Finiteness of Circulant Weighing Matrices of Fixed Weight

Ka Hin Leung
Department of Mathematics
National University of Singapore
Kent Ridge, Singapore 119260
Republic of Singapore

Bernhard Schmidt
Division of Mathematical Sciences
School of Physical & Mathematical Sciences
Nanyang Technological University
Singapore 637371
Republic of Singapore

Abstract

Let n be any fixed positive integer. Every circulant weighing matrix of weight n arises from what we call an irreducible orthogonal family of weight n. We show that the number of irreducible orthogonal families of weight n is finite and thus obtain a finite algorithm for classifying all circulant weighing matrices of weight n. We also show that, for every odd prime power q, there are at most finitely many proper circulant weighing matrices of weight q.

1 Introduction

A **circulant weighing matrix of order v** is a square matrix of the form

$$M = \begin{pmatrix} a_1 & a_2 & \cdots & a_v \\ a_v & a_1 & \cdots & a_{v-1} \\ \cdots & \cdots & \cdots & \cdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix}$$

with $a_i \in \{-1, 0, 1\}$ for all i and $MM^T = nI$ where n is a positive integer and I is the identity matrix. The integer n is called the *weight* of the matrix.

To study of circulant weighing matrices it is very convenient to use the group ring language. Let C_v denote the cyclic group of order v, and let g be a generator of C_v. A circulant matrix M as above satisfies $MM^T = nI$ if and only if $XX^{(-1)} = n$ where X is the element of the group ring $\mathbb{Z}[C_v]$ defined by $X = \sum_{i=1}^{v} a_i g^i$ and $X^{(-1)} = \sum_{i=1}^{v} a_i g^{-i}$. Thus a circulant weighing matrix of order v and weight n is equivalent to an element X of $\mathbb{Z}[C_v]$ with coefficients $-1, 0, 1$ only and $XX^{(-1)} = n$. This is the formulation we will use in the rest of our paper. Note that the weight of a circulant weighing matrix must be a square as $|\sum a_i|^2 = n$.

The existence and structure of circulant weighing matrices has been studied intensively, see [3] for a survey, [18] for many related results, and [14] for more background on weighing matrices in general. There are only a few infinite families [4, 11, 17] and sporadic examples [3, 5] of circulant weighing matrices known. The *spectrum* of circulant weighing matrices of fixed weight n, i.e. the set of positive integers v such that a circulant weighing matrix of weight n exists, has been determined for $n = 4$ [12], $n = 9$ [1, 21], and $n = 16$ [5, 6, 13].

In the present paper, we study the problem of classifying all circulant weighing matrices of fixed weight. A substantial difficulty that arises in this context is that there is no obvious way to decide when two such matrices should be viewed as "equivalent". A usual, but only partially satisfactory, approach is to restrict the attention to "proper" circulant weighing matrices. A circulant weighing matrix $X \in \mathbb{Z}[C_v]$ is called *proper* if there is no $g \in C_v$ and no proper divisor w of v such that $Xg \in \mathbb{Z}[C_w]$.

For some cases this is enough to get nice results: We will show that for every fixed odd prime power n, there are only finitely many proper circulant weighing matrices of weight n. However, such a result cannot be true in general. For instance, let $v = 2p$ where p is an odd prime. Let g respectively h be elements of C_v of order 2 respectively p. Then $X = 1 + g + h - gh$ is a proper circulant weighing matrix of weight 4. Thus there are infinitely many distinct proper circulant weighing matrices of weight 4. But of course these weighing matrices are "equivalent" in some sense and an attempted classification of circulant weighing matrices of fixed weight should reflect this. In fact, all these weighing matrices arise from the same "irreducible orthogonal family" ($\{1 + g, 1 - g\}$), a notion we introduce in this paper.

We will show that for every fixed weight n there are only finitely many irreducible orthogonal families and that can give rise to circulant weighing matrices of weight n and that every circulant weighing matrix of weight n can be constructed in this way. This shows that, for any fixed n, there is a finite algorithm for finding all circulant weighing matrices of weight n. Hence we provide satisfactory framework for the classification of these matrices.

It should be mentioned that there is a close connection between the "orthogonal families" used in the present paper and the notion of "building sets" introduced in the groundbraking paper of Davis and Jedwab [10]. In fact, if we extend the notion of orthogonal families used in the present paper from cyclic to abelian groups, a major result of Davis and Jedwab can be phrased as an recursive construction of orthogonal families over abelian groups G whose weight is equal to $|G|$. Though the result of Davis and Jedwab only concerns abelian groups of relatively low exponent, the appearance of orthogonal families in the classification of circulant weighing matrices shows that their main idea is relevant even for cyclic groups!

2 Main results

By C_v we denote the cyclic group of order v. For a divisor w of v, we identify the subgroup of order w of C_v with C_w.

Definition 2.1 Let v be a positive integer, let w be a divisor of v, and let g be a generator of C_v. Every $X \in \mathbb{Z}[C_v]$ can be uniquely written in the form

$$X = \sum_{i=0}^{v/w-1} X_i g^i \text{ with } X_i \in \mathbb{Z}[C_w].$$

If $X_i X_j = 0$ for all $i \neq j$, then we say that X is *orthogonal over* C_w. We say that a subset S of $\mathbb{Z}[C_v]$ is *orthogonal over* C_w if every element of S is orthogonal over C_w.

Definition 2.2 Let v be a positive integer, and let $B = \{A_1, ..., A_k\}$ be a finite set of elements of $\mathbb{Z}[C_v]$ with $A_i \neq 0$ for all i. We call B an *orthogonal family over* C_v if $A_i A_j = 0$ for all $i \neq j$. We call B *reducible* if there is a proper divisor w of v such that B is orthogonal over C_w and *irreducible* otherwise. If $\sum_{i=1}^{k} A_i A_i^{(-1)} = n$ where n is an integer, we say that B has *weight* n.

Definition 2.3 Let v be a positive integer, let w be divisor of v, and let $B = \{A_1, ..., A_k\}$ be an orthogonal family over C_w. We say that $X \in \mathbb{Z}[C_v]$ *is a coset combination of* B if X has the form

$$X = \sum_{i=1}^{k} A_i g_i$$

where $g_1, ..., g_k$ are representatives of distinct cosets of C_w in C_v.

The following is the main result of this paper. It shows that, for fixed n, all circulant weighing matrices of weight n can be determined by a finite algorithm.

Theorem 2.4 *Let n be a positive integer.*

(a) Every circulant weighing matrix of weight n is a coset combination of an irreducible orthogonal family of weight n.

(b) The number of irreducible orthogonal families of weight n is finite, and they can be enumerated by a finite algorithm.

In the case where the weight is an odd prime power, we can go much further. To formulate our result in this case we need some more terminology.

Definition 2.5 Let $B = \{A_1, ..., A_k\}$ be an orthogonal family over C_v (recall that this requires $A_i \neq 0$ for all i). We call B *nontrivial* if $k \geq 2$. We say that B *has coefficients* $-1, 0, 1$ if all A_i have coefficients $-1, 0, 1$ only.

Theorem 2.6 *There is no nontrivial orthogonal family with coefficients* $-1, 0, 1$ *of odd prime power weight.*

Corollary 2.7 *Let* n *be an odd prime power. Then there are at most finitely many proper circulant weighing matrices of* n*.*

3 Preliminaries

In this section, we introduce some notation and basic facts we need in the rest of paper. Let G be a finite abelian group. We write $o(g)$ for the order of an element g of G. Let R be a ring. We will always identify a subset A of G with the element $\sum_{g\in A} g$ of the group ring $R[G]$. For $B = \sum_{g\in G} b_g g \in R[G]$ and an integer t we write $B^{(t)} := \sum_{g\in G} b_g g^t$ and $|B| := \sum_{g\in G} b_g$. The elements b_g are called the *coefficients* of B. We call $\{g \in G : b_g \neq 0\}$ the *support* of B. A group homomorphism $G \to H$ is always assumed to be extended to a homomorphism $R[G] \to R[H]$ by linearity.

We denote the group of complex characters of G by G^*. The character sending all elements of G to 1 is called *trivial*. For a subgroup W of G, we write $W^\perp$ for the subgroup of G^* consisting of all characters which are trivial on W.

For a positive integer t, we write $\zeta_t = \exp(2\pi i/t)$.

We repeatedly will make use of the following elementary properties of characters of finite abelian groups. For a proof, see [8, Section VI.3].

Result 3.1 *Let* G *be a finite abelian group.*

a) Let $D = \sum_{g\in G} d_g g \in \mathbb{C}[G]$*. Then*

$$d_g = \frac{1}{|G|} \sum_{\chi\in G^*} \chi(Dg^{-1})$$

for all $g \in G$ (Fourier Inversion Formula). In particular, two elements of $\mathbb{C}[G]$ are equal if and only if all their character values are equal.

b) (Orthogonality relations) Let U be a subgroup of G. If $\chi \in G^*$ is nontrivial on U, then $\chi(U) = 0$. If $g \in G \setminus U$, then $\sum_{\chi \in U^\perp} \chi(g) = 0$.

c) If H is a subgroup of G and $A, B \in \mathbb{Z}[G]$ with $\chi(A) = \chi(B)$ for all $\chi \in G^* \setminus H^\perp$, then $A = B + XH$ for some $X \in \mathbb{Z}[G]$.

Lemma 3.2 *Let G be a finite abelian group and $D = \sum a_g g \in \mathbb{Z}[G]$. For a subset S of G write $D \cap S := \sum_{g \in S} a_g g$. Let U be a subgroup of G and $h \in G$. Let χ be any character of G. Then*

$$\chi(D \cap Uh) = \frac{\chi(h)}{|U^\perp|} \sum_{\tau \in U^\perp} \chi\tau(Dh^{-1})$$

(here $\chi\tau$ is the character which sends $g \in G$ to $\chi(g)\tau(g)$).

Proof Using the orthogonality relations, we compute

$$\begin{aligned}
\sum_{\tau \in U^\perp} \chi\tau(Dh^{-1}) &= \sum_{\tau \in U^\perp} \sum_{g \in G} a_g \chi\tau(gh^{-1}) \\
&= \sum_{g \in G} a_g \chi(gh^{-1}) \sum_{\tau \in U^\perp} \tau(gh^{-1}) \\
&= |U^\perp| \sum_{gh^{-1} \in U} a_g \chi(gh^{-1}) \\
&= \chi(h)^{-1} |U^\perp| \sum_{k \in Uh} a_k \chi(k) \\
&= \chi(h)^{-1} |U^\perp| \chi(D \cap Uh).
\end{aligned}$$

This proves the lemma. □

This follows from part b of Result 3.1. □

For a prime p and a positive integer t let $\nu_p(t)$ be defined by $p^{\nu_p(t)} || \ t$, i.e. $p^{\nu_p(t)}$ is the highest power of p dividing t. By $\mathcal{D}(t)$ we denote the set of prime divisors of t. The following definition is the basis for the field descent method [19] which we will use in the next section.

Definition 3.3 *Let m, n be integers greater than 1. For $q \in \mathcal{D}(n)$ let*

$$m_q := \begin{cases} \prod_{p \in \mathcal{D}(m) \setminus \{q\}} p & \text{if } m \text{ is odd or } q = 2, \\ 4 \prod_{p \in \mathcal{D}(m) \setminus \{2,q\}} p & \text{otherwise.} \end{cases}$$

Set

$$\begin{aligned} b(2,m,n) &= \max_{q \in \mathcal{D}(n) \setminus \{2\}} \left\{ \nu_2(q^2-1) + \nu_2(\mathrm{ord}_{m_q}(q)) - 1 \right\} \text{ and} \\ b(r,m,n) &= \max_{q \in \mathcal{D}(n) \setminus \{r\}} \left\{ \nu_r(q^{r-1}-1) + \nu_r(\mathrm{ord}_{m_q}(q)) \right\} \end{aligned}$$

for primes $r > 2$ with the convention that $b(2,m,n) = 2$ if $\mathcal{D}(n) = \{2\}$ and $b(r,m,n) = 1$ if $\mathcal{D}(n) = \{r\}$. We define

$$F(m,n) := \gcd(m, \prod_{p \in \mathcal{D}(m)} p^{b(p,m,n)}).$$

Note that $F(m,n)$ and m have the same prime divisors since b_i is positive for all i. We note the following important property of $F(m,n)$ which follows directly from the definition.

Result 3.4 *Let n be a positive integer, let P be a finite set of primes, and let Q be the set of all positive integers which are products of powers of primes in P. Then there is a efficiently computable constant positive integer $C(P,n)$, only depending on P and n, such that $F(m,n)$ divides $C(P,n)$ for all $m \in Q$.*

The following result was proved in [19].

Result 3.5 *Assume $X\overline{X} = n$ for $X \in \mathbb{Z}[\zeta_m]$ where n and m are positive integers. Then*

$$X\xi_m^j \in \mathbb{Z}[\xi_{F(m,n)}]$$

for some j.

The following is a special case of [16, Thm. B] (take $n = p^b$).

Result 3.6 *Let p be an odd prime, and let r and w be positive integers with $(p,w) = 1$. Let $G = \langle \alpha \rangle \times H$ where $o(\alpha) = p^r$ and H is an abelian group of order w. Write $\beta = \alpha^{p^{r-1}}$. Let $P = \langle \beta \rangle$ be the subgroup of G of order p. Let*

t be a primitive root modulo p. Suppose D is an element of $\mathbb{Z}[G]$ such that $|\chi(D)|^2 = p^b$ for all $\chi \in G^* \setminus P^\perp$ where b is a positive integer.

Then there are $g \in H$ with $o(g)|(p-1)$, $h \in G$, $\epsilon \in \{0,1\}$, $X \in \mathbb{Z}[G]$, and $E \in \mathbb{Z}[H]$ such that

$$Dh = E\sum_{i=1}^{p-1}(\epsilon g)^i \beta^{t^i} + PX.$$

4 Proof of Theorem 2.4

The following is a slight modification of a special case of [15, Thm. 1]. Since it can be proved in the same way as [15, Thm. 1] with minimal changes, we skip the proof.

Result 4.1 *Let v and n be coprime positive integers. Let $A \in \mathbb{Z}[C_v]$ with $AA^{(-1)} = n$ and let t be a positive integer coprime to v. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_v)/\mathbb{Q})$ be defined by $\zeta_v^\sigma = \zeta_v^t$. If σ fixes all prime ideals above $\chi(A)\mathbb{Z}[\zeta_v]$ for all characters χ of C_v, then there is $g \in C_v$ with*

$$(Ag)^{(t)} = Ag.$$

Theorem 4.2 *Let p be a prime, and Let $v = p^a w$ where a and w are positive integers with $(p,w) = 1$. Let $A \in \mathbb{Z}[C_v]$ with $AA^{(-1)} = n$ where n is a positive integer. If $p > 4^n + 1$, then there is $g \in C_v$ with $Ag \in \mathbb{Z}[C_w]$.*

Proof Let g be an element of C_v of order p^a. Write

$$A = \sum_{i=1}^{s} A_i g^{a_i} \tag{1}$$

with $A_i \in \mathbb{Z}[C_w]$ and the a_i are distinct elements of $\{a_1, ..., a_n\}$. Since the sum of the squares of the coefficients of A is n, we can assume $s \leq n$.

Claim Let χ be any complex character of C_v. Then there is a root of unity η such that $\eta\chi(A) \in \mathbb{Z}[\zeta_w]$.

Write $\beta = \chi(g)$. Note that β is a primitive p^bth root of unity for some nonnegative integer b. If $b = 0$, then there is nothing to show, so we assume

$b \geq 1$. By (1), we have

$$\chi(A) = \sum_{i=1}^{s} \chi(A_i)\beta^{a_i}. \tag{2}$$

By removing all terms with $\chi(A_i) = 0$, if necessary, we can assume $\chi(A_i) \neq 0$ for all i. From (2), we get

$$n = |\chi(A)|^2 = \sum_{i,j=1}^{s} \chi(A_i)\overline{\chi(A_j)}\beta^{a_i - a_j}. \tag{3}$$

Let $\rho : \mathbb{Z}[\zeta_w][C_{p^b}] \to \mathbb{Z}[\zeta_{wp^b}]$ be an epimorphism that sends a generator of C_{p^b} to ζ_{p^b}. Note that the kernel of ρ is

$$\{XP : X \in \mathbb{Z}[\zeta_w][C_{p^b}]\}$$

where P is the subgroup of C_{p^b} of order p. Taking preimages under ρ in (3), we get

$$n + XP = \sum_{i,j=1}^{s} \chi(A_i)\overline{\chi(A_j)}h^{a_i - a_j} \tag{4}$$

where $X \in \mathbb{Z}[\zeta_w][C_{p^b}]$ and h is a generator of C_{p^b}. Note that the right hand side of (4) has at most $n^2 - n + 1$ nonzero coefficients since $s \leq n$. However, if $XP \neq 0$, then the left hand side of (4) has at least $p - 1$ nonzero coefficients. This is a contradiction, since, by assumption, $p - 1 > 4^n > n^2 - n + 1$. Hence $XP = 0$ and thus

$$n = \sum_{i,j=1}^{s} \chi(A_i)\overline{\chi(A_j)}h^{a_i - a_j}. \tag{5}$$

Now assume $s \geq 2$. By [9, Thm. 1, p. 13] there is a positive integer $t < p$ and integers b_i with

$$\frac{ta_i}{p} = b_i + \epsilon_i \tag{6}$$

with $|\epsilon_i| \leq (p-1)^{-1/s}$. Since $s \leq n$ and $p > 4^n + 1$, we conclude $|\epsilon_i| < 1/4$ for all i. Write $c_i = ta_i$ and $e_i = \epsilon_i p$ Note $|e_i| < p/4$ and that (6) implies that e_i is an integer for all i. From (6) we obtain

$$c_i \equiv e_i \bmod p. \tag{7}$$

Let e_x the largest and e_y the smallest e_i. Since $|e_i| < p/4$ for all i, we conclude

$$c_x - c_y \not\equiv c_i - c_j \mod p \tag{8}$$

for all pairs $(i,j) \neq (x,y)$. Applying the isomorphism of $\mathbb{Z}[\zeta_w][C_{p^b}]$ defined by $h \mapsto h^t$ and $\zeta_w \mapsto \zeta_w$ to (5) we get

$$n = \sum_{i,j=1}^{s} \chi(A_i)\overline{\chi(A_j)}h^{c_i - c_j}. \tag{9}$$

Since $\chi(A_i) \neq 0$ for all i, and the difference $c_x - c_y$ occurs only once mod p, the coefficient of $h^{c_x - c_y}$ on the right hand side of (9) is nonzero. But this contradicts (9). Hence $s = 1$, and this proves the Claim in view of (2).

Now let t be an integer such that $t \equiv 1 \mod w$ and the order of t mod p^b is $(p-1)p^{b-1}$. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{wp^b})/\mathbb{Q})$ be defined by $\zeta_{wp^b}^{\sigma} = \zeta_{wp^b}^{t}$. Note that σ fixed $\mathbb{Q}(\zeta_w)$. Hence Claim 1 implies that σ fixes the ideal $\chi(A)\mathbb{Z}[\zeta_v]$ for every character χ of C_v. Thus Result 4.1 shows that, replacing A by Ag for some $g \in C_v$, if necessary, we have

$$A^{(t)} = A. \tag{10}$$

Now write $A = \sum_{i=0}^{p^a-1} X_i g^i$ with $X_i \in \mathbb{Z}[C_w]$ where at most n of the X_i a nonzero. Note that $X_i^{(t)} = X_i$ for all i and thus

$$\sum_{i=0}^{p^a-1} X_i g^{it} = \sum_{i=0}^{p^a-1} X_i g^i. \tag{11}$$

This implies that $X_i = X_j$ if i and j are in the same orbit of $x \mapsto tx \mod p^a$. Note that all such orbits different from $\{0\}$ have size at least $p-1$. Hence, if $X_i \neq 0$ for some $i > 0$, then at least $p-1$ of the X_i are nonzero. Hence $p - 1 < n$, a contradiction. Thus $A = X_0 \in \mathbb{Z}[C_w]$. $\square$

Lemma 4.3 *Let $v = wp^a$ where p is a prime and $a \geq 2$, $w \geq 1$ are integers. Let b be an integer with $1 \leq b < a$, and let $X = \sum_{i=0}^{p^{a-b}-1} X_i \zeta_{p^a}^i$ where $X_i \in \mathbb{Z}[\zeta_{wp^b}]$. If more than one X_i is nonzero, then there is no root of unity η such that $X\eta \in \mathbb{Z}[\zeta_{wp^b}]$.*

Proof This follows from the well known fact that $\{1, \zeta_{p^a}, ..., \zeta_{p^a}^{p^{a-b}-1}\}$ is independent over $\mathbb{Q}(\zeta_{wp^b})$. $\square$

Lemma 4.4 *Let $v = wp^a$ where p is a prime and a, w are positive integers. Let $X \in \mathbb{Z}[C_v]$ with*

$$|\chi(X)|^2 \leq n$$

for all characters χ of C_v for some constant n. Assume that for all characters τ of C_v there is a root of unity $\eta(\tau)$ such that $\eta(\tau)\tau(X) \in \mathbb{Z}[\zeta_{wp^b}]$ where b is an integer with $1 \leq b < a$. Furthermore, assume $p^{a-b} > n$.

Let $c < a$ be any positive integer with $p^{c-b+1} > n$. Then X is orthogonal over $C_{p^c w}$.

Proof Write

$$X = \sum_{i=0}^{p^{a-c}-1} X_i h^i \tag{12}$$

where $X_i \in \mathbb{Z}[C_{p^c w}]$ and h is an element of C_v of order p^a. We have to show $X_i X_j = 0$ for all $i \neq j$. Let χ be a character of C_v with $\chi(h) = \xi$ where ξ is a primitive p^{a-c+f}th root of unity for some f with $b \leq f \leq c$. Then

$$\chi(X) = \sum_{i=0}^{p^{a-c}-1} \chi(X_i)\xi^i \tag{13}$$

with $\chi(X_i) \in \mathbb{Z}[\zeta_{wp^f}]$. Recall that $a - c \geq 1$ by assumption. Now assume that $\chi(X_i) \neq 0$ for at least two values of i. Then, by (13) and Lemma 4.3, we conclude that there is no root of unity η with $\eta\chi(X) \in \mathbb{Z}[\zeta_{wp^f}]$. But since $f \geq b$, this contradicts the assumptions.

Let τ be any character of C_v. Note that $\tau(h)$ is a primitive p^{a-c+f}th root of unity for some f with $b \leq f \leq c$ if and only if the restriction of τ to $\mathbb{Z}[C_{p^c w}]$ has order divisible by p^b. Hence, in summary, we have shown that for every character ψ of $C_{p^c w}$ whose order is divisible by p^b, we have $\psi(X_i) \neq 0$ for at most one i.

Note that the number of characters ψ of $C_{p^c w}$ of order divisible by p^b is $w(p^c - p^{b-1})$. By what we have shown, we have

$$\psi(X_i X_j) = 0 \text{ for all } \ i \neq j \tag{14}$$

for all these characters ψ. Since $|\chi(X)| = \sqrt{n}$ for all characters χ of C_v, we have

$$|\psi(X_i)| \leq \sqrt{n} \tag{15}$$

for all i by Lemma 3.2. Now assume that $X_iX_j \neq 0$ for some $i \neq j$. Let $k \in C_{p^c w}$ have coefficient $x \neq 0$ in X_iX_j. Then by (14), (15) and the inversion formula,

$$1 \leq |x| \leq \frac{1}{wp^c}\left((wp^c - w(p^c - p^{b-1}))n\right) = np^{b-c-1}.$$

But this contradicts the assumption $p^{c-b+1} > n$. Hence $X_iX_j = 0$ for all $i \neq j$. $\square$

Definition 4.5 Let n be a positive integer, let $\{p_1, ..., p_r\}$ be the set of all primes $\leq 4^n + 1$, and let $P = \prod_{i=1}^{r} p_i$. Let the constant $C(P, n)$ as defined in Result 3.4 and write $C(P, n) = \prod_{i=1}^{r} p_i^{b_i}$. For each i, let c_i be smallest positive integer with $p^{c_i - b_i + 1} > n$. We define

$$T(n) = \prod_{i=1}^{r} p_i^{c_i}.$$

Theorem 4.6 *Let n and v be a positive integers, and let $X \in \mathbb{Z}[C_v]$ such that $|\chi(X)|^2 \in \{0, n\}$ for all characters χ of G. Then X is orthogonal over C_d where $d = \gcd(T(n), v)$.*

Proof Let $\{p_1, ..., p_r\}$ be the set of all primes $\leq 4^n + 1$. By Theorem 4.2 there is a divisor w of v of the form

$$w = \prod_{i=1}^{r} p_i^{a_i},\ a_i \geq 0,$$

such that $Xg \in \mathbb{Z}[C_w]$ for some $g \in C_v$. Hence we can assume $X \in \mathbb{Z}[C_w]$.

Write $T(n) = \prod_{i=1}^{r} p_i^{c_i}$. Let k be an integer with $1 \leq k \leq r$ and let

$$w_k = \left(\prod_{i=1}^{k-1} p_i^{\min(a_i, c_i)}\right)\left(\prod_{i=k}^{r} p_i^{a_i}\right).$$

Note that $w_{r+1} = \gcd(T(n), w)$ is a divisor of $\gcd(T(n), v) = d$. Hence it suffices to show that X is orthogonal over $C_{w_{r+1}}$.

Claim X is orthogonal over C_{w_k} for $k = 1, ..., r + 1$.

We proof the Claim by induction on k. Since $w_1 = w$ and $X \in \mathbb{Z}[C_w]$ it trivially holds for $k = 1$. Let g be a generator of C_w. Assume that the Claim is true for some value of k. Thus

$$X = \sum_{i=0}^{w/w_k - 1} X_i g^i \tag{16}$$

with $X_i \in \mathbb{Z}[C_{w_k}]$ and $X_i X_j = 0$ for all $i \neq j$. Write

$$X_i = \sum_{j=0}^{w_k/w_{k+1} - 1} Y_{ij} h^j \tag{17}$$

for $i = 0, ..., w/w_k - 1$ with $Y_{ij} \in \mathbb{Z}[C_{w_{k+1}}]$ where h is a generator of C_{w_k}. To verify the Claim for $k + 1$, we need to show

$$Y_{ij} Y_{st} = 0 \text{ whenever } (i, j) \neq (s, t). \tag{18}$$

If $c_k \geq a_k$, then $w_{k+1} = w_k$ and there is nothing to show. Hence we can assume $c_k < a_k$.

Now fix any $i \in \{0, ..., w/w_k - 1\}$. Since $|\chi(X)|^2 \in \{0, n\}$ for all characters χ of C_w, we have $|\tau(X_i)|^2 \in \{0, n\}$ for all i and all characters τ of C_w. Let $C(P, n) = \prod_{i=1}^{r} p_i^{b_i}$ as in Definition 4.5. Let τ be any character of C_{w_k}. Note that $p_k^{c_k}$ is the highest power of p_k dividing w_{k+1} since we assume $c_k < a_k$. Since $|\tau(X_i)|^2 \in \{0, n\}$, by Result 3.5, there is a root of unity $\eta(\tau)$ such that $\tau(X_i)\eta(\tau) \in \mathbb{Z}[\zeta_{p_k^{b_k - c_k} w_{k+1}}]$. Note that $p_k^{b_k}$ is the highest power of p_k dividing $p_k^{b_k - c_k} w_{k+1}$ and that $p_k^{c_k - b_k + 1} > n$ by the definition of $T(n)$. Hence, using Lemma 4.4, we conclude that X_i is orthogonal over $C_{w_{k+1}}$. This implies

$$Y_{ij} Y_{it} = 0 \text{ for all } j \neq t \text{ and all } i. \tag{19}$$

Let ψ be any character of C_{w_k} and $i \in \{0, ..., w/w_k - 1\}$. From (19) we conclude that $\psi(Y_{ij}) \neq 0$ for at most one j. Now let $i' \in \{0, ..., w/w_k - 1\}$, $i' \neq i$. Then, by the same argument, $\psi(Y_{i'j}) \neq 0$ for at most one j. Assume that there are j, j' such that $\psi(Y_{ij}) \neq 0$ and $\psi(Y_{i'j'}) \neq 0$. Then $\psi(X_i) \neq 0$ and $\psi(X_{i'}) \neq 0$ by (17). But this contradicts the orthogonality of X over C_{w_k}.

In summary, we have shown that $\psi(Y_{ij}Y_{st}) = 0$ for every character ψ of C_{w_k} whenever $(i,j) \neq (s,t)$. This implies (18) and concludes the proof of the Claim. Taking $k = r+1$ in the Claim, we infer that X is orthogonal over $C_{w_{r+1}}$ and this proves the theorem. $\square$

Proof of Theorem 2.4 Let v and n be positive integers and let $X \in \mathbb{Z}[C_v]$ be a circulant weighing matrix of weight n. Let d be the smallest divisor of v such that X is orthogonal over C_d. Then $X = \sum_{i=0}^{v/d-1} X_i g^i$ where $X_i \in C_d$, and g is a generator of C_v and $X_i X_j = 0$ for all $i \neq j$. Let t be the number of nonzero X_i, $i = 0, ..., v/d-1$. There are integers $a_1, ..., a_t$ such that $X = \sum_{i=1}^{t} X_{a_i} g^{a_i}$. Furthermore, for every proper divisor w of d, there is at least one X_{a_i}, $i \in \{1, ..., t\}$, which is not orthogonal over C_w (otherwise X would be orthogonal over C_w in contradiction to the minimality of d). Hence $B = \{X_{a_1}, ..., X_{a_t}\}$ is an irreducible orthogonal family and X is a coset combination of B. This proves part (a) of Theorem 2.4.

For the proof of part (b), let $B = \{X_1, ..., X_t\}$, $X_i \in \mathbb{Z}[C_v]$, be an irreducible orthogonal family of weight n. If v does not divide $T(n)$, then all X_i are orthogonal over C_d for some proper divisor d of v by Theorem 4.6, a contradiction to the irreducibility of B. Hence v divides $T(n)$.

Recall that $\sum_{i=1}^{t} X_i X_i^{(-1)} = n$ by the definition of a orthogonal family of weight n. Since the coefficient of 1 in $X_i X_i^{(-1)}$ is at least 1, this implies $t \leq n$. Furthermore, the coefficients of all X_i cannot exceed $\sqrt{n}$ in absolute value.

For every divisor v of $T(n)$, there are only finitely many t-subsets of $\mathbb{Z}[C_v]$ with $t \leq n$ and all coefficients bounded in absolute value by $\sqrt{n}$. Since $T(n)$ has only finitely many divisors, this implies that there are only finitely many irreducible orthogonal families of weight n, and they can be enumerated in finitely many steps by brute force. This concludes the proof of Theorem 2.4. $\square$

5 Some necessary conditions on orthogonal families

Lemma 5.1 *Let v and n be positive integers. If an orthogonal family over C_v of weight n exists, then n is a square.*

Proof Let $\{A_1, ..., A_k\}$ be an orthogonal family over C_v of weight n. Let χ_0 be the trivial character of C_v. Then there is j with $|\chi_0(A_j)|^2 = n$ and $\chi_0(A_j)$ is an integer. $\square$

Lemma 5.2 *Let Γ be a cyclic p-group, and let M_i denote the set of elements of Γ of order p^i. Suppose that M is a union of some M_i and does not contain the identity element of Γ. Let j be the smallest positive integer such that M_j is contained in M. Then $|M|$ is not divisible by p^j.*

Proof Note that $|M_i| = p^i - p^{i-1}$ for $i \geq 1$. Hence $|M| = p^j - p^{j-1} + R$ where R is divisible by p^j. Thus $|M|$ is not divisible by p^j. $\square$

Definition 5.3 Let v be a positive integer, and let $B = \{A_1, ..., A_k\}$ be an orthogonal family over C_v. Let C_v^* denote the group of complex characters of C_v. We define

$$\mathcal{A}_i = \{\chi \in C_v^* : \chi(X_i) \neq 0\}$$

for $i = 1, \ldots, k$.

Remark 5.4 *If $\chi \in \mathcal{A}_i$, then $\chi^t \in \mathcal{A}_i$ for any t relatively prime to v.*

Lemma 5.5 *Let $B = \{A_1, ..., A_k\}$ be an orthogonal family over C_v of weight n and let $\mathcal{A}_i$ be defined as above. Then each $\mathcal{A}_i$ is a union of $C_{(v,n)}^{\perp}$-cosets.*

Proof Let p be a prime divisor of v and write $v = p^r w$ with $(p, w) = 1$. Let $\chi, \tau \in C_v^*$ such that $(p, \circ(\chi)) = 1$ and $\circ(\tau)$ is a p-power that divides $v/(n, v)$.

Claim If $\chi \in \mathcal{A}_i$ then $\chi\tau \in \mathcal{A}_i$.

Assume the contrary, i.e., $\chi \in \mathcal{A}_i$ and $\chi\tau \notin \mathcal{A}_i$. Write $C_v = \langle g \rangle \times \langle h \rangle$ where g has order p^r and h has order w. Let $\rho : \mathbb{Z}[C_v] \to \mathbb{Z}[\zeta_w][C_{p^r}]$ be the homomorphism defined by $\rho(g) = g$ and $\rho(h) = \chi(h)$. Note that

$$\gamma\chi = \gamma \circ \rho \tag{20}$$

for every character γ of C_{p^r}. Write $B_i = \rho(A_i)$ for all i. Let γ be any character of C_{p^r}. Since the A_i are an orthogonal family, we have $|\gamma(B_i)|^2$ for one i and $\gamma(B_j) = 0$ for $j \neq i$. Let χ_0 denote the trivial character of C_{p^r}. Since $\chi \in \mathcal{A}_i$ and $\chi\tau \notin \mathcal{A}_i$, we have $|\chi_0(B_i)|^2$ and $\tau(B_i) = 0$. Hence there is a j such that $\chi_0(B_j) = 0$ and $|\tau(B_j)|^2 = n$. Let T be the set of characters γ of C_{p^r} with $|\gamma(B_j)|^2 = n$. Note that, by Remark 5.4, T is a union of some M_k where M_k is the set of elements of $C^*_{p^r}$ of order p^k. By the inversion formula, the coefficient of 1 in $B_j B_j^{(-1)}$ is

$$\frac{1}{p^r} \sum_{\gamma \in C^*_{p^r}} |\gamma(B_j)|^2 = \frac{1}{p^r}|T|n. \tag{21}$$

Since $\chi_0 \notin T$ and $\tau \in T$, Lemma 5.2 implies that $|T|$ is not divisible by $o(\tau)$. As $o(\tau)$ divides $p^r/(n, p^r)$, we conclude that $|T|$ is not divisible by $p^r/(n, p^r)$. Thus $n|T|$ is not divisible by p^r, contradicting (21). This proves the claim.

Now write $v/(v, n) = \prod_{i=1}^t p_i^{a_i}$ where the p_i are distinct primes. Applying the Claim with the trivial character of C_v for χ and a τ of order $p_1^{a_1}$, we conclude that $\mathcal{A}_i$ is a union of cosets of the subgroup of order $p_1^{a_1}$ of C_v^*. Repeating this arguments, we see that $\mathcal{A}_i$ is a union of cosets of the subgroup of order $v/(v, n)$ of C_v^*. This proves Lemma 5.5. □

Corollary 5.6 *Let v and n be coprime positive integers. Then there is no nontrivial orthogonal family of weight n over C_v.*

Proof Suppose that $B = \{A_1, ..., A_k\}$ is an orthogonal family over C_v with $k \geq 2$. As $A_1 \neq 0$, there is $\chi \in C_v^*$ with $\chi(A_1) \neq 0$. Thus $\tau(A_1) \neq 0$ for all $\tau \in C_v^*$ by Lemma 5.5. Since $A_1 A_2 = 0$, this implies $\tau(A_2) = 0$ for all $\tau \in C_v^*$. Hence $A_2 = 0$ by Result 3.1, part a, a contradiction. □

6 Building block families of odd prime power weight

In this section, we prove Theorem 2.6 and Corollary 2.7. We need the following lemma which is a generalization of [7, Lem. 3.4].

Lemma 6.1 *Let p be an odd prime, and let r and w be positive integers with $(p, w) = 1$. Let $G = \langle\alpha\rangle \times H$ where $o(\alpha) = p^r$ and H is an abelian group of order w. Let P be the subgroup of G of order p. Let c be any positive integer. There is no $A \in \mathbb{Z}[G]$ with coefficients $-1, 0, 1$ only satisfying*

$$AA^{(-1)} = p^{2c} - p^{2c-1}P. \tag{22}$$

Proof From (22) we infer

$$\begin{array}{rcll} |\chi(A)|^2 & = & p^{2c} & \text{if } \chi \in G^* \setminus P^\perp, \\ \chi(A) & = & 0 & \text{if } \chi \in P^\perp. \end{array} \tag{23}$$

Let t be a primitive element mod p. In view of (23), Result 3.6 implies

$$Ah = E\sum_{i=1}^{p-1}(\epsilon g)^i \alpha^{t^i p^{r-1}} + PX \tag{24}$$

with $h \in G$, $E \in \mathbb{Z}[H]$, $\epsilon = \pm 1$, $g \in H$, $o(g)|(p-1)$, and $X \in \mathbb{Z}[G]$.

We first show $\epsilon = 1$. Suppose $\epsilon = -1$ and let χ be character of G of order p^r. Then $\chi \in H^\perp \setminus P^\perp$ and thus $x := \chi(E)$ is an integer $\chi(g) = 1$, and $\chi(P) = 0$. Hence $\chi(Ah) = x\sum_{i=1}^{p-1}(-1)^i\zeta^{t^i}$ by (24) where $\zeta = \chi(\alpha^{p^{r-1}})$ is a primitive pth root of unity. Note that $\sum_{i=1}^{p-1}(-1)^i\chi(h)^{t^i}$ is a quadratic Gauss sum of absolute value $\sqrt{p}$ [22, Lemma 6.1]. Hence $|\chi(A)|^2 = |\chi(Ah)|^2 = px^2$. But from (23) we have $|\chi(A)|^2 = p^{2c}$, a contradiction. This proves $\epsilon = 1$.

Let $\chi \in P^\perp \setminus \langle g\rangle^\perp$. Then $\chi(A) = 0$ by (23) and

$$\chi(\sum_{i=1}^{p-1} g^i \alpha^{t^i p^{r-1}}) = \frac{p-1}{o(g)}\chi(\langle g\rangle) = 0$$

by Result 3.1, part b. Thus $\chi(PX) = 0$ by (24). Hence we have $\tau(PX) = 0$ for all $\tau \in G^* \setminus (P\langle g\rangle)^\perp$. By Result 3.1, part c, we can write $PX = P\langle g\rangle Y$ for some $Y \in \mathbb{Z}[G]$. Replacing A by Ah^{-1} and using $\epsilon = 1$, we get

$$A = E\sum_{i=1}^{p-1} g^i \alpha^{t^i p^{r-1}} + P\langle g\rangle Y \tag{25}$$

from (24).

W.l.o.g. we assume that the elements in the support of Y are all from distinct cosets of $P\langle g\rangle$. We will show that Y has coefficients $-1, 0, 1$ only. If $k \in G$ has coefficient $z \notin \{-1, 0, 1\}$ in Y, then every $l \in Pk$ has coefficient z in $P\langle g\rangle Y$. But since $E \sum g^i \alpha^{t^i p^{r-1}}$ does not contain any full coset of P, this implies that A has at least one coefficient equal to z. This contradicts the assumption that A has coefficients $-1, 0, 1$ only. Hence Y has coefficients $-1, 0, 1$ only.

Now let $\rho : G \mapsto G/P$ be the natural epimorphism and write $\bar{g} = \rho(g)$. Note that $\rho(A) = 0$ by (23) and Result 3.1, part a. Hence we get

$$0 = \rho(A) = \frac{p-1}{o(g)} \rho(E)\langle \bar{g}\rangle + p\langle \bar{g}\rangle \rho(Y) \tag{26}$$

from (25). Since the elements in the support of Y are all from distinct cosets of $P\langle g\rangle$ and Y has coefficients $-1, 0, 1$ only, $\langle \bar{g}\rangle \rho(Y)$ also has coefficients $-1, 0, 1$ only. Thus (26) implies $\rho(Y) = 0$, i.e. $Y = 0$, or $o(g) = p - 1$. In both cases (25) shows that both x_1 and x_2 are divisible by $p - 1$ where x_1 respectively x_2 is the number of coefficients of A equal to 1 respectively -1. By (22) we have $x_1 - x_2 = |A| = 0$. Comparing the coefficient of 1 on both sides of (22) we get $x_1 + x_2 = p^{2c} - p^{2c-1}$. Hence $x_1 = p^{2c-1}(p-1)/2$ is not divisible by $p - 1$, a contradiction. $\square$

Proof of Theorem 2.6 Let p be an odd prime and suppose that a nontrivial orthogonal family $\{A_1, ..., A_k\}$ of weight $n = p^d$ over C_v exists where d is a positive integer. By Lemma 5.1, we have $n = p^{2c}$ for some positive integer c. Write $v = p^r w$ with $(p, w) = 1$. By Corollary 5.6, we have $r \geq 1$.

By Lemma 5.5, we can assume $|\chi(A_1)|^2 = n$ for all $\chi \in C_v^* \setminus C_p^\perp$. Furthermore, by Result 3.6, we have

$$A_1 = T + C_p X \tag{27}$$

with $T \in \mathbb{Z}[C_{pw}]$ and $X \in \mathbb{Z}[C_v]$. Since $\{A_1, ..., A_k\}$ is a nontrivial orthogonal family there is $\tau \in C_p^\perp$ with $\tau(A_1) = 0$. Thus $\tau(T) \equiv 0 \bmod p$ by (27). Since $T \in \mathbb{Z}[C_{pw}]$ we have $\psi(T) = \tau(T)$ for all $\psi \in C_p^\perp$. This shows

$$\psi(T) \equiv 0 \bmod p \tag{28}$$

for all characters $\psi \in C_p^{\perp}$. Let $\rho : C_v \to C_v/C_p$ be the natural epimorphism. By (28) we have $\kappa(\rho(T)) \equiv 0 \bmod p$ for all characters κ of C_v/C_p. Since $\rho(T) \in \mathbb{Z}[C_{pw}/C_p]$ and p does not divide $|C_{pw}/C_p|$, this implies $\rho(T) \equiv 0 \bmod p$ by Result 3.1, part a. Hence, in view of (27), we have

$$\rho(A_1) \equiv 0 \mod p. \tag{29}$$

Now assume $\rho(A_1) = 0$. Then $\chi(A_1) = 0$ for all $\chi \in C_p^{\perp}$ and $|\chi(A_1)|^2 = n = p^{2c}$ for $\chi \in C_v * \backslash C_p^{\perp}$. Hence $A_1 A_1^{(-1)} = p^{2c} - p^{2c-1} C_p$ by Result 3.1, part a. But this is impossible by Lemma 6.1. Hence $\rho(A_1) \neq 0$.

Now let $i > 1$. Since $\chi(A_1) \neq 0$ for all $\chi \in C_v^* \setminus C_p^{\perp}$, we have $\chi(A_i) = 0$ for all these characters. This means that $\phi(A_i) = 0$ where $\phi : \mathbb{Z}[C_v] \to \mathbb{Z}[\zeta_{p^r}][C_w]$ is the homomorphism which sends a generator of C_{p^r} to ζ_{p^r} and whose restriction to C_w is the identity map. Note that the kernel of ϕ is $\{XC_p : X \in \mathbb{Z}[C_v]\}$. Hence we have $A_i = X_i C_p$ with $X_i \in \mathbb{Z}[C_v]$. This implies

$$\rho(A_i) \equiv 0 \mod p \quad \text{for } i = 2, ..., k. \tag{30}$$

Since $A_i \neq 0$ and $\chi(A_i) = 0$ for all $\chi \in C_v^* \setminus C_p^{\perp}$, there is $\tau_i \in C_p^{\perp}$ with $\tau_i(A_i) \neq 0$. This shows $\rho(A_i) \neq 0$ for $i = 2, ..., k$.

In summary, we have shown $\rho(A_i) \equiv 0 \mod p$ and $\rho(A_i) \neq 0$ for $i = 1, ..., k$. Note that $\rho(A_i)/p$, $i = 1, ..., k$, are elements of $\mathbb{Z}[C_v/C_p]$ with coefficients $-1, 0, 1$ only since the A_i have coefficients $-1, 0, 1$ only. Hence $\{\rho(A_i)/p : i = 1, ..., k\}$ is an orthogonal family of weight p^{2c-2} over $\mathbb{Z}[C_v/C_p]$.

Repeating this argument, we finally obtain an orthogonal family over a cyclic group whose order is coprime to the weight of the orthogonal family. But this is impossible by Corollary 5.6. □

Proof of Corollary 2.7 Suppose $X \in \mathbb{Z}[C_v]$ is a proper circulant weighing matrix with $XX^{(-1)} = n$ where n is an odd prime power. By Theorem 2.4, X is a coset combination of an irreducible orthogonal family B over C_w for some divisor w of v. By Theorem 2.6, B has only one element, i.e., $B = \{A_1\}$ with $A_1 \in \mathbb{Z}[C_w]$ and $X = A_1 g$ for some $g \in C_v$. Since X is proper, we conclude $w = v$. Hence $\{X\}$ is also an irreducible orthogonal family of weight n. Since there at most finitely many such families by Theorem 2.4, there are also at most finitely many proper circulant weighing matrices of weight n. □

References

[1] M.H. Ang, K.T. Arasu, S.L. Ma, Y. Strassler: Study of proper circulant weighing matrices with weight 9. *Discrete Math.* **308** (2008), 2802-2809.

[2] K.T. Arasu: A reduction theorem for circulant weighing matrices. *Australas. J. Combin.* **18** (1998), 111-114.

[3] K.T. Arasu, J.F. Dillon: Perfect ternary arrays. *In: Difference sets, sequences and their correlation properties, NATO Adv Sci Inst Ser C Math Phys Sci* **542**, Kluwer 1999, 1-15.

[4] K.T. Arasu, J.F. Dillon, D. Jungnickel, A. Pott: The solution of the Waterloo problem. *J. Combin. Theory A* **71** (1995), 316-331.

[5] K.T. Arasu, K.H. Leung, S.L. Ma, A. Nabavi, D.K. Ray-Chaudhuri: Determination of all possible orders of weight 16 circulant weighing matrices. *Finite Fields Appl.* **12** (2006) 498538.

[6] K.T. Arasu, K.H. Leung, S.L. Ma, A. Nabavi, D.K. Ray-Chaudhuri: Circulant weighing matrices of weight 2^{2t}. *Des. Codes Crypt.* **41** (2006), 111-123.

[7] K.T. Arasu, S.L. Ma: Some new results on circulant weighing matrices. *J. Alg. Comb.* **14** (2001), 91-101.

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

[9] J.W.S. Cassels: *An Introduction to Diophantine Approximation.* Cambridge University Press 1957.

[10] J.A. Davis and J. Jedwab: A unifying construction of difference sets. *J. Combin. Theory A* **80** (1997), 13-78.

[11] P. Eades: Circulant (v, k, λ)-designs. *In: Combinatorial Mathematics VII, Lecture Notes in Math.* **829**, Springer 1980, 83-93.

[12] P. Eades, R.M. Hain: On Circulant Weighing Matrices. *Ars Comb.* **2** (1976), 265-284.

[13] L. Epstein: *The classification of circulant weighing matrices of weight 16 and odd order*. M.Sc. Thesis, Bar-Ilan University, 1998.

[14] C. Koukouvinos, J. Seberry: Weighing matrices and their applications. *J. Stat. Plann. Inf.* **62** (1997), 91-101.

[15] R.L. McFarland: *On multipliers of abelian difference sets.* Ph.D. Dissertation, Ohio State University 1970.

[16] K.H. Leung and B. Schmidt, The Field Descent Method. *Des. Codes Crypt.* **36** (2005), 171-188.

[17] K.H. Leung, S.L. Ma, B. Schmidt: Constructions of Relative Difference Sets with Classical Parameters and Circulant Weighing Matrices. *J. Combin. Theory A* **99** (2002), 111-127.

[18] A. Pott: *Finite geometry and character theory.* Lecture Notes 1601, Springer 1995.

[19] B. Schmidt: Cyclotomic integers and finite geometry. *J. Am. Math. Soc.* **12** (1999), 929-952.

[20] B. Schmidt: *Characters and cyclotomic fields in finite geometry.* Lecture Notes in Mathematics **1797**, Springer 2002.

[21] Y. Strassler: *The classification of circulant weighing matrices of weight 9.* Ph.D. Thesis, Bar-Ilan University 1997.

[22] L.C. Washington: *Introduction to Cyclotomic Fields.* Graduate Texts in Math. 83, Springer, Berlin/Heidelberg/New York 1997.