Proper Circulant Weighing Matrices of Weight p^2

by

K.H. Leung and S.L. Ma

National University of Singapore

Weighing Matrices

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

$$M\,M^{\mathrm{T}} = n\,I$$

where I is the identity matrix of order n and M^{T} is the transpose of M.

The matrix $M = (b_{ij})$ is called circulant if every row is obtained from the previous row by a cyclic shift to the right, i.e. for all i and j, $b_{ij} = b_{1,\,j-i}$.

Perfect Sequences

Suppose $M=(b_{ij})$ is a circulant weighing matrix of order v and weight n.

Let $a_i = b_{1,j+1}$ for $j = 0, 1, ..., v-1$.

Then the sequence $(a_0, a_1, ..., a_{v-1})$ is a perfect sequence.

A perfect sequence is a sequence $\boldsymbol{a} = (a_0, a_1, ..., a_{v-1})$ with zero out-of-phase auto-correlation, i.e.

$$\mathrm{Aut}_{\boldsymbol{a}}(t) = \frac{1}{v}\sum_{j=0}^{v-1} a_j a_{j+t \ (\mathrm{mod}\ v)} = 0$$

for all $t \not\equiv 0 \pmod{v}$.

Group Matrices

Let G be a finite of order v and $A = \sum_{g \in G} a_g g \in \mathbf{Z}[G]$.

Define the group matrix $M = (b_{gh})_{g,h \in \mathrm{G}}$, where the rows and columns of M are indexed by the elements of G and $b_{gh} = a_\gamma$ if $gh^{-1} = \gamma$.

If G is cyclic, then with a proper indexing of rows and columns, M is a circulant matrix.

$W(G, n)$ and $CW(v, n)$

M is a weighing matrix of weight n if and only if A satisfies

(W1) $a_g \in \{-1, 0, +1\}$;

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

where $A^{(-1)} = \sum_{g \in G} a_g g^{-1} \in \mathbf{Z}[G]$.

A is called a $W(G, n)$ if it satisfies (W1) and (W2).

If G is cyclic, A is called a $CW(v, n)$.

Proper Group Weighing Matrices

Obviously, if H is a subgroup of G and $A \in \mathbf{Z}[H]$ is a $W(H, n)$, then by regarding A as an element in $\mathbf{Z}[G]$, it is clear that gA is a $W(G, n)$ for any $g \in G$.

To classify all group weighing matrices, it is natural to ignore these types.

$A \in \mathbf{Z}[G]$ is called proper if the support of A is not contained in any coset of any proper subgroup of G.

(The corresponding group matrix is also called proper.)

$CW(v, 4)$

Proper $CW(v, 4)$ exits if and only if either v is even or $v = 7$. (Eades and Hain, 1976)

Let G be a cyclic group of order v. If $A \in \mathbf{Z}[G]$ is a $CW(v, 4)$, then there exist $g \in G$ and t an integer relatively prime to v such that either $gA^{(t)}$ or $-gA^{(t)}$ is equal to the one of the A_i listed.

1. With $\gamma, a, b \in G$ such that $o(\gamma) = 2$ and $\{a, \gamma a\} \cap \{b, \gamma b\} = \varnothing$,

$$A_1 = (1 + \gamma)\,a + (1 - \gamma)\,b.$$

2. With $h \in G$ such that $o(h) = 7$,

$$A_2 = -1 + h + h^2 + h^4.$$

$CW(v, 9)$

Proper $CW(v, 9)$ exits if and only if $v = 13$, 26 or 24.
(Ang, Arasu, Ma and Strasslerd, 2008)

Let G be a cyclic group of order v. If $A \in \mathbf{Z}[G]$ is a $CW(v, 9)$, then there exist $g \in G$ and t an integer relatively prime to v such that either $gA^{(t)}$ or $-gA^{(t)}$ is equal to the one of the A_i listed.

1. With $h \in G$ such that $o(h) = 13$,

$$A_1 = (h + h^3 + h^9) \pm [(h^2 + h^5 + h^6) - (h^4 + h^{10} + h^{12})].$$

2. With $\gamma, h \in G$ such that $o(\gamma) = 2$ and $o(h) = 13$,

$$A_2 = \gamma\,(h + h^3 + h^9) \pm [(h^2 + h^5 + h^6) - (h^4 + h^{10} + h^{12})].$$

3. With $\omega, a \in G$ such that $o(\omega) = 3$ and $o(a) = 8$,

$$A_3 = -1 + (a + a^3)(1 - a^4) + (\omega + \omega^2)(1 + a^4).$$

$CW(v, p^2)$

Let p be an odd prime. Our main aim is to determine all $CW(v, p^2)$, in particular, $p = 5$.

In the attempt to solve the problem, we find that the following two cases are very different:

I. v and p are relatively prime;

II. v is divisible by p.

We suspect that if v is divisible by p (i.e. Case II), no proper $CW(v, p^2)$ exists for $p \geq 5$.

Case II: A Known Result

Theorem (Arasu and Ma, 2001)

Let p be an odd prime and let $G = \langle \alpha \rangle \times H$ be an abelian group where $o(\alpha) = p^s$ and $\gcd(|H|, p) = 1$.

Then there is no proper $W(G, p^2)$ if $s > 1$.

Corollary No Proper $CW(p^s w, p^2)$ if $s > 1$.

Case II: Main Structural Result

The following is an improved version of a result by Arasu and Ma, 2001.

Theorem Let p be an odd prime and let $G = \langle \alpha \rangle \times H$ be an abelian group where $o(\alpha) = p$ and $\gcd(|H|, p) = 1$.

1. If $p \geq 7$, there exists a proper $W(G, p^2)$ if and only if there exist $\beta \in H$, with $o(\beta) = 2$, a subset $Z \subset H - \langle \beta \rangle$, with $Z \cap \beta Z = \emptyset$, and disjoint subsets $X, Y \subset (H/\langle \beta \rangle) - \{1\}$ such that

$$\left[1 + (1 - \beta)Z\right]\left[1 + (1 - \beta)Z\right]^{(-1)} = p - \tfrac{p-1}{2}\left\langle \beta \right\rangle$$

and

$$[1 + 2(X - Y)]\,[1 + 2(X - Y)]^{(-1)} = p^2.$$

Case II: Main Structural Result

2. If there exists a proper $W(G, 25)$, there exist $\beta \in H$, with $o(\beta) = 2$, and disjoint subsets $X, Y \subset (H/\langle\beta\rangle) - \{1\}$ such that

$$[1 + 2(X - Y)]\,[1 + 2(X - Y)]^{(-1)} = 25.$$

Case II: Questions

A. Let H be a finite cyclic group of even order with $\gcd(|H|, p) = 1$ and let $\beta \in H$ with $o(\beta) = 2$.

Does there exist $Z \subset H - \langle \beta \rangle$ such that $Z \cap \beta Z = \varnothing$ and

$$\left[1 + (1-\beta)Z\right]\left[1 + (1-\beta)Z\right]^{(-1)} = p - \tfrac{p-1}{2}\left\langle \beta \right\rangle \ ?$$

B. Let K be a finite cyclic group with $\gcd(|K|, p) = 1$.

Does there exist disjoint subsets $X, Y \subset K - \{1\}$ such that

$$[1 + 2(X - Y)]\,[1 + 2(X - Y)]^{(-1)} = p^2 \ ?$$

Case II: Question A - A Nonexistence Result

Theorem Let H be a finite group of even order and let $\beta \in H$ with $o(\beta) = 2$.

If there exist $Z \subset H - \langle\beta\rangle$ such that $Z \cap \beta Z = \emptyset$ and

$$\left[1+(1-\beta)Z\right]\left[1+(1-\beta)Z\right]^{(-1)} = m - \tfrac{m-1}{2}\left\langle\beta\right\rangle$$

for some integer m, then $m \equiv 1 \pmod 4$ and $|Z| = (m-1)/4$.

Proof Counting the coefficients of the identity element in both side of the equation, we have

$$\begin{aligned} 1 + 2|Z| &= \text{the sum of squares of the coefficients on LHS} \\ &= m - \tfrac{m-1}{2} \end{aligned}$$

which implies $|Z| = (m-1)/4$ and hence $m \equiv 1 \pmod 4$.

Case II: Question A - A Nonexistence Result

Corollary For $p \geq 7$, no proper $CW(pw, p^2)$ exists if $p \equiv 3 \pmod 4$.

Case II: Question A - Some Examples

By trial-and error, we find some solutions to Question A:

$p = 5$: $H = \langle g \rangle$, $Z = \{g\}$ and $\beta = g^2$ where $o(g) = 4$.

$p = 13$: $H = \langle g, \omega \rangle$, $Z = \{g, g^2\omega, g^2\omega^2\}$ and $\beta = g^2$ where $o(g) = 4$ and $o(\omega) = 3$.

$p = 17$: $H = \langle h, \omega \rangle$, $Z = \{h, h^3, h^4\omega, h^4\omega^2\}$ and $\beta = h^4$ where $o(h) = 8$ and $o(\omega) = 3$.

$p = 29$: $H = \langle g, \pi \rangle$, $Z = \{\pi, \pi^6, g\pi, g\pi^6, g^3, g^3\pi^3, g^3\pi^4\}$ and $\beta = g^2$ where $o(g) = 4$ and $o(\pi) = 7$.

Case II: Question B - Basic Results

Let K be a finite cyclic group with $\gcd(|K|, p) = 1$.

Suppose there exist disjoint subsets $X, Y \subset K - \{1\}$ such that $[1 + 2(X - Y)]\,[1 + 2(X - Y)]^{(-1)} = p^2$ where $p \equiv 1 \pmod 4$.

(i) $X^{(p)} = X$ and $Y^{(p)} = Y$.

(ii) $|X| = \frac{1}{8}(p^2 + 2p - 3)$ and $|Y| = \frac{1}{8}(p^2 - 2p + 1)$.

(iii) $(X + Y)^{(-1)} = X + Y$.

Without lost of generality, we assume that K is the smallest cyclic group that contains both X and Y, i.e. $K = \langle X, Y \rangle$.

Case II: Question B - A Non-Existence Result

Theorem Suppose $|K|$ divides $p^2 - 1$. Then there do not exist disjoint subsets $X, Y \subset K - \{1\}$ such that

$$[1 + 2(X - Y)]\,[1 + 2(X - Y)]^{(-1)} = p^2.$$

Corollary For $p \geq 5$, no proper $CW(pw, p^2)$ exists if w divides $p^2 - 1$.

Case II: Question B - Orbits Under the Action $g \to g^p$

Recall that $X^{(p)} = X$ and $Y^{(p)} = Y$.

In particular, if $g \in X$ (or Y), then

$$\{ g^{p^k} \in K : k \in \mathbf{Z} \} \subset X \text{ (respectively, } Y\text{).}$$

For convenience, we define

$$\theta_p(g) = \{ g^{p^k} \in K : k \in \mathbf{Z} \}.$$

We say that $\theta_p(g)$ is the orbit of g.

$|\theta_p(g)|$ is equal to the smallest positive integer r such that $o(g)$ divides $p^r - 1$.

Case II: Question B - $p = 5$

Lemma For any $g \in X \cup Y$, $\theta_p(g)$ and $\theta_p(g^{-1})$ are two disjoint orbits in $X \cup Y$.

Theorem There do not exist disjoint subsets $X, Y \subset K - \{1\}$ such that $[1 + 2(X - Y)]\,[1 + 2(X - Y)]^{(-1)} = 25$.

Proof Assume there exists such X and Y.

We know that $|X| = 4$ and $|Y| = 2$.

Take any $g \in X \cup Y$. By the lemma, $|\theta_p(g)| \le 2$ and hence $o(g)$ divides $5^2 - 1$.

But this means $|K|$ divides $5^2 - 1$. This contradicts one of our previous result.

Case II: Question B - $p = 5$

Corollary No proper $CW(5w, 25)$ exists.

Case I: A Classical Construction

Theorem Let $L = \langle \alpha \rangle \times G$ be a group of order $2mu$ such that $o(\alpha) = 2$ and G is a group of order mu.
Suppose there exists an $(m, 2u, n, \lambda)$-relative difference set $D = X \cup \alpha Y$ in L relative to $\langle \alpha \rangle \times N$ where N is a normal subgroup of G of order u and X, Y are subsets of G.
Then $A = X - Y$ is a proper $W(G, n)$.

By the classical geometric construction, for any divisor w of $p - 1$, there exists a $(p^2 + p + 1, w, p^2, (p^2 - p)/w)$-relative difference set in the cyclic group of order $(p^2 + p + 1)w$.

Thus for odd p, there exists a proper $CW((p^2 + p + 1)w/2, p^2)$ where w is a divisor of $p - 1$ such that $w \equiv 2 \pmod 4$.

In particular, there exists a proper $CW(31, 5)$.

Case I: Basic Results

Let G be a finite cyclic group of order v with $\gcd(v, p) = 1$. Suppose $A = X - Y$ is a $CW(v, p^2)$ where X and Y are disjoint subsets of K.

(i) $X^{(p)} = X$ and $Y^{(p)} = Y$.

(ii) $|X| = \frac{1}{2}(p^2 \pm p)$ and $|Y| = \frac{1}{2}(p^2 \mp p)$.

In particular, if $p = 5$, $\{|X|, |Y|\} = \{15, 10\}$.

Case I: Our Strategy

Our aim is to determine all the proper $CW(v, p^2)$, in particular, $CW(v, 25)$ (probably with the help of a computer).

To do so, we first need to limit the possible choices of v.

There is a very rough result given by Ang, Arasu, Ma and Strasslerd, 2008.

Lemma v divides the least common multiple of $p-1$, p^2-1, ..., p^u-1 where $u = (p^2+p)/2$.

The possible choices of v is too much even for $p = 5$.

Case I: Our Strategy

In order to reduce the possible choices of v, we need to work on the orbit sizes $|\theta_p(g)|$ for $g \in X \cup Y$.

For example, we can show that there are at least two "irreducible" orbits of the largest size. With this result, the statement of the previous lemma can be refined to:

Lemma v divides the least common multiple of $p-1$, p^2-1, ..., p^u-1 where $u=(p^2-p)/2$.

We have also obtained some better bounds on $|\theta_p(g)|$. But those results are too technical to be stated here.

$CW(v, 25)$

By a computer search, we have found proper $CW(v, 25)$ for $v = 31, 62, 124, 71, 142, 33$.

Let G be a cyclic group of order $v \in \{31, 62, 124, 71, 142, 33\}$. If $A \in \mathbf{Z}[G]$ is a $CW(v, 4)$, then there exist $g \in G$ and t an integer relatively prime to v such that either $gA^{(t)}$ or $-gA^{(t)}$ is equal to the one of the A_i listed.

$v = 31$: With $a \in G$ such that $o(a) = 31$,

$$A_1 = -1 + \theta_5(a) + \theta_5(a^2) + \theta_5(a^3) + \theta_5(a^6) + \theta_5(a^{11}) - \theta_5(a^4) - \theta_5(a^{16}) - \theta_5(a^{17});$$

$$A_2 = -1 + \theta_5(a) + \theta_5(a^2) + \theta_5(a^3) + \theta_5(a^8) + \theta_5(a^{17}) - \theta_5(a^{11}) - \theta_5(a^{12}) - \theta_5(a^{16}).$$

$CW(v, 25)$

$v = 62$: With $\gamma, a \in G$ such that $o(\gamma) = 2$ and $o(a) = 31$,

$$A_3 = -1 + \gamma\theta_5(a) + \theta_5(a^2) + \theta_5(a^3) + \theta_5(a^6) + \gamma\theta_5(a^{11}) - \gamma\theta_5(a^4) - \gamma\theta_5(a^{16}) - \theta_5(a^{17});$$

$$A_4 = -1 + \gamma\theta_5(a) + \theta_5(a^2) + \gamma\theta_5(a^3) + \theta_5(a^8) + \gamma\theta_5(a^{17}) - \gamma\theta_5(a^{11}) - \theta_5(a^{12}) - \theta_5(a^{16});$$

$$A_5 = -1 + (1+\gamma)\theta_5(a) + (1-\gamma)\theta_5(a^{11}) + \gamma\theta_5(a^6) + \theta_5(a^8) - \gamma\theta_5(a^3) - \theta_5(a^{12});$$

$$A_6 = -1 + (1+\gamma)\theta_5(a) - (1-\gamma)\theta_5(a^{16}) + \theta_5(a^6) + \theta_5(a^8) - \gamma\theta_5(a^3) - \gamma\theta_5(a^{12});$$

$$A_7 = -1 + (1+\gamma)\theta_5(a) + (1-\gamma)\theta_5(a^{17}) + \gamma\theta_5(a^4) + \theta_5(a^{12}) - \gamma\theta_5(a^8) - \theta_5(a^{16});$$

$$A_8 = -1 + (1+\gamma)\theta_5(a) - (1-\gamma)\theta_5(a^{11}) + \theta_5(a^4) + \theta_5(a^{12}) - \gamma\theta_5(a^8) - \gamma\theta_5(a^{16});$$

$CW(v, 25)$

$$A_9 = -1 - (1+\gamma)\theta_5(a) + (1-\gamma)\theta_5(a^2) + \gamma\theta_5(a^6) + \gamma\theta_5(a^{11}) + \theta_5(a^{12}) + \theta_5(a^{16});$$

$$A_{10} = -1 - (1+\gamma)\theta_5(a) + (1-\gamma)\theta_5(a^{17}) + \theta_5(a^6) + \gamma\theta_5(a^{11}) + \gamma\theta_5(a^{12}) + \theta_5(a^{16}).$$

$v = 124$: With $\beta, a \in G$ such that $o(\beta) = 4$ and $o(a) = 31$,

$$A_{11} = -1 + (1+\beta)\theta_5(a) + (1-\beta)\theta_5(a^{11}) + \beta^3\theta_5(a^6) + \beta^2\theta_5(a^8) - \beta^3\theta_5(a^3) - \beta^2\theta_5(a^{12});$$

$$A_{12} = -1 + (1+\beta)\theta_5(a) + (1-\beta)\theta_5(a^{17}) + \beta^3\theta_5(a^4) + \beta^2\theta_5(a^{12}) - \beta^3\theta_5(a^8) - \beta^2\theta_5(a^{16}).$$

$CW(v, 25)$

$v = 71$: With $b \in G$ such that $o(b) = 71$,

$$A_{13} = \theta_5(b) + \theta_5(b^2) + \theta_5(b^7) - \theta_5(b^{22}) - \theta_5(b^{42});$$

$$A_{14} = \theta_5(b) + \theta_5(b^3) + \theta_5(b^{18}) - \theta_5(b^2) - \theta_5(b^{21});$$

$$A_{15} = \theta_5(b) + \theta_5(b^3) + \theta_5(b^{42}) - \theta_5(b^{11}) - \theta_5(b^{18});$$

$$A_{16} = \theta_5(b) + \theta_5(b^3) + \theta_5(b^{13}) - \theta_5(b^{14}) - \theta_5(b^{22}).$$

$v = 142$: With $\gamma, b \in G$ such that $o(\gamma) = 2$ and $o(b) = 71$,

$$A_{15} = \theta_5(b) + \theta_5(b^3) + \gamma\theta_5(b^{42}) - \theta_5(b^{11}) - \theta_5(b^{18});$$

$$A_{16} = \gamma\theta_5(b) + \theta_5(b^3) + \theta_5(b^{13}) - \theta_5(b^{14}) - \theta_5(b^{22}).$$

$CW(v, 25)$

$v = 33$: With $\omega, c \in G$ such that $o(\omega) = 3$ and $o(c) = 11$,

$$A_{17} = (1 - \omega - \omega^2)\theta_5(c) + (\omega + \omega^2)\theta_5(c^2)$$
$$= \theta_5(c) - \theta_5(\omega c) + \theta_5(\omega c^2).$$

Conclusion

We are still in the process of refining some of our works on $CW(v, 25)$ with v relatively prime to 5.

However, we believe that there are no other proper $CW(v, 25)$ besides those we have listed in the previous slides.

Open Problems

1. We have solutions to the equation

$$\left[1+(1-\beta)Z\right]\left[1+(1-\beta)Z\right]^{(-1)} = p - \tfrac{p-1}{2}\langle\beta\rangle$$

   in cyclic groups with $p = 5,\ 13,\ 17$ and 29.

   Are there other solutions for large p?

   Note that solutions to the equation in cyclic groups can give us ternary "almost perfect" sequences.

2. Find solutions of the equation in other groups, say, abelian groups.

Open Problems

3. Prove or disprove that the equation

$$[1 + 2(X - Y)]\,[1 + 2(X - Y)]^{(-1)} = p^2$$

has no solution in cyclic groups.

4. Find solutions of the equation in other groups.

Note that solutions of the two equations in Questions 1 and 3 can be used to construct group weighing matrices of weight p^2.

Open Problems

5. Determine all proper $CW(v, 49)$.

6. Determine all proper $W(G, p^2)$, where G is abelian, for small values of p.

7. Apart from the classical construction of proper $CW((p^2 + p + 1)w/2, p^2)$ where w is a divisor of $p - 1$ such that $w \equiv 2 \pmod 4$. Are there other (infinite) families of proper $CW(v, p^2)$?