times H)$. Note that $\chi(X_{0,1})\overline{\chi(X_{0,1})} = p^{2r}$ for all characters χ of $\langle \alpha^p \rangle \times H$ which are nonprincipal on P_1. By applying Lemma 3.1.4 again, we get

$$X_{0,1} = \alpha^{pc_2} (X_{0,2} + P_1 X_2)$$

for $c_2 \in \mathbb{Z}$, $X_{0,2} \in \mathbb{Z}[\langle \alpha^{p^2} \rangle \times H]$ and the support of X_2 is contained in $G \setminus (\langle \alpha^{p^2} \rangle \times H)$. Thus

$$A = \alpha^{c_1 + pc_2} [X_{0,2} + P_1 X_{1,2}]$$

where the support of $X_{1,2} = \alpha^{-pc_2} X_{1,1} + X_2$ is contained in $G \setminus (\langle \alpha^{p^2} \rangle \times H)$. By applying Lemma 3.1.4 repeatedly $s-1$ times, we will get the result of this lemma. □

Remark 3.2.3 *Recently, a more general version of Lemma 3.2.2 was proved independently by Leung and Schmidt [31]. Their result is too involved to be stated here.*

Lemma 3.2.4 *Let $G = \langle \alpha \rangle \times H$ where $o(\alpha) = p^s$, $exp(H) = e$, $(p, e) = 1$ and p is an odd prime. Let P_i be the subgroup of $\langle \alpha \rangle$ of order p^i, i.e. $P_i = \langle \alpha^{p^{s-i}} \rangle$. Then there is no element $A = X_0 + P_1 X_1 + \cdots + P_{s-1} X_{s-1}$ in $\mathbb{Z}[G]$ that satisfies*

1. *$A A^{(-1)} = p^{2r} - p^{2r-s} P_s$;*

2. *the coefficients of* A *are* $0, \pm 1$*;*

3. $X_i \in \mathbb{Z}[P_{i+1} \times H]$ *for all* i*; and*

4. *the supports of* $X_0, P_1X_1, \ldots, P_{s-1}X_{s-1}$ *are disjoint.*

Proof Assume that there exists $A \in \mathbb{Z}[G]$ that satisfies the conditions listed in the lemma. For each $i = 0, 1, \ldots, s-1$ and for each $g \in \mathrm{supp}(P_iX_i)$, without the loss of generality, we can assume that not all the coefficients of $\alpha^{kp^{s-i-1}}g$, $k = 0, 1, \ldots, p-1$, in P_iX_i are the same; otherwise, we can re-define X_i and X_{i+1} so that $g \in \mathrm{supp}(P_{i+1}X_{i+1})$.

Let $\eta_{P_{s-1}}$ be the natural epimorphism from G to G/P_{s-1}. Let

$$Y = \eta_{P_{s-1}}(X_0 + P_1X_1 + \cdots + P_{s-2}X_{s-2}) \in \mathbb{Z}[\eta_{P_{s-1}}(H)].$$

Note that by the assumption of the coefficients of $X_0, P_1X_1, \ldots, P_{s-2}X_{s-2}$, the coefficients of Y lie between $\pm(p^{s-1}-1)$.

Now, let $\eta' = \tau \circ \eta_{P_{s-1}}$ where τ is the natural epimorphism from G/P_{s-1} to $(G/P_{s-1})/\eta_{P_{s-1}}(P_s) \cong G/P_s$. By Condition 1, we have $\eta'(A)\eta'(A)^{(-1)} = 0$. This implies that $\chi(\eta'(A)) = 0$ for all characters χ of $(G/P_{s-1})/\eta_{P_{s-1}}(P_s)$. Hence $\eta'(A) = 0$. On the other hand, $\eta'(A) = \eta'(Y) + p^{s-1}\eta'(X_{s-1})$. So $\eta'(Y) \equiv 0 \bmod p^{s-1}$. Since $Y \in \mathbb{Z}[\eta_{P_{s-1}}(H)]$ and $\eta'|_{\eta_{P_{s-1}}(H)}$ is bijective, we get $Y \equiv 0 \bmod p^{s-1}$ and hence $Y = 0$.

Thus $\eta_{P_{s-1}}(A) = p^{s-1}\eta_{P_{s-1}}(X_{s-1})$. This implies that

$$\begin{aligned}
\eta_{P_{s-1}}(X_{s-1})\eta_{P_{s-1}}(X_{s-1})^{(-1)} &= \frac{1}{p^{2(s-1)}}\eta_{P_{s-1}}(AA^{(-1)}) \\
&= p^{2(r-s+1)} - p^{2(r-s+1)-s}\eta_{P_{s-1}}(P_s) \\
&= p^{2(r-s+1)} - p^{2(r-s+1)-s}p^{s-1}\langle\eta_{P_{s-1}}(\alpha)\rangle \\
&= p^{2(r-s+1)} - p^{2(r-s+1)-1}\langle\eta_{P_{s-1}}(\alpha)\rangle
\end{aligned}$$

where $o(\eta_{P_{s-1}}(\alpha)) = p$. Note that $\eta_{P_{s-1}}(X_{s-1}) \in \mathbb{Z}[\langle \eta_{P_{s-1}}(\alpha)\rangle \times \eta_{P_{s-1}}(H)]$. Thus by Lemma 3.2.1, $\eta_{P_{s-1}}(X_{s-1})$ does not exist. □

Theorem 3.2.5 *Let $G = \langle\alpha\rangle \times H$ where $o(\alpha) = p^s$, $s \geq 2$, $exp(H) = e$, $(p, e) = 1$ and p is an odd prime. Let P_i be the subgroup of $\langle\alpha\rangle$ of order p^i, i.e. $P_i = \langle\alpha^{p^{s-i}}\rangle$. If A is a $W(G, p^{2r})$, then*

$$A = \alpha^c(X_0 + P_1X_1 + \cdots + P_{s-1}X_{s-1})$$

where $c \in \mathbb{Z}$, $X_i \in \mathbb{Z}[P_{i+1} \times H]$ and the supports of $X_0, P_1X_1, \ldots, P_{s-1}X_{s-1}$ are disjoint.

Proof We prove by mathematical induction.

By Lemma 3.2.2, we get

$$A = \alpha^c(W_0 + P_1W_1)$$

where $c \in \mathbb{Z}$, $W_0 \in \mathbb{Z}[P_1 \times H]$ and $W_1 \in \mathbb{Z}[G \setminus (P_1 \times H)]$. Let

$$D = \{g \in \text{supp}(W_0) \mid \text{the coefficients of } g, \alpha^{p^{s-1}}g, \ldots, \alpha^{(p-1)p^{s-1}}g \text{ in } W_0 \text{ are the same}\}.$$

We can rewrite

$$A = \alpha^c(X_0 + P_1Z_1)$$

where $X_0 \in \mathbb{Z}[P_1 \times H]$ and $Z_1 \in \mathbb{Z}[G]$ such that $\text{supp}(X_0) = \text{supp}(W_0) \setminus D$ and the supports of X_0 and Z_1 are disjoint. Note that for each $g \in \text{supp}(X_0)$, not all the coefficients of $\alpha^{kp^{s-1}}g$, $k = 0, 1, \ldots, p-1$, in X_0 are the same.

Now suppose that for $0 \leq u \leq s-3$,

$$A = \alpha^c(X_0 + P_1X_1 + \cdots + P_{u-1}X_{u-1} + P_uZ_u)$$

where $X_i \in \mathbb{Z}[P_{i+1} \times H]$, $Z_u \in \mathbb{Z}[G]$, the supports of $X_0, P_1X_1, \ldots, P_{u-1}X_{u-1}, P_uZ_u$ are disjoint and for each $g \in \text{supp}(P_iX_i)$, $0 \leq i \leq u-1$, not all the coefficients of $\alpha^{kp^{s-i-1}}g$, $k = 0, 1, \ldots, p-1$, in X_i are the same.

Let $X = X_0 + P_1X_1 + \cdots + P_{u-1}X_{u-1} \in \mathbb{Z}[P_u \times H]$. Then

$$A = \alpha^c(X + P_uZ_u).$$

Let η_{P_u} be the natural epimorphism from G to G/P_u and let $\bar{\alpha} = \eta_{P_u}(\alpha)$. We have

$$\eta_{P_u}(A) = \bar{\alpha}^c[\eta_{P_u}(X) + p^u\eta_{P_u}(Z_u)]$$

where $\eta_{P_u}(X) \in \mathbb{Z}[\eta_{P_u}(H)]$. From the inductive assumption, the coefficients of $\eta_{P_u}(X)$ lies between $\pm(p^u - 1)$.

On the other hand, by Lemma 3.2.2, we get

$$\eta_{P_u}(A) = \bar{\alpha}^d(Y_0 + \langle\bar{\alpha}^{p^{s-u-1}}\rangle Y_1)$$

where $d \in \mathbb{Z}$, $Y_0 \in \mathbb{Z}[\langle\bar{\alpha}^{p^{s-u-1}}\rangle \times \eta_{P_u}(H)]$, $Y_1 \in \mathbb{Z}[\eta_{P_u}(G)\backslash(\langle\bar{\alpha}^{p^{s-u-1}}\rangle \times \eta_{P_u}(H))]$. Then

$$\begin{aligned}\bar{\alpha}^d(1 - \bar{\alpha}^{p^{s-u-1}})Y_0 &= (1 - \bar{\alpha}^{p^{s-u-1}})\eta_{P_u}(A) \\ &= \bar{\alpha}^c\left[(1 - \bar{\alpha}^{p^{s-u-1}})\eta_{P_u}(X) + p^u(1 - \bar{\alpha}^{p^{s-u-1}})\eta_{P_u}(Z_u))\right].\end{aligned}$$

We now claim that $\bar{\alpha}^c \in \bar{\alpha}^d\langle\bar{\alpha}^{p^{s-u-1}}\rangle$. Assume that it is not. Then

$$\text{supp}\left(\bar{\alpha}^d(1 - \bar{\alpha}^{p^{s-u-1}})Y_0\right) \cap \text{supp}\left(\bar{\alpha}^c(1 - \bar{\alpha}^{p^{s-u-1}})\eta_{P_u}(X)\right) = \emptyset.$$

So,

$$\bar{\alpha}^c(1 - \bar{\alpha}^{p^{s-u-1}})\eta_{P_u}(X) \equiv 0 \bmod p^u \quad \Rightarrow \quad \eta_{P_u}(X) \equiv 0 \bmod p^u \quad \Rightarrow \quad \eta_{P_u}(X) = 0.$$

Let χ be any character of G. If χ is nonprincipal on P_u, then

$$\chi(X)\overline{\chi(X)} = \chi(A)\overline{\chi(A)} = p^{2r}.$$

If χ is principal on P_u, then $\chi = \chi' \circ \eta_{P_u}$, for some character χ' of G/P_u. Hence

$$\chi(X)\overline{\chi(X)} = \chi'(\eta_{P_u}(X))\overline{\chi'(\eta_{P_u}(X))} = 0.$$

So $XX^{(-1)} = p^{2r} - p^{2r-u}P_u$ which is impossible by Lemma 3.2.4. Thus $\bar{\alpha}^c \in \bar{\alpha}^d\langle\bar{\alpha}^{p^{s-u-1}}\rangle$.

Note that $\bar{\alpha}^d = \bar{\alpha}^{c+jp^{s-u-1}}$ for some j. So, $\bar{\alpha}^d(Y_0 + \langle\bar{\alpha}^{p^{s-u-1}}\rangle Y_1) = \eta_{P_u}(A) = \bar{\alpha}^c(\eta_{P_u}(X) + p^u\eta_{P_u}(Z_u))$ implies

$$p^u\bar{\alpha}^c\eta_{P_u}(Z_u) = \bar{\alpha}^c(Y_0' + \langle\bar{\alpha}^{p^{s-u-1}}\rangle Y_1').$$

where $Y_0' \in \mathbb{Z}[\langle\bar{\alpha}^{p^{s-u-1}}\rangle \times \eta_{P_u}(H)]$ and $Y_1' \in \mathbb{Z}[\eta_{P_u}(G)]$. We can choose Y_0' and Y_1' such that the supports of Y_0' and $\langle\bar{\alpha}^{p^{s-u-1}}\rangle Y_1'$ are disjoint and for each $h \in \mathrm{supp}(Y_0')$, not all the coefficients of $\bar{\alpha}^{kp^{s-u-1}}h$, $k = 0, 1, \ldots, p-1$, in Y_0' are the same. This follow by

$$\alpha^c P_u Z_u = \alpha^c(P_u X_u + P_{u+1}Z_{u+1})$$

for some $X_u \in \mathbb{Z}[P_{u+1} \times H]$, $Z_{u+1} \in \mathbb{Z}[G]$ and the support of P_uX_u and $P_{u+1}X_{u+1}$ are disjoint.

Hence

$$A = \alpha^c(X_0 + P_1X_1 + \cdots + P_uX_u + P_{u+1}Z_{u+1})$$

where $X_i \in \mathbb{Z}[P_{i+1} \times H]$, $Z_{u+1} \in \mathbb{Z}[G]$, the supports of $X_0, P_1X_1, \ldots, P_uX_u, P_{u+1}Z_{u+1}$ are disjoint and for each $g \in \mathrm{supp}(P_iX_i)$, $0 \le i \le u$, not all the coefficients of $\alpha^{kp^{s-i-1}}g$, $k = 0, 1, \ldots, p-1$, in X_i are the same. Therefore, the theorem follows by induction. □

Corollary 3.2.6 *Let $G = \langle\alpha\rangle \times H$ where $o(\alpha) = p^s$, $s \ge 2$, $exp(H) = e$, $(p, e) = 1$ and p is an odd prime. Let $A \in \mathbb{Z}[G]$ be a $W(G, p^{2r})$ where $r \le s-1$. Then A is not proper.*

Proof

Let P_i be the subgroup of $\langle\alpha\rangle$ of order p^i, i.e. $P_i = \langle\alpha^{p^{s-i}}\rangle$. By Theorem 3.2.5, there exists an integer c such that

$$\alpha^{-c}A = X_0 + P_1X_1 + \cdots + P_{s-1}X_{s-1} \tag{3.3}$$

where $X_i \in \mathbb{Z}[P_{i+1} \times H]$ and the supports of $X_0, P_1X_1, \ldots, P_{s-1}X_{s-1}$ are disjoint. Note that the coefficients of elements in each P_iX_i are $0, \pm 1$.

Let $\eta_{P_{s-1}}$ be the natural epimorphism from G to G/P_{s-1}. Let $\overline{\alpha} = \eta_{P_{s-1}}(\alpha)$. Then

$$\overline{\alpha}^{-c}\eta_{P_{s-1}}(A) = \eta_{P_{s-1}}(X) + p^{s-1}\eta_{P_{s-1}}(X_{s-1})$$

where $X = X_0 + P_1X_1 + \cdots + P_{s-2}X_{s-2} \in \mathbb{Z}[P_{s-1} \times H]$. Suppose $r < s - 1$. By comparing the coefficients of the identity in both sides of the equation $\eta_{P_{s-1}}(A)\eta_{P_{s-1}}(A)^{(-1)} = p^{2r}$, the only possible solution is $\eta_{P_{s-1}}(X_{s-1}) = 0$. This implies $P_{s-1}X_{s-1} = 0$, i.e. $A = X$ is not proper.

Now, assume that $r = s-1$. As the coefficient of the identity in $\eta_{P_{s-1}}(A)\eta_{P_{s-1}}(A)^{(-1)}$ is p^{2r}, we know that either $\eta_{P_{s-1}}(X) = 0$ or $\eta_{P_{s-1}}(X_{s-1}) = 0$. If $\eta_{P_{s-1}}(X_{s-1}) = 0$, our claim is true. Suppose $\eta_{P_{s-1}}(X) = 0$, i.e. $P_{s-1}X = 0$. Note that by Equation (3.3), $\chi(X)\overline{\chi(X)} = \chi(A)\overline{\chi(A)} = p^{2r}$ if χ is nonprincipal on P_{s-1} and $\chi(X) = 0$ if χ is principal on P_{s-1}. So $XX^{(-1)} = p^{2r} - p^{2r-s+1}P_{s-1}$. By Lemma 3.2.4, X does not exist. □

3.3 The Study of the Existence of Proper Circulant Weighing Matrices with Weight 9

By [2], we know that $CW(n, 9)$ only exist for n which are multiples of 13 and 24. In this section, we shall further prove that proper $CW(n, 9)$ only exist for $n = 13, 26, 24$. Recall that if K is a subgroup of G, then η_K is the natural epimorphism from G to G/K.

Example 3.3.1 *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 $\eta_{\langle g^{13}\rangle} : G \longrightarrow G/\langle g^{13}\rangle$. It can be shown that $\eta_{\langle g^{13}\rangle}(A)$ is a proper $CW(13, 9)$.

Example 3.3.2 *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 $CW(24, 9)$.

Throughout this section, we shall denote $\mathrm{Ord}_n(p)$ as the smallest positive integer γ such that $p^\gamma \equiv 1 \bmod n$ or in other words, γ is the smallest positive integer such that $p^\gamma - 1 \equiv 0 \bmod n$ where p is a prime. For an element h of a group, $\theta(h, p)$ will be identified as the set $\{h, h^p, h^{p^2}, \dots\}$.

We first consider the case where $(n, 3) = 1$. The proof of the following lemma can be found in [10].

Lemma 3.3.3 *Let G be an abelian group with $|G| = n$ and $(n, p) = 1$ where p is a prime. If $A \in \mathbb{Z}[G]$ such that $AA^{(-1)} = p^{2r}$, then there exists $g \in G$ such that*

$$(gA)^{(p)} = gA.$$

Lemma 3.3.4 *Let G be a group of order n and $(n, p) = 1$ where p is a prime. Let $A = \sum_{i=1}^{s} a_i X_i \in \mathbb{Z}[G]$ where $a_1, a_2, \dots, a_s$ are distinct nonzero integers and $X_1, X_2, \dots, X_s$ are pairwise disjoint subsets of G. If $AA^{(-1)} = p^{2r}$ and the support of A are not contained in any coset of any proper subgroup G, then n is a divisor of the smallest common multiple of $p - 1, p^2 - 1, \dots, p^{|u|} - 1$ where $u = max\{|X_i| \mid i = 1, 2, \dots, s\}$*

Proof By Lemma 3.3.3, we know that there exists $g \in G$ such that

$$(gA)^{(p)} = gA. \tag{3.4}$$

Clearly, $(gA)(gA)^{(-1)} = p^{2r}$ and the support of gA is not contained in any coset of any proper subgroup of G too. 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 and $a_1, a_2, \ldots, a_s$ are distinct nonzero integers. Without the loss of generality, we can assume that $|X_1| \geq |X_i|$ for all $i \geq 2$. Let $h \in \text{supp}(gA)$. Then by Equation (3.4), if $h \in gX_i$, then $\theta(h,p) \subset gX_i$. 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 every $h \in \text{supp}(gA)$, $o(h) \mid p^t - 1$ where $t = \text{Ord}_{o(h)}p \leq |X_1|$, n is a divisor of the smallest common multiples of $p-1, p^2-1, \ldots, p^{|u|}-1$. □

Lemma 3.3.5 *Let G be a cyclic group of order n and $(n,p) = 1$ where p is a prime. Let $A = \sum_{i=1}^{s} a_i X_i \in \mathbb{Z}[G]$ such that $AA^{(-1)} = p^{2r}$ with $a_1, a_2, \ldots, a_s$ are distinct nonzero integers; $X_1, X_2, \ldots, X_s$ are pairwise disjoint subsets of G and $|X_1| > |X_i|$ for all $i \geq 2$. If q is a prime divisor of n such that $q^f \mid n$ and $ord_{q^f}(p) \geq |X_i|$ 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 $supp(C) \subset K$ where $K = \{g \in G \mid q^f \nmid o(g)\}$ is a proper subgroup of G.

Proof For any $h \in \text{supp}(A)$, if $q^f \mid o(h)$, then $|\theta(h,p)| \geq \text{ord}_{q^f}(p)$. This implies that $h \in \text{supp}(X_1)$ and thus $\theta(h,p) \subset X_1$. 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 $\text{supp}(C) \subset K$. □

Theorem 3.3.6 *If $(n,3) = 1$, then there exists a proper $CW(n,9)$ if and only if $n = 13$ or $n = 26$.*

Proof 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 Proposition 1.2.7, 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 $|X_2| = 3$. By the choice of g, we know that ${X_i}^{(3)} = X_i$ for all i. Thus if $h \in \mathrm{supp}(X_i)$, then $\theta(h,3) \subset \mathrm{supp}(X_i)$ too. By Lemma 3.3.4, n is a divisor of the smallest common multiples 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

$$\begin{aligned}
3-1 = 2 &\Rightarrow \mathrm{Ord}_2 3 = 1;\\
3^2-1 = 2^3 &\Rightarrow \mathrm{Ord}_{2^2} 3 = \mathrm{Ord}_{2^3} 3 = 2;\\
3^3-1 = 2 \times 13 &\Rightarrow \mathrm{Ord}_{13} 3 = \mathrm{Ord}_{13\times 2} 3 = 3;\\
3^4-1 = 2^4 \times 5 &\Rightarrow \mathrm{Ord}_{2^4} 3 = \mathrm{Ord}_5 3 = \mathrm{Ord}_{2^4\times 5} = \mathrm{Ord}_{2^3\times 5} = \mathrm{Ord}_{2^2\times 5} = 4;\\
3^5-1 = 2 \times 11^2 &\Rightarrow \mathrm{Ord}_{11} 3 = \mathrm{Ord}_{11^2} 3 = \mathrm{Ord}_{2\times 11} 3 = \mathrm{Ord}_{2\times 11^2} 3 = 5;\\
3^6-1 = 13 \times 7 \times 2^3 &\Rightarrow \mathrm{Ord}_7 3 = \mathrm{Ord}_{7\times 13} 3 = \mathrm{Ord}_{7\times 2} 3 = \mathrm{Ord}_{7\times 2^2} 3\\
&\quad = \mathrm{Ord}_{7\times 2^3} 3 = \mathrm{Ord}_{13\times 2^2} 3 = \mathrm{Ord}_{13\times 2^3} 3\\
&\quad = \mathrm{Ord}_{13\times 7\times 2} 3 = \mathrm{Ord}_{13\times 7\times 2^2} 3 = \mathrm{Ord}_{13\times 7\times 2^3} 3 = 6.
\end{aligned} \tag{3.5}$$

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

There exists an element $h \in \mathrm{supp}(gA)$ such that $11 \mid o(h)$ as A is proper. Note that $\theta(h,3) = 5$ and $o(h) = 11, 11^2, 2\times 11, 2\times 11^2$. By Lemma 3.3.5

$$gA = C + \theta(h,3)$$

where $\mathrm{supp}(C) \subset K = \{g \in G \mid 11 \nmid o(g)\}$. Let H be a subgroup of G such that

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

Then

$$\eta_H(gA) = \eta_H(C) + 5\mu.$$

where $\mu \in G/H$, $o(\mu) = 1$ or 2 and the coefficients of $\eta_H(C)$ are 0 ± 1. This is a contradiction as the coefficient of $\eta_H(1)$ in $\eta_H(gA)\eta_H((gA)^{(-1)})$ is at least $(5-1)^2 + (4-1) = 19$.

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

There exists an element $h \in \text{supp}(gA)$ such that $\varpi \mid o(h)$ as A is proper. Note that $\theta(h,3) = 4$ if $\varpi = 2^4$ or 5; and $\theta(h,3) = 6$ if $\varpi = 7$. By Lemma 3.3.5,

$$gA = C + \theta(h,3)$$

where $\text{supp}(C) \subset K = \{g \in G \mid \varpi \nmid o(g)\}$. Let H be a subgroup of G such that

$$|H| = \begin{cases} 2^3 a & \text{if } \varpi = 2^4, \\ a & \text{if } \varpi = 5 \text{ or } 7. \end{cases}$$

Note that $\varpi a \mid 2^4 \times 5 \times 7 \times 11^2 \times 13$ and $K \subset H$. Then

$$\eta_H(gA) = \begin{cases} -1 + 4\eta_H(h) & \text{if } \varpi = 2^4, \\ -1 + \theta(\eta_H(h), 3) & \text{if } \varpi = 5, \\ -3 + \theta(\eta_H(h), 3) & \text{if } \varpi = 7. \end{cases}$$

where $\eta_H(h)$ is not the identity. Therefore, the coefficient of $\eta_H(1)$ in $\eta_H(gA)$ $\eta_H((gA)^{(-1)})$ is either 17, 5 or 15. This contradicts $AA^{(-1)} = \eta_H(gA)\,\eta_H((gA)^{(-1)}) = 9$.

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

Let $h \in G$. Note that

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

(a) Suppose that $o(h) \neq 13$ or 26 for all $h \in X_2$. Then $X_2 \subset P$ where P is the Sylow 2-subgroup of G. Since A is proper,

$$\eta_P(gA) = -3 + X \text{ or } Y$$

where $X, Y \subset G/P$ such that $|X| = 6$ and $|Y| = 3$. The coefficient of $\eta_P(1)$ in $(-3+X)(-3+X^{(-1)})$ is 15 and the coefficient of $\eta_P(1)$ in $YY^{(-1)}$ is 3. Both contradict with $\eta_P(gA)\eta_P((gA)^{(-1)}) = 9$.

(b) Suppose $X_2 = \theta(h_1, 3)$ for some $h_1 \in G$ of order 13 or 26.

If $X_1 \subset P$ where P is the Sylow 2-subgroup of G, then $\eta_P(gA) = 6 - \theta(\eta_P(h_1))$, a contradiction. Hence there exists $h_2 \in X_1$ such that $13 \mid o(h_2)$. If $o(h_2) = 52$ or 104, then

$$\eta_P(gA) = 2X - Y \text{ or } Z$$

where $X, Y, Z \subset G/P$, $X \cap Y = \emptyset$, $|X| = |Y| = |Z| = 3$, and both cases contradict with $\eta_P(gA)\eta_P((gA)^{(-1)}) = 9$. So $o(h_2) = 13$ or 26. Since A is proper, $X_1 = g_1 + \theta(g_2, 3) + \theta(h_2, 3)$ where $o(g_1) = 1$ or 2, $o(g_2) = 4$ or 8 and $o(h_2) = 13$ or 26. Let L be a subgroup of G of order 26. Then

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

This contradicts with $\eta_L(gA)\eta_L((gA)^{(-1)}) = 9$. □

We shall now consider the case where $(n, 3) \neq 1$. By Theorem 3.1.3, we know that all $CW(n, 3^2)$ where $3^s \mid n$ with $s > 1$ are not proper. Thus, we can assume $3 \parallel n$. The following lemma is a particular case of Lemma 3.5 of [5].

Lemma 3.3.7 *Let $G = P \times H$ be an abelian group where $P = \langle \alpha \rangle$, $o(\alpha) = 3$, and $(3, |H|) = 1$. Let $A \in \mathbb{Z}[G]$ 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*

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

where $g, \beta \in H$, $o(\beta) = 1$ *or* 2 *and* $\epsilon = \pm 1$.

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

Lemma 3.3.8 *Let* $G = P \times H$ *be an abelian group where* $P = \langle \alpha \rangle$, $o(\alpha) = 3$, *and* $(3, |H|) = 1$. *Let* $A \in \mathbb{Z}[G]$ *such that for* $t \equiv 2 \bmod 3$ *and* $t \equiv 1 \bmod |H|$,

$$A^{(t)} = \beta A + (1-\beta)Pg. \tag{3.6}$$

where $g, \beta \in H$ *and* $o(\beta) = 2$. *Let* $K = \langle \alpha, \beta \rangle$ *and let* $A = \sum_{h \in I} hA_h$ *where* I *is the complete set of coset representatives of* K *and* $A_h = a_h + a_{h\beta}\beta + a_{h\alpha}\alpha + a_{h\alpha^2}\alpha^2 + a_{h\beta\alpha}\beta\alpha + a_{h\beta\alpha^2}\beta\alpha^2 \in \mathbb{Z}[K]$. *Then*

$$A_h = a_h(1+\beta) + a_{h\alpha}(\alpha + \alpha^2) + a_{h\alpha^2}(\alpha^2 + \alpha\beta) \tag{3.7}$$

if $hK \neq gK$ *and otherwise*

$$A_g = a_g + (a_g - 1)\beta + a_{g\alpha}\alpha + (a_{g\alpha} - 1)\alpha^2\beta + a_{g\alpha^2}\alpha^2 + (a_{g\alpha^2} - 1)\alpha\beta. \tag{3.8}$$

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 $hK \neq gK$. 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

$$\beta A_h = a_{h\beta} + a_h\beta + a_{h\beta\alpha}\alpha + a_{h\alpha}\alpha\beta + a_{h\beta\alpha^2}\alpha^2 + a_{h\alpha^2}\alpha^2\beta; \tag{3.9}$$

$${A_h}^{(t)} = a_h + a_{h\beta}\beta + a_{h\alpha^2}\alpha + a_{h\alpha}\alpha^2 + a_{h\beta\alpha^2}\beta\alpha + a_{h\beta\alpha}\beta\alpha^2. \tag{3.10}$$

By comparing the coefficients of (3.9) and (3.10), 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 (3.6),

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

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 3.3.9 *Let $G = P \times H$ be a cyclic group where $P = \langle\alpha\rangle$, $o(\alpha) = 3$, and $(3, |H|) = 1$. If $A \in \mathbb{Z}[G]$ is a proper $CW(n, 9)$, then*

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

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.

Proof By Lemma 3.3.7, for $t \equiv 2 \bmod 3$ and $t \equiv 1 \bmod |H|$, there exists an integer b such that

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

where $g, \beta \in H$, $o(\beta) = 1$ or 2 and $\epsilon = \pm 1$. By replacing A with $\alpha^b A$ and if $\epsilon = -1$, replacing g with $g\beta$, we can assume

$$A^{(t)} = \beta A + (1-\beta)Pg. \tag{3.11}$$

Suppose $o(\beta) = 2$. Then Lemma 3.3.8 can be applied. By using the notation of Lemma 3.3.8, we have the following 4 cases.

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

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

By Proposition 1.2.7, we can assume that $A = X_1 - X_2$ where X_1, X_2 are disjoint subsets of G such that $|X_1| = 6$ and $|X_2| = 3$. Since all elements in A_h with coefficients $+1$ and -1 for $Kh \neq Kg$ come in pairs as in (3.7), either one or three of the coefficients of A_g are -1 in order to have $|X_2| = 3$. Hence case 1 and case 2 are impossible.

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

If there are 2 elements in the support of A_g that have coefficient 1 and one element in the support of A_g that have coefficient -1, then $\eta_K(A) = g(1+2h_1+2h_2-2h_3)$ where h_1, h_2, h_3 are nonidentity elements in G/K. Note that contradiction occurs as the coefficient of $\eta_K(1)$ in the equation $\eta_K(A)\eta_K(A^{(-1)})$ 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.

Let $\beta = 1$ in (3.11) and thus $A^{(t)} = A$. Let $A = \sum_{h \in J} hB_h$, where J is the complete set of coset representatives of P and $B_h \in \mathbb{Z}[P]$. For $h \in J$, $B_h = \delta_1 + \delta_2(\alpha + \alpha^2)$ where $\delta_1, \delta_2 = 0, \pm 1$. 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 $\delta_1 = \pm 1$ and $\delta_2 = 0$, then $h \in \text{supp}(B)$; if $\delta_1 = 0$ and $\delta_2 = \pm 1$, then $h \in \text{supp}(C)$; if $\delta_1 = -\delta_2 = \pm 1$, then $h \in \text{supp}(D)$; and if $\delta_1 = \delta_2 = \pm 1$, then $h \in \text{supp}(E)$. $\square$

Theorem 3.3.10 *If $(n,3) \neq 1$, 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 $P = \langle \alpha \rangle$, $o(\alpha) = 3$, $|H| = e'$ and $(3, e') = 1$. If $A \in \mathbb{Z}[G]$ is a proper $CW(n,9)$, by Lemma 3.3.9,

$$A = B + (P-1)C + (P-2)D + PE \tag{3.12}$$

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 coefficient of α in $AA^{(-1)} = 9$, we obtain

$$|\mathrm{supp}(C)| - |\mathrm{supp}(D)| + 3|\mathrm{supp}(E)| = 0. \tag{3.13}$$

By (3.12), $\eta_P(A) = \eta_P(B) + 2\eta_P(C) + \eta_P(D) + 3\eta_P(E)$. If $|\mathrm{supp}(E)| \geq 1$, then the coefficient of $\eta_P(1)$ in $\eta_P(A)\eta_P(A)^{(-1)} > 9$ as $|\mathrm{supp}(D)|$ is not 0 in this case by (3.13). Hence $|\mathrm{supp}(\eta_P(E))| = 0$ and thus $|\mathrm{supp}(E)| = 0$ as $E \in \mathbb{Z}[H]$. Now by (3.13), $|\mathrm{supp}(\eta_P(C))| = |\mathrm{supp}(\eta_P(D))|$ and thus by comparing the coefficient of $\eta_P(1)$ in $\eta_P(A)\eta_P(A)^{(-1)} = 9$,

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

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

$$\eta_P(A) = \eta_P(B) + 2\gamma h_1 + \epsilon h_2$$

where $\gamma, \epsilon = \pm 1$ and h_1, h_2 are distinct elements in $(G/P) \backslash \mathrm{supp}(\eta_P(B))$. By Lemma 3.3.3, there exists $g \in G/P$ such that

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

Let us write

$$X = \gamma g \eta_P(A) = 2h + X_1 - X_2$$

where $h = gh_1$ and X_1 and X_2 are disjoint subsets of G/P. Note that

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

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

$$4 + |X_1| + |X_2| = 9 \qquad \text{and} \qquad 2 + |X_1| - |X_2| = \pm 3. \tag{3.14}$$

By solving (3.14), we get either $|X_1| = 0$ and $|X_2| = 5$ or $|X_1| = 3$ and $|X_2| = 2$. By Lemma 3.3.4, e' is a divisor of the smallest common multiples of $3 - 1, 3^2 - 1, \ldots, 3^5 - 1$, i.e. $2^4 \times 5 \times 11^2 \times 13$.

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

There exists an element $x \in \mathrm{supp}(X)$ such that $11 \mid o(x)$ as A is proper. Since $\theta(x, 3) = 5$, we have $|X_1| = 0$ and $|X_2| = 5$. Note also that $o(x) = 11, 11^2, 2 \times 11, 2 \times 11^2$. Without the loss of generality, we can assume that $x = gh_2$ and hence

$$\gamma g_0 A = -\sum_{i=1}^{4} {x_0}^{3^i} + (P-1)h_0 + (P-2)x_0$$

where $g_0, h_0, x_0 \in H$ such that $\eta_P(g_0) = g$, $\eta_P(h_0) = h$, $\eta_P(x_0) = x$. Note that $11 \mid o(x_0)$ and $o(h_0) = 1$ or 2. Let $K = \langle x \rangle$. Then $\eta_K(\gamma g_0 A) = -6 + P + (P-1)h_0$ if $o(h_0) = 2$ and $2 \nmid o(x)$, otherwise $\eta_K(\gamma g_0 A) = -7 + 2P$. Note that in both situations, the coefficient of $\eta_K 1$ in $\eta_K(AA^{(-1)}) > 9$.

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

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

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

Clearly $x', h \in K$. Then

$$\eta_K(X) = \begin{cases} 1 - 4\eta_K(x) & \text{if } \varpi = 2^4, \\ 1 - \theta(\eta_K(x), 3) & \text{if } \varpi = 5. \end{cases}$$

where $\eta_K(x)$ is not the identity. This is a contradiction as the coefficient of $\eta_K(1)$ in $\eta_K(X)\eta_K((X)^{(-1)})$ are respectively, 17 and 5.

Case 3: Assume that $n = 13a$ for some positive integer a. There exists an element $x \in \mathrm{supp}(X)$ such that $13 \mid o(x)$ as A is proper. Note that $o(x) = 13$ or 26. Since $\theta(x, 3) = 3$ and there are at most two elements f in G/P such that $f^3 = f$, we have

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

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

Thus $e' = 2^3 = 8$. □

By Theorems 3.3.6 and 3.3.10, we come to the following conclusion.

Theorem 3.3.11 *There exists a proper $CW(n, 9)$ if and only if $n = 13$, 26 or 24.*

Chapter 4

Generalized Dihedral Group Weighing Matrices

In this chapter, we shall first give some basic properties of generalized dihedral group weighing matrices and then followed by a construction of generalized dihedral group weighing matrices of even weight. Lastly, we shall give some non-existent results of proper generalized dihedral group weighing matrices.

4.1 Basic Properties of Generalized Dihedral Group Weighing Matrices

Let $D_H = H \cup \theta H$ be a group where H is a finite abelian group, $o(\theta) = 2$ and $h\theta = \theta h^{-1}$ for all $h \in H$. The group D_H is called a *generalized dihedral group*. If $H \cong C_m$, then D_H is the dihedral group of order $2m$. We shall denote D_m as dihedral group of order $2m$. Below is a basic property of D_H.

Lemma 4.1.1 *All subgroups K of D_H are of the form*

i) K is a subgroup of H; or

ii) $K = L \cup \theta\mu L$ where L is a subgroup of H and $\mu \in H$.

Proof If K is a subgroup of H, then clearly, K is a subgroup of D_H. It is also obvious that K in (ii) is a subgroup of D_H.

Assume that K is not a subgroup of H. Let $L = K \cap H$ and let $\theta\mu$, $\mu \in H$, be an element of K. Then, $g \in L$ implies $\theta\mu g \in K$.

On the other hand, let $g \in K \backslash L$, i.e. $g = \theta h$ for some $h \in H$. But $\theta\mu g \in K$ implies $\mu^{-1}h \in K \cap H = L$. So $h \in \mu L$ or $g \in \theta\mu L$. Hence K has the form of $L \cup \theta\mu L$. □

Assume that there exists a $W(D_H, w)$ says A. Write $A = X + \theta Y \in \mathbb{Z}[D_H]$, where $X, Y \in \mathbb{Z}[H]$.

Proposition 4.1.2 *If $A = X + \theta Y$ is a $W(D_H, w)$, where $X, Y \in \mathbb{Z}[H]$, then*

$$XX^{(-1)} + YY^{(-1)} = w \quad \textit{and} \quad XY^{(-1)} = YX^{(-1)} = 0. \tag{4.1}$$

Proof As $AA^{(-1)} = w$, we have

$$\begin{aligned} w &= (X + \theta Y)(X + \theta Y)^{(-1)} \\ &= XX^{(-1)} + YY^{(-1)} + \theta(YX^{(-1)} + X^{(-1)}Y). \end{aligned}$$

By comparing the coefficients of the above equation , we have $XX^{(-1)} + YY^{(-1)} = w$ and $2YX^{(-1)} = YX^{(-1)} + X^{(-1)}Y = 0$. □

Example 4.1.3 *Let $G = D_4 = \langle a \rangle \cup \theta\langle a \rangle$, where $\theta^2 = 1$ and $o(a) = 4$. Let $A = X + \theta Y \in \mathbb{Z}[G]$, where $X = 1 + g, Y = 1 - g \in \mathbb{Z}[G]$, and $g = a^2$. Note that $XY^{(-1)} = YX^{(-1)} = 0$ and thus $AA^{(-1)} = 4$. Hence A is a $W(G, 4)$ and has the form of $\begin{pmatrix} \Delta_1 & \Delta_2 \\ {\Delta_2}^T & {\Delta_1}^T \end{pmatrix}$ where*

$$\Delta_1 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \textit{ and } \Delta_2 = \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}.$$

Remark 4.1.4 *In general, with a suitable ordering of elements in D_m, every $W(D_m, w)$ can have a matrix form of $\begin{pmatrix} \Delta_1 & \Delta_2 \\ {\Delta_2}^T & {\Delta_1}^T \end{pmatrix}$, where Δ_1 and Δ_2 are both circulant matrices.*

Lemma 4.1.5 *Let $A = X + \theta Y$ be a $W(D_H, w)$ with $X, Y \in \mathbb{Z}[H]$. Then X, Y satisfy* (4.1) *if and only if either $\chi(X)\chi(X^{(-1)}) = w$, $\chi(Y) = 0$ or $\chi(Y)\chi(Y^{(-1)}) = w$, $\chi(X) = 0$ for all $\chi \in H^*$.*

Proof The lemma follows by the fact that X, Y satisfy (4.1) if and only if

$$\chi(X)\chi(X^{(-1)}) + \chi(Y)\chi(Y^{(-1)}) = w \text{ and } \chi(X)\chi(Y^{(-1)}) = \chi(Y)\chi(X^{(-1)}) = 0$$

for all $\chi \in H^*$. □

Let $\mathcal{A} = \{\chi \in H^* \mid \chi(XX^{(-1)}) = w\}$ and $\mathcal{B} = \{\chi \in H^* \mid \chi(YY^{(-1)}) = w\}$. In addition, we know that $\mathcal{A} = \{\chi \in H^* \mid \chi(Y) = 0\}$ and $\mathcal{B} = \{\chi \in H^* \mid \chi(X) = 0\}$. By Proposition 4.1.5, we know that $\{\mathcal{A}, \mathcal{B}\}$ is a partition of H^*. Thus, $|H| = |\mathcal{A}| + |\mathcal{B}|$.

Proposition 4.1.6 *$|\mathcal{A}| = \frac{|H|a}{w}$ and $|\mathcal{B}| = \frac{|H|b}{w}$ where a and b are the coefficients of 1 in $XX^{(-1)}$ and $YY^{(-1)}$ respectively.*

Proof Recall from page 10 that for $g \in H$, we have $\tau_g \in H^{**}$ such that $\tau_g(\chi) = \chi(g)$. By the Fourier Inversion Formula, we have for any $g \in H$,

$$\begin{aligned}
\tau_g(\mathcal{A}) &= \sum_{\chi \in \mathcal{A}} \chi(g) \\
&= \frac{1}{w}\{\sum_{\chi \in H^*} \chi(XX^{(-1)})\chi(g)\} \\
&= \frac{|H|}{w}\{\frac{1}{|H|}\sum_{\chi \in H^*} \chi(XX^{(-1)})\chi(g)\} \\
&= \frac{|H|}{w}(\text{coefficient of } g^{-1} \text{ in } XX^{(-1)}).
\end{aligned}$$

Similarly, we can show that $\tau_g(\mathcal{B}) = \frac{|H|}{w}(\text{coefficient of } g^{-1} \text{ in } YY^{(-1)})$ for any $g \in H$. If $g = 1$, then $\tau_g(\mathcal{A}) = \sum_{\chi \in \mathcal{A}} \chi(1) = |\mathcal{A}|$ and $\tau_g(\mathcal{B}) = \sum_{\chi \in \mathcal{B}} \chi(1) = |\mathcal{B}|$. Thus, $|\mathcal{A}| = \frac{|H|a}{w}$ and $|\mathcal{B}| = \frac{|H|b}{w}$. □

4.2 A Construction of Generalized Dihedral Group Weighing Matrices with Even Weight

We shall now give a construction of generalized dihedral group weighing matrices with even weight. The construction is similar to Construction 2.1.2. Before that, we need the following lemma.

Lemma 4.2.1 *Let H be an abelian group. Let $G = \langle\alpha\rangle \times H$ be a group with $o(\alpha) = 2^s$. Suppose there exists an $E \in \mathbb{Z}[H]$ and $C \in \mathbb{Z}[G/M]$ where $M = \langle\alpha^{2^{s-1}}\rangle$, such that E is a $W(H, w)$ and C is a $W(G/M, w)$. Let $C_1 \in \mathbb{Z}[G]$ such that $\eta_M(C_1) = C$ where η_M is the natural epimorphism from G to G/M. Let $Y = (1 - \alpha^{2^{s-1}})E$ and $X = (1 + \alpha^{2^{s-1}})C_1$. Then*

$$XY^{(-1)} = 0 \qquad \text{and} \qquad XX^{(-1)} + YY^{(-1)} = 4w$$

Proof Note that

$$\begin{aligned} XY^{(-1)} &= (1 + \alpha^{2^{s-1}})(1 - \alpha^{2^{s-1}})C_1E^{(-1)} = 0 \\ XX^{(-1)} &= (2 + 2\alpha^{2^{s-1}})C_1{C_1}^{(-1)} \\ YY^{(-1)} &= (2 - 2\alpha^{2^{s-1}})EE^{(-1)}. \end{aligned}$$

Let χ be a character of G. Suppose $\chi \in M^{\perp}$, i.e. $\chi(\alpha^{2^{s-1}}) = 1$. Then $\chi = \chi' \circ \eta_M$ for some $\chi' \in G/M^*$. Hence $\chi(YY^{(-1)}) = 0$ and $\chi(XX^{(-1)}) = 4\chi'(CC^{(-1)}) = 4w$. Suppose $\chi \notin M^{\perp}$, i.e. $\chi(\alpha^{2^{s-1}}) = -1$. Then $\chi(XX^{(-1)}) = 0$ and $\chi(YY^{(-1)}) = 4\chi(EE^{(-1)}) = 4w$.

Thus $\chi(XX^{(-1)} + YY^{(-1)}) = 4w$ for every $\chi \in G^*$. Hence, the result follows by Corollary 1.4.2. □

Construction 4.2.2 *Let H be an abelian group. Let $G = \langle\alpha\rangle \times H$ be a group with $o(\alpha) = 2^s$. Suppose there exists an $E \in \mathbb{Z}[H]$ and $C \in \mathbb{Z}[G/M], M = \langle\alpha^{2^{s-1}}\rangle$ such*

that E is a $W(H,w)$ and C is a $W(G/M,w)$. Let $C_1 \in \mathbb{Z}[G]$ such that $\eta_M(C_1) = C$ where η_M is the natural epimorphism from G to G/M. Let $Y = (1-\alpha^{2^{s-1}})E$ and $X = (1+\alpha^{2^{s-1}})C_1$. Then $A = X + \theta Y$ is a $W(D_G, 4w)$. In addition, A is proper if for any proper subgroup K of H, supp(X) or supp(Y) is not contained in a cosets of K.

Proof The result is clear by Lemma 4.1.1, Lemma 4.2.1 and Lemma 4.1.5. □

Example 4.2.3 *Let $G = \langle\alpha\rangle \times \langle\beta\rangle \cong C_{14}$ where $o(\alpha) = 2$ and $o(\beta) = 7$. Choose $E = -1 + \beta + \beta^2 + \beta^4$ which is the proper $CW(7,4)$ given in Example 1.2.4, and $C_1 = E$. Let $Y = (1-\alpha)E$ and $X = (1+\alpha)C_1$. Clearly supp(X) and supp(Y) are not contained in the cosets of the same proper subgroup of G. Thus by Construction 4.2.2, we have a proper $W(D_G, 16)$. Similarly, if there exists a proper $W(H,w)$ where H is abelian, then there exists a proper $W(D_H, 4w)$.*

4.3 Some Non-existent Results of Proper Generalized Dihedral Group Weighing Matrices

We start the study of the non-existence results of $W(D_H, w)$.

Proposition 4.3.1 *Let H be an abelian group with size m and A is a $W(D_H, w)$. If $(m,w) = 1$, then A is a trivial extension of a $W(H,w)$.*

Proof If $(m,w) = 1$, then either $\mathcal{A} = 0$ or $\mathcal{B} = 0$ by Proposition 4.1.6. This implies that either $\chi(X)\overline{\chi(X)} = 0$ or $\chi(Y)\overline{\chi(Y)} = 0$ for all $\chi \in H^*$. This follows by either $\chi(X) = 0$ or $\chi(Y) = 0$ for all $\chi \in H^*$, which means that $X = 0$ or $Y = 0$ by Corollary 1.4.2. Hence, A is a trivial extension of a $W(H,w)$. □

Proposition 4.3.2 *Let H be an abelian group with $e = exp(H)$. Let r be some positive integer such that $r^n \equiv 1 \bmod e$. Let G be a semi-direct product of H with K where $K = \langle\beta\rangle$ is a cyclic group of order n and $h\beta = \beta h^r$ for all $h \in H$. If there exists a proper $W(D_H, w)$, then there is a proper $W(G, w)$.*

Proof Suppose $A = X + \theta Y$ is a proper $W(D_H, w)$, where $X, Y \in \mathbb{Z}[H]$. By Proposition 4.1.2,

$$\begin{aligned}
& (X + \beta Y^{(r)})(X + \beta Y^{(r)})^{(-1)} \\
= \;& XX^{(-1)} + \beta^n Y^{(r^n)} Y^{(-r^n)} + \beta Y^{(r)} X^{(-1)} + \beta^{n-1} X^{(r^{n-1})} Y^{(-r^n)} \\
= \;& XX^{(-1)} + YY^{(-1)} + \beta^{n-1} X^{(r^{n-1})} Y^{(-1)} + \beta Y^{(r)} X^{(-1)} \\
= \;& w.
\end{aligned}$$

Hence, $X + \beta Y^{(r)}$ is a $W(HK, w)$.

Suppose that A is not proper. Then $\mathrm{supp}(X + \beta Y) \subset aL$ where L is a proper subgroup of G. Let $K' = H \cap L$. For any $h_1, h_2 \in \mathrm{supp}(X)$, since $\mathrm{supp}(X) \subset aL$, $a^{-1}h_1, a^{-1}h_2 \in L$ and hence

$$h_1{}^{-1}h_2 = (a^{-1}h_1)^{-1}(a^{-1}h_2) \in H \cap L = K'.$$

So $\mathrm{supp}(X) \subset h_1 K'$ where $h_1 \in \mathrm{supp}(X)$. Similarly, $\mathrm{supp}(Y)$ is also contained in a coset of K'. As A is proper, by Lemma 4.1.1, we have $K' = H$ and thus $H \subseteq L$.

Because of $X \neq 0$ and $Y \neq 0$, there exists $g_1 \in \mathrm{supp}(X)$ and $g_2 \in \mathrm{supp}(Y)$ and hence $a^{-1}g_1, a^{-1}\beta g_2 \in L$. Since $H \subseteq L$, $g_1, g_2 \in L$. This implies

$$\beta = (a^{-1}g_1)^{-1}(a^{-1}\beta g_2){g_1}^r {g_2}^{-1} \in L$$

and thus $L = G$. Therefore A is proper. □

Proposition 4.3.3 *Let G be an abelian group and H is a subgroup of G such that G/H is cyclic. If there exists a proper $W(D_H, w)$, then there is a proper $W(G, w)$.*

Proof Suppose $A = X + \theta Y$ is a proper $W(D_H, w)$, where $X, Y \in \mathbb{Z}[H]$. Let $\alpha \in G \backslash H$ such that $G/H = \langle \eta_H(\alpha) \rangle$ where η_H is the natural epimorphism from G to G/H. Define $A' = X + \alpha Y$. Then

$$A'A'^{(-1)} = XX^{(-1)} + YY^{(-1)} + \alpha^{-1}XY^{(-1)} + \alpha YX^{(-1)} = w.$$

Similar to the proof in Proposition 4.3.2, we can prove that A' is proper. □

Corollary 4.3.4 *If there exists a proper $W(D_H, w)$ where H is an abelian group, then there exists a proper $W(H \times K, w)$ for any cyclic group K.*

Proof This corollary is a particular case of Proposition 4.3.2 as well as Proposition 4.3.3. □

Corollary 4.3.5 *Let $H = \langle \alpha \rangle \times H'$ be an abelian group with $o(\alpha) = p^s$ and $(exp(H'), p) = 1$. No proper $W(D_H, p^{2f})$ exists for any odd prime p and $f \geq 1$.*

Proof Assume that there exists a proper $W(D_H, p^{2f})$. Define $G = \langle \gamma \rangle \times H'$ such that $\gamma^{p^i} = \alpha$ and $i + s > f$. By Proposition 4.3.3 there exists a proper $W(G, p^{2f})$ as $G/H \cong C_{p^i}$. But by Corollary 3.2.6, $W(G, p^{2f})$ is not proper as $f < i + s$ where $p^{i+s} = o(\gamma)$. Contradiction occurred and thus no proper $W(D_H, p^{2f})$ exists where p is an odd prime and $f \geq 1$. □

Note that examples of proper $W(D_H, 2^{2f})$ do exist for $f > 0$ by Construction 4.2.2.

Chapter 5

Symmetric Abelian Group Weighing Matrices

In this chapter we shall concentrate on symmetric group weighing matrices of an abelian group G. We first give some properties of symmetric group weighing matrices. Next we give some constructions of symmetric abelian group weighing matrices. Some of the constructions are particular case of those given in chapter 2. Lastly we shall study some exponent bounds on abelian groups that admit symmetric group weighing matrices.

5.1 Some Properties of Symmetric Group Weighing Matrices

Let $A \in \mathbb{Z}[G]$ be a $W(G, w)$. It can be easily checked that the weighing matrix constructed by A is symmetric if and only if

(W3) $A^{(-1)} = A$.

In short, $A \in \mathbb{Z}[G]$ is a *symmetric* $W(G, w)$, denoted as $SW(G, w)$ if it satisfies conditions (W1), (W2) (given in Proposition 1.2.2) and (W3).

Lemma 5.1.1 *Let G be an abelian group. If $A \in \mathbb{Z}[G]$ satisfies $A^2 = \nu^2$ for some integer ν, then for any character χ of G, $\chi(A) = \pm\nu$. In particular, if A is an*

$SW(G, \nu^2)$, then for any character χ of G, $\chi(A) = \pm\nu$.

Proof The first part of the lemma is obvious and the second part is a consequence of conditions (W2) and (W3). □

Lemma 5.1.2 *Let G be an abelian group and A is an $SW(G, \nu^2)$, then $A^{(t)} = A$ for all integers t relatively prime to $n = |G|$.*

Proof The result is clear by Lemma 5.1.1 and Lemma 1.4.6. □

Let G be a group of order n. Recall that as given in section 1.4, for every $g \in G$, g can be used as a character in G^{**}. Suppose $A \in \mathbb{Z}[G]$ satisfies $\chi(A) = \nu$ or ϖ for all characters χ of G where ν and ϖ are two distinct integers. By Lemma 1.4.6, $A^{(-1)} = A$. Define

$$A^*(\nu) = \sum_{\chi \in G^*, \chi(A) = \nu} \chi \in \mathbb{C}[G^*].$$

Then by finite Fourier transform,

$$\widehat{A} = \nu A^*(\nu) + \varpi \left(\sum_{\chi \in G*} \chi - A^*(\nu) \right) = (\nu - \varpi) A^*(\nu) + \varpi \sum_{\chi \in G*} \chi,$$

Hence by Proposition 1.4.4,

$$nA = nA^{(-1)} = \widehat{\widehat{A}} = (\nu - \varpi)\widehat{A^*(\nu)} + \varpi n.$$

We have the following lemma.

Lemma 5.1.3 *Use the notation above. For any $g \in G$*

$$g(A^*(\nu)) = \begin{cases} \dfrac{-\varpi n}{\nu - \varpi} + \dfrac{n}{\nu - \varpi}(\textit{the coefficient of } 1 \textit{ in } A) & \textit{if } g = 1 \\ \dfrac{n}{\nu - \varpi}(\textit{the coefficient of } g \textit{ in } A) & \textit{if } g \neq 1 \end{cases}$$

In particular, if A is an $SW(G, \nu^2)$, then for any $g \in G$,

$$g(A^*(\nu)) = \begin{cases} \dfrac{n}{2} + \dfrac{n}{2\nu}\varepsilon_0 & \textit{if } g = 1 \\ \pm\dfrac{n}{2\nu} & \textit{if } g \neq 1 \textit{ and } g \in \mathrm{supp}(A) \\ 0 & \textit{if } g \neq 1 \textit{ and } g \notin \mathrm{supp}(A) \end{cases}$$

where ε_0 is the coefficient of 1 in A, which is either 0 or ± 1.

Theorem 5.1.4 *Let G be an abelian group of order n. If there exists an $SW(G, \nu^2)$, then n must be divisible by 2ν.*

Proof By Lemma 5.1.3, $g(A^*(\nu))$ are rational for all $g \in G$. Since $g(A^*(\nu)) = \sum_{\chi \in A^*(\nu)} g(\chi) = \sum_{\chi \in A^*(\nu)} \chi(g)$ are contained in $\mathbb{Z}[\zeta_n] \cap \mathbb{Q} = \mathbb{Z}$, we conclude that $n/(2\nu)$ is an integer. □

The following result will be used in section 5.2 and section 5.3.

Lemma 5.1.5 *Let $G = \langle \theta \rangle \times H$ where $o(\theta) = 2$ and H is an abelian group of odd order. If A is an $SW(G, \nu^2)$ where ν is odd, then*

$$hA = 1 + (1 + \theta)B + (1 - \theta)C$$

where $h = \pm 1$ or $\pm\theta$, $B, C \in \mathbb{Z}[H]$, coefficients of B, C are $0, \pm 1$, the support of $1, B, C$ are pairwise disjoint, $B^{(-1)} = B$, $C^{(-1)} = C$,

$$(1 + 2B)(1 + 2B^{(-1)}) = \nu^2 \quad \textit{and} \quad (1 + 2C)(1 + 2C^{(-1)}) = \nu^2.$$

Proof Since $A^2 = AA^{(-1)} = \nu^2$, $A^{(2)} \equiv A^2 \equiv 1 \bmod 2$. We have

1. either 1 or θ is contained in $\mathrm{supp}(A)$ but not both; and
2. for any $g \in H \backslash \{1\}$, either both g and θg are contained in $\mathrm{supp}(A)$ or both not.

So $hA = 1 + (1 + \theta)B + (1 - \theta)C$ where $h = \pm 1$ or $\pm\theta$, $B, C \in \mathbb{Z}[H]$, coefficients of B, C are $0, \pm 1$ and the support of $1, B, C$ are pairwise disjoint. Note that $B^{(-1)} = B$ and $C^{(-1)} = C$ as $(hA)^{(-1)} = hA$. Finally $(1 + 2B)(1 + 2B^{(-1)}) = \nu^2$ and $(1 + 2C)(1 + 2C^{(-1)}) = \nu^2$ as $(hA)(hA)^{(-1)} = \nu^2$. □

5.2 Constructions of Symmetric Group Weighing Matrices

We shall first go through the construction in chapter 2 that will give us symmetric weighing matrices. Note that a difference set (divisible difference set) D is said to be *reversible* if $D^{(-1)} = D$. The following construction is a particular case of Construction 2.2.3.

Construction 5.2.1 *Let D be a reversible $(4m^2,\ 2m^2-m,\ m^2-m)$-difference set in a group G. Then $A = D-(G-D) = 2D-G$ is a proper $SW(G, 4m^2)$.*

Example 5.2.2 *Let $G = \mathbb{Z}_4^b \times \mathbb{Z}_{2^{c_1}}^2 \times \cdots \times \mathbb{Z}_{2^{c_r}}^2$ where $b, c_1, \ldots, c_r$ are nonnegative integers and let $H = \mathbb{Z}_2^2 \times \mathbb{Z}_3^{2d} \times \mathbb{Z}_{p_1}^4 \times \cdots \times \mathbb{Z}_{p_s}^4$ where d is a nonnegative integer and $p_1, \ldots, p_s$ are odd primes. By Theorem 14.46 in Chapter VI of [11], we know that reversible Hadamard difference sets required by Construction 5.2.1 exist in G and $G \times H$. Hence there exist proper $SW(G, 4m_1^2)$ and $SW(G \times H,\ 4m_2^2)$ where $m_1 = 2^{b+c_1+\cdots+c_r-1}$ and $m_2 = 2^{b+c_1+\cdots+c_r} 3^d p_1^2 \cdots p_s^2$.*

The next construction is a particular case of Construction 2.2.6.

Construction 5.2.3 *Let $G = \langle\theta\rangle \times H$ where $o(\theta) = 2$. If there exists a reversible (v, k, λ)-difference set $D = X \cup \theta Y$, $X, Y \subset H$, in G, then $A = X - Y$ is an $SW(H, k-\lambda)$.*

Example 5.2.4 *Let D be a $(4000, 775, 150))$ McFarland Difference set in $G = {\mathbb{Z}_2}^5 \times {\mathbb{Z}_5}^3$. Thus by Construction 5.2.3 and Theorem 2.2.7, there exists a proper $SW({\mathbb{Z}_2}^4 \times {\mathbb{Z}_5}^3, 625)$.*

Example 5.2.5 *Let $H = \mathbb{Z}_2 \times \mathbb{Z}_3^{2d} \times \mathbb{Z}_{p_1}^4 \times \cdots \times \mathbb{Z}_{p_s}^4$ and $G = \mathbb{Z}_2 \times H$ where d is a nonnegative integer and $p_1, \ldots, p_s$ are odd primes. By Theorem 14.46 in Chapter*

VI of [11], we know that reversible $(4m^2, 2m^2 - m, m^2 - m)$*-Hadamard difference sets exist in* G *with* $m = 3^d p_1^2 \cdots p_s^2$ *and hence there exist proper* $SW(H, m^2)$ *as* m *is odd.*

By [11], we know that if D is a reversible difference set, then either D is a $(4000, 775, 150)$-difference set or D is a $(4m^2, 2m^2 - m, m^2 - m)$-Hadamard difference set.

Construction 5.2.6 *Let* $G = \langle\theta\rangle \times G'$ *be a finite group where* $o(\theta) = 2$*. Let* $N = \langle\theta\rangle \times N'$ *be a subgroup of* G*. Suppose* G *admits a reversible* $(|G|/|N|, |N|, k, \lambda_1, \lambda_2)$*-divisible difference set* $X \cup \theta Y$ *where* $X, Y \subset G'$*, then* $X - Y$ *is an* $SW(G', k - \lambda_1)$*.*

It is clear that Construction 5.2.6 is a particular case of Construction 2.3.3. Below are two examples constructed from two known families of reversible relative difference sets.

Example 5.2.7 *By [4], We know that if there exists a reversible* $(4m^2, 2m^2 \pm m, m^2 \pm m)$*-Hadamard difference set* D' *in a group* K*, then* $D = (\{0\} \times D') \cup (\{1\} \times (G \backslash D'))$ *is a reversible* $(4m^2, 2, 4m^2, 2m^2)$*-relative difference set in* $\mathbb{Z}_2 \times K$ *relative to* $\mathbb{Z}_2 \times \{1\}$*. Thus by Construction 5.2.6 and Theorem 2.3.5, we have proper* $SW(K, 4m^2)$*. Note that the weighing matrices constructed are actually Hadamard matrices. These matrices are the same as those constructed using Construction 5.2.1.*

Example 5.2.8 *Let* R *be a finite local ring with maximal idea* I *such that* $R/I \cong GF(2^d)$ *and* $I^s = 0$*. Let* H *be an elementary 2-group with* 2^t *elements where* $0 < t \leq d$*. By [28], we know that there exists a reversible* $(2^{2sd}, 2^t, 2^{2sd}, 2^{2sd-t})$*-relative difference set in* $H \times R \times R$ *relative to* $H \times \{0\} \times \{0\}$*. Thus by Construction 5.2.6 and Theorem 2.3.5, we have proper* $SW(H', 2^{2sd} - 2^{2sd-t})$ *where* H' *is an*

elementary 2-group with 2^{t-1} elements. In Construction 5.2.11, we shall study a more general construction which gives us all the matrices in this example.

Construction 5.2.9 *In Construction 2.4.3, if ${g_i}^2 = 1$ for all i, then A is an $SW(G, q^{2s})$.*

Example 5.2.10 *In Construction 5.2.9, suppose $q > 2$. Let $K = \langle\theta_1\rangle \times \cdots \times \langle\theta_f\rangle$ be an elementary 2-group and $f \leq (r-1)/2$. We can choose the set $J = \{g_0, g_1, \ldots, g_{(r-1)/2}\}$ such that J is not contained in any coset of any proper subgroup in K. In particular, choose J such that $1, \theta_1, \ldots, \theta_f \in J$. Then by Construction 5.2.9 and Theorem 2.4.4, A is a proper $SW(K \times L, q^{2s})$ where L is the $(s+1)$-dimensional vector space over $GF(q)$ that is given in Construction 2.4.3.*

Construction 5.2.11 *In Construction 2.5.1, if ${g_i}^2 = 1$ for all i, then A is an $SW(G, 2^{2sd})$.*

Example 5.2.12 *In Construction 5.2.11, Let K be an elementary 2-group such that $|K| \leq 2^{2^{d-1}-1}$ and let $g_1, g_2, \ldots, g_{2^{d-1}}$ be elements (not necessarily distinct) of K. Same as Example 5.2.10, we can choose the set $J = \{g_1, g_2, \ldots, g_{2^{d-1}}\}$ such that J is not contained in any coset of any proper subgroup in K. Then by Construction 5.2.11 and Theorem 2.5.4, A is a proper $SW(K \times R \times R, 2^{2sd})$ where R is the local ring that is given in Construction 2.5.1.*

The idea of the next construction comes from Lemma 5.1.5.

Construction 5.2.13 *Let H be a finite group and $B, C \in \mathbb{Z}[H]$ such that the coefficients of B, C are $0, \pm 1$, the supports of $1, B, C$ are pairwise disjoint,*

$$(1+2B)(1+2B^{(-1)}) = \nu^2 \quad \textit{and} \quad (1+2C)(1+2C^{(-1)}) = \nu^2$$

for some integer ν. Let $G = \langle\theta\rangle \times H$ where $o(\theta) = 2$. Then

$$A = 1 + (1+\theta)B + (1-\theta)C$$

is a $W(G, \nu^2)$. Furthermore, if $B^{(-1)} = B$ and $C^{(-1)} = C$, then A is an $SW(G, \nu^2)$.

Proof Note that $(1+2B)(1+2B^{(-1)}) = (1+2C)(1+2C^{(-1)}) = \nu^2$ implies $B + B^{(-1)} + 2BB^{(-1)} = C + C^{(-1)} + 2CC^{(-1)} = (\nu^2 - 1)/2$. Thus

$$\begin{aligned} AA^{(-1)} &= [1 + (1+\theta)B + (1-\theta)C]\left[1 + (1+\theta)B^{(-1)} + (1-\theta)C^{(-1)}\right] \\ &= 1 + (1+\theta)\left[B + B^{(-1)} + 2BB^{(-1)}\right] + (1-\theta)\left[C + C^{(-1)} + 2CC^{(-1)}\right] \\ &= 1 + (1+\theta)\frac{\nu^2-1}{2} + (1-\theta)\frac{\nu^2-1}{2} = \nu^2. \end{aligned}$$

□

Example 5.2.14 *Let $H = \mathbb{Z}_{p_1}^4 \times \cdots \times \mathbb{Z}_{p_s}^4$ where for each i, p_i is a prime and $p_i \geq 5$. Let $G = \langle\theta\rangle \times H$ where $o(\theta) = 2$. By Theorem 14.46 in Chapter VI of [11], we have an $SW(G, \nu^2)$ say A with $\nu = p_1^2 p_2^2 \cdots p_s^2$. Thus by Lemma 5.1.5*

$$hA = 1 + (1+\theta)B + (1-\theta)C$$

where $h = \pm 1$ or $\pm\theta$, $B, C \in \mathbb{Z}[H]$, coefficients of B, C are $0, \pm 1$, the support of $1, B, C$ are pairwise disjoint, $B^{(-1)} = B$, $C^{(-1)} = C$,

$$(1+2B)(1+2B^{(-1)}) = \nu^2 \quad \textit{and} \quad (1+2C)(1+2C^{(-1)}) = \nu^2.$$

By comparing the coefficient of the identity of the two equations above, we learn that $|supp(B)| = |supp(C)| = (\nu^2 - 1)/4$. Since $p_i \geq 5$ for all i, both $supp(B)$ and $supp(C)$ cannot be contained in any coset of any proper subgroup of H. Let $G' = \langle\theta\rangle \times K_1 \times K_2 \times K_3$ be a group such that $K_1 \times K_2 \cong K_2 \times K_3 \cong H$. Let $\phi : H \to K_1 \times K_2$ and $\psi : H \to K_2 \times K_3$ be isomorphisms such that $\phi^{-1}(g) = \psi^{-1}(g)$ for all $g \in K_2$. Note that if the supports of $1, B, C$ are pairwise disjoint, then the supports of $1, \phi(B), \psi(C)$ are pairwise disjoint. Then

$$A' = 1 + (1+\theta)\phi(B) + (1-\theta)\psi(C)$$

is a proper $SW(G', \nu^2)$ *as it is clear that* $\phi(B)^{(-1)} = \phi(B)$, $\psi(C)^{(-1)} = \psi(C)$;

$$(1 + 2\phi(B))(1 + 2\phi(B^{(-1)})) = \nu^2 \quad \textit{and} \quad (1 + 2\psi(C))(1 + 2\psi(C^{(-1)})) = \nu^2.$$

5.3 Exponent Bounds on Abelian Groups Admit Symmetric Group Weighing Matrices

In this section, we shall study the exponent bounds on abelian groups that admit symmetric group weighing matrices.

Theorem 5.3.1 *Let* G *be an abelian group of order* n *and exponent* e. *Let* p *be a prime divisor of* n *such that* $p^r || n$ *and* $p^s || e$. *Suppose there exists an* $SW(G, \nu^2)$ *such that* $p^t || \nu$. *Then* $s \leq r - t$ *if* p *is odd; and* $s \leq r - t + 1$ *if* $p = 2$.

Proof Assume that $s > r - t$ if p is odd; and $s > r - t + 1$ if $p = 2$. Let K be a p-subgroup of G such that the Sylow p-subgroup of G/K is a cyclic group of order p^s and let $\eta_K : G \to G/K$ be the natural epimorphism. Let A be an $SW(G, \nu^2)$. Since $\eta_K(A)^2 = \eta_K(A^2) = \nu^2$, we have $\chi(\eta_K(A)) = \pm\nu \equiv 0 \bmod p^t$ for all characters χ of G/K. By Ma's Lemma (Lemma 1.4.5), there exist $X_1, X_2 \in \mathbb{Z}[G/K]$ such that

$$\eta_K(A) = p^t X_1 + P X_2$$

where P is the unique subgroup of G/K of order p. Let h be any element of P. Then

$$(1 - h)\eta_K(A) = p^t(1 - h)X_1.$$

The coefficients on the left-hand-side lie between $-2p^{r-s}$ and $2p^{r-s}$. Since $2p^{r-s} < p^t$, the only possible solution is $(1 - h)\eta_K(A) = 0$. So we have $h\eta_K(A) = \eta_K(A)$ for all $h \in P$, i.e. $\eta_K(A) = PX$ for some $X \in \mathbb{Z}[G/K]$. But $\eta_K(A)^2 = pPX^2$ contradicts that of $\eta_K(A)^2 = \nu^2$. □

For the next bound, we need to work on the dual group, i.e. the group of characters. The notation used below follows that is defined in page 56 of Section 5.1.

Lemma 5.3.2 *Let G be an abelian group of exponent e and let p be a prime divisor of e such that $p^s||e$. Suppose $A \in \mathbb{Z}[G]$ satisfies $\chi(A) = \nu, \varpi$ for all characters χ of G where ν and ϖ are two distinct integers. If there is $g \in supp(A)$ such that $p^s \mid o(g)$, then there exists a p-subgroup K^* of G^* such that the Sylow p-subgroup of G^*/K^* is a cyclic group of order p^s and*

$$\eta^*_{K^*}(A^*(\nu)) \not\equiv 0 \bmod P^*$$

where $\eta^*_{K^*} : G^* \to G^*/K^*$ is the natural epimorphism and P^* is the unique subgroup of G^*/K^* of order p.

Proof Let $g \in G$ such that g is an element in the support of A and $p^s|o(g)$. We use g as a character of G^*. Let

$$K^* = \ker(g) \cap (\text{the Sylow } p\text{-subgroup of } G^*).$$

Note that K^* is a p-subgroup of G^* such that the Sylow p-subgroup of G^*/K^* is a cyclic group of order p^s. Let $\eta^*_{K^*} : G^* \to G^*/K^*$ be the natural epimorphism. Then there exists a character h of G^*/K^* such that $h \circ \eta^*_{K^*} = g$. Assume that

$$\eta^*_{K^*}(A^*(\nu)) \equiv 0 \bmod P^*$$

where P^* is the unique subgroup of G^*/K^* of order p. Since $\ker(h) = \ker(g)/K^*$, h is nonprincipal on P^* and hence

$$g(A^*(\nu)) = h(\eta^*_{K^*}(A^*(\nu))) = 0.$$

This contradicts Lemma 5.1.3 and that g is an element in the support of A. □

Theorem 5.3.3 *Let G be an abelian group of exponent e and let p be a prime divisor of e such that $p^s||e$. Suppose there exists a proper $SW(G,\nu^2)$ such that $p^t||\nu$. Then $s \leq t$ if p is odd; and $s \leq t+2$ if $p=2$.*

Proof Assume that $s > t$ if p is odd; and $s > t+2$ if $p = 2$. Let K^* be any p-subgroup of G^* such that the Sylow p-subgroup of G^*/K^* is a cyclic group of order p^s and let $\eta^*_{K^*} : G^* \to G^*/K^*$ be the natural epimorphism. Suppose $p^r||\,|G|$. Let A be an $SW(G,\nu^2)$. By Lemma 5.1.3, for all characters h of G^*/K^*, $h(\eta^*_{K^*}(A^*(\nu))) \equiv 0 \bmod p^{t'}$ where $t' = r-t$ if p is odd and $t' = r-t-1$ if $p=2$. By Ma's Lemma (Lemma 1.4.5), there exist $Y_1, Y_2 \in \mathbb{Z}[G^*/K^*]$ such that

$$\eta^*_{K^*}(A^*(\nu)) = p^{t'}Y_1 + P^*Y_2$$

where P^* is the unique subgroup of G^*/K^* of order p. Following the same argument as in the proof of Theorem 5.3.1, we have $\eta^*_{K^*}(A^*(\nu)) = P^*Y$ for some $Y \in \mathbb{Z}[G^*/K^*]$. By Lemma 5.3.2, A cannot be proper. □

As a consequence of Theorems 5.1.4 and 5.3.3, we have the following corollary.

Corollary 5.3.4 *Let G be an abelian group of order n. Suppose there exists a proper $SW(G,\nu^2)$. Then n and ν have the same odd prime divisors.*

The bound in Theorem 5.3.3 can be improved for the following case. First, we need a lemma.

Lemma 5.3.5 *Let G be a cyclic group of order p^s where p is a prime. If $A \in \mathbb{Z}[G]$ such that $A^{(t)} = A$ for all integers t relatively prime to p, then*

$$A = b_0P_0 + b_1P_1 + \cdots + b_sP_s$$

where $b_0, b_1, \ldots, b_s$ are integers and for $i = 1, \ldots, s$, P_i is the unique subgroup of order p^i in G.

Proof This result is a consequence of the fact that if $g \in P_i \backslash P_{i-1}$ for some i, then $\{g^t \mid (t,p) = 1\} = P_i \backslash P_{i-1}$. □

Theorem 5.3.6 *Let p be a prime such that $p \geq 5$. If there exists a proper $SW(G, p^{2t})$ where G is an abelian group of order $2p^r$, then $exp(G) = 2p^s$ for $s < t$.*

Proof Let $G = \langle\theta\rangle \times H$ be a group where $o(\theta) = 2$ and H is an abelian group of order p^r and exponent p^s. By Theorem 5.3.3, it suffices to show that there is no proper $SW(G, p^{2s})$. Suppose $A \in \mathbb{Z}[G]$ is an $SW(G, p^{2s})$. By Lemma 5.1.5,

$$hA = 1 + (1+\theta)B + (1-\theta)C$$

where $h = \pm 1$ or $\pm\theta$, $B, C \in \mathbb{Z}[H]$, the coefficients of B, C are $0, \pm 1$, the supports of $1, B, C$ are pairwise disjoint, $B^{(-1)} = B$, $C^{(-1)} = C$,

$$(1+2B)(1+2B^{(-1)}) = p^{2s} \text{ and } (1+2C)(1+2C^{(-1)}) = p^{2s}.$$

For any character χ of H,

$$\chi(B) = (-1 \pm p^s)/2 \text{ and } \chi(C) = (-1 \pm p^s)/2.$$

Let K^* be a subgroup of H^* such that H^*/K^* is a cyclic group of order p^s and let $\rho : H^* \to H^*/K^*$ be the natural epimorphism. Let $\nu = (-1+p^s)/2$ and $\varpi = (-1-p^s)/2$. Note that for any character h of H^*/K^*, $h \circ \rho$ is a character of H^*. Also, we know that $h \circ \rho$ is the principal character of H^* when $h = 1$. By Lemma 5.1.3, as $n = |H| = p^r$ and $1 \notin \text{supp}(B)$, we have

$$h(\rho(B^*(\nu))) = \begin{cases} \frac{1}{2}(p^r + p^{r-s}) & \text{if } h = 1 \\ 0, \pm p^{r-s} & \text{if } h \neq 1. \end{cases}$$

By Lemma 1.4.6 and Lemma 5.3.5, we can write

$$\rho(B^*(\nu)) = b_0 P_0^* + b_1 P_1^* + \cdots + b_s P_s^* \tag{5.1}$$

where $b_0, b_1, \ldots, b_s$ are integers and for $i = 1, \ldots, s$, P_i^* is the unique subgroup of order p^i in H^*/K^*. Here, $P_s^* = H^*/K^*$ and $P_0^* = \{\chi_0\}$ where χ_0 is the identity element in H^*/K^*. Note that the coefficients of the left hand side of (5.1) lie between 0 and p^{r-s} while $b_i + b_{i+1} + \cdots + b_s$ is the coefficient of $P_i * \backslash P_{i-1} *$ in $\rho(B * (\mu))$. Thus for $i = 0, 1, \ldots, s$,

$$0 \leq b_i + b_{i+1} + \cdots + b_s \leq p^{r-s}.$$

Let $h_0 = 1$ and for $i = 1, \ldots, s$, let h_i be the character of H^*/K^* that is nonprincipal on P_i^* but principal on P_{i-1}^*. Then $b_0 = h_1(\rho(B^*(\nu)))$. Note that $h_i(\rho(B^*(\nu))) = p^{i-1}b_{i-1} + p^{i-2}b_{i-2} + \cdots + b_0$ and thus $b_i p^i = h_{i+1}(\rho(B^*(\nu))) - h_i(\rho(B^*(\nu)))$ for $i = 1, \ldots, s$. Hence, $|b_i p^i| \leq 2p^{r-s}$ for $i = 1, \ldots, s-1$. Note also that $h_{s+1} = h_0$. Hence $b_s p^s = \frac{1}{2}[p^r + (1 - 2\varepsilon)p^{r-s}]$, where $\varepsilon = 0, \pm 1$. Thus

1. $b_0 = 0, \pm p^{r-s}$;

2. for $i = 1, \ldots, s-1$, $|b_i| \leq 2p^{r-s-i}$; and

3. $b_s = \frac{1}{2}[p^{r-s} + (1 - 2\varepsilon)p^{r-2s}]$, where $\varepsilon = 0, \pm 1$, and hence $\frac{1}{2}(p^{r-s} - p^{r-2s}) \leq b_s \leq \frac{1}{2}(p^{r-s} + 3p^{r-2s})$.

If $b_0 = -p^{r-s}$, then

$$\begin{aligned} b_0 + b_1 + \cdots + b_s &\leq -p^{r-s} + (2p^{r-s-1} + \cdots + 2p^{r-2s+1}) + \frac{p^{r-s} + 3p^{r-2s}}{2} \\ &= \frac{-(p-5)p^{r-s} - (p-3)p^{r-2s}}{2(p-1)} < 0, \end{aligned}$$

is a contradiction.

If $b_0 = p^{r-s}$, then

$$\begin{aligned} b_0 + b_1 + \cdots + b_s &\geq p^{r-s} - (2p^{r-s-1} + \cdots + 2p^{r-2s+1}) + \frac{p^{r-s} - p^{r-2s}}{2} \\ &= p^{r-s} + \frac{(p-5)p^{r-s} + (3p+1)p^{r-2s}}{2(p-1)} > p^{r-s}, \end{aligned}$$

is also a contradiction.

The only possible solution is $b_0 = 0$. But this means

$$\rho(B^*(\nu)) \equiv 0 \bmod P_1^*.$$

By Lemma 5.3.2, B is contained in a subgroup of H of exponent p^{s-1}. Following the same argument, C is also contained in a subgroup of H of exponent p^{s-1}. So A is not proper. □

Corollary 5.3.7 *Let p be a prime such that $p \geq 5$. There exists no $SW(G, p^2)$ in any abelian group G of order $2p^r$.*

For all the known examples, the Sylow p-subgroups of the groups that admit symmetric group weighing matrices are all elementary except $p = 2$. Also, for $p \geq 5$, we do not have any symmetric group weighing matrices of weight ν^2 such that $p^{2t+1}||\nu$.

Bibliography

[1] Antweiler M., Bömer L. and Lüke H. D., Perfect Ternary Arrays, *IEEE Tranc. Inform. Theory*, 36(1990), 696-705.

[2] Arasu K.T. and Dillon J.F, Perfect ternary arrays, in Different Sets, sequences and Their Correlation Properties, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 542, Kluwer Acad. Publ., Dordrecht, 1999, 1-15.

[3] Arasu K. T., Dillon J.F., Leung K.H. and Ma S.L., Cyclic relative Difference Sets with Classical Parameters, *J. of Combin. Theory Series A*, 94(2001), 118-126.

[4] Arasu K.T., Jungnickel D. and Pott A., Divisible difference sets with multiplier -1, *J. Algebra*, 133(1990), 35-62.

[5] Arasu K.T. and Ma S.L., Some new results on circulant weighing matrices, *Journal of Algebraic Combinatorics*, 14(2001), 91-101.

[6] Arasu K.T. and Ma S.L., A nonexistence result on difference sets and divisible difference sets, *Journal of Statistical Planning and Inference*, 95(2001), 67-73.

[7] Arasu K.T. and Seberry J., Circulant weighing matrices, *J. Combin. Designs*, 4(1996), 439-447.

[8] Arasu K.T. and Seberry J., On circulant weighing matrices, *Australasian J. Combin.*, 17(1998), 21-37.

[9] Arasu K.T. and Torban D., New weighing matrices of weight 25, *J. Combin. Designs*, 7(1999), 11-15.

[10] Arasu K.T. and Xiang Q., Multiplier Theorems, *J. Comb. Designs*, 3(1995), 257-268.

[11] Beth T., Jungnickel D. and Lenz H. (1999). *Design Theory*, 2nd edition, Cambridge University Press, Cambridge.

[12] Bömer L. and Antweiler M., Perfect binary Arrays with 36 elements, *Electron. Lett.*, 23(1987), 730-732.

[13] Calabro D. and Wolf J.K, On The synthesis of two-dimensional arrays with desirable correlation properties, *Informa. Contr.*, 11(1968), 537-560.

[14] Chan Y. K., Siu M. K. and Tong P., Two dimensional binary arrays with good autocorrelation, *Informa. Contr.*, 42(1979), 125-130.

[15] Chang J. A., Ternary Sequences with Zero correlation *Proceeding of the IEEE*, 55(1967), 1211-1213.

[16] Craigen R., Weighing matrices and conference matrices, in *The CRC Handbook of Combinatorial Designs*, eds. C.J. Conlbourn and J.H. Dinitz, CRC Press, Boca Raton, 1996, 496-504.

[17] Dillon J.F., The Waterloo Problem, in F. Hoffman (ed.), Proceedings of the tenth southeastern Conference on Combinatorics, Graph Theory and Computing, Congressus Numerantium XXIV, Utilitas Math. Publishing Co., Winnipeg, 1979, pg. 924.

[18] Eades P. and Hain R. M., Circulant Weighing Matrices, *Ars Combinatorica*, 2(1976), 265-284.

[19] Elliott J. E. H. and Butson A. T., Relative Difference Sets *Illinois J. Math.*, 10(1966), 517-531.

[20] Games R.A., The Geometry of quadrics and correlations of sequences, *IEEE Trans. Inform. Theory*, 32(1986), 423-426.

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

[22] Gordon James and Martin Liebeck (1993), *Representation and Characters of Groups*, Cambridge University Press, Britain.

[23] Høholdt T. and Justesen J., Ternary Sequences with perfect periodic autocorrelation, *IEEE Trans. Inform. Theory*, 29(1983), 597-600.

[24] Hou X.D., Leung K.H. and Ma S.L., On the groups of units of finite commutative chain rings, *Finite Field Appl.*, 9(2003), 20-38.

[25] Ipatov V.P., Contribute to the theory of sequences with perfect periodic autocorrelation properties *Radio Eng. Electron. Phys.*, 25(April 1980), 31-34.

[26] Ipatov V.P., Platonov V.D. and Samilov I.M., A New Class of Ternary Sequences with ideal periodic autocorrelation properties, *Soviet Math. (Izvestiya Vuz) English Translation*, 27(1983), 57-61.

[27] Jedwaib J. and Mitchell C., Constructing New Perfect Binary Arrays, *Electron. Lett.*, 24(1988), 650-652.

[28] Leung K.H. and Ma S.L., Construction of partial difference sets and relative difference sets on p-groups, *Bull. London Math. Soc.*, 22(1990), 533-539.

[29] Leung K.H. and Ma S.L., Preprint *Circulant matrices of weight* 2^{2t}.

[30] Leung K.H., Ma S.L. and Schmidt B., Constructions of relative difference sets with classical parameters and circulant weighing matrices, *J. of Combin. Theory Series A*, 99(2002), 111-127.

[31] Leung K.H. and Schmidt B., The field descent method, in preparation.

[32] Lüke H. D., Sequences and Arrays with Perfect Periodic Correlation, *IEEE Trans. Aerosp. Electron. Syst.*, AES-24(1988), 287-294.

[33] Lüke H. D., Zweidimensionsionale Folgen mit perfekten periodischen Korrelationfunktionen, *IEEE Trans. Aerosp. Electron. Syst.*, 41(1987), 131-137.

[34] Lüke H. D. and Bömer L., Perfect Binary Arrays, *Signal Processing*, 17(1989), 69-80.

[35] Ma S.L., Planar Function, Relative Different Sets, and Character Theory, *J. of Algebra*, 185(1996), 342-356.

[36] Ma S.L., reversible relative difference sets, *Combinatorica*, 12(1992), 425-432.

[37] Mac Williams F.J. and Sloane N.J.A., Pseudo-random Sequences and Arrays, *Proc. IEEE*, 64(1976), 1715-1729.

[38] Martin Isaacs I. (1994), *Character Theory of Finite Groups*, Dover Publications, INC., New York.

[39] McDonald B.R. (1974), *Finite Rings with Identity*, Dekker, New York.

[40] McFarland R.L., A family of difference sets in non-cyclic groups, *J. Combin. Theory Ser. A*, 15(1970), 1-10.

[41] Menon P.K., On difference sets whose parameters satisfy a certain relation, *Proc. Amer. Math. Soc.*, 13(1962), 739-745.

[42] Moharir P. S., Generalized PN Ternary Sequences *IEEE Trans. Inform. Theory*, 23(1977), 782-784.

[43] Mullin R.C., A note on Balanced weighing Matrices, in Combinatorical Mathematics III, Preceeding of the third Australian Conference, Lecture Notes in Mathematics 452, Spring of Berlin-Heidelberg, New York, 1975, 28-41.

[44] Mullin R.C. and Stanton R.G., Group Matrices and Balanced weighing designs, *Utilities Math.*, 8(1975), 277-301.

[45] Mullin R.C. and Stanton R.G., Balanced weighing designs and Group Divisible Designs, *Utilities Math.*, 8(1975), 303-310.

[46] Pott A. (1995). Finite Geometry and Character Theory, Lecture Notes in Mathematics, **1601**, Springer, Berlin.

[47] Raghavarao D., Some Aspects of Weighing Designs, *Ann. Math. Stat.*, 31 (1960), 878-884.

[48] Raghavarao D.(1971). Constructions and Combinatorial Problems in Design of Experiments, Wiley Series in Probability and Mathematical Statistics, John Wiley and Sons Inc, New York.

[49] Singer J., A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.*, 43(1938), 377-385.

[50] Sloane Neil J.A. and Harwit Martin, Mask for Hadamard Transform Optics and Weighing Designs, Appl. Optics, 15(1975), 107-114.

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

[52] Turyn R., Sequences with small correlation, in Error Correcting Codes, ed. H.B. Mann, Wiley, New York, 1969, 195-228.

[53] Vincent A., Applications of Combinatorial designs to the theory of communications, Phd thesis, RHBNC, University of London, (1989).

[54] Wallis (Seberry) J. and Whiteman A.L., Some Results on Weighing Matrices, *Bull. Austral. Math. Soc.*, 12(1975), 433-447.

[55] Wild P., Infinite Families of Perfect Binary Arrays, *Electron. Lett.*, 24(1988), 845-847.