Circulant Weighing Matrices

by

Goldwyn Millar

A Thesis submitted to

the Faculty of Graduate Studies

In Partial Fulfillment of the Requirements for the Degree of

MASTER OF SCIENCE

Department of Mathematics

University of Manitoba

Winnipeg, Manitoba

Circulant Weighing Matrices

By

Goldwyn Millar

A Thesis/Practicum submitted to the Faculty of Graduate Studies of The University of Manitoba in partial fulfillment of the requirement of the degree

Of

Master of Science

Abstract

A *circulant matrix* is a matrix such that each of its rows, after the first, can be obtained from the row above it by a right cyclic shift. A *circulant weighing matrix* of order n and weight w (a $CW(n,w)$) is a $n \times n$ circulant $(0, \pm 1)$-matrix W such that $WW^T = wI$.

Circulant weighing matrices can be constructed by exploiting properties of quadrics in projective and affine space. Group characters provide a link between $CW(n,w)$'s and elements of absolute value $\sqrt{w}$ in $\mathbb{Z}[\zeta_n]$ (the cyclotomic field over the n^{th} roots of unity). By making use of this link, it is possible to translate facts about the decomposition groups of prime ideals in $\mathbb{Z}[\zeta_n]$ into necessary conditions for the existence of $CW(n,w)$'s; this technique is the basis of several powerful methods for studying $CW(n,w)$'s: the Self-conjugacy method, the Multiplier method, and the Field descent method.

I would like to thank my supervisor, Dr. Craigen, for 3 and 1/2 years of valuable guidance and criticism and for the financial support he has provided for me throughout this entire process. I would like to extend my thanks to my thesis committee, Dr. Davidson, Dr. Gunderson, and Dr. Li, for their valuable feedback. Further, I am grateful to the University of Manitoba mathematics department for the partial financial support I received during the first two years of my studies. I would also like to thank my parents, Barbara and Scott Millar, and my partner, Molly Davidson, for all of their support and encouragement.

Contents

Chapter 1

Introduction

Let $w, n \in \mathbb{N}$ and let $w \leq n$. A *weighing matrix* of *order* n and *weight* w is a $n \times n$ $(0, \pm 1)$ matrix W such that $WW^T = wI$. We may also refer to W as a $W(n, w)$ or, alternatively, as a *weighing matrix with paramaters* (n, w). The row vectors of W are mutually orthogonal and each contains exactly w non-zero entries.

The following matrix is a $W(4, 3)$ (throughout this thesis, $-$'s will be used to represent -1's in matrices).

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

Since every invertible matrix commutues with its inverse, it follows that W commutes with W^T. Therefore, W^T is also a weighing matrix of weight w. So the column vectors of W are also mutually orthogonal and each contains exactly w non-zero

entries. By taking the transpose of the above $W(4,3)$, we obtain another $W(4,3)$.

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

If W_0 can be obtained from W by a permutation of the rows and columns of W, then the rows of W_0 are mutually orthogonal and they each contain exactly w non-zero entries. Thus, W_0 is also a weighing matrix of weight w. Likewise, if W_0 can be obtained by multiplying some of the rows and columns of W by -1, then W_0 is still a weighing matrix of weight w. Two weighing matrices that can be obtained from one another by permutation of rows and columns or by multiplication of rows and columns by -1 are considered *equivalent as weighing matrices.*

The following two matrices are equivalent $W(6,4)$'s, since the second can be obtained from the first via a permutation of the first two rows and a multiplication of the second column by -1.

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

A *circulant matrix* is a matrix such that each of its rows, after the first, is obtained from the row above it by a right cyclic shift. A circulant matrix is determined by its first row; if $A = [a_{ij}]$ is a circulant, then A can be written as $\text{circ}(a_{11}, a_{12}, ..., a_{1n})$. Following convention, we will refer to a circulant weighing matrix of order n and weight w as a $CW(n, w)$. The second matrix in the above example is a $CW(6, 4)$.

Most research about weighing matrices is concerned with determining the parameters n and w such that there exists a $W(n, w)$. However, other questions regarding structure and equivalence (in various senses of the word) are also considered.

The study of circulant weighing matrices is interesting within the broader context of the study of weighing matrices. For instance, for each prime power q, there exists a $CW(q^2 + q + 1, q^2)$ (see Chapter 2 for two, out of many possible, justifications of this fact); these weighing matrices are, in a sense, optimal (see Theorem 1.4.2 below). Further, Antweiler, Bomer, and Luke [ABL90] discovered, via a computer search, a $CW(33, 25)$; this filled an open entry in Craigen's weighing matrix table [Cra96]. Arasu and Torban [AT99] later provided a theoretical explanation of the existence of this matrix.

Circulant weighing matrices are also interesting objects in their own right. Weighing matrices in general and circulant weighing matrices in particular have applications in statistics and engineering (see [Moo46], [GG05], [Hai77], and [HJ83], for instance). The study of circulant weighing matrices began in the late 1960's and the early 1970's with the discovery that they can be constructed using projective geometries (see [Cha67] and [DGS71]). In fact, because of the group structure underlying these matrices, results and techniques from diverse branches of mathematics, such as num-

ber theory, character theory, and combinatorics, are used to study them. Research on circulant weighing matrices appears in both the Mathematics and Engineering literature, and this research has been particularly intensive during the last 10 years. The primary purpose of this thesis is to elucidate the major results and techniques from the literature on circulant weighing matrices. I will also attempt to explain how the techniques in question can be applied in specific cases.

Though I've added a few minor results of my own to the mix (see Appendix A), this thesis is mainly an exposition of known results. Further, due to the sheer number of results pertaining to these objects, proofs of some results are omitted or merely sketched.

In this introductory chapter I will attempt to motivate the study of circulant weighing matrices and to explore the basic definitions and results pertaining to circulant weighing matrices and some closely related classes of combinatorial objects.

1.1 Hadamard Matrices

In 1893, J. Hadamard [Had93] proved the following result. The proof given here is from [Cra09]. In what follows, $*$ denotes the conjugate transpose.

Theorem 1.1.1. *Let*

$$H = \begin{pmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_n \end{pmatrix} \in \mathbb{C}_{n\times n}.$$

Then $|det(H)| \leq ||\mathbf{v}_1|| \cdots ||\mathbf{v}_n||$ *(where* $||\cdot||$ *denotes the usual complex norm) and equality holds if and only if for each pair* i, j *such that* $i \neq j$, $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = 0$ *(where*

$\langle \cdot, \cdot \rangle$ *denotes the usual complex inner product).*

Proof. Let $\mathbf{u}_1 = \mathbf{v}_1$ and, for $i > 1$, let $E_i = \text{span}\{\mathbf{u}_j\}_{j<i}$, let $\mathbf{w}_i = \text{proj}_{E_i}\mathbf{v}_i$, and let $\mathbf{u}_i = \mathbf{v}_i - \mathbf{w}_i$. Define

$$K = \begin{pmatrix} \mathbf{u}_1 \\ \vdots \\ \mathbf{u}_n \end{pmatrix}.$$

Since for each i, $\mathbf{w}_i \in E_i$, K can be obtained from H by adding multiples of rows to one another. Then, since the rows of K are pairwise orthogonal,

$$|\det(H)| = |\det(K)| = \sqrt{\det(KK^*)} = \sqrt{||\mathbf{u}_1||^2 \cdots ||\mathbf{u}_n||^2} = ||\mathbf{u}_1|| \cdots ||\mathbf{u}_n||.$$

For each $i > 1$, $\mathbf{v}_i = \mathbf{u}_i + \mathbf{w}_i$. Note that $\langle \mathbf{u}_i, \mathbf{w}_i \rangle = 0$. So, by the Pythagorean Theorem, $||\mathbf{v}_i||^2 = ||\mathbf{u}_i||^2 + ||\mathbf{w}_i||^2$. It follows that $||\mathbf{v}_i|| \geq ||\mathbf{u}_i||$, and that equality holds if and only if $\mathbf{w}_i = \mathbf{0}$, i.e. $\mathbf{v}_i = \mathbf{u}_i$. But the condition that, for each i, $\mathbf{v}_i = \mathbf{u}_i$ is equivalent to the condition that for each pair i, j such that $i \neq j$, $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = 0$. □

Corollary 1.1.2. *Let $A = [a_{ij}]$ be such that, for each i, j, $|a_{ij}| \leq 1$. Then $|det(A)| \leq n^{\frac{n}{2}}$. Further, equality is attained if and only if $AA^* = nI$ and each entry of A lies on the unit circle.*

Proof. Let

$$A = \begin{pmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_n \end{pmatrix}.$$

Then, by Theorem 1.1.1, $|\det(A)| \leq ||\mathbf{v}_1|| \cdots ||\mathbf{v}_n|| \leq \sqrt{n}^n = n^{n/2}$, and equality is attained, in the first inequality, if and only if the vectors $\mathbf{v}_i$ are pairwise orthogonal.

Further, since for each i, j, $|a_{ij}| \leq 1$, it follows that, for each i, $||v_i|| \leq \sqrt{n}$. So equality is attained in the second inequality if and only if each entry of A lies on the unit circle. □

Lemma 1.1.3. *Let W be a $W(n, w)$. Then $|det(W)| = w^{n/2}$.*

A *Hadamard matrix of order n* is a $n \times n$ (± 1) matrix H such that $HH^T = nI$; in other words, Hadamard matrices are $W(n, n)$'s. If A is a real matrix, then the bound in Corollary 1.1.2 is met if and only if A is a Hadamard matrix. Because of this property, Hadamard matrices have many important applications (see [SY92]). The study of Hadamard matrices predates the study of weighing matrices (qua weighing matrices).

The following matrix is a Hadamard matrix of order 8.

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

For a $n \times n$ matrix A, $|\det(A)|$ is equal to the content (n-dimensional volume) of the parallelepiped spanned by the row (or column) vectors of A. So, by Corollary 1.1.2, if there exists a Hadamard matrix of order n, then a parallelepiped spanned by a set of vectors that lie within the n-dimensional unit cube has maximum possible

content if and only if the set of vectors form the set of row vectors of a Hadamard matrix.

Hadamard also proved the following simple, yet important, result.

Theorem 1.1.4. *If there exists a Hadamard matrix of order n, then n is either* 1, 2, *or a multiple of* 4.

Proof. [1] is a Hadamard matrix of order 1 and

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

is a Hadamard matrix of order 2. By considering all cases explicitly, it is possible to rule out the existence of a Hadamard matrix of order 3.

Suppose that H is a hadamard matrix of order $n \geq 4$. Then, by negating and permuting the columns of H appropriately, it is possible to generate an equivalent Hadamard matrix H_0 whose first three rows can be written as follows:

$1 \cdots 1$	$1 \cdots 1$	$1 \cdots 1$	$1 \cdots 1$
$1 \cdots 1$	$1 \cdots 1$	$- \cdots -$	$- \cdots -$
$1 \cdots 1$	$- \cdots -$	$1 \cdots 1$	$- \cdots -$
a	b	c	d

From the orthogonality of these three rows, we deduce the next three equations:

$$a - b + c - d = 0 \tag{1.1}$$

$$a - b - c + d = 0 \tag{1.2}$$

$$a + b - c - d = 0 \tag{1.3}$$

By adding (1.1) to (1.2), we deduce that $a = b$. By adding (1.1) to (1.3), we deduce that $a = d$. And by adding (1.2) to (1.3) we deduce that $a = c$. So, $n = a + b + c + d = 4a$. □

Hadamard conjectured that there exists a Hadamard matrix of order $4t$, for every $t \geq 1$. Over the last 115 years, many constructions of Hadamard matrices have been discovered. However, Hadamard's conjecture still remains unresolved.

It is known that there exist circulant Hadamard matrices of order 1 (the matrix (1)) and order 4 (given by $\mathrm{circ}(-, 1, 1, 1)$). All the evidence (see [Tur65], [Sch99], [LS05], and [Sch]) supports the conjecture (due to Ryser, see [Rys63]) that these are the only circulant Hadamard matrices. In fact, Schmidt and Leung [LS05] have shown that there exists no circulant Hadamard Matrix of order n, for $4 < n < 548,964,900$. However, this conjecture is also still open. Some of the techniques devised by Richard Turyn [Tur65] and Bernhard Schmidt [Sch99], [LS05], [Sch] to rule out the existence of circulant Hadamard matrices can be adapted to prove powerful non-existence results for circulant weighing matrices (see Chapter 3).

In 1933, Paley [Pal33] discovered an infinite class of Hadamard matrices that are very nearly circulant. Let q be a prime such that $q \equiv 3 \pmod 4$. Let $\mathbf{j}$ be the row vector of all 1's and of length q. Paley showed that there exists a $q \times q$ circulant

matrix Q with all entries ± 1 such that

$$\begin{pmatrix} 1 & \mathbf{j} \\ \mathbf{j}^T & Q \end{pmatrix}$$

is a Hadamard matrix; Q is called the *circulant core* of the Hadamard matrix. Throughout this thesis, J_t will denote the $t \times t$ matrix of all 1's. So we have that $QQ^T = qI - (J_q - I_q)$.

1.2 Hotelling's Weighing Problem

In this section, I discuss the type of application that originally motivated the study of weighing matrices (see, for instance, Hotelling's paper [Hot42]); in the next section, I will discuss a type of application that requires *circulant* weighing matrices. Consider the following problem: A chemist has an unbiased 2 pan scale that ascertains the difference between the weight of the load in the left pan and the weight of the load in the right pan with error σ and variance σ^2. She wants to determine the weight of two objects.

If she were to weigh each object separately, the estimates that she would obtain for the weights of both objects would have variance σ^2 and error σ.

A better strategy is to first weigh both objects together in the left pan, and then to record the weight when one object is placed in each pan. This yields the following two equations for the weights, a and b, of the two objects:

$$a + b = z_1, \quad a - b = z_2,$$

for some z_1, z_2, measured in whatever units the scale uses. Consequently,

$$a = \frac{(z_1 + z_2)}{2}, \quad b = \frac{(z_1 - z_2)}{2}.$$

It is well known [Was04] that if two estimates X_1 and X_2 have variances ϵ_1 and ϵ_2, respectively, then the variance of $X_1 \pm X_2$ is $\epsilon_1 + \epsilon_2$. Further, for any estimate X with variance ϵ and for any number c, cX has variance $c^2\epsilon$. So a and b each have variance $2\sigma^2/4 = \sigma^2/2$ and error $\sigma/\sqrt{2}$. This is a significant improvement over the first method.

Now suppose that she needs to weigh n objects in n weighings and that the scale can weigh, at most, w of these objects simultaneously, where $w \leq n$. Label the n objects $1, 2, ..., n$. For a given set of n weighings, define the $(0, \pm 1)$ matrix $X = [x_{ij}]$ by the rule that $x_{ij} = 1$ if the j^{th} object is in the left pan in the i^{th} weighing, $x_{ij} = -1$ if the j^{th} object is in the right pan in the i^{th} weighing, and $x_{ij} = 0$ otherwise. X is called a *weighing design.* For each i, let b_i be the true weight of the i^{th} object. Let $\mathbf{b} = (b_1, ..., b_n)^T$. For each i, let y_i be the scale reading for the i^{th} weighing. Let $\mathbf{y} = (y_1, ..., y_n)^T$. For each i, let ϵ_i be the error in the scale reading for the i^{th} weighing. Let $\epsilon = (\epsilon_1, ..., \epsilon_n)^T$. Then we have that

$$X\mathbf{b} = \mathbf{y} + \epsilon. \quad (1)$$

For two random variables Z and Y with expected values $E(Z) = \mu$ and $E(Y) = \gamma$, the *covariance* of Z and Y is defined as $\text{cov}\,(Z, Y) = E((Z - \mu)(Y - \gamma))$. Covariance measures how variables vary together relative to their expected values. In the case that $Z = Y$, covariance reduces to variance. Let $\hat{\mathbf{b}}$ be an estimate for $\mathbf{b}$. For each

i, j, let $\sigma_{i,j} = \text{cov}\left(\hat{b}_i, \bar{b}_j\right)$. Then the *variance matrix* is defined as $\text{Var}\left(\hat{\mathbf{b}}\right) = [\sigma_{ij}]$. The variance matrix is the multivariate generalization of the concept of variance.

A symmetric, square, and real matrix M is *positive semi-definite* if, for each row vector $\mathbf{x}$, $\mathbf{x}M\mathbf{x}^T \geq 0$. For example,

$$\begin{pmatrix} 1 & -2 & 0 \\ -2 & 4 & 0 \\ 0 & 0 & 721 \end{pmatrix}$$

is positive semi-definite since, for any row vector $\mathbf{x} = (x_1, x_2, x_3)$,

$$(x_1, x_2, x_3) \begin{pmatrix} 1 & -2 & 0 \\ -2 & 4 & 0 \\ 0 & 0 & 721 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = (x_1 - x_2)^2 + 721x_3^2 > 0.$$

Positive semi-definite matrices play a role similar to that of non-negative numbers; for instance, they have all real, non-negative eigenvalues [Bha07]. Positive semi-definite matrices induce a partial ordering on the set of matrices: $M_1 \gg M_2$ if and only if $M_1 - M_2$ is a positive semi-definite matrix. It turns out that $\text{Var}\left(\hat{\mathbf{b}}\right)$ is positive semi-definite [Was04].

For a given system, such as (1), the best linear unbiased estimator is the estimate $\hat{\mathbf{b}}$ such that, for each estimate $\mathbf{c} \neq \hat{\mathbf{b}}$, $\text{Var}(\mathbf{c}) \gg \text{Var}\left(\hat{\mathbf{b}}\right)$. It follows, by the Gauss-Markov Theorem (see [Hot42] for instance), that the best linear unbiased estimator $\hat{\mathbf{b}}$ is given by the formula

$$\hat{\mathbf{b}} = \left(X^T X\right)^{-1} X^T \mathbf{y},$$

with $\text{Var}\left(\hat{\mathbf{b}}\right) = \left(X^T X\right)^{-1}\sigma^2$.

There are also two useful scalar generalizations of variance: generalized variance and total variance. The content of the parallelepiped generated by the row vectors of $\text{Var}\left(\hat{\mathbf{b}}\right)$ is an indicator of the amount of variance in the system. Since $\text{Var}\left(\hat{\mathbf{b}}\right)$ is positive semi-definite, it has all non-negative eigenvalues. Consequently, $\left|\det\left(\text{Var}\left(\hat{\mathbf{b}}\right)\right)\right| = \det\left(\text{Var}\left(\hat{\mathbf{b}}\right)\right)$. *Generalized variance* is defined as $\det\left(\text{Var}\left(\hat{\mathbf{b}}\right)\right)$, *i.e.* as the content of the parallelepiped generated by the row vectors of $\text{Var}\left(\hat{\mathbf{b}}\right)$. So, the choice of weighing design which minimizes generalized variance is one which minimizes the determinant of $\left(X^T X\right)^{-1}$ and which, consequently, maximizes the determinant of X. By Hadamard's Theorem (Theorem 1.1.1) then, optimal weighing designs are obtained when X is chosen to be a weighing matrix (hence, the name *weighing* matrix). In this case, $\det(X) = w^{n/2}$. Maximum accuracy is attained by choosing w as large as possible (of course, the ability to choose a large w depends not only on the existence of a $W(n,w)$, but also on the equipment available to the chemist).

Total variance is defined as $\text{Trace}\left(\text{Var}\left(\hat{\mathbf{b}}\right)\right) = \sum_{i=1}^{n}\sigma_{ii} = \sum_{i=1}^{n}\text{var}\left(\hat{b}_i\right)$. Total variance can also be minimized by choosing the weight as large as possible.

Although the problem was stated in terms of weighings, the procedure described in this section is applicable in many situations in which a scientist needs measurements of various quantities, including measurements of lengths, voltages, resistances, and concentrations of chemicals in solutions [Moo46] and also design of agricultural experiments and GPS navigation [Cra09].

Weighing matrices also find applications in optics. They have been used to improve the performance of instruments called spectrometers (see, for instance, [Hal77]).

1.3 Sequences With Good Autocorrelation Properties

We define the *correlation* between two vectors $(a_1, ..., a_n)$ and $(b_1, ..., b_n)$ (in $\mathbb{C}^n$) as their Euclidean inner product $\langle (a_1, ..., a_n), (b_1, ..., b_n) \rangle = \sum_{i=1}^{n} a_i \overline{b_i}$, so that parallel vectors have a high magnitude correlation, and vectors that are closer to being orthogonal have a low correlation. The *correlation* between two complex-valued functions f and g, defined and integrable on the real interval $[0, T]$, is the integral $\int_0^T f(x)\overline{g(x)}dx$. If we view the vectors $(a_1, ..., a_n)$ and $(b_1, ..., b_n)$ as step functions α and β, respectively, defined on $[0, n)$ such that, for each $i = 1, ..., n$, $\alpha(x) = a_i$ and $\beta(x) = b_i$ on the sub-interval $[i-1, i)$, then $\int_0^T \alpha(x)\overline{\beta(x)}dx = \sum_{i=1}^{n} a_i \overline{b_i}$. Consequently, the definition of correlation between two integrable functions can be viewed as a generalization of the definition of correlation between two vectors.

Let f and g be two periodic functions with period of length T, shifted, if necessary, so that they both have periods that begin at $x = 0$. Define the function $P_{f,g}$ by the rule $P_{f,g}(\tau) = \int_0^T f(t)\overline{g(t+\tau)}dt$. $P_{f,g}(\tau)$ is therefore equal to the correlation of $f(t)$ and $g(t+\tau)$; $P_{f,g}$ is called the *periodic cross-correlation function* of f and g. The function $P_{f,f}$ is the *periodic autocorrelation function* of f.

Similarly, for two complex sequences $\{s_i\}_{i=0,...,n-1}$ and $\{t_i\}_{i=0,...,n-1}$, define $P_{s,t} : \mathbb{Z} \to \mathbb{C}$ by the rule $P_{s,t}(\tau) = \sum_{i=0}^{n-1} s_i \overline{t_{i+\tau}}$. $P_{s,t}$ is the periodic cross-correlation function of the sequences $\{s_i\}_{i=0,...,n-1}$ and $\{t_i\}_{i=0,...,n-1}$ (if we regard the sequences as periodic step functions, this definition reduces to a special case of the definition of the periodic cross-correlation of two functions). $P_{s,s}$ is the periodic autocorrelation function of $\{s_i\}_{i=0,...,n-1}$.

Suppose that f and g are two (not necessarily periodic) functions that are defined and integrable on the interval $[0, T]$. Define the function $A_{f,g}$ by the rule $A_{f,g}(\tau) = \int_0^{T-\tau} f(t)\overline{g(t+\tau)}dt$. $A_{f,g}$ is called the *aperiodic cross-correlation function* of f and g. $A_{f,f}$ is the *aperiodic autocorrelation function* of f.

Similarly, for two complex sequences $\{s_i\}_{i=0,...,n-1}$ and $\{t_i\}_{i=0,...,n-1}$, define $A_{s,t} : \mathbb{Z} \to \mathbb{C}$ by the rule $A_{s,t}(\tau) = \sum_{i=0}^{n-\tau-1} s_i\overline{t_{i+\tau}}$. $A_{s,t}$ is the aperiodic cross-correlation of $\{s_i\}_{i=0,...,n-1}$ and $\{t_i\}_{i=0,...,n-1}$. $A_{s,s}$ is the aperiodic autocorrelation of $\{s_i\}_{i=0,...,n-1}$. We say that two sequences $\{s_i\}_{i=0,...,n-1}$ and $\{t_i\}_{i=0,...,n-1}$ have *good periodic cross-correlation properties* if, for each τ, $P_{s,t}(\tau)$ is "small." Likewise, we say that $\{s_i\}_{i=0,...,n-1}$ has *good periodic autocorrelation properties* if, for each τ that is not a multiple of n, $|P_{s,s}(\tau)|$ is "small;" $\{s_i\}_{i=0,...,n-1}$ has *perfect periodic autocorrelation* if, for each τ that is not a multiple of n, $P_{s,s}(\tau) = 0$. Good aperiodic cross-correlation and autocorrelation are defined similarly.

Now suppose that there exists a circulant matrix $W = \text{circ}(a_0, ..., a_{n-1})$. For each $i = 0, ..., n-1$ let $\mathbf{r}_i$ be the i^{th} row of W. Notice that, since W is circulant, for any $i, j \in [0, n-1]$, $\mathbf{r}_i \cdot \mathbf{r}_j = \mathbf{r_0} \cdot \mathbf{r}_{j-i}$. Therefore, W is a weighing matrix if and only if, for each $\tau = 1, ..., n-1$, $\mathbf{r}_0 \cdot \mathbf{r}_\tau = 0$. But, $\mathbf{r}_0 \cdot \mathbf{r}_\tau = \sum_{i=0}^{n-1} a_i a_{i-\tau}$. Consequently, W is a circulant weighing matrix if and only if $\{a_i\}_{i=0,...,n-1}$ is a ternary sequence with perfect periodic autocorrelation. Similarly, the circulant core of a Paley Hadamard matrix defines a sequence $\{a_i\}_{i=0,...,n-1}$ such that, if τ is not a multiple of n, $P_{a,a}(\tau) = -1$. So that $\{a_i\}_{i=0,...,n-1}$ is a binary sequence with good periodic autocorrelation properties.

Sequences with good correlation properties have applications to radar and sonar (see [GG05]). For instance, in radar applications, the goal is often to determine the

distance between the radar station and some object. To ascertain this distance, an impulse of energy is sent from the station and bounced off of the object, and the time that it takes for the energy to return to the radar station is measured.

When the energy returns to the radar station, the signal registered is correlated against an idealized version of the function representing the energy burst that was originally sent. In order that the measurements be as precise as possible, the autocorrelation function should spike at the precise instant that the burst completely returns to the station.

If it could be done, the best way to do this would be to use a short burst of energy with a high amplitude, so that enough energy would return to the station that it would be possible to get a good reading (some energy will be lost in transmission and when bouncing off the object). However, it is physically impractical to send a large amount of energy in a short burst [GG05]. So longer bursts of energy must be used to attain a sufficiently high amplitude. The problem with using longer bursts of energy is that, in the presence of noise, it becomes difficult to ascertain exactly when the autocorrelation function reaches its peak. But if the signal is sent at power levels varying according to the step function associated with a sequence with good autocorrelation properties, then it becomes possible to send a longer signal such that the autocorrelation function has a clear spike at the instant the signal returns to the station. If the signal can only be sent once, then sequences with good aperiodic autocorrelation properties must be used. But, if a signal can be sent multiple times (consecutively), then sequences with good periodic correlation properties can be used [GG05]. Apparently, this technique was used in 1961 by the Jet Propulsion Laboratory to measure the distance from Venus to Earth. This was

the first successful radar measurement of the distance to another planet in the solar system. Further, the distance obtained by the measurement made it possible to improve the precision of the astronomical unit (which is the basic unit of measurement for distances within the solar system) by three orders of magnitude [GG05].

Since it is desirable that the spike be as large as possible, binary sequences are preferable to ternary sequences (with identical correlation properties) and sequences obtained from large weight circulant weighing matrices are preferable to sequences obtained from small weight circulant weighing matrices. Circulant Hadamard matrices are, therefore, the gold standard (for periodic autocorrelation). However, as mentioned in Section 1.1, Schmidt and Leung [LS05] have already shown that there exist no circulant Hadamard matrices of a size that might be used in any kind of practical application. Sequences comprised of complex units may also be used [GG05].

A *Barker sequence* $\{a_i\}_{i=0,\ldots,n-1}$ is a binary sequence such that, for any τ that is not a multiple of n, $|A_{a,a}(\tau)| \leq 1$. Such sequences, should they exist, would be ideal for applications that call for sequences with good aperiodic autocorrelation properties. Unfortunately, Schmidt and Leung [LS05] have shown that there exist no Barker sequences of length ℓ, with $13 < \ell < 10^{22}$. Jedwab [Jed08] has produced a survey about different types of combinatorial objects that may be used instead of Barker sequences. A question that does not appear to have received much consideration is whether or not there exist any ternary $(0, \pm 1)$ Barker sequences of "large weight." A number of ternary Barker sequences have been discovered by computer search (see [Moh74] and [MR96]).

In order that a single radar station be used to simultaneously range several tar-

gets, it is useful to have sets of sequences that are easily distinguishable both from time-shifted versions of themselves and from one another. Thus, it is useful to have sets of sequences that have both good auto-correlation properties and good cross-correlation properties.

1.4 Weighing Matrices of Odd Order

In this section, we obtain some necessary conditions for the existence of weighing matrices of odd order. As far as I know, all of these results are folklore. The proofs are the ones given in [GS79].

A complex matrix A is *unitary* if $AA^* = I$. I will refer to a complex matrix as *w-unitary* if $AA^* = wI$, where w is a real number. *Orthogonal* and *w-orthogonal* matrices are unitary and w-unitary matrices with all real entries, respectively. Observe that weighing matrices are w-orthogonal matrices with the restriction that all of their entries are either 0 or ± 1.

Theorem 1.4.1. *[GS79] Let W be a w-unitary matrix of order n and weight w, where w is an integer and n is odd. Further, assume that $\det(W) \in \mathbb{Z}$. Then w is an integer square.*

Proof. By Lemma 1.1.3, $\det(W)^2 = w^n$. So, there exists an integer ℓ such that $w^n = \ell^2$. By the Fundamental Theorem of Arithmetic, there exist factorizations of w and ℓ into prime powers $p_1^{\alpha_1}$, ..., $p_k^{\alpha_k}$ and $p_1^{\beta_1}$, ..., $p_t^{\beta_t}$, respectively, such that $p_1^{n\alpha_1} \cdots p_k^{n\alpha_k} = p_1^{2\beta_1} \cdots p_t^{2\beta_t}$ and, since factorization into primes is unique, $p_i^{n\alpha_i} = p_i^{2\beta_i}$. Consequently, for each i, $n\alpha_i = 2\beta_i$. But n is odd, so, for each i, α_i is even and there exists c_i such that $\alpha_i = 2c_i$. Hence, w is a square. □

In particular, Theorem 1.4.1 implies that odd order weighing matrices must have square weight. Let W be a weighing matrix of order n and weight w. Then the $(0,1)$-*complement* of W is the $n \times n$ matrix $B = [b_{ij}]$ such that $b_{ij} = 1$ if $w_{ij} = 0$ and $b_{ij} = 0$ otherwise. Note that, since there are w nonzero entries in each row of W, there are $n - w$ nonzero entries in each row of B.

The next result provides an upper bound on the weight of an odd order weighing matrix. This is an important result; the best weighing designs are obtained by using large weight weighing matrices (see Section 1.2). Further, large weight circulant weighing matrices are preferable to small weight circulant weighing matrices for applications concerning radar and sonar (Section 1.3). Some of the most sought after open problems in the theory of circulant weighing matrices concern proving or disproving the existence of large weight $CW(n,w)$'s in the case that n is even.

Theorem 1.4.2. *[GS70] Let W be a weighing matrix of order n and weight $w = k^2$, where n is odd and $w > 1$. Let B be the $(0,1)$-complement of W. Then $n \geq k^2+k+1$, and equality holds if and only if $BB^T = (n-w)I + (J_n - I)$, (where J_n denotes the $n \times n$ matrix of all 1's).*

Proof. Let $\mathbf{r}_i$ and $\mathbf{r}_t$ be two distinct rows of W. For ease of exposition, I have arranged the entries of these rows in a certain pattern; the proof in no way depends upon the entries assuming this pattern.

$\mathbf{r}_i$:	$1\cdots1-\cdots-$	$1\cdots1-\cdots-$	$1\cdots1-\cdots-$	$0\cdots00\cdots0$	$0\cdots0$
$\mathbf{r}_t$:	$1\cdots1-\cdots-$	$-\cdots-1\cdots1$	$0\cdots00\cdots0$	$1\cdots1-\cdots-$	$0\cdots0$
# cols:	a	b	c	d	e

Since $\mathbf{r}_i \cdot \mathbf{r}_t = 0$,

$$a - b = 0,$$

so that

$$c + d + e = n - 2a.$$

But, since there are k non-zero entries in both rows,

$$c = d.$$

Consequently,

$$e = n - 2a - 2c.$$

And, since n is odd, e is an odd number. So the diagonal entries of BB^T are $n - w$ and the off diagonal entries are positive odd numbers.

W^T is a weighing matrix of weight w, so each column of B contains $n - w$ ones. Further, each column of B^T contains $n - w$ ones. Let $\mathbf{e}$ be the n-tuple of all ones. Then

$$(n-w)^2\mathbf{e} = (n-w)\mathbf{e}B^T = (\mathbf{e}B)B^T = \mathbf{e}(BB^T) = ((n-w)+s_1, ..., (n-w)+s_n),$$

where each s_i is a sum of $n-1$ positive odd numbers. Thus,

$$(n-w)^2 \geq (n-w)+(n-1),$$

or, equivalently,

$$n^2 - 2n(w+1) + (w^2+w+1) \geq 0,$$

and equality holds if and only if each of the off diagonal entries of BB^T is equal to 1.

Let

$$f(x) = x^2 - 2(w+1)x + w^2 + w + 1.$$

Then, by the Quadratic Formula, the roots of f are $w+1 \pm \sqrt{w}$. Since

$$n^2 - 2(w+1) + (w^2+w+1) \geq 0,$$

we must have that either

$$n \geq w+1+\sqrt{w}$$

or

$$n \leq w+1-\sqrt{w}.$$

Further, since $w > 1$,

$$w+1-\sqrt{w} < w.$$

Therefore,

$$n \leq w+1-\sqrt{w}$$

is absurd. So

$$n \geq w + 1 + \sqrt{w} = k^2 + k + 1.$$

□

The case of equality in Theorem 1.4.2 can be studied using mathematical structures called projective planes. A is a structure composed of objects called "points" and objects called "lines" and a relation called "incidence" (geometries are sometimes referred to as "hypergraphs" in the combinatorial literature). A *projective plane* P is a geometry that satisfies the following axioms:

(i) any two points are incident with exactly one line,

(ii) any two lines intersect one another in a unique point (i.e. they are incident with exactly one of the same points),

(iii) each line is incident with at least three points, and

(iv) there exist at least two lines.

It can be shown [BR98] that axioms (iii) and (iv) are equivalent to

$(iii)'$ there exist four points, no three of which are collinear (such points are said to form a *quadrangle*, or *frame*).

Projective planes are members of a more general class of structures called projective geometries, which will be introduced in the next chapter.

Finite projective planes are projective planes with a finite point sets. For any finite projective plane P, it can be shown (see [BR98]) that there exists a number k such that each line is incident with $k+1$ points and each point is incident with $k+1$ lines and such that P contains k^2+k+1 points and k^2+k+1 lines. The number k is called the *order* of P.

The smallest projective plane has order 2; it is called the Fano plane (after the

geometer Gino Fano). In the diagram below, the dots represent points of the plane and each arc containing 3 dots represents a line of the plane.

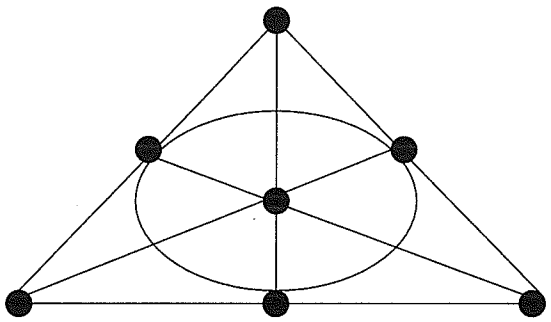

Figure 1.1: The Fano Plane

It is well known that, for each prime power p^e, there exists a projective plane of order p^e (a justification is provided in Chapter 2). There are no known examples of projective planes of composite order; it is generally believed that there are none. The question of whether or not this is the case is one of the most famous unsolved problems in combinatorics. The major theoretical result in this direction is the Bruck-Ryser Theorem (see [Bau71] for a proof).

Theorem 1.4.3. *If $k \equiv 1 \pmod 4$ or $k \equiv 2 \pmod 4$ and a projective plane of order k exists, then k must be a sum of two (integral) squares.*

It follows, for instance, that there exists no projective plane of order 6, since 6 is not a sum of two (integral) squares. Lam [Lam91] has verified, using a massive computer search, that there exists no finite projective plane of order 10. The smallest open case is for order 12.

Let P be a finite projective plane of order k. Enumerate the points and lines of P.

Then the *incidence matrix* of P (relative to the enumeration) is the $(k^2+k+1) \times (k^2+k+1)$ matrix $B = [b_{ij}]$ such that $b_{ij} = 1$ if point i is on line j and $b_{ij} = 0$ otherwise. For example, an incidence matrix of the Fano Plane is

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

Since each point is incident with $k+1$ lines, there are $k+1$ ones in each row of B. Further, since every pair of points is incident with exactly one line, for every i_1, i_2 there is exactly one number j such that $b_{i_1 j} = 1 = b_{i_2 j}$. So $BB^T = kI + J_n$. Likewise, since every pair of lines intersect in exactly one point, $B^T B = kI + J_n$.

A *balanced incomplete* (v, b, k, r, λ) *block design* (see [Jr.98]) is a set S of v objects together with b "blocks" (subsets of S) such that each block contains k objects, each object is contained in r different blocks, and every pair of distinct objects occurs together in λ blocks. Finite projective planes are examples of block designs; in the next chapter we will encounter another class of examples: difference sets. In general, the incidence matrix B of a balanced incomplete block design satisfies the equation $BB^T = (k-\lambda)I + \lambda J_v$.

A geometry G is *r-uniform* (for $r \in \mathbb{N}$) if each line of G is incident with exactly r points (I have lifted this concept from the hypergraph literature).

Lemma 1.4.4. *Let $n > r \geq 3$ and let H be an r-uniform geometry with a point set of size n. If H satisfies the first two finite projective plane axioms, then H is a finite projective plane.*

Proof. Let L_1 be a line of H. Since $n > r$ and since every point is contained in at least one line (this follows from axiom (i)), there is another line, L_2, of H. Since L_1 intersects L_2 in exactly one point (axiom (ii)), there are two points that lie on L_1 that do not lie on L_2 and there are two points that lie on L_2 that do not lie on L_1. Let Q be the set of these four points. Suppose that there is a line L that contains more than three points of Q. Then either two points of L_1 lie on L or two points of L_2 lie on L. Either way, there are two distinct points that are connected by two distinct lines. This contradicts axiom (i). Hence, Q is a quadrangle. □

Corollary 1.4.5. *Let $k \geq 2$. Then there exists a projective plane of order k if and only if there exists a $n \times n$ $(n = k^2+k+1)$ $(0,1)$-matrix A such that $AA^T = kI + J_n$ and $A^TA = kI + J_n$.*

Proof. If there exists a projective plane of order k, then A can be chosen as its incidence matrix.

So suppose that there exists a matrix $A = [a_{ij}]$ such that $AA^T = kI + J_n$ and $A^TA = kI + J_n$. Define a geometry H with k^2+k+1 lines and k^2+k+1 points by the condition that a point x_i lies on a line L_j iff $a_{ij} = 1$. Since the dot product of any two rows of A is equal to one, for every pair of points in H, there is exactly one line that connects them. Further, the dot product of any two rows of A^T is equal to one. Hence, for every two lines in the geometry, there exists exactly one point that lies on both.

Since each column of A contains exacly $k+1$ ones, each line of H contains $k+1$

points. But, since $k \geq 2$, $k+1 \geq 3$. Further, there are $k^2+k+1 > k+1$ points in H. Thus, by Lemma 1.4.4, H is a finite projective plane of order k. □

Finite projective geometries, it turns out, are very useful for constructing other types of combinatorial objects. In the next chapter, I will demonstrate how they can be used to build circulant weighing matrices. The following theorem, which investigates the extremal case in Theorem 1.4.2, goes the other way; it shows that the existence of a weighing matrix with certain parameters implies the existence of a finite projective plane.

Theorem 1.4.6. *[GS79] Let $k \geq 2$. Then the existence of a $W(k^2+k+1, k^2)$ implies the existence of a finite projective plane of order k.*

Proof. Let W be a $W(k^2+k+1, k^2)$. Let $B = [b_ij]$ be the $(0,1)$-complement of W. Then, by Theorem 1.4.2,

$$BB^T = kI + J.$$

Since W^T is also a $W(k^2+k+1, k^2)$ and since B^T is the $(0,1)$-complement of W^T, Theorem 1.4.2 also implies that

$$B^TB = kI + J.$$

So, by Corollary 1.4.5, B is the incidence matrix of finite projective plane of order k. □

By the Bruck-Ryser Theorem (Theorem 1.4.3), there is no projective plane of order 6; it follows that there exists no $W(43, 36)$.

Corollary 1.4.7. *Let $k \geq 2$ be such that either $k \equiv 1 \pmod 4$ or $k \equiv 2 \pmod 4$. If there exists a $W(k^2+k+1, k^2)$, then k must be the sum of two integral squares.*

1.5 Group Developed Weighing Matrices

Let $g_1, g_2, ..., g_n$ be the elements of a finite group $\mathbf{G}$. The division table for $\mathbf{G}$ is the array with $g_i g_j^{-1}$ in entry i, j. For instance, let $\mathbf{H} = \langle h \rangle$ be the cyclic group of order 4. Then the division table of $\mathbf{H}$ is given by the following array.

	1	h	h^2	h^3
1	1	h^3	h^2	h
h	h	1	h^3	h^2
h^2	h^2	h	1	h^3
h^3	h^3	h^2	h	1

By the cancellation property, each element of $\mathbf{G}$ appears exactly once in every row and every column of the division table. For $g_k \in \mathbf{G}$, let $P_k = [p_{ij}]$ be the permutation matrix (a $0,1$ matrix with exactly one 1 in every row and every column) such that $p_{ij} = 1$ if $g_i g_j^{-1} = g_k$ and $p_{ij} = 0$ otherwise. For instance, relative to the cyclic group $\mathbf{H}$, the matrices P_1, P_2, P_3, and P_4 are

$$P_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} P_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} P_3 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} P_4 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Let $\varphi : \mathbf{G} \to \mathbf{M}_{n\times n}(\mathbb{C})$ be defined by the rule $\varphi(g_k) = P_k$. Let $\delta : \{0,1,...,n-1\}^3 \to \{0,1\}$ be the map defined by the rule that $\delta_{i,j}^t = 1$ if $g_i g_j^{-1} = g_t$ and $\delta_{i,j}^t = 0$ otherwise. Let $g_k, g_t \in \mathbf{G}$ be such that $g_k g_t = g_u$. Then $\varphi(g_k)\varphi(g_t) = P_k P_t = \left[\delta_{i,j}^k\right]_{i,j}\left[\delta_{r,s}^t\right]_{r,s} = \left[\sum_{\ell=0}^{n-1}\delta_{i,\ell}^k\delta_{\ell,s}^t\right]_{i,s} = \left[\delta_{i,s}^u\right]_{i,s} = P_u = \varphi(g_u) = \varphi(g_k g_t)$. So, φ is a homomorphism. For any $n \in \mathbb{N}$, a homomorphism from a group $\mathbf{G}$ to a subgroup of $GL(n,\mathbf{C})$ is called a *representation of order* n of the group $\mathbf{G}$. The map φ is known as the *Cayley representation* of $\mathbf{G}$.

We say that a $n\times n$ matrix M is *group developed* over the group $\mathbf{G}$ (or alternatively, $\mathbf{G}$-*developed*) if

$$M = a_1P_1 + \cdots + a_nP_n,$$

where the matrices P_i are the permutation matrices corresponding to the Cayley representation of $\mathbf{G}$. Consider the $n \times n$ matrix $X = circ(0,1,0,...,0)$. X is called the *right shift matrix* since, for any $m\times n$ matrix A, multiplying A on the right by X shifts the entries of A one position to the right. X is the image of x under the Cayley representation of the cyclic group $\langle x\rangle$ of order n. Note that $X^2 = circ(0,0,1,0,...,0)$, $X^3 = circ(0,0,0,1,0,...,0)$, ..., $X^{n-1} = circ(0,0,...,1)$, and $X^n = I_n$. Thus, each circulant matrix can be written as a polynomial in terms of the right shift matrix as follows: $circ(a_0,a_1,...,a_{n-1}) = a_0I_n + a_1X + a_2X^2 + ... + a_{n-1}X^{n-1}$. Circulant matrices are matrices developed over cyclic groups.

The *group ring* is the ring of all formal polynomials in $\mathbf{G}$ with coefficients from $\mathbb{Z}$ (wherein the identity of the group is identified with 1). The following conventions will be used frequently in this text. For $S = \sum a_k g_k \in \mathbb{Z}\mathbf{G}$ and $t \in \mathbb{Z}$, we introduce the notation $S^{(t)} = \sum a_k g_k^t$. More generally, if σ is some map from $\mathbf{G}$ to itself, we stipulate that $(\sum a_i g_i)^\sigma = \sum a_i\sigma(g_i)$. Further, for $T \subset \mathbf{G}$, in the context of $\mathbb{Z}\mathbf{G}$, T

denotes $\sum_{x \in T} x$.

For any group $\mathbf{G}$, the Cayley representation extends to an isomorphism from the group ring $\mathbb{Z}\mathbf{G}$ to the ring of all $\mathbf{G}$-developed matrices with entries in $\mathbb{Z}$. If C is a group developed matrix with integer entries, then I call $\varphi^{-1}(C)$ the *group ring polynomial* of C. For instance, let $\langle g \rangle$ be the cyclic group of order 6. Then the group ring polynomial of the $CW(6,4)$ from page 2 is $-1+g+g^3+g^4$.

Alternatively, let θ be the homomorphism from the ring of all circulant matrices with integer entries to the ring $\mathbb{Z}[x]/\langle x^n-1\rangle$ defined by the rule $\theta(X)=x$ (where X denotes the right shift matrix). θ is also an isomorphism and, if C is a circulant matrix with integer entries, $\theta(C)$ is called the *Hall polynomial* of C (after Marshall Hall).

Let W be a $n \times n$ $\mathbf{G}$-developed matrix such that $W = \sum a_i P_i$. $WW^T = wI$ iff $\varphi^{-1}\left(WW^T\right) = w\varphi^{-1}(I) = w$.

Let P be a permutation matrix. The $(i,j)-$th entry p_{ij}^* of PP^T is equal to the dot product of the i^{th} row of P with the j^{th} row of P. Thus, since P contains exactly one 1 in every row and every column, $PP^T = I$. Therefore,

$$\varphi^{-1}\left(WW^T\right) = \varphi^{-1}\left(\left(\sum a_i P_i\right)\left(\sum a_i P_i\right)^T\right) = \varphi^{-1}\left(\left(\sum a_i P_i\right)\left(\sum a_i P_i^{-1}\right)\right)$$

$$= \left(\sum a_i g_i\right)\left(\sum a_i g_i^{-1}\right) = \varphi^{-1}(W)\left(\varphi^{-1}(W)\right)^{(-1)}.$$

Thus, we have proven the following (folklore) lemma, which turns out to be crucial.

Lemma 1.5.1. *A $\mathbf{G}$-developed $(0,\pm 1)$ matrix W is a weighing matrix of weight w if and only if $\varphi^{-1}(W)\left(\varphi^{-1}(W)\right)^{(-1)} = w$.*

As an initial application of Lemma 1.5.1, we prove the following result, which

shows how circulant weighing matrices can be combined and altered in various ways to create larger circulant weighing matrices. The first two parts of the next result are folklore. The third part was first presented in a survey on circulant weighing matrices [AD96] (it can also be obtained by a well known technique for constructing weighing matrices known as the "orthogonal pairs method").

Lemma 1.5.2. *Suppose that there exists a $CW(n_1, w_1)$ and a $CW(n_2, w_2)$.*
(i) For each natural number t, there exists a $CW(tn_1, w_1)$.
(ii) There exists a $W(n_1n_2, w_1w_2)$ developed over the abelian group obtained by taking the direct product of the cyclic groups of orders n_1 and n_2. If $(n_1, n_2) = 1$, then this weighing matrix is circulant.
(iii) Let m and n_2 be odd and let $m > 1$. Then there exists a $CW(2mn_2, 4w_2)$.

Proof. (i) Let W_1 be a $CW(n_1, w_1)$ with group ring polynomial $\theta(x)$ over the cyclic group $\langle x \rangle$ of order n_1. Let $\langle y \rangle$ be the cyclic group of order tn_1, for some t. Then, since $\langle y^t \rangle$ is the subgroup of $\langle y \rangle$ of order n_1, $\theta(y^t)$ is the group ring polynomial for a $CW(tn_1, w_1)$.

(ii) Let $\langle x \rangle$ be the cyclic group of order n_1 and let $\langle y \rangle$ be the cyclic group of order n_2. Let $\theta_1(x)$ be the group ring polynomial of a $CW(n_1, w_1)$ and let $\theta_2(y)$ be the group ring polynomial of a $CW(n_2, w_2)$. Then $\theta_1(x)\theta_2(y)$ is a $0, \pm 1$ polynomial in the ring $\mathbb{Z}[\langle x \rangle \bigotimes \langle y \rangle]$. Further, for any $r, s \in \mathbb{N}$, $(x^r y^s)^{-1} = x^{-r}y^{-s}$. So, since $\langle x \rangle \bigotimes \langle y \rangle$ is abelian, $\theta_1(x)\theta_2(y)\,(\theta_1(x)\theta_2(y))^{(-1)} = \theta_1(x)\theta_2(y)\theta_1(x^{-1})\theta_2(y^{-1}) = \theta_1(x)\theta_1(x^{-1})\theta_2(y)\theta_2(y^{-1}) = w_1w_2$. Thus, $\theta_1(x)\theta_2(y)$ is the group ring polynomial of a $W(n_1n_2, w_1w_2)$ developed over $\langle x \rangle \bigotimes \langle y \rangle$. If $(n_1, n_2) = 1$, then $\langle x \rangle \bigotimes \langle y \rangle$ is cyclic with generator xy. Therefore (in this case), $\theta_1(x)\theta_2(y)$ is the group ring polynomial of a $CW(n_1n_2, w_1w_2)$.

(*iii*) Let $\langle x \rangle$ be the cyclic group of order $2mn_2$. By part (i), there exists a $CW(2mn_2, w_2)$ with group ring polynomial $\theta_1(x^{2m})$, obtained from a $CW(n_2, w_2)$ by the method from (*i*). $\frac{1-x^{mn_2}}{2}$ and $\frac{1+x^{mn_2}}{2}$ are orthogonal idempotents, i.e.

$$\frac{1-x^{mn_2}}{2}\frac{1-x^{mn_2}}{2} \equiv \frac{1-x^{mn_2}}{2} \pmod{x^{2mn_2}-1},$$

$$\frac{1+x^{mn_2}}{2}\frac{1+x^{mn_2}}{2} \equiv \frac{1+x^{mn_2}}{2} \pmod{x^{2mn_2}-1},$$

and

$$\frac{1-x^{mn_2}}{2}\frac{1+x^{mn_2}}{2} \equiv 0 \pmod{x^{2mn_2}-1}.$$

By exploiting this fact, we can construct a $CW(2mn_2, 4w_2)$.

Let $\theta_3(x) = (1-x^{mn_2})\theta_1(x^{2m}) + x(1+x^{mn_2})\theta_1(x^{2m})$. Each power of x in the polynomial $\theta_1(x^{2m})$ is congruent to 0 (mod $2m$). Since m and n_2 are odd, the powers of x in $x^{mn_2}\theta_1(x^{2m})$ are congruent to m (mod $2m$). The powers of x in $x\theta_1(x^{2m})$ and $xx^{mn_2}\theta_1(x^{2m})$ are congruent to 1 and $m+1$ (mod $2m$), respectively. Thus $\theta_3(x)$ is a $0, \pm 1$ polynomial. Further,

$$\theta_3(x)\theta_3(x^{-1}) = 2(1-x^{mn_2})w_2 + 2(1+x^{mn_2})w_2 = 4w_2.$$

So, θ_3 is the group ring polynomial of a $CW(2mn_2, 4w_2)$. □

For example, $-1+x+x^2+x^4$ is the group ring polynomial of a $CW(7,4)$, developed over the cyclic group $\langle x \rangle$ of order 7. $-y+y^2-y^3+y^5+y^6+y^7+y^8-y^9+y^{11}$ is the group ring polynomial of a $CW(13,9)$, developed over the cyclic group $\langle y \rangle$ of order 13 (in the next chapter I will demonstrate how these circulant weighing matrices can be generated).

From the proof of part (i), $-1+z^2+z^4+z^8$ is the group ring polynomial of a $CW(14,4)$ over the cyclic group $\langle z\rangle$ of order 14.

Let $t=xy$. Then, since $(7,13)=1$, t is a generator of $\langle x\rangle\times\langle y\rangle$. And, by the proof of part (ii),

$$(-1+x+x^2+x^4)(-y+y^2-y^3+y^5+y^6+y^7+y^8-y^9+y^{11})$$

$$=y-y^2+y^3-y^5-y^6-y^7-y^8+y^9-y^{11}-xy+xy^2-xy^3+xy^5+xy^6+xy^7+xy^8-xy^9+xy^{11}-x^2y$$

$$+x^2y^2-x^2y^3+x^2y^5+x^2y^6+x^2y^7+x^2y^8-x^2y^9+x^2y^{11}-x^4y+x^4y^2-x^4y^3+x^4y^5+x^4y^6+x^4y^7$$

$$+x^4y^8-x^4y^9+x^4y^{11}$$

$$\equiv t^{14}-t^{28}+t^{42}-t^{70}-t^{84}-t^7-t^{21}+t^{35}-t^{63}-t+t^{15}-t^{29}+t^{57}+t^{71}+t^{85}+t^8-t^{22}+t^{50}-t^{79}+t^2-t^{16}$$

$$+t^{44}+t^{58}+t^{72}+t^{86}-t^9+t^{37}-t^{53}+t^{67}-t^{81}+t^{18}+t^{32}+t^{46}+t^{60}-t^{74}+t^{11}$$

is the group ring polynomial of a $CW(91,36)$.

Let $\langle s\rangle$ be the cyclic group of order 98. By part (i), $-1+s^{14}+s^{28}+s^{56}$ is the Hall polynomial of a $CW(98,4)$. Thus, by part (iii),

$$(1-s^{49})(-1+s^{14}+s^{28}+s^{56})+s(1+s^{49})(-1+s^{14}+s^{28}+s^{56})$$

$$=-1+s^{14}+s^{28}+s^{56}+s^{49}-s^{63}-s^{77}-s^7-s+s^{15}+s^{29}+s^{57}-s^{50}+s^{64}+s^{78}+s^8$$

is the Hall polynomial of a $CW(98,16)$.

1.6 Row sums

We can deduce a powerful necessary condition for the existence of group developed weighing matrices by examining a simple property of their row sums. A matrix A is *k-row-regular* if the sum of the entries in every row is equal to k. Column regular matrices are defined similarly. If a square matrix is k-row-regular and c-column-regular, then the sum of the entries in the matrix is equal to both nk and nc; it follows that $k = c$. In this case, we refer to the matrix as *k-regular.*

J. Kappor [Kap75] proved that an orthogonal matrix can be written as a sum $\sum a_i P_i$, where the P_i's are disjoint permutation matrices, only if $\sum a_i = \pm 1$. Mullin [Mul75] proved that there exists a k-regular (and, in particular, a group developed) $W(n, w)$ only if $w = k^2$. I noticed that the technique from Mullin's proof can be adapted to prove a more general result that implies both Mullin and Kapoor's results as a consequence.

Theorem 1.6.1. *If there exists a $n \times n$ w-unitary k-regular matrix W, then $w = k\overline{k}$.*

Proof. Let $\mathbf{e}$ be the $1 \times n$ column matrix of all 1's. $WW^*\mathbf{e} = \overline{k}W\mathbf{e} = \overline{k}k\mathbf{e}$ and $WW^*\mathbf{e} = wI\mathbf{e} = w\mathbf{e}$. Thus, $w = \overline{k}k$. □

If W can be written as a sum $W = \sum a_i P_i$ of multiples of disjoint permutation matrices, then W is k-regular, where $k = \sum a_i$. Thus, we have the following generalization of Kapoor's result as a corollary.

Corollary 1.6.2. *If a w-unitary matrix W can be written as a sum $\sum a_i P_i$ of disjoint permutation matrices, then $\sum a_i$ lies on the circle of radius $\sqrt{w}$ in the complex plane.*

If $W = \sum a_i P_i$ is a unitary matrix, $\sum a_i$ lies on the unit circle and, if W is orthogonal, $\sum a_i = \pm 1$. Note that a group developed weighing matrix W can be written as a sum $W = \sum a_i P_i$ of disjoint permutation matrices and is therefore k-regular, where $k = \sum a_i$, and the a_i's are all either 0 or ± 1.

Corollary 1.6.3. *[Mul75] If W is a k-regular weighing matrix (for example, a group developed weighing matrix) of weight w, then $w = k^2$.*

Let W be a k-regular weighing matrix. Let a be the number of ones in each row of W and let b be the number of negative ones in each row of W. Then $a + b = k^2$ and $a - b = k$. The next result follows upon solving this linear system.

Corollary 1.6.4. *[Mul75] If W is a k-regular weighing matrix, then it has $\frac{k^2+k}{2}$ ones and $\frac{k^2-k}{2}$ negative ones in each of its rows.*

1.7 Negacyclic Weighing Matrices

A *negacyclic matrix* is a matrices that is a polynomial in the matrix Y given below:

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

Negacyclic matrices are a close relative of circulant matrices. Roughly speaking, negacyclic matrices are like circulant matrices except that their entries become

negated when they "wrap around" from one side of the matrix to the other. We will refer to a $n \times n$ negacyclic weighing matrix of weight w as a $NW(n, w)$. If Y is $n \times n$, then $Y^n = -I$. It follows that $\sigma : \sum a_i Y^i \to \sum a_i y^i$ is an isomorphism from the ring of integer valued negacyclic matrices to the quotient ring $\mathbb{Z}[y]/\langle y^n + 1\rangle$. The image of a negacyclic matrix under σ will be referred to as its *nega-Hall polynomial.* The following (folklore) result is a negacyclic analogue of Lemma 1.5.1.

Lemma 1.7.1. *A $n \times n$ negacyclic $(0, \pm 1)$-matrix W is a weighing matrix of weight w if and only if its nega-Hall polynomial $\sigma(W)$ satisfies the equation*

$$\sigma(W)\sigma(W)^{(-1)} \equiv w \pmod{\langle y^n + 1\rangle}.$$

Notice that, although the set of powers of Y is a representation of the cyclic group of order $2n$, the negacyclic matrices are not group developed in the sense defined above. Further, negacyclic matrices are not regular. So, for instance, Corollary 1.6.3 does not apply to them.

Let $\theta(y)$ be the nega-Hall polynomial of a negacyclic weighing matrix W_1. Replacement of the variable y with the variable $-y$ is a bijection ϕ from the ring $\mathbb{Z}[y]/\langle y^n+1\rangle$ to the ring $\mathbb{Z}[-y]/\langle(-y)^n - 1\rangle$. If n is odd, then $\mathbb{Z}[-y]/\langle(-y)^n + 1\rangle$ is isomorphic to $\mathbb{Z}[x]/\langle x^n - 1\rangle$. Thus, the image of $\phi(\theta(y))$ in $\mathbb{Z}[x]/\langle x^n - 1\rangle$ is the Hall polynomial of a circulant matrix. On the other hand, if n is even, then $\mathbb{Z}[-y]/\langle(-y)^n + 1\rangle$ is isomorphic to $\mathbb{Z}[y]/\langle y^n+1\rangle$, so, in this case, the image of $\phi(\theta(y))$ in $\mathbb{Z}[y]/\langle y^n+1\rangle$ is the nega-Hall polynomial of another negacyclic matrix. In either case, the matrix W_2 corresponding to the image of $\phi(\theta(y))$ is obtained by multiplying every second row and every second column of W by -1. The orthogonality of the rows of a weighing

matrix is invariant under multiplication of the rows or columns of the matrix by -1. Thus, W_2 is also a weighing matrix.

Reversing this procedure shows that odd order circulant weighing matrices can be transformed into negacyclic weighing matrices. The following theorem is folklore.

Theorem 1.7.2. *If n is odd, then there exists a $NW(n,w)$ if and only if there exists a $CW(n,w)$.*

Consider the following $CW(7,4)$.

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

By negating every second row and every second column of this matrix, we obtain a $NW(7,4)$.

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

We now generalize the concept of negacyclic matrices; the concepts presented in this section to are similar to, and based upon, some ideas of Craigen [Cra95a]. A *signed group of order n* is a group of order $2n$ with a distinguished central element, denoted -1, of order 2. For instance, the group $\mathbf{Q}$ of Quaternions, with presentation

$$\mathbf{Q} = \langle i, j : i^2 = j^2 = -1; ij = -ji \rangle$$

is a signed group of order 4.

It follows as a corollary to the Fundamental Theorem of Abelian Groups (see [Gal04]) that, if $\mathbf{G}$ is an abelian group and t divides the order of $\mathbf{G}$, then $\mathbf{G}$ has a subgroup of order t. Since the only group of order 2 is the cyclic group of order 2, it follows that all abelian groups of even order contain an element of order 2. Therefore, all abelian groups of even order are signed groups.

Signed groups are useful for constructing weighing matrices; in particular, they are useful for constructing Hadamard matrices [Cra95a].

A *signed permutation matrix* is a matrix with entries all either 0 or ± 1 and with exactly one non-zero entry in each row and column. Let $\mathbf{G}$ be a signed group of order n. Then a *remrep* (real monomial representation) is a representation of $\mathbf{G}$ whose image is a subgroup of $\mathbf{SP}_n$ (the group of signed permutation matrices of order n,; cf. Lemma 1.5.1 and Lemma 1.7.1) and which maps -1 to $-I$. Let

$$\{I, P_1, ..., P_{n-1}, -I, -P_1, ..., -P_{n-1}\}$$

be the image of $\mathbf{G}$ under a remrep. If $W = a_0 I + a_1 P_1 + \cdots + a_{n-1} P_{n-1}$ is a $W(n, w)$, then we refer to W as a $SW(n, w; \mathbb{R})$ (in Craigen's definition of signed

group weighing matrices, the entries of the matrix come from the signed group; the notation $\mathbb{R}$ serves to distinguish the two different kinds of signed group weighing matrices).

1.8 Equivalence

Notice that if $\theta_1(g)$ is the group ring polynomial for a $W(n,w)$ developed over the group $\mathbf{G}$, then, for each $h \in \mathbf{G}$, $\theta_2(g) = h\theta_1(g)$ is the group ring polynomial of another $\mathbf{G}$-developed $W(n,w)$. Likewise, for any automorphism σ of $\mathbf{G}$, $\theta_1(g)^\sigma \left(\theta_1(g)^\sigma\right)^{(-1)} = \left(\theta_1(g)\theta_1(g)^{(-1)}\right)^\sigma = w^\sigma = w$, so that $\theta_1(g)^\sigma$ is also the group ring polynomial of a $\mathbf{G}$-developed $W(n,w)$.

For example, $\theta(x) = -1 + x + x^2 + x^3$ is the group ring polynomial, defined over the cyclic group $\langle x \rangle$ of order 4, of a circulant Hadamard matrix. The map $\sigma : \langle x \rangle \to \langle x \rangle$ defined by the rule $\sigma(x) = x^3$ is an automorphism of $\langle x \rangle$. So the polynomial $x^2\theta(x^3) = 1 + x - x^2 + x^3$ defines another circulant Hadamard matrix.

If W is a $CW(2n,w)$ with group ring polynomial $\theta(x)$, then $\theta(-x)$ is the group ring polynomial of another $CW(2n,w)$. Further, for any $CW(n,w)$ W, $-W$ is also a $CW(n,w)$. So, for example, since $\theta(g) = -1 + g + g^3 + g^4$ is the group ring polynomial, over the group $\langle g \rangle$, of the $CW(6,4)$ from page 2, $-\theta(-g) = 1 + g + g^3 - g^4$ is the group ring polynomial of another $CW(6,4)$.

Let W_1 and W_2 be two $\mathbf{G}$-developed $W(n,w)$'s with group ring polynomials $\theta_1(g)$ and $\theta_2(g)$, respectively. Then W_1 and W_2 are *equivalent as* $\mathbf{G}$*-developed weighing matrices* if and only if

$$\theta_2(g) = \epsilon h \theta_1(\delta g)^\sigma,$$

where σ is some automorphism of $\mathbf{G}$, $h \in \mathbf{G}$, and $\epsilon, \delta \in \{-1, 1\}$.

As a matter of convention, if W is a circulant weighing matrix with negative row sum, we choose to speak instead about the equivalent circulant weighing matrix $-W$. In the next chapter I will demonstrate the existence of multiple inequivalent circulant weighing matrices for some parameter pairs.

Theorem 1.8.1. *Let W_1 and W_2 be $\mathbf{G}$-developed weighing matrices that are equivalent as $\mathbf{G}$-developed weighing matrices. Then they are also equivalent as weighing matrices.*

Proof. Let $\theta_1(g) = \sum a_k g_k$ and $\theta_2(g)$ be the group ring polynomials of W_1 and W_2, respectively. Let $\theta_2(g) = \epsilon\theta_1\left(\delta g\right)^\sigma$. I will demonstrate how W_2 can be obtained from W_1 via row and column permutations and multiplications of rows and columns by -1.

Let $\mathbf{G} = \{1 = g_0, g_1, ..., g_{n-1}\}$. Index the rows and columns of W_1 as if it were the division table for $\mathbf{G}$, so that W_1 is the core (the array with the first row and column deleted) of the array

	1	g_1	$\cdots$	g_{n-1}
1	w_{00}	$w_{0,1}$	$\cdots$	$w_{0,n-1}$
g_1^{-1}	$w_{1,0}$	$w_{1,1}$	$\cdots$	$w_{1,n-1}$
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
g_{n-1}^{-1}	$w_{n-1,0}$	$w_{n-1,1}$	$\cdots$	$w_{n-1,n-1}$

Then $w_{ij} = a_k$ if and only if $g_i^{-1}g_j = g_k$. Permute the columns of W_1 so that, for

each j, the column indexed by g_j is sent to the column indexed by g_j^σ. Permute the rows of W_1 so that, for each i, the row indexed by g_i^{-1} is sent to the row indexed by $\left(g_i^{-1}\right)^\sigma$. Call the matrix so obtained $W_4 = \left[w_{ij}^4\right]$. Then $w_{st}^4 = a_k$ if and only if $g_s^{-1}g_t = \left(g_i^\sigma\right)^{-1} g_j^\sigma = \left(g_i^{-1}g_j\right)^\sigma = g_k^\sigma$. So that W_4 is a $\mathbf{G}$-developed matrix with group ring polynomial $\sum a_k g_k^\sigma$.

Permute the columns of W_4 so that, for each j, the column indexed by g_j is sent to the column indexed by hg_j. Call the matrix so obtained $W_3 = \left[w_{ij}^3\right]$. Then $w_{ij}^3 = a_k$ if and only if $g_i^{-1}g_j = hg_k^\sigma$. So W_3 is a $\mathbf{G}$-developed matrix with group ring polynomial $\sum a_k h g_k^\sigma$.

Now multiply each row of W_3 by ϵ, and multiply every second row and column of W_4 by δ to obtain W_2, with group ring polynomial $\epsilon h\theta_1 \left(\delta g\right)^\sigma$. □

It is not known whether or not the converse of Theorem 1.8.1 is true. In other words, if W_1 and W_2 are $\mathbf{G}$-developed weighing matrices that are equivalent as weighing matrices, does it follow that they are equivalent as $\mathbf{G}$-developed weighing matrices?

1.9 Eigenvalues of Group Developed Matrices

Let $\mathbf{G} = \{1 = g_0, g_1, ..., g_{n-1}\}$ be a finite group of exponent v. Let φ be the Cayley representation for $\mathbf{G}$ and, for each i, let $\varphi\left(g_i\right) = P_i$. For each $i = 0, 1, ..., n-1$, there exists $s_i | v$ such that $g_i^{s_i} = 1$. Since representations are homomorphisms, for each i, $P_i^{s_i} = I$. For some i, let $\lambda_i \in \mathbb{C}$ be an eigenvalue of P_i with eigenvector $\mathbf{v}_i$. Then $\mathbf{v}_i = I\mathbf{v}_i = P_i^{s_i}\mathbf{v}_i = \lambda_i^{s_i}\mathbf{v}_i$. Therefore, λ_i is a s_i^{th} root of unity.

Let M be a $\mathbf{G}$-developed matrix, so that $M = \sum_{i=0}^{n-1} a_i P_i$. Then each eigenvalue of

M has the form $\sum_{i=0}^{n-1} a_i\zeta_i$, where, for each i, ζ_i is a s_i^{th} root of unity. It follows that each eigenvalue of M lies in the ring $\mathbb{Z}[\zeta_v]$.

The eigenvalues of group developed weighing matrices have a remarkable property (which is, as far as I know, folklore).

Theorem 1.9.1. *Let* $\mathbf{G}$ *be a finite group, let* $W = \sum_{i=0}^{n-1} a_iP_i$ *be a* $\mathbf{G}$*-developed* $W(n,w)$*, and let* $\lambda = \sum_{i=0}^{n-1} a_i\zeta_i$ *be an eigenvalue of* W*. Then* λ *lies on the circle (of the complex plane), centered at the origin, of radius* $\sqrt{w}$*.*

Proof. For each i, $P_i^T = P_i^{-1}$. Consequently, if ζ_i is an eigenvalue of P_i, then $\overline{\zeta_i} = \zeta_i^{-1}$ is an eigenvalue of P_i^T. It follows that $\overline{\lambda}$ is an eigenvalue of W^T, so that $\lambda\overline{\lambda}$ is an eigenvalue of $WW^T = wI$. Therefore, $\lambda\overline{\lambda} = w$. □

1.10 Large Weight Circulant Weighing Matrices

We have already freely used the term "large weight weighing matrix;" now we will make the meaning(s) of this term precise. There are two ways to define the term: under one definition, a weighing matrix W has large weight if W is a $W(n, n-a)$, where a is a "small" number; another way of defining this term is to stipulate that W has large weight if W is a $W(n,w)$, where $\frac{w}{n} \approx 1$. Under the second definition a weighing matrix W can have large weight, even if it contains a number of zeroes, so long as it is large enough that the ratio of the number of zeroes to the size of the matrix is negligible. In this section, we will present a few results about large weight circulant weighing matrices in the first sense of the term. In the next chapter, we will explain how to generate a class of $CW(n,w)$'s such that, as $n, w \to \infty$, $\frac{w}{n} \to 1$. Finally, Schmidt's bound on large weight circulant weighing matrices is discussed

at the end of chapter 3.

Circulant Hadamard matrices have already been mentioned (Section 1.1). The next case to consider is the case of the *circulant conference matrices*, the $CW(n, n-1)$'s. It turns out that there are none of these, other than the 2×2 identity matrix. This fact was first proved by Mullin and Stanton [MS76]. Later, Jungnickel [Jun90] proved the more general result that, for any abelian group $\mathbf{G}$, there exist no $\mathbf{G}$-developed conference matrices (other than the 2×2 identity). He also obtained restrictions on the existence of conference matrices developed over non-abelian groups. Craigen [Cra94] reproved Mullin and Stanton's result. Craigen's method is the simplest of the three. What's more, it can be extended to prove a more general result that, while different than Jungnickel's result, also implies the non-existence of conference matrices developed over abelian groups.

Craigen's method makes use of symmetry, eigenvalues, and the trace function. It was motivated by the following result, which was proven by D. Gregory [Cra94].

Theorem 1.10.1. *Let n be odd. Then there exists no symmetric $W(n, w)$ with a zero diagonal.*

Proof. Suppose W is a symmetric $W(n, w)$ that has a zero diagonal. Since $W^2 = wI$, the eigenvalues of W are $\lambda_i = \pm\sqrt{w}$, $i = 1, ..., n$. But $tr(W) = 0 = \sum_{i=1}^{n} \lambda_i = t\sqrt{w}$, for some t. Since n is odd, so is t. Therefore, $t \neq 0$, which is impossible. □

Note that, by Theorem 1.4.2, if there exists a conference matrix of order $n > 1$, then n is even. The following result (from [Cra94]), provides a crucial link between symmetric weighing matrices and group developed conference matrices (since group developed matrices are regular). A conference matrix is in *standard position* if each of its zeroes lies along the main diagonal.

Theorem 1.10.2. *([Cra04]) Every regular conference matrix in standard position is symmetric.*

Proof. Let W be a k-regular $W(n, k^2)$ (see Corollary 1.6.3) in standard position. Without loss of generality, the first two rows of W are

0	x	1	·	·	1	1	·	·	1	−	·	·	−	−	·	·	−
y	0	1	·	·	1	−	·	·	−	1	·	·	1	−	·	·	−
		a				b				c				d			

The next four equations follow by orthogonality and regularity

$$a+b+c+d=k^2-1,$$

$$x+a+b-c-d=k,$$

$$y+a-b+c-d=k,$$

$$a-b-c+d=0.$$

Adding these four equations together yields

$$x+y+4a=k^2+2k-1.$$

But k is odd, so that

$$x+y\equiv 1+2-1\equiv 2 \pmod 4.$$

It follows that $x=y$. By similarly arranging the i^{th} and j^{th} rows, one may deduce

that the (i,j) and (j,i) entries of W are equal, i.e. that W is symmetric. □

Now we are in a position to prove the main result of this section (which generalizes a result from [Cra94]).

Theorem 1.10.3. *There exist no conference matrices, other than the* 2×2 *identity, developed over a signed group (in the sense of the term "group developed" defined in Section 1.5).*

Proof. Let $\mathbf{G}$ be a signed group (of order $n > 2$), and let W be a $\mathbf{G}$-developed conference matrix in standard position. By Theorem 1.10.2, W is symmetric.
Let φ be the Cayley representation of $\mathbf{G}$. Let $\varphi(-1) = P$. Then, since $(-1)(-1) = 1$, $P^2 = I$, *i.e.*, $P = P^{-1} = P^T$. If A_1 and A_2 are symmetric matrices that commute, then $A_1A_2 = A_2A_1 = A_2^TA_1^T = (A_1A_2)^T$, so that A_1A_2 is also symmetric. Since -1 is, by definition, in the centre of $\mathbf{G}$, W and P commute. Therefore, WP is a symmetric $\mathbf{G}$-developed conference matrix (note that $PP^T = I$) with either all 1's or all -1's along the main diagonal.
Assume, without loss of generality, that WP has all 1's along the main diagonal. Let $k = \sqrt{n-1}$. Then, since each eigenvalue of WP is either k or $-k$ and since the trace of a matrix is equal to the sum of its eigenvalues,

$$tr(WP) = tk = n,$$

for some t. Since $k = \sqrt{n-1}$, this is impossible unless $n = 2$. □

Interestingly, although there exist no conference matrices developed over signed groups, there do exist $SW(n, n-1; \mathbb{R})$'s. In fact, if q is an odd prime power, then

there exists a $NW(q+1,q)$ (see Section 2.2.6 for the proof of a more general result). It is generally believed [AD96] that there exist no $CW(n,n-2)$'s for parameters other than $(3,1)$ and $(6,4)$, however, this is still an unproven conjecture. Craigen [AD96] conjectures that for each a, there exist m such that, for all $n > m$, there exists no $CW(n,n-a)$. This is true for odd n, by Theorem 1.4.2.

Some traction can be made into the problem of large weight circulant weighing matrices by using the number theoretic fact that perfect squares are congruent to either 0 or 1 $(\text{mod } 4)$. Let W be a $\mathbf{G}$-developed $W(k^2+2,k^2)$, and let $k>1$, so that k^2+2 must be even (by Theorem 1.4.2). Then we must have that $k^2 \equiv 0 \ (\text{mod } 4)$. Likewise, if W is a $W(k^2+3,k^2)$, then (for $k>1$) $k^2 \equiv 1 \ (\text{mod } 4)$.

Let $\theta_1(x)$ be the Hall polynomial of a $4u^2 \times 4u^2$ circulant Hadamard matrix. Then $\theta_2(x) = \theta_1(x) \ (\text{mod } x^{2u^2}-1)$ is the Hall polynomial of a $2u^2 \times 2u^2$ $(0,\pm 2)$ matrix W. Further, $\theta_2(x)\,\theta_2(x^{-1}) \equiv 4u^2 \ (\text{mod } x^{2u^2}-1)$, so that $WW^T = 4u^2 I$. Therefore, $\frac{1}{2}W$ is a $CW(2u^2,u^2)$. This is an example of a technique called *folding*, wherein the existence of a circulant weighing matrix is shown to imply the existence of a smaller circulant weighing matrix. This technique was known at least as early as 1977 [Hal77]. Arasu [Ara98] uses folding to obtain a reduction theorem for circulant weighing matrices under the so-called self-conjugacy assumption. In Section 3.2.2, I use this technique to obtain another reduction theorem under the self-conjugacy assumption (Theorem 3.2.7).

Let W_1 be a $CW(4u^2+2,4u^2)$, let $\mathbf{r}_i = \left(r_{i1}, r_{i2}, ..., r_{i(4u^2+2)}\right)$ and $\mathbf{r}_t = \left(r_{t1}, r_{t2}, ..., r_{t(4u^2+2)}\right)$ be two rows of W_1, and suppose that there exists a number j such that $r_{ij} = r_{tj} = 0$. Then, since $\mathbf{r}_i \cdot \mathbf{r}_j = 0$ and since $4u^2+2$ is even, there must exist a number $s \neq j$

such that $r_{is} = r_{ts} = 0$. This is only possible if the first row of W_1 is some shift of

$$0 \quad a_1 \quad \ldots \quad a_{2u^2} \quad 0 \quad a_{2u^2+2} \quad \ldots \quad a_{4u^2+1},$$

where, for each i, $a_i \neq 0$. In other words, the Hall polynomial $\theta_1(x)$ of W_1 must have the form

$$x^j \left(a_1 x + \cdots + a_{2u^2} x^{2u^2} + a_{2u^2+2} x^{2u^2+2} + \cdots + a_{4u^2+1} x^{4u^2+1} \right),$$

for some $j = 0, 1, ..., 4u^2 + 1$. Assume, without loss of generality, that $j = 0$. Let $\theta_2(x)$ be such that

$$\theta_2(x) \equiv \theta_1(x) \pmod{x^{2u^2+1} - 1} = (a_1 + a_{2u^2+2}) x + \cdots + (a_{2u^2} + a_{4u^2+1}) x^{2u^2},$$

so that $\theta_2(x)$ is the Hall polynomial of a $(2u^2 + 1) \times (2u^2 + 1)$ circulant $(0, \pm 2)$ matrix C. Further,

$$\theta_2(x) \theta_2\left(x^{-1}\right) = 4u^2 \pmod{x^{2u^2+1} - 1},$$

so that $CC^T = 4u^2 I$. Therefore, $W_2 = \frac{1}{2}C$ is a $CW(2u^2 + 1, u^2)$.

Consider the $CW(4u^2 + 2, 4u^2)$ W_3 with Hall polynomial $\theta_1(-x)$. Two matrices $M_1 = \left[m_{ij}^1\right]$ and $M_2 = \left[m_{ij}^2\right]$ are disjoint if $m_{ij}^1 \neq 0$ implies that $m_{ij}^2 = 0$, and vice versa. Since W_3 has order $4u^2 + 2$ and since W_3 is obtained from W_1 by multiplying every second row and column by -1, one can obtain a $CW(2u^2 + 1, u^2)$ W_4, disjoint from W_2, by folding W_3.

Now let W_5 be a $CW(4u^2 + 4, 4u^2)$ with Hall polynomial $\theta_5(x)$. Without loss of

generality, the first row of W is

$$0 \quad w_1 \quad \ldots \quad w_{a-1} \quad 0 \quad x_1 \quad \ldots \quad x_{b-1} \quad 0 \quad y_1 \quad \ldots \quad y_{c-1} \quad 0 \quad z_1 \quad \ldots \quad z_{d-1}$$

where a is the number of entries from the first zero to the entry before the second zero, and b, c, and d are defined similarly. Let $\mathbf{r}_0$ be the first row of W and, for each t, let $\mathbf{r}_t$ be the row obtained by cyclicly shifting $\mathbf{r}_0$ t times. Since $\mathbf{r}_0 \cdot \mathbf{r}_a = 0$, either $a = b$, $a = c$, or $a = d$.

Suppose first that $a = b$. Since $\mathbf{r}_0 \cdot \mathbf{r}_c = 0$, either $c = a$, in which case $c = b$ and therefore, by orthogonality, $c = d$ also, or $c = d$. Suppose that $c = d$. By orthogonality, $c + d = a$ is impossible. Therefore, since $\mathbf{r}_0 \cdot \mathbf{r}_{c+d} = 0$, $c + d = a + b$ and, consequently, $a = b = c = d$.

Now suppose that $a = c$. Then, since $\mathbf{r}_0 \cdot \mathbf{r}_b = 0$, either $b = a$, in which case $b = c$ and, by orthogonality, $b = d$, or $b = d$.

Finally, suppose that $a = d$. then, since $\mathbf{r}_0 \cdot \mathbf{r}_b = 0$, either $b = a$ (in which case $b = d$ and, by orthogonality, $b = c$) or $b = c$. So suppose that $b = c$. $b + c = d$ is impossible by orthogonality. Therefore, since $\mathbf{r}_0 \cdot \mathbf{r}_{b+c} = 0$, $b + c = d + a$, so that $a = b = c = d$.

In any case, we have that $a = c$ and $b = d$. Let $\theta_5(x)$ be the Hall polynomial of W_5. Define $\theta_6(x)$ so that $\theta_6(x) \equiv \frac{1}{2}\theta_5(x) \pmod{x^{2u^2+2} - 1}$. Then $\theta_6(x)$ is the Hall polynomial of a $CW\left(2u^2 + 2, u^2\right)$.

All of this information is collected in the following theorem, which is well known (see [AD96] and [Hal77]).

Theorem 1.10.4. *(i) If there exists a circulant Hadamard matrix of order n, then $n = 4u^2$, for some u, and there exists a CW $\left(2u^2, u^2\right)$.*

(ii) If there exists a $CW(n, n-2)$, *then* $n = 4u^2 + 2$, *for some* u, *and there exist two disjoint* $CW(2u^2+1, u^2)$*'s.*

(iii) If there exists $CW(n, n-3)$ *then* $n = u^2 + 3$, *for some* $u^2 \equiv 1 \pmod 4$.

(iv) If there exists a $CW(n, n-4)$, *then* $n = 4u^2 + 4$, *for some* u, *and there exists a* $CW(2u^2+2, u^2)$.

It is an open question whether or not this procedure can be pushed any further (can $CW(n, n-6)$'s be folded? Can $CW(n, n-2t)$'s?). Additional structural results concerning large weight weighing matrices are obtained in [Cra95b].

1.11 Hankel Weighing Matrices

A Hankel matrix A is usually (see [Par88]) defined by the condition that, for each entry a_{ij} of A, $a_{ij} = a_{i-1,j+1}$ (for $i > 0$, $j < n$). Since it is convenient for our purposes, we will work with a different definition of Hankel matrices: A matrix A is a *Hankel matrix* if for each entry a_{ij} of A, $a_{ij} = a_{i-1,j-1}$ (for $1 \leq i, j \leq n$). These matrices can be transformed into the usual Hankel matrices by inverting the order in which the rows apear. Since the orthogonality of the rows of a matrix is invariant under row permutation, there is no harm done by working with the non-standard definition.

The following is an example of a 7×7 Hankel $(0, \pm 1)$ matrix.

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

We use the notation $HW(n, w)$ to refer to Hankel weighing matrices of order n and weight w. With this definition, it's apparent that every $CW(n, w)$ and every $NW(n, w)$ is a $HW(n, w)$.

Simone Severeni [Sev08] asked whether anything was known about Hankel weighing matrices. I couldn't find anything in the literature so I decided to investigate on my own. I was surprised to discover the following little result.

Theorem 1.11.1. *Every $HW(n, w)$ is either a $CW(n, w)$ or a $NW(n, w)$.*

Proof. Let A be a $HW(n, w)$. Since there are w nonzero entries in each row of A, we have that, for each i, $\sum_j |a_{ij}| = \sum_j |a_{i-1,j}|$. So $|a_{i,1}| = |a_{i-1,n}|$, i.e. $a_{i-1,n} = \epsilon_i a_{i1}$, for $\epsilon_i = \pm 1$. Since the dot product of any pair of rows is equal to zero, we have that, for any i, t, $\sum_j a_{i,j} a_{t,j} = \sum_j a_{i-1,j} a_{t-1,j}$. Thus, since A is a Hankel matrix, $a_{i,1} a_{t,1} = a_{i-1,n} a_{t-1,n} = \epsilon_i a_{i,1} \epsilon_t a_{t,1}$. Therefore, $\epsilon_i \epsilon_t = 1$. Since this holds for any choice of i and t, $\epsilon_1 = \cdots = \epsilon_n \in \{\pm 1\}$. Consequently, either $a_{i,1} = a_{i-1,n}$ for each i, or $a_{i,1} = -a_{i-1,n}$ for each i. It follows that A is either a $CW(n, w)$ or a $NW(n, w)$. □

Chapter 2

Constructing Circulant Weighing Matrices

Beyond the sparse infinite families obtained by composing small circulant weighing matrices using the tools given in Lemma 1.5.2, there are known to exist several infinite classes of circulant weighing matrices. Among these, the most important are circulant weighing matrices with the so-called *Singer parameters*, $\left(t\frac{q^{d+1}-1}{q-1}, q^d\right)$, where q is a prime power, d is even, and either $t = 1$ or $t|2(q-1)$, depending on whether q is even or odd. See ([AT99] and [EH76]) for infinite classes of non-Singer-type circulant weighing matrices.

Over the past 40 years, a number of papers have been published proving the existence of classes of circulant weighing matrices with Singer parameters. It's unclear who first discovered that such weighing matrices exist. In 1975, Wallis and Whiteman [WW75] generated a class of $CW\,(q^2+q+1, q^2)$'s, where q is a prime power. However, at around the same time, Blake claimed the same result, generalizing a previous result of Mullin. Another construction, due to L. G. Kovacs, appeared in

Richard Hain's Master's thesis [Hai77]. Craigen [Cra95a] constructed a large class of weighing matrices, a sub-class of which has paramaters (q^2+q+1, q^2). This sub-class, it turns out, is equivalent to a class of circulant weighing matrices.

In 1976, Eades [Ead80] proved the existence of $CW\left(\frac{q^{d+1}-1}{q-1}, q^d\right)$'s, with q odd. His proof makes use of relative difference sets. Ipatov [Ipa82] proved the same result in 1982 using shift register sequences. Dillon [ADJP95], Hoholdt and Justesen [HJS3], and Games [Gam86] all published proofs of the even case; their proofs make use of some of the same techniques from projective geometry that Kovacs used to prove the special case that appeared in Hain's thesis. Lately, I was able to extend their approach somewhat, showing that it is often possible to obtain a number of inequivalent circulant weighing matrices in some parameters [Mil09].

In 2001 [ADLM01] and 2003 [LMS02], a group of authors discovered a new approach to building circulant weighing matrices; using relative difference sets and discrete Fourier transforms to obtain an affine analogue of the earlier projective geometry construction.

Jackson and Wild [JW92] showed that Ipatov's shift-register construction is equivalent to a special case of the construction method outlined by Games [Gam86]. Beyond this, it is an open question which of these constructions yield equivalent circulant weighing matrices. Because of the correspondence between relative difference sets and shift register sequences (see [But63]), I conjecture that Ipatov's construction is equivalent to one of the relative difference set constructions (for q odd).

In order to come to terms with the present state of knowledge regarding circulant weighing matrices with Singer parameters, it is necessary to consider both the pro-

jective geometry approach from ([ADJP95], [HJ83], and [Cam86]) and the relative difference set approach from [ADLM01]. I will sketch the former technique and examine the latter somewhat more in depth.

The chapter concludes with a discussion of negacyclic weighing matrices with Singer parameters. By borrowing some ideas from [ADLM01], I am able to extend the construction from [DGS71] to obtain a construction that proves to be a minor generalization of all previously known constructions of negacyclic weighing matrices.

2.1 Prerequisites

2.1.1 Background from Projective Geometry

A *projective space* P (see [BR98]) is a structure comprised of objects called "points" and objects called "lines" and a relation called "incidence" such that P satisfies projective plane axioms *i*) and *iii*) (see p.21) and the following axiom

ii') if A, B, C, and D are four points such that the line AB (the unique line that contains both A and B) intersects CD, then AC intersects BD (so any two lines that "lie in the same plane" intersect one another).

Some authors [BR98] also require that projective spaces satisfy projective plane axiom iv), but I will not make this stipulation, thus allowing the "projective line" into the class. A *finite projective space* is a projective space with a finite point set. We can use vector spaces to construct finite projective spaces (see, for instance, [BR98, p.56]). Let q be a prime and let $d \in \mathbb{N}$. Let $\mathbf{V}$ be a $(d+1)$-dimensional vector space developed over $\mathbf{GF}(q)$. Let $P(\mathbf{V})$ be an incidence structure comprised of points and lines that are defined as follows: its points have the form $\mathbf{p}\backslash\{0\}$,

where $\mathbf{p}$ is a one dimensional subspace of $\mathbf{V}$, and its lines have the form $\ell\backslash\{0\}$, where ℓ is a 2 dimensional subspace of $\mathbf{V}$. If $\mathbf{v} \in \mathbf{p}\backslash\{0\}$, then we may write $\mathbf{p}\backslash\{0\}$ as $\langle\mathbf{v}\rangle\backslash\{0\}$. In this case, if $\mathbf{V} = \mathbf{GF}(q)^{d+1}$ and $\mathbf{v} = (a_0, ..., a_{d+1})$, then we say that $\mathbf{p}$ has *homogeneous coordinates* $(a_0; a_1; , ...; a_{d+1})$. Of course, homogeneous coordinates are not uniquely determined by the point they represent.

Choose two points $\langle\mathbf{v}_1\rangle\backslash\{0\}$, $\langle\mathbf{v}_2\rangle\backslash\{0\} \in P(\mathbf{V})$ These points are contained in exactly one line: $\langle\mathbf{v}_1, \mathbf{v}_2\rangle\backslash\{0\}$. This verifies axiom i).

Axiom *ii'*) holds trivially when $d = 1$. So suppose that $d > 1$. Now suppose that

$$\langle\mathbf{v}_1, \mathbf{v}_2\rangle\backslash\{0\} \cap \langle\mathbf{v}_3, \mathbf{v}_4\rangle\backslash\{0\} \neq \varnothing,$$

i.e. suppose that there exists $\mathbf{v}\backslash\{0\} \in \langle\mathbf{v}_1, \mathbf{v}_2\rangle\backslash\{0\} \cap \langle\mathbf{v}_3, \mathbf{v}_4\rangle\backslash\{0\}$. So let

$$\mathbf{v} = a\mathbf{v}_1 + b\mathbf{v}_2 = c\mathbf{v}_3 + d\mathbf{v}_4,$$

where $a, b, c, d \in \mathbf{GF}(q)$. Then $\mathbf{v}_2 = b^{-1}(\mathbf{v} - a\mathbf{v}_1)$ and $\mathbf{v}_3 = c^{-1}(\mathbf{v} - d\mathbf{v}_4)$. Thus,

$$\dim\langle\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4\rangle = \dim\langle\mathbf{v}, \mathbf{v}_1, \mathbf{v}_4\rangle \leq 3.$$

In a vector space of dimension 3, every pair of subspaces of dimension 2 intersect one another in a subspace of dimension greater than or equal to 1. So

$$\langle\mathbf{v}_1, \mathbf{v}_3\rangle\backslash\{0\} \cap \langle\mathbf{v}_2, \mathbf{v}_4\rangle\backslash\{0\} \neq \varnothing.$$

This verifies axiom ii). It's clear that axiom iii) holds.

We will use this construction to build a projective plane of order 2. Consider the

vector space $\mathbf{GF}(2)^3$. The following table gives the points and lines of the Fano plane (see Section 1.4).

points	lines
$(1,0,0)$	$\{(1,0,0),(0,1,0),(1,1,0)\}$
$(0,1,0)$	$\{(1,0,0),(0,0,1),(1,0,1)\}$
$(0,0,1)$	$\{(1,0,0),(0,1,1),(1,1,1)\}$
$(1,1,0)$	$\{(0,1,0),(0,0,1),(0,1,1)\}$
$(1,0,1)$	$\{(0,1,0),(1,0,1),(1,1,1)\}$
$(0,1,1)$	$\{(0,1,0),(1,0,1),(1,1,1)\}$
$(1,1,1)$	$\{(1,1,0),(0,1,1),(1,0,1)\}$

Let P be a projective space and let $U \subset P$. U is a *linear subspace* of P if for every two points $A, B \in U$, the line AB is in U as well. A projective space, along with each of its subspaces, is called a *projective geometry*. The terms 'projective geometry' and 'projective space' will be used interchangeably, since they are extensionally identical. If $S \subset P$, then $\langle S \rangle$ denotes the smallest linear subspace that contains S. A set $B \subset P$ is called *independent* iff for every $B^* \subset B$ and for each $Q \in B \setminus B^*$, $Q \notin \langle B^* \rangle$. We say that a set $B \subset P$ *spans* P if $\langle B \rangle = P$. Suppose that there exists a finite, independent set of points $A_0, A_1, ..., A_d$ that span P, i.e., suppose that $P = \langle A_0, A_1, ..., A_d \rangle$. Then it can be shown that every minimal spanning set of P has the same number, $d+1$, of elements (see [BR98, p.18]). The number d is called the *dimension* of P. If the vector space $\mathbf{V}$ has dimension $d+1$, then the projective geometry $P(\mathbf{V})$ has dimension d.

Linear subspaces are projective spaces of lesser dimension. In general, for a $(d+1)$-

dimensional vector space $\mathbf{V}$ developed over $\mathbf{GF}(q)$, the t dimensional subspaces of $P(\mathbf{V})$ have the form $\mathbf{S}\backslash\{0\}$, where $\mathbf{S}$ is a $t+1$ dimensional subspace of $\mathbf{V}$.

Subspaces of dimension $d-1$ are called *hyperplanes.* Line up the basis vectors of a subspace $\mathbf{S}$ of a vector space $\mathbf{V}$ such that $\mathbf{S}\backslash\{0\}$ is a hyperplane of $P(\mathbf{V})$ as the rows of a matrix. Then the matrix has range d and, by the Dimension Theorem, its kernel has dimension 1. So there exists a point, represented by the vector $\mathbf{u} = (u_0, ..., u_n)$, such that the hyperplane is the set of points $\langle\mathbf{x}\rangle\backslash\{0\} = \langle(x_0, ..., x_n)\rangle\backslash\{0\}$ such that $\mathbf{x}$ satisfies the equation $\mathbf{u}\cdot\mathbf{x} = 0$. We use the notation $\pi(\mathbf{u})$ to refer to the hyperplane. The following fact about hyperplanes is useful for our purposes (see [BR98]).

Theorem 2.1.1. *Let P be a projective geometry. A subspace H of P is a hyperplane of P if and only if, for each subspace S of P of dimension t, $S \cap H$ is a subspace of P of dimension $t-1$.*

Two projective geometries are *isomorphic* if there exists a subspace preserving bijection between them; this bijection is called an *isomorphism.* It can be shown that for every finite projective geometry P of dimension ≥ 3, there exists a vector space $\mathbf{V}$ such that P is isomorphic to $P(\mathbf{V})$ (see [BR98]). There are however, projective planes for which this is not the case (again, see [BR98]).

Every line of a finite projective geometry P is incident with the same number, $n+1$ of points ([BR98, p.23]). The number n is called the *order* of P. If $\mathbf{V}$ is a $d+1$-dimensional vector space developed over $\mathbf{GF}(q)$, then the order of $P(\mathbf{V})$ is q. It is well known ([BR98, p.24]) that every t-dimensional subspace U of P contains exactly $\frac{n^{t+1}-1}{n-1}$ points and $\frac{(n^t+n^{t-1}+\cdots+n+1)(n^{t-1}+\cdots+n+1)}{n+1}$ lines. Let P have dimension d. Then P contains exactly $\frac{n^{d+1}-1}{n-1}$ points. Further ([BR98, p.24]), each point of P is incident with $n^{d-1}+\cdots+n+1$ lines. So, in particular, $P(\mathbf{V})$ contains $\frac{q^{d+1}-1}{q-1}$

points and each point of $P(\mathbf{V})$ is incident with exactly $q^{d-1} + \cdots q + 1$ lines.

2.1.2 Background From Affine Geometry

An *affine geometry* A is an incidence structure comprised of "points" and "subspaces" that can be obtained from a projective geometry P by deleting one of its hyperplanes H_∞, referred to as the *hyperplane at infinity*, and all of the points and subspaces contained in that hyperplane. The subspaces of the affine geometry are the remaining subspaces, truncated so that they contain no points of the hyperplane at infinity. We refer to the affine geometry by writing $A = P/H_\infty$. A *finite affine geometry* is an affine geometry with a finite point set.

An *affine space* is an incidence structure comprised of the points and lines of an affine geometry. The terms "affine space" and "affine geometry' will be used interchangeably, since they are extensionally identical.

Important constructive results about circulant weighing matrices and related combinatorial objects have been proven using facts about projective geometry; one of the major themes explored in this chapter is that these results can often be generalized by using analogous facts about affine geometry.

Affine geometries can also be treated axiomatically. For instance, affine planes (affine geometries obtained by deleting a line from a projective plane) can be axiomatized as follows [BR98].

Theorem 2.1.2. *Let A be an incidence structure comprised of "points" and "lines." Then A is an affine plane if and only if the "points" and "lines" of A satisfy the following three axioms:*

1) If p_1 and p_2 are two "points," then there is exactly one "line" that passes through both p_1 and p_2.

2) If ℓ is a "line" and p is a "point" that does not lie on ℓ, then there exists exactly one line, incident with p, that contains no points in common with ℓ.

3) There exist three "points" which do not all lie on the same line.

Theorem 2.1.2 implies that the euclidean plane is, in fact, an affine plane. The question then arises: what is the projective plane P and line at infinity ℓ_∞ such that $\mathbb{R}^2 = P/\ell_\infty$?

Define an equivalence relation $||$ on the lines of $\mathbb{R}^2$ as follows: Two lines ℓ_1 and ℓ_2 satisfy $\ell_1||\ell_2$ if and only if either $\ell_1 = \ell_2$ or ℓ_1 and ℓ_2 share no common point. If $\ell_1||\ell_2$, then we say that ℓ_1 and ℓ_2 are in the same *parallel class.* Each line of $\mathbb{R}^2$ belongs to exactly one parallel class.

Define a new geometry P as follows: The point set of P is comprised of both the points of $\mathbb{R}^2$ and the parallel classes of $\mathbb{R}^2$. If ℓ is a line of $\mathbb{R}^2$ belonging to parallel class C, then $\ell \cup C$ is a line of P. Further, the line ℓ_∞, consisting of each parallel class of $\mathbb{R}^2$, is also a line of P. P is a projective geometry and $\mathbb{R}^2 = P/\ell_\infty$.

There is a nice way to generate affine geometries using vector spaces. Let q be a prime, let $d \in \mathbb{N}$, let $\mathbf{V}_1 = \mathbf{GF}(q)^{d+1}$, and let $\mathbf{V}_2 = \mathbf{GF}(q)^d$. Let $\mathbf{u}_0 = (1, 0, ..., 0) \in \mathbf{V}_1$ and let H_∞ be the hyperplane $\pi(\mathbf{u}_0)$ of $P(\mathbf{V}_1)$. Let $A(\mathbf{V}_2) = P(\mathbf{V}_1)/H_\infty$.

If $(b_0; b_1; ...; b_{d+1})$ are the homogeneous coordinates of a point $\mathbf{p}\backslash\{0\}$ of $P(\mathbf{V}_1)$ lying outside of H_∞, then $b_0 \neq 0$. Hence, $\mathbf{p}\backslash\{0\}$ also has homogeneous coordinates $(1; a_1; ...; a_d)$, for some uniquely determined $a_1, ..., a_d$. We call $(a_1; ...; a_d)$ the *inhomogeneous coordinates* of $\mathbf{p}\backslash\{0\}$. Likewise, we can associate each point of $A(\mathbf{V}_2)$ with a d-tuple $(c_1; ...; c_d)$ of inhomogeneous coordinates (and conversely).

Let ℓ be a line of $P(\mathbf{V}_1)$ that is not contained in H_∞. Then, by Theorem 2.1.1, ℓ intersects H_∞ in exactly one point, with homogeneous coordinates $(0; b_1; ...; b_d)$. Let $\mathbf{p}\backslash\{0\}$ be another point on ℓ and suppose that $\mathbf{p}\backslash\{0\}$ has homogeneous coordinates $(1; a_1; ...; a_d)$. Then each point of $A(\mathbf{V}_2)$ contained in ℓ has homogeneous coordinates $(1; a_1; ...; a_d) + a(0; b_1; ...; b_d)$, for some $a \in \mathbf{GF}(q)$. It follows that the inhomogeneous coordinates of the points of $A(\mathbf{V}_2)$ that lie on ℓ can be written as $(a_1; ...; a_d) + a(b_1; ...; b_d)$, for some $a \in \mathbf{GF}(q)$. So, we can associate the line ℓ with the coset $(a_1; ...; a_d) + \langle(b_1; ...; b_d)\rangle$ of $\langle(b_1; ...; b_d)\rangle$. Likewise, we can associate each line of $A(\mathbf{V}_2)$ with a coset of a one-dimensional subspace of $\mathbf{V}_2$ (and conversely). Two affine geometries are *isomorphic* if there is a subspace preserving bijection between them. The following result is well known (see, for instance, [BR98]).

Theorem 2.1.3. *Let q be a prime, let $d \in \mathbb{N}$, let $\mathbf{V}_1 = \mathbf{GF}(q)^{d+1}$, and let $\mathbf{V}_2 = \mathbf{GF}(q)^d$. Let $\mathbf{u}_0 = (1, 0, ..., 0) \in \mathbf{V}_1$. Let $A(\mathbf{V}_2)$ be a geometry in which incidence is defined as set theoretical containment and the points and lines are as follows:*
The points are the vectors $\mathbf{v} \in \mathbf{V}_2$.
The lines are the cosets of the one dimensional subspaces of $\mathbf{V}_2$.
Then $A(\mathbf{V}_2)$ is an affine geometry isomorphic to the affine geometry obtained by deleting the hyperplane $\pi(\mathbf{u}_0)$ from the projective geometry $P(\mathbf{V}_1)$.

The following table gives the points and lines of the affine plane obtained from

the Fano Plane.

points	lines
$(0,0)$	$\{(0,0),(1,0)\}$
$(1,0)$	$\{(0,0),(0,1)\}$
$(0,1)$	$\{(0,0),(1,1)\}$
$(1,1)$	$\{(0,1),(1,1)\}$
	$\{(1,0),(1,1)\}$
	$\{(1,0),(0,1)\}$

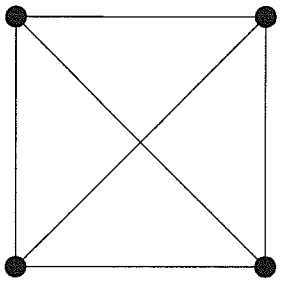

Figure 2.1: The Affine Fano Plane

2.1.3 The Trace Function

If E is an extension field of F, then the *field trace function* Tr is defined by the rule that, for any $\alpha \in E$,

$$\mathrm{Tr}(\alpha) = \sum_{\gamma \in \mathbf{Gal}(E/F)} \gamma(\alpha).$$

If context requires that the fields E and F be specified, then Tr may be written as $\mathrm{Tr}_{E/F}$. We restrict our attention to the field extension $\mathbf{GF}(q^m)$ of $\mathbf{GF}(q)$, where q is a prime power. The Galois group of this field extension is generated by the *Froebenius map* $\gamma : \alpha \to \alpha^q$ (see [Gal04], p. 554 for details). So, for $\alpha \in \mathbf{GF}(q^m)$,

$$\mathrm{Tr}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}.$$

In what follows, we make use of the fact that

$$\left(\sum x_i\right)^{q^t} = \sum x_i^{q^t},$$

for $x_i \in GF(q^m)$ (see [Gal04], p. 248, exercise 41).

For $x \in GF(q^m)$, $x^q = x$ if and only if $x \in GF(q) \subset GF(q^m)$. Let $\alpha, \beta \in GF(q^m)$. Then

$$\mathrm{Tr}(\alpha)^q = \left(\sum_{i=0}^{m-1} \alpha^{q^i}\right)^q = \sum_{i=0}^{m-1} \alpha^{q^i}.$$

So Tr maps $GF(q^m)$ into $GF(q)$. Further,

$$\mathrm{Tr}(\alpha+\beta) = \sum_{i=0}^{m-1} (\alpha+\beta)^{q^i} = \sum_{i=0}^{m-1} (\alpha^{q^i} + \beta^{q^i}) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$$

and, if $c \in GF(q)$, then

$$\mathrm{Tr}(c\alpha) = \sum_{i=0}^{m-1} (c\alpha)^{q^i} = \sum_{i=0}^{m-1} c\alpha^{q^i} = c\mathrm{Tr}(\alpha).$$

Finally, Ker (Tr) (the kernel of the trace function) is the set of roots of the polyno-

mial

$$\sum_{i=0}^{m-1} x^{q^i}.$$

Since this polynomial has degree q^{m-1}, it has at most q^{m-1} roots. But there are q^m elements in $GF(q^m)$, so Ran (Tr) (the range of the trace function) is non-trivial. Thus, since Tr preserves scalar multiplication, Tr is an onto mapping. The following lemma [MM07] summarizes the foregoing discussion.

Lemma 2.1.4. *Tr is a linear transformation that maps $GF(q^m)$ onto $GF(q)$.*

We will make multiple uses of the next lemma [MM07].

Lemma 2.1.5. *Every linear transformation from $GF(q^m)$ to $GF(q)$ can be defined as a map of the form $L_\beta : \alpha \to Tr(\beta\alpha)$, for some $\beta \in GF(q^m)$.*

Proof. Since both Tr and $\alpha \to \beta\alpha$, $\beta \in GF(q^m)$, are linear transformations, $L_\beta : \alpha \to \mathrm{Tr}(\beta\alpha)$ is a linear transformation. Moreover, if $\beta \neq \lambda$, if $\mathrm{Tr}(\alpha) \neq 0$, and if $\alpha^* = (\beta - \lambda)^{-1}\alpha$, then

$$\mathrm{Tr}((\beta - \lambda)\alpha^*) = \mathrm{Tr}(\alpha) \neq 0.$$

So $L_\beta \neq L_\lambda$.

Since a linear transformation is determined by its action on a basis, there are q^m linear transformations from $GF(q^m)$ to $GF(q)$. But there are q^m distinct linear transformations of the form L_β. □

If $q = p^\epsilon$, where p is a prime and $\epsilon > 1$, then $\mathrm{Tr} : \mathbf{GF}(q^m) \to \mathbf{GF}(q)$ is called the *relative trace* and $\mathrm{Tr} : \mathbf{GF}(q^m) \to \mathbf{GF}(p)$ is called the *absolute trace.*

Lemma 2.1.6. *[MM07] Let q be a prime power and let $m|n \in \mathbb{N}$. Let $K = \mathbf{GF}(q)$, $F = \mathbf{GF}(q^m)$, and $E = \mathbf{GF}(q^n)$. Let $\alpha \in E$. Then $Tr_{E/K}(\alpha) = Tr_{F/K}(Tr_{E/F}(\alpha))$.*

Proof.

$$\mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(\alpha)) = \mathrm{Tr}_{F/K}\left(\sum_{j=0}^{\frac{n}{m}-1}\alpha^{q^{jm}}\right) = \sum_{i=0}^{m-1}\left(\sum_{j=0}^{\frac{n}{m}-1}\alpha^{q^{jm}}\right)^{q^i} = \sum_{i=0}^{m-1}\sum_{j=0}^{\frac{n}{m}-1}\alpha^{q^{jm+i}}$$

$$= \sum_{t=0}^{n-1}\alpha^{q^t} = \mathrm{Tr}_{E/K}(\alpha).$$

□

The additive version of Hilbert's 90th Theorem (see [Hil65]) states that if E is an extension field of F and if $\mathbf{Gal}\,(E/F)$ is generated by γ, then, for each $x \in E/F$, $Tr(x) = 0$ if and only if there exists $y \in E/F$ such that $x = y - \gamma(y)$. For a proof of this result, the reader is invited to see [Kar88]. I have devised my own proof, which is very simple, but works only in the finite case. This is the finite additive version of Hilbert's 90th theorem.

Theorem 2.1.7. *Let q be a prime power, let $d \in \mathbb{N}$, and let $x \in \mathbf{GF}(q^d)$. Then $Tr(x) = 0$ if and only if there exists $y \in \mathbf{GF}(q^d)$ such that $x = y - y^q$.*

Proof. Let $\mathbf{G}$ be the additive group of $\mathbf{GF}(q^d)$. Then Tr is a homomorphism from $\mathbf{G}$ to itself, and so is

$$g : y \to y - y^q,$$

for $y \in \mathbf{GF}(q^d)$.

$$\mathrm{Ker}(g) = \{y \in \mathbf{GF}(q^d) : y - y^q = 0\} = \mathbf{GF}(q).$$

So

$$|\mathrm{Ran}(g)| = \frac{|\mathbf{GF}(q^d)|}{|\mathbf{GF}(q)|} = \frac{q^d}{q} = q^{d-1}.$$

But, by Lemma 2.1.4,

$$\mathrm{Ran}\,(\mathrm{Tr}) = \mathbf{GF}(q).$$

So

$$|\mathrm{Ker}\,(\mathrm{Tr})\,| = \frac{|\mathbf{GF}(q^d)|}{|\mathbf{GF}(q)|} = \frac{q^d}{q} = q^{d-1}.$$

For any $y \in \mathbf{GF}(q^d)$,

$$Tr(y - y^q) = Tr(y) - Tr(y^q) = Tr(y) - Tr(y) = 0.$$

Thus,

$$\{x \in \mathbf{GF}(q^d) : Tr(x) = 0\} = \{y - y^q : y \in \mathbf{GF}(q^d)\}.$$

□

2.2 Constructing Circulant Weighing Matrices Using Projective Geometry

In this section I will sketch a construction of circulant weighing matrices that makes use of tools from projective geometry. In particular, the results presented in this section imply that, for each prime power q and for each $d \in 2\mathbb{N}$, there exists a

$CW\left(\frac{q^{d+1}-1}{q-1}, q^d\right)$. Note that, for each $d \in 2\mathbb{N}$,

$$\lim_{q\to\infty} \frac{q^d}{q^d + q^{d-1} + \cdots + 1} = 1.$$

Consequently, by choosing q large enough, one can find circulant weighing matrices with (almost) as large weight as one desires, in the second sense of the term 'large weight,' from section 1.1.0.

As I mentioned in the introduction, there are (at least) three papers from the literature in which this construction is pursued: [ADJP95], [HJ83], and [Gam86]. The construction depends on properties of two types of mathematical objects, cyclic difference sets and quadrics, both of which will be introduced in this section.

2.2.1 Cyclic Difference Sets

A *cyclic difference set* $D = \{d_1, ..., d_k\}$, with parameters v, k, and λ, is a set of k residues $\pmod v$ such that, for each residue $\alpha \not\equiv 0$, there are exactly λ pairs (d_i, d_j), with $d_i, d_j \in D$, such that $d_i - d_j \equiv \alpha \pmod v$.

For example, $\{0, 2, 3\}$ is a cyclic difference set with parameters $(7, 3, 1)$. If D is a set of residues mod v, then the *polynomial associated with* D is the element $d(x)$ of the polynomial ring $\mathbb{Z}[x]/\langle x^v - 1\rangle$ defined as follows:

$$d(x) = \sum_{d\in D} x^d.$$

For any r, let

$$T_r(x) = 1 + x + \cdots + x^{r-1}.$$

It follows that D is a difference set if and only if its associated polynomial $d(x)$ satisfies the equation

$$d(x)d(x^{-1}) \equiv (k-\lambda) + \lambda T_v(x) \pmod{x^v - 1}.$$

For example, the polynomial of the difference set $\{0,1,3\}$ is $1+x+x^3$, and it is straightforward to verify that

$$(1+x+x^3)(1+x^{-1}+x^{-3}) \equiv 2 + T_7(x) \pmod{x^7 - 1}.$$

Difference set polynomials make it easy to verify two basic facts about cyclic difference sets.

Lemma 2.2.1. *Let D be a (v,k,λ) cyclic difference set. Then, for each residue $t \pmod v$, $D+t$ is also a (v,k,λ) cyclic difference set. Further, if $(t,v)=1$, then tD is a (v,k,λ) cyclic difference set.*

Proof. Let $d(x)$ be the difference set polynomial of D. Then $x^t d(x)$ is the difference set polynomial of $D+t$. But

$$x^t d(x) x^{-t} d\left(x^{-1}\right) = d(x) d\left(x^{-1}\right) = (k-\lambda) + \lambda T_v(x).$$

This verifies the first claim.

Let $(t,v)=1$. Note that $d\left(x^t\right)$ is the difference set polynomial of tD. For $f(x) \in \mathbb{Z}[x]/\langle x^v - 1\rangle$, let $f(x)^{(t)} = f\left(x^t\right)$. Then

$$d\left(x^t\right) d\left(x^{-t}\right) = \left(d(x)\, d\left(x^{-1}\right)\right)^{(t)} = \left((k-\lambda) + \lambda T_v(x)\right)^{(t)} = (k-\lambda) + \lambda T_v(x).$$

This verifies the second claim. □

So, for example, since $\{0, 2, 3\}$ is a $(7, 3, 1)$ cyclic difference set, so is

$$\{0, 2, 3\} + 3 = \{3, 5, 6\}.$$

And, since $(2, 7) = 1$,

$$2\{0, 2, 3\} = \{0, 4, 6\}$$

is also a $(7, 3, 1)$ cyclic difference set.

Let $\mathbf{G}$ be the cyclic group of order v. A (v, k, λ) cyclic difference set D could alternately be regarded as equivalent to an element d of the group ring $\mathbb{Z}\mathbf{G}$ satisfying

$$dd^{(-1)} = (k - \lambda) + \lambda\mathbf{G}.$$

More generally, let $\mathbf{G} = \{g_1, g_2, ..., g_n\}$ be a finite group. A (v, k, λ) $\mathbf{G}$ difference set is a subset D of $\mathbf{G}$ such that each $g \in \mathbf{G}$ has exactly λ representations as a "difference" $g_i g_j^{-1}$, where $g_i, g_j \in D$. The existence of D is equivalent to the existence of an element $d \in \mathbb{Z}[G]$ such that

$$dd^{(-1)} = (k - \lambda) + \lambda\mathbf{G}.$$

Since the ring of polynomials mod $x^v - 1$ is isomorphic to the ring of $v \times v$ circulant matrices (p.27-28), every polynomial associated with a set of residues is the Hall polynomial of a circulant matrix C with either 0 or 1 in each entry. Further, if the

set is a (v, k, λ) cyclic difference set, then

$$CC^T = (k - \lambda)I + \lambda J,$$

so that C is the incidence matrix of a balanced incomplete block design (see section 1.4).

The matrix representation of cyclic difference sets makes it easy to deduce that if D is a (v, k, λ) cyclic difference set, then D^c, the complement of D, is a $(v, v-k, v-2k+\lambda)$ cyclic difference set. Let C be the matrix corresponding to D, and let C^c be the matrix corresponding to D^c. Then

$$C^c = J - C.$$

Consequently,

$$C^c\left(C^c\right)^T = (J - C)(J - C)^T = vJ - 2kJ + (k - \lambda)I + \lambda J$$

$$= (k - \lambda)I + (v - 2k + \lambda)J = ((v - k) - (v - 2k + \lambda))I + (v - 2k + \lambda)J.$$

For a matrix M, let abs(M) be the matrix whose entries are the absolute values of the entries in M. A weighing matrix W is *balanced* if abs(W) is the incidence matrix of a balanced incomplete block design.

In the circulant case, the incidence matrix of a balanced incomplete block design is also a matrix corresponding to a cyclic difference set. We say that a cyclic difference set D has a Waterloo Decomposition if D can be partitioned into a union of disjoint sets A and B such that $A - B$ is the Hall polynomial of a circulant weighing matrix.

(actually, the definition of a Waterloo Decomposition is more general and will be given in a later section).

2.2.2 Singer's Theorem

In 1938, J. Singer [Sin38] discovered an important class of difference sets that can be constructed using projective geometry.

Theorem 2.2.2. *For each positive integer d and for each prime power q, there exists a (v, k, λ) cyclic difference set, where $v = \frac{q^{d+1}-1}{q-1}$, $k = \frac{q^d-1}{q-1}$, and $\lambda = \frac{q^{d-1}-1}{q-1}$.*

Proof. It is well known that $\mathbf{GF}\left(q^{d+1}\right)^*$, the multiplicative group of $\mathbf{GF}\left(q^{d+1}\right)$, is cyclic, say $\mathbf{GF}\left(q^{d+1}\right)^* = \langle\alpha\rangle$. By a result from elementary field theory (see [Jr.98]), α is a root of a polynomial $F(x)$, with coefficients from $\mathbf{GF}(q)$ and of degree $d+1$, that is irreducible over $\mathbf{GF}(q)$. Let

$$F(x) = x^{d+1} + c_d x^d + ... + c_1 x + c_0.$$

Then we have that

$$\alpha^{d+1} = -c_0 - c_1\alpha - ... - c_d\alpha^d.$$

So, for each i, there exists a set $\{a_0, a_1, ..., a_d\}$ of elements from $\mathbf{GF}(q)$ such that

$$\alpha^i = a_0 + a_1\alpha + ... + a_d\alpha^d.$$

Let $f : \mathbf{GF}\left(q^{d+1}\right) \to \mathbf{GF}\left(q\right)^{d+1}$ be the map defined by the rules that $f(0) = (0, ..., 0, 0)$ and that, for each $1 \leq i \leq q^{d+1} - 1$, $f\left(\alpha^i\right) = (a_d, ..., a_1, a_0)$. Then f is a vector space isomorphism.

Furthermore, α^v generates $\mathbf{GF}(q)$ as a subfield of $\mathbf{GF}(q^{d+1})$, and it follows that, for any i,j, $f(\alpha^i)$ and $f(\alpha^j)$ belong to the same point of $P\left(\mathbf{GF}(q)^{d+1}\right)$ if and only if $i \equiv j \pmod{v}$.

Label the v hyperplanes of $P\left(\mathbf{GF}(q)^{d+1}\right)$ $H_0, ..., H_{v-1}$. Define a $v \times v$ matrix $C = [c_{ij}]$ as follows: $c_{ij} = 1$ if the point of $P\left(\mathbf{GF}(q)^{d+1}\right)$ that contains $f(\alpha^i)$ is in H_j and $c_{ij} = 0$ otherwise. Since any two hyperplanes intersect in a subspace of dimension $d-2$,

$$CC^T = (k-\lambda)I + \lambda J. \tag{2.1}$$

The remainder of the proof is devoted to showing that the hyperplanes of $P\left(\mathbf{GF}(q)^{d+1}\right)$ can be labeled in a manner such that C is circulant.

Let $\phi : \mathbf{GF}\left(q^{d+1}\right) \rightarrow \mathbf{GF}\left(q^{d+1}\right)$ be defined by the rules that $\phi(0) = 0$ and that, for each i, $\phi(\alpha^i) = \alpha^{i+1}$. Define a map $\gamma : \mathbf{GF}(q)^{d+1} \rightarrow \mathbf{GF}(q)^{d+1}$ by the rule $\gamma = f(\phi(f^{-1}))$. Then, for each $(a_d, ..., a_0)$,

$$\gamma((a_d, ..., a_0)) = (a_{d-1} - a_d c_d, ..., a_0 - a_d c_1, -a_d c_0).$$

Let $u_0, ..., u_t \in \mathbf{GF}(q)^{d+1}$ be a linearly independent set of vectors. Then, for any $b_0, ..., b_t \in GF(q)$,

$$\gamma(b_0 u_0 + ... + b_t u_t) = b_0\gamma(u_0) + \cdots + b_t\gamma(u_t).$$

Thus,

$$b_0 u_0 + \cdots + b_t u_t = 0$$

if and only if

$$b_0\gamma(u_0) + \cdots b_t\gamma(u_t) = 0.$$

It follows that $\gamma(u_0), ..., \gamma(u_t)$ is a linearly independent set of vectors. So γ maps subspaces of $P\left(\mathbf{GF}(q)^{d+1}\right)$ onto subspaces of equal dimension; in particular, it sends hyperplanes onto hyperplanes.

We wish to show that, for each $j < v$, γ^j does not map any hyperplane into itself. Suppose, for the sake of contradiction, that γ^j fixes a hyperplane H. There exists some number t such that γ^j maps vectors $f(\alpha^i)$ that lie inside points of H in cycles $\left(f(\alpha^i), f(\alpha^{i+j}), f(\alpha^{i+2j}), ..., f\left(\alpha^{i+(t-1)j}\right)\right)$ of length t. Since γ^j fixes H, it follows that t divides k. But since $\gamma^v = 1$, t also divides v.

Note that $v - qk = 1$, so that v and k are relatively prime. Thus $t = 1$, and it follows that γ^j is the identity mapping. But, for $j < v$, γ^j is not the identity mapping. This contradiction implies that γ maps the hyperplanes of $P\left(\mathbf{GF}(q)^{d+1}\right)$ in a cycle of length v.

Choose any hyperplane and label it H_0. Then let $H_1 = \gamma(H_0)$, $H_2 = \gamma^2(H_0)$, ..., and $H_{v-1} = \gamma^{v-1}(H_0)$. It follows that the resulting matrix C is circulant. This fact, combined with equation 2.1, implies that C is a matrix corresponding to a (v, k, λ) cyclic difference set. □

Note that, in the above proof, since $\mathbf{GF}\left(q^{d+1}\right)$ and $\mathbf{GF}(q)^{d+1}$ are isomorphic vector spaces, one could also construct the matrix C using $P\left(\mathbf{GF}\left(q^{d+1}\right)\right)$. To do so, label the v hyperplanes of $P\left(\mathbf{GF}\left(q^{d+1}\right)\right)$ H_0, ..., H_{v-1}. Let $C = [c_{ij}]$ be defined by the rule that $c_{ij} = 1$ if the point of $P\left(\mathbf{GF}\left(q^{d+1}\right)\right)$ that contains α^i lies in the hyperplane H_j, and $c_{ij} = 0$ otherwise. For the purposes of the above proof, it was convenient to work in $P\left(\mathbf{GF}(q)^{d+1}\right)$ in order to prove the linearity of the map γ.

Let $L : GF(q^{d+1}) \rightarrow GF(q)$ be a linear transformation. Then $\dim(\text{ran}(L)) = 1$. It follows, by the Dimension Theorem, that $\dim(\ker(L)) = d$, so that $\text{Ker}(L)/\{0\}$ is a hyperplane of $P\left(\mathbf{GF}\left(q^{d+1}\right)\right)$. Therefore, in order to construct a Singer difference set, we need only find the kernel (minus 0) of a linear transformation from $GF(q^{d+1})$ to $GF(q)$.

The degree 3 polynomial $x^3 - x + 1$ is irreducible over $\mathbf{GF}(3)$. Let α be a generator of $\mathbf{GF}(3^3)^*$ that is also a root of $x^3 - x + 1$. Then the following correspondence specifies an isomorphism f between the vector spaces $\mathbf{GF}(3^3)$ and $\mathbf{GF}(3)^3$:

$\mathbf{GF}(3^3)$	$\mathbf{GF}(3)^3$	$\mathbf{GF}(3^3)$	$\mathbf{GF}(3)^3$	$\mathbf{GF}(3^3)$	$\mathbf{GF}(3)^3$	$\mathbf{GF}(3^3)$	$\mathbf{GF}(3)^3$
0	(0,0,0)	1	(0,0,1)	α	(0,1,0)	α^2	(1,0,0)
α^3	(0,1,−1)	α^4	(1,−1,0)	α^5	(−1,1,−1)	α^6	(1,1,1)
α^7	(1,−1,−1)	α^8	(−1,0,−1)	α^9	(0,1,1)	α^{10}	(1,1,0)
α^{11}	(1,1,−1)	α^{12}	(1,0,−1)	α^{13}	(0,0,−1)	α^{14}	(0,−1,0)
α^{15}	(−1,0,0)	α^{16}	(0,−1,1)	α^{17}	(−1,1,0)	α^{18}	(1,−1,1)
α^{19}	(−1,−1,−1)	α^{20}	(−1,1,1)	α^{21}	(1,0,1)	α^{22}	(0,−1,−1)
α^{23}	(−1,−1,0)	α^{24}	(−1,−1,1)	α^{25}	(−1,0,1)	α^{26}	(0,0,1)

Making use of this correspondence, we deduce that

$$\text{Ker}(\text{Tr})/\{0\} = \{1, \alpha, \alpha^3, \alpha^9, \alpha^{13}, \alpha^{14}, \alpha^{16}, \alpha^{22}\}.$$

Thus, since the set of elements of $\mathbf{GF}(3) \subset \mathbf{GF}(3^3)$ is $\{0, 1, \alpha^{13}\}$, it follows that the set $\{\langle 1\rangle, \langle\alpha\rangle, \langle\alpha^3\rangle, \langle\alpha^9\rangle\}$ constitutes a hyperplane of $P(\mathbf{GF}(3^3))$. Therefore, by the proof of Singer's theorem, $1 + x + x^3 + x^9$ is the polynomial of a $(13, 4, 1)$ cyclic difference set and, consequently, $\{0, 1, 3, 9\}$ is a $(13, 4, 1)$ cyclic difference set. The complement of a $\left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right)$ Singer Difference Set has parameters $\left(\frac{q^{d+1}-1}{q-1}, q^d, q^{d-1}(q-1)\right)$. The complement $\{2, 4, 5, 6, 7, 8, 10, 11, 12\}$ of $\{0, 1, 3, 9\}$ is a $(13, 9, 6)$ cyclic difference set.

$x^3 + x^2 + 1$ is irreducible over $\mathbf{GF}(2)$. Let α be a root of $x^3 + x^2 + 1$ that generates

$\mathbf{GF}(2^3)^*$. Then the following correspondence specifies an isomorphism f between the two vector spaces $\mathbf{GF}(2^3)$ and $\mathbf{GF}(2)^3$:

$\mathbf{GF}(2^3)$	$\mathbf{GF}(2)^3$	$\mathbf{GF}(2^3)$	$\mathbf{GF}(2)^3$	$\mathbf{GF}(2^3)$	$\mathbf{GF}(2)^3$
0	$(0,0,0)$	1	$(0,0,1)$	α	$(0,1,0)$
α^2	$(1,0,0)$	α^3	$(1,0,1)$	α^4	$(1,1,1)$
α^5	$(0,1,1)$	α^6	$(1,1,0)$	α^7	$(0,0,1)$

It follows that $\mathrm{Ker}\,(Tr)/\{0\} = \{\alpha^3, \alpha^5, \alpha^6\}$. So $\{3,5,6\}$ is a $(7,3,1)$ Singer Difference Set. The complement of $\{3,5,6\}$ is $\{0,1,2,4\}$, a $(7,4,2)$ cyclic difference set.

2.2.3 Quadrics and Quadratic Sets

Let q be a prime, let $d \in \mathbb{N}$, let $\mathbf{V}$ be a d-dimensional vector space defined over $\mathbf{GF}(q)$, and let $\{\mathbf{v}_1, ..., \mathbf{v}_d\}$ be a basis for $\mathbf{V}$. For each $i, j \leq d$, let $a_{ij}, b_i \in \mathbf{GF}(q)$. Then the map $F : \mathbf{V} \to \mathbf{GF}(q)$ defined by the rule that

$$F\left(\sum_{i=1}^{d} b_i v_i\right) = \sum_{i,j=1}^{d} a_{ij} b_i b_j$$

is called a *quadratic form.*

For example, let $\mathbf{V}' = \mathbf{GF}(2^3)$ and let α generate the cyclic group $\mathbf{GF}(2^3)^*$. Then $\{\alpha, \alpha^2, \alpha^4\}$ is a basis for $\mathbf{V}'$. Consider the map $F' : \mathbf{GF}(2^3) \to \mathbf{GF}(2)$ defined by the rule that, for $\beta \in \mathbf{GF}(2^3)$,

$$F'(\beta) = \mathrm{Tr}\left(\beta^3\right).$$

For $\beta_1, \beta_2 \in \mathbf{GF}(2^3)$,

$$(\beta_1 + \beta_2)^2 = \beta_1^2 + \beta_2^2.$$

It follows that, for $a_i \in \mathbf{GF}(q)$,

$$\mathrm{Tr}\left(\left(\sum_{i=0}^{2} a_i \alpha^{2^i}\right)^3\right) = \mathrm{Tr}\left(\sum_{i=0}^{2} a_i \alpha^{2^i} \cdot \sum_{i=0}^{2} a_i \alpha^{2^{i+1}}\right)$$

$$= \left(a_0^2 + a_1 a_2\right)\mathrm{Tr}\left(\alpha^3\right) + \left(a_0 a_1 + a_2^2\right)\mathrm{Tr}\left(\alpha^5\right) + a_0 a_2 \mathrm{Tr}\left(\alpha^2\right) + a_1 a_0 \mathrm{Tr}\left(\alpha^4\right)$$

$$+ \left(a_1^2 + a_2 a_0\right)\mathrm{Tr}\left(\alpha^6\right) + a_2 a_1 \mathrm{Tr}\left(\alpha\right) = a_0 a_2 + a_1 a_0 + a_2 a_1.$$

So, F' is a quadratic form.

Let F be a quadratic form over a d-dimensional $\mathbf{GF}(q)$ vector space $\mathbf{V}$. Then the set Q of all points $\langle \mathbf{v} \rangle \backslash \{0\} \in P(\mathbf{V})$ such that $F(\mathbf{v}) = 0$ is called the *quadric of* $P(\mathbf{V})$ *corresponding to* F. For example, $Q' = \{\langle \alpha \rangle \backslash \{0\}, \langle \alpha^2 \rangle \backslash \{0\}, \langle \alpha^4 \rangle \backslash \{0\}\}$ is the quadric of $P(\mathbf{V}')$ corresponding to F'. Let β generate the cyclic group $\mathbf{G}$ of order $\frac{q^d-1}{q-1}$. Then can associate Q with the element $\sum a_i \beta^i$ of the group ring $\mathbb{Z}[\mathbf{G}]$ defined by the rule that

$$a_i = \begin{cases} 1 & \text{if } \langle \alpha^i \rangle \backslash \{0\} \in Q \\ 0 & \text{otherwise} \end{cases}.$$

For example, the group ring polynomial of Q' is $\beta + \beta^2 + \beta^4$.

The study of geometry from an axiomatic perspective, as it was pursued in Euclid, is called *synthetic geometry.* The study of geometry using coordinate systems is called *analytic geometry.* For example, Descartes coordinatized the plane and was thus able to study Euclidean geometry from an analytic perspective.

Projective spaces developed over vector spaces in general and quadrics in particular are analytic concepts. However, I was unable to find a complete analytic proof of the main theorem of this section in the literature; a partial proof is contained in [HJ83]. The synthetic analogue of a quadric is an object called a quadratic set.

Let P be a projective space and let $\mathcal{Q}$ be a subset of the point set of P. We say that a line of P is tangent to $\mathcal{Q}$ if it is contained in $\mathcal{Q}$ or if it intersects $\mathcal{Q}$ in exactly one point. The tangent space of a point p in $\mathcal{Q}$ is the set of all points that lie on lines that are tangent to $\mathcal{Q}$ and that pass through p. A set $\mathcal{Q}$ in the projective geometry P is called a *quadratic set* if it satisfies the following conditions:

(i) If a line intersects $\mathcal{Q}$ in three points, then it is contained in $\mathcal{Q}$.

(ii) For each point $p \in \mathcal{Q}$, the tangent space of p is either a hyperplane or the entire space P.

The notion of a quadratic set is due to F. Bueckenhout [Buc69], as is much of the basic theory pertaining to quadratic sets.

We wish to establish that the concept of a quadratic set is indeed an appropriate synthetic analogue of the concept of a quadric. In order to do so, we will require two lemmas about quadrics.

Lemma 2.2.3. *Let q be a prime, let $d \in \mathbb{N}$, let $\mathbf{V}$ be a vector space defined over $\mathbf{GF}(q)$, and let $\{\mathbf{v}_1, ..., \mathbf{v}_d\}$ be a basis for $\mathbf{V}$. Let $F : \mathbf{V} \to \mathbf{GF}(q)$ be a quadratic form defined by the rule that, for any $f_i \in \mathbf{GF}(q)$,*

$$F\left(\sum_{i=1}^{d} f_i \mathbf{v}_i\right) = \sum_{i,j=1}^{d} a_{ij} f_i f_j.$$

If the map $B : \mathbf{V} \times \mathbf{V} \to \mathbf{GF}(q)$ *is defined by the rule that*

$$B(\mathbf{v}, \mathbf{w}) = F(\mathbf{v} + \mathbf{w}) - F(\mathbf{v}) - F(\mathbf{w}),$$

then B *is a symmetric bilinear form.*

Proof. For $i = 1, ..., d$, let $b_i, c_i \in \mathbf{GF}(q)$. Let $\mathbf{v} = \sum_{i=1}^{d} b_i \mathbf{v}_i$ and let $\mathbf{w} = \sum_{i=1}^{d} c_i \mathbf{v}_i$. Then

$$B(\mathbf{v}, \mathbf{w}) = \sum_{i,j=1}^{d} a_{ij} (b_i + c_i)(b_j + c_j) - \sum_{i,j=1}^{d} a_{ij} b_i b_j - \sum_{i,j=1}^{d} a_{ij} c_i c_j$$

$$= \sum_{i,j=1}^{d} a_{ij} (b_i c_j + b_j c_i).$$

Consequently,

$$B(\mathbf{v}, \mathbf{w}) = B(\mathbf{w}, \mathbf{v})$$

and, if $\beta \in \mathbf{GF}(q)$, then

$$B(\beta \mathbf{v}, \mathbf{w}) = \beta B(\mathbf{v}, \mathbf{w}).$$

Furthermore, it is easy to verify that, if $\mathbf{u} \in \mathbf{V}$, then

$$B(\mathbf{u} + \mathbf{v}, \mathbf{w}) = B(\mathbf{u}, \mathbf{w}) + B(\mathbf{v}, \mathbf{w}).$$

It follows that B is a symmetric bilinear form. □

The map B is called the *symmetric bilinear form associated with* F.

Lemma 2.2.4. *Let* q *be a prime and let* $\mathbf{V}$ *be a vector space developed over* $\mathbf{GF}(q)$. *Let* $F : \mathbf{V} \to \mathbf{GF}(q)$ *be a quadratic form with associated symmetric bilinear form*

B and let Q be the quadric in $P(\mathbf{V})$ associated with F. Let $\langle \mathbf{p} \rangle \backslash \{0\} \in Q$. Then the tangent space $T_{\mathbf{p}}$ of $\langle \mathbf{p} \rangle \backslash \{0\}$ is $\{\langle \mathbf{x} \rangle \backslash \{0\} \in P(\mathbf{V}) \,|\, B(\mathbf{x}, \mathbf{p}) = 0\}$.

Proof. Let $\langle \mathbf{x} \rangle \backslash \{0\} \in Q$ and let ℓ be the line that passes through $\langle \mathbf{p} \rangle \backslash \{0\}$ and $\langle \mathbf{x} \rangle \backslash \{0\}$. Then, since $\langle \mathbf{p} \rangle \backslash \{0\}$, $\langle \mathbf{x} \rangle \backslash \{0\} \in Q$, for each t,

$$F(\mathbf{x} + t\mathbf{p}) = B(\mathbf{x}, t\mathbf{p}) + F(\mathbf{x}) + F(t\mathbf{p}) = tB(\mathbf{x}, \mathbf{p}) + t^2 F(\mathbf{p}) = tB(\mathbf{x}, \mathbf{p}).$$

$\ell \in T_{\mathbf{p}}$ if and only if, for each t, $F(\mathbf{x} + t\mathbf{p}) = 0$, i.e. if and only if $B(\mathbf{x}, \mathbf{p}) = 0$.
Let $\langle \mathbf{x} \rangle \backslash \{0\} \in P(\mathbf{V}) \setminus Q$ and let ℓ be the line through $\langle \mathbf{x} \rangle \backslash \{0\}$ and $\langle \mathbf{p} \rangle \backslash \{0\}$. Then, since $\langle \mathbf{p} \rangle \backslash \{0\} \in Q$, for each t, $F(\mathbf{x} + t\mathbf{p}) = tB(\mathbf{x}, \mathbf{p}) + F(\mathbf{x})$. So that $B(\mathbf{x}, \mathbf{p}) \neq 0$ if and only if ℓ intersects Q at the point $\langle \mathbf{x} + t_0\mathbf{p} \rangle \backslash \{0\}$, where $t_0 = \frac{-F(\mathbf{x})}{B(\mathbf{x}, \mathbf{p})}$. In other words, $\ell \in T_{\mathbf{p}}$ if and only if $B(\mathbf{x}, \mathbf{p}) = 0$. □

It follows easily from Lemma 2.2.4 that T_p is a subspace of $P(\mathbf{V})$.

Theorem 2.2.5. *Every quadric is a quadratic set.*

Proof. Let Q be a quadric with quadratic form F. Let $\langle \mathbf{a} \rangle \backslash \{0\}$, $\langle \mathbf{b} \rangle \backslash \{0\}$, and $\langle \mathbf{c} \rangle \backslash \{0\}$ be points of Q that all lie on the same line. Then, for some $t_0 \neq 0$, we can write $\mathbf{c} = \mathbf{a} + t_0\mathbf{b}$. So we have that

$$0 = F(\mathbf{a} + t_0\mathbf{b}) = F(\mathbf{a}) + t_0 F_1 + t_0^2 F(\mathbf{b}) = t_0 F_1,$$

where F_1 is some function of $\mathbf{a}$ and $\mathbf{b}$ that does not depend on t_0. Then $F_1 = 0$. Hence, for each t, $F(\mathbf{a} + t\mathbf{b}) = 0$. So the line is contained in Q.
Let $\langle \mathbf{p} \rangle \backslash \{0\}$ be a point of Q and let ℓ be a line of $P(\mathbf{V})$. We will show that ℓ intersects $T_{\mathbf{p}}$ in at least one point; by Theorem 2.1.1, this is sufficient to ensure

that $T_{\mathbf{p}}$ is either a hyperplane or the entire projective space. Let $\langle \mathbf{x} \rangle \backslash \{0\}$, $\langle \mathbf{u} \rangle \backslash \{0\}$ be points on ℓ. Suppose that $\langle \mathbf{x} \rangle \backslash \{0\}$ and $\langle \mathbf{u} \rangle \backslash \{0\}$ are not contained in $T_{\mathbf{p}}$. $\langle \mathbf{x} + t\mathbf{u} \rangle \backslash \{0\} \in T_{\mathbf{p}}$ if and only if

$$0 = B(\mathbf{x} + t\mathbf{u}, \mathbf{p}) = B(\mathbf{x}, \mathbf{p}) + tB(\mathbf{u}, \mathbf{p})$$

if and only if

$$t = -\frac{B(\mathbf{x}, \mathbf{p})}{B(\mathbf{u}, \mathbf{p})},$$

so ℓ intersects T_p in at least one point. It follows that Q is a quadratic set. □

Conversely, Bueckenhout [Bue69] has shown that every quadratic set is either a quadric or a type of object called an ovoid. Further, Segre [Seg54] has shown that every ovoid in a projective space of dimension 2 is a quadric. It is well known that if $d > 3$ and P is a projective space of dimension d, then there exist no ovoids in P (see [Tha74] for a proof of a more general result). There are ovoids that are not quadrics in projective spaces of dimension 3 [O'K96] but, for our purposes, projective spaces of odd dimension turn out to be of minimal interest. Consequently, we shall not discuss ovoids.

We shall now state the main result of this section. For a proof, see [BR98], Corollary 4.5.2 (although the result they prove is less general, it is not difficult to extend their result to the general case). A quadratic set is if it contains a point whose tangent space is the entire projective geometry.

Theorem 2.2.6. *Let q be a prime power and let d, f be such that $d = 2f$. Assume that Q is a non-degenerate quadric in $P\left(\mathbf{GF}\left(q^{d+1}\right)\right)$. Then the hyperplanes of $P\left(\mathbf{GF}\left(q^{d+1}\right)\right)$ intersect Q in sets of sizes λ, β, and γ and with multiplicities A, B,*

and C, respectively, where:

$$\lambda = \frac{q^{2f-1}-1}{q-1}, \quad A = \frac{q^{2f}-1}{q-1},$$

$$\beta = \lambda - q^{f-1}, \quad B = \frac{q^{2f}-q^f}{2},$$

$$\gamma = \lambda + q^{f-1}, \quad C = \frac{q^{2f}+q^f}{2}.$$

The set of hyperplanes that intersect Q in λ points is the set of tangent hyperplanes.

2.2.4 Building Circulant Weighing Matrices Using Quadrics

The next result appears in both [HJ83] and [ADJP95].

Theorem 2.2.7. *Let v, k, and λ be as in the statement of Singer's Theorem. Let D be the group ring polynomial (over the cyclic group $\mathbf{G} = \mathbf{GF}\left(q^{d+1}\right)^* / \mathbf{GF}(q)^*$ of order v) of a Singer Difference Set and let Q be the group ring polynomial of a non-degenerate quadric. Further, suppose that, for some r such that $(r, v) = 1$, $Q = D^{(r)}$. Then*

$$C = \frac{1}{q^{f-1}}\left(DQ^{(-1)} - \lambda \mathbf{G}\right)$$

is the group ring polynomial of a CW $\left(v, q^d\right)$.

Proof. Let α generate $\mathbf{G}$. For each j, the coefficient of α^j in $DQ^{(-1)}$ is equal to $|D\alpha^{-j} \cap Q|$. However, by the proof of Singer's Theorem, $\alpha^{-j}D$ is the group ring polynomial corresponding to a hyperplane. It follows, by Theorem 2.2.6, that the coefficients of C are all either 0 or ± 1. Further, recall that, since $Q = D^{(r)}$, Q is the

group ring polynomial of (v, k, λ) difference set. So,

$$CC^{(-1)} = \frac{1}{q^{f-1}}\left(DQ^{(-1)} - \lambda\mathbf{G}\right)\left(\frac{1}{q^{f-1}}\left(DQ^{(-1)} - \lambda\mathbf{G}\right)\right)^{(-1)} =$$

$$= \frac{1}{q^{2f-2}}\left((k-\lambda)^2 + 2(k-\lambda)\lambda\mathbf{G} + \lambda^2 v\mathbf{G} - 2k^2\lambda\mathbf{G} + \lambda^2 v\mathbf{G}\right) = q^{2f}.$$

□

For instance, let $q = d = 2$. Let α generate $GF\left(q^3\right)^*$. On page 72, we determined that $Q' = \{\langle\alpha\rangle\backslash\{0\}, \langle\alpha^2\rangle\backslash\{0\}, \langle\alpha^4\rangle\}\backslash\{0\}$ is a quadric in $P\left(\mathbf{GF}\left(2^3\right)\right)$. Further, on page 71, we determined that $D = \{\langle\alpha^3\rangle\backslash\{0\}, \langle\alpha^5\rangle\backslash\{0\}, \langle\alpha^6\rangle\backslash\{0\}\}$ is a hyperplane of $P\left(\mathbf{GF}\left(2^3\right)\right)$ corresponding to a $(7, 3, 1)$ Singer difference set. Therefore, by the proof of Singer's Theorem, the lines of $P\left(\mathbf{GF}\left(2^3\right)\right)$ are

$$D,\quad D\alpha = \{\langle\alpha^4\rangle\backslash\{0\}, \langle\alpha^6\rangle\backslash\{0\}, \langle 1\rangle\backslash\{0\}\},\quad D\alpha^2 = \{\langle\alpha^5\rangle\backslash\{0\}, \langle 1\rangle\backslash\{0\}, \langle\alpha\rangle\backslash\{0\}\},$$

$$D\alpha^3 = \{\langle\alpha^6\rangle\backslash\{0\}, \langle\alpha\rangle\backslash\{0\}, \langle\alpha^2\rangle\backslash\{0\}\},\quad D\alpha^4 = \{\langle 1\rangle\backslash\{0\}, \langle\alpha^2\rangle\backslash\{0\}, \langle\alpha^3\rangle\backslash\{0\}\},$$

$$D\alpha^5 = \{\langle\alpha\rangle\backslash\{0\}, \langle\alpha^3\rangle\backslash\{0\}, \langle\alpha^4\rangle\backslash\{0\}\},\quad D\alpha^6 = \{\langle\alpha^2\rangle\backslash\{0\}, \langle\alpha^4\rangle\backslash\{0\}, \langle\alpha^5\rangle\backslash\{0\}\}.$$

It follows, then, that $T_{\langle\alpha\rangle} = D\alpha^2$, $T_{\langle\alpha^2\rangle} = D\alpha^4$, and $T_{\langle\alpha^4\rangle} = D\alpha$, so that Q' is a non-degenerate quadric. Note that, since $Q' = \{\langle x\rangle\backslash\{0\} \in P\left(\mathbf{GF}\left(2^3\right)\right) : tr\left(x^3\right) = 0\}$, and since $(7, 5) = 1$, it follows that $Q' = D^{(5)}$ $\left(5 = 3^{-1}\right)$. Therefore, by Theorem 2.2.7,

$$D\left(Q'\right)^{(-1)} - \mathbf{G} = \left(\alpha^3 + \alpha^5 + \alpha^6\right)\left(\alpha^6 + \alpha^5 + \alpha^3\right) - \mathbf{G} = -1 + \alpha + \alpha^2 + \alpha^4$$

is the group ring polynomial corresponding to a $CW(7, 4)$.

The question that naturally arises from Theorem 2.2.7 is "how does one generate quadrics of the type specified in the statement of the theorem?" The following result is well known (see [HJ83], [ADJP95], or [JW92]).

Theorem 2.2.8. *Let q be a prime and let $d = 2f$. Let D be the Singer Difference Set. For some i, j, let $r = (q^i + q^j)^{-1}$. Further, suppose that $(r, v) = 1$. Then $D^{(r)}$ is a quadric.*

In [HJ83], the authors claimed that, so long as $q^i + q^j$ is not a power of q, $D^{(r)}$ is a non-degenerate quadric. However, Games [Gam86] showed that this is incorrect. He produced the following example: let $q = 2$, $d = 8$, and $r^{-1} = 1 + 8 = 9$, then the quadric $D^{(r)}$ turns out to be degenerate. Games also showed that degenerate quadrics of the type $D^{(r)}$ could be used to construct circulant weighing matrices, albeit ones of smaller weight (in both senses of the term).
Arasu, Dillon, Jungnickel, and Pott [ADJP95] were able to generate classes of non-degenerate quadrics of the type $D^{(r)}$. In particular, they proved the following result.

Theorem 2.2.9. *If q is an even prime and $r^{-1} = q+1$, then $D^{(r)}$ is a non-degenerate quadric. If q is an odd prime and $r^{-1} = 2$, then $D^{(r)}$ is a non-degenerate quadric.*

Of course, this left open the question of whether or not there were other non-degenerate quadrics that work and whether, if there are other such non-degenerate quadrics, the matrices derived thereby are inequivalent to one another. I have at least partially answered this question [Mil09]. Let ϕ be the euler toilent function, let q be a prime, and let $d = 2f$. Then, it turns out that there one can construct at least $\frac{\phi(d+1)}{2}$ inequivalent circulant weighing matrices using Theorem 2.2.7. Further, I found that the ratio of any of the cross-correlation values of any pair of

ternary sequences obtained from these circulant weighing matrices to the weight q^d is bounded in absolute value by a function that behaves roughly like $\frac{1}{q}$.

Consequently, by choosing d so that $\phi(d+1)$ is large enough, one can generate as many inequivalent ternary sequences with perfect periodic autocorrelation as one desires. And, by choosing q large enough, one can obtain sequences with as large weight (in the second sense of the term) and as "small" (relative to the weight) periodic cross-correlation as one desires.

2.3 The Relative Difference Set Construction

2.3.1 Relative Difference Sets and Their Connection to Group Developed Weighing Matrices

Let $\mathbf{G}$ be a group of size nm and let $\mathbf{N}$ be a normal subgroup of $\mathbf{G}$ of size n. A (m, n, k, λ) $\mathbf{G}$-*relative difference set* (relative to $\mathbf{N}$) is a subset R of $\mathbf{G}$ such that each $g \in \mathbf{G}\backslash\mathbf{N}$ has exactly λ representations as a "difference" $g_i g_j^{-1} = g$, where $g_i, g_j \in R$, and no element of $\mathbf{N}$ has such a representation. The normal subgroup $\mathbf{N}$ is sometimes referred to as the *forbidden set.* For example $\{1, 2, 4\}$ is a $(4, 2, 3, 1)$ relative difference set in $\mathbb{Z}_8$ with forbidden set $\{0, 4\}$. A relative difference set with $\mathbf{N} = \{e\}$ is a difference set. The existence of a (m, n, k, λ) $\mathbf{G}$-relative difference set with forbidden set $\mathbf{N}$ is equivalent to the existence of an element R of the group ring $\mathbb{Z}\mathbf{G}$ with $0, 1$ coefficients that satisfies the equation

$$RR^{(-1)} = k + \lambda(\mathbf{G} - \mathbf{N}).$$

This group ring element can of course be associated with a group developed matrix via the Cayley representation.

A cyclic relative difference set (a relative difference set defined over the cyclic group of order mn) could alternatively be regarded as equivalent to an element $r(x)$ of the ring $\mathbb{Z}[x]$ satisfying the equation

$$r(x)r(x^{-1}) = k + \lambda T_n(x^m)(T_m(x) - 1) \pmod{x^{mn} - 1}.$$

The next theorem is due to Elliot and Butson [BE66].

Theorem 2.3.1. *Let* $\mathbf{G}$ *be a group of order* mn, *let* $\mathbf{N}$ *be a normal subgroup of* $\mathbf{G}$ *of size* n, *and let* R *be a* (m, n, k, λ) $\mathbf{G}$*-relative difference set (relative to* $\mathbf{N}$*). If* $\mathbf{U}$ *is a normal subgroup of* $\mathbf{N}$, *then there exists a* $(m, n/|\mathbf{U}|, k, \lambda|\mathbf{U}|)$ $\mathbf{G}/\mathbf{U}$*-relative difference set (relative to* $\mathbf{N}/\mathbf{U}$*).*

Proof. Let σ be the canonical homomorphism from $\mathbf{G}$ to $\mathbf{G}/\mathbf{U}$ ($\sigma(g) = g\mathbf{U}$). Suppose that, for $g \neq h \in R$, $g\mathbf{U} = h\mathbf{U}$. Then $gh^{-1}\mathbf{U} = \mathbf{U}$, so $gh^{-1} \in \mathbf{U} \subset \mathbf{N}$. But this is impossible. So $\sigma(R)$ is a set of size k.

Every element from each coset of $\mathbf{N}$ (other than $\mathbf{N}$ itself) appears exactly λ times as a difference of elements of R. So each element of $(\mathbf{G}/\mathbf{U})\backslash(\mathbf{N}/\mathbf{U})$ has exactly $\lambda|\mathbf{U}|$ representations as a "difference" of elements of $\sigma(R)$. Further, since no element of $\mathbf{N}$ is a "difference" of elements of R, no element of $\sigma(\mathbf{N})$ is a "difference" of elements of $\sigma(R)$. □

In 1942, Bose generalized Singer's theorem [Bos42]; by using affine geometry and mimicking Singer's proof, Bose was able to construct a class of relative difference sets (actually, Bose obtained a partial result; the most general version of Bose's

Theorem was first proved by Elliot and Butson in 1966 [BE66]). The proof given here is from [BJL99].

Theorem 2.3.2. *Let q be a prime power and let $d \in \mathbb{N}$. Let $R = \{x \in \mathbf{GF}(q^d) : Tr_{q^d/q}(x) = 1\}$. Then R is a $(\frac{q^d-1}{q-1}, q-1, q^{d-1}, q^{d-2})$ cyclic relative difference set (relative to $N = \mathbf{GF}(q)^*$) in $\mathbf{GF}(q^d)^*$.*

Proof. Tr is a homomorphism from the additive group $\mathbf{G}$ of $\mathbf{GF}(q^d)$ onto $\mathbf{GF}(q)$. So R is non-empty. Let $x_0 \in R$. Then $R = x_0 + \mathrm{Ker}\,(\mathrm{Tr})$, so that R is an affine hyperplane, and

$$|R| = |\mathrm{Ker}\,(\mathrm{Tr})\,| = \frac{|\mathbf{GF}(q^d)|}{|\mathbf{GF}(q)|} = q^{d-1}.$$

So, for $g \in \mathbf{G}$, $Rg = \{(x_0+y)g : y \in \mathrm{Ker}\,(\mathrm{Tr})\}$. Now, $y \in R \cap Rg$ if and only if $y \in R$ and there exists $x \in R$ such that $y = gx$, i.e. such that $yx^{-1} = g$. If $g \in \mathbf{GF}(q)^*$, then $Rg = \{x \in \mathbf{GF}(q^d) : \mathrm{Tr}(x) = g\}$, so that $Rg \cap R = \varnothing$.

Fix $g \in \mathbf{GF}(q^d)/\mathbf{GF}(q)$. By the proof of Singer's Theorem, $g\mathrm{Ker}\,(\mathrm{Tr})$ is a subspace (distinct from $\mathrm{Ker}\,(\mathrm{Tr})$) of $\mathbf{GF}(q^d)$ of dimension $d-1$. So $g\mathrm{Ker}\,(\mathrm{Tr}) \cap \mathrm{Ker}\,(\mathrm{Tr})$ has dimension $d-2$. The restriction f of Tr to $g\mathrm{Ker}\,(\mathrm{Tr})$ is a homomorphism from $g\mathrm{Ker}\,(\mathrm{Tr})$ to $\mathbf{GF}(q)$. Since $\mathrm{Ran}\,(f)$ is a subspace of $\mathbf{GF}(q)$ that contains non-zero elements, $\mathrm{Ran}\,(f) = \mathbf{GF}(q)$. So, for each $t \in \mathbf{GF}(q)$,

$$|\{x \in g\mathrm{Ker}\,(\mathrm{Tr}) : \mathrm{Tr}(x) = t\}| = q^{d-2}.$$

It follows that

$$|\{x \in g(x_0 + \mathrm{Ker}\,(Tr)) : Tr(x) = 1\}| = q^{d-2}.$$

Thus, for any $g \in \mathbf{GF}(q^d)/\mathbf{GF}(q)$, $|R \cap Rg| = q^{d-2}$. □

For instance, let α be a root of the polynomial x^3-x+1, which is irreducible over $\mathbf{GF}(3)$. The correspondence between $\mathbf{GF}(3^3))$ and $\mathbf{GF}(3)^3$ is given in the following table.

1	$(0,0,1)$	α	$(0,1,0)$	α^2	$(1,0,0)$
α^3	$(0,1,2)$	α^4	$(1,2,0)$	α^5	$(2,1,2)$
α^6	$(1,1,1)$	α^7	$(1,2,2)$	α^8	$(2,0,2)$
α^9	$(0,1,1)$	α^{10}	$(1,1,0)$	α^{11}	$(1,1,2)$
α^{12}	$(1,0,2)$	α^{13}	$(0,0,2)$	α^{14}	$(0,2,0)$
α^{15}	$(2,0,0)$	α^{16}	$(0,2,1)$	α^{17}	$(2,1,0)$
α^{18}	$(1,2,1)$	α^{19}	$(2,2,2)$	α^{20}	$(2,1,1)$
α^{21}	$(1,0,1)$	α^{22}	$(0,2,2)$	α^{23}	$(2,2,0)$
α^{24}	$(2,2,1)$	α^{25}	$(2,0,1)$	α^{26}	$(0,0,1)$

Making use of this correspondence, it's easy to verify that

$$R = \{x \in \mathbf{GF}(3^3)^* : Tr(x) = 1\} = \{\alpha^5, \alpha^8, \alpha^{15}, \alpha^{17}, \alpha^{19}, \alpha^{20}, \alpha^{23}, \alpha^{24}, \alpha^{25}\}$$

is a $(13, 2, 9, 3)$ cyclic relative difference set with forbidden set $\{1, \alpha^{13}\}$.

Bose's Theorem and Theorem 2.3.1 imply that, for any prime power q, there exists a cyclic difference set with parameters $\left(\frac{q^d-1}{q-1}, q^{d-1}, q^{d-1} - q^{d-2}\right)$. These are the same parameters that the complements of Singer difference sets have (in fact, the cyclic difference sets obtained are the complements of Singer difference sets, see [BJL99]).

Let R be a (m, n, k, λ) $\mathbf{G}$-relative difference set. R has a *Waterloo decomposition* if $R = A \cup B$, where the group ring element $A - B$ satisfies $(A - B)(A - B)^{(-1)} = k$. The connection between relative difference sets and group developed weighing matrices appeared in [Rad80] and later in [ADJP95], but was not fully developed

until [ADLM01]. Later on in this chapter I will discuss the connection between relative difference sets and negacyclic weighing matrices.

Theorem 2.3.3. *The following coexist:*
(I) A (m, n, k, λ) $\mathbf{G}$*-relative difference set* R *with forbidden set* $\boldsymbol{N}$ *that has a Waterloo Decomposition* $R = A \cup B$.
(II) A $(m, 2n, k, \frac{\lambda}{2})$ $\mathcal{G} = \boldsymbol{G} \times \langle\theta\rangle$*-relative difference set* $\mathcal{R} = A + B\theta$, *with forbidden set* $\mathcal{N} = \mathbf{N} \times \langle\theta\rangle$, *where* θ *has order 2.*

Proof. Assume the existence of (I). Then

$$(A+B)(A+B)^{-1} = AA^{(-1)} + BB^{(-1)} + AB^{(-1)} + BA^{(-1)} = k + \lambda(\mathbf{G} - \mathbf{N})$$

and

$$(A-B)(A-B)^{(-1)} = AA^{(-1)} + BB^{(-1)} - AB^{(-1)} - BA^{(-1)} = k.$$

So, by adding these two equations together, we deduce that

$$AA^{(-1)} + BB^{(-1)} = k + \frac{\lambda}{2}(\mathbf{G} - \mathbf{N})$$

and, by subtracting the second equation from the first, we deduce that

$$AB^{(-1)} + BA^{(-1)} = \frac{\lambda}{2}(\mathbf{G} - \mathbf{N}).$$

Let $\mathcal{R} = A + B\theta$ be an element of $\mathbb{Z}\mathcal{G}$. Then

$$\mathcal{R}\mathcal{R}^{(-1)} = AA^{(-1)} + BB^{(-1)} + (AB^{(-1)} + BA^{(-1)})\theta = k + \frac{\lambda}{2}(\mathcal{G} - \mathcal{N}).$$

Assume the existence of (II). By reversing the reasoning from the first part of the proof, one can deduce that

$$(A-B)(A-B)^{(-1)} = k$$

and

$$(A+B)(A+B)^{(-1)} = k + \lambda(\mathbf{G} - \mathbf{N})$$

Suppose there is an element $x \in A \cap B$. Then $x, x\theta \in \mathcal{R}$ and

$$x(x\theta)^{-1} = (xx^{-1})\theta = \theta.$$

This, however, is impossible, since θ is in the forbidden set. Thus, A and B are disjoint and it follows that $R = A + B$ is the group ring element corresponding to (I). □

Corollary 2.3.4. *A (m, n, k, λ) relative difference set admits a Waterloo decomposition only if λ is even.*

Let q be an odd prime power. By Bose's Theorem, for any d, there exists a cyclic relative difference set with parameters $\left(\frac{q^d-1}{q-1}, q-1, q^{d-1}, q^{d-2}\right)$. So by Theorem 2.3.1, there exists a $\left(\frac{q^d-1}{q-1}, 2, q^{d-1}, \frac{2q^{d-2}}{q-1}\right)$ relative difference set. If d is odd, then $\frac{q^d-1}{q-1} = q^{d-1} + \cdots + q + 1$ is odd, so the cyclic group of order $2\frac{q^d-1}{q-1}$ can be written as a direct product $\mathbf{G} \times \langle\theta\rangle$, where $\mathbf{G}$ is the cyclic group of order $\frac{q^d-1}{q-1}$ and θ has order 2. Thus, we deduce the following result.

Theorem 2.3.5. *If q is an odd prime power and d is an odd integer then there exists a balanced CW $\left(\frac{q^d-1}{q-1}, q^{d-1}\right)$ obtained via a Waterloo Decomposition of a difference*

set. Further, if $q = 4k + 3$ *and* $t|\frac{q-1}{2}$, *then there exists a CW* $\left(\frac{q^d-1}{2t}, q^{d-1}\right)$ *obtained via a Waterloo Decomposition of a relative difference set.*

The second part of this result has not explicitly appeared in the literature but follows, via essentially the same line of reasoning as the first part, as an easy consequence of Theorem 2.3.3.

If $\langle\alpha\rangle$ is the cyclic group of order 26, $\langle\beta\rangle$ is the cyclic group of order 13, and $\langle\theta\rangle$ is the cyclic group of order 2, then $\langle\alpha\rangle$ is isomorphic to $\langle\beta\rangle \times \langle\theta\rangle$ via the map $\sigma : \alpha \longrightarrow (\beta, \theta)$. Under this isomorphism, the relative difference set R described in my earlier example corresponds to $\{(\beta^5, \theta), (\beta^8, 1), (\beta^2, \theta), (\beta^4, \theta), (\beta^6, \theta), (\beta^7, 1), (\beta^{10}, \theta),$ $(\beta^{11}, 1), (\beta^{12}, \theta)\}$. Thus, $-\beta^2 - \beta^4 - \beta^5 - \beta^6 + \beta^7 + \beta^8 - \beta^{10} + \beta^{11} - \beta^{12}$ is the Hall polynomial of a circulant balanced weighing matrix with parameters $(13, 9)$, as is its negation $\beta^2 + \beta^4 + \beta^5 + \beta^6 - \beta^7 - \beta^8 + \beta^{10} - \beta^{11} + \beta^{12}$. This group ring polynomial is obtained by decomposing the complement of a Singer difference set (p. 70), which has parameters $(13, 9, 6)$. Here is the corresponding circulant balanced

weighing matrix.

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

Now we will consider the case where q is an even prime power.

2.3.2 Background from Character Theory

Let $\mathbf{G}$ be an abelian group of exponent v and let $\chi : \mathbf{G} \to \mathbb{C}$ be a homomorphism. We say that χ is a *character of* $\mathbf{G}$. Throughout the remainder of this thesis, the notation ζ_v will denote a primitive v^{th} root of unity. Note that, for each $g \in \mathbf{G}$, there exists a number j such that $\chi(g) = \zeta_v^j$, so that $\chi\left(g^{-1}\right) = \overline{\chi\left(g\right)}$. Further, χ can

be extended to a ring homomorphism from $\mathbb{Z}[\mathbf{G}]$ to $\mathbb{Z}[\zeta_v]$ by the rule

$$\chi\left(\sum a_i g_i\right) = \sum a_i \chi\left(g_i\right).$$

Actually, characters can be defined over any group. However, all that is required for our purposes is the abelian sub-case and, by considering only the abelian characters, we greatly simplify our presentation. For a general account of group characters and of how abelian characters fit into the general case, see, for instance, [Ser96] or [Cra06]. The proofs given in this section are taken from [BJL99].

Let q be a prime power and let $d \in \mathbb{N}$. Consider the characters of the additive group $\mathbf{G}$ of $\mathbf{GF}(q^d)$. Each character χ can be regarded as a map defined by the rule $\chi(x) = \zeta_q^{\ell(x)}$, where ℓ is a function that maps $\mathbf{GF}(q^d)$ into $\mathbf{GF}(q)$. Since χ is a homomorphism, for $x, y \in \mathbf{G}$, $\zeta_q^{\ell(x+y)} = \chi(x+y) = \chi(x)\chi(y) = \zeta_q^{\ell(x)}\zeta^{\ell(y)} = \zeta_q^{\ell(x)+\ell(y)}$. Thus, $\ell(x+y) = \ell(x) + \ell(y)$. Let $a \in \mathbf{GF}(q)$. Then $\ell(ax) = \ell(x + x + \cdots + x) = \ell(x)+\ell(x)+\cdots+\ell(x) = a\ell(x)$. It follows that ℓ is a linear transformation from $\mathbf{GF}(q^d)$ to $\mathbf{GF}(q)$. By lemma 2.1.5 then, for each $x \in \mathbf{GF}(q^d)$, there exists $w \in \mathbf{GF}(q^d)$ such that $\ell(x) = Tr(wx)$. Since there are exactly q^d characters corresponding to q^d linear transformations, it follows that for each character χ of $\mathbf{G}$, there exists $w \in \mathbf{GF}\left(q^d\right)$ such that $\chi = \chi_w$, where χ_w is defined by the rule that $\chi_w(x) = \zeta_q^{\mathrm{Tr}(wx)}$.

Note that characters of an abelian group of order n form a group of order n under "pointwise" multiplication. The *character table* for an abelian group $\mathbf{G}$ is the square array whose rows are indexed by the characters of $\mathbf{G}$ and whose columns are indexed by the elements of $\mathbf{G}$. The entry in row χ column g is $\chi(g)$. Let $\langle y \rangle$ be the cyclic

group of order 4. Then the following is the character table for $\langle y \rangle$.

	1	y	y^2	y^3
χ_0	1	1	1	1
χ_1	1	$-i$	-1	i
χ_2	1	-1	1	-1
χ_3	1	i	-1	$-i$

We shall refer to the character that maps each element to 1 as the *principal character.* In the above example, χ_0 is the principal character. The following result states that the row or column sum of any but the first row or column of a character table is equal to 0.

Theorem 2.3.6. *(Character Orthogonality Relations) Let* $\mathbf{G}$ *be an abelian group of order* n *and let* χ_0 *be the principal character of* $\mathbf{G}$*. Then*

$$\sum_{\chi} \chi(g) = \begin{cases} n, & \text{if } g = 1 \\ 0, & \text{otherwise} \end{cases},$$

and

$$\sum_{g \in \mathbf{G}} \chi(g) = \begin{cases} n, & \text{if } \chi = \chi_0 \\ 0, & \text{otherwise} \end{cases}.$$

Proof.

$$\sum_{\chi} \chi(1) = \sum_{\chi} 1 = n.$$

Let $g \neq 1$. Then there exists a character χ^* such that $\chi^*(g) \neq 1$. Thus, since the characters form a group,

$$\chi^*(g)\sum_{\chi}\chi(g) = \sum_{\chi}(\chi^*\chi)(g) = \sum_{\chi}\chi(g).$$

Therefore,

$$\sum_{\chi}\chi(g) = 0.$$

Now,

$$\sum_{g\in\mathbf{G}}\chi_0(g) = \sum_{g\in\mathbf{G}}1 = n.$$

Let $\chi \neq \chi_0$ be a character of $\mathbf{G}$. Then there exists $h \in \mathbf{G}$ such that $\chi(h) \neq 1$. Therefore,

$$\chi(h)\sum_{g\in\mathbf{G}}\chi(g) = \sum_{g\in\mathbf{G}}\chi(h)\chi(g) = \sum_{g\in\mathbf{G}}\chi(gh) = \sum_{g\in\mathbf{G}}\chi(g).$$

Hence,

$$\sum_{g\in\mathbf{G}}\chi(g) = 0.$$

□

The following corollary states that the rows and columns of the character table of an abelian group of order n are orthogonal under the standard inner product over $\mathbb{C}^n$; it follows as an immediate consequence of Theorem 2.3.6, the fact that the characters of an abelian group form a group, and the fact that the inverse of a character χ is the character $\overline{\chi}$.

Corollary 2.3.7. *Let* $\mathbf{G}$ *be an abelian group of order* n, *let* $t \neq h \in \mathbf{G}$, *and let*

$\chi_a \neq \chi_b$ be two characters of $\mathbf{G}$. *Then*

$$\sum_{\chi} \chi(t)\overline{\chi(h)} = \sum_{g \in \mathbf{G}} \chi_a(g)\overline{\chi_b(g)} = 0.$$

The following result also proves to be useful; it allows us to glean information about the coefficients of a group ring element from its character values.

Theorem 2.3.8. *Let* $A = \sum_{g \in \mathbf{G}} a_g g \in \mathbb{C}[\mathbf{G}]$. *Then, for each* $h \in \mathbf{G}$,

$$a_h = \frac{1}{|\mathbf{G}|} \sum_{\chi \in \overline{\mathbf{G}}} \chi(A)\chi(h^{-1}).$$

Therefore, if for $B \in \mathbb{C}[\mathbf{G}]$ *we have that, for each character* χ, $\chi(A) = \chi(B)$, *it follows that* $A = B$.

Proof. By Theorem 2.3.6,

$$\sum_{\chi} \chi(A)\chi\left(h^{-1}\right) = \sum_{\chi} \sum_{g \in \mathbf{G}} a_g \chi(g)\chi\left(h^{-1}\right) = \sum_{g \in \mathbf{G}} \sum_{\chi} a_g \chi\left(gh^{-1}\right) = n a_h.$$

□

Corollary 2.3.9. *Let* $\mathbf{G} = \{g_1, ..., g_n\}$ *be an abelian group, let* $\mathbf{H}$ *be a subgroup of* $\mathbf{G}$, *and let* $A, B \in \mathbb{Z}[\mathbf{G}]$. *Suppose that, for each character* χ *of* $\mathbf{G}$ *that is nonprincipal on* $\mathbf{H}$, $\chi(A) = \chi(B)$. *Then* $A = B + X\mathbf{H}$, *for some* $X \in \mathbb{Z}[\mathbf{G}]$.

Proof. Let $C = \sum c_i g_i = A - B$. Let $g \in \mathbf{G}$. By Theorem 2.3.8,

$$c_g = \frac{1}{n} \sum_{\chi} \chi(C)\chi\left(g^{-1}\right).$$

Let $h \in \mathbf{H}$. By hypothesis, for each character χ that is nonprincipal on $\mathbf{H}$, $\chi(C) = 0$. Therefore, by Theorem 2.3.8,

$$c_{gh} = \frac{1}{n}\sum_{\chi}\chi(C)\chi\left((gh)^{-1}\right) = \frac{1}{n}\sum_{\chi}\chi(C)\chi\left(g^{-1}\right) = c_g.$$

Consequently, there exists $X \in \mathbb{Z}[\mathbf{G}]$ such that $C = X\mathbf{H}$. The result follows. □

2.3.3 The Walsh-Hadamard Transform

Discrete analogues of the Fourier Transform can be defined over finite groups (see, for instance, [SMA05], [MR97], and [SY92]). Again, although a general treatment is possible, we consider only the abelian case. Let $\mathbf{G}$ be a finite abelian group, let $f : \mathbf{G} \to \mathbb{C}$, and let χ be a character of $\mathbf{G}$. Then

$$\hat{f}(\chi) = \frac{1}{\sqrt{|G|}}\sum_{x\in\mathbf{G}} f(x)\chi\left(x^{-1}\right) = \frac{1}{\sqrt{|G|}}\sum_{x\in\mathbf{G}} f(x)\overline{\chi(x)}$$

is called the *Fourier transform* of f at χ. The definition we have given is not standard: in the book [SMA05] $|\mathbf{G}|$ occurs in place of $\sqrt{|\mathbf{G}|}$, but our definition here is implied by the way the transform is used to construct circulant weighing matrices in [ADLM01]. Note that since character values are roots of unity and since, for any θ, $e^{i\theta} = \sin\theta + i\cos\theta$, the Finite Fourier Transform, like the regular Fourier Transform, "represents" functions as a sum of trigonometric functions.

Let q be a prime power and let $d \in \mathbb{N}$. Consider the Fourier Transform defined over the additive group $\mathbf{G}$ of $\mathbf{GF}(q^d)$. For any function f defined over $\mathbf{G}$, this transform

can be seen as a function defined over $\mathbf{G}$ by the rule

$$\hat{f}(w) = \hat{f}(\chi_w) = \frac{1}{q^{d/2}} \sum_{x \in \mathbf{G}} f(x) \zeta_q^{Tr(wx)}.$$

In the special case that $q = 2$, the transform is given by

$$\hat{f}(w) = \frac{1}{q^{d/2}} \sum_{x \in \mathbf{G}} f(x)(-1)^{Tr(wx)}.$$

This is known as the *Walsh-Hadamard transform.* It was apparently discovered by Walsh [Wal23]. Note that, by Theorem 2.3.6, the character table of the additive group $\mathbf{G}$ of $\mathbf{GF}(2^d)$ is a $2^d \times 2^d$ Hadamard matrix H (matrices of this type are usually referred to as *Sylvester Hadamard matrices*). Label the elements of $\mathbf{G}$ $g_1, g_2, ..., g_{2^d}$. Let $\mathbf{f}$ be the row vector

$$\mathbf{f} = (f(g_1), f(g_2), ..., f(g_{2^d})).$$

Then the Walsh-Hadamard Transform could alternatively be defined by the rule

$$\hat{f}(w) = \frac{1}{2^{d/2}} \mathbf{f} H^T.$$

The following result is an analogue of Parseval's Theorem [Apo74].

Theorem 2.3.10. *Let* $\mathbf{G}$ *be a finite abelian group. For any complex functions* f_1, f_2 *defined on* $\mathbf{G}$, $\sum_\chi \hat{f}_1(\chi)\overline{\hat{f}_2(\chi)} = \sum_{x \in \mathbf{G}} f_1(x)\overline{f_2(x)}$.

Proof.

$$\sum_\chi \hat{f}_1(\chi)\overline{\hat{f}_2(\chi)} = \sum_\chi \frac{1}{|\mathbf{G}|} \sum_{x \in \mathbf{G}} f_1(x)\overline{\chi(x)} \sum_{x \in \mathbf{G}} \overline{f_2(x)}\chi(x)$$

$$= \frac{1}{|\mathbf{G}|} \sum_{x_1,x_2 \in \mathbf{G}} f_1(x_1)\overline{f_2(x_2)} \sum_{\chi} \chi(x_1^{-1})\chi(x_2).$$

By Theorem 2.3.6, $x_1 \neq x_2$ implies that

$$\sum_{\chi} \overline{\chi(x_1)}\chi(x_2) = 0.$$

Therefore,

$$\sum_{\chi} \hat{f}_1(\chi)\overline{\hat{f}_2(\chi)} = \sum_{x \in \mathbf{G}} f_1(x)\overline{f_2(x)},$$

as required. □

2.3.4 The Construction for $q = 2^t$

Assume that q is a power of 2 and that d is an odd integer. In what follows, Tr refers to $\mathrm{Tr}_{\mathbf{GF}(q^d)/\mathbf{GF}(2)}$; for other traces, subscripts will be given explicitly. By Bose's Theorem, the affine hyperplane

$$R = \{x \in \mathbf{GF}(q^d) : Tr_{\mathbf{GF}(q^d)/\mathbf{GF}(q)}(x) = 1\}$$

is a cyclic relative difference set with parameters $\left(\frac{q^d-1}{q-1}, q-1, q^{d-1}, q^{d-2}\right)$. The authors of [ADLM01] were able to show that R admits a Waterloo Decomposition. Their proof makes use of the affine quadric $\{x \in \mathbf{GF}\left(q^d\right) : \mathrm{Tr}\left(x^{q+1}\right) = 0\}$. Note that, by Corollary 2.3.4, if q is an odd prime power, then the affine hyperplane does not admit a Waterloo Decomposition.

Theorem 2.3.11. *Let $\epsilon = 0, 1$ and let $C_\epsilon = \{1+\gamma^q+\gamma^{q^{-1}} : \gamma \in \mathbf{GF}(q^d), Tr(\gamma^{q+1}+\gamma) = \epsilon\}$. Then the relative difference set R has a Waterloo Decomposition $R = A+B$*

such that $\{A, B\} = \{C_0, C_1\}$ *(as unordered sets).*

Proof. Define a function $Q : \mathbf{GF}(q^d) \to \mathbf{GF}(q)$ by the rule $Q(x) = Tr(x^{q+1})$ and define the real-valued function $\mathcal{Q}$ by the rule $\mathcal{Q}(x) = (-1)^{Q(x)}$. Since q is a power of 2 and d is odd, $(q+1, q-1) = (q+1, q^d-1) = 1$ (since $q^d-1 = (q-1)(q^{d-1}+\cdots+q+1)$). Thus, since $\mathbf{GF}\left(q^d\right)^*$ has order $q^d - 1$, each element of $\mathbf{GF}(q^d)$ has the form x^{q+1}, for some $x \in \mathbf{GF}(q^d)$.

Let $\delta_{x,y}$ be defined so that

$$\delta_{x,y} = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases}.$$

Since Tr is an onto map, there exists $\beta \in \mathbf{GF}\left(q^d\right)$ such that $\mathrm{Tr}\left(\beta\right) = 1$. Therefore,

$$|\{x \in \mathbf{GF}(q^d) | \mathrm{Tr}(x) = 1| = |\beta + \mathrm{Ker}\left(\mathrm{Tr}\right)| = |\mathrm{Ker}\left(\mathrm{Tr}\right)|.$$

It follows that, for each $\alpha \in \mathbf{GF}(q^d)$,

$$(1) \qquad q^d \delta_{1,\alpha} = \sum_{x \in \mathbf{GF}(q^d)} (-1)^{\mathrm{Tr}([\alpha^{q+1}+1]x^{q+1})} = \sum_{x \in \mathbf{GF}(q^d)} (-1)^{Q(\alpha x)+Q(x)}$$

$$= \sum_{x \in \mathbf{GF}(q^d)} \mathcal{Q}(\alpha x)\mathcal{Q}(x) = \sum_{x \in \mathbf{GF}(q^d)} \hat{\mathcal{Q}}(\alpha x)\hat{\mathcal{Q}}(x),$$

where $\hat{\mathcal{Q}}$ is the Walsh-Hadamard Transform of $\mathcal{Q}$ and the last equality is a consequence of the version of Parseval's Theorem proved in the previous section.

Let $\beta \in \mathbf{GF}(q^d)$. Then

$$\hat{\mathcal{Q}}(\beta) = \frac{1}{q^{d/2}} \sum_{x \in \mathbf{GF}(q^d)} (-1)^{\mathrm{Tr}(x^{q+1}+\beta x)}.$$

Note that, for $x, y \in \mathbf{GF}\left(q^d\right)$,

$$(x+y)^{q+1} = x^{q+1} + y^{q+1} + x^q y + x y^q.$$

Further, note that, since $\left(q, q^d - 1\right) = 1$, each element of $\mathbf{GF}\left(q^d\right)$ can be written in the form x^q, for some $x \in \mathbf{GF}\left(q^d\right)$. So, since $\mathbf{GF}(q^d)$ has characteristic 2 and since, for each $x \in \mathbf{GF}\left(q^d\right)$, $\mathrm{Tr}(x^q) = \mathrm{Tr}(x)$,

$$(\hat{\mathcal{Q}}(\beta))^2 = \frac{1}{q^d} \sum_{x \in \mathbf{GF}(q^d)} (-1)^{\mathrm{Tr}(x^{q+1}+\beta x)} \sum_{y \in \mathbf{GF}(q^d)} (-1)^{\mathrm{Tr}(y^{q+1}+\beta y)}$$

$$= \frac{1}{q^d} \sum_{x \in \mathbf{GF}(q^d)} (-1)^{\mathrm{Tr}(x^{q+1}+\beta x)} \sum_{y \in \mathbf{GF}(q^d)} (-1)^{\mathrm{Tr}((x+y)^{q+1}+\beta(x+y))}$$

$$= \frac{1}{q^d} \sum_{y \in \mathbf{GF}(q^d)} (-1)^{\mathrm{Tr}(y^{q+1}+\beta y)} \sum_{x \in \mathbf{GF}(q^d)} (-1)^{\mathrm{Tr}(x^q y + y^q x)}$$

$$= \frac{1}{q^d} \sum_{y \in \mathbf{GF}(q^d)} (-1)^{\mathrm{Tr}(y^{q+1}+\beta y)} \sum_{x \in \mathbf{GF}(q^d)} (-1)^{\mathrm{Tr}([y^{q^2}+y]x)}.$$

But $\sum_{x \in \mathbf{GF}(q^d)} (-1)^{\mathrm{Tr}([y^{q^2}+y]x)} = 0$ unless $y^{q^2} + y = 0$. Since d is odd, $\mathbf{GF}\left(q^2\right)$ is not a subfield of $\mathbf{GF}\left(q^d\right)$. Thus, $y^{q^2} + y = 0$ if and only if $y \in \mathbf{GF}\left(q\right)$. So

$$(\hat{\mathcal{Q}}(\beta))^2 = \sum_{y \in \mathbf{GF}(q)} (-1)^{\mathrm{Tr}(y^{q+1}+\beta y)}.$$

By Lemma 2.1.6,

$$\mathrm{Tr}(y^{q+1}+\beta y) = \mathrm{Tr}_{\mathbf{GF}(q)/\mathbf{GF}(2)}(\mathrm{Tr}_{\mathbf{GF}(q^d)/\mathbf{GF}(q)}(y^{q+1}+\beta y))$$

$$= \mathrm{Tr}_{\mathbf{GF}(q)/\mathbf{GF}(2)}(\mathrm{Tr}_{\mathbf{GF}(q^d)/\mathbf{GF}(q)}([1+\beta]y))$$

$$= \mathrm{Tr}_{\mathbf{GF}(q)/\mathbf{GF}(2)}(\mathrm{Tr}_{\mathbf{GF}(q^d)/\mathbf{GF}(q)}(1+\beta)y)$$

$$= \mathrm{Tr}_{\mathbf{GF}(q)/\mathbf{GF}(2)}((1+\mathrm{Tr}_{\mathbf{GF}(q^d)/\mathbf{GF}(q)}(\beta))y).$$

By way of explanation for the final equality, note that, since d is odd,

$$\mathrm{Tr}_{\mathbf{GF}(q^d)/\mathbf{GF}(q)}(1) = 1.$$

It follows that

$$(\hat{\mathcal{Q}}(\beta))^2 = \sum_{y\in\mathbf{GF}(q)} (-1)^{\mathrm{Tr}_{\mathbf{GF}(q)/\mathbf{GF}(2)}\left((1+\mathrm{Tr}_{\mathbf{GF}(q^d)/\mathbf{GF}(q)}(\beta))y\right)} = q\delta_{1,\mathrm{Tr}_{\mathbf{GF}(q^d)/\mathbf{GF}(q)}(\beta)}.$$

So the $\{-1,0,1\}$ valued function $E = q^{-1/2}\hat{\mathcal{Q}}$ has support R. Furthermore, by (1), for each $\alpha \in \mathbf{GF}(q^d)$,

$$q^{d-1}\delta_{1,\alpha} = \sum_{x\in\mathbf{GF}(q^d)} E(\alpha x)E(x).$$

Since $E(0) = 0$, we have that for each $\alpha \in \mathbf{GF}(q^d)^*$,

$$q^{d-1}\delta_{1,\alpha} = \sum_{x\in\mathbf{GF}(q^d)^*} E(\alpha x)E(x).$$

Let x be a generator for $\mathbf{GF}(q^d)^*$. Let C be the element of the group ring $\mathbb{Z}\left[\mathbf{GF}(q^d)^*\right]$

such that $E(x^t)$ is the coefficient of x^t in C. It then follows directly from the above equality that $CC^{(-1)} = q^{d-1}$. So we have obtained a Waterloo Decomposition of R. The remainder of the proof is devoted to finding an explicit formula for this decomposition.

Again, note that, since d is odd, $y = y^{q^2}$ if and only if $y \in \mathbf{GF}(q)$. It follows, by virtue of a slight modification of my proof of Theorem 2.1.7, that

$$\mathrm{Ker}\left(\mathrm{Tr}_{\mathbf{GF}(q^d)/\mathbf{GF}(q)}\right) = \{\gamma + \gamma^{q^2} : \gamma \in \mathbf{GF}\left(q^d\right)\}$$

(recall that we are working in a field of characteristic 2). For any $y \in \mathbf{GF}\left(q^d\right)$, $\mathrm{Tr}(y^{q^{-1}}) = \mathrm{Tr}(y)$. Consequently (since $x \to x^{q^{-1}}$ is an automorphism of $\mathbf{GF}\left(q^d\right)$),

$$\mathrm{Ker}\left(\mathrm{Tr}_{\mathbf{GF}(q^d)/\mathbf{GF}(q)}\right) = \{\gamma^{q^{-1}} + \gamma^q : \gamma \in \mathbf{GF}\left(q^d\right)\}.$$

Therefore, since $\mathrm{Tr}_{\mathbf{GF}\left(q^d\right)/\mathbf{GF}(q)}(1) = 1$,

$$R = \{1 + \gamma^{q^{-1}} + \gamma^q : \gamma \in \mathbf{GF}(q^d)\}.$$

For any $\gamma \in \mathbf{GF}(q^d)$,

$$\hat{\mathcal{Q}}(1 + \gamma^q + \gamma^{q^{-1}}) = \frac{1}{q^{d/2}} \sum_{x \in \mathbf{GF}(q^d)} (-1)^{\mathrm{Tr}(x^{q+1} + (1+\gamma^q+\gamma^{q^{-1}})x)}$$

$$= \frac{1}{q^{d/2}} \sum_{x \in \mathbf{GF}(q^d)} (-1)^{\mathrm{Tr}((x+\gamma)^{q+1} + (1+\gamma^q+\gamma^{q^{-1}})(x+\gamma))}$$

$$= \frac{1}{q^{d/2}} \sum_{x \in \mathbf{GF}(q^d)} (-1)^{\mathrm{Tr}(x^{q+1} + x^q\gamma + x\gamma^q + \gamma^{q+1} + x + \gamma + x\gamma^q + \gamma^{q+1} + x^q\gamma + \gamma^{q^{-1}} + 1)}$$

$$= \frac{1}{q^{d/2}} \sum_{x \in \mathbf{GF}(q^d)} (-1)^{\mathrm{Tr}(x^{q+1}+x+\gamma+\gamma^{q^{-1}+1})}$$

$$= \frac{1}{q^{d/2}} \sum_{x \in \mathbf{GF}(q^d)} (-1)^{\mathrm{Tr}(x^{q+1}+x)} (-1)^{\mathrm{Tr}\left(\gamma^{q+1}+\gamma\right)} = (-1)^{Tr(\gamma^{q+1}+\gamma)} \hat{\mathcal{Q}}(1).$$

It follows that C_0 and C_1 satisfy the relations given in the statement of the theorem.

□

By way of an example, consider the multiplicative group $\mathbf{GF}(64)^* = \mathbf{GF}(4^3)^*$ of the finite field of order 64. Let α generate this group. Then one can verify by straightforward calculations that

$$R = \{1 + \gamma^4 + \gamma^{16} : \gamma \in \mathbf{GF}(64)^*\}$$

$$= \{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^9, \alpha^{13}, \alpha^{16}, \alpha^{18}, \alpha^{19}, \alpha^{26}, \alpha^{32}, \alpha^{36}, \alpha^{38}, \alpha^{41}, \alpha^{52}\},$$

and that

$$C_0 = \{1, \alpha^9, \alpha^{13}, \alpha^{18}, \alpha^{19}, \alpha^{26}, \alpha^{36}, \alpha^{38}, \alpha^{41}, \alpha^{52}\},$$

and, finally, that

$$C_1 = \{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}\}.$$

It then follows from Theorem 2.3.11 that

$$1 - \alpha - \alpha^2 - \alpha^4 - \alpha^8 + \alpha^9 + \alpha^{13} - \alpha^{16} + \alpha^{18} + \alpha^{19} + \alpha^{26} - \alpha^{32} + \alpha^{36} + \alpha^{38} + \alpha^{41} + \alpha^{52}$$

is the group ring polynomial of a $CW(63, 16)$.

Theorem 2.3.3 and Theorem 2.3.11 imply that, for each even prime power q and each odd number d, there exists a $\mathcal{G} = \mathbf{G} \times \langle\theta\rangle$ relative difference set with parameters

$\left(\frac{q^d-1}{q-1}, 2(q-1), q^{d-1}, \frac{1}{2}q^{d-2}\right)$, where $\mathbf{G}$ is the cyclic group of order q^d-1, $\langle\theta\rangle$ is the cyclic group of order 2 (as a consequence, $\mathcal{G}$ is also cyclic), and the forbidden set is $\mathbf{N}\times\langle\theta\rangle$ (for some normal subgroup $\mathbf{N}$ of $\mathbf{G}$). So Elliot and Butson's result (Theorem 2.3.1) implies that, for each divisor t of $q-1$, there exists a relative difference set with parameters $\left(\frac{q^d-1}{t}, 2\frac{q-1}{t}, q^{d-1}, \frac{tq^{d-2}}{2}\right)$ in the cylic group $\mathbf{H}\times\langle\theta\rangle$, for some subgroup $\mathbf{H}$ of $\mathbf{G}$, and with forbidden set $\mathbf{U}\times\langle\theta\rangle$, for some normal subgroup $\mathbf{U}$ of $\mathbf{N}$. By Theorem 2.3.3, the next theorem follows as a consequence.

Theorem 2.3.12. *Let q be a power of 2, let d be odd, and let $t|(q-1)$. Then there exists a circulant weighing matrix with parameters $\left(\frac{q^d-1}{t}, q^{d-1}\right)$ that can be obtained via a Waterloo Decomposition of a relative difference set.*

This construction is relatively new (2001). As we have established, before it was discovered, it was already known that for each prime power q and each odd $d\in\mathbb{N}$, there exists a $CW\left(\frac{q^d-1}{q-1}, q^{d-1}\right)$. It then follows by Lemma 1.5.2, part (i), that, for each s, there exists a $CW\left(s\frac{q^d-1}{q-1}, q^{d-1}\right)$ and hence, in particular, for each $t|(q-1)$, there exists a $CW\left(\frac{q^d-1}{t}, q^{d-1}\right)$. However, for $t<q-1$ (and for q even), these matrices are inequivalent to the ones generated by the relative difference set construction. Two circulant weighing matrices, with group ring polynomials W_1 and W_2, respectively, of the same order and the same weight are equivalent only if $\mathrm{Supp}(W_1)$ and $\mathrm{Supp}(W_2)$ are equivalent (under the circulant weighing matrix equivalence operations). However, suppose that W_1 is generated by applying Lemma 1.5.2, part (i), to a smaller circulant weighing matrix and that W_2 is obtained via a Waterloo Decomposition of a relative difference set. Then, under any equivalence operation e, $e(\mathrm{Supp}(W_1))(e(\mathrm{Supp}(W_1)))^{-1}$ is a group ring element with nonzero coefficients only for elements of some proper subgroup of $\mathbf{G}$. On the other hand,

for any equivalence operation f, $f(\mathrm{Supp}(W_2))(f(\mathrm{Supp}(W_2)))^{-1} = k + \lambda(\mathbf{G} - \mathbf{N})$, where N is some normal subgroup of $\mathbf{G}$. In particular, the latter group ring element has a nonzero coefficient for some generator of $\mathbf{G}$, whereas the former does not. It follows that W_1 and W_2 are inequivalent. The fact that it can generate multiple inequivalent circulant weighing matrices in some orders is the primary reason that, for q even, the relative difference set approach is an improvement on the previous projective geometry approach.

The existence of the circulant weighing matrix derived in the last example was actually known before this construction was discovered. In 1998, Epstein [Eps98] discovered, via computer search, the existence of the circulant weighing matrix in question and that it is the only $CW(63, 16)$, up to equivalence, other than the one that can be obtained by applying Lemma 1.5.2, part (i), to a $CW(21, 16)$ (circulant weighing matrices with these parameters can be derived from both the relative difference set construction and the projective geometry construction; Epstein found, by another computer search, that there is, up to equivalence, only one of these).

Simone Severeni conjectured (personal correspondence with Dr. Craigen, 2009) that, for every $\epsilon > 0$, there exists a $W(n, w)$ W such that the ratio of any of the off diagonal entries of $\mathrm{abs}(W)\mathrm{abs}(W)^{(-1)}$ to the weight w is smaller than epsilon. Note the the class of circulant weighing matrices given in Theorem 2.3.11 proves this conjecture true, whereas the class of circulant weighing matrices generated by decomposing the complements of Singer difference sets does not.

One might ask whether it is possible to obtain a circulant weighing matrix via a Waterloo Decomposition of a relative difference set with parameters $\left(\frac{q^d-1}{q-1}, 2(q-1), q^{d-1}, \frac{1}{2}q^{d-2}\right)$ (d odd; q a power of 2). In fact, this is the case, as was

shown in [LMS02], whose authors made use of some of the same methods used in the proof of Theorem 2.3.11.

2.3.5 Constructing Negacyclic Weighing Matrices

Consider the incidence structure $S = (\mathcal{P}, \mathcal{B}, \mathcal{I})$. We say that S is a $(m, n, k, \lambda_1, \lambda_2)$ *divisible design* if the point set $\mathcal{P}$ can be partitioned into m disjoint classes, each of which consist of n points, such that the following three properties are satisfied:
(I) Each pair of points from a single point class is contained in exactly λ_1 blocks.
(II) Each pair of points from distinct point classes is contained in exactly λ_2 blocks.
(III) Each block is incident with exactly k points.
Note that the class of divisible designs contains the class of balanced incomplete block designs. Further, if a $CW(mn, k)$ W is obtained via a Waterloo Decomposition of a (m, n, k, λ) relative difference set, where $n > 1$, then abs(W) is not the incidence matrix of a balanced incomplete block design. It is, however, the incidence matrix of a divisible design with $\lambda_1 = 0$. In light of this fact, if W is a weighing matrix such that $abs(W)$ is the incidence matrix of a divisible design, then we will say that W is a *divisible* weighing matrix. There is some historical precedence for this definition. In 1977, Berman [Ber77] used techniques from projective and affine geometry to prove the following result.

Theorem 2.3.13. *(I) Let q be an odd prime power and let t be an odd natural number. Then there exists a divisible NW $\left(\frac{q^{t+1}-1}{2(q-1)}, q^{t-1}\right)$.*
(II) Let q be an odd prime power and let $t \in \mathbb{N}$. Then there exists a divisible NW $\left(\frac{q^t-1}{2}, q^{t-1}\right)$.
(III) Let $t \in \mathbb{N}$ be odd and let p be an odd prime of the form $4k+3$ (for some k).

Let $d, r \in \mathbb{N}$ be such that $d < r$ and $d|r$. Then there exists a NW $\left(\frac{(p^r)^t-1}{2(p^d-1)}, (p^r)^{t-1}\right)$.

There is a connection between relative difference sets and negacyclic weighing matrices. Versions of this connection have appeared in [DGS71] and [ADJP95]. In [DGS71], the authors proved the following result.

Theorem 2.3.14. *There exists a $(v, 2, v-1, \frac{v-2}{2})$ cyclic relative difference set if and only if there exists a negacyclic conference matrix with parameters $(v, v-1)$.*

Corollary 2.3.15. *Let q be an odd prime power. Then there exists a $NW(q+1, q)$.*

The corollary follows from Theorem 2.3.2, with $d = 1$. In [ADJP95], the authors prove the following.

Theorem 2.3.16. *If there exists a cyclic relative difference set with parameters $(m, 2, k, \lambda)$, then there exists a balanced $NW(m, k)$.*

Corollary 2.3.17. *Let q be an odd prime power and let d be any integer. Then there exists a balanced negacyclic weighing matrix with parameters $\left(\frac{q^d-1}{q-1}, q^{d-1}\right)$.*

Again, the Corollary follows from Theorem 2.3.2.

Here is a more general construction of negacyclic weighing matrices from relative difference sets than appears in the literature. I obtained the next result by a fairly straightforward extension of the proof of Theorem 2.3.14.

Theorem 2.3.18. *Let R be a (m, n, k, λ) cyclic relative difference set and let n be even. Let $a \in \mathbb{N}$, $b \in 2\mathbb{N}$ be such that $ab = n$ Then there exists a divisible $NW(am, k)$ W such that $abs(W)$ is the incidence matrix of a cyclic relative difference set with parameters $(m, a, k, b\lambda)$.*

Proof. Let $r(x)$ be the polynomial associated with R. Then

$$r(x)r(x^{-1}) \equiv k + \lambda\left(T_n\left(x^m\right)\right)\left(T_m(x) - 1\right) \pmod{\langle x^{mn} - 1\rangle}.$$

It follows that

$$r(x)r(x^{-1}) \equiv k + \lambda T_a(x^m)T_b(x^{am})(T_m(x) - 1) \pmod{\langle x^{mn} - 1\rangle}.$$

Since b is even, every root of $x^{am}+1$ is also a root of $x^{mn}-1$. Thus, $(x^{am}+1) \mid (x^{mn}-1)$. Further, $(x^{am}+1) \mid T_b(x^{am})$. It follows that

$$r(x)r(x^{-1}) \equiv k \pmod{\langle x^{am} + 1\rangle}.$$

The proof of Theorem 2.3.1 implies that $r(x) \pmod{\langle x^{am}+1\rangle}$ is a $0, \pm 1$ polynomial. Therefore, $r(x) \pmod{\langle x^{am}+1\rangle}$ is the nega-Hall polynomial of a $NW(am, k)$. Since $(x^{am}-1) \mid (x^{mn}-1)$,

$$r(x)r(x^{-1}) \equiv k + b\lambda T_a(x^m)(T_m(x) - 1) \pmod{\langle x^{am} - 1\rangle}.$$

The proof of Theorem 2.3.1 implies that $r(x) \pmod{\langle x^{am}-1\rangle}$ is a $0, 1$ polynomial. Therefore, $r(x) \pmod{\langle x^{am}-1\rangle}$ is the Hall polynomial of a cyclic relative difference set with parameters $(m, a, k, b\lambda)$. □

By Theorem 2.3.2 then, we infer the following result.

Corollary 2.3.19. *Let q be an odd prime power, let d be a positive integer, and let $c \mid \frac{q-1}{2}$. Then there exists a divisible NW $\left(\frac{q^d-1}{2c}, q^{d-1}\right)$ W such that abs(W) is the inci-*

dence matrix of a cyclic relative difference set with parameters $\left(\frac{q^d-1}{q-1}, \frac{q-1}{2c}, q^{d-1}, 2cq^{d-2}\right)$.

Cleary, Corollary 2.3.19 implies the $\Longrightarrow$ direction of Corollaries 2.3.15 and 2.3.17. In fact, it also implies Theorem 2.3.13. Note that (I) follows by a substitution of q^2 for q while (II) and (III) are direct Corollaries. Corollary 2.3.19 also yields some (apparently) new negagcyclic weighing matrices.

For instance, let $q = 19$, let $d = 2$, and let α be a generator of $\mathbf{GF}(361)^*$.

$$R = \{\alpha, \alpha^4, \alpha^{19}, \alpha^{31}, \alpha^{32}, \alpha^{76}, \alpha^{87}, \alpha^{125}, \alpha^{206}, \alpha^{213}, \alpha^{215}, \alpha^{223}, \alpha^{229}, \alpha^{248}, \alpha^{277}, \alpha^{282},$$

$$\alpha^{314}, \alpha^{318}, \alpha^{340}\}$$

is the $(20, 18, 19, 1)$ cyclic relative difference set $\{\gamma \in \mathbf{GF}(361) : Tr(\gamma) = 1\}$. Note that $\frac{361-1}{6} = 60$. By reducing the polynomial corresponding to R modulo $x^{60} + 1$, we deduce that

$$\theta(x) = x+x^4+x^8-x^{14}-x^{16}-x^{18}+x^{19}-x^{26}-x^{27}+x^{31}+x^{32}-x^{33}-x^{35}+x^{37}-x^{40}+x^{42}$$

$$-x^{43} - x^{49}$$

is the nega-Hall polynomial of a divisible $NW(60, 19)$. The existence of this matrix is not implied by any of the other constructions I have outlined.

It's interesting to compare Corollary 2.3.19 to Theorem 2.3.5. The classical cyclic relative difference sets can be used to construct negacyclic weighing matrices in orders for which they cannot be used to construct circulant weighing matrices.

By closely mimicking the proof of Theorem 2.3.14 given in [DGS71], one can obtain the following partial converse to Theorem 2.3.18.

Theorem 2.3.20. *Let W be a $NW(mn, k)$ such that $abs(W)$ is the incidence matrix of a (m, n, k, λ) cyclic relative difference set. Then λ is even and there exists a $\left(m, 2n, k, \frac{\lambda}{2}\right)$ cyclic relative difference set.*

Proof. Let $r(x)$ be the nega-Hall polynomial of W. Let $r(x) = f(x) - g(x)$ and let $\theta(x) = f(x) + x^{mn}g(x)$. Then

$$\theta(x)\theta\left(x^{-1}\right) \equiv k \pmod{x^{mn}+1}$$

and

$$\theta(x)\theta\left(x^{-1}\right) \equiv k + \lambda T_n\left(x^m\right)\left(T_m(x) - 1\right) \pmod{x^{mn}-1}.$$

Thus,

$$\theta(x)\theta\left(x^{-1}\right) \equiv k + \frac{\lambda}{2}\left(x^{mn}+1\right)T_n\left(x^m\right)\left(T_m(x) - 1\right) \pmod{x^{2mn}-1}$$

$$= k + \frac{\lambda}{2}T_{2n}\left(x^m\right)\left(T_m(x) - 1\right) \pmod{x^{2mn}-1}.$$

Therefore, θ is the Hall polynomial of a $\left(m, 2n, k, \frac{\lambda}{2}\right)$ cyclic relative difference set and we must have that λ is even. □

The condition in Theorem 2.3.20 that λ must be even can be viewed as a nega-cyclic counterpart to Corollary 2.3.4.

Corollary 2.3.21. *Let q be an odd prime power, let d be any natural number, and let t be an odd divisor of $q-1$. There exists no $NW\left(\frac{q^d-1}{t}, q^{d-1}\right)$ W such that $abs(W)$ is the incidence matrix of a cyclic relative difference set with parameters $\left(\frac{q^d-1}{q-1}, \frac{q-1}{t}, q^{d-1}, tq^{d-2}\right)$.*

Chapter 3

Algebraic Non-Existence Results

The aim of this chapter is to elucidate the algebraic techniques used to prove non-existence results for circulant weighing matrices. These techniques were not originally developed with circulant weighing matrices in mind, but to study difference sets and finite geometries with nice automorphism groups. Only later did it become clear that they had applications in all areas of algebraic design theory, of which the study of circulant weighing matrices is one part. In their survey [AD96], Arasu and Dillon mention that most of the known non-existence results that are stated in terms of circulant weighing matrices can be extended to more general classes of group developed weighing matrices using standard methods. I will attempt to do so wherever possible.

Broadly speaking, there are three methods used to prove non-existence results for group developed weighing matrices: the self-conjugacy method, the multiplier method, and the field descent method. These methods, which are sometimes referred to as *character methods*, have their origin in the work of Marshall Hall [Jr.47]. They were developed further in the 1960's in the seminal work of Mann [Man64],

Yamomoto [Yam63], and Turyn [Tur65]. Some recent discoveries ([Sch99], [LS05], and [AM98]) have given new life to these approaches and yielded a whole host of new results.

Let $\mathbf{G}$ be a finite group and let $k \leq n \in \mathbb{N}$. Recall that the existence of a $\mathbf{G}$-developed $W(n,k)$ is equivalent to the existence of an element $\theta(g)$ (g ranges over the elements of $\mathbf{G}$) of the group ring $\mathbb{Z}\mathbf{G}$ with coefficients $0, 1$, and -1 that satisfies the equation $\theta(g)\theta(g)^{(-1)} = k$. Let v be the exponent of $\mathbf{G}$. Recall that if $\mathbf{G}$ is an abelian group, then each character of $\mathbf{G}$ is a homomorphism from $\mathbf{G}$ to the cyclic group generated by the principal v^{th} root of unity ζ_v. Thus, these characters can be extended to homomorphisms from $\mathbb{Z}\mathbf{G}$ to $\mathbb{Z}[\zeta_v]$. Note that the ring $\mathbb{Z}[\zeta_v]$ lies inside $\mathbb{Q}(\zeta_v)$, the v^{th} *cyclotomic field*. Thus, group developed weighing matrices can be associated with elements of cyclotomic fields.

The basic intuition of the character methods (in weighing matrix terms) is that facts about cyclotomic fields can be used to find constraints on the parameters for which there might exist an (abelian) group-developed weighing matrix.

3.1 Background From Algebraic Number Theory

Let us begin by mentioning some facts about prime ideals in cyclotomic fields.

This first result follows from a standard result about algebraic number fields (finite dimensional extensions of $\mathbb{Q}$). See ([IR82], Ch. 12 and 13) for a proof (of the more general result).

Theorem 3.1.1. *Let ζ_v be a primitive v^{th} root of unity. Every ideal in $\mathbb{Z}[\zeta_v]$ has a unique factorization as a product of prime ideals $P_1^{s_1}P_2^{s_2}\cdots P_t^{s_t}$.*

For a proof of the next result, see ([IR82], p.215-216).

Lemma 3.1.2. *Every root of unity in* $\mathbb{Q}(\zeta_m)$ *has the form* $\pm\zeta_m^i$, *for* $i = 1, ..., m$.

Let $m \in \mathbb{N}$ and let P be a prime ideal in $\mathbb{Z}[\zeta_m]$. The group of all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ such that $P^{(\sigma)} = P$ is called the *decomposition group* of P (decomposition groups are used to decompose extension fields into sequences of intermediate extension fields; hence the term "decomposition" [Ser79]). Most of the major results in this chapter rely on the following theorem about the decomposition groups of prime ideals. The proof given here is from [BJL99].

Theorem 3.1.3. *Let* $m \in \mathbb{N}$ *and let* ζ_m *be a primitive* m^{th} *root of unity. Let* $p \in \mathbb{Q}$ *be a prime and let* P *be a prime ideal of* $\mathbb{Z}[\zeta_m]$ *that contains* p. *Write* $m = m^*p^a$, *for some* a, *where* $(m^*, p) = 1$. *Then each* $\sigma \in Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ *for which there is an integer* j *such that* $\sigma(\zeta_{m^*}) = \zeta_{m^*}^{p^j}$ *is an element of the decomposition group of* P.

The proof begins with a series of six preliminary lemmas. Recall that if $k, w \in \mathbb{N}$ are such that $(k, w) = 1$, the k^{th} cyclotomic polynomial $\phi_k(x) = \prod(x - \zeta_k^j)$ (where j ranges over the group of units of k) is the minimal polynomial for the k^{th} roots of unity over $\mathbb{Q}(\zeta_w)$ and, consequently, it is also both monic and irreducible (see [Gal04]).

Lemma 3.1.4. *Let* p *be a prime and let* $a \in \mathbb{N}$. *Then*

$$f(x) = x^{(p-1)p^{a-1}} + x^{(p-2)p^{a-1}} + \cdots + x^{p^{a-1}} + 1$$

is the p^a*-th cyclotomic polynomial* ϕ_{p^a} *over* $\mathbb{Q}$.

Proof. Since $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$, for any primitive p^{th} root of unity ζ_p,

$$\zeta_p^{p-1} + \cdots + \zeta_p + 1 = 0.$$

Hence, since $\zeta_{p^a}^{p^{a-1}}$ is a primitive p^{th} root of unity, $f(\zeta_{p^a}) = 0$. It follows by Theorem 21.3 in [Gal04] that ϕ_{p^a} divides f. Since every integer that isn't a power of p is relatively prime to p^a, the number of integers less than p^a and relatively prime to p^a is $(p-1)p^{a-1}$. Thus, ϕ_{p^a} is a monic polynomial of degree $(p-1)p^{a-1}$ such that $\phi_{p^a} | f$. It follows that $f = \phi_{p^a}$. □

Lemma 3.1.5. *Let $j > 1$ and let $(j,p) = 1$. Then $\langle 1 - \zeta_{p^a} \rangle$ and $\langle 1 - \zeta_{p^a}^j \rangle$ are equal as ideals of $\mathbb{Z}[\zeta_{p^a}]$.*

Proof. Assume that t is an integer such that $jt \equiv 1 \bmod p^a$. Let

$$u = \frac{1 - \zeta_{p^a}^j}{1 - \zeta_{p^a}} = \zeta_{p^a}^{j-1} + \cdots + \zeta_{p^a} + 1 \in \mathbb{Z}\left[\zeta_{p^a}\right].$$

Then

$$u^{-1} = \frac{1 - \zeta_{p^a}}{1 - \zeta_{p^a}^j} = \frac{1 - \zeta_{p^a}^{jt}}{1 - \zeta_{p^a}^j} = \zeta_{p^a}^{j(t-1)} + \zeta_{p^a}^{j(t-2)} + \cdots + 1 \in \mathbb{Z}[\zeta_{p^a}].$$

$$u\left(1 - \zeta_{p^a}\right) = 1 - \zeta_{p^a}^j$$

and

$$u^{-1}\left(1 - \zeta_{p^a}^j\right) = 1 - \zeta_{p^a}.$$

Therefore,

$$\langle 1 - \zeta_{p^a} \rangle = \langle 1 - \zeta_{p^a}^j \rangle.$$

□

Lemma 3.1.6. *$\langle p \rangle$ and $\langle (1-\zeta_{p^a})^{(p-1)p^{a-1}} \rangle$ are equal as ideals of $\mathbb{Z}[\zeta_{p^a}]$.*

Proof.

$$\phi_{p^a} = \prod \left(x - \zeta_{p^a}^j\right),$$

where j ranges over the group of units of p^a. Thus, ϕ_{p^a} has order $(p-1)^{p^{a-1}}$.
By Lemma 3.1.4,

$$\langle p \rangle = \langle \phi_{p^a}(1) \rangle$$

and, by Lemma 3.1.5,

$$\langle \phi_{p^a}(1) \rangle = \langle \prod \left(1 - \zeta_{p^a}^j\right) \rangle = \langle \prod (1 - \zeta_{p^a}) \rangle = \langle (1-\zeta_{p^a})^{(p-1)p^{a-1}} \rangle.$$

□

Lemma 3.1.7. *Let $\sigma \in Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ and suppose that j is an integer such that $\sigma(\zeta_{m^*}) = \zeta_{m^*}^{p^j}$. Then, for any $A \in \mathbb{Z}[\zeta_{m^*}]$, $A^{(\sigma)} \equiv A^{p^j} \mod P$.*

Proof. Set $A = \sum_{i=0}^{m^*-1} a_i \zeta_{m^*}^i$. Then

$$A^{(\sigma)} = \sum_{i=0}^{m^*-1} a_i (\zeta_{m^*}^i)^{p^j} \equiv \left(\sum_{i=0}^{m^*-1} a_i \zeta_{m^*}^i \right)^{p^j} = A^{p^j} \pmod{p}.$$

□

Lemma 3.1.8. $\zeta_{p^a} \equiv 1 \pmod{P}$.

Proof. By Lemma 3.1.6,

$$\langle (1-\zeta_{p^a})^{(p-1)p^{a-1}} \rangle \subset P.$$

Thus, since P is a prime ideal, $(1-\zeta_{p^a}) \in P$. The result follows. □

Lemma 3.1.9. *Let $\sigma \in Gal(\mathbb{Q}(\zeta_{p^a})/\mathbb{Q})$. Then, for any $i \in \mathbb{Z}$, $\left(\zeta_{p^a}^i\right)^\sigma \equiv 1 \ mod\ P$.*

Proof. For any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^a})/\mathbb{Q})$, σ sends p^a-th roots of unity to p^a-th roots of unity. Thus, by Lemma 3.1.2, for any integer i there exists an integer j such that $\left(\zeta_{p^a}^i\right)^\sigma = \zeta_{p^a}^j$. Therefore, the result follows by the previous lemma. □

Now we proceed to the proof of the main theorem.

Proof of Theorem 3.1.3. Since $(m^*, p) = 1$, for any integer i, there exist integers t, s such that $i = tm^* + sp^a$. So for any $y \in P$, there exist $A_s \in \mathbb{Z}[\zeta_m^*]$ such that $y = \sum_{s=0}^{p^a-1} A_s \zeta_{p^a}^s$. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ and suppose that j is an integer such that $\sigma(\zeta_{m^*}) = \zeta_{m^*}^{p^j}$. By Lemma 3.1.9,

$$y^{(\sigma)} = \sum_{s=0}^{p^a-1} A_s^{(\sigma)} (\zeta_{p^a}^s)^{(\sigma)} \equiv \sum_{s=0}^{p^a-1} A_s^{(\sigma)} = \left(\sum_{s=0}^{p^a-1} A_s\right)^{(\sigma)}.$$

By Lemma 3.1.7 and Lemma 3.1.8,

$$\left(\sum_{s=0}^{p^a-1} A_s\right)^{(\sigma)} \equiv \left(\sum_{s=0}^{p^a-1} A_s\right)^{p^j} \equiv \left(\sum_{s=0}^{p^a-1} A_s \zeta_{p^a}^s\right)^{p^j} = y^{p^j} \pmod{P}.$$

Since $y^{p^j} \in P$, $y^{(\sigma)} \in P$. It follows that $P^{(\sigma)} \subset P$ and, since σ is an automorphism, that $P^{(\sigma)} = P$. □

Consider the Gaussian integers $\mathbb{Z}[i]$; in particular, let $m = 4$, $p = 2$, and $m^* = 1$. The ideal $\langle 1 - i \rangle$ is a prime ideal in $\mathbb{Z}[i]$ ([Gal04], Ch. 18). Further, $2 \in \langle 1 - i \rangle$, since $(1 - i)(1 + i) = 2$. Each element σ of $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ satisfies $1^{(\sigma)} = 1^2$. Consequently, by Theorem 3.1.3, the ideal $\langle 1 - i \rangle$ is fixed under every automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$.

Proofs of the next two lemmas can be found in ([IR82], p. 195 and p. 216).

Lemma 3.1.10. $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$ *(recall that* $\phi(m)$ *denotes the Euler Toilent function: the number of integers less than* m *and relatively prime to* m*).*

Lemma 3.1.11. *Let* $\alpha \in \mathbb{Q}(\zeta_m)$ *be such that, for each* $\sigma \in Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, $\sigma(\alpha) \leq 1$. *Then* α *is a root of unity.*

Lemma 3.1.11 is sometimes referred to as Kronecker's Lemma.
The following result is a fairly simple consequence of Kronecker's Lemma; a proof can be found in [Ma96].

Lemma 3.1.12. *Let* ω_1, ω_2 *be cyclotomic integers such that* $\omega_1 \in \omega_2\mathbb{Z}[\zeta_m]$ *and* $|\omega_1| = |\omega_2|$. *Then there exists an integer* c *such that* $\omega_1 = \pm\omega_2\zeta_m^c$.

Let q be a prime power and let χ be a character of the multiplicative group of $\mathbf{GF}(q)$. Then $\sum_t \chi(t)\zeta_q^t$ is the *Gauss sum* on $\mathbf{GF}(q)$ belonging to χ. A proof for the next result can be found in ([IR82], p. 92).

Lemma 3.1.13. *Let* q *be a prime power. If* $\chi \neq \chi_0$ *are two characters defined on the multiplicative group of* $\mathbf{GF}(q)$, *then*

$$\left|\sum_t \chi(t)\zeta_p^t\right| = \sqrt{p}.$$

I will also need a couple of results from (non-algebraic) number theory. The first result is sometimes used as an auxillary result in the proof of the second result. A proof can be obtained by a fairly straightforward modification of the techniques employed in ([IR82], p.39-43). The notation $\mathrm{ord}_t n$ (for $(t, n) = 1$) refers to the least positive integer e such that $n^e \equiv 1 \pmod{t}$.

Lemma 3.1.14. *Let p be a prime and let $b \in \mathbb{Z}$.*

(a) If $(p,b) \neq (2,1)$ and if s is any integer satisfying $s \equiv 1 \pmod{p^b}$ and such that s is not equivalent to 1 modulo p^{b+1}, then $ord_{p^c}(s) = p^{c-b}$ for each $c \geq b$.

(b) Let $s,t \in \mathbb{Z}$ be such that $ord_{p^b}(s) = ord_{p^b}(t) = p^c$ (for some c). Also, suppose that $s \equiv t \equiv 1 \pmod 4$ when $p = 2$. Then s and t are generators of the same subgroup of the multiplicative group $\mathbb{Z}^*_{p^b}$.

A proof of the following result can be found in ([IR82], p.43).

Lemma 3.1.15. *Let p be a prime and let $\ell \in \mathbb{N}$. Then the group of units mod p^ℓ is cyclic of order $p^{\ell-1}(p-1)$.*

3.2 The Self-Conjugacy Method

In 1965, Turyn [Tur65] showed that under the so-called self-conjugacy assumption, one could deduce strong necessary conditions for the existence of algebraic designs such as cyclic difference sets and circulant Hadamard matrices. Arasu and Seberry [AS96], [Ara98] later showed that Turyn's techniques, in concert with a result of Ma [Ma85], could be used to obtain necessary conditions for the existence of circulant weighing matrices. The purpose of this section is to illuminate this technique.

Let p be a (rational) prime and let $m = m^*p^a$, where $(m^*, p) = 1$. Then we say that p is *self-conjugate* modulo m if there exists an integer j such that $p^j \equiv -1 \bmod m^*$. In general, an integer n is *self-conjugate* modulo m if every prime divisor of n is self-conjugate modulo m. The next corollary clarifies the reason for the terminology "self-conjugate."

Corollary 3.2.1. *Let p be a rational prime that is self-conjugate modulo some integer m. Let P be a prime ideal of $\mathbb{Z}[\zeta_m]$ that contains p. Then P is invariant under complex conjugation.*

Proof. The map sending m^{th} roots of unity to their inverses is an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ (this map is equivalent to complex conjugation). By Theorem 3.1.3 then, P is invariant under complex conjugation. □

Corollary 3.2.2. *Let $X \in \mathbb{Z}[\zeta_m]$ and let $X\overline{X} \equiv 0$ mod u^2, where u is self-conjugate modulo m. Then $X \equiv 0$ mod u.*

Proof. By Theorem 3.1.1, there exist, for some r, prime ideals P_1, ..., P_r and integers $t_1, ..., t_r$ such that $\langle u \rangle = P_1^{t_1} P_2^{t_2} \cdots P_r^{t_r}$ and, consequently, $\langle u^2 \rangle = P_1^{2t_1} P_2^{2t_2} \cdots P_r^{2t_r}$. By Corollary 3.2.1, for each prime divisor p of u, each prime ideal that contains p is invariant under complex conjugation. Thus, since, for each i, P_i is prime, X and $\overline{X}$ are both contained in P_i. Further, for each s, $X \in P_i^s$, if and only if $\overline{X} \in P_i^s$. Therefore, for each i, X, $\overline{X} \in P_i^{t_i}$, and it follows that $X \equiv 0 \pmod{u}$. □

This result allows us to infer that, for any group ring element Y over a group $\mathbf{G}$ of order n and for any character χ of $\mathbf{G}$, if $k^2 = \chi(YY^{-1}) = \chi(Y)\chi(Y^{-1}) = \chi(Y)\overline{\chi(Y)}$, if $p^{2t}|k$, and if p is self conjugate modulo n, then $\chi(Y) \equiv 0 \pmod{p^t}$. Corollary 3.2.2 is a powerful tool that was originally discovered by Turyn [Tur65].

3.2.1 Ma's Lemma

In this section we present results that allow us to infer facts about group ring elements from their character values. The first result is folklore.

Theorem 3.2.3. *Let $A = \sum_{g \in \mathbf{G}} a_g g$ be an element of $\mathbb{C}\mathbf{G}$, where $\mathbf{G}$ is a group of order n. Let $k \in \mathbb{N}$ be such that $(k, n) = 1$. Suppose that, for each character χ of $\mathbf{G}$, $\chi(A) \equiv 0 \pmod{k}$. Then, for each $g \in \mathbf{G}$, $a_g \equiv 0 \pmod{k}$.*

Proof. By the inversion formula (Theorem 2.3.8) and the fact that $(k, n) = 1$, for each $g \in \mathbf{G}$,

$$a_g = \frac{1}{|\mathbf{G}|} \sum_{\chi \in \overline{\mathbf{G}}} \chi(A)\chi(g^{-1}) \equiv 0 \bmod k.$$

□

The following theorem, due to Arasu, Davis, et. al [ADJ+96], generalizes an important lemma of Siu Lun Ma [Ma85]. It allows us to deal with the case where $(k, |\mathbf{G}|) > 1$. Recall that, for a prime p, the *Sylow p-subgroup* of a group $\mathbf{G}$ is the largest subgroup of $\mathbf{G}$ whose order is a power of p.

Theorem 3.2.4. *Let $s \in \mathbb{N}$ and let $\mathbf{G}$ be a finite abelian group with a cyclic Sylow p-subgroup $\mathbf{P}$ of order p^s (where p is a prime). Suppose that $Y \in \mathbb{Z}\mathbf{G}$ and that there exists $a \in \mathbb{N}$ such that, for each character χ of $\mathbf{G}$, $\chi(Y) \equiv 0 \ mod\ p^a$ Let $r = min(a, s)$. Then there exist group ring elements $X_0, X_1, ..., X_r$ (for some $r \in \mathbb{N}$) such that*

$$Y = p^a X_0 + p^{a-1} P_1 X_1 + ... + p^{a-r} P_r X_r, \tag{3.1}$$

where, for each i, P_i is the group ring element corresponding to the unique subgroup of $\mathbf{G}$ of order p^i.

Proof. Set $\mathbf{G} = \mathbf{P} \times \mathbf{H}$ and let $Y = \sum_{h \in \mathbf{H}} A_h h$, where $A_h \in \mathbb{Z}\mathbf{P}$. Let $\mathbf{H} = \{h_1, ..., h_t\}$ and let χ be a character of $\mathbf{G}$. Let $z = (\chi(A_{h_1}), \chi(A_{h_2}), ..., \chi(A_{h_t}))^T$, let $\overline{\mathbf{H}}$ be the group of characters of $\mathbf{H}$, and let $C = (\tau(h))_{\tau \in \overline{\mathbf{H}}, h \in \mathbf{H}}$ be the matrix correspond-

ing to the character table of $\mathbf{G}$. For $\tau \in \overline{\mathbf{H}}$, the entry of Cz corresponding to τ is $\sum_{h\in\mathbf{H}} \chi(A_h)\tau(h)$. We can define a character $\chi \otimes \tau$ by the rule$(\chi \otimes \tau)(\ell h) = \chi(\ell)\tau(h)$, for $\ell \in \mathbf{P}, h \in \mathbf{H}$. Set $A_h = \sum_{\ell\in\mathbf{P}} b_{h\ell}\ell$. Then

$$(\chi \otimes \tau)(Y) = (\chi \otimes \tau)\left(\sum_{h\in\mathbf{H}}\sum_{\ell\in\mathbf{P}} b_{h\ell}h\ell\right)$$

$$= \sum_{h\in\mathbf{H}}\sum_{\ell\in\mathbf{P}} b_{h\ell}\chi(\ell)\tau(h) = \sum_{h\in\mathbf{H}} \chi(A_h)\tau(h),$$

the entry of Cz corresponding to τ.

By hypothesis,

$$(\chi \otimes \tau)(Y) \equiv 0 \bmod p^a,$$

and it follows that each entry of Cz is congruent to 0 mod p^a. But, by Character orthogonality relations (Theorem 2.3.6), $C^{-1} = |\mathbf{H}|^{-1}C^T$. Therefore, each entry of $z = |\mathbf{H}|^{-1}C^T(Cz)$ is congruent to 0 mod p^a, i.e.

$$\chi(A_h) \equiv 0 \bmod p^a$$

for each $h \in \mathbf{H}$. Thus, we may assume that $y \in \mathbb{Z}\mathbf{P}$, since if the implication holds for elements in this sub-ring, it holds for all group ring elements.

For $i \in [0, r]$, let χ_i be a (group ring) character such that $\dim\ (\mathrm{Ran}(\chi_i)) = p^{s-i}$. χ_i is an epimorphism from $\mathbb{Z}\mathbf{G}$ onto $\mathbb{Z}[\zeta_{p^{s-i}}]$. Thus, we can choose sets $X_0, X_1, ..., X_i$

recursively as follows:

$$\chi_i(X_0) = p^{-a}\chi_i(Y);$$
$$\chi_i(X_1) = p^{-a}\chi_i(Y) - \chi_i(X_0);$$
$$\vdots$$
$$\chi_i(X_i) = p^{-a}\chi_i(Y) - \sum_{j=0}^{i-1}\chi_i(X_j). \tag{3.2}$$

Let τ_i be a character such that $\dim(\mathrm{Ran}(\tau_i)) = p^{s-i}$, so that τ_i is an epimorphism onto $\mathbb{Z}(\zeta_{p^{s-i}})$. Then $\tau_i = \chi_i^{(\sigma)}$, where $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^{s-i}}))$ and $\chi_i^{(\sigma)}$ is defined by the rule $\chi^{(\sigma)}(A) = (\chi_i(A))^{(\sigma)}$. Applying σ to both sides of 3.2, we deduce that

$$\tau_i(X_i) = p^{-a}\tau_i(Y) - \sum_{j=0}^{i-1}\tau_i(X_j).$$

By the Dimension Theorem, $\dim(\mathrm{Ker}(\tau_i)) = p^i$ (here $\mathrm{Ker}(\tau_i)$ refers to the set $\{x \in \mathbf{P} : \tau_i(x) = 1\}$). Since $\mathbf{P}$ is cyclic, it contains a unique subgroup, $\mathbf{P}_i$, of order p^i. Therefore, $\mathrm{Ker}(\tau_i) = \mathbf{P}_i$. So, by Character orthogonality relations (Theorem 2.3.6), for any $j \leq i$, $\tau_i(\mathbf{P}_j) = p^j$ and for any $j > i$, $\tau_i(\mathbf{P}_j) = 0$. Thus, we get the following string of equalities

$$\tau_i(p^a X_0 + p^{a-1}\mathbf{P}_1 X_1 + \cdots + p^{a-r}\mathbf{P}_r X_r)$$

$$= p^a\tau_i(X_0) + p^{a-1}p\tau_i(X_1) + \cdots + p^{a-i}p^i\tau_i(X_i) = p^a\sum_{j=0}^{i}\tau_i(X_j) = \tau_i(Y).$$

So for each character of $\mathbf{P}$ that is non-trivial on $\mathbf{P}_r$, both sides of 3.1 have the same character value.

It follows, by Corollary 2.3.9, that

$$Y = p^aX_0 + p^{a-1}P_1X_1 + \cdots + p^{a-r}P_rX_r + P_rX,$$

for some $X \in \mathbb{Z}\mathbf{P}$. If $r = a$, then we can complete the proof by replacing X_r with $X_r + X$. So suppose that $r = s$. Then for each $g \in \mathbf{P}$, $g\mathbf{P}_s = \mathbf{P}_s$ ($\mathbf{P} = \mathbf{P}_s$). So $X\mathbf{P}_r = X(1)\mathbf{P}_r$, where $X(1)$ is interpreted as the sum of the coefficients of X. Let χ_0 be the trivial character on $\mathbf{P}$. $\chi_0(Y) \equiv 0 \pmod{p^a}$, so $Y(1) \equiv 0 \pmod{p^a}$. It follows that $X(1) \equiv 0 \pmod{p^{a-r}}$. So $X\mathbf{P}_r = tp^{a-r}\mathbf{P}_r$, for some $t \in \mathbb{Z}$. The proof can now be completed by replacing X_r with $X_r + t$. □

Ma's Lemma, which I referred to earlier, follows as a special case.

Lemma 3.2.5. *Let $\mathbf{G}$ be a finite abelian group with a cyclic sylow p-subgroup of order p^s, where p is a prime. Let $Y \in \mathbb{Z}\mathbf{G}$ satisfy $\chi(Y) \equiv 0 \bmod p^a$ for each non-trivial character of χ of $\mathbf{G}$. Then there exist $X_1, X_2 \in \mathbb{Z}\mathbf{G}$ such that $Y = p^aX_1 + PX_2$, where P is the group ring element corresponding to the unique subgroup of $\mathbf{G}$ of order p.*

Note that the assumption that $\chi_0(Y) \equiv 0 \pmod{p^a}$ (where χ_0 denotes the trivial character) was used only in the last part of the proof of Theorem 3.2.4.

3.2.2 Applications of the Self-Conjugacy Method

In [AS96], Arasu and Seberry made use of the self-conjugacy method to obtain necessary conditions for the existence of circulant weighing matrices. Later Arasu proved a reduction theorem that strengthed these conditions in some cases [Ara98]. Both of these results are contained in the following theorem (Arasu states the reduction condition somewhat differently [Ara98], but my version is equivalent to his).

Theorem 3.2.6. *Let W be a weighing matrix of order n and weight k developed over an abelian group $\mathbf{G}$ of order n with a (possibly trivial) cyclic Sylow p-subgroup and let $p^{2t}||k$. If there exists a divisor m of n such that p is self-conjugate modulo m^*, where, for some subgroup $\mathbf{H}$ of order $\frac{n}{m}$, m^* is the exponent of $\mathbf{G}/\mathbf{H}$, then the following two conditions hold:*

(i) If $p|m$, then $\frac{2n}{m} \geq p^t$ and, if $n = m$, there exists a $W(n/2, k/4)$ developed over the group $\mathbf{G}/\mathbf{P}$, where $\mathbf{P}$ is a subgroup of $\mathbf{G}$ of order 2.

(ii) If $(p, m) = 1$, then $\frac{n}{m} \geq p^t$.

As Schmidt remarks in [Sch99], p is self-conjugate modulo n only if, for every pair q_1, q_2 of prime divisors of n, $\mathrm{ord}_{q_1} p = \mathrm{ord}_{q_2} p = 2r$, for some r. Thus, speaking informally, the likelihood that p is self-conjugate modulo n decreases rapidly as the number of prime divisors of n increases.

That being said, the hypothesis of the above theorem requires only that p be self-conjugate modulo some divisor of n. Thus, it has a reasonably wide range of applicability and it is worthwhile to strengthen it as much as possible. In the course of learning the proof of this theorem, I noticed that it can be slightly improved. Firstly, by applying Theorem 3.2.4, one can show that some parameters, previously

known to be subject to the bound in part (i), are actually subject to the bound in part (ii), which is stronger. Secondly, by exploiting the folding technique discussed in Section 1.10, one can make the following improvement to part (ii) of the bound.

Theorem 3.2.7. *In part (ii) of Theorem 3.2.6, either* $\frac{n}{m} \geq 2p^t$ *or there exists a* $W(m, k/p^{2t})$ *developed over the group* $\mathbf{G}/\mathbf{H}$, *where* $\mathbf{H}$ *is a subgroup of* $\mathbf{G}$ *of order* $\frac{n}{m}$.

Thirdly, one can show that the inequalities in the bounds are, for the most part, strict. Note that Theorem 3.2.4 is strongest when m is chosen to be as large as possible, so there is no loss of generality in making the assumption suggested in the following result.

Theorem 3.2.8. *In Theorem 3.2.6, assume that if* p^e *is the largest power of* p *that divides* n, *then* $p^e|m$. *Both possible bounds given by the improvement to part (ii) (Theorem 3.2.7) are strict. Also, if* $p^t \neq 2$, *the bound in part (i) is strict.*

Here is the revised version of Theorem 3.2.6.

Theorem 3.2.9. *Let* W *be a weighing matrix of order* n *and weight* k *developed over an abelian group* $\mathbf{G}$ *of order* n *with a (possibly trivial) cyclic Sylow* p*-subgroup of order* p^a *and let* $p^{2t}||k$. *Suppose that there exists a divisor* m *of* n *such that* p *is self-conjugate modulo* m^*, *where, for some subgroup* $\mathbf{H}$ *of order* $\frac{n}{m}$, m^* *is the exponent of* $\mathbf{G}/\mathbf{H}$. *Assume that if* p^e *is the largest power of* p *that divides* n, *then* $p^e|m$. *The following two conditions hold:*

(i) If $t \leq a$, *then* $\frac{2n}{m} \geq p^t$. *This inequality is strict unless* $p^t = 2$, *in which case there exists a* $W(n/2, k/4)$ *developed over the group* $\mathbf{G}/\mathbf{P}$, *where* $\mathbf{P}$ *is a subgroup of* $\mathbf{G}$ *of order* 2.

(ii) If $t > a$, *then* $\frac{n}{m} > p^t$, *and either* $\frac{n}{m} > 2p^t$ *or there exists a* $W(m, k/p^{2t})$ *developed over the group* $\mathbf{G}/\mathbf{H}$.

Proof. (*i*) Let $A - B$ be the group ring element corresponding to the $W(n,k)$ developed over $\mathbf{G}$. It follows from the Fundamental Theorem of Abelian Groups (see [Gal04]) that there exists a subgroup $\mathbf{H}$ of $\mathbf{G}$ of order $\frac{n}{m}$ such that $\mathbf{G}/\mathbf{H}$ is a group of order m. Let m^* be the exponent of $\mathbf{G}/\mathbf{H}$ and suppose that p is self-conjugate modulo m^*. Let σ be the canonical homomorphism from $\mathbb{Z}[\mathbf{G}]$ to $\mathbb{Z}[\mathbf{G}/\mathbf{H}]$. Then

$$(A^{(\sigma)} - B^{(\sigma)})(A^{(\sigma)} - B^{(\sigma)})^{(-1)} = \left((A-B)(A-B)^{(-1)}\right)^{\sigma} = k^{(\sigma)} = k.$$

So, for any character χ of $\mathbf{G}$,

$$\chi(A^{(\sigma)} - B^{(\sigma)})\overline{\chi(A^{(\sigma)} - B^{(\sigma)})} = \chi(A^{(\sigma)} - B^{(\sigma)})\chi((A^{(\sigma)} - B^{(\sigma)})^{(-1)})$$

$$= \chi((A^{(\sigma)} - B^{(\sigma)})(A^{(\sigma)} - B^{(\sigma)})^{(-1)}) = k \equiv 0 \pmod{p^{2t}}.$$

Thus, by Corollary 3.2.2,

$$\chi((A^{(\sigma)} - B^{(\sigma)}) \equiv 0 \pmod{p^t}.$$

So, by Lemma 3.2.5,

$$A^{(\sigma)} - B^{(\sigma)} = p^t X_1 + \mathbf{P} X_2,$$

where $X_1, X_2 \in \mathbb{Z}[\mathbf{G}/\mathbf{H}]$ and $\mathbf{P} = \langle y \rangle$ is a subgroup of $\mathbf{G}/\mathbf{H}$ of order p.

Since $A - B$ has $0, \pm 1$ coefficients, the coefficients of $A^{(\sigma)} - B^{(\sigma)}$ are contained in

the interval $[-\frac{n}{m}, \frac{n}{m}]$. But, since $(1-y)P = 0$,

$$(1-y)(A^{(\sigma)} - B^{(\sigma)}) \equiv 0 \pmod{p^t}.$$

However, the coefficients of $(1-y)\left(A^{(\sigma)} - B^{(\sigma)}\right)$ are contained in the interval $[\frac{2n}{m}, \frac{2n}{m}]$ and, since there exist characters χ such that $\chi(y) \neq 1$, $(1-y)(A^{(\sigma)} - B^{(\sigma)})$ is non-zero. Thus, $\frac{2n}{m} \geq p^t$. Assume that equality holds, i.e. that $\frac{2n}{m} = p^t$. Then, unless $p^t = 2$, there exists a power of p that divides n but that does not divide m, which is impossible.

Suppose that $m = n$, so that $p^t = 2$ and

$$(1-y)(A-B) \equiv 0 \pmod{2}. \tag{3.3}$$

. Let γ be the canonical homomorphism from $\mathbf{G}$ to $\mathbf{G/P}$. It follows from 3.3 that $A^\gamma - B^\gamma$ is a $0, \pm 2$ matrix. Thus, $\frac{1}{2}(A^\gamma - B^\gamma)$ is a $W(n/2, k/4)$ developed over $\mathbf{G/P}$.

(ii) As above, by Corollary 3.2.2, for each character χ,

$$\chi(A^{(\sigma)} - B^{(\sigma)}) \equiv 0 \bmod p^t.$$

Thus, since $t > a$, by Theorem 3.2.4,

$$A^{(\sigma)} - B^{(\sigma)} \equiv 0 \bmod p^t.$$

So $\frac{n}{m} \geq p^t$. Assume that $\frac{n}{m} = p^t$. Then there exists some power of p that divides n but that does not divide m, which is impossible.

If each non-zero coefficient of $A^{(\sigma)} - B^{(\sigma)}$ is $\pm p^t$, then $\frac{1}{p^t}\left(A^{(\sigma)} - B^{(\sigma)}\right)$ is a $W(n/m, k/p^{2t})$,

developed over $\mathbf{G}/\mathbf{H}$. If at least one coefficient of $A^{(\sigma)} - B^{(\sigma)}$ is greater than p^t (in absolute value), then $\frac{n}{m} \geq 2p^t$. □

As the reader will discover in the next section, there are systematic methods for studying circulant weighing matrices of prime power weight. The improvement given in Theorem 3.2.7 is useful because it reduces, in some cases, a question about the existence of a circulant weighing matrix of composite weight to a question about the existence of a circulant weighing matrix of prime power weight. In order to apply my improvement, I will make use of results which classify all orders in which there exist circulant weighing matrices of weights 9 and 16.

Theorem 3.2.10. *[AAMS08] There exists a $CW(n, 9)$ if and only if n is a multiple of* 13 *or* 24.

Theorem 3.2.11. *[ALM+06b] There exists a $CW(n, 16)$ if and only if n (> 14, obviously) is a multiple of* 14, 21, *or* 31.

In the table below, the non-existence of a $CW(n, k)$ with parameters given in the left hand column is implied by Theorem 3.2.7 and the non-existence of a $CW(m, k/p^{2t})$ with parameters given in the right hand column. Note that the non-existence of these $CW(n, k)$'s is not implied by the previous Theorem 3.2.6.

Table 3.1: $CW(n,k)$'s whose non-existence is implied by Theorem 3.2.7 but not by Theorem 3.2.6

(n,k)	m	p^t	p^j	$(m, k/p^{2t})$
$(51,36)$	17	2	2^4	$(17,9)$
$(66,36)$	33	2	2^5	$(33,9)$
$(99,36)$	33	2	2^5	$(33,9)$
$(258,36)$	129	2	2^7	$(129,9)$
$(387,36)$	129	2	2^7	$(129,9)$
$(99,64)$	33	2	2^5	$(33,16)$
$(130,64)$	65	2	2^6	$(65,16)$
$(195,64)$	65	2	2^6	$(65,16)$
$(258,64)$	129	2	2^7	$(129,16)$
$(387,64)$	129	2	2^7	$(129,16)$
$(488,144)$	244	3	3^5	$(244,16)$
$(732,144)$	244	3	3^5	$(244,16)$

A variation on the Self-Conjugacy Method can be used to obtain necessary conditions for the existence of symmetric group developed weighing matrices. Let $k, t \in \mathbb{N}$, let p be a prime, and let $p^{2t}|k$. Let $\theta(g)$ be the group ring polynomial corresponding to a symmetric $W(n,k)$ developed over an abelian group $\mathbf{G}$ with a cyclic Sylow p-subgroup (possibly trivial). Let v be the exponent of $\mathbf{G}$. Then, for each irreducible character χ of $\mathbf{G}$,

$$\chi(\theta(g)\theta(g)^{(-1)}) = \chi(\theta(g))\chi(\theta(g)) = \chi(\theta(g))^2 \equiv 0 \pmod{p^{2t}}.$$

Thus, for each prime ideal P of $\mathbb{Z}[\zeta_v]$ that contains p, $\chi(\theta(g)) \in P$. It follows that $\chi(\theta(g)) \equiv 0 \pmod{p^t}$. So Theorem 3.2.3 and Ma's Lemma can be used to obtain strong necessary conditions on the existence of symmetric group developed weighing matrices (see, for example, [Ma90] and [AM05]) . This symmetry assumption

effectively serves as a substitute for the self-conjugacy assumption.

I have discovered one more result of this type; it is based on the following Turyn-like folklore result which plays an important role in the study of circulant weighing matrices whose weight is a prime power. The proof given here is from [EK97].

Lemma 3.2.12. *Let p be a prime and let $t, r \in \mathbb{N}$. Let $X \in \mathbb{Z}[\zeta_{p^t}]$ and suppose that $X\overline{X} \in \langle p^{2r} \rangle$. Then $X \in \langle p^r \rangle$.*

Proof. Define the map $\pi : \mathbb{Z}[\zeta_{p^t}] \to \mathbb{Z}_p$ such that ζ_{p^t} is sent to 1 and such that $\pi/\mathbb{Z}$ is the natural epimorphism from $\mathbb{Z}$ to $\mathbb{Z}_p$. $\mathrm{Ker}\,(\pi) = \langle p \rangle \cup \langle 1 - \zeta_{p^t} \rangle$. But, by Lemma 3.1.6, $\langle p \rangle = \langle (1 - \zeta_{p^t})^{(p-1)p^{t-1}} \rangle$. Hence, $\mathrm{Ker}\,(\pi) = \langle 1 - \zeta_{p^t} \rangle$.

Let s be the greatest integer such that $(1 - \zeta_{p^t})^s \,|X$. Then there exists $X_1 \in \mathbb{Z}\,[\zeta_{p^t}]$ such that $\pi(X_1) \neq 0$ and such that $X = (1 - \zeta_{p^t})^s X_1$. By Lemma 3.1.5,

$$X\overline{X} = (1 - \zeta_{p^t})^{2s} X_2,$$

with $X_2 = uX_1\overline{X_1}$ for some unit u.

By Lemma 3.1.6,

$$p = v(1 - \zeta_{p^t})^{(p-1)p^{t-1}}$$

for some unit v. Since $X\overline{X} \in \langle p^{2r} \rangle$,

$$2s \geq 2r(p-1)p^{t-1}$$

and, consequently,

$$s \geq r(p-1)p^{t-1}.$$

It follows that

$$X = (1 - \zeta_{p^t})^s X_1 \in \langle p^r \rangle.$$

□

I presented a less general version of the next theorem to Dr. Craigen, who made the suggestion to work in a more general group and "fold down." Although this result is similair to Theorem 3.2.6 part (i), the results apply, in general, in a very different set of circumstances.

Theorem 3.2.13. *Let p be a prime and let $m, n, t, r \in \mathbb{N}$. Let $\mathbf{G}$ be an abelian group of order np^t with a cyclic Sylow p-subgroup. Further, assume that $(n, p) = 1$. Then there exists a $\mathbf{G}$-developed $W(np^t, p^{2r}m^2)$ only if $p^r \leq 2n$. This inequality is strict unless $p^r = 2$.*

Proof. Suppose that A is the group ring polynomial of a $CW(np^t, p^{2r}m^2)$ over the cyclic group $\mathbf{G} = \langle \alpha \rangle \times \mathbf{H}$, where $o(\alpha) = p^t$, $|H| = n$, and $(n, p) = 1$. Let σ be the canonical epimorphism from $\mathbf{G}$ to $\mathbf{G}/\mathbf{H}$. For each character χ,

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

Hence, by Lemma 3.2.12,

$$\chi(A^{(\sigma)}) \equiv 0 \pmod{p^r}.$$

So, by Ma's Lemma,

$$A^{(\sigma)} = p^r x_0 + \langle \alpha^{p^{t-1}} \rangle x_1,$$

for some $x_1, x_2 \in \mathbb{Z}[\langle\alpha\rangle]$. Thus

$$\left(1-\alpha^{p^{t-1}}\right)A^{(\sigma)} \equiv 0 \pmod{p^r}.$$

Since there exists a character χ such that $\chi\left(\alpha^{p^{t-1}}\right) \neq 0$,

$$\left(1-\alpha^{p^{t-1}}\right)A^{\sigma} \neq 0.$$

But the coefficients of $(1-\alpha^{p^{t-1}})A^{\sigma}$ are contained in the interval $[-2n, 2n]$. So

$$p^r \leq 2n.$$

Unless $p^r = 2$, the assumption that $(n,p) = 1$ implies this inequality is strict. □

It follows from Theorem 3.2.13 that there exist no weighing matrices developed over abelian groups with cyclic Sylow p-subgroups and with parameters $(147, 49)$, $(98, 49)$, $(125, 25)$, $(128, 64)$, $(625, 25)$, $(625, 100)$, $(625, 225)$, $(625, 400)$, $(216, 36)$, $(216, 144)$, etc.

It is a consequence of the Field descent method discussed in the final section of this chapter that there exist only finitely many "half-full" circulant weighing matrices (circulant weighing matrices of order n and weight $\frac{n}{2}$). Half-full circulant weighing matrices are of interest because of their connection to circulant Hadamard matrices (see Theorem 1.10.4). Theorem 3.2.13 implies another result in this direction (there does, in fact, exist a $CW(8,4)$- see the next section).

Corollary 3.2.14. *Let p be a prime and let $t, r \in \mathbb{N}$. Let $\mathbf{G}$ be an abelian group of order $2p^t$ with a cyclic Sylow p-subgroup. There exists a $W(2p^{2r}, p^{2r})$ developed*

over $\mathbf{G}$ *if and only if* $p^r = 2$.

It was already known that, for $p > 3$, there exist no group developed $W(2p^2, p^2)$'s obtainable, via folding, from group developed $W(4p^2, 4p^2)$'s (see [AD96]). However, in the case of abelian groups with cyclic Sylow p-subgroups, Corollary 3.2.14 is a significant improvement on this result. It follows directly from Theorem 3.2.13 that there exist no circulant Sylvester Hadamard matrices (other than [1] and circ(−111)). However, Turyn has already proven the much more general result that if there exists a circulant Hadamard matrix of order $v = 4u^2$, then u must be odd [Tur65]. It also follows from Corollary 3.2.14 that, for each prime p, there exists no circulant Hadamard matrix of order $4p^t$ (Schmidt has already obtained a somewhat more general result of this type, see [Sch]).

Theorem 3.2.13 is, to the best of my knowledge, new (in the sense that it hasn't shown up elsewhere in the literature). However, it follows from standard results and techniques and likely won't come as much of a suprise.

3.3 Multipliers and the Classification of Circulant Weighing Matrices of Prime Power Weight

The Self-Conjugacy Method and the Field Descent Method were (originally) designed in an attempt to prove the Circulant Hadamard Matrix Conjecture and to derive general exponent bounds for difference sets. The techniques explored in this section have a different purpose. They are well suited to answering the question "Given a prime power p^{2t}, what are the orders n such that $(n, p) = 1$ and there exists a $CW(n, p^{2t})$?".

Let σ be an automorphism of a group $\mathbf{G}$. We say that σ is a *multiplier* of a group ring element A if there exists $g \in \mathbf{G}$ such that $A^{(\sigma)} = gA$. If $A^{(\sigma)} = A$, then σ is called a *fixing multiplier*. If σ is defined by the rule $\sigma(h) = h^t$, then we also say that t is a multiplier of A. For instance, consider the element $A = -1 + x + x^2 + x^4$ of the group ring $\mathbb{Z}[\langle x \rangle]$ over the cyclic group $\langle x \rangle$ of order 7 (this is the group ring polynomial of a $CW(7,4)$). $A^{(2)} = A$, so 2 is a multiplier of A (in fact, 2 is a fixing mutiplier). The existence of a multiplier imposes rather strict conditions on the structure of a group ring element.

There are essentially two main types of multiplier results: *Type 1* results that are useful for studying the case in which the weight and the order are relatively prime and *Type 2* results that are useful for studying the case in which they are not. We shall discuss both types of results and illustrate them by discussing how the authors of [AAMS08] use them to classify all possible values n such that there exists a $CW(n,9)$. Hopefully this will illustrate how such classifications can be achieved generally and, in particular, how one might tackle the next open case: the classification of all possible orders n such that there exists a $CW(n,25)$.

3.3.1 Type 1 Multiplier Results

The next lemma is a straightforward generalization of a result of Marshall Hall; the proof is adapted from the one given in [BJL99].

Lemma 3.3.1. *Let $\mathbf{G}$ be an abelian group of order v, let $A \in \mathbb{Z}[\mathbf{G}]$, and let $|Supp(A)| = k$. Suppose that $(v,k) = 1$. There exists $g \in \mathbf{G}$ such that, for each multiplier σ of A, $(Ag)^{(\sigma)} = Ag$ (i.e. σ is a fixing multiplier of Ag).*

Proof. Let $\mathrm{Supp}(A) = \{g_1, ..., g_k\}$. Since $(v,k) = 1$, the map $a \to a^k$ (for $a \in \mathbf{G}$)

is an automorphism of $\mathbf{G}$. Hence, there exists a unique element $g \in \mathbf{G}$ such that $g_1 \cdots g_k g^k = 1$. Let σ be a multiplier of A. Then $(Ag)^{(\sigma)} = Ah$, for some $h \in \mathbf{G}$.

$$1 = \left(g_1 \cdots g_k g^k\right)^{(\sigma)} = \left((g_1 g) \cdots (g_k g)\right)^{(\sigma)} = (g_1 h) \cdots (g_k h) = g_1 \cdots g_k h^k.$$

Therefore $h = g$. □

The first major multiplier result (relevant to circulant weighing matrices) is due to McFarland [McF70]; it was originally proven as an auxillary result in his study of multipliers of abelian difference sets. Arasu and Seberry were perhaps the first to recognize its utility in the study of circulant weighing matrices [AS96]. The proof given here is mostly taken from the one given in E. S. Lander's book [Lan83]. However, his proof makes use of properties of p-adic numbers. Borrowing some ideas from [AM98], I have managed to make do with the character approach already pervasive in this thesis.

Theorem 3.3.2. *([McF70]) Let p be a prime and let $m, e \in \mathbb{N}$. Let $p^e || m$ and define $M(m)$ as the product of the distinct prime factors of m, $M(m^2/p^{2e})$, $p-1$, p^2-1, ..., $p^{u(m)}-1$, where $u(2) = 3$, $u(3) = 5$, $u(4) = 7$, and, for $m \geq 5$, $u(m) = \frac{1}{2}(m^2 - m)$. Let $\mathbf{G}$ be a group such that $|\mathbf{G}| = w$, where $(w, M(m)) = 1$, and let $A = \sum_{i=1}^{w} a_i g_i \in \mathbb{Z}[\mathbf{G}]$ satisfy $AA^{(-1)} = m^2$. Further, assume that $\sum_{i=1}^{w} a_i = m$ (as opposed to $-m$). Then $A = mg$, for some $g \in \mathbf{G}$.*

Proof. The proof proceeds by induction. If m has no prime factors, then, for some $g \in \mathbf{G}$, $A = g$. So assume that m has s prime factors, for some $s > 0$. Let $\langle p \rangle =$

$P_1^{t_1} \cdots P_k^{t_k}$ be the prime ideal decomposition of $\langle p \rangle$. For each character χ,

$$\chi(A)\chi\left(A^{(-1)}\right) = m^2 \equiv 0 \pmod{p^{2e}}.$$

Thus, for each P_i, either $\chi(A) \in P_i$ or $\chi\left(A^{(-1)}\right) \in P_i$. Let v be the exponent of $\mathbf{G}$. By Theorem 3.1.3, the automorphism, call it ρ, of $\mathbb{Z}[\zeta_v]$ that sends ζ_v to ζ_v^p is an element of the decomposition group of each P_i. Thus, for each i, if $\chi(A) \in P_i$, then $\chi\left(A^{(p)}\right) = \chi(A)^{(\rho)} \in P_i$. It follows that $\chi\left(A^{(p)}\right)\chi\left(A^{(-1)}\right) \in \langle p^{2e} \rangle$. Hence, since $(w, p) = 1$, Theorem 3.2.3 implies that $A^{(p)}A^{(-1)} \equiv 0 \pmod{p^{2e}}$.
Therefore, $V = \frac{1}{p^{2e}}A^{(p)}A^{(-1)} \in \mathbb{Z}[\mathbf{G}]$. Further,

$$VV^{(-1)} = p^{-4e}A^{(p)}A^{(-1)}A(A^{(p)})^{(-1)} = \left(\frac{m^2}{p^{2e}}\right)^2.$$

$(w, M(m^2/p^{2e})) = 1$ and $\frac{m^2}{p^{2e}}$ has one fewer prime factor than m. So, by the induction hypothesis, there exists $g \in \mathbf{G}$ such that $V = \frac{m^2}{p^{2e}}g$. Hence, $A^{(p)}A^{(-1)} = m^2 g$. Multiplying both sides of this equation by A, we conclude that $A^{(p)} = gA$, i. e. that p is a multiplier of A. By Lemma 3.3.1, there exists $h \in \mathbf{G}$ that $(Ah)^{(p)} = Ah$. Define $B \in \mathbb{Z}[\mathbf{G}]$ to be such that $B = \sum_{j=1}^{w} b_j g_j = Ah$.
Since w is relatively prime to $p-1$, p^2-1, ..., $p^{u(m)}-1$, if $g_j \neq 1$, then the size of the orbit of g_j under the automorphism $a \to a^p$ $(a \in \mathbf{G})$, denoted by $|\mathrm{orb}_p(h)|$, is greater than $u(m)$. Let $i > 1$ and let $t = b_i$. It follows that

$$m^2 = \sum_{j=1}^{w} b_j^2 \geq t^2(u(m)+1).$$

$f(x) = \frac{2x^2}{x^2-x}$ is a decreasing function, so

$$4 \geq \frac{m^2}{\frac{1}{2}(m^2-m)} > \frac{m^2}{u(m)+1} \geq t^2.$$

Hence $t = 0$ or ± 1.

Let $b_1 = b$, and let there be α and γ values b_j (for $j > 1$) such that $b_j = 1$ and $b_j = -1$, respectively.

$$b^2 + \alpha + \gamma = m^2$$

and

$$b + \alpha - \gamma = m.$$

So

$$\gamma = \frac{1}{2}(m^2 - m) - \frac{1}{2}(b^2 - b) \leq u(m). \tag{3.4}$$

However, since $a \to a^p$ maps elements of $\mathbf{G}$ in orbits of size $\geq u(m) + 1$, 3.4 is impossible unless $\gamma = 0$. But if $\gamma = 0$, then either $b = m$ or $b = 1 - m$. If $b = 1 - m$, then $\alpha = 2m - 1 \leq u(m)$, which is impossible, since $a \to a^p$ maps elements of $\mathbf{G}$ in orbits of size $\geq u(m) + 1$. Thus, we conclude that $b = m$ and, consequently, that $B = m$. It follows that $A = mh^{-1}$. □

It's possible to make ad hoc improvements on the values of $M(m)$ given in the previous theorem. I will prove part (i) of the following result. For the details concerning parts (ii) and (iii), see [Lan83].

Theorem 3.3.3. *The conclusion of Theorem 3.3.2 remains true with the following values of $M(m)$:*

(i) $M(2) = 2 \cdot 7$,

(ii) $M(3) = 2 \cdot 3 \cdot 11 \cdot 13$, *and*

(iii) $M(4) = 2 \cdot 3 \cdot 7 \cdot 31$.

Proof. The value of $M(2)$ used in Theorem 3.3.2 was $2 \cdot 3 \cdot 7$. In the proof of Theorem 3.3.2 (with $m = 2$), we deduced that, for $h \neq 1$, $|\text{orb}_2(h)| \geq 4$. If we assume only that $(w, 2 \cdot 7) = 1$, then it may be the case that $\mathbf{G}$ has elements of order 3 and, consequently, that there exist elements $h \in \mathbf{G}$ such that $|\text{orb}_2(h)| = 2$. B has at most 4 non-zero terms, so that $\text{Supp}(B)$ contains at most 2 orbits of size 2. Let $\text{Supp}(B) \subseteq \{1\} \cup \{g_1, g_1^2\} \cup \{g_2, g_2^2\}$. $b_{g_1} = b_{g_1^2}$ and $b_{g_2} = b_{g_2^2}$. Thus,

$$b_1^2 + 2b_{g_1}^2 + 2b_{g_2}^2 = 4$$

and

$$b_1 + 2b_{g_1} + 2b_{g_2} = 2.$$

The only integer valued solution to this system of equations is $(b_1, b_{g_1}, b_{g_2}) = (2, 0, 0)$. □

In one of the earliest circulant weighing matrix papers, Eades and Hain [EH76] classified all values of n such that there exists a $CW(n, 4)$. If $7|n$, then one can obtain a $CW(n, 4)$ by applying Lemma 1.5.2, part (i), to the $CW(7, 4)$ with Hall polynomial $-1 + x + x^2 + x^4$. If $n \geq 4$ and $2|n$, then for each $i \neq 0, \frac{n}{2}$, $-1 + x^{\frac{n}{2}} + x^i + x^{i+\frac{n}{2}}$ is the Hall polynomial of a $CW(n, 4)$. If $(n, 7) = (n, 2) = 1$, then, by Theorems 3.3.2 and 3.3.3, there exists no $CW(n, 4)$. Eades and Hain originally gave a direct proof of this fact that involved a lot of calculations and consideration of special cases; Arasu et. al [ALM+06b] were the first to note that it follows as a direct corollary of McFarland's result.

Theorem 3.3.4. *There exists a $CW(n,4)$ if and only if $n \geq 4$ and either $2|n$ or $7|n$.*

The next result is (almost) the most general known multiplier existence theorem that applies to circulant weighing matrices. It is from [AX95] (actually the result given there is more general since I consider only the case in which the weight and order are relatively prime). In the interest of simplicity, I have eliminated one condition that, although easy to include, never applies to circulant weighing matrices, by the Self-Conjugacy bound (Theorem 3.2.6).

Theorem 3.3.5. *Let $v, v^* \in \mathbb{N}$ and let $A = \sum_{i=1}^{v} a_i g_i \in \mathbb{Z}[\mathbf{G}]$, where $\mathbf{G}$ is an abelian group of order v and exponent v^*. Assume that $AA^{(-1)} = m^2$, for some $m \in \mathbb{N}$, and assume that $\sum_{i=1}^{v} a_i = m$ (as opposed to $-m$). Suppose that $(v,m) = 1$. Let $s \in \mathbb{N}$, let $e_1, ..., e_s \in \mathbb{N}$, and let $p_1, ..., p_s$ be primes. Further assume that $k = p_1^{e_1} \cdots p_s^{e_s}$ divides m. Now assume that there exists $t \in \mathbb{N}$ such that, for each $i = 1, ..., s$, there exists $f_i \in \mathbb{Z}$ such that $p^{f_i} \equiv t \pmod{v^*}$. If $(v, M(m^2/k^2)) = 1$, then t is a multiplier of A.*

Proof. For every character χ of $\mathbf{G}$, $\chi(A)\overline{\chi(A)} = m^2$. Let $p_i^{e_i} || k$ and let $\langle p_i^{2e_i} \rangle = P_1^{r_1} \cdots P_u^{r_u}$ be the unique prime ideal decomposition of $\langle p_i^{2e_i} \rangle$. For each $j = 1, ..., u$ and for each χ, either $\chi(A) \in P_j$ or $\overline{\chi(A)} \in P_j$. If $\chi(A) \in P_j$, then, by Theorem 3.1.3, $\chi(A^{(t)}) = \chi(A)^{(p^{f_i})} \in P_j$. It follows that $\chi(A^{(t)}A^{(-1)}) = \chi(A^{(t)})\chi(A^{(-1)}) \in \langle p_i^{2e_i} \rangle$. Since $(p_i, v) = 1$, we have, by Theorem 3.2.3, that $A^{(t)}A^{(-1)} \equiv 0 \pmod{p_i^{2e_i}}$. Applying this procedure to each prime divisor of k, we deduce that $A^{(t)}A^{(-1)} \equiv 0 \pmod{k^2}$ and, consequently, $V = \frac{1}{k^2} A^{(t)} A^{(-1)} \in \mathbb{Z}[\mathbf{G}]$.

$VV^{(-1)} = \frac{m^4}{k^4}$. Since $(v, M(m^2/k^2)) = 1$, Theorem 3.3.2 implies that $V = \frac{m^2}{k^2} g$,

for some $g \in \mathbf{G}$. Multiplying both sides of this equation by A, we deduce that $A^{(t)} = gA$. □

The next result is one of the main tools used in the classification of circulant weighing matrices of prime power weight; it follows directly from Lemma 3.3.1 and Theorem 3.3.5.

Corollary 3.3.6. *Let $A \in \mathbb{Z}[\mathbf{G}]$, where $\mathbf{G}$ is an abelian group of order n, and assume that $AA^{(-1)} = p^{2r}$. Further, assume that $(p, n) = 1$. Then there exists $g \in \mathbf{G}$ such that $(gA)^{(p)} = gA$.*

For instance, let β generate the cyclic group of order 13. We showed, in Section 2.3.1, that $\theta(\beta) = \beta^2 + \beta^4 + \beta^5 + \beta^6 - \beta^7 - \beta^8 + \beta^{10} - \beta^{11} + \beta^{12}$ is the group ring polynomial of a $CW(13, 9)$. Note that $\theta(\beta)^{(3)} = \theta(\beta)$.

The following definition plays a central role in all of the theoretical material to be presented in the remainder of this thesis. $A \in \mathbb{Z}[\mathbf{G}]$ is *proper* if there is no subgroup $\mathbf{S}$ of $\mathbf{G}$ such that Supp(A) lies in a coset of $\mathbf{S}$. Obviously, if one can find all proper circulant weighing matrices of weight k^2, then one can find all circulant weighing matrices of weight k^2.

The following lemma, from [AAMS08], is similar to Theorem 3.3.2; the difference is that, for a given prime number p and $r \in \mathbb{N}$, it allows us to determine a *finite* set of integers that includes all possible orders n such that $(n, p) = 1$ and such that there exists a proper $CW(n, p^{2r})$. For each $a \in \mathbf{G}$, let $o(a)$ denote the order of a.

Lemma 3.3.7. *Let $\mathbf{G}$ be the cyclic group of order n and suppose that p is a prime that does not divide n. Let $A = \sum_{i=1}^{s} a_i X_i \in \mathbb{Z}[\mathbf{G}]$, where $X_1, ..., X_s$ are pairwise disjoint subsets of $\mathbf{G}$. Assume that $AA^{(-1)} = p^{2r}$ and that A is proper. Then n is a*

divisor of the least common multiple of $p-1$, p^2-1, ..., p^u-1, *where* $u = max\{|X_i| : i = 1, ..., s\}$.

Proof. By Corollary 3.3.6 we can assume, replacing A with one of its translates if necessary, that $A^{(p)} = A$. Let $h \in \mathrm{Supp}(A)$. If $h \in X_i$, then $\mathrm{orb}_p(h) \subseteq X_i$. So, for each $h \in \mathrm{Supp}(A)$,

$$\mathrm{ord}_{o(h)}p = |\mathrm{orb}_p(h)| \leq |X_i| \leq u.$$

Since A is proper, $\mathbf{G} = \langle \mathrm{Supp}(A) \rangle$. For each $h \in \mathrm{Supp}(A)$, $o(h)|p^t - 1$, where $t = \mathrm{ord}_{o(h)}p \leq u$. It follows that n is a divisor of the least common multiple of $p-1$, p^2-1, ..., p^u-1. □

For example, by Corollary 1.6.4, the group ring polynomial of a $CW(n, 9)$ has 6 coefficients equal to 1 and 3 equal to -1. So it follows from Lemma 3.3.7 that if there exists a proper $CW(n, 9)$ such that $(3, n) = 1$, then n is a divisor of $2^4 \times 5 \times 7 \times 11^2 \times 13$.

The next lemma, also from [AAMS08], helps us deal with these cases. Note that there is no loss of generality from the assumption that $A^{(p)} = A$, because of Corollary 3.3.6.

Lemma 3.3.8. *Let* $\mathbf{G}$ *be the cyclic group of order* n *and suppose that* p *is a prime that does not divide* n. *Let* $A = \sum_{i=1}^{s} a_i X_i \in \mathbb{Z}[\mathbf{G}]$, *where* $X_1, ..., X_s$ *are pairwise disjoint subsets of* $\mathbf{G}$ *such that* $|X_1| \geq |X_i|$ *for each* $i \geq 2$. *Assume that* $AA^{(-1)} = p^{2r}$ *and that* A *is proper. Further, suppose that* $A^{(p)} = A$ *and that there exists a prime* q *and an integer* f *such that* $q^f | n$ *and* $ord_{q^f}p > |X_i|$, *for each* $i \geq 2$. *Then*

$$A = C + a_1 \sum_{i=1}^{d} orb_p h_i,$$

where $h_1, ..., h_d \in Supp\,(X_1)$ *and* $Supp\,(C) \subseteq K = \{g \in \mathbf{G} | q^f$ *does not divide* $o(g)\}$.

Proof. Let $h \in \mathrm{Supp}\,(A)$ and suppose that $q^f | o(h)$. Then $|\mathrm{orb}_p h| \geq \mathrm{ord}_{q^f} p$. So $h \in \mathrm{Supp}\,(X_1)$ and $\mathrm{orb}_p h \subseteq X_1$. It follows that

$$A = C + a_1 \sum_{i=1}^{d} \mathrm{orb}_p h_i,$$

where $h_1, ..., h_d \in \mathrm{Supp}\,(X_1)$ and $C \subseteq K$. □

For example, suppose that there exists a proper $CW(n, 9)$ with Hall polynomial A such that $n = ma$ is a divisor of $2^4 \times 5 \times 7 \times 11^2 \times 13$ and m is either equal to 2^4, 5, or 7. Assume further that $A^{(3)} = A$. Since A is proper, there exists $h \in \mathrm{Supp}(A)$ such that $m | o(h)$. $\mathrm{ord}_{2^4} 3 = \mathrm{ord}_5 3 = 4$ and $\mathrm{ord}_7 3 = 6$. If $m = 2^4$ or $m = 5$, then $|\mathrm{orb}_3 h|$ is a multiple of 4. Hence, since $|\mathrm{orb}_3 h| \leq 6$, $|\mathrm{orb}_3 h| = 4$. Likewise, if $m = 7$, $|\mathrm{orb}_3 h| = 6$. Further, in each case, we infer that $o(h) = m$. Since A can contain at most one orbit of size 4 or 6, Lemma 3.3.8 implies that $A = C + \mathrm{orb}_p \mathbf{h}$, where $\mathrm{Supp}(C) \subseteq K = \{g \in \mathbf{G} | m$ does not divide $o(g)\}$.

Let $\mathbf{H}$ be a subgroup of $\mathbf{G}$ such that $|\mathbf{H}| = 2^3 a$ if $m = 2^4$ and $|\mathbf{H}| = a$ if $m = 5$ or $m = 7$. Let $\tau_{\mathbf{H}}$ be the canonical epimorphism from $\mathbf{G}$ onto $\mathbf{G}/\mathbf{H}$. If $o(h) = 2^4$, then $\tau_{\mathbf{H}}(A) = -1 + 4\tau_{\mathbf{H}}(h)$. If $o(h) = 5$, then $\tau_{\mathbf{H}}(A) = -1 + \mathrm{orb}_3 \tau_{\mathbf{H}}(h)$. And if $o(h) = 7$, then $\tau_{\mathbf{H}}(A) = -3 + \mathrm{orb}_3 \tau_{\mathbf{H}}(h)$. In each case, $\tau_{\mathbf{H}}(h) \neq 1$. It follows that the coefficients of the identity in $\tau_{\mathbf{H}}(A)\,(\tau_{\mathbf{H}}(A))^{(-1)}$ are 17, 5, and 15, respectively. Each contradicts the fact that, since A is the Hall polynomial of a $CW(n, 9)$,$\tau_{\mathbf{H}}(A)\,(\tau_{\mathbf{H}}(A))^{(-1)} = 9$. Thus, the exists no proper $CW(n, 9)$ such that $n = ma$.

Considering the remaining special cases ($m = 2, 2^2, 2^3, 11, 11^2, 13$) and arguing in a similar fashion, the authors of [AAMS08] are able to establish that the only orders

n, relatively prime to 3, such that there exists a proper $CW(n,9)$ are 13 and 26. We display a proper $CW(13,9)$ in Section 2.2.2.

3.3.2 Type 2 Multiplier Results

A different set of tools is required to deal with the case that the weight and order have a common divisor. The results given in this section require separate treatment for the case that the weight is an odd prime power and the case that the weight is an even prime power. This is a recurring phenomenon in number theory ([IR82], p.43). Recall that, earlier in this thesis, separate methods were presented for constructing $CW(\frac{q^d+1}{q-1}, q^d)$'s in these two cases.

In order to avoid getting bogged down in technical detail, I will consider only the case in which q is an odd prime power. Analogous techniques for dealing with the even prime power case were developed in [ALM+06a] and used in [ALM+06b] to classify all possible orders of circulant weighing matrices of weight 16.

The ideas presented in this section had their origin in a paper of Ma [Ma96] from 1996 and were developed and refined by Arasu and Ma in a series of papers ([AM98], [AM01a], [AM01b], [ALM+06a], [ALM+06b], and [AAMS08]). The first result is from [Ma96] and it will be used often. In what follows, for a finite group $\mathbf{G}$, $\exp(\mathbf{G})$ refers to the exponent of $\mathbf{G}$.

Lemma 3.3.9. *Let $\mathbf{G} = \langle\alpha\rangle \times \mathbf{H}$ be an abelian group. Let $o(\alpha) = p^r$, for some prime p, and let $exp(\mathbf{H}) = w$. If $(w,p) = 1$ and if $\sigma : \mathbb{Z}[\zeta_w][\mathbf{G}] \to \mathbb{Z}[\zeta_{wp^r}][\mathbf{H}]$ is the ring homomorphism defined by $\sigma(\alpha) = \zeta_{p^r}$ and $\sigma(h) = h$ (for each $h \in \mathbf{H}$), then*

$$Ker(\sigma) = \{\langle\alpha^{p^{r-1}}\rangle x \,|\, x \in \mathbb{Z}[\zeta_w][\mathbf{G}]\}$$

(here $\langle \alpha^{p^{r-1}} \rangle$ denotes the sub-group of $\mathbf{G}$ generated by $\alpha^{p^{r-1}}$).

Proof. Clearly, $\{\langle \alpha^{p^{r-1}} \rangle x \,|\, x \in \mathbb{Z}[\zeta_w][\mathbf{G}]\} \subseteq \mathrm{Ker}(\sigma)$. Set $y = \sum_{h \in \mathbf{H}} \sum_{i=0}^{p^r-1} a_{ih} \alpha^i h$, where $a_{ih} \in \mathbb{Z}[\zeta_w]$. $\sigma(y) = 0$ implies that $\sum_{i=0}^{p^r-1} a_{ih} \zeta_{p^r}^i = 0$, for each h. But $\langle \alpha^{p^{r-1}} \rangle$ is the cyclotomic polynomial for ζ_{p^r} over $\mathbb{Z}[\zeta_w]$. Hence, for each $h \in \mathbf{H}$, $\langle \alpha^{p^{r-1}} \rangle$ divides $\sum_{i=0}^{p^r-1} a_{ih} \alpha^i$. □

By applying Lemma 3.3.9 repeatedly, we deduce the following lemma.

Lemma 3.3.10. *Let $\mathbf{G} = \langle \alpha \rangle \times \mathbf{H}$ be an abelian group. Let $o(\alpha) = u$, let $exp(\mathbf{H}) = w$, and let $(w, u) = 1$. If $\sigma : \mathbb{Z}[\zeta_w][\mathbf{G}] \to \mathbb{Z}[\zeta_{wu}][\mathbf{H}]$ is the ring homomorphism defined by the rule $\sigma(\alpha) = \zeta_u$ and $\sigma(h) = h$ (for each $h \in \mathbf{H}$), then $Ker(\sigma) = \{\sum_i^r \langle \alpha^{u/p^i} \rangle x_i \,|\, x_i \in \mathbb{Z}[\zeta_w][\mathbf{G}]\}$, where $p_i, ..., p_r$ are all of the prime divisors of u.*

The next result, from [AM98], allows us, in some cases, to establish a multiplier-like condition when the weight and order are not relatively prime.

Lemma 3.3.11. *Let $\mathbf{G} = \langle \alpha \rangle \times \mathbf{H}$ be an abelian group. Suppose that $\mathbf{G}$ has exponent $v = uw$, where $o(\alpha) = u$ and w is the exponent of $\mathbf{H}$ (so $(u, w) = 1$). Suppose that $y \in \mathbb{Z}[\mathbf{G}]$ and $\sigma \in Gal(\mathbb{Q}(\zeta_v)/\mathbb{Q})$ satisfy the following two conditions:*

(i) there exists $n \in \mathbb{N}$ with $(n, w) = 1$ and such that, for each character χ of $\mathbb{Z}[\mathbf{G}]$ such that $\chi(\alpha) = \zeta_u$, $\chi(y)\overline{\chi(y)} = n$;

(ii) each prime ideal divisor of $\langle n \rangle$ is fixed under the action of σ.

If $\sigma(\zeta_v) = \zeta_v^t$, then

$$y^{(t)} = \pm \beta y + \sum_{i=1}^{r} \langle \alpha^{u/p_i} \rangle x_i$$

where $\beta \in \mathbf{G}$, $x_1, ..., x_r \in \mathbb{Z}[\mathbf{G}]$, and $p_1, ..., p_r$ are all of the prime divisors of u. If u is even, then the sign of βy can be chosen arbitrarily.

Proof. Define a ring homomorphism $\rho : \mathbb{Z}[\mathbf{G}] \to \mathbb{Z}[\zeta_u][\mathbf{G}]$ by the rule $\rho(\alpha) = \zeta_u$ and $\rho(h) = h$, for $h \in \mathbf{H}$. Let $y_1 = \rho(y)$ and let $y_2 = \rho\left(y^{(t)}\right)$. By condition (i) and Theorem 3.2.3,

$$y_1\overline{y_1}^{(-1)} = n.$$

Let P be a prime ideal that contains n. Then, by condition (ii), for each character χ of $\mathbb{Z}[\mathbf{G}]$, if $\chi(y_1) \in P$, then $\chi(y_2) \in P$. Thus, $\chi(y_2)\overline{\chi(y_1)} \in \langle n \rangle$. Consequently, by Theorem 3.2.3, there exists $x \in \mathbb{Z}[\mathbf{G}]$ such that

$$y_2\overline{y_1}^{(-1)} = nx. \tag{3.5}$$

But

$$n^2 x\overline{x}^{(-1)} = y_2\overline{y_2}^{(-1)}y_1\overline{y_1}^{(-1)} = n^2,$$

so that $x\overline{x}^{(-1)} = 1$. Now write $x = \sum_{h\in\mathbf{H}} \theta_h h$, where, for each $h \in \mathbf{H}$, $\theta_h \in \mathbb{Z}[\zeta_u]$. Let $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_u)/\mathbb{Q})$. Then

$$\left(\sum_{h\in\mathbf{H}} \theta_h^\tau h\right)\left(\sum_{h\in\mathbf{H}} \overline{\theta_h^\tau} h^{(-1)}\right) = \left(x\overline{x}^{(-1)}\right)^\tau = 1^\tau = 1.$$

So, for each $h \in \mathbf{H}$, $\theta_h^\tau\overline{\theta_h^\tau} \leq 1$. It then follows by Lemma 3.1.2 and Lemma 3.1.11 that $x = \pm\zeta_u^c h$, for some $c \in \mathbb{Z}$, $h \in \mathbf{H}$. Multiplying both sides of 3.5 by y_1, we deduce that $y_2 = \pm\zeta_u^c h y_1$. The result then follows by Lemma 3.3.10. If u is even, the sign of βy can be chosen arbitrarily, since $\zeta_u^{u/2} = -1$. □

Now I will focus on the odd prime techniques referred to above.

Lemma 3.3.12. *[AMOS] Let $\mathbf{G} = \langle\alpha\rangle \times \mathbf{H}$ be an abelian group and p be an odd*

prime such that $o(\alpha) = p^s$, *exp* $(\mathbf{H}) = w$, *and* $(p, w) = 1$. *Further assume that there exists* $A \in \mathbb{Z}[\mathbf{G}]$ *such that* $\chi(A)\overline{\chi(A)} = p^{2r}$ *for each character* χ *of* $\mathbb{Z}[\mathbf{G}]$ *such that* $\chi(\alpha) = \zeta_{p^s}$. *Suppose that* $t \in \mathbb{Z}$ *is a primitive root modulo* p^s *that is congruent to* 1 *modulo* w. *Then there exists* $b \in \mathbb{Z}$ *such that*

$$\left(\alpha^b A\right)^{(t)} = \beta\alpha^b A + \langle \alpha^{p^{s-1}} \rangle X$$

for some $X \in \mathbb{Z}[\mathbf{G}]$ *where* $\beta \in \mathbf{H}$ *and* $o(\beta) \mid (p-1, w)$.

Proof. Define a ring homomorphism $\rho : \mathbb{Z}[\mathbf{G}] \to \mathbb{Z}[\zeta_{p^s}][\mathbf{H}]$ by the rule $\rho(\alpha) = \zeta_{p^s}$ and, for $h \in \mathbf{H}$, $\rho(h) = h$. Note that, by Lemma 3.1.15 and the Chinese Remainder Theorem, there exists an integer t such that t is a primitive root modulo p^s and such that $t \equiv 1 \pmod{w}$. Define $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^s w})/\mathbb{Q})$ by the rule $\sigma(\zeta_{p^s w}) = \zeta_{p^s w}^t$. By Theorem 3.1.3, each prime ideal divisor of $\langle p^r \rangle$ is fixed under the action of σ. Thus, by Lemma 3.3.11, there exists $\beta \in \mathbf{H}$ and $a \in \mathbb{Z}$ such that

$$\rho(A)^{(\sigma)} = \pm\beta\zeta_{p^s}^a \rho(A). \tag{3.6}$$

By Lemma 3.1.15,

$$\rho(A) = \rho(A)^{\left(\sigma^{p^{s-1}(p-1)}\right)} = \beta^{p^{s-1}(p-1)}\rho(A).$$

Since $(p, w) = 1$, it follows that $o(\beta) \mid (p-1, w)$.

There exists $c \in \mathbb{Z}$ such that $\chi_0(\rho(A)) = \epsilon\zeta_{p^s}^c p$, where $\epsilon = \pm 1$ and χ_0 is the principal character of $\mathbf{H}$. One can deduce that $\zeta_{p^s}^{tc} = \pm\zeta_{p^s}^{a+c}$ by applying χ_0 to 3.6. It follows that $\left(\zeta_{p^s}^b \rho(A)\right)^\sigma = \beta\zeta_{p^s}^b \rho(A)$ for $b = -c$. Finally, by Lemma 3.3.9, we conclude that

$\left(\alpha^b A\right)^{(t)} = \beta\alpha^b A + \langle\alpha^{p^{s-1}}\rangle X$, for some $X \in \mathbb{Z}[\mathbf{G}]$. □

The next result, also from [AM98], shows that if we restrict our attention to $CW(n, p^2)$'s and assume that p strictly divides n, we can say even more.

Lemma 3.3.13. *Let $\mathbf{G} = \langle\alpha\rangle \times \mathbf{H}$ be an abelian group such that $o(\alpha) = p$ (for some odd prime p), $exp(\mathbf{H}) = w$, and $(p, w) = 1$. Further assume that $A \in \mathbb{Z}[\mathbf{G}]$ satisfies $\chi(A)\overline{\chi(A)} = p^2$ for each character χ such that $\chi(\alpha) = \zeta_p$. Suppose that $t \in \mathbb{Z}$ is a primitive root modulo p that is congruent to 1 modulo w. Then there exists $b \in \mathbb{Z}$ such that*

$$\left(\alpha^b A\right)^{(t)} = \beta\alpha^b A + \epsilon(1-\beta)\langle\alpha\rangle g$$

for $\epsilon = \pm 1$, $g \in \mathbf{H}$, and $\beta \in \mathbf{H}$ such that $o(\beta) \mid (p-1, w)$.

Proof. It follows from Lemma 3.3.12 that there exists $X \in \mathbb{Z}[\mathbf{G}]$, $\beta \in \mathbf{H}$, and $b, s \in \mathbb{Z}$ such that

$$\left(\alpha^b A\right)^{(t)} = \beta\alpha^b A + \langle\alpha\rangle X \tag{3.7}$$

and such that $o(\beta) \mid (p-1, w)$. Let τ be the natural epimorphism from $\mathbf{G}$ to $\mathbf{G}/\langle\alpha\rangle$. Since $t \equiv 1 \pmod{w}$, $\tau(A) = \tau\left(A^{(t)}\right)$. So, by applying τ to 3.7, we deduce that

$$(1 - \tau(\beta))\tau(A) = p\tau(X). \tag{3.8}$$

Note that, for each c, $\alpha^c\langle\alpha\rangle = \langle\alpha\rangle$, so $\langle\alpha\rangle X = \langle\alpha\rangle\tau(X)$. But, if $\beta = 1$, then, by 3.8, $\tau(X) = 0$, and it follows that $\langle\alpha\rangle X = 0$ (which completes the proof, in this case). So assume that $\beta \neq 1$. It then follows, by 3.8, that the identity coefficient of $\tau(X)\tau(X)^{(-1)}$ is 2. Consequently, we infer that $\mathrm{Supp}(\tau(X))$ contains exactly 2 elements. So, by 3.8, $\tau(X) = \epsilon(1 - \tau(\beta))g^*$, for $\epsilon = \pm 1$ and $g^* \in \mathbf{G}/\langle\alpha\rangle$.

Therefore, $\langle\alpha\rangle X = \epsilon(1-\beta)\langle\alpha\rangle g$, where $\tau(g) = g^*$. Further, we may, without loss of generality, choose $g \in \mathbf{H}$ (since $\alpha^c\langle\alpha\rangle = \langle\alpha\rangle$). □

Lemma 3.3.13 is important since, by the results in the next section, there exists a proper $CW(n, p^2)$ such that $p|n$ only if $p||n$. In [AM01b], Lemma 3.3.13 is used to deduce some results about $CW(n, p^2)$'s where $p|n$ and $p > 7$. However, as I mentioned earlier, I will focus on outlining how the authors of [AAMS08] use Lemma 3.3.13 to classify circulant weighing matrices of weight 9 (in fact, the remainder of the results in this section are from [AAMS08]).

Note that for $p = 3$, the β in Lemma 3.3.13 must have order 1 or order 2. For the rest of this section, let $o(\alpha) = 3$ and let $\mathbf{P} = \langle\alpha\rangle$.

Lemma 3.3.14. *Let $\mathbf{G} = \mathbf{P} \times \mathbf{H}$ be an abelian group and let $(|\mathbf{H}|, 3) = 1$. Suppose that $A \in \mathbb{Z}[\mathbf{G}]$ is such that, for some t such that $t \equiv 2 \pmod 3$ and $t \equiv 1 \pmod{|\mathbf{H}|}$, $A^{(t)} = \beta A + (1-\beta)\mathbf{P}g$, where $g, \beta \in \mathbf{H}$ and $o(\beta) = 2$. Let $\mathbf{K}$ be the group generated by α and β. Let $A = \sum_{h\in I} A_h h$, where I is a complete set of coset representatives of $\mathbf{K}$ that includes g, and $A_h \in \mathbb{Z}[\mathbf{K}]$. Then*

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

for each h such that $\mathbf{K}h \neq \mathbf{K}g$, and

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

If the coefficients of A are $0, \pm 1$, then $a_g, a_{g\alpha}, a_{g\alpha^2} \in \{0, 1\}$ and $|Supp(A)| = 3$.

Proof. Let h be such that $\mathbf{K}h \neq \mathbf{K}g$. Then $A_h^{(t)} = \beta A_h$. Let

$$A_h = a_h + a_{h\beta}\beta + a_{h\alpha}\alpha + a_{h\alpha^2}\alpha^2 + a_{h\beta\alpha}\beta\alpha + a_{h\beta\alpha^2}\beta\alpha^2.$$

We have that

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

and

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

By comparing coefficients of like terms, we deduce that $a_h = a_{h\beta}$, $a_{h\alpha^2} = a_{h\alpha\beta}$, and $a_{h\alpha} = a_{h\beta\alpha^2}$. It follows that

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

as required.

A_g, on the other hand, satisfies $A_g^{(t)} = \beta A_g + (1-\beta)\mathbf{P}$. By reasoning similar to that used in the first part of this proof, we deduce that $a_g = a_{g\beta} + 1$, $a_{g\alpha^2} = a_{g\beta\alpha} + 1$, and $a_{g\alpha} = a_{g\beta\alpha^2} + 1$. Thus,

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

If we make the restriction that A has $0, \pm 1$ coefficients, then it follows from the above equation that we must have $a_{\mathbf{g}}, a_{\mathbf{g}\alpha}, a_{\mathbf{g}\alpha^2} \in \{0, 1\}$ and, consequently, that $|\mathrm{Supp}A_{\mathbf{g}}| = 3$. □

The following lemma anticipates the Field Descent results presented in the next section.

Lemma 3.3.15. *Let* $\mathbf{G} = \mathbf{P} \times \mathbf{H}$ *be an abelian group and let* $(|\mathbf{H}|, 3) = 1$. *Suppose that* $A \in \mathbb{Z}[\mathbf{G}]$ *is the group ring polynomial of a* $CW(n, 9)$ *developed over* $\mathbf{G}$. *Then there exists* $b \in \mathbb{Z}$ *such that*

$$\alpha^b A = B + (\mathbf{P} - 1) C + (\mathbf{P} - 2) D + \mathbf{P} E$$

for some $B, C, D, E \in \mathbb{Z}[\mathbf{H}]$ *with* $0, \pm 1$ *coefficients and pairwise disjoint support.*

Proof. By Lemma 3.3.13 there exist $t, b \in \mathbb{Z}$ such that $t \equiv 2 \pmod 3$, $t \equiv 1 \pmod{|\mathbf{H}|}$, and $\left(\alpha^b A\right)^{(t)} = \beta \alpha^b A + \epsilon (1 - \beta) \mathbf{P} g$, where $g, \beta \in \mathbf{H}$, $o(\beta) = 1$ or 2, and $\epsilon = \pm 1$. Replace A with $\alpha^b A$. If $\epsilon = -1$, replace g with $g\beta$. It then follows that

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

Assume that $o(\beta) = 2$. Then, by Lemma 3.3.14, the non-zero coefficients of A_g comprise one of the following four sets: (i) $\{1, 1, 1\}$, (ii) $\{-1, 1, 1\}$, (iii) $\{-1, -1, 1\}$, and (iv) $\{-1, -1, -1\}$. By Corollary 1.6.4, $A = X_1 - X_2$, where X_1, X_2 are group ring elements, with $0, 1$ coefficients, such that $|X_1| = 6$ and $|X_2| = 3$. For each $h \in \mathbf{G}$ such that $\mathbf{K}h \neq \mathbf{K}g$, elements of A_h with any given coefficient come in pairs. Hence, since $|X_2| = 3$, A_g contains either one or three -1's. This rules out cases (i) and (iii).

Suppose that case (ii) holds. Let $\tau_{\mathbf{K}}$ be the canonical epimorphism from $\mathbf{G}$ to $\mathbf{G}/\mathbf{K}$. Then $\tau_{\mathbf{K}}(A) = g(1 + 2h_1 + 2h_2 - 2h_3)$, where h_1, h_2, h_3 are non-indentity elements of $\mathbf{G}/\mathbf{K}$. If h_1, h_2, h_3 are all distinct, then the identity coefficient of $\tau(A)\tau(A)^{(-1)}$ is

13. If $h_1 = h_2 \neq h_3$, then the identity coefficient of $\tau(A)\tau(A)^{(-1)}$ is 21. If h_1 equals either h_2 or h_3, then the identity coefficient of $\tau(A)\tau(A)^{(-1)}$ is 5. Each possibility contradicts the fact that, since A is the Hall polynomial of a $CW(n,9)$, the identity coefficient of $\tau(A)\tau(A)^{(-1)}$ is 9.

Suppose that case (iv) holds. Then $\tau_{\mathbf{K}}(A) = -3g + \tau_{\mathbf{K}}(X_1)$. Thus, since $\tau(A)\tau(A)^{(-1)} = 9$, we must have that $\tau_{\mathbf{K}}(X_1) = 0$, which is impossible.

Thus, it must be the case that $o(\beta) = 1$, so that $A^{(t)} = A$. Then, since t is a primitive root modulo 3, it follows, by Lemma 3.3.14, that

$$A = Y_0 + \mathbf{P}Y_1, \tag{3.9}$$

for $Y_0, Y_1 \in \mathbb{Z}[\mathbf{H}]$.

Write $A = \sum_{h\in J} B_h h$, where $B_h \in \mathbb{Z}[\mathbf{P}]$ and J is a complete set of coset representatives of $\mathbf{P}$. By 3.9, for each $h \in J$, $B_h = \delta + \omega(\alpha + \alpha^2)$, where $\delta, \omega \in \{0, \pm 1\}$. Define elements $B, C, D, E \in \mathbb{Z}[\mathbf{H}]$ by the following rules: For each $h \in J$: $\delta = \pm 1$ and $\omega = 0$ if and only if $h \in \mathrm{Supp}B$; $\delta = 0$ and $\omega = \pm 1$ if and only if $h \in \mathrm{Supp}C$; $\delta = -\omega = \pm 1$ if and only if $h \in \mathrm{Supp}D$; $\delta = \omega = \pm 1$ if and only if $h \in \mathrm{Supp}E$. Then

$$A = B + (\mathbf{P} - 1)C + (\mathbf{P} - 2)D + \mathbf{P}E,$$

as required. □

The tools are now in place to complete the proof of Theorem 3.2.10 (except that we defer to the next section the demonstration that if there exists a proper $CW(n,p^2)$ such that $p|n$, then $p||n$). I believe that I have found an error in the proof from [AAMS08], but I've figured out how to patch it up with an ugly proof

of my own.

Theorem 3.3.16. *There exists a proper $CW(n,9)$, where $3|n$, if and only if $n = 24$.*

Proof. Let A be the group ring polynomial of a proper $CW(n,9)$ developed over the cyclic group $\mathbf{G} = \mathbf{P} \times \mathbf{H}$, where $|\mathbf{H}| = w$ and $(w,3) = 1$. By Lemma 3.3.15, there exist pairwise disjoint elements $B, C, D, E \in \mathbb{Z}[\mathbf{H}]$, with $0, \pm 1$ coefficients, such that

$$A = B + (\mathbf{P} - 1) C + (\mathbf{P} - 2) D + \mathbf{P}E. \tag{3.10}$$

Let $\tau_{\mathbf{P}}$ be the canonical epimorphism from $\mathbf{G}$ to $\mathbf{G}/\mathbf{P}$. Since $AA^{(-1)} = 9$, it follows, by considering the coefficient of α in $AA^{(-1)}$, that

$$|\mathrm{Supp}\,(\tau_{\mathbf{P}}(C))| - |\mathrm{Supp}\,(\tau_{\mathbf{P}}(D))| + 3|\mathrm{Supp}\,(\tau_{\mathbf{P}}(E))| = 0. \tag{3.11}$$

By 3.10,

$$\tau_{\mathbf{P}}(A) = \tau_{\mathbf{P}}(B) + 2\tau_{\mathbf{P}}(C) + \tau_{\mathbf{P}}(D) + 3\tau_{\mathbf{P}}(E).$$

Suppose that $|\mathrm{Supp}\,(\tau_{\mathbf{P}}(E))| \geq 1$. Then, by 3.11, $|\mathrm{Supp}(D)| \geq 1$, so that $\tau_{\mathbf{P}}(A)\,\tau_{\mathbf{P}}(A)^{(-1)} > 9$, which is impossible. Thus, $|\mathrm{Supp}\,(\tau_{\mathbf{P}}(E))| = 0$ and, consequently, so is $|\mathrm{Supp}(E)|$. It follows, by 3.11, that $|\mathrm{Supp}\,(\tau_{\mathbf{P}}(C))| = |\mathrm{Supp}\,(\tau_{\mathbf{P}}(D))|$. So, by examining the coefficient of the identity element in $\tau_{\mathbf{P}}(A)\,\tau_{\mathbf{P}}(A)^{(-1)} = 9$, we infer that $|\mathrm{Supp}\,(\tau_{\mathbf{P}}(B))| + 5|\mathrm{Supp}\,(\tau_{\mathbf{P}}(C))| = 9$.

Since A is a proper $CW(n,9)$, we cannot have $|\mathrm{Supp}\,(\tau_{\mathbf{P}}(C))| = 0$. So the only possibility is that $|\mathrm{Supp}\,(\tau_{\mathbf{P}}(B))| = 4$ and $|\mathrm{Supp}\,(\tau_{\mathbf{P}}(C))| = |\mathrm{Supp}\,(\tau_{\mathbf{P}}(D))| = 1$. Hence,

$$\tau_{\mathbf{P}}(A) = \tau_{\mathbf{P}}(B) + 2\gamma h_1 + \epsilon h_2, \tag{3.12}$$

for $\gamma, \epsilon = \pm 1$ and $h_1 \neq h_2 \in (\mathbf{G}/\mathbf{P}) \setminus \mathrm{Supp}(\tau_{\mathbf{P}}(B))$. By Corollary 3.3.6, there exists $g \in \mathbf{G}$ such that $(g\tau_{\mathbf{P}}(A))^{(3)} = g\tau_{\mathbf{P}}(A)$. So let $X = \gamma g \tau_{\mathbf{P}}(A) = 2x + X_1 - X_2$, where $x = gh_1$ and X_1 and X_2 are disjoint subsets of $\mathbf{G}/\mathbf{P}$ such that x is not an element of $X_1 \cup X_2$. Since x is the only element in the support of X with coefficient 2, $X^{(3)} = X$ implies that $o(x)$ is either 1 or 2. Since $XX^{(-1)} = 9$, we have, by Corollary 1.6.3, that

$$4 + |X_1| + |X_2| = 9$$

and

$$2 + |X_1| - |X_2| = \pm 3. \tag{3.13}$$

The system of equations 3.13 has solution $(|X_1|, |X_2|) = (0, 5)$ or $(3, 2)$. Therefore, by Lemma 3.3.7, w is a divisor of $\mathrm{lcm}(3-1, 3^2-1, ..., 3^5-1) = 2^4 \times 5 \times 11^2 \times 13$. These possible values for m will be divided into separate cases.

Case 1: $w = 11a$, for some $a \in \mathbb{Z}$. Since A is proper, there exists $h \in \mathrm{Supp}X$ such that $11|o(h)$. Thus, $|\mathrm{orb}_3(h)| = 5$ and, consequently, we must have that $|X_1| = 0$ and $|X_2| = 5$. We can assume, without loss of generality, that $h = gh_2$.

Therefore, by 3.10 and 3.12,

$$\gamma g^* A = -\sum_{i=1}^{4} h^{*3^i} + (\mathbf{P} - 1)\, x^* - (\mathbf{P} - 2)\, h^* \tag{3.14}$$

for $g^*, h^*, x^* \in \mathbf{H}$ such that $\tau_{\mathbf{P}}(g^*) = g$, $\tau_{\mathbf{P}}(h^*) = h$, and $\tau_{\mathbf{P}}(x^*) = x$.

In what follows, I make essential use of the fact that $h \in \mathbf{H}$.

Since $h^{3^5} = 1$, $o(h) \,|11^2 \times 2$. Thus, since $o(x)$ is either 1 or 2, and since A is proper, $|H||11^2 \times 4$.

Suppose first that $o(x) = 1$. Then, since there exist no i, j such that $h^{*3^i} h^*$ is

equal to either $h^{*^{3^j}}$ or h^*, and since $h^{*^2} \neq 1$, $\mathbf{r}_1 \cdot \mathbf{r}_{h^*} = -2$, where $\mathbf{r}_1$ and $\mathbf{r}_{h^*}$ are, respectively, the 1^{st} and $h^{*^{th}}$ rows (the rows are indexed by group elements as in the Cayley Representation) of the matrix W associated with A. But this is impossible, since W is a circulant weighing matrix.

Now suppose that $o(x) = 2$. Let $\mathbf{S} = \langle h \rangle$ and suppose that x is not an element of $\mathbf{S}$. Let $T = \tau_{\mathbf{H}}(\gamma\tau_{\mathbf{P}}(A))$. Then $T = 2x - 5$. So the identity coefficient of $TT^{(-1)}$ is 29, which contradicts the fact that, since A the the group ring polynomial of a $CW(n, 9)$, $TT^{(-1)} = 9$.

So let $x \in \mathbf{S}$. Then $|\mathbf{S}|$ is either 22 or 242.

Let $|\mathbf{S}| = 22$. Then $X = -h^3 - h^9 - h^5 - h^{15} + 2h^{11} - h$. So $\mathbf{r}_1 \cdot \mathbf{r}_{h^4} = -1$, where $\mathbf{r}_1$ and $\mathbf{r}_{h^4}$ are, respectively, the 1^{st} and $h^4 -$ th rows of the matrix W associated with X. But this is impossible, since $XX^{(-1)} = 9$.

Suppose that $|\mathbf{S}| = 242$. Then $hh^{120} = x$, but $xh^{120} \neq h$. Further, for $i = 0, ..., 4$, $h^{3^i}h^{120} \neq h^{3^i}$. So $\mathbf{r}_1 \cdot \mathbf{r}_{h^{120}} = -2$, where $\mathbf{r}_1$ and $\mathbf{r}_{h^{120}}$ are, respectively, the 1^{st} and $h^{120} -$ th rows of the matrix W associated with A. Again, this is impossible.

Case 2: $w = ma$, for m equal to either 2^4 or 5. Since A is proper, there exists $h \in \text{Supp}(X)$ such that $m|o(h)$. Then, $|\text{orb}_3(h)| = 4$, and it follows that $|X_1| = 0$ and $|X_2| = 5$. So, we must have that $X = 2x - \text{orb}_3(h) - y$, where $y \neq x$, and $o(y)$ is either 1 or 2 (since $|\text{orb}_3(y)| = 1$). Define $\mathbf{K}$ as the (unique) subgroup of $\mathbf{G/P}$ such that, if $m = 2^4$, $|\mathbf{K}| = 2^3a$, and, if $m = 5$, $|\mathbf{K}| = a$. Then, in both cases $x, y \in \mathbf{K}$.

Let $\tau_{\mathbf{K}}$ be the natrural epimorphism from $\mathbf{G/P}$ to $(\mathbf{G/P})/\mathbf{K}$. If $m = 2^4$, $\tau_{\mathbf{K}}(X) = 1 - 4\tau_{\mathbf{K}}(\mathbf{h})$. If $m = 5$, then $\tau_{\mathbf{K}}(X) = 1 - \text{orb}_3(\tau_{\mathbf{K}}(h))$. So, the identity coefficient in $\tau_{\mathbf{K}}(X)\tau_{\mathbf{K}}(X)^{(-1)}$ is either 17 or 5. Both possibilities contradict the fact that,

since A is the Hall polynomial of a $CW(n,9)$, the coefficient in question is equal to 9.

Case 3: $w = ma$, for $m = 13$. There exists an element $h \in \mathrm{Supp}(X)$ such that $13|o(h)$. Since $|\mathrm{orb}_3(h)| \leq 5$, we must have that either $o(h) = 13$ or $o(h) = 26$. So $|\mathrm{orb}_3(h)| = 3$.

$\mathbf{G/P}$ contains at most two elements y such that $y^3 = y$. Suppose that it does contain two (say 1 and y) and that both are in $\mathrm{Supp}(X)$. Then $X = \pm(1-y) \pm \mathrm{orb}_3(h)$, so that the identity coefficient of $XX^{(-1)}$ is 5, which is impossible.

Thus, we must have that $X = 2x - z - z^3 \pm \mathrm{orb}_3(h)$, where $z^8 = 1$ and $o(z) \neq 2$ (so that $o(z)$ is either 4 or 8). Let χ be a character of $\mathbf{G}$ such that $\chi(h) = 1$ and $\chi(z) = -1$. It follows that $\chi(x) = 1$. So $\chi(X) = \chi\left(X^{(-1)}\right) = 4 \pm 3$, and, consequently, $XX^{(-1)} \neq 9$ (contradiction).

Case 4: $w = 4$. By Theorem 3.2.9, there exists no $CW(12,9)$.

Therefore, we must have that $w = 2^3$, and, in fact, if we let $\langle h \rangle$ be the cyclic group of order 8, $A = -1 + (1-h^4)(h+h^3) + (\alpha+\alpha^2)(1+h^4)$ is the Hall polynomial of a proper $CW(24,9)$. □

Instead of 3.14, the authors of [AAMS08] claim that

$$\gamma g^* A = -\sum_{i=1}^{4} h^{*3^i} + (\mathbf{P}-1)x^* + (\mathbf{P}-2)h^* \quad (?)$$

for $g^*, h^*, x^* \in \mathbf{H}$ such that $\tau_{\mathbf{P}}(g^*) = g$, $\tau_{\mathbf{P}}(h^*) = h$, and $\tau_{\mathbf{P}}(x^*) = x$. They proceed to use arguments like the one presented at the end of the "Type 1 Multiplier Results" section to rule out case 1. However, I believe that (?) is incorrect. Furthermore, if it is correct, then no further arguments are needed to rule out case 1, since (?) implies

that $\gamma \mathbf{g}^* A$ has five coefficients equal to -1 and four coefficients equal to 1, which is impossible, since A is the group ring polynomial of a $CW(n, 9)$ and, consequently, must have six coefficients equal to 1 and three equal to -1.

3.4 The Field Descent Method

The method of using "field descent" arguments to study combinatorial designs with an underlying group structure provides the key to proving non-existence results beyond the reach of the self-conjugacy approach and the multiplier method presented earlier in this chapter. Field descent arguments first appeared in papers of Ma [Ma96] and Schmidt [Sch] in the late 1990's. Schmidt was the first to develop these kinds of arguments into a comprehensive method [Sch99]. Ma and Arasu later developed the ideas from [Ma96] in the papers ([AM98], [AM01a], [AM01b], [ALM+06a], [ALM+06b], and [AAMS08]) alongside their Type 2 multiplier results (Section 3.3.2).

Initially, Schmidt's approach to this method was different than Ma's. In Schmidt's early field descent papers (see [Sch99] and [Sch], for instance), it was shown that any cyclomic integer $X \in \mathbb{Z}[\zeta_m]$ of absolute value n must lie, up to multiplication by a root of unity, in the subfield (hence, "field descent") $\mathbb{Z}\left[\zeta_{F(m,n)}\right]$, where $F(m, n)$ is an integer that is often much smaller than m (it is "usually" equal to the square-free part of m). As a consequence of this result, Schmidt was able to derive bounds on the parameters of difference sets, large weight group developed weighing matrices, etc.

The approach taken by Ma and Arasu, on the other hand, was to show that, under certain conditions, a group ring element whose character values all have absolute

value n admits a decomposition into a sum of two group ring elements with disjoint support: one lying in a proper sub-group ring and another that is somewhat well behaved.

In 2005, Schmidt and Leung [LS05] combined these approaches. As a result, they were able both to generalize Arasu and Ma's results and some of the bounds from [Sch99] (unfortunately, not the weighing matrix bound) and to provide a unified framework in which to view two apparently disparate methods. Further, they were able to use their difference set bound to verify the Circulant Hadamard Matrix Conjecture for each order v such that $4 < v < 548,964,900$.

Beyond providing the only bound on the weight of large weight group developed weighing matrices (other than the non-existence of circulant conference matrices), the field descent method also provides the tools to prove the important result of Arasu and Ma, referred to in the previous section, that, for any prime p, there exists a proper $CW(n, p^2)$ such that $p|n$ only if $p||n$.

3.4.1 The Main Result

We begin by defining the function $F(m, n)$. Let $m, n \in \mathbb{N}$ and suppose that $m = \prod_{i=1}^{t} p_i^{c_i}$ is the prime power decomposition of m. For each prime $q|n$, let $m_q = \prod_{p_i \neq q} p_i$ if m is odd or $q = 2$ and let $m_q = 4 \prod_{p_i \neq 2,q} p_i$ otherwise.

Define $F(m, n) = \prod_{i=1}^{t} p_i^{b_i}$ to be the minimum multiple of the prime divisors of m such that, for each $i = 1, ..., t$ and for each prime $q|n$, at least one of the following conditions holds:

(a) $q = p_i$ and $(p_i, b_i) \neq (2, 1)$,

(b) $b_i = c_i$,

(c) $q \neq p_i$ and $q^{\mathrm{ord}_{m_q}(q)}$ is not equivalent to 1 modulo $p_i^{b_i+1}$.

Theorem 3.4.1. *[LS05] Let $\mathbf{G} = \langle\alpha\rangle \times \mathbf{H}$ be an abelian group, let $o(\alpha) = u$, and let $exp(H) = w$. Suppose that $(u, w) = (n, w) = 1$. Let $A \in \mathbb{Z}[\mathbf{G}]$ be such that $|\chi(A)| = n$ for each character χ such that $\chi(\alpha) = \zeta_u$. Define $F_u = gcd(u, F(uw, n))$ and let $\mathbf{S}$ be the subgroup of $\langle\alpha\rangle$ of order F_u. Then there exists $A_{\mathbf{S}} \in \mathbb{Z}[\mathbf{S} \times \mathbf{H}]$ such that $A = \alpha^e A_{\mathbf{S}} + \sum_{i=1}^{r} \langle\alpha^{u/p_i}\rangle x_i$, for some $e \in \mathbb{Z}$, $x_1, ..., x_r \in \mathbb{Z}[\mathbf{G}]$, and where $p_1, ..., p_r$ are all of the prime divisors of u. Further, we can choose $A_{\mathbf{S}}$ so that the support of $\sum_{i=1}^{r} \langle\alpha^{u/p_i}\rangle x_i$ is contained in $\mathbf{G} \backslash \alpha^e (\mathbf{S} \times \mathbf{H})$.*

Proof. Let $u = \prod_{i=1}^{r} p_i^{c_i}$ and let $F_u = \prod_{i=1}^{r} p_i^{b_i}$. By the Chinese Remainder Theorem, we can choose $t \in \mathbb{Z}$ such that, for each p_i, $t \equiv 1 \pmod{p_i^{b_i}}$ and t is not equivalent to 1 modulo $p_i^{b_i+1}$. Then, by Lemma 3.1.14, $\mathrm{ord}_{p_i^{c_i}}(t) = p_i^{c_i - b_i}$ (if $p_i^{c_i} = 2$, then $\mathrm{ord}_{p_i^{c_i}}(t) = p_i^{c_i - b_i} = 1$). Let σ be the automorphism of $\mathbb{Q}(\zeta_{uw})$ defined by $\zeta_{uw}^{(\sigma)} = \zeta_{uw}^t$. First, we show that σ fixes each prime ideal that contains n.

Let $uw = \prod_{i=1}^{s} p_i^{c_i}$, for some $s \geq r$. Let q be a prime such that $q|n$, let $u_q = \prod_{i=1, p_i \neq q}^{s} p_i^{c_i}$, and let $Q = q^{\mathrm{ord}_{m_q}(q)}$. By the definition of m_q, for each $i \leq r$ such that $p_i \neq q$, $Q \equiv 1 \pmod{p_i}$. Further, if uw is even and $q \neq 2$, then $Q \equiv 1 \pmod{4}$. It then follows, from the definition of $F(uw, n)$ and from Lemma 3.1.14, that, for each $i \leq r$ such that $p_i \neq q$, $\mathrm{ord}_{p_i^{c_i}}(Q)$ is a power of p_i greater than or equal to $\mathrm{ord}_{p_i^{c_i}}(t) = p_i^{c_i - b_i}$. So, by Lemma 3.1.14, part b, for each $i \leq r$ such that $p_i \neq q$, there exists an integer $s(i)$ such that $Q^{s(i)} \equiv t \pmod{p_i^{c_i}}$. Further, since $(n, w) = 1$, $(Q, w) = 1$. Thus, since $t \equiv 1 \pmod{w}$, for each $p_i^{c_i}|w$, there exists an integer $s(i)$ such that $Q^{s(i)} \equiv t \pmod{p_i^{c_i}}$. By the Chinese Remainder Theorem, we can choose an integer h such that, for each i with $p_i \neq q$, $h \equiv s(i) \pmod{p_i^{c_i}}$. Hence, $Q^h \equiv t \pmod{p_i^{c_i}}$ for each i such that $p_i \neq q$, and it follows that $Q^h \equiv t \pmod{u_q}$. Thus,

since Q is a power of q and since q is an arbitrary prime divisor of n, Theorem 3.1.3 implies that σ fixes each prime ideal that contains n.

Since w is the exponent of $\mathbf{H}$ and since $(w,n)=1$, Lemma 3.3.11 implies that

$$A^{(t)} = (-1)^{\ell} bA + \sum_{i=1}^{r} \langle \alpha^{u/p_i} \rangle x_i, \tag{3.15}$$

for some $\ell \in [0,1]$, $b \in \mathbf{G}$, $x_1, ..., x_r \in \mathbb{Z}[\mathbf{G}]$, and where ℓ can be chosen to be zero if u is even. Define a homomorphism $\rho : \mathbb{Z}[\mathbf{G}] \to \mathbb{Z}[\zeta_u][\mathbf{H}]$ by the rule $\rho(\alpha) = \zeta_u$ and $\rho(h) = h$, for each $h \in \mathbf{H}$. Interpret σ as the automorphism of $\mathbb{Z}[\zeta_u][\mathbf{H}]$ acting according to the rule $\left(\sum_{h\in\mathbf{H}} a_h h\right)^{(\sigma)} = \sum_{h\in\mathbf{H}} a_h^{(\sigma)} h$, where $a_h \in \mathbb{Z}[\zeta_u]$. Let $E = \rho(A)$. Then, since $\zeta_u^{(\sigma)} = \zeta_u^t$ and since, for each $h \in \mathbf{H}$, $h^t = h$, $E^{(\sigma)} = E^{(t)}$. So, by 3.15,

$$E^{(\sigma)} = (-1)^{\ell} c \zeta_u^j E, \tag{3.16}$$

for $c \in \mathbf{H}$, $j \in \mathbb{Z}$ such that $\rho(b) = \zeta_u^j c$. Define $y = \mathrm{ord}_{uw}(t)$. It follows, from the definition of t, that $y = \prod_{i=1}^{r} p_i^{c_i - b_i}$. Since $(u,w) = 1$, it follows that $(y,w) = 1$. Applying 3.16 repeatedly, we deduce

$$E = E^{(\sigma^y)} = (-1)^{\ell y} c^y \zeta_u^{j\left(\frac{t^y-1}{t-1}\right)} E.$$

So $E\left(1 - (-1)^{\ell y} \mathbf{c}^y \zeta_u^{j(t^y-1)/(t-1)}\right) = 0$ in $\mathbb{Z}[\zeta_u][\mathbf{H}]$. For each character χ of $\mathbf{H}$, $\chi(E) = n$ (this follows from "appending" χ to a non-principal character of $\langle \alpha \rangle$). So, for each character χ of $\mathbf{H}$, $\chi\left(1 - (-1)^{\ell y} c^y \zeta_u^{j(t^y-1)/(t-1)}\right) = 0$. Therefore, by Theorem 2.3.8,

$$(-1)^{\ell y} c^y \zeta_u^{j(t^y-1)/(t-1)} = 1 \tag{3.17}$$

in $\mathbb{Z}[\zeta_u][\mathbf{H}]$. Since $(y, w) = 1$, we must have $c = 1$. Further, $\ell = 0$. For, if u is even, we can choose $\ell = 0$, and, if u is odd, then y is odd, and, since -1 is an even root of unity, it follows that, if $\ell = 1$, the left side of 3.17 is a negative number, which is impossible. So, by 3.16,

$$E^{\sigma} = \zeta_u^j E \tag{3.18}$$

and, since $\zeta_u^{j(t^y-1)/(t-1)} = 1$,

$$j\frac{t^y - 1}{t-1} \equiv 0 \pmod{u}. \tag{3.19}$$

For each $i = 1, ..., r$, the exact power of p_i dividing $t-1$ is p^{b_i} and, by Lemma 3.1.14, the exact power of p_i dividing $t^y - 1$ is $p_i^{c_i}$ (since $y = \prod_{i=1}^{r} p_i^{c_i - b_i}$). Therefore, the exact power of p_i dividing $(t^y - 1)/(t-1)$ is $p_i^{c_i - b_i}$. By 3.19,

$$j(t^y - 1)/(t-1) \equiv 0 \pmod{p^{c_i}}.$$

So we have that

$$j \equiv 0 \pmod{p_i^{b_i}}.$$

For each i, $p_i^{b_i+1}$ does not divide $t-1$. So, by the Chinese Remainder Theorem, there exists $d \in \mathbb{Z}$ that satisfies the simultaneous set of congruences

$$(t-1)d + j \equiv 0 \pmod{p_i^{c_i}}, \quad i = 1, ..., r$$

(if $b_i = c_i$, choose d so that $d \equiv 0 \pmod{p_i^{c_i}}$). Then, by 3.18,

$$\left(E\zeta_u^d\right)^{(\sigma)} = E\zeta_u^{j+dt} = E\zeta_u^d. \tag{3.20}$$

Let $E\zeta_u^d = \sum_{h\in\mathbf{H}} E_h h$, for $E_h \in \mathbb{Z}[\zeta_u]$. By 3.20, for each $h \in \mathbf{H}$, $E_h^{(\sigma)} = E_h$. Consequently, $E_h \in \mathbb{Z}[\zeta_{F_u}]$, since $\mathbb{Q}(\zeta_{F_u})$ is the fixed field of $\sigma|_{Q(F_u)}$. Since ρ is onto, there exists $A_{\mathbf{S}} \in \mathbb{Z}[\mathbf{S}\times\mathbf{H}]$ such that $\rho(A_{\mathbf{S}}) = E\zeta_u^d$. Then $\rho(A) = E = \rho\left(\alpha^{-d}A_{\mathbf{S}}\right)$ and, by Lemma 3.3.10,

$$A = \alpha^{-d}A_{\mathbf{S}} + \sum_{i=1}^{r}\langle\alpha^{u/p_i}\rangle x_i,$$

where $x_1, ..., x_r \in \mathbb{Z}[\mathbf{G}]$.

Since $p_1\cdots p_r$ is a divisor of F_u, $\langle\alpha^{u/p_i}\rangle \subseteq \mathbf{S}\times\mathbf{H}$. For each i, write $x_i = x_i^* + x_i^{**}$, where $x_i^* \in (\mathbf{S}\times\mathbf{H})$ and $x_i^{**} \in \mathbf{G}/(\mathbf{S}\times\mathbf{H})$. If we replace $\alpha^{-d}A_{\mathbf{S}}$ by $\alpha^{-d}A_{\mathbf{S}} + \sum_{i=1}^{r}\langle\alpha^{u/p_i}\rangle x_i^*$ and x_i by x_i^{**}, then $\mathrm{Supp}\left(\sum_{i=1}^{r}\langle\alpha^{u/p_i}\rangle x_i\right) \subseteq \mathbf{G}\backslash\alpha^{-d}(\mathbf{S}\times\mathbf{H})$. □

Notice that if, for some odd prime p, $u = p^r$, and $n = p^s$ in the above result, then $F_u = p$. This result will come in handy in the next section.

Theorem 3.4.1 is the most general known field descent result. However, under more restrictive assumptions, it is possible to guarantee an even steeper descent (i.e. a decomposition such that $\mathbf{S}$ is an even smaller subgroup). Schmidt and Leung obtain such a result [LS05]. It is rather complicated to state; the next result, which I state without proof, is an important sub-case of Schmidt and Leung's result that was originally obtained by Arasu and Ma [AM01b].

Lemma 3.4.2. *Let $\mathbf{G} = \langle\alpha\rangle \times \mathbf{H}$ be an abelian group of order $v = p^t w$ such that $o(\alpha) = p^t$, where p is an odd prime. Further suppose that $|\mathbf{H}| = w$ and $(p(p-1), w) = 1$. Let $y \in \mathbb{Z}[\mathbf{G}]$ satisfy $\chi(y)\overline{\chi(y)} = p^{2r}$ (for some integer r) for each character χ that is non-principal on $\langle\alpha^{p^{t-1}}\rangle$. Then $y = \alpha^c x_0 + \langle\alpha^{p^{t-1}}\rangle x_1$, where $x_1 \in \mathbb{Z}[\mathbf{G}]$ and $c \in \mathbb{Z}$ and where $x_0 \in \mathbb{Z}[\mathbf{H}]$ is such that $x_0 x_0^{(-1)} = p^{2r}$.*

Some field descent conditions are obtained in [ALM+06b] and [ALM+06a] that

work in the case that the weight is an even prime power.

3.4.2 A Reduction Theorem

All of the results in this section are from [AM01b] (although, Arasu and Ma deduce the reduction theorem in question from their own field descent result, which is less general than the one given in the previous section). We begin with two lemmas.

Lemma 3.4.3. *Let* $\mathbf{G} = \langle \alpha \rangle \times \mathbf{H}$ *be an abelian group such that* $o(\alpha) = p$*, where* p *is an odd prime,* $exp(\mathbf{H}) = w$*, and* $(p, w) = 1$*. Let* $t \in \mathbb{Z}$ *be a primitive root modulo* p *such that* $t \equiv 1 \pmod{w}$*. Assume that* $A \in \mathbb{Z}[\mathbf{G}]$ *is such that, for some* $\beta \in \mathbf{H}$*,* $A^{(t)} = \beta A$*. Let* $m = o(\beta)$ *and let* $\{\mathbf{h_1}, ..., \mathbf{h_v}\}$ *be a complete set of coset representatives of* $\langle \beta \rangle$ *in* $\mathbf{H}$*. Write* $Q_j = \{\alpha^{t^i}\beta^{j-i} | i = 0, 1, ..., p-2\}$*, for* $j = 0, 1, ..., m-1$*. Let* B *be the cyclic group generated by* β*. Then we have that*

$$A = B\sum_{k=1}^{v} a_k \mathbf{h_k} + \sum_{j=0}^{m-1}\sum_{k=1}^{v} b_{jk} Q_j \mathbf{h_k},$$

for some $a_k, b_{jk} \in \mathbb{Z}$*.*

Proof. The result follows from the assumption that $A^{(t)} = \beta A$, since then, for each j, the coefficient of $\beta^j h_k$ is the same as the coefficient of $\beta^{j+1} h_k$ and, for each i, j, the coefficient of $\alpha^{t^i}\beta^j h_k$ is the same as the coefficient of $\alpha^{t^{i-1}}\beta^{j+1} h_k$. □

Lemma 3.4.4. *Let* $\mathbf{G} = \langle \alpha \rangle \times \mathbf{H}$ *be an abelian group such that* $o(\alpha) = p$*, where* p *is an odd prime,* $exp(\mathbf{H}) = w$*, and* $(p, w) = 1$*. There exists no element* $A \in \mathbb{Z}[\mathbf{G}]$ *with* $0, \pm 1$ *coefficients such that* $AA^{(-1)} = p^2 - p\langle \alpha \rangle$*.*

Proof. Suppose that there does exist such an A. Let $t \in \mathbb{Z}$ be a primitive root

modulo p such that $t \equiv 1 \pmod{w}$. By Lemma 3.3.12, there exists $b \in \mathbb{Z}$ such that

$$\left(\alpha^b A\right)^{(t)} = \alpha^b \beta A + \langle\alpha\rangle X, \tag{3.21}$$

where $\beta \in \mathbf{H}$, $X \in \mathbb{Z}[\mathbf{G}]$, and $m = o(\beta)$ is a divisor of $(w, p-1)$. Since $AA^{(-1)} = p^2 - p\langle\alpha\rangle$, for each character χ that is principal on $\langle\alpha\rangle$, $\chi(A) = 0$. Consequently, since $\chi(\langle\alpha\rangle) = 0$ for each character χ that is non-principal on $\langle\alpha\rangle$, for all characters χ of $\mathbf{G}$, $\chi(\langle\alpha\rangle A) = 0$. So, by Theorem 2.3.8, $\langle\alpha\rangle A = 0$. Multiplying each side of 3.21 by $\langle\alpha\rangle$ and using the fact that $\langle\alpha\rangle = \langle\alpha\rangle^{(t)}$, we can deduce that $\langle\alpha\rangle X = 0$, so that $\left(\alpha^b A\right)^{(t)} = \alpha^b \beta A$. Thus, by Lemma 3.4.3,

$$\alpha^b A = \langle\beta\rangle \sum_{k=1}^{v} a_k \mathbf{h_k} + \sum_{j=0}^{m-1} \sum_{k=1}^{v} b_{jk} Q_j \mathbf{h_k}, \tag{3.22}$$

for $a_k, b_{jk} \in \{0, \pm 1\}$. Since $\langle\alpha\rangle Q_j = [(p-1)/m]\langle\alpha\rangle\langle\beta\rangle$, we can deduce, by multiplying both sides of 3.22 by $\langle\alpha\rangle$, that, for each k,

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

Since $a_k \in \{0, \pm 1\}$, either $p - 1 = m$ or, for each k, $a_k = 0$. But $\langle\beta\rangle Q_j = \langle\beta\rangle(\langle\alpha\rangle - 1)$, so, if $a_k = 0$ for each k (and, consequently, $\sum_{j=0}^{m-1} b_{jk} = 0$ for each k), then

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

which is impossible, since $AA^{(-1)} = p^2 - p\langle\alpha\rangle \neq 0$. Thus, $p - 1 = m$. Define x_1 and x_2 as the number of $+1$ coefficients of A and the number of -1 coefficients of

A, respectively. By examining the coefficient of 1 in $AA^{(-1)}$ we can deduce that $x_1 + x_2 = p^2 - p$ and, by applying the principal character to $\langle\alpha\rangle A = 0$, we can deduce that $x_1 - x_2 = 0$. So $x_1 = x_2 = p(p-1)/2$. From 3.22, x_1 and x_2 are divisible by $p-1$, which is impossible since p is an odd prime. □

Now we are ready to prove the main result in this section, which completes the justification of Theorem 3.3.16.

Theorem 3.4.5. *Let* $\mathbf{G} = \langle\alpha\rangle \times \mathbf{H}$ *be an abelian group such that* $o(\alpha) = p^s$, $exp(\mathbf{H}) = w$, *and* $s > 1$. *Assume that* $(w, p) = 1$. *Let* $A \in \mathbb{Z}[\mathbf{G}]$ *satisfy* $AA^{(-1)} = p^2$ *and suppose that the coefficients of* A *are* 0 *and* ± 1. *Then there exists* $b \in \mathbb{Z}$ *such that* $\alpha^b A \in \mathbb{Z}\left[\langle\alpha^{p^{s-1}}\rangle \times \mathbf{H}\right]$.

Proof. Set $\mathbf{P} = \langle\alpha^{p^{s-1}}\rangle$. By Theorem 3.4.1, there exists $b \in \mathbb{Z}$, $B \in \mathbf{Z}[\mathbf{P} \times \mathbf{H}]$, and $C \in \mathbb{Z}[\mathbf{G}]$, with $\mathrm{Supp}(C) \subseteq \mathbf{G}/(\mathbf{P} \times \mathbf{H})$, such that

$$\alpha^b A = B + \mathbf{P}C.$$

Let $\tau_{\mathbf{P}}$ be the canonical epimorphism from $\mathbf{G}$ to $\mathbf{G}/\mathbf{P}$.

$$\tau_{\mathbf{P}}\left(\alpha^b A\right) = \tau_{\mathbf{P}}(B) + p\tau_{\mathbf{P}}(C).$$

But $\tau_{\mathbf{P}}\left(\alpha^b A\right)\tau_{\mathbf{P}}\left(\alpha^b A\right)^{(-1)} = p^2$. Hence, either $\tau_{\mathbf{P}}(C) = 0$ or $\tau_{\mathbf{P}}(B) = 0$ and $\tau_{\mathbf{P}}(C) = \pm g$, for some $g \in \mathbf{G}/\mathbf{P}$.

Assume the second case holds. Then $\mathbf{P}B = 0$ and $A = B \pm \mathbf{P}h$, for some $h \in \mathbf{G}\backslash(\mathbf{P} \times \mathbf{H})$. Hence, since $\left(\alpha^b A\right)\left(\alpha^b A\right)^{(-1)} = p^2$, $BB^{(-1)} = p^2 - p\mathbf{P}$. But, since B has $0, \pm 1$ coefficients, this contradicts Lemma 3.4.4.

So assume that $\tau_{\mathbf{P}}(C) = 0$. Then $\mathbf{P}C = 0$ and, consequently, $\alpha^b A = B \in \mathbb{Z}[\mathbf{P} \times \mathbf{H}]$.

□

Arasu and Ma were able to show that we can sometimes say something even stronger (like Lemma 3.4.2, this result will be stated without proof).

Theorem 3.4.6. *Let* $\mathbf{G} = \langle\alpha\rangle \times \mathbf{H}$, *where* $o(\alpha) = p^s$, $exp(\mathbf{H}) = w$, $(p(p-1), w) = 1$, *and* p *is a prime greater than* 3. *Let* $A \in \mathbb{Z}[\mathbf{G}]$ *satisfy* $AA^{(-1)} = p^{2r}$ *and suppose that* A *has* $0, \pm 1$ *coefficients. Then there exists* $b \in \mathbb{Z}$ *such that* $\alpha^b A \in \mathbb{Z}[\mathbf{H}]$.

See ([ALM+06b], [ALM+06a], and [AM01b]) for even more results of this type.

3.4.3 A Bound on Large Weight Circulant Weighing Matrices

Using Theorem 3.4.1, it is possible to recover Schmidt's bound on large weight group developed weighing matrices from [Sch99]. In [Sch], Schmidt and Leung improve Schmidt's bound on difference sets [Sch99] by using an approach that combines group ring algebra with number theory. However, the argument they use to establish this improvement seems to depend crucially on the assumption that the group ring elements (being used in the argument) have positive coefficients, and there is no clear way to remedy the situation so that their method applies to group ring elements with both positive and negative coefficients. It is then an open question whether or not the weighing matrix bound obtained in this section is the best possible that one can obtain from the Field Descent Method.

We shall need the following lemma, which Schmidt describes as "ugly as well as necessary," from [Sch99].

Lemma 3.4.7. *Let $m = \prod_{i=1}^{t} p_i^{a_i}$, where the p_i's are distinct primes. Let $k|m$, say $k = \prod_{i=1}^{s} p_i^{b_i}$, where $s \leq t$ and, for each i, $1 \leq b_i \leq a_i$. Then*

$$B_{m,k} = \left\{ \prod_{i=1}^{s} \zeta_{p_i^{a_i}}^{r_i} \prod_{i=s+1}^{t} \zeta_{p_i}^{k_i} \zeta_{p_i^{a_i}}^{l_i} : 0 \leq r_i \leq p_i^{a_i - b_i} - 1, \;\; 0 \leq k_i \leq p_i - 2, \;\; 0 \leq l_i \leq p_i^{a_i - 1} - 1 \right\}$$

is an integral basis for $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}(\zeta_k)$. Let $X \in \mathbb{Z}[\zeta_m]$ have the form

$$X = \sum_{j=0}^{m-1} b_j \zeta_m^j \tag{3.23}$$

where $b_0, ..., b_{m-1} \in \mathbb{Z}$ are such that, for all j, $|b_j| \leq C$, for some constant C. Then

$$X = \sum_{x \in B_{m,k}} x \sum_{j=0}^{k-1} c_{x,j} \zeta_k^j, \tag{3.24}$$

where, for each x, j, $c_{x,j} \in \mathbb{Z}$ and $|c_{x,j}| \leq 2^{t-s} C$.

Proof. By Lemma 3.1.4, $\zeta_{p_i}^{p_i - 1} = -1 - \zeta_{p_i} - \cdots - \zeta_{p_i}^{p_i - 2}$. Consequently, the set comprised of elements of $B_{m,k}$ with scalar coefficients from $\mathbb{Z}[\zeta_k]$ spans $\mathbb{Z}[\zeta_m]$. But, by Lemma 3.1.10, $|B_{m,k}| = \dim(\mathbb{Z}[\zeta_m] : \mathbb{Z}[\zeta_k]) = \phi(m)/\phi(k)$. So, $B_{m,k}$ is a basis for $\mathbb{Z}[\zeta_m]$ over $\mathbb{Z}[\zeta_k]$.

For each j,

$$\zeta_m^j = \zeta_k^{u_j} \prod_{i=1}^{s} \zeta_{p_i^{a_i}}^{r_{ij}} \prod_{i=s+1}^{t} \zeta_{p_i}^{k_{ij}} \zeta_{p^{a_i}}^{l_{ij}} \tag{3.25}$$

where $0 \leq u_j \leq k-1$, $0 \leq r_{ij} \leq p_i^{a_i - b_i} - 1$, $0 \leq k_{ij} \leq p_i - 1$, and $0 \leq l_{ij} \leq p_i^{a_i - 1} - 1$. To transform X from the representation given in 3.23 to the one given in 3.24, we have to factor out all the terms $b_j \zeta_m^j$ in 3.23 that contain a factor $\zeta_{p_i}^{p_i - 1}$ in the representation 3.25 using the identity $\zeta_{p_i}^{p_i - 1} = -1 - \zeta_{p_i} - \cdots - \zeta_{p_i}^{p_i - 2}$. This can be

done step by step for $i = s+1, ..., t$. In each of these $t-s$ steps, the range of the coefficients at most doubles. Consequently, for each x, j, $|c_{x,j}| \leq 2^{t-s}C$. □

Let $\delta(r)$ denote the number of distinct prime divisors of r. The next lemma is also from [Sch99] (a tighter bound can be obtained if one assumes that the coefficients in question are non-negative).

Lemma 3.4.8. *Let*

$$X = \sum_{i=0}^{m-1} a_i \zeta_m^i,$$

where $a_0, ..., a_{m-1} \in \mathbb{Z}$ *and, for all* i, $|a_i| \leq C$, *for some constant* C. *Assume further that* $X \in \mathbb{Z}[\zeta_f]$, *for some divisor* f *of* m, *and that* $X\overline{X}$ *is an integer. Then* $X\overline{X} \leq 2^{2\delta(m)-\delta(f)}C^2 f$.

Proof. By Lemma 3.4.7,

$$X = \sum_{x \in B_{m,f}} x \sum_{j=0}^{f-1} b_{x,j} \zeta_f^j, \tag{3.26}$$

where $|b_{x,j}| \leq 2^{\delta(m)-\delta(f)}C$. Since $X \in \mathbb{Z}[\zeta_f]$, each term $\sum_{j=0}^{f-1} b_{x,j}\zeta_f^j$ in 3.26 with $x \neq 1$ vanishes. Hence,

$$X = \sum_{j=0}^{f-1} b_{1,j} \zeta_f^j.$$

So,

$$X\overline{X} = \sum_{k=0}^{f-1} c_k \zeta_f^k,$$

where $|c_k| \leq 2^{2\delta(m)-2\delta(f)}C^2 f$. Note that $B_{f,1}$ is an integral basis of $\mathbb{Q}(\zeta_f)$ over $\mathbb{Q}$. So, again by Lemma 3.4.7,

$$X\overline{X} = \sum_{x \in B_{f,1}} d_x x,$$

where $|d_x| \leq 2^{2\delta(m)-\delta(f)}C^2 f$. Since $X\overline{X}$ is an integer, for each $x \neq 1$, $d_x = 0$. So $X\overline{X} = d_1 \leq 2^{2\delta(m)-\delta(f)}C^2 f$. □

Refer the definition of $F(m,n)$, given at the beginning of Section 3.4.1.

Theorem 3.4.9. *Assume that there exists a* $\mathbf{G}$*-developed* $W(m,s^2)$*. Suppose further that* $\mathbf{U}$ *is a normal subgroup of* $\mathbf{G}$ *such that* $\mathbf{G}/\mathbf{U}$ *is a cyclic group of order* e*. Then*

$$s^2 \leq 2^t F(e,s)|\mathbf{U}|^2,$$

where t *is the number of (distinct) prime divisors of* e*. If there exists a* $CW(m,s^2)$*, then*

$$s^2 \leq 2^r F(m,s),$$

where r *is the number of (distinct) prime divisors of* m*.*

Proof. Let A be the group ring polynomial of a $\mathbf{G}$-developed $W(m,s^2)$ and let $\tau_{\mathbf{U}}$ be the canonical epimorphism from $\mathbf{G}$ to $\mathbf{G}/\mathbf{U}$. Then the each coefficient of $\tau_{\mathbf{U}}(A)$ is smaller in magnitude than $|\mathbf{U}|$ (since the coefficients of A are $0, \pm 1$).

Let α generate $\mathbf{G}/\mathbf{U}$ and let χ be a character of $\langle\alpha\rangle$ that maps $\langle\alpha\rangle$ onto $\mathbb{Z}[\zeta_e]$. By Theorem 3.4.1, there exists $b \in \mathbb{Z}$ such that $\alpha^b A = B + \sum_{i=1}^{r}\langle\alpha^{u/p_i}\rangle x_i$, where $p_1, ..., p_r$ are all of the prime divisors of e and where $B \in \mathbb{Z}[\mathbf{S}]$ ($\mathbf{S}$ is the subgroup of $\langle\alpha\rangle$ of order $F(e,s)$). Further, the support of B is disjoint from the support of $\sum_{i=1}^{r}\langle\alpha^{u/p_i}\rangle x_i$, so that the coefficients of B are also bounded in magnitude by $|\mathbf{U}|$. Since, for each subgroup $\langle\beta\rangle$ of $\langle\alpha\rangle$, $\chi(\langle\beta\rangle) = 0$, it follows that $\chi(A) \in \mathbb{Z}\left[\zeta_{F(e,s)}\right]$. And, since χ is an isomorphism, $\chi(A) = \sum_{j=0}^{F(e,s)-1} a_i \zeta_{F(e,s)}^j$, where, for each j,

$|a_j| \leq |U|$. Thus, by Lemma 3.4.8,

$$s^2 = \chi(\tau_{\mathbf{U}}(A))\,\overline{\chi(\tau_{\mathbf{U}}(A))} \leq 2^t F(e,s)|\mathbf{U}|^2.$$

□

Let m_0 be the square-free part of m. Then the best we can hope for is that $F(m,s) = m_0$ and the worst that we can hope for is that $F(m,s) = m$. The reason that the bound from Theorem 3.4.9 is useful is that $F(m,s)$ often turns out to be equal, roughly, to m_0. In fact, Schmidt [Sch99]) provides an informal argument to establish that if m is (roughly) a product of squared primes, then we can expect that $F(m,s)$ will almost always be (roughly) equal to m_0. So, if m has many factors of the form $p_i^{c_i}$, where p_i is an odd prime and $c_i > 1$, then Theorem 3.4.9 puts severe constraints on the possible weights of a circulant weighing matrix of order m.

As an example, let us use Theorem 3.4.9 to show that there exists no $CW(147,144)$. Note that $147 = 7^2 \cdot 3$ and $144 = 3^2 \cdot 2^4$. Further, $m_2 = 7 \cdot 3 = 21$ and $m_3 = 7$. By straightforward calculation, one can deduce that $o_{m_2}(2) = 6$ and that $2^{o_{m_2}(2)}$ is not congruent to 1 modulo 7^2. Likewise, one can deduce that $o_{m_3}(3) = 7$ and that $3^{o_{m_3}(3)} = 729 \equiv 43 \pmod{7^2}$. It follows that $F(147,12) = 7 \cdot 3 = 21$. Therefore, by Theorem 3.4.9,

$$144 \leq 2^2 \cdot F(147,12) = 4 \cdot 7 \cdot 3 = 84,$$

which is impossible. So there is no $CW(147,144)$.

Schmidt's bound is useful for ruling out the existence of particular large weight circulant weighing matrices, such as $CW(147,144)$'s. However, since the bound is dependent upon the function $F(m,s)$, it does not imply any (other) general

results about large weight circulant weighing matrices. Consequently, the intriguing questions raised in Section 1.10 remain open.

Appendix A

Original contributions

The purpose of this appendix is to note both original contributions to the theory of circulant weighing matrices (and related types of mathematical objects) that have appeared in my thesis and results I have discovered as a consequence of the work done in my thesis.

1) By means of a very straightforward generalization of Craigen's proof that there exist no circulant conference matrices of order $n > 2$, I was able to show that there exist no conference matrices of order $n > 2$ developed over a signed group (Theorem 1.10.3).

2) I proved that every Hankel weighing matrix is either a negacyclic matrix or a circulant matrix (Theorem 1.11.1).

3) I showed that for every prime power q and every $d \in 2n$, there exist $\phi(d)/2$ inequivalent $CW\left(\frac{q^{d+1}-1}{q-1}, q^d\right)$'s, where ϕ is the Euler Toilent function (this improves upon the established result that there exists at least one $CW\left(\frac{q^{d+1}-1}{q-1}, q^d\right)$). Fur-

ther, I showed that the ratio of the cross-correlation of any pair of perfect ternary sequences derived from these matrices to the weight q^d is bounded by a function on the order of $\frac{1}{q}$. These results and the proofs thereof do not appear in this thesis; see [Mil09].

4) By means of a straightforward generalization of a method from [DGS71], I was able to deduce a more general method for constructing negacyclic weighing matrices than has thus far appeared in the literature (see Theorem 2.3.18 and Corollary 2.3.19). By further generalizing results from [DGS71], I was also able to obtain some non-existence results (see Theorem 2.3.20 and Corollary 2.3.21).

5) By making use of a well-known technique called "folding" and by making some fairly obvious observations, I was able to make several improvements to the necessary conditions for the existence of circulant weighing matrices implied by the Self-conjugacy method. See Theorem 3.2.6 for a statement of the previously known result; see Theorem 3.2.9 for my revised version.

6) By making use of a well-known Lemma (Lemma 3.2.12), I obtained some necessary conditions for the existence of circulant weighing matrices (Theorem 3.2.13). This result, which, although unpublished, is probably already well-known to experts in the field, is similar to Theorem 3.2.9.

7) I identified an error in the proof, from [AAMS08], of the result that there exists a $CW(n, 9)$ if and only if n is a multiple of either 13 or 24. I was able to repair the

proof (see p.149-152).

Bibliography

[AAMS08] Miin Huey Ang, K. T. Arasu, Siu Lun Ma, and Yoseph Strassler, *Study of proper circulant weighing matrices with weight 9*, Discrete Mathematics **308** (2008), 2802–2809. (Cited on pages 124, 130, 136, 137, 138, 139, 144, 147, 151, 152 and 168.)

[ABL90] M. Antweiler, L. Bomer, and H. D. Luke, *Perfect ternary arrays*, IEEE Transactions on Information Theory **36** (1990), 696–705. (Cited on page 3.)

[AD96] K. T. Arasu and J. F. Dillon, *Perfect ternary sequences*, Difference Sets, Sequences, and their Correlation Properties (P. V. Kumar T. Helleseth, A. Pott and D. Jungnickel, eds.), Springer, 1996. (Cited on pages 29, 44, 46, 107 and 129.)

[ADJ+96] K. T. Arasu, J. A. Davis, J. Jedwab, Siu Lun Ma, and R. L. McFarland, *Exponent bounds for a family of abelian difference sets*, Groups, Difference Sets, and the Monster (K. T. Arasu, J. F. Dillon, K. Harada, S. Sehgal, and R. Solomon, eds.), no. 129-143, Walter De Gruyer, 1996. (Cited on page 116.)

[ADJP95] K. T. Arasu, J. F. Dillon, D. Jungnickel, and A. Pott, *The solution of the Waterloo problem*, Journal of Combinatorial Theory (A) **17** (1995), 316–331. (Cited on pages 50, 51, 63, 77, 79, 83 and 103.)

[ADLM01] K. T. Arasu, J. F. Dillon, Ka Hin Leung, and Siu Lun Ma, *Cyclic relative difference sets*, Journal of Combinatorial Theory (A) **94** (2001), 118–126. (Cited on pages 50, 51, 84, 92 and 94.)

[ALM+06a] K. T. Arasu, Ka Hin Leung, Siu Lun Ma, Ali Nabavi, and D. K. Ray-Chaudhuri, *Circulant weighing matrices of weight* 2^{2t}, Designs, Codes, and Cryptography **41** (2006), 111–123. (Cited on pages 139, 152, 157 and 161.)

[ALM+06b] ———, *Determination of all possible orders of weight 16 circulant weighing matrices*, Finite Fields and Their Applications **12** (2006), 498–538. (Cited on pages 124, 134, 139, 152, 157 and 161.)

[AM98] K. T. Arasu and Siu Lun Ma, *Abelian difference sets without self-conjugacy*, Designs, Codes, and Crytography **15** (1998), 223–230. (Cited on pages 108, 131, 139, 140, 141, 143 and 152.)

[AM01a] ———, *A non-existence result on difference sets, partial difference sets, and divisible difference sets*, Journal of Statistical Planning and Inference **95** (2001), 67–73. (Cited on pages 139 and 152.)

[AM01b] ———, *Some new results on circulant weighing matrices*, Journal of Algebraic Combinatorics **14** (2001), 91–101. (Cited on pages 139, 144, 152, 157, 158 and 161.)

[AM05] Miin Huey Ang and Siu Lun Ma, *Symmetric weighing matrices constructed using group matrices*, Designs, Codes, and Cryptography **37** (2005), 195–210. (Cited on page 125.)

[Apo74] Tom M. Apostol, *Mathematical analysis: A modern approach to advanced calculus*, Addison Wesley, 1974. (Cited on page 93.)

[Ara98] K. T. Arasu, *A reduction theorem for circulant weighing matrices*, Australasian Journal of Combinatorics **18** (1998), 111–114. (Cited on pages 44, 114 and 120.)

[AS96] K. T. Arasu and Jennifer Sebbery, *Circulant weighing designs*, Journal of Combinatorial Designs **4** (1996), no. 6, 439–447. (Cited on pages 114, 120 and 131.)

[AT99] K. T. Arasu and Dina Torban, *New weighing matrices of weight 25*, Journal of Combinatorial Designs **7** (1999), no. 1, 11–15. (Cited on pages 3 and 49.)

[AX95] K. T. Arasu and Qing Xiang, *Multiplier theorems*, Journal of Combinatorial Designs **3** (1995), 257–268. (Cited on page 135.)

[Bau71] L. D. Baumert, *Cyclic difference sets*, Lecture Notes, vol. 182, Springer-Verlag, 1971. (Cited on page 22.)

[BE66] A. T. Butson and J. E. H. Elliot, *Relative difference sets*, Illinois Journal of Mathematics **10** (1966), 517–531. (Cited on pages 81 and 82.)

[Ber77] Gerald Berman, *Families of skew circulant weighing matrices*, Ars Combinatoria **4** (1977), 293–307. (Cited on page 102.)

[Bha07] Rajendra Bhatia, *Positive definite matrices*, Princeton Series in Applied Mathematics, 2007. (Cited on page 11.)

[BJL99] T. Beth, Dieter Jungnickel, and H. Lenz, *Design theory*, Cambridge University Press, 1999. (Cited on pages 82, 83, 88, 109 and 130.)

[Bos42] R. C. Bose, *An affine analogue of Singer's theorem*, Journal of the Indian Mathematical Society **6** (1942), 1–15. (Cited on page 81.)

[BR98] Albert Beutelspacher and Ute Rosenbaum, *Projective geometry: From foundations to applications*, Cambridge University Press, 1998. (Cited on pages 21, 51, 53, 54, 55, 57 and 76.)

[Bue69] F. Bueckenhout, *Ensembles quadratiques des espaces projectifs*, Math. Z. **110** (1969), 306–318. (Cited on pages 73 and 76.)

[But63] A. T. Butson, *Relations among generalized Hadamard matrices, relative difference sets, and maximal length linear recurring sequences*, Canadian Journal of Mathematics **15** (1963), 42–48. (Cited on page 50.)

[Cha67] J. A. Chang, *Ternary sequences with zero correlation*, Proceedings of the IEEE **55** (1967), 1211–1213. (Cited on page 3.)

[Cra94] R. Craigen, *Trace, symmetry, and orthogonality*, Canadian Mathematical Bulletin **37** (1994), no. 4, 461–467. (Cited on pages 41, 42 and 43.)

[Cra95a] ———, *Signed groups, sequences, and the asymptotic existence of hadamard matrices*, Journal of Combinatorial Theory (Series A) **71** (1995), 241–254. (Cited on pages 36 and 50.)

[Cra95b] ———, *The structure of weighing matrices having large weights*, Designs, Codes, and Cryptography **5** (1995), 199–216. (Cited on page 47.)

[Cra96] ———, *Weighing matrices and conference matrices*, The CRC Handbook of Combinatorial Designs (Colburn and Dinitz, eds.), CRC Press, 1996. (Cited on page 3.)

[Cra06] ———, *Representations of groups, character theory, and orthogonal matrices in combinatorics*, Course Notes for Math 8510, 2006. (Cited on page 88.)

[Cra09] ———, *Thoughts on weighing matrices and weighing problems, circulant matrices and eigenvalues*, Talk delivered to the Applied and Computational Mathematics Seminar at the University of Manitoba, April 2009. (Cited on pages 4 and 12.)

[DGS71] P. Delsarte, J. M. Goethals, and J. J. Seidal, *Orthogonal matrices with zero diagonal II*, Canadian Journal of Mathematics **23** (1971), 816–832. (Cited on pages 3, 51, 103, 105 and 168.)

[Ead80] Peter Eades, *Circulant (v, k, μ)-designs*, Combinatorial Mathematics, VII, vol. 829, Springer, 1980. (Cited on pages 50 and 83.)

[EH76] Peter Eades and Richard Hain, *On circulant weighing matrices*, Ars Combinatoria **2** (1976), 265–284. (Cited on pages 49 and 134.)

[EK97] S. Eliahou and M. Kervaire, *A note on the equation $\theta\overline{\theta} = k + \lambda + \sum$*, Journal of Statistical Planning and Inference **62** (1997), 21–34. (Cited on page 126.)

[Eps98] L. Epstein, *The classification of circulant weighing matrices of weight 16 and odd order*, Master's thesis, Bar-Ilan University, 1998. (Cited on page 101.)

[Gal04] Joseph Gallian, *Contemporary abstract algebra*, Brooks Cole, 2004. (Cited on pages 36, 59, 109, 110, 112 and 122.)

[Gam86] Richard A. Games, *The geometry of quadrics and correlations of sequences*, IEEE Transactions on Information Theory **IT-32** (1986), no. 3, 423–426. (Cited on pages 50, 51, 63 and 79.)

[GG05] Solomon W. Goloumb and Guang Gong, *Signal design for good correlation*, Cambridge University Press, 2005. (Cited on pages 3, 14, 15 and 16.)

[GS79] A. V. Geramita and J. Seberry, *Orthogonal designs: Quadratic forms and Hadamard matrices*, M. Dekker, 1979. (Cited on pages 17, 18 and 25.)

[Had93] Jacques Hadamard, *Resolution d'une question relative aux determinants*, Bulletin des Sciences Mathematical **17** (1893), no. 2, 240–246. (Cited on page 4.)

[Hai77] Richard Hain, *Circulant weighing matrices*, Master's thesis, Australian National University, February 1977. (Cited on pages 3, 12, 44, 46 and 50.)

[Hil65] David Hilbert, *Gesammelte abhandlungen*, AMS Chelsea, 1965. (Cited on page 61.)

[HJ83] Tom Hoholdt and Jorn Justesen, *Ternary sequences with perfect periodic autocorrelation*, IEEE Transactions on Information Theory **IT-29** (1983), no. 4, 597–600. (Cited on pages 3, 50, 51, 63, 73, 77 and 79.)

[Hot42] Harold Hotelling, *The prediction of personal adjustment*, The American Journal of Sociology **48** (1942), no. 1, 61–76. (Cited on pages 9 and 11.)

[Ipa82] V. P. Ipatov, *Contribution to the theory of sequences with perfect periodic autocorrelation properties*, Radio Engrg. Electron. Phys. (1982), no. 4, 723–727. (Cited on page 50.)

[IR82] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, Graduate Texts in Mathematics, vol. 84, Springer-Verlag, 1982. (Cited on pages 108, 109, 113, 114 and 139.)

[Jed08] Jonathan Jedwab, *What can be used instead of a Barker sequence?*, Contemporary Mathematics, vol. 461, American Mathematical Society, 2008. (Cited on page 16.)

[Jr.47] Marshall Hall Jr., *Cyclic projective planes*, Duke Journal of Mathematics **14** (1947), 1079–1090. (Cited on page 107.)

[Jr.98] ———, *Combinatorial theory*, John Wiley and Sons, 1998. (Cited on pages 23 and 67.)

[Jun90] Dieter Jungnickel, *On automorphism groups of divisible designs II: Group invariant generalized conference matrices*, Arch. Math. **54** (1990), 200–208. (Cited on page 41.)

[JW92] W. A. Jackson and P. R. Wild, *Relations between two perfect ternary sequence constructions*, Designs, Codes, and Crytography **2** (1992), 325–332. (Cited on pages 50 and 79.)

[Kap75] J. Kapoor, *Orthogonal matrices as linear combinations of permutation matrices*, Linear Algebra and its Applications **12** (1975), no. 3, 189–196. (Cited on page 32.)

[Kar88] Gregory Karpilovsky, *Field theory: Classical foundations and multiplicative groups*, M. Dekker, 1988. (Cited on page 61.)

[Lam91] C. W. H. Lam, *The search for a finite projective plane of order 10*, American Mathematical Monthly **98** (1991), 305–318. (Cited on page 22.)

[Lan83] E. S. Lander, *Symmetric designs: An algebraic approach*, London Mathematical Society Lecture Note Series, no. 74, Cambridge University Press, 1983. (Cited on pages 131 and 133.)

[LMS02] Ka Hin Leung, Siu Lun Ma, and Bernhard Schmidt, *Constructions of relative difference sets with classical parameters and circulant weighing matrices*, Journal of Combinatorial Theory (A) **99** (2002), 111–127. (Cited on pages 50 and 102.)

[LS05] Ka Hin Leung and Bernhard Schmidt, *The field descent method*, Designs, Codes, and Crytography **36** (2005), no. 2, 171–188. (Cited on pages 8, 16, 108, 153, 154 and 157.)

[Ma85] Siu Lun Ma, *Polynomial addition sets*, Ph.D. thesis, University of Hong Kong, 1985. (Cited on pages 114 and 116.)

[Ma90] ———, *Polynomial addition sets and symmetric difference sets*, Coding Theory and Design Theory, Part II: Design Theory (D. K. Ray-Chaudhuri, ed.), vol. 21, Springer-Verlag, 1990. (Cited on page 125.)

[Ma96] ———, *Planar functions, relative difference sets, and character theory*, Journal of Algebra **185** (1996), 342–356. (Cited on pages 113, 139 and 152.)

[Man64] H. B. Mann, *Balanced incomplete block designs and abelian difference sets*, Illinois Journal of Mathematics **8** (1964), 252–261. (Cited on page 107.)

[McF70] R. L. McFarland, *On multipliers of abelian difference sets*, Ph.D. thesis, Ohio State University, 1970. (Cited on page 131.)

[Mil09] Goldwyn Millar, *Crosscorrelation properties of perfect ternary sequences*, in preparation. (2009). (Cited on pages 50, 79 and 168.)

[MM07] Gary L. Mullen and Carl Mummert, *Finite fields and applications*, AMS Bookstore, 2007. (Cited on page 60.)

[Moh74] P. S. Moharir, *Ternary Barker codes*, Electronics Letters **10** (1974), no. 22, 460–461. (Cited on page 16.)

[Moo46] A. M. Mood, *On Hotelling's weighing problem*, Annals of Mathematical Statistics **17** (1946), no. 4, 432–446. (Cited on pages 3 and 12.)

[MR96] P. S. Moharir and K. S. Rao, *Self co-operative ternary pulse compression sequences*, Sadhana, vol. 21, 1996. (Cited on page 16.)

[MR97] David K. Maslen and Daniel Rockmore, *Generalized ffts- a survey of recent results*, Groups and Computation, II, vol. 28, American Mathematical Society, 1997. (Cited on page 92.)

[MS76] R. C. Mullin and R. G. Stanton, *On the nonexistence of a class of circulant balanced weighing matrices*, SIAM Journal of Applied Mathematics **30** (1976), no. 1, 98–102. (Cited on page 41.)

[Mul75] R. C. Mullin, *A note on balanced weighing matrices*, Combinatorial Mathematics, III, vol. 452, Springer, 1975. (Cited on pages 32 and 33.)

[O'K96] Christiane M. O'Keefe, *Ovoids in pg(3,q): A survey*, Discrete Mathematics **151** (1996), 175–188. (Cited on page 76.)

[Pal33] R. E. A. C. Paley, *On orthogonal matrices*, Journal of Mathematical Physics **12** (1933), 311–320. (Cited on page 8.)

[Par88] J. R. Parlington, *An introduction to hankel operators*, LMS Student Texts, vol. 13, Cambridge University Press, 1988. (Cited on page 47.)

[Rys63] H. J. Ryser, *Combinatorial mathematics*, vol. 27, MR, no. 51, Wiley, 1963. (Cited on page 8.)

[Sch] Bernhard Schmidt, *Towards Ryser's conjecture (pre-print)*. (Cited on pages 8, 129, 152 and 161.)

[Sch99] ———, *Cyclotomic integers and finite geometry*, Journal of the American Mathematical Society **12** (1999), no. 4, 929–952. (Cited on pages 8, 108, 120, 152, 153, 161, 163 and 165.)

[Seg54] B. Segre, *Sulle ovali nei piani finiti*, Atti Accad. Naz. Lincei Rendic. **17** (1954), 141–142. (Cited on page 76.)

[Ser79] Jean Pierre Serre, *Local fields*, GTM, vol. 67, Springer-Verlag, 1979. (Cited on page 109.)

[Ser96] Jean-Pierre Serre, *Linear representations of finite groups*, Springer, 1996. (Cited on page 88.)

[Sev08] Simone Severeni, Personal correspondence to R. Craigen, 2008. (Cited on page 48.)

[Sin38] James Singer, *A theorem in finite projective geometry and some applications to number theory*, Transactions of the American Mathematical Society **43** (1938), no. 3, 377–385. (Cited on page 67.)

[SMA05] Radomir S. Stankovic, Claudio Moraga, and Jaako T. Astola, *Fourier analysis on finite groups with applications in signal processing and system design*, John Wiley and Sons, 2005. (Cited on page 92.)

[SY92] Jennifer Seberry and Mieko Yamada, *Hadamard matrices, sequences, and block designs*, Contemporary Design Theory: A Collection of Surveys (Jeffrey H. Dinitz and Douglas R. Stinson, eds.), John Wiley and Sons, 1992. (Cited on pages 6 and 92.)

[Tha74] J. A. Thas, *On semi-ovals and semi-ovoids*, Geometriae Dedicata **3** (1974), no. 2, 229–231. (Cited on page 76.)

[Tur65] Richard Turyn, *Character sums and difference sets*, Pacific Journal of Mathematics **15** (1965), no. 1, 319–346. (Cited on pages 8, 108, 114, 115 and 129.)

[Wal23] J. L. Walsh, *A closed set of normal orthogonal functions*, American Journal of Mathematics **45** (1923), no. 1, 5–24. (Cited on page 93.)

[Was04] Larry Wasserman, *All of statistics: A concise course in statistical inference*, 2004. (Cited on pages 10 and 11.)

[WW75] Jennifer Seberry Wallis and Albert Leon Whiteman, *Some results on weighing matrices*, Bulletin of the Australian Mathematical Society **12** (1975), no. 3, 433–447. (Cited on page 49.)

[Yam63] K. Yamamoto, *Decomposition fields of difference sets*, Pacific Journal of Mathematics **13** (1963), 337–352. (Cited on page 108.)

Index