A reduction theorem for circulant weighing matrices

K.T. Arasu*

Department of Mathematics and Statistics
Wright State University
Dayton, OH 45435, U.S.A.

Abstract

Circulant weighing matrices of order n with weight k, denoted by $WC(n,k)$, are investigated. Under some conditions, we show that the existence of $WC(n,k)$ implies that of $WC(\frac{n}{2},\frac{k}{4})$. Our results establish the nonexistence of $WC(n,k)$ for the pairs (n,k) = (125,25), (44,36), (64,36), (66,36), (80,36), (72,36), (118,36), (128,36), (136,36), (128,100), (144,100), (152,100), (88,36), (132,36), (160,36), (166,36), (176,36), (198, 36), (200, 36), (200,100). All these cases were previously open.

1 Introduction

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

$$WW^t = kI_n,$$

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

A circulant weighing matrix of order n with weight k, denoted by $W = WC(n,k)$ is a weighing matrix in which each row (except the first) is obtained from its preceding row by a right cyclic shift. We label the columns of W by a cyclic group G of order n, say generated by g.

Define

$$P = \{g^i \mid W(1,i) = 1, i = 0,1,\dots,(n-1)\}$$

and

$$N = \{g^i \mid W(1,i) = -1, i = 0,1,\dots,(n-1)\}.$$

Obviously, $|P| + |N| = k$. It is well known that k is a perfect square, say $k = s^2$. It can be shown that $\{|P|,|N|\} = \left\{\frac{s^2 \pm s}{2}\right\}$ (see [7], for instance).

For recent constructions and nonexistence results, refer to [1, 2, 3, 4, 5, and 8]. In this paper, we state and prove a reduction theorem for $WC(n,k)$ using which nonexistence of several previously open $WC(n,k)$ is established.

*Research partially supported by AFOSR grant F49620-96-1-0328 and NSA grant MDA 904-97-1-0012.

2 Preliminaries

Let G be a multiplicatively written group and $\mathbb{Z}G$ be the group ring of G over $\mathbb{Z}$. We will only consider cyclic groups G here. A character χ of G is a homomorphism from G to the multiplicative group of nonzero complex numbers. We can extend χ linearly to $\mathbb{Z}G$, obtaining a homomorphism χ from $\mathbb{Z}G$ to the field C of complex numbers. For each subset S of G we let S denote the element $S = \sum_{x \in S} x$ of $\mathbb{Z}G$. For $A = \sum_{g} a_g g \in \mathbb{Z}G$ and $t \in \mathbb{Z}$, we define $A^{(t)} = \sum_{g} a_g g^t$.

The following theorem is well known (see [1] or [8], for instance).

Theorem 1. *A $WC(n, s^2)$ exists if and only if there exist disjoint subsets P and N of $\mathbb{Z}_n$ ($\mathbb{Z}_n$ written multiplicatively) such that*

$$(P - N)(P - N)^{(-1)} = s^2. \tag{1}$$

We also require two further results.

Theorem 2. *(Turyn [9]). Let p be a prime and $G = H \times P$, an abelian group, where P is the Sylow p-subgroup of G. Assume that there exists an integer f such that $p^f \equiv -1 (\operatorname{mod} \exp H)$. Let χ be a nonprincipal character of G and let α be a positive integer. Suppose $A \in \mathbb{Z}G$ satisfies $\chi(A)\overline{\chi(A)} \equiv 0 (\operatorname{mod} p^{2\alpha})$. Then $\chi(A) \equiv 0 (\operatorname{mod} p^{\alpha})$.*

Theorem 3. *(Ma[6]) Let p be a prime and G an Abelian group with a cyclic Sylow p-subgroup. If $A \in \mathbb{Z}G$ satisfies $\chi(A) \equiv 0 (\operatorname{mod} p^{\alpha})$ for all nonprincipal characters χ of G, then there exist $x_1, x_2 \in \mathbb{Z}G$ such that*

$$A = p^{\alpha} x_1 + Q x_2$$

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

3 Main result

We now state and prove our reduction theorem for $WC(n, k)$

Theorem 4. *Suppose that a $WC(p^a.m, p^{2b}.u^2)$ exists where p is a prime, a, b, m, u are positive integers satisfying $(p, m) = (p, u) = 1$. Assume that there exists an integer f such that $p^f \equiv -1 (\operatorname{mod} m)$.*

Then

(i) $p = 2$ and $b = 1$

and

(ii) there exists a $WC(p^{a-1}.m = 2^{a-1}.m; p^{2b-2}u^2 = u^2)$.

Proof: By (1), there exist disjoint subsets P and N of $G = \langle g \rangle, o(g) = p^a.m$, such that

$$(P-N)(P-N)^{(-1)} = p^{2b}.u^2. \tag{2}$$

For each nonprincipal character χ of G, from (2), we have

$$\chi(P-N)\,\overline{\chi(P-N)} \equiv 0 \pmod{p^{2b}}. \tag{3}$$

Applying Theorem 2, we get

$$\chi(P-N) \equiv 0 \pmod{p^b}. \tag{4}$$

Theorem (3) now yields:

$$P - N = p^b x_1 + Q x_2 \tag{5}$$

where $Q = \langle h \rangle$ is the unique subgroup of G of order p.

From (5), we obtain

$$(P-N)(1-h) \equiv 0 \pmod{p^b} \tag{6}$$

Since the coefficients of $P-N$ lie in $[-1,1]$ it follows that the coefficients of $(P-N)(1-h)$ lie in $[-2,2]$. Then (6) implies that $p^b \leq 2$. (Note that $(P-N)(1-h)$ is nonzero, because there exists some character χ of G such that $\chi(h) \neq 1$). We can now conclude that $p=2$ and $b=1$, proving (i).

Hence (6) becomes:

$$(P-N)(1-h) \equiv 0 \pmod 2 \tag{7}$$

where $o(h) = 2$.

Let σ denote the canonical homomorphism from G to $G/_{\langle h \rangle}$. Then σ extends linearly to a ring homomorphism from $\mathbb{Z}G$ to $\mathbb{Z}\left[G/_{\langle h \rangle}\right]$. From (7) we see that $(P-N)^\sigma$ has coefficients $0, 2$, or -2. Hence $\frac{1}{2}(P-N)^\sigma$ has coefficients $0, 1$ or -1.

We now use (2) and obtain

$$\frac{1}{2}(P-N)^\sigma \frac{1}{2}\left((P-N)^\sigma\right)^{(-1)} = 2^{2b-2} \cdot u^2 = u^2. \tag{8}$$

shows that $\frac{1}{2}(P-N)^\sigma$ defines a $WC(2^{a-1}m, u^2)$, completing the proof of Theorem 4.

4 Applications

Proposition 1: $WC(n,k)$ does not exist for the following pairs (n,k) : (i) (125, 25), (ii) (44, 36), (iii) (64, 36), (iv) (66, 36), (v) (80,36), (vi) (72,36), (vii) (118, 36), (viii) (128, 36), (ix) (136, 36), (x) (128, 100), (xi) (144, 100), (xii) (152, 100), (xiii) (88,36), (xiv) (132,36), (xv) (160,36), (xvi) (166,36), (xvii) (176,36), (xviii) (198, 36), (xix) (200, 36), (xx) (200,100).

Proof: The case (125, 25) follows from (i) of Theorem 4. For the remaining pairs, we apply Theorem 4, Part (ii), noting that $WC(\frac{n}{2}, \frac{k}{4})$ does not exist in each of the remaining 19 cases. The nonexistence of these smaller order (and smaller weight) circulant weighing matrices follows from methods of [2].

References

[1] K.T. Arasu, J.F. Dillon, D. Jungnickel and A. Pott, The Solution of the Waterloo Problem, J. Comb. Th. (A) 17 (1995), 316-331.

[2] K.T. Arasu and J. Seberry, Circulant Weighing Designs, J. Comb. Designs, 4 (1996), 439-447.

[3] K.T. Arasu and J. Seberry, On Circulant Weighing Matrices, submitted.

[4] K.T. Arasu and D. Torban, New Weighing Matrices of Weight 25, to appear in J. Comb. Designs.

[5] K.T. Arasu and Y. Strassler, A New Class of Circulant Weighing Matrices of Order 24t with Weight 9, submitted.

[6] S.L. Ma, Polynomial Addition Sets, Ph.D. thesis, University of Hong Kong, 1985.

[7] R.C. Mullin, A Note on Balanced Weighing Matrices, Lecture Notes in Mathematics, Vol. 452, Springer, New York, (1975), 28-41.

[8] Y. Strassler, New Circulant Weighing Matrices of Prime Order in $CW(31,16), CW(71,25), CW(127,64)$ to appear in Bose Conference issue of JSPI.

[9] R.J. Turyn, Character Sums and Difference Sets, Pacific J. Math, 15 (1965), 319-346.

(Received 11/8/97)