BALANCED GROUP MATRICES

THEORY AND APPLICATIONS

THOMAS PENDER

Department of Mathematics and Computer Science
University of Lethbridge
LETHBRIDGE, ALBERTA, CANADA

BALANCED GROUP MATRICES
THEORY AND APPLICATIONS

THOMAS PENDER

Dr. Hadi Kharaghani
Supervisor, Professor, Ph.D.

Dr. Amir Akbary-Majdabadno
Committee Member, Professor, Ph.D.

To my mother,

who instilled in her sons an admiration of and an aspiration towards intellectual achievement; her passion for mathematics has engendered my own.

Acknowledgments

There are many individuals who deserve to be recognized. Foremost is my supervisor, Dr. Hadi Kharaghani, whose talent both as a researcher and as a teacher, along with possessing a singular patience, has provided excellent ground upon which one may cultivate their knowledge of and appreciation for this subject.

Dr. Amir Akbary-Mojdabadno, whose comments and insights greatly improved the presentation of this work, also deserves special thanks.

More generally, I should like to thank each of the faculty members of the Department of Mathematics and Computer Science, from whom I have had the priviledge of being taught, for the influence they have had in shaping my career as an undergraduate student at the University of Lethbridge. It has been a most rewarding experience.

Abstract

It is the purpose of this essay to explore the relationships of a particular collection of group matrices, namely, balanced generalized weighing matrices, to related combinatorial configurations. In particular, we will endevour to apply these most interesting objects to the construction of symmetric balanced incomplete block designs; orthogonal designs; and binary, constant weight codes.

The entries of the balanced generalized weighing matrices used here will be from a particular subgroup of the automorphism group of the objects to which they are being applied. This application of group members will be effected through a generalized Kronecker product. These constructions will lead both to novel constructions of known families of objects and to constructions of parametrically new families of objects.

Contents

Introduction

Weighing matrices have captivated researchers for a century now, and interest in these objects has proliferated precipitously as new and important applications are continually being found. Towards constructing these objects, researchers have, as is so often the case in mathematics, abstracted away from particulars and applied these general properties to new objects. Of these more general objects, we will be concerning ourselves with the so-called balanced generalized weighing matrices (henceforth, BGWs).

BGW matrices are a kind of group matrix, whose entries come from some finite group and also include the symbol 0. Alternatively, if G is our finite group, and if R is some commutative ring, then we take the entries of the matrix from the group ring $R[G]$. Importantly, these matrices exhibit a kind of balance between the various rows and columns. By setting all of the non-zero entries of the BGW to unity, one sees that we now have the incidence matrix of a block design; hence, the entries of the matrix have a kind of inter-positional balance. More than this, however, the entries, as we will see, are also balanced with respect to the group itself; that is, the matrix also displays a kind of intra-positional balance. It is these properties that make these matrices most intriguing and applicable.

Since the following applications of BGWs will be to a number of different objects, we must, therefore, begin with some preliminaries before proceeding to the constructions. Part I will consist of these preliminaries that will place BGWs in their proper place and will contain Chapters 1–3.

Chapter 1 will introduce the idea of incidence necessary to study such objects. In particular, we will introduce the very general incidence structres and use these to define the needed balanced incomplete block designs. Elementary properties of these objects will be described, and we will introduce the important idea of resolvability of a block design.

In Chapter 2 we will introduce the most basic weighing matrices, namely, those whose entries are from the set $\{-1, 0, 1\}$. Motivation for these objects will be discussed, as will their properties. Following this, important examples of such matrices are developed, and we place these objects in their appropriate place by inviting the reader to consider many of their relations to other combinatorial objects that are of interest presently.

Chapter 3 will contain many examples of generalizations of weighing

matrices. It is in this chapter that we introduce BGW matrices, and we construct the important family of classical-parameter BGWs. We show that BGWs are an extremal case of the so-called generalized Bhaskar Rao designs.

After the conclusion of the preliminaries, Part II will introduce the constructions developed over the course of the preparation of this essay. These will be developed over Chapters 4–6.

Chapter 4 will introduce the Kronecker product, and will present several of its elementary properties. We then generalize this product in such a way that we can use a BGW matrix as the multiplicand of the product. This realization allows us to construct BGW matrices that have additional symmetries, namely, they will be symmetric and skew-symmetric, predicated on simple parametric conditions. After this, we will apply the classical BGWs to present a novel construction of the Rajkundlia family of matrices.

In Chapter 5 we will study an extension of Hadamard matrices; in particular, we will consider those matrices with unimodular entries from the set $\{\frac{\pm 1 \pm i\sqrt{m}}{\sqrt{m+1}}, \frac{\pm i \pm \sqrt{m}}{\sqrt{m+1}}\}$ such that the rows (columns) of the matrix are pairwise orthogonal under the usual Hermitian inner product. We will extend particular constructions of these matrices as well as a morphism that will yield quaternary complex Hadamard matrices, i.e. those Hadamard matrices with entries from the set $\{\pm 1, \pm i\}$.

In Chapter 6, the final chapter, we will apply BGW matrices to construct parametrically new families of orthogonal designs. These matrices, along with those constructed in the previous chapter, will give us new orders of real and complex Hadamard matrices. At the conclusion of the chapter, BGW matrices will be applied to reproduce several of the best known upper bounds for the number of code words in binary constant weight codes.

In order to preserve the continuity of the work, citations of results will be found at the end of each chapter in a "Notes" section.

The novel results compiled in this essay are:

i. Theorems 4.16, 5.5(ii), 5.7, 6.1, 6.2, 6.10, 6.12, 6.15, 6.17

ii. Propositions 4.19, 5.1(ii), 5.2(ii), 5.10, 5.11, 6.3, 6.5, 6.7, 6.8, 6.9

iii. Corollaries 5.3, 5.4, 5.6, 5.8, 5.9, 6.11, 6.13, 6.14, 6.16

An index of terms and an index of notations are available for the reader to reference as they work their way through this essay.

Part I

Combinatorial Preliminaries

Chapter 1

Balanced Incomplete Block Designs

1.1 Definitions

Consider the following situation. From a group of individuals, one must choose a number of committees, each of identical size, such that the appearances of every individual among the various committees are equinumerous, as are the appearances of each t individuals. More concretely we might ask something such as: Given eight objects, can we arrange them in some number of groups of size four such that every triple appears together in a single group and every singleton is replicated the same number of times?

We can answer this question in the affirmative with the following configuration. Let the group of objects be represented by $\{a, b, c, d, e, f, g, h\}$. Then the required groups may be given by

$$\begin{array}{ll} \{a, b, e, f\}, & \{c, d, g, h\}, \\ \{a, c, e, g\}, & \{b, d, f, h\}, \\ \{a, d, e, h\}, & \{b, c, f, g\}, \\ \{a, b, c, d\}, & \{e, f, g, h\}, \\ \{a, b, g, h\}, & \{c, d, e, f\}, \\ \{a, c, f, h\}, & \{b, d, e, g\}, \\ \{a, d, f, g\}, & \{b, c, e, h\}. \end{array}$$

Such a configuration is an example of a *t-design*. For the special case in which $t = 2$, the configuration is termed a *balanced incomplete block design*.

In order to study these objects successfully and to place them in their correct position relative to the other objects of design theory, we make use of the so-called incidence structures defined thus.

Definition. An *incidence structure* is a triple $S = (\mathfrak{p}, \mathfrak{B}, I)$, where $\mathfrak{p}$ and $\mathfrak{B}$ are sets such that $\mathfrak{p} \cap \mathfrak{B} = \emptyset$, and where $I \subseteq \mathfrak{p} \times \mathfrak{B}$. The sets $\mathfrak{p}$, $\mathfrak{B}$,

and I are referred to as the *points*, *blocks*, and *flags* of the incidence structure, respectively. We write $p\ I\ \mathcal{B}$ and say *"p is incident with $\mathcal{B}$"* whenever $(p, \mathcal{B}) \in I$.

To each incident structure $S = (\mathfrak{p}, \mathfrak{B}, I)$ there are many associated structures. The *dual* of S is the triple $\bar{S} = (\bar{\mathfrak{p}}, \bar{\mathfrak{B}}, \bar{I})$ defined as $\bar{\mathfrak{p}} = \mathfrak{B}$, $\bar{\mathfrak{B}} = \mathfrak{p}$, and $(\mathcal{B}, p) \in \bar{I}$ if and only if $(p, \mathcal{B}) \in I$.

The *complement* of S is the triple $S' = (\mathfrak{p}', \mathfrak{B}', I')$ defined as $\mathfrak{p}' = \mathfrak{p}$, $\mathfrak{B}' = \mathfrak{B}$, and $I' = (\mathfrak{p} \times \mathfrak{B}) - I$.

Let $\mathfrak{q} \subseteq \mathfrak{p}$, and let $\mathfrak{F} \subseteq \mathfrak{B}$. Further define $I^* = (\mathfrak{q} \times \mathfrak{F}) \cap I$. The triple $(\mathfrak{q}, \mathfrak{F}, I^*)$ is a *substructure* of S.

We will consider four important examples of substructures of S. In order to accomplish this, we introduce the following notations. For each $p \in \mathfrak{p}$ and $\mathcal{B} \in \mathfrak{B}$, define

$$(p) = \{\mathcal{B} \mid p\ I\ \mathcal{B}\}, \text{ and } \quad (\mathcal{B}) = \{p \mid \mathcal{B}\ I\ p\}$$

Further, we use $[p] = |(p)|$ and $[\mathcal{B}] = |(\mathcal{B})|$. The number $[p]$ is the *replication number of* p, and $[\mathcal{B}]$ is the *cardinality of* $\mathcal{B}$. Fix $p \in \mathfrak{p}$ and $\mathcal{B} \in \mathfrak{B}$ of S. We define the following *internal structures*.

$$S_p = \Big(\mathfrak{p} - \{p\}, (p), \big((\mathfrak{p} - \{p\}) \times (p)\big) \cap I\Big), \text{ and}$$
$$S_{\mathcal{B}} = \Big((\mathcal{B}), \mathfrak{B} - \{\mathcal{B}\}, \big((\mathcal{B}) \times (\mathfrak{B} - \{\mathcal{B}\})\big) \cap I\Big).$$

Similarly, we define the following *external structures*.

$$S^p = \Big(\mathfrak{p} - \{p\}, \mathfrak{B} - (p), \big((\mathfrak{p} - \{p\}) \times (\mathfrak{B} - (p))\big) \cap I\Big), \text{ and}$$
$$S^{\mathcal{B}} = \Big(\mathfrak{p} - (\mathcal{B}), \mathfrak{B} - \mathcal{B}, \big((\mathfrak{p} - (\mathcal{B})) \times (\mathfrak{B} - \{\mathcal{B}\})\big) \cap I\Big).$$

In the literature it is customary to refer to S_p and S^p as the *point-derived* and *point-residual* substructures of S; while $S_{\mathcal{B}}$ and $S^{\mathcal{B}}$ are analogously referred to as the *block-derived* and *block-residual* substructures of S.

If S is finite, i.e. there exist positive integers v and b such that $\mathfrak{p} = \{p_1, p_2, \ldots, p_v\}$ and $\mathfrak{B} = \{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_b\}$, then we may associate to S the $v \times b$ *incidence matrix* $A = [a_{ij}]$ defined as

$$a_{ij} = \begin{cases} 1 & \text{if } p_i\ I\ \mathcal{B}_j; \text{ and} \\ 0 & \text{if } p_i \not I\ \mathcal{B}_j. \end{cases}$$

Example 1.1. The preliminary example given at the start of this section has the following incidence matrix.

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

We now have the appropriate framework to precisely define 2-designs.

Definition. By a *balanced incomlpete block design*, we mean a finite incidence structure $S = (\mathfrak{p}, \mathfrak{B}, I)$ such that:

i. $|\mathfrak{p}| = v$ and $|\mathfrak{B}| = b$, for some $v \in \mathbb{Z}_+$ and $b \in \mathbb{Z}_+$;

ii. there are $r \in \mathbb{Z}_+$ and $k \in \mathbb{Z}_+$ such that, for every $p \in \mathfrak{p}$ and $\mathcal{B} \in \mathfrak{B}$, we have $[p] = r$ and $[\mathcal{B}] = k$; and

iii. there is a $\lambda \in \mathbb{Z}_+$ such that, for every 2-set $\{p_i, p_j\}$ of $\mathfrak{p}$, we have that $[\{p_i, p_j\}] = \lambda$.

We will use the notation BIBD(v, b, r, k, λ), and we will see that the parameters are closely related; hence, it is customary to refer only to the paramters (v, k, λ) unless more detail is required. If $v = k$ (equiv. $k = r$), then we say that the design is *symmetric*.

Example 1.2. We illustrate a BIBD$(7, 3, 1)$ with point set $\{1, 2, 3, 4, 5, 6, 7\}$ below.

$$\begin{array}{ll}
\{1,2,3\} & \{1,4,5\}\\
\{1,6,7\} & \{2,4,6\}\\
\{2,5,7\} & \{3,4,7\}\\
\{3,5,6\} &
\end{array}$$

This is the famous *Fano plane*.

Example 1.3. We note that our definition of BIBDs does not preclude the instances in which the collection of blocks contains repeated blocks. To

achieve a BIBD(7,3,2) we may extend the above BIBD(7,3,1) in the following way.

$$\begin{array}{lll} \{1,2,3\} & \{1,4,5\} & \{1,6,7\} \\ \{2,4,6\} & \{2,5,7\} & \{3,4,7\} \\ \{3,5,6\} & \{1,2,3\} & \{1,4,7\} \\ \{1,5,6\} & \{2,4,5\} & \{2,6,7\} \\ \{3,4,6\} & \{3,5,7\} & \end{array}$$

Note the block $\{1,2,3\}$ appears twice in the block set.

Example 1.4. If $|\mathfrak{p}| = v$, and if $\mathfrak{B}$ consists of all the k-subsets of $\mathfrak{p}$, then the resulting structure is a BIBD$\left(v, k, \binom{v-2}{k-2}\right)$.

The following section includes a more detailed discussion of the associations between the parameters of BIBDs.

1.2 Properties

We begin this section with the following general result.

Proposition 1.5. Let $S = (\mathfrak{p}, \mathfrak{B}, I)$ be a finite incidence structure. Then

$$\sum_{p \in \mathfrak{p}} [p] = \sum_{\mathcal{B} \in \mathfrak{B}} [\mathcal{B}], \tag{1.1}$$

and, after fixing a point $q \in \mathfrak{p}$,

$$\sum_{p \neq q} [\{p, q\}] = \sum_{\mathcal{B} \ \mathrm{I} \ q} [\mathcal{B}] - [q]. \tag{1.2}$$

Proof. To show (1.1), we count the number of flags in S. First, we count the replications of points, and then we count the points incident with each block.

To show (1.2), we fix $q \in \mathfrak{p}$ and count flags $(p, \mathcal{B})$ such that $p \neq q$ and $\mathcal{B} \in (p) \cap (q)$. First, for each point p distinct from q, we count the blocks that are incident with both p and q. Second, we count the points incident with each block containing q. But we have then counted $[q]$ flags of the form $(q, \mathcal{B})$ which must be deducted. *Q.E.D.*

Corollary 1.6. If S is a BIBD(v, b, r, k, λ), then (1.1) and (1.2) become

$$vr = bk, \tag{1.3}$$

and

$$\lambda(v-1) = r(k-1). \tag{1.4}$$

From (1.3) and (1.4), it follows that

$$bk(k-1) = \lambda v(v-1).$$

Equivalently, counting the number of ordered pairs appearing in the design, including repititions, we find that

$$b\binom{k}{2} = \lambda\binom{v}{2}.$$

The following beautiful result was shown by Fischer in the first half of the twentieth century. The importance of this result cannot be overstated since it places fundamental restrictions on the structure of BIBDs that have immediate consequences for the experimental designs modeled after them. To illustrate the various methods employed in the study of combinatorial designs, we will give two proofs of the proposition.

Theorem 1.7. [Fischer's Inequality] For every BIBD(v, b, r, k, λ), it holds that $b \geq v$.

PROOF. (1^{st}) We will prove the more general result known as The Non-Uniform Fischer's Inequality. Let S be a finite set of v elements, and let $\mathfrak{B}$ be a collection of b subsets of S such that $|\mathcal{B}_1 \cap \mathcal{B}_2| = \lambda > 0$, for every distinct $\mathcal{B}_1$ and $\mathcal{B}_2$ in $\mathfrak{B}$. We will show that $b \leq v$, from which the result follows by applying the non-uniform equality to the dual of the design.

Suppose first that there is a $\mathcal{B} \in \mathfrak{B}$ such that $|\mathcal{B}| = \lambda$. It follows that $\mathcal{A} \cap \mathcal{B} = \mathcal{B}$, for every $\mathcal{A}$ in $\mathfrak{B}$. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be distinct sets in $\mathfrak{B}$. Define $\mathcal{C} = \mathcal{B}_1 \cap \mathcal{B}_2$ so that $|\mathcal{C}| = \lambda$. Then $\mathcal{B} = \mathcal{B} \cap \mathcal{B}_1 \cap \mathcal{B}_2 = \mathcal{B} \cap \mathcal{C}$. Since $|\mathcal{B}| = |\mathcal{C}| = \lambda$, it follows that $\mathcal{B} = \mathcal{C}$. Therefore, in the usual way, form the collection of mutually disjoint sets $\mathfrak{B}^* = \{\mathcal{B}_i - \mathcal{B} \mid \mathcal{B}_i \in \mathfrak{B}\}$. Then $b = |\mathfrak{B}^*| \leq |S - \mathcal{B}| + 1 \leq v$.

We may now assume that $|\mathcal{B}| > \lambda$ for each $\mathcal{B} \in \mathfrak{B}$. Let P be the space of linear polynomials $\sum_{i=1}^{v} a_i x_i + a$ with rational coefficients. To each set $\mathcal{B} \in \mathfrak{B}$ associate the linear polynomial $f_{\mathcal{B}} = \sum_{i \in \mathcal{B}} x_i - \lambda$. Then, for $\mathcal{A} \in \mathfrak{B}$, $f_{\mathcal{B}}(\mathcal{A}) = |\mathcal{A} \cap \mathcal{B}| - \lambda$.

We first consider the $\mathbb{Q}$-independence of the set $\{f_{\mathcal{B}}\}_{\mathcal{B} \in \mathfrak{B}}$. Assume that $\sum a_{\mathcal{B}} f_{\mathcal{B}} = 0$, and fix $\mathcal{A}$ in $\mathfrak{B}$. Then $\sum a_{\mathcal{B}} f_{\mathcal{B}}(\mathcal{A}) = a_{\mathcal{A}}(|\mathcal{A}| - \lambda) = 0$; whence, $a_{\mathcal{A}} = 0$.

We next show that $1 \notin \text{span}\{f_{\mathcal{B}}\}_{\mathcal{B} \in \mathfrak{B}}$. Assume to the contrary, that there are rationals $\{a_{\mathcal{B}}\}_{\mathcal{B} \in \mathfrak{B}}$ such that $\sum a_{\mathcal{B}} f_{\mathcal{B}} = 1$. Then $\sum a_{\mathcal{B}} f_{\mathcal{B}}(\mathcal{A}) = a_{\mathcal{A}}(|\mathcal{A}| - \lambda) = 1$. It follows that $1 = \sum(|\mathcal{B}| - \lambda)^{-1} f_{\mathcal{B}}$. In an analogous manner, $1 = \sum(|\mathcal{B}| - \lambda)^{-1} f_{\mathcal{B}}(\emptyset) = -\sum \lambda/(|\mathcal{B}| - \lambda) < 0$, a contradiction.

We have shown that $\text{span}\{f_{\mathcal{B}}\}_{\mathcal{B} \in \mathcal{B} \cup \{1\}}$ is $\mathbb{Q}$-independent. Hence, $b+1 \leq v+1$, and the result has been shown. *Q.E.D.*

PROOF. (2^{nd}) The following is an application of *various counting*. Let $S = (\mathfrak{p}, \mathfrak{B}, I)$ be a BIBD(v, b, r, k, λ). Fix a block $\mathcal{B}$, and let $\mathcal{A}$ represent any

block distinct from $\mathcal{B}$. For $i \in \{0, 1, \ldots, k\}$, let n_i be the number of blocks $\mathcal{A}$ such that $[\mathcal{A} \cap \mathcal{B}] = i$. It follows immeditaley that

$$\sum_{i=0}^{k} n_i = b - 1. \tag{1.5}$$

Next, We count flags $(p, \mathcal{A})$ such that $p \; I \; \mathcal{A}$ and $p \; I \; \mathcal{B}$ in two ways. There are k points incident with $\mathcal{B}$, and each of these is incident with $r - 1$ other blocks. Thus,

$$\sum_{i=0}^{k} i n_i = k(r - 1). \tag{1.6}$$

Finally, we count, in an analogous manner, triples $(p_1, p_2, \mathcal{A})$ where $p_i \; I \; \mathcal{A}$ and $p_i \; I \; \mathcal{B}$, for $i = 1$ and 2, in two ways. We have

$$\sum_{i=0}^{k} i(i - 1) n_i = k(k - 1)(\lambda - 1). \tag{1.7}$$

From (1.5), (1.6), and (1.7), we find that

$$\sum_{i=0}^{k} i^2 n_i = k(r - 1) + k(k - 1)(\lambda - 1).$$

Then

$$\sum_{i=0}^{k} (x - i)^2 n_i = (b - 1)x^2 - 2k(r - 1)x + (k(r - 1) + k(k - 1)(\lambda - 1)),$$

for an indeterminant x. Since the sum is non-negative, it follows that its discriminant is non-positive. Initially, the discriminant is expressed in terms of b, r, k, and λ. Using Corollary 1.6, it is possible to express it in terms of v, k, and r as

$$(k - r)r(v - k)^2 \leq 0.$$

Therefore, $r \geq k$ (equiv. $b \geq v$). *Q.E.D.*

Note that symmetric BIBDs are the extremal case of Fischer's Inequality. If a BIBD(v, k, λ) has constant block intersection size, it follows by Theorem 1.7 and its non-uniform counterpart that it must be symmetric. We will show the converse.

Proposition 1.8. Let A be a (0,1)-matrix of order v. Then A is the incidence matrix of a symmetric BIBD(v, k, λ) if and only if

$$AA^t = A^t A = (k - \lambda)I + \lambda J \tag{1.8}$$

PROOF. Towards the necessity, we note that A is the incidence matrix of a BIBD(v, b, r, k, λ) if and only if $AA^t = (r-\lambda)I + \lambda J$, $A\mathbf{j} = r\mathbf{j}$, and $A^t\mathbf{j} = k\mathbf{j}$, where $\mathbf{j}$ is the column of all 1s.

To show the sufficiency, we first note that

$$\det(AA^t) = \det^2(A) = \det((k-\lambda)I + \lambda J) = (k + \lambda(v-1))(k-\lambda)^{v-1}.$$

Then A is non-singular. Since $A\mathbf{j} = k\mathbf{j}$, we have that $A^{-1}\mathbf{j} = \frac{1}{k}\mathbf{j}$. Conjugating (1.8) with A, we find

$$A^tA = (k-\lambda)I + \frac{\lambda}{k}JA.$$

Comparing the diagonal entries a_i, it follows that $a_i = k-\lambda+\lambda a_i/k$; whence, $a_i = k$ is the column sum of A. This shows that A is the incidence matrix of a symmetric BIBD(v, k, λ). *Q.E.D.*

Corollary 1.9. The dual of a design S is also a design if and only if S is a symmetric design.

We conclude this section with a discussion of the parameters of the block-residual and block-derived designs associated with a symmetric design.

Proposition 1.10. Let $S = (\mathfrak{p}, \mathfrak{B}, I)$ be a symmetric BIBD(v, k, λ), and fix a block $\mathcal{B} \in \mathfrak{B}$. Then:

i. $S^{\mathcal{B}}$ is a BIBD$(v-k, v-1, k, k-\lambda, \lambda)$ if $\lambda \geq 2$, and

ii. $S_{\mathcal{B}}$ is a BIBD$(k, v-1, k-1, \lambda, \lambda-1)$ if $k-\lambda \geq 2$.

PROOF. To see the parametric values most easily, note that the associated incidence matrix is permutation equivalent to

$$\begin{bmatrix} \mathbf{0} & A \\ \mathbf{j} & B \end{bmatrix},$$

where A and B are the incidence matrices of the block-residual and block-derived designs associated with the image of the block $\mathcal{B}$ under the previously mentioned automorphism.

There only remains to be shown two nessecary conditions on the parameters, which, of course, are furnished by the assumptions $\lambda \geq 2$ and $k - \lambda \geq 2$.

i. $S_{\mathcal{B}}$ is a design if $v - k \geq k - \lambda$. The contrary is equivalent to $(k - \lambda)(k-\lambda-1) \leq 0$. By our assumptions, this is a contradiction; whence, we have the desired inequality.

ii. In the case of $S^{\mathcal{B}}$, we need $k \geq \lambda$. This quickly follows from the facts $v \geq k$ and $\lambda(v-1) = k(k-1)$.

We have shown that $S^{\mathcal{B}}$ and $S_{\mathcal{B}}$ are as claimed. *Q.E.D.*

Designs whose parameters satisfy (i) and (ii) of Proposition **??** will be called *quasi-residual* and *quasi-derived* designs respectively. Those quasi-residual and quasi-derived designs which are actually the residual and derived designs of some larger symmetric design, will be called *embeddable*.

In the following chapters, we will refer to the block-residual and block-derived designs simply as the residual and derived designs.

1.3 Resolvability

The definition of balanced incomplete block designs is sufficiently broad to allow for many applications in fields like statistics and the theory of error-correcting codes. However, in order to apply the constructions of this treatise, we will usually require additional internal structure in the design; indeed, this idea, applied in other directions in the following sections, will be fundamental. In this section, we will focus on the resolvability of a design.

Definition. Let $S = (\mathfrak{p}, \mathcal{B}, I)$ be a BIBD(v, k, λ), and let $\mathfrak{C} \subset \mathfrak{B}$. Then:

i. If there is an $\alpha_{\mathfrak{C}} \in \mathbb{Z}_+$ such that each point in $\bigcup_{\mathcal{B}\in\mathfrak{C}}(\mathcal{B})$ appears $\alpha_{\mathfrak{C}}$ times, we call $\mathfrak{C}$ a *resolution class* of S. A partition of $\mathfrak{B}$ into resolution classes is called a *resolution* of S. If $\alpha_{\mathfrak{C}} = \alpha$, for all $\mathfrak{C}$, we say that S is α-resolvable.

ii. If $\mathfrak{C}$ is a resolution class of S such that $\alpha_{\mathfrak{C}} = 1$, then $\mathfrak{C}$ is a *parallelism* of S. If there is a parition of $\mathfrak{B}$ into parallelisms, then S is said to be *resolvable*.

iii. A resolution of S is said to be *affine* if the cardinality of the intersection between any two distinct blocks of $\mathfrak{B}$ is predicated solely on the resolution classes of which they are a part.

Example 1.11.

i. Let q be a prime power and $n \in \mathbb{Z}_+$. It is known that BIBDs with parameters

$$\left(q^n, \frac{q(q^n-1)}{q-1}, \frac{q^n-1}{q-1}, q^{n-1}, \frac{q^{n-1}-1}{q-1}\right)$$

exist for every such q and n. It is customary in the literature to refer to such BIBDs as an *n-dimensional affine geometry* over $\mathbb{F}_q$ (see Notes

for further discussion) and to denote this as $\mathrm{AG}_{n-1}(n, q)$. We follow custom and use this terminology and notation to refer to such designs. It is well-known that affine geometries admit an affine resolution. The following is a manifestation of $\mathrm{AG}_1(2, 3)$ in which the resolution classes are clearly manifest.

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

This construction is typical of using the *generalized Hadamard matrices* (see Chapter 3).

ii. The binary array given in Example 1.1 is an example of the so-called *Hadamard 3-designs*, and is also seen to be resolvable. Hadamard 3-designs and affine geometries are the only known families of affine resolvable balanced incomplete block designs.

Fischer's Inequality (Theorem 1.7) may be improved for those designs which admit a resolution. Moreover, this improved bound is tight in the case that the resolution is affine; indeed, we will see that it completely characterizes this case.

Theorem 1.12 (Bose's Inequality)**.** Let $S = (\mathfrak{p}, \mathfrak{B}, I)$ be a $\mathrm{BIBD}(v, b, r, k, \lambda)$ admitting a resolution $\mathscr{R}$ that partitions $\mathfrak{B}$. Then:

i. We have that $b \geq v + |\mathscr{R}| - 1$; and

ii. if the resolution is affine, then the bound on b is tight.

Proof.

i. The proof closely follows that of Theorem 1.7. Let P be the space of linear polynomials $\sum_{i=1}^{b} a_i x_i + a$ with rational coefficients. For each point $p \in \mathfrak{p}$, and for each resolution class $\mathfrak{C} \in \mathscr{R}$, define the polynomials $f_p = \sum_{\mathcal{B} \ni p} x_{\mathcal{B}} - \lambda$ and $g_{\mathfrak{C}} = \sum_{\mathcal{B} \in \mathfrak{C}} x_{\mathcal{B}} - \alpha_{\mathfrak{C}}$. Just as in the proof of Theorem 1.7, it follows *mutatis mutandis* that the set $\mathcal{V} = \{f_p\}_{p \in \mathfrak{p}} \cup \{g_{\mathfrak{C}}\}_{\mathfrak{C} \in \mathscr{R}}$ is $\mathbb{Q}$-independent. Since this is a subspace of P, we have that $v + |\mathscr{R}| \leq b + 1$.

ii. Assume that $\mathscr{R}$ is affine and has the ordering $\mathscr{R} = \{\mathfrak{C}_1, \mathfrak{C}_2, \ldots, \mathfrak{C}_t\}$. Let $[\mathcal{A} \cap \mathcal{B}] = m_{ij}$, for $\mathcal{A} \in \mathfrak{C}_i$ and $\mathcal{B} \in \mathfrak{C}_j$, and let $V = \text{span } \mathcal{V}$. It suffices to show that $V = P$, and this will be accomplished by showing that each $x_{\mathcal{B}} \in V$. Define the polynomial

$$h = \sum f_p - k \sum g_{\mathfrak{C}_i} = \sum a_{\mathcal{B}} x_{\mathcal{B}} + a.$$

It follows that $a_{\mathcal{B}} = [\mathcal{B}] - k = 0$; whence, h is constant. Since $\mathcal{V}$ is a $\mathbb{Q}$-independent set, we have $h \neq 0$.
For $\mathcal{B} \in \mathfrak{C}_j$, $j \in \{1, 2, \ldots, t\}$, consider now the polynomial

$$h_{\mathcal{B}} = \sum_{p \in \mathcal{B}} f_p - \sum_{i=1}^{t} m_{ij} g_{\mathfrak{C}_i} = \sum a_{\mathcal{B}} x_{\mathcal{B}} + a.$$

As above, $a_{\mathcal{B}} = k - m_{jj}$. If $k - m_{jj} = 0$, then, for any blocks $\mathcal{A}$ and $\mathcal{B}$ in $\mathfrak{C}_j$, we have that $[\mathcal{A} \cap \mathcal{B}] = [\mathcal{A}] = [\mathcal{B}]$. This is a contradiction since $[\mathfrak{C}_j] \geq 2$, so there would be points not appearing in the resolution class; whence, $a_{\mathcal{B}} \neq 0$. Similarily, if $\mathcal{A} \neq \mathcal{B}$ and $\mathcal{A} \in \mathfrak{C}_i$, then $a_{\mathcal{A}} = [\mathcal{A} \cap \mathcal{B}] - m_{ij} = 0$ so that $h_{\mathcal{B}} = a_{\mathcal{B}} x_{\mathcal{B}} - a$. The result now follows. *Q.E.D.*

We complete our analysis of the extremal case of Bose's inequality with the following two result.

Lemma 1.13. Let $S = (\mathfrak{p}, \mathfrak{B}, I)$ be a BIBD(v, b, r, k, λ) admitting a resolution $\mathscr{R}$ of pairwise disjoint resolution classes such that $b = v + |\mathscr{R}| - 1$ (we are not immediately assuming it covers $\mathfrak{B}$). Then $\mathscr{R}$ is a resolution.

Proof. We have shown that each $x_{\mathcal{B}} \in V$. Expanding each $x_{\mathcal{B}}$ by employing the same methods used in the proof of the previous result, we obtain

$$x_{\mathcal{B}} = \frac{1}{r - \lambda} \sum f_p + \sum a_{\mathfrak{C}}^{(\mathcal{B})} g_{\mathfrak{C}}. \tag{1.9}$$

Assume there is some block $\mathcal{A}$ distinct from $\mathcal{B}$ and not in any resolution class of $\mathscr{R}$. Comparing the coefficient for $x_{\mathcal{A}}$ on both sides of (1.9), it follows that

$$0 = \frac{[\mathcal{A} \cap \mathcal{B}]}{r - \lambda}.$$

Therefore, $(\mathcal{A}) \cap (\mathcal{B}) = \emptyset$. However, by Fischer's inequality, we have that $b = v + |\mathscr{R}| - 1 \geq v$; hence, $|\mathscr{R}| \geq 1$. We have derived our contradiction, and the result is shown. *Q.E.D.*

Theorem 1.14. Let $S = (\mathfrak{p}, \mathfrak{B}, I)$ be a BIBD(v, b, r, k, λ) admitting a resolution $\mathscr{R}$ such that $b = v + |\mathscr{R}| - 1$. Then:

i. Any two distinct blocks of the same resolution class meet in $k - r + \lambda$ points;

ii. for any resolution class $\mathfrak{C} \in \mathscr{R}$, we have $|\mathfrak{C}| = v\alpha_{\mathfrak{C}}/k$;

iii. any two blocks from distinct resolution classes meet in k^2/v points; and

iv. $\mathscr{R}$ is an affine resolution.

PROOF.

i. Using the same reasoning in the proofs of previous results, we expand each $x_{\mathcal{B}}$ as
$$(r - \lambda)x_{\mathcal{B}} = \sum f_p - \sum b_{\mathfrak{C}}^{(\mathcal{B})} g_{\mathfrak{C}}. \tag{1.10}$$
Following the standard approach of comparing coefficients, we find that $r - \lambda = [\mathcal{B}] - b_{\mathfrak{C}\ni\mathcal{B}}^{\mathcal{B}}$. Again comparing coefficients of $x_{\mathcal{B}}$ for the blocks $\mathcal{A} \neq \mathcal{B}$ of the same resolution class, it follows $[\mathcal{A}\cap\mathcal{B}] - b_{\mathfrak{C}\ni\mathcal{A}}^{(\mathcal{B})} = 0$; and i. follows.

ii. We count flags $(p, \mathcal{B})$ in two ways. First, each block is incident with k points, and there are $|\mathfrak{C}|$ blocks. Second, each point appears $\alpha_{\mathfrak{C}}$ times in $\mathfrak{C}$, and there are v points. Hence, $k|\mathfrak{C}| = v\alpha_{\mathfrak{C}}$.

iii. Let $\mathcal{B} \in \mathfrak{C}_i$. Counting flags $(p, \mathcal{A})$, where $\mathcal{A} \in \mathfrak{C}_j$, $i \neq j$, and where $p \in (\mathcal{A}) \cap (\mathcal{B})$, we find $k\alpha_{\mathfrak{C}_j} = |\mathfrak{C}_j|[\mathcal{A} \cap \mathcal{B}]$. The left-hand side follows since there are k points in $(\mathcal{B})$, and each of these points appears $\alpha_{\mathcal{C}_j}$ times. The right-hand side follows after noting that the reasoning in i. demonstrates that each block $\mathcal{A} \in \mathfrak{C}_j$ meets $\mathcal{B}$ in $b_{\mathfrak{C}_j}^{(B)}$ points, and there are $|\mathfrak{C}_j|$ blocks like $\mathcal{A}$.

iv. The previous points show precisely that $\mathscr{R}$ is an affine resolution. *Q.E.D.*

The previous result shows clearly that the dual incidence structure of each resolution class $\mathfrak{C}$ yields a BIBD$(|\mathfrak{C}|, \alpha_{\mathfrak{C}}, k - r - \lambda)$. Moreover, it can be shown that $\mathscr{R}$ is unique.

We will pursue further imposed structural properties in Chapter 3 when we discuss the so-called *intra-positional balance*.

1.4 Notes

Combinatorial design theory has been developing at an exceptional rate since its formal inception during the first half of the twentieth century. The standard introduction to the field is presented in Beth, Jungnickel, and Lenz

[BJL99a, BJL99b]; while a more elementary introduction is given in Stinson [Sti04]. The monograph Ionin,Shrikhande [IS06] provides an in-depth examination into the theory of symmetric designs and has been indespensable to the development of this treatise.

Incidence structures, as they apply to combinatorial designs, are studied in the opening chapters of [BJL99a] and [IS06]. The notations and results of §1.1 follow Dembowski [Dem97], which is the standard monograph on the beautiful theory of finite geometries. For a more introductory invitation to the subject of finite geometries, the reader is referred to Batten [Bat97].

The material in §1.2 closely follows the second chapters of [Dem97] and [Bat97]. Fisher's Inequality was shown in Ficher [Fis40]. The Non-Uniform Fischer's Inequality was first shown in Majumdar [Maj53]. Our first proof the Non-Uniform Inequality is taken from [IS06], while the second proof is taken from Cameron [Cam94]. The demonstration of the natures of the derived and residual designs of a symmetric design are a recapitualtion of those found in [Sti04].

The account of resolvability given in §1.3 is a special case of the more general treatment given in [IS06]. In that work resolvability is addressed for the structures known as (r, λ)-designs. These are similar to the balanced incomplete block designs studied here, but the condition that the cardinality of each block be the same is relaxed. The resolvability of balanced incomplete block designs is thoroughly addressed in Shrikhande [Shr76].

Chapter 2

Weighing Matrices

2.1 Definitions

Imagine performing an experiment in which you must weigh four objects using a balance with two pans. Let the error of the balance be denoted by ε that has mean 0 and variance σ^2. We will further denote the unknown weights as a_i and their measurments as y_i, $i \in \{1, 2, 3, 4\}$. It follows that the errors associated with each weight will be given by ε_i, $i \in \{1, 2, 3, 4\}$, respectively. If we then weigh each object individually, the associated weighings are then $a_i = y_i + \varepsilon_i$, each with variance σ^2.

Suppose we use a different scheme instead: We weigh all four objects at once, and we replicate these weighings with different configurations. We need a way to optimize such a configuration, and one such optimal system of weighings is given by the following.

$$\begin{aligned} a_1 + a_2 + a_3 + a_4 &= y_1 + \varepsilon_1, \\ a_1 - a_2 + a_3 - a_4 &= y_2 + \varepsilon_2, \\ a_1 + a_2 - a_3 - a_4 &= y_3 + \varepsilon_3, \text{ and} \\ a_1 - a_2 - a_3 + a_4 &= y_4 + \varepsilon_4, \end{aligned}$$

where the positive coefficients indicate being placed on the right pan, and the negative coefficients indicate being placed on the left pan. Notice that the coefficient matrix has pairwise orthogonal rows; hence, we may solve for each a_i. The estimate for each weight is then given by

$$\hat{a}_i = \frac{y_1 + y_2 + y_3 + y_4}{4} = a_i - \frac{\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4}{4}.$$

Since the variance of a sum of independent random variables is the sum of the variances (see Notes at the end of this chapter), we have that the variance for any one estimate is $\hat{a}_i = \sigma^2/4$. This is an improvement by a factor of four. We call the above configuration a *weighing design*.

The success of this scheme is owing to the form of the coefficient matrix. In this case the coefficient matrix is

$$W = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ 1 & 1 & - & - \\ 1 & - & - & 1 \end{bmatrix}.$$

Notice that since the rows are pairwise orthogonal, we have that $WW^t = 4I$. This motivates the following definition.

Definition. A weighing matrix W of order n and weight k is a (0,1,-1)-matrix of order n such that $WW^t = kI$. We will denote this as $W(n, k)$.

From $WW^t = kI$, it follows that $W^tW = kI$ and $W^{-1} = k^{-1}W^t$. Since the non-zero entries of W are plus or minus unity, we have shown that there are k non-zero entries in every row and column.

From the above discussion, we see that the optimum weighing designs are those that admit a $W(n, n)$. These are the important *Hadamard matrices*, and they play fundamental roles in exciting fields such as the design of experiments, performance of optical instruments, and error-correcting codes.

If there does not exist a $W(n, n)$, then the next optimum weighing design is given by a $W(n, n-1)$. We call the weighing matrices of this special case a *conference matrix*.

Example 2.1. Consider

$$W_1 = \begin{bmatrix} 0&1&1&1&1&1&1&1&1&1 \\ 1&0&-&1&-&1&-&1&-&1 \\ 1&-&0&1&1&1&-&-&1&- \\ 1&1&1&0&-&-&-&1&1&- \\ 1&-&1&-&0&1&1&1&-&- \\ 1&1&1&-&1&0&-&-&-&1 \\ 1&-&-&-&1&-&0&1&1&1 \\ 1&1&-&1&1&-&1&0&-&- \\ 1&-&1&1&-&-&1&-&0&1 \\ 1&1&-&-&-&1&1&-&1&0 \end{bmatrix} \quad \text{and} \quad W_2 = \begin{bmatrix} 0&1&0&1&1&0&0&-&-&1&1&-&1 \\ 1&0&1&0&1&1&0&0&-&-&1&1&- \\ -&1&0&1&0&1&1&0&0&-&-&1&1 \\ 1&-&1&0&1&0&1&1&0&0&-&-&1 \\ 1&1&-&1&0&1&0&1&1&0&0&-&- \\ -&1&1&-&1&0&1&0&1&1&0&0&- \\ -&-&1&1&-&1&0&1&0&1&1&0&0 \\ 0&-&-&1&1&-&1&0&1&0&1&1&0 \\ 0&0&-&-&1&1&-&1&0&1&0&1&1 \\ 1&0&0&-&-&1&1&-&1&0&1&0&1 \\ 1&1&0&0&-&-&1&1&-&1&0&1&0 \\ 0&1&1&0&0&-&-&1&1&-&1&0&1 \\ 1&0&1&1&0&0&-&-&1&1&-&1&0 \end{bmatrix}$$

Each of these are weighing matrices of weight nine; however, they are each endowed with an additional parculiar structure: W_1 is a symmetric $W(10, 9)$, and W_2 is a circulant $W(13, 9)$.

Properties of these matrices will be considered in the following section.

2.2 Properties

The initial questions when working with a new object are first "Where do they exist?" and second "What are the limitations on their existence?". We explored the second question for balanced incomplete block designs in §1.2. This section will briefly explore these questions for weighing matrices. In adressing these questions, we will begin with the special cases of Hadamard matrices and conference matrices.

Hadamard matrices appear to have first come to attention in the works of the English mathematician Sylvester during the nineteenth century. To begin, he noticed the Hadamard matrix of order two given by

$$H = \begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix}.$$

The next step is to notice that if H is a Hadamard matrix of order n, then

$$\begin{bmatrix} H & H \\ H & -H \end{bmatrix}$$

is a Hadamard matrix of order $2n$. This gives a family of symmetric Hadamard matrices of order 2^n.

Alternatively, let S_n be a matrix of order 2^n, and index the rows and columns by the elements of $\mathbb{Z}_2^n$. Finally, define $S_n = \left[(-1)^{\langle \mathbf{x},\mathbf{y}\rangle}\right]$, where $\langle \mathbf{x}, \mathbf{y}\rangle$ is the binary inner product of the sequences $\mathbf{x}$ and $\mathbf{y}$. The following is a straightforward computation.

Proposition 2.2. The matrix S_n, as defined above, is Hadamard matrix of order 2^n.

Proof. We need the following result:

$$\sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{\langle \mathbf{x},\mathbf{y}\rangle} = 2^n \delta_{\mathbf{0}}^{\mathbf{y}},$$

where $\mathbf{y}$ is some fixed element of $\mathbb{Z}_2^n$, and where $\delta_i^j = 1$ if $i = j$ and 0 otherwise. This follows from the fact that there are the same number of even weighted binary sequences in $\mathbb{Z}_2^n$ as there are odd weighted sequences. Considering the inner product between any two rows of S_n indexed by $\mathbf{x}$ and $\mathbf{y}$, we find

$$\begin{aligned} \sum_{\mathbf{z}\in\mathbb{Z}_2^n} (-1)^{\langle \mathbf{x},\mathbf{z}\rangle}(-1)^{\langle \mathbf{y},\mathbf{z}\rangle} &= \sum_{\mathbf{z}\in\mathbb{Z}_2^n} (-1)^{\langle \mathbf{x}+\mathbf{y},\mathbf{z}\rangle} \\ &= 2^n \delta_{\mathbf{x}}^{\mathbf{y}}. \end{aligned}$$

This shows that S_n is as asserted. *Q.E.D.*

Example 2.3. The first three iterations of Sylvester's construction are

$$\begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ 1 & 1 & - & - \\ 1 & - & - & 1 \end{bmatrix}, \text{ and } \quad \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & - & 1 & - & 1 & - & 1 & - \\ 1 & 1 & - & - & 1 & 1 & - & - \\ 1 & - & - & 1 & 1 & - & - & 1 \\ 1 & 1 & 1 & 1 & - & - & - & - \\ 1 & - & 1 & - & - & 1 & - & 1 \\ 1 & 1 & - & - & - & - & 1 & 1 \\ 1 & - & - & 1 & - & 1 & 1 & - \end{bmatrix}.$$

There is a strong necessary parametric condition for the existence of a Hadamard matrix which we show below.

Proposition 2.4. A $W(n, n)$ exists only if n is 1, 2, or a multiple of 4.

Proof. The cases that n is 1 or 2 are

$$[1], \text{ and } \begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix}.$$

Otherwise, the first three rows are signed permutation equivalent to

$$\underbrace{\begin{matrix} 1 & \dots & 1 \\ 1 & \dots & 1 \\ 1 & \dots & 1 \end{matrix}}_{a} \quad \underbrace{\begin{matrix} 1 & \dots & 1 \\ 1 & \dots & 1 \\ - & \dots & - \end{matrix}}_{b} \quad \underbrace{\begin{matrix} 1 & \dots & 1 \\ - & \dots & - \\ 1 & \dots & 1 \end{matrix}}_{c} \quad \underbrace{\begin{matrix} 1 & \dots & 1 \\ - & \dots & - \\ - & \dots & - \end{matrix}}_{d}$$

This gives rise to the linear system

$$\begin{aligned} a + b + c + d &= n, \\ a + b - c - d &= 0, \\ a - b + c - d &= 0, \text{ and} \\ a - b - c + d &= 0, \end{aligned}$$

which has the solution $a = b = c = d = \frac{n}{4}$. *Q.E.D.*

We will present a construction of conference matrices that is due to Paley. Let q be an odd prime power, and let $\mathbb{F}_q$ be the finite field of order q. Define the extended quadratic residue function as

$$\chi(\alpha) = \begin{cases} 0 & \text{if } \alpha = 0; \\ 1 & \text{if } \alpha \text{ is a square; and} \\ -1 & \text{if } \alpha \text{ is not a square.} \end{cases}$$

for $\alpha \in \mathbb{F}_q$. The following lemmata will be required.

Lemma 2.5. Let q be an odd prime power. Then $\sum_{\alpha\in\mathbb{F}_q}\chi(\alpha)\chi(\alpha+\beta) = -1$, whenever $\beta \neq 0$.

PROOF. Clearly, $\chi(0)\chi(0+\beta) = 0$. By the field structure of $\mathbb{F}_q$, if $\alpha \neq 0$, then there is a unique $\gamma \neq 1$ such that $\alpha + \beta = \alpha\gamma$. As α ranges over the non-zero elements of $\mathbb{F}_q$, it follows that γ ranges over all those elements different from 1. Then

$$\begin{aligned}\sum_{\alpha\in\mathbb{F}_q}\chi(\alpha)\chi(\alpha+\beta) &= \sum_{\alpha\in\mathbb{F}_q^\times}\chi(\alpha)^2\chi(\gamma)\\ &= \sum_{\gamma\in\mathbb{F}_q}\chi(\gamma) - \chi(1)\\ &= -1,\end{aligned}$$

because $\sum_{\gamma\in\mathbb{F}_q}\chi(\gamma)$. *Q.E.D.*

Let $\mathbb{F}_q = \{\alpha_1 = 0, \alpha_2, \ldots, \alpha_q\}$. Define the *Paley matrix* $P = [p_{ij}]$ as $p_{ij} = \chi(\alpha_j - \alpha_i)$. Since $\chi(\alpha_j - \alpha_i) = \chi(-1)\chi(p_i - p_j)$, P is symmetric if $q \equiv 1 \bmod 4$, and P is skew-symmetric if $q \equiv -1 \bmod 4$. The following is an immediate consequence of the previous lemma.

Lemma 2.6. Let P be a Paley matrix defined as above. Then:

i. $PP^t = qI - J$, and

ii. $PJ = JP = 0$.

Proposition 2.7. Let q be an odd prime power. If $q \equiv 1 \bmod 4$, then there is a symmetric conference matrix of order $q + 1$. If $q \equiv -1 \bmod 4$, then there is a skew-symmetric conference matrix of order $q + 1$.

PROOF. If $q \equiv 1 \bmod 4$, define

$$W_1 = \begin{bmatrix} 0 & \mathbf{j}^t \\ \mathbf{j} & P \end{bmatrix};$$

while if $q \equiv -1 \bmod 4$, then define

$$W_2 = \begin{bmatrix} 0 & \mathbf{j}^t \\ -\mathbf{j} & P \end{bmatrix}.$$

In either case, W_1 and W_2 are seen to be the required matrices. *Q.E.D.*

Corollary 2.8. If $q \equiv -1 \bmod 4$ is a prime power, then there is a Hadamard matrix of order $q+1$; while if $q \equiv 1 \bmod 4$, then there is a Hadamard matrix of order $2(q + 1)$.

PROOF. If A is a skew-symmetric (0,1,-1)-matrix of order n such that $AA^t = (n-1)I$, then $I + A$ is a Hadamard matrix. Now, apply the result. If B is a symmetric (0,1,-1)-matrix with zero diagonal of order n such that $BB^t = (n-1)I$, then $\left[\begin{smallmatrix} I+B & -I+B \\ -I+B & -I-B \end{smallmatrix}\right]$ is the required matrix. *Q.E.D.*

Clearly, a conference matrix of odd order cannot exist, but we have shown the existence for orders that are 0 or 2 modulo 4. The next result provides a particular characterization of conference matrices in these cases, whenever they exist.

Theorem 2.9 (Delsarte, Goethals, Seidel)**.** Let W be a $W(n, n-1)$. Then:

i. If $n \equiv 0 \bmod 4$, then W is signed permutation equivalent to a skew-symmetric conference matrix; and

ii. if $n \equiv 2 \bmod 4$, then W is signed permutation equivalent to a symmetric conference matrix.

We next give a few simple necessary conditions for the existence of more general cases of weighing matrices.

Proposition 2.10. Let n be odd. There exists a $W(n, k)$ only if:

i. k is a square, and

ii. $(n-k)^2 - (n-k) \geq n-1$.

PROOF.

i. We have $\det(WW^t) = \det^2(W) = k^n$. Since n is odd, it follows that k must be a square.

ii. Let $*$ denote the Hadamard product, that is, component-wise multiplication. Then $A = W * W$ is (0,1)-matrix with k non-zero entries in every row and column. Then $AJ = A^tJ = kJ$ so that $AA^tJ = k^2J$. If the rows of W are denoted by $r_1, r_2, \ldots, r_n$, then, for any fixed j,

$$\sum_{i \neq j} r_i r_j^t = k^2 - k.$$

Moreover, the inner product between any distinct rows of A must be even since W is a weighing matrix.
Define $B = J - A$. Then the inner product between any two rows is odd so that

$$(n-k)^2 - (n-k) \geq n-1,$$

which is what was to be shown. *Q.E.D.*

Our last result in this section provides a characterization of the case in which the order of the weighing matrix is congruent to 2 modulo 4.

Proposition 2.11. A $W(n,k)$, for $n \equiv 2 \bmod 4$, exists only if k is the sum of two squares.

PROOF. Let $W = [w_{ij}]$ be a $W(n,k)$ such that $n \equiv 2 \bmod 4$. If $n = 2$, then the existence of a $W(2,k)$, for $k = 1$ or 2, is given by I_2 and $\left[\begin{smallmatrix} 1 & 1 \\ 1 & - \end{smallmatrix}\right]$. We now assume that $n = 4w + 2$ for some $w \in \mathbb{Z}^+$. Define

$$L_j = \sum_{i=1}^{n} w_{ij} x_i,$$

where $x_1, \ldots, x_n$ are indeterminates. Then

$$L_j^2 = \sum_{i=1}^{n} \sum_{h=1}^{n} w_{ij} w_{hj} x_i x_h$$

so that

$$\begin{aligned} \sum_{j=1}^{n} L_j^2 &= \sum_{j=1}^{n} \sum_{i=1}^{n} \sum_{h=1}^{n} w_{ij} w_{hj} x_i x_h \\ &= \sum_{i=1}^{n} \sum_{h=1}^{n} \left(\sum_{j=1}^{n} w_{ij} w_{hj} \right) x_i x_h \\ &= k \sum_{j=1}^{n} x_j^2. \end{aligned}$$

We now define $x_1, \ldots, x_n$ in terms of new indeterminates $y_1, \ldots, y_n$. For $1 \le h \le n$, let $\bar{y}_h = (y_{4h-3}, y_{4h-2}, y_{4h-1}, y_{4h})$ and $\bar{x}_h = (x_{4h-3}, x_{4h-2}, x_{4h-1}, x_{4h})$. Let $k = k_1^2 + k_2^2 + k_3^2 + k_4^2$, where each $k_i \in \mathbb{Z}^+ \cup \{0\}$. Let

$$C = \begin{pmatrix} k_1 & k_2 & k_3 & k_4 \\ \bar{k}_2 & k_1 & \bar{k}_4 & k_3 \\ \bar{k}_3 & k_4 & k_1 & \bar{k}_2 \\ \bar{k}_4 & \bar{k}_3 & k_2 & k_1 \end{pmatrix}$$

so that $CC^t = kI_4$. Next, define $\bar{y}_h = \bar{x}_h C$, $y_{n-1} = x_{n-1}$, and $y_n = x_n$. It follows that

$$\begin{aligned} \sum_{i=0}^{3} y_{4h-i}^2 &= \bar{y}_h \bar{y}_h^t \\ &= \bar{x}_h C C^t \bar{x}_h^t \\ &= k \sum_{i=0}^{3} x_{4h-i}; \end{aligned}$$

whence,

$$\sum_{i=1}^{n} L_i^2 = \sum_{i=1}^{n-2} y_i^2 + k(y_{n-1}^2 + y_n^2).$$

We have already that each L_i is an integral sum of the x_i's. Since $C^{-1} = \frac{1}{k}C^t$, it follows that we can express each x_i as a rational linear combination of the y_i's. Then

$$L_1 = \sum_{i=1}^{n} e_i y_i$$

for rational e_i. If $e_1 \neq 1$, then let $y_1 = L_1$; while if $e_1 = 1$, then let $y_1 = -L_1$. Thus, y_1 is expressed as a rational linear combination of $y_2, \ldots, y_n$ such that $L_1^2 = y_1^2$. Whence,

$$\sum_{i=2}^{n} L_i^2 = \sum_{i=2}^{n-2} y_i^2 + k(y_{n-1}^2 + y_n^2).$$

Continuing in this way, we see that

$$L_{n-1}^2 + L_n^2 = k(y_{n-1^2} + y_n^2).$$

Taking $y_{n-1} = 1$ and $y_n = 0$, we see that k is expressible as a sum of rational squares, namely, $k = L_{n-1}^2 + L_n^2$. But a non-negative integer is expressible as a sum of two rational squares if and only if it is expressible as a sum of two integral squares (see Notes at the end of this chapter). This is what we wanted to prove. *Q.E.D.*

2.3 Related Configurations

In the previous section we used the idea of *signed permutation equivalence* of weighing matrices. To make this idea more precise, let P and Q be signed permutation matrices of order n. If W is a weighing matrix of order n, then PWQ is a weighing matrix. This is seen by

$$(PWQ)(PWQ)^t = PWQQ^tW^tP^t = PWW^tP^t = P(kI)P^t = kI.$$

We will drop the modifier and simply refer to W and PWQ as equivalent. From this we see that every $W(n,n)$ is equivalent to one in which the first row and column consist entirely of unity. These will be called *normalized* Hadamard matrices and yield the following.

Proposition 2.12. The existence of a Hadamard matrix of order $4n$ is equivalent to the existence of a symmetric BIBD$(4n-1, 2n-1, n-1)$.

PROOF. Assume the existence of a Hadamard matrix of order $4n$ (say K), and note that we may assume that it is normalized. Let H be the matrix obtained by deleting the first row and column of K, and define $A = \frac{1}{2}(J+H)$. Since K can be assumed to be normalized, we see that each row and column (save the first of each) have $2n$ 1s and $2n$ -1s. Thus, we only need to comment on the λ of the putative design. It follows from the proof of Proposition 2.4, that each row has $n-1$ 1s in common; whence, $\lambda = n-1$. The sufficiency finally follows from Proposition 1.8.

The necessity is demonstrated by simply reversing the above reasoning. *Q.E.D.*

The rows of the incidence matrices of any design form a set of binary strings. Moreover, these binary strings have a constant number of non-zero entries, and they disagree in the same number of positions. It is these properties of designs that allow them to play a fundamental role in the theory of error-correcting codes. We define codes thus.

Definition. Let A be a finite set of q letters that include the symbol 0. We define the following.

i. A *code* C is a subset of the product A^n. It is customary to denote $|C|$ as M.

ii. If $\mathbf{x} \in C$, and if $\mathbf{y} \in C$, then the *Hamming distance* between $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ is given by $d(x,y) = |\{i \mid x_i \neq y_i\}|$. The minimum distance of the code is $d(C) = \min\{d(\mathbf{x},\mathbf{y}) \mid \mathbf{x},\mathbf{y} \in C)\}$. Note that the minimum distance forms a metric on the code.

iii. The *Hamming weight* of any codeword $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ of C is defined to be $wt(\mathbf{x}) = |\{i \mid x_i \neq 0\}|$. The minimum weight of the code is $wt(C) = \min\{wt(\mathbf{x}) \mid \mathbf{x} \in C\}$.

If $C \subset A^n$ is a code with minimum distance d and $|C| = M$, where $|A| = q$, then we will say that C is an $(n, M, d)_q$-code. We will often drop the subscript from the denotation.

In applications one must send strings of encoded information through a "noisy" channel. It follows that the message received may not be the message that was sent. The importance of the minimum distance in detecting and correcting these errors is shown by the next result.

Proposition 2.13. Let C be an (n, M, d)-code. Then:

i. If $d \geq t+1$, then C can detect up to t errors; and

ii. if $d \geq 2t+1$, then C can correct up to t errors.

PROOF.

i. If the codeword $\mathbf{x}$ was sent and then received with t or fewer errors, it follows that the distance between the received word and $\mathbf{x}$ is less than the minimum distance of the code; hence, we see that the received word is not a codeword.

ii. Again, let $\mathbf{x}$ be the codeword that was transmitted, and let $\mathbf{y}$ be the word that was received with t or fewer errors. Since d is a metric on C, we find that, for any codeword $\mathbf{z} \neq \mathbf{x}$, $d(\mathbf{z}, \mathbf{y}) \geq t+1$; for otherwise, by the triangle inequality, we have that $d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z}) \leq 2t$, which is a contradiction. Therefore, $\mathbf{x}$ is the "closest" codeword to $\mathbf{y}$, so we decode $\mathbf{y}$ as $\mathbf{x}$. *Q.E.D.*

It is not difficult to see that a BIBD(v, b, r, k, λ) gives a binary, constant weight, equidistant $(b, v, 2(r-\lambda))$-code; while appending the binary complement to the code gives a $(b, 2v, d)$-code, where $d \in \{0, b, 2(r-\lambda), b-2(r-\lambda)\}$.

In practise one may have a given code length and minimum distance in mind. The problem becomes, therefore, maximizing the number of codewords given a length and minimum distance. Often this approach is undertaken with particular cases or families of codes, but there are some general bounds that can be obtained.

Theorem 2.14 (Hamming Bound)**.** Let C be an $(n, M, 2t+1)_q$-code. Then

$$M \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq q^n.$$

PROOF. Let $\mathbf{x} \in C$. Define the closed sphere of radius r about $\mathbf{x}$ as $\bar{S}_r(\mathbf{x}) = \{\mathbf{y} \mid d(\mathbf{x}, \mathbf{y}) \leq r\}$. It follows by straightforward counting that

$$|\bar{S}_r(\mathbf{x})| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

By ii. of Proposition 2.13, it follows that the spheres of radius t are disjoint. Hence,

$$M \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq |A^n| = q^n,$$

which is what was to be shown. *Q.E.D.*

The Hamming Bound is tight, as the following example shows. Such codes are called *perfect*.

Example 2.15. We begin with the incidence matrix of a Hadamard BIBD(7,3,1), and then append the binary complement, to construct the following perfect binary (7,14,3)-code (transposed).

$$\begin{bmatrix} 0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1 \\ 1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,0\,0\,1\,1 \\ 0\,0\,1\,1\,0\,0\,1\,1\,1\,0\,0\,1\,1\,0 \\ 1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1 \\ 0\,1\,0\,0\,1\,0\,1\,1\,0\,1\,1\,0\,1\,0 \\ 1\,0\,0\,0\,0\,1\,1\,0\,1\,1\,1\,1\,0\,0 \\ 0\,0\,1\,0\,1\,1\,0\,1\,1\,0\,1\,0\,0\,1 \end{bmatrix}$$

In the case of binary codes, we can produce a further bound.

Theorem 2.16 (Plotkin Bound)**.** For any binary (n, M, d)-code C, if $n < 2d$, then

$$M \leq 2 \left\lfloor \frac{d}{2d-n} \right\rfloor.$$

Proof. We count the sum $S = \sum_{\mathbf{u}\in C} \sum_{\mathbf{v}\in C} d(\mathbf{u}, \mathbf{v})$ in two ways. First, we note that there are $M(M-1)$ pairs such that $d(\mathbf{u}, \mathbf{v}) \geq d$, and there are M pairs such that $d(\mathbf{u}, \mathbf{v}) = 0$. Hence, $S \geq M(M-1)d$.

Second, let A be the (0,1)-matrix whose rows are the codewords of C, and let x_i be the number of 1s in the i^{th} column of A. Each column contributes $2x_i(M - x_i)$ to the sum; whence, $S = \sum_{i=1}^{n} 2x_i(M - x_i)$.

If M is even, then the sum is maximized precisely when $2x_i = M$. Therefore, $S \leq nM^2/2$ so that $M(M-1)d \leq nM^2/2$; that is, $M(2d-n) \leq 2d$. Since $n < 2d$, we have that

$$M \leq \left\lfloor \frac{2d}{2d-n} \right\rfloor = 2 \left\lfloor \frac{d}{2d-n} \right\rfloor.$$

If M is odd, then the sum is maximized if $2x_i = M + 1$ or $M - 1$. Therefore, $S \leq n(M^2-1)/2$, and we arrive at

$$M \leq \frac{n}{2n-d} = \frac{2d}{2d-n} - 1.$$

We finally obtain

$$M \leq \left\lfloor \frac{2d}{2d-n} \right\rfloor - 1 \leq 2 \left\lfloor \frac{d}{2d-n} \right\rfloor - 1.$$

Corollary 2.17. If d is even and $n \leq 2d$, then

$$M \leq 2\left\lfloor \frac{d}{2d-n} \right\rfloor \qquad \text{if the inequality is strict, and}$$
$$M \leq 4d \qquad \text{if we have equality.}$$

If, on the other hand, d is odd and $n \leq 2d+1$, then

$$M \leq 2\left\lfloor \frac{d+1}{2d-n+1} \right\rfloor \qquad \text{if the inequality is strict, and}$$
$$M \leq 4(d+1) \qquad \text{if we have equality.}$$

The following example illustrates the Plotkin bound is tight; in fact, the following code is developed from a Hadamard matrix.

Example 2.18. We show an (11,12,6)-code.

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

We conclude this section with the following application of Hadamard matrices to codes meeting the Plotkin Bound. Essentially, the result states that if enough Hadamard matrices exist, then there are perfect codes. For brevity, we omit the proof.

Theorem 2.19 (Levenshtein's Theorem)**.** Let n and k be positive integers. In each of the following cases we have equality in the Plotkin Bounds.

i. n is even, and there exists Hadamard matrices of orders $4k$ and $4k+4$;

ii. n is odd, k is even, and there exists Hadamard matrices of orders $2k$ and $4k+4$; and

iii. n and k are odd, and there exists Hadamard matrices of orders $4k$ and $2k+2$.

2.4 Notes

The opening example was retrieved from MacWilliams, Sloane [MS77a]; though, Hotelling [Hot44] appears to be the first to note the applications of the matrices of this chapter to weighing designs. The result that the variance of the sum of independent random variables is the sum of the variances, is shown in Sahoo [Sah13].

The study of weighing matrices appears to have began with the special case of Hadamard matrices. Many of the initial contributors to the study of these matrices include some very prominent names inluding Sylvester, Hadamard, and Paley.

Sylvester [Syl67] appears to be the first individual to comment on Hadamard matrices and discovered the family bearing his name while investigating orthogonal matrices and their applications generally. This particular family is probably the most studied of any known, and it is still a fruitful area of study today. See for example Mitrouli [Mit13].

Hadamard [Had93] independantely discovered Hadamard matrices while studying analysis. In particular, he studied the question of maximal determinants, and he began by showing the Vandermonde matrix has maximal determinant when its entries are roots of unity. Then he considered the cases of the unit circle and gave examples of orders 12 and 20, which turned out to be Hadamard matrices. The question of maximal determinant was partially answered by showing that, for the cases of matrices of orders $n = 1, 2$, and $4k$, where $k \in \mathbb{Z}_+$, the matrix has maximal determinant if and only if it is a Hadamard matrix (see [Cam94]). Proposition 2.4 is also due to Hadamard.

Proposition 2.7 and the subsequent results are due to the analyst Paley [Pal33]. A comprehensive treatment of Paley's beautiful results and their consequences are found in Hall [Hal86].

While the theory of weighing matrices had been around for some time, the fervor about the subject seems to have started during 1970s as a result of their broadening applications. Theorem 2.9 is found in Delsarte, Goethals, Seidel [DGS71]. Proposition 2.10 is found in Seberry [Seb17], and Proposition 2.11 is asked in the excersises of Stinson [Sti04] where the proof is essentially a reproduction of the techniques used to prove the famed *Bruck-Ryser-Chowla Theorem* (See [Hal86] and [Sti04] for expositions of this result).

To show that a non-negative integer is the sum of two rational squares if and only if it is the sum of two integral squares follows by an application of Fermat's two squares Theorem (see [Ros00]). It suffices to comment on sufficiency. Fermat's result shows that a natural number is the sum of two integral squares if and only if it has no prime factor congrent to -1 modulo 4 that has an odd power. If for some positive integer n, we have that $n = \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2$, then nc^2 must have only even powers of those primes -1 modulo 4. Since an even integer subtracted from an odd integer is odd, it

must be that n also has even powers of those primes -1 modulo 4. Therefore, by Fermat's result, n is also the sum of two integral squares.

Hadamard designs yield an important family of symmetric designs. Proposition 2.12 can be found in most references on the subject. The version given here is taken from [Hal86]. The application of Hadamard matrices to the theory of error correcting codes is well documented, and exceptional references are MacWilliam's, Sloane [MS77b], [MS77a] and van Lint [vL99]. Horadam [Hor07] provides an in-depth introduction of the applications of Hadamard matrices to the theory of signal processing. Cameron, van Lint [CvL91] further discusses the connections of designs, graphs, and codes. Levenshtein's Theorem 2.19 is shown in Levenshtein [Lev61].

Chapter 3

Generalizations

3.1 Generalizations of Weighing Matrices

To motivate the discussion of this section, we introduce the following operation on complex matrices. Let $W = [w_{ij}]$ be a matrix over $\mathbb{C}$, and let $\overline{z}$ be the complex conjugate of $z \in \mathbb{C}$. Define $\overline{W}$ by $w_{ij} \mapsto \overline{w}_{ij}$. Finally, the *Hermitian transpose* is the composition defined by $W^* \equiv (\overline{W})^t$.

We can now consistenly extend our definition of weighing matrices to more general cases. In what follows, let $\mathbb{T}$ be those complex numbers of unit modulus.

Definition. A *unit weighing matrix* W of order n and weight k is a square matrix of order n over $\mathbb{T} \cup \{0\}$ such that $WW^* = kI$. It is customary to denote this as $\mathrm{UW}(n, k)$.

As before, we see that there are k non-zero entries in every row and column. In the case that $n = k$, we call the matrix a *unit Hadamard matrix* and denote this as $\mathrm{UH}(n)$.

Example 3.1. Let $D = [d_{st}]$ be defined as $d_{st} = \omega^{(s-1)(t-1)}$, for $s, t \in \{1, 2, \ldots, 13\}$.

Then

$$D = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 & \omega^8 & \omega^9 & \omega^{10} & \omega^{11} & \omega^{12} \\
1 & \omega^2 & \omega^4 & \omega^6 & \omega^8 & \omega^{10} & \omega^{12} & \omega & \omega^3 & \omega^5 & \omega^7 & \omega^9 & \omega^{11} \\
1 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} & \omega^2 & \omega^5 & \omega^8 & \omega^{11} & \omega & \omega^4 & \omega^7 & \omega^{10} \\
1 & \omega^4 & \omega^8 & \omega^{12} & \omega^3 & \omega^7 & \omega^{11} & \omega^2 & \omega^6 & \omega^{10} & \omega & \omega^5 & \omega^9 \\
1 & \omega^5 & \omega^{10} & \omega^2 & \omega^7 & \omega^{12} & \omega^4 & \omega^9 & \omega & \omega^6 & \omega^{11} & \omega^3 & \omega^8 \\
1 & \omega^6 & \omega^{12} & \omega^5 & \omega^{11} & \omega^4 & \omega^{10} & \omega^3 & \omega^9 & \omega^2 & \omega^8 & \omega & \omega^7 \\
1 & \omega^7 & \omega & \omega^8 & \omega^2 & \omega^9 & \omega^3 & \omega^{10} & \omega^4 & \omega^{11} & \omega^5 & \omega^{12} & \omega^6 \\
1 & \omega^8 & \omega^3 & \omega^{11} & \omega^6 & \omega & \omega^9 & \omega^4 & \omega^{12} & \omega^7 & \omega^2 & \omega^{10} & \omega^5 \\
1 & \omega^9 & \omega^5 & \omega & \omega^{10} & \omega^6 & \omega^2 & \omega^{11} & \omega^7 & \omega^3 & \omega^{12} & \omega^8 & \omega^4 \\
1 & \omega^{10} & \omega^7 & \omega^4 & \omega & \omega^{11} & \omega^8 & \omega^5 & \omega^2 & \omega^{12} & \omega^9 & \omega^6 & \omega^3 \\
1 & \omega^{11} & \omega^9 & \omega^7 & \omega^5 & \omega^3 & \omega & \omega^{12} & \omega^{10} & \omega^8 & \omega^6 & \omega^4 & \omega^2 \\
1 & \omega^{12} & \omega^{11} & \omega^{10} & \omega^9 & \omega^8 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega
\end{bmatrix},$$

where ω is a complex primitive complex 13^{th} root of unity. It follows without much difficulty that D is a UH(13).

The construction in the above example can be extended to every n in the obvious manner (the so called Discrete Fourier Transforms). Thus, we have that there is a unit Hadamard matrix of every order. The following example evinces a proper unit weighing matrix.

Example 3.2. The following is a UW(57, 49).

$$\begin{bmatrix}
1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3&0&6&4&1&5&6&3&4&4&4&6&2&5&5&2&4&2&6&5\\
6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3&0&6&4&1&5&6&3&4&4&4&6&2&5&5&2&4&2&6\\
1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3&0&6&4&1&5&6&3&4&4&4&6&2&5&5&2&4&2\\
3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3&0&6&4&1&5&6&3&4&4&4&6&2&5&5&2&4\\
5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3&0&6&4&1&5&6&3&4&4&4&6&2&5&5&2\\
3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3&0&6&4&1&5&6&3&4&4&4&6&2&5&5\\
6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3&0&6&4&1&5&6&3&4&4&4&6&2&5\\
6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3&0&6&4&1&5&6&3&4&4&4&6&2\\
3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3&0&6&4&1&5&6&3&4&4&4&6\\
1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3&0&6&4&1&5&6&3&4&4&4\\
5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3&0&6&4&1&5&6&3&4&4\\
5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3&0&6&4&1&5&6&3&4\\
5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3&0&6&4&1&5&6&3\\
4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3&0&6&4&1&5&6\\
1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3&0&6&4&1&5\\
6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3&0&6&4&1\\
2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3&0&6&4\\
5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3&0&6\\
1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3&0\\
0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2&3\\
4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6&2\\
3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0&6\\
1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0&0\\
0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1&0\\
0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1&1\\
2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3&5&4&3&1\\
2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&3&5&4&3\\
4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&3&5&4\\
5&4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&3&5\\
6&5&4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2&3\\
4&6&5&4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2&2\\
3&4&6&5&4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6&2\\
3&3&4&6&5&4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2&6\\
1&3&3&4&6&5&4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2&2\\
3&1&3&3&4&6&5&4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0&2\\
3&1&3&3&4&6&5&4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6&0\\
0&3&3&1&3&3&4&6&5&4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0&6\\
1&0&3&3&1&3&3&4&6&5&4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6&0\\
0&1&0&3&3&1&3&3&4&6&5&4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4&6\\
1&0&1&0&3&3&1&3&3&4&6&5&4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5&4\\
5&1&0&1&0&3&3&1&3&3&4&6&5&4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5&5\\
6&5&1&0&1&0&3&3&1&3&3&4&6&5&4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6&5\\
6&6&5&1&0&1&0&3&3&1&3&3&4&6&5&4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0&6\\
1&6&6&5&1&0&1&0&3&3&1&3&3&4&6&5&4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6&0&5&6&5&2&5&4&0&5&2&0\\
6&1&6&3&6&5&0&6&3&0&1&6&6&5&1&0&1&0&3&3&1&3&3&4&6&5&4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2&6\\
1&0&6&1&6&3&6&5&0&6&3&0&1&6&6&5&1&0&1&0&3&3&1&3&3&4&6&5&4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1&2\\
3&1&0&6&1&6&3&6&5&0&6&3&0&1&6&6&5&1&0&1&0&3&3&1&3&3&4&6&5&4&2&2&0&0&1&3&4&0&1&5&2&6&1&4&5&5&5&1&3&6&6&3&5&3&1&6&1
\end{bmatrix}$$

where the non-zero entries are the logarithms of a primitive complex 6^{th} root of unity.

The above two examples are part of an important subclass of unit weighing matrices, namely, the so-called *Butson weighing matrices*. The non-zero entries of these matrices are restricted to come from some group of primitive complex roots of unity. A Butson weighing matrix of order n, weight k, over the primitive p^{th} roots of unity is denoted by $\text{BW}(n, k; p)$. Hence, the UW(57,49) above is a BH(57,49;6). We again distinguish the case that $n = k$ by calling them *Butson Hadamard matrices*, and we denote this as $\text{BH}(n, p)$. Thus, the above UH(13) is, in fact, a BH(13,13).

If we further restrict ourselves to the case of primitive fourth roots of unity, we call the matrix a *quaternary complex weighing matrix* (respectively, *quaternary complex Hadamard matrix*). It is customary to denote this as $\mathrm{CW}(n,k)$ (respectively, $\mathrm{CH}(n)$) for a quaternary complex weighing matrix of order n and weight k.

Example 3.3. The following is a CW(31,25).

$$\begin{bmatrix}
j & j & 0 & 0 & 1 & j & i & i & j & -0 & j & i & 0 & i & 0 & 1 & i & -0 & 1 & 1 & 1 & j & -j & i & j & 1 & 1 & i \\
1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 & j & i & 0 & i & 0 & 1 & i & -0 & 1 & 1 & 1 & j & -j & i & j & 1 & 1 \\
j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 & j & i & 0 & i & 0 & 1 & i & -0 & 1 & 1 & 1 & j & -j & i & j & 1 \\
j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 & j & i & 0 & i & 0 & 1 & i & -0 & 1 & 1 & 1 & j & -j & i & j \\
-j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 & j & i & 0 & i & 0 & 1 & i & -0 & 1 & 1 & 1 & j & -j & i \\
1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 & j & i & 0 & i & 0 & 1 & i & -0 & 1 & 1 & 1 & j & -j \\
-1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 & j & i & 0 & i & 0 & 1 & i & -0 & 1 & 1 & 1 & j & - \\
i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 & j & i & 0 & i & 0 & 1 & i & -0 & 1 & 1 & 1 & j \\
-i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 & j & i & 0 & i & 0 & 1 & i & -0 & 1 & 1 & 1 \\
j & -i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 & j & i & 0 & i & 0 & 1 & i & -0 & 1 & 1 \\
j & j & -i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 & j & i & 0 & i & 0 & 1 & i & -0 & 1 \\
j & j & j & -i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 & j & i & 0 & i & 0 & 1 & i & -0 \\
0 & j & j & j & -i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 & j & i & 0 & i & 0 & 1 & i & - \\
i & 0 & j & j & j & -i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 & j & i & 0 & i & 0 & 1 & i \\
1 & i & 0 & j & j & j & -i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 & j & i & 0 & i & 0 & 1 \\
j & 1 & i & 0 & j & j & j & -i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 & j & i & 0 & i & 0 \\
0 & j & 1 & i & 0 & j & j & j & -i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 & j & i & 0 & i \\
1 & 0 & j & 1 & i & 0 & j & j & j & -i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 & j & i & 0 \\
0 & 1 & 0 & j & 1 & i & 0 & j & j & j & -i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 & j & i \\
1 & 0 & 1 & 0 & j & 1 & i & 0 & j & j & j & -i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 & j \\
-1 & 0 & 1 & 0 & j & 1 & i & 0 & j & j & j & -i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & -0 \\
0 & -1 & 0 & 1 & 0 & j & 1 & i & 0 & j & j & j & -i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j & - \\
i & 0 & -1 & 0 & 1 & 0 & j & 1 & i & 0 & j & j & j & -i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i & i & j \\
-i & 0 & -1 & 0 & 1 & 0 & j & 1 & i & 0 & j & j & j & -i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i & i \\
1 & -i & 0 & -1 & 0 & 1 & 0 & j & 1 & i & 0 & j & j & j & -i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 & j & i \\
1 & 1 & -i & 0 & -1 & 0 & 1 & 0 & j & 1 & i & 0 & j & j & j & -i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 & j \\
-1 & 1 & -i & 0 & -1 & 0 & 1 & 0 & j & 1 & i & 0 & j & j & j & -i & -1 & -j & j & 1 & j & j & 0 & 0 & 1 \\
j & -1 & 1 & -i & 0 & -1 & 0 & 1 & 0 & j & 1 & i & 0 & j & j & j & -i & -1 & -j & j & 1 & j & j & 0 & 0 \\
0 & j & -1 & 1 & -i & 0 & -1 & 0 & 1 & 0 & j & 1 & i & 0 & j & j & j & -i & -1 & -j & j & 1 & j & j & 0 \\
0 & 0 & j & -1 & 1 & -i & 0 & -1 & 0 & 1 & 0 & j & 1 & i & 0 & j & j & j & -i & -1 & -j & j & 1 & j & j \\
-0 & 0 & j & -1 & 1 & -i & 0 & -1 & 0 & 1 & 0 & j & 1 & i & 0 & j & j & j & -i & -1 & -j & j & 1 & j
\end{bmatrix}$$

where $j = -i$.

To motivate the results of the next section, we need to be more general. To this end, we remind the reader about the group ring. If G is a group and R a ring, we define $R[G]$ to be the collection of all formal sums $\sum a_g g$, where $a_g \in R$ and $g \in G$, such that all but a finite number of the a_gs are 0. To form $R[G]$ into a ring, one simply defines sums and products in the usual way. We will always make the identification $G = \sum_{g \in G} g$.

We also need to extend the Hermitian transpose to matrices over $R[G]$. Let λ be any involution over G. We naturally extend this to $R[G]$ by $\lambda(\sum a_g g) = \sum a_g \lambda(g)$. If $W = [w_{ij}]$ is a matrix over $R[G]$, define W^λ

by $w_{ij} \mapsto \lambda(w_{ij})$. Then the Hermitian transpose becomes $W^* \equiv (W^\lambda)^t$. In what follows, we will take λ to be the inversion operation on G.

In every case involving real, Butson, and quaternary complex weighing matrices, we notice that the non-zero elements come from some finite signable group G; that is, a group with a unique subgroup of order 2. Moreover, if $\sum u_i \bar{v}_i$ is the usual the Hermitian inner product between any two distinct vectors $v = (v_i)_{i=1}^n$ and $u = (u_i)_{i=1}^n$ in $\mathbb{C}^n$, then we see that the Hermitian product between distinct rows vanishes because it evaluates to $\sum_{g \in G} a_g(g - g) = 0$, for some integral constants a_g. For the above two examples, we actually have that the product becomes $a \sum_{g \in G} g = 0$ (note that a may be different when considering the product of different pairs of rows). This motivates the following definition.

Definition. Let G be a finite group. A *generalized weighing matrix* W of order n and weight k over the group G is a square matrix of order n with monomial entries from $\mathbb{Z}[G]$ such that $WW^* \equiv kI$ modulo the ideal $\mathbb{Z}G$. This is denoted as $GW(n, k; G)$.

Example 3.4. The following is a GW$(12, 9; Z_3)$.

$$\begin{bmatrix}
0 & \omega & 1 & \omega & 1 & 1 & 0 & 1 & 0 & 1 & \omega^2 & \omega^2 \\
1 & \omega & \omega^2 & 0 & 0 & \omega & 1 & 1 & 1 & \omega^2 & 1 & 0 \\
1 & 1 & 0 & \omega^2 & 1 & 0 & \omega^2 & 0 & \omega & 1 & 1 & \omega \\
\omega^2 & 0 & 1 & 1 & 1 & \omega & 1 & \omega^2 & \omega & 0 & 0 & 1 \\
0 & \omega^2 & 1 & 1 & \omega^2 & 1 & 0 & 1 & 0 & \omega & 1 & \omega \\
1 & \omega^2 & \omega & 0 & 0 & 1 & 1 & \omega^2 & 1 & 1 & \omega & 0 \\
1 & 0 & \omega^2 & 1 & 1 & 1 & \omega & \omega & \omega^2 & 0 & 0 & 1 \\
\omega^2 & 1 & 0 & 1 & \omega & 0 & \omega & 0 & 1 & 1 & 1 & \omega^2 \\
0 & 1 & 1 & \omega^2 & \omega & 1 & 0 & 1 & 0 & \omega^2 & \omega & 1 \\
1 & 1 & 1 & 0 & 0 & \omega^2 & 1 & \omega & 1 & \omega & \omega^2 & 0 \\
\omega & 1 & 0 & \omega & \omega^2 & 0 & 1 & 0 & \omega^2 & 1 & 1 & 1
\end{bmatrix}$$

We close this section by generalizing real weighing matrices in a different direction. Up to this point we have only considered those matrices over some explicit group. We now consider the case when the entries are simply commuting indeterminants.

Definition. Let $\{x_i\}_{i=1}^s$ be real commuting indeterminants. An *orthogonal design* X is a square matrix of order n with entries from $\{0\} \cup \{\pm x_i\}_{i=1}^s$ such that $XX^t = (\sum s_i x_i^2)I$. We denote this as OD$(n; s_1, s_2, \ldots, s_\alpha)$, and we say that X is of type $(s_1, s_2, \ldots, s_\alpha)$.

We say that two matrices are amicable if $AB^t - BA^t = 0$; while they are anti-amicable if $AB^t + BA^t = 0$. From the definition it is clear that we can express an OD$(n; s_1, s_2, \ldots, s_\alpha)$ (say X) as $X = \sum x_i W_i$, where each W_i is a (0,1,-1)-matrix. Since $XX^t = (\sum s_i x_i^2)I$, we have that, for $i \neq j$, $W_i * W_j = 0$, $W_i W_j^t + W_j W_i^t = 0$, and $W_i W_i^t = s_i I$. Thus, the existence of an OD$(n; s_1, s_2, \ldots, s_\alpha)$ is equivalent to the existence of a set $\{W_i\}_{i=1}^{\alpha}$ (0,1,-1)-matrices satisfying the above properties.

The decomposition of an OD into a linear sum of weighing matrices is related to the early work of the analyst Radon. A *Hurwitz-Radon family of order n* is a set $\{W_i\}_{i=1}^{s}$ of square, skew-symmetric, mutually anti-amicable, orthogonal matrices of the same order n. Let $n = 2^a b$, where b is odd. Let $a = 4c + d$, for $0 \leq d < 4$. Define the *Radon arithmetic function* as $\rho(n) = 8c + 2^d$. Radon's main result is shown below.

Theorem 3.5. A Hurwitz-Radon family of order n can have at most $\rho(n)$ members; moreover, there is a family having $\rho(n) - 1$ members.

We have the following important result in the theory of orthogonal designs.

Theorem 3.6. For any positive integer n, there can be at most $\rho(n)$ indeterminants in any OD of order n; moreover, this bound is tight for every n.

The properties of amicability and anti-amicablility become fundamental in this context as well. If we have two amicable ODs X and Y of order n and of types $(s_1, s_2, \ldots, s_\alpha)$ and $(t_1, t_2, \ldots, t_\beta)$, respectively, then we say that the ordered pair (X, Y) is an amicable design, and we write (X, Y) is an AOD$(n; (s_1, s_2, \ldots, s_\alpha); (t_1, t_2, \ldots, t_\beta))$. Similarly, if X and Y are anti-amicable, then say that (X, Y) is an anti-amicable design, and we write AAOD$(n; (s_1, s_2, \ldots, s_\alpha); (t_1, t_2, \ldots, t_\beta))$.

Example 3.7. The following pairs (X_i, Y_i) constitute an AOD$(2; (1, 1); (1, 1))$ and an AOD$(4; (1, 1, 2); (1, 1, 2))$.

$$X_1 = \begin{bmatrix} a & b \\ \bar{b} & a \end{bmatrix} \qquad Y_1 = \begin{bmatrix} c & d \\ d & \bar{c} \end{bmatrix}$$

$$X_2 = \begin{bmatrix} a & b & c & c \\ \bar{b} & a & c & \bar{c} \\ c & c & \bar{a} & \bar{b} \\ c & \bar{c} & b & \bar{a} \end{bmatrix} \quad Y_2 = \begin{bmatrix} d & e & f & f \\ e & \bar{d} & f & \bar{f} \\ \bar{f} & f & e & d \\ \bar{f} & f & d & \bar{e} \end{bmatrix}$$

The example (X_1, Y_1) above will play a fundamental role in later chapters. Amicable designs have immediate constructive applications. The following result is instructive, and the proof follows by replacing the variables of a design with an amicable pair. The rest is a straightforward computation.

Proposition 3.8. If there exists an OD$(n; s_1, s_2)$, then:

i. there is an OD$(2n; s_1, s_2, s_2, s_2)$, and

ii. there is an OD$(4n; s_1, s_1, 2s_1, s_2, s_2, 2s_2)$.

We note that many of the above ideas can be obtained in a more general setting. By letting the coefficients of the non-zero entries of a design X instead come from the set $\{\pm 1, \pm i\}$, such that $XX^* = (\sum s_i x_i^2)I$, then we say that X is a *complex orthogonal design*. This is denoted as COD$(n; s_1, s_2, \ldots, s_\alpha)$.

We now have the appropriate framework to delve into the idea of *intra-positional balance* in the next section.

3.2 Intra-Positional Balance

Consider W_2 of Example 2.1. If we take $A = W_2 * W_2$, then we find that A is the incidence matrix of a BIBD(13,9,6). In the notation of the previous section, we see that the inner product between distinct rows evaluates to $\frac{6}{|G|}G$, where $G = \langle -1 \rangle$, the cyclic group of order 2 generated by -1. Similarly, the matrices of Examples 3.2 and 3.3 yield the incidence matrices of BIBDs when the non-zero entries are replaced with unity; however, the matrix of Example 3.4 does not.

Balanced incomplete block designs can best be described as having a kind of *inter-positional balance*. The examples of group matrices stated above are also balanced with respect to the group itself. This can best be thought of as a kind of *intra-positional balance*. The latter clearly imlpies the former, but the former does not by itself imply the latter. To capture this idea, we have the following definition.

Definition. Let G be a finite group. A *generalized Bhaskar Rao design* X is a $v \times b$ $(0,G)$-matrix such that every column contains k non-zero entries and $XX^* = rI + \frac{\lambda}{|G|}G(J - I)$, where λ is some multiple of $|G|$. We denote this as GBRD$(v, b, r, k, \lambda; G)$. A *quasi-GBRD* is defined in the same way except that $XX^* = rI + (\frac{\lambda}{|G|}G - 1_G)(J - I)$, and is denoted by quasi-GBRD$(v, b, r, k, \lambda; G)$.

From the definition, we see that every (quasi-)GBRD$(v, b, r, k, \lambda; G)$ gives a BIBD(v, b, r, k, λ) upon replacing the non-zero entries with unity; hence,

by Fischer's Inequality (Theorem 1.7), we see that $v \leq b$. The extremal case is again distinguished, and we call these balanced group matrices *balanced generalized weighing matrices*. These are denoted by $\mathrm{BGW}(v, k, \lambda; G)$. The case that $k = v - 1$ is called a *generalized conference matrix*. Finally, in the case that $v = k$, we call these *generalized Hadamard matrices*, and we denote these as $\mathrm{GH}(G, \lambda)$.

Example 3.9. A $\mathrm{GBRD}(5, 3, 3; Z_3)$.

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & \omega & \omega^2 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & \omega^2 & \omega & 0 & \omega & \omega^2 & 0 & 1 \\ 0 & 1 & 0 & \omega^2 & 0 & \omega & 1 & 0 & \omega & \omega \\ 0 & 0 & 1 & 0 & \omega^2 & \omega & 0 & \omega^2 & 1 & \omega^2 \end{bmatrix}$$

In what follows, we shall be primarily concerned with the extremal cases of Fischer's Inequality, that is, BGW matrices. If P and Q are monomial $(0,G)$-matrices, and if W is a BGW over G, then we say that PWQ and W are *monomially equivalent*. The following proposition justifies this notion.

Proposition 3.10. If W is a $\mathrm{BGW}(v, k, \lambda; G)$, and if P and Q are monomial $(0, G)$-matrices, then PWQ is a $\mathrm{BGW}(v, k, \lambda; G)$.

Proof. Let $W = [w_{ij}]$, and let $g \in G$. We have that $(w_{ij}g)(w_{hj}g)^{-1} = w_{ij}w_{hj}^{-1}$; whence WQ is a $\mathrm{BGW}(v, k, \lambda; G)$. Further, $(gw_{ij})(gw_{hj})^{-1} = g(w_{ij}w_{hj}^{-1})g^{-1}$. Since conjugation by g is an automorphism of G, it follows that every element of G appears $\lambda/|G|$ times in the Hermitian inner product between any two distinct rows of PW. We have shown that PWQ is as desired. *Q.E.D.*

We next consider the invariance of the property of being a BGW under homomorphic images.

Proposition 3.11. Let G and H be finite groups, and let $\varphi : \mathbb{Z}[G] \to \mathbb{Z}[H]$ be a ring homomorphism such that $\varphi(G) = H$. If $W = [w_{ij}]$ is a $\mathrm{BGW}(v, k, \lambda; G)$, then $W^\varphi = [\varphi(w_{ij})]$ is a $\mathrm{BGW}(v, k, \lambda; H)$.

Proof. It is sufficient to note that $\varphi(w_{ij})\varphi(w_{hj})^{-1} = \varphi(w_{ij}w_{hj}^{-1})$; whence, each element of H appears $\lambda/|H|$ times in the hermitian inner product between distinct rows of W^φ. *Q.E.D.*

Corollary 3.12. Let $W = [w_{ij}]$ be a $\mathrm{BGW}(v, k, \lambda; G)$. Then $\sum_{i=1}^{v} w_{ij}w_{ih}^{-1} = \sum_{g \in G} a_g g$, where $\sum a_g = \lambda$.

Proposition 3.13. Let W be a BGW$(v, k, \lambda; G)$. Then W^* is a BGW$(v, k, \lambda; G)$.

PROOF. Note that $WW^* \equiv kI$ modulo the ideal $\mathbb{Z}G$. Hence, if $\varphi : \mathbb{Z}[G] \to \mathbb{Z}[G]/\mathbb{Z}G$ is the natural ring homomorphism, we have that $W^\varphi(W^\varphi)^* = kI$. Therefore, $(W^\varphi)^{-1} = \frac{1}{k}(W^\varphi)^*$. We then have $(W^\varphi)^*W^\varphi = kI$; whence, $W^*W = kI + U$, where $U = [u_{ij}G]$ is a matrix over $\mathbb{Z}G$. Corollary 3.12 then implies that $u_{ii} = 0$ and that $u_{ij} = \lambda/|G|$, whenever $i \neq j$. It follows that $U = \lambda(J - I)/|G|$, and we have shown that W^* is as required. *Q.E.D.*

Corollary 3.14. Let W be a BGW$(v, k, \lambda; G)$, where G is a finite abelian group. Then W^μ and W^t are also BGW$(v, k, \lambda; G)$s, where μ is the group inversion operation of G.

PROOF. Since G is abelian, the inversion operation is a group automorphism; whence, W^μ is a BGW$(v, k, \lambda; G)$ by Proposition 3.11. Further, $(W^\mu)^* = W^t$, so W^t is a BGW$(v, k, \lambda; G)$ by the result. *Q.E.D.*

BGWs have proven to be elusive; there are only a few known infinite families of these matrices. In the following section, we will construct an important family of BGW matrices, the so-called classical parameter BGW matrices.

We close this section by extending the definitions of residual and derived designs of a symmetric BIBD to BGW matrices.

Definition. Let W be a BGW$(v, k, \lambda; G)$, for some finite group G. We may assume that W has the form

$$\begin{bmatrix} \mathbf{0} & A \\ \mathbf{j} & B \end{bmatrix}.$$

Note that A is a GBRD$(v - k, v - 1, k, k - \lambda, \lambda; G)$ and B is a quasi-GBRD$(k, v-1, k-1, \lambda, \lambda-1; G)$. We call A the *residual part* of W, and we call B the *derived part* of W. Any GBRD whose parameters satisfy $r = k+\lambda$ is call a *quasi-residual* GBRD, and any quasi-GBRD whose parameters satisfy $k = \lambda + 1$ is call a *quasi-derived* GBRD.

3.3 Classical Parameter BGW Matrices

We recall the definitions and notations of §2.3 regarding codes. If the alphabet $\mathcal{A}$ is a field, then we may regard $\mathcal{A}^n$ as a linear space. If C is a subspace of $\mathcal{A}^n$, then we say that C is a linear $[n, k]_q$-code, where $k = \dim C$, and where $q = |\mathcal{A}|$. For the remainder of this work, we will take $\mathcal{A} \equiv \mathbb{F}_q$.

By a *generator matrix* G of a linear $[n, k]_q$-code C, we mean a $k \times n$ matrix over $\mathbb{F}_q$, with linearly independent rows, such that C is the space of

all linear combinations of the rows of G, i.e. the rows of G form a basis for the code C. We introduce the following important linear code.

Definition. Let G be the matrix whose columns are distinct representatives of all one-dimensional subspaces of the linear space $\mathbb{F}_q^n$. The *simplex code* $S_n(q)$ is the linear $[v, n]_q$-code whose generator matrix is G, where $v = (q^n - 1)/(q - 1)$.

The following result is a characterization of simplex codes.

Theorem 3.15. Let q be a prime power, and let $v = (q^n - 1)/(q - 1)$, where $n \in \mathbb{Z}_{\geq 2}$. A linear $[v, n]_q$-code C is an $S_n(q)$ if and only if $wt(\mathbf{x}) = q^{n-1}$ for every non-zero codeword $\mathbf{x} \in C$.

PROOF. We first lay down some preliminaries. Let $\{\mathbf{x}_i\}_{i=1}^v$ be representatives of the distinct one-dimensional subspaces of C, and let these be the consecutive rows of the matrix $\Gamma = [\gamma_{ij}]$. We may assume that the first n rows of Γ form the generator matrix G of C. Take $\{\mathbf{y}_i\}_{i=1}^v$ to be the columns of Γ, and let $Y = \text{span}\{\mathbf{y}_i\}_{i=1}^v$. It follows that rank Γ = dim C = dim Y. Finally, let U_i be the hyperplane of $\mathbb{F}_q^v$ consisting of the strings with 0 for the i^{th} components.

To begin, assume that C is an $S_n(q)$. Then no two of the columns of G are proportional; hence, no two columns of Γ are proportional. Note that $Y \not\subseteq U_i$, for any i, for otherwise the string $\mathbf{x}_i = \mathbf{0}$, contradicting the construction of Γ. It follows that dim $Y \cap U_i = n - 1$ so that $Y \cap U_i$ has $(q^{n-1} - 1)/(q - 1)$ distinct one-dimensional subspaces. Then $wt(\mathbf{x}_i) = v - (q^{n-1} - 1)/(q - 1) = q^{n-1}$.

On the other hand, assume that C is a linear $[v, n]_q$-code such that $wt(\mathbf{x}) = q^{n-1}$ for every non-zero codeword $\mathbf{x} \in C$. Since C is linear, $d(\mathbf{x}_1, \mathbf{x}_2) = wt(\mathbf{x}_1 - \mathbf{x}_2) = q^{n-1}$ whenever $\mathbf{x}_1 \neq \mathbf{x}_2$. For $i \neq j$, if $Y \cap U_i = Y \cap U_j$, then $\mathbf{x}_i$ and $\mathbf{x}_j$ have zeros in the same $(q^{n-1} - 1)/(q - 1)$ positions. If $\gamma_{ik} \neq 0$, then $\gamma_{jk} \neq 0$; and $\gamma_{ik} = \alpha\gamma_{jk}$, for some $\alpha \in \mathbb{F}_q$. Clearly, then, $d(\mathbf{x}_i, \alpha\mathbf{x}_j) \leq q^{n-1} - 1$, which contradicts our assumption. Thus, $Y \cap U_i \neq Y \cap U_j$, and dim $Y \cap U_i \cap U_j = n - 2$. Therefore, there are $(q^{n-2} - 1)/(q - 1)$ positions in which $\mathbf{x}_i$ and $\mathbf{x}_j$ both have zeros. If we, for a moment, consider the non-zero entries to be unity, then we have the following configuration (after suitably permuting the columns)

$$\overbrace{\begin{array}{cccccccccccc} 1 & \dots & 1 & 1 & \dots & 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 1 & \dots & 1 & 0 & \dots & 0 & 1 & \dots & 1 & 0 & \dots & 0 \end{array}}^{\frac{q^n-1}{q-1}}$$

$$\underbrace{}_{x} \quad \underbrace{}_{\frac{q^{n-1}-1}{q-1}} \quad \underbrace{}_{\frac{q^{n-1}-1}{q-1}} \quad \underbrace{}_{\frac{q^{n-2}-1}{q-1}},$$

where $x = (q^n - 1)/(q - 1) - 2(q^{n-1} - 1)/(q - 1) + (q^{n-2} - 1)/(q - 1) = q^{n-1} - q^{n-2}$; whence, we have a symmetric design. Therefore, no two columns of Γ are poportional.

To conclude the proof, it suffices to show that no two rows of G are proportional. To the contrary, let $\{\mathbf{z}_i\}_{i=1}^{v}$ be the columns of G, and suppose that $\mathbf{z}_j = \alpha\mathbf{z}_k$, for some $\alpha \in \mathbb{F}_q$. Hence, $\gamma_{ij} = \alpha\gamma_{ik}$, for $i \leq n$. Since the $\{\mathbf{x}_i\}_{i=1}^{n}$ form a basis of C, we have that $\mathbf{x}_l = \sum_{i=1}^{n} \beta_i \mathbf{x}_i$, for some $\beta_i \in \mathbb{F}_q$. Then $\gamma_{lj} = \sum_{i=1}^{n} \beta_i\gamma_{ij} = \alpha \sum_{i=1}^{n} \beta_i\gamma_{ik} = \alpha\gamma_{lk}$. But then $\mathbf{y}_j = \alpha\mathbf{y}_k$, contrary to our assumptions. Therefore, no two rows of Γ are proportional so that no two rows of G are proportional. Therefore, C is a simplex code as desired. *Q.E.D.*

We are now ready to present the most prominent family of BGW matrices.

Theorem 3.16. Let q be a prime power, and let $n \in \mathbb{Z}_+$. If G is a cyclic group such that $|G|$ divides $q - 1$, then there is a BGW over G with parameters

$$\left(\frac{q^{n+1} - 1}{q - 1}, q^n, q^n - q^{n-1} \right). \tag{3.1}$$

Proof. Let $W = [w_{ij}]$ be the matrix whose rows consist of representatives from the one-dimensional subspaces of $S_{n+1}(q)$. Then W has order $v = (q^{n+1} - 1)/(q - 1)$. From Theorem 3.15, it follows that W has q^n non-zero entries in every row and column. By the same result, we have that the multiset $P_{ij} = \{w_{ik}w_{jk}^{-1} \mid 1 \leq k \leq v\}$ has $q^n - q^{n-1}$ entries. To complete the proof, we show that every element of the multiplicative subgroup of the field $\mathbb{F}_q$ appears precisely q^{n-1} times in P_{ij}. Indeed, assume that there is some $\alpha \in \mathbb{F}_q$ which appears more than q^{n-1} times in P_{ij}. Then there are more than $(q^{n-1} - 1)/(q - 1) + q^{n-1}$ indices k for which $w_{ik} = \alpha w_{jk}$. In this case, then,

$$wt(\mathbf{x}_i - \alpha\mathbf{x}_j) = d(\mathbf{x}_i, \alpha\mathbf{x}_j) = \frac{q^{n+1} - 1}{q - 1} - \frac{q^{n-1} - 1}{q - 1} - q^{n-1} = q^n,$$

which contradicts our assumptions; whence, each element of $\mathbb{F}_q^{\times}$ appears at most q^{n-1} times in P_{ij}. Now, since $|P_{ij}| = q^{n-1}(q - 1)$, it is clear that there are at most q^{n-1} replications of element of $\mathbb{F}_q^{\times}$. The remainder follows from Proposition 3.11. *Q.E.D.*

It is often helpful to have BGW matrices with additional structure. To this end, we introduce the ω-circulant matrices. By this, we mean a square matrix $A = [a_{ij}]$ of order n over the finite cyclic group $\langle\omega\rangle$ such that

$$a_{ij} = \begin{cases} a_{i-1,j-1} & \text{if } i, j > 1, \text{ and} \\ \omega a_{i-1,n} & \text{if } i > 1 \text{ and } j = 1. \end{cases}$$

It can be shown that an ω-circulant BGW matrix with parameters (3.1) exists for every prime power q and positive integer n. To be explicit, let N and Tr be the usual norm and trace functions $\mathbb{F}_{q^{n+1}} \to \mathbb{F}_q$. Let β be any primitive element of $\mathbb{F}_{q^{n+1}}$, and take $\omega = [N(\beta)]^{-1}$. Let W be the ω-circulant matrix with first row $(Tr\beta^0, Tr\beta, \ldots, Tr\beta^{v-1})$, where $v = (q^{n+1}-1)/(q-1)$. It can be shown that W is the required matrix. The proof of this result requires a detailed discussion of linear feedback shift register sequences and would take us too far afield. To reference this result, we record it below.

Theorem 3.17. Let q be a prime power, $n \in \mathbb{Z}_+$. If $G = \langle \omega^{-1} \rangle$ is a cyclic group whose order divides $q-1$, then there is an ω-circulant BGW matrix over G with parameters (3.1).

The matrices given in Examples 3.2 and 3.3 are ω-circulant BGWs where ω is given by -1 and $-i$, respectively. The base case of the classical parameters, that is, the generalized conference matrices with parameters $(q+1, q, q-1)$, deserve explicit description. First, we extend the notion of a skew-symmetric matrix. Let G be a finite abelian group with a unique normal subgroup $\langle \varepsilon \rangle$ of order two, and let W be a $(0, G)$-matrix. We say that W is skew-symmetric whenever $W^t = \varepsilon W$.

Proposition 3.18. Let q be a prime power, and let G be a cyclic group whose order n divides $q-1$. Then there exists a generalized conference matrix W of order $q+1$ over G. Moreover, if $q(q-1)/n$ is even, then W is symmetric; while if $(q-1)/n$ and $n \equiv 0 \bmod 2$, then W is skew-symmetric.

PROOF. This is essentially a generalization of Paley's construction 2.7. Let $\mathbb{F}_q = \{\alpha_1 = 0, \ldots, \alpha_q\}$, and let $C = [c_{ij}]$ be the matrix defined by $c_{ij} = \alpha_j - \alpha_i$. Then

$$W = [w_{ij}] = \begin{bmatrix} 0 & \mathbf{1} \\ -\mathbf{1} & C \end{bmatrix}$$

is seen to be a skew-symmetric generalized conference matrix over $\mathbb{F}_q^\times$ whenever q is odd, while W is symmetric if the field has characteristic 2. Note that the non-zero elements of W can be represented by β^j, for some primitive element β of $\mathbb{F}_q$ and $j \in \{0, 2, \ldots, q-2\}$. If $\langle \omega \rangle = G$, then we apply the epimorphism $\beta^j \mapsto \omega^{j \bmod n}$. The rest follows from Proposition 3.11. *Q.E.D.*

We close this section with a result on Generalized Hadamard matrices.

Proposition 3.19. For every prime power q, there exists a $\mathrm{GH}(\mathbb{F}_q^+, 1)$.

PROOF. Let $\mathbb{F}_q = \{\alpha_1, \alpha_2, \ldots, \alpha_q\}$, and let $H = [h_{ij}]$ be the matrix defined by $h_{ij} = \alpha_i \alpha_j$. Since the multiset $\{\alpha_i \alpha_k - \alpha_j \alpha_k\}$ is the group $\mathbb{F}_q^+$, we are done. *Q.E.D.*

3.4 Notes

Balanced generalized weighing matrices have been studied by many different authors, in many different contexts. The first person studying these topics appears to have been Delsarte [Del68]. Generalized Hadamard matrices were pursued by Drake in [Dra79]. Rajkundlia studied these structures and BGWs in [Raj83]. Tonchev [Ton09] studied the conections of BGW and GH matrices with self-dual codes and perfect quantum error-correcting codes. Unit weighing matrices appear in the study of quantum informatics (see Durt *et al*[DEBŻ10]) and signal processing (see Adams *et al* [AKP07]). Butson matrices were studied in Butson [But62, But63], Shrikhande [Shr64], and Berman [Ber78]. The monograph Seberry [Seb17] is the standard monograph on orthogonal designs.

Radon's result given here is shown in [Rad22], and Hurwitz extended this result in [Hur22]. The Theorems 3.6 and 3.8 are obtained from [Seb17]. The results listed in §§ 3.2 and 3.3, as shown, are taken from Ionin,Shrikhande [IS06]. Classical parameter BGW matrices were obtained initially in [Ber78]. The construction given here, using simplex codes and registers, are due to Jungnickel, Tonchev [JT99, JT02]. Valuable discussion of BGW matrices an their connections to other combinatorial objects can be found in Jungnickel, Kharaghani [JK04].

Part II

Constructions

Chapter 4

The Kronecker Product

4.1 Definitions and Properties

The Kronecker Product is a kind of matrix multiplication that produces a block matrix from two smaller matrices. We define the product thus.

Definition. Let R be any ring. The *Kronecker Product* is a map $\otimes : {}^nR^m \times {}^sR^t \to {}^{ns}R^{mt}$ defined as follows. If $A = [a_{ij}] \in {}^nR^m$ and $B \in {}^sR^t$, then $A \otimes B = [a_{ij}B]$.

Example 4.1. It is expected that the product is not commutative. Indeed, if $H = \left[\begin{smallmatrix} 1 & 1 \\ 1 & - \end{smallmatrix}\right]$ and $K = \left[\begin{smallmatrix} 1 & 1 \\ - & 1 \end{smallmatrix}\right]$, then

$$H \otimes K = \begin{bmatrix} 1 & 1 & 1 & 1 \\ - & 1 & - & 1 \\ 1 & 1 & - & - \\ - & 1 & 1 & - \end{bmatrix}, \text{ and}$$

$$K \otimes H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ - & - & 1 & 1 \\ - & 1 & 1 & - \end{bmatrix}.$$

The following properties are readily established.

Proposition 4.2. Let A, B, C, and D be matrices over a commutative ring such that the following operations of addition and multiplication are defined. Then:

i. $(A \otimes B) \otimes C = A \otimes (B \otimes C)$;

ii. $(A + B) \otimes C = A \otimes C + B \otimes C$ and $A \otimes (B + C) = A \otimes B + A \otimes C$;

iii. $(rA) \otimes B = A \otimes (rB) = r(A \otimes B)$, for any scalar r; and

iv. $(A \otimes B)(C \otimes D) = AC \otimes BD$.

Using the Kronecker Product, we see that Paley's result 2.7 for prime powers $q \equiv 1 \bmod 4$, can be stated as

$$H = W_1 \otimes \begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix} + I \otimes \begin{bmatrix} 1 & - \\ - & - \end{bmatrix}$$

is a Hadamard matrix of order $2(q+1)$, where W_1 is an in the proof of Theorem 2.7. We can, in fact, be more general.

Lemma 4.3. Let S be a matrix of order n such that $S^t = \varepsilon S$, $\varepsilon = \pm 1$, and $SS^t = (n-1)I$. Let A and B be matrices of order m such that $AA^t = BB^t = mI$ and $AB^t = -\varepsilon BA^t$. Then for $K = A \otimes I + B \otimes S$, we have that $KK^t = mnI$.

PROOF. This follows by straight forward computation. Observe:

$$\begin{aligned} KK^t &= (A \otimes I + B \otimes S)(A^t \otimes I + B^t \otimes S^t)^t \\ &= AA^t \otimes I_n + AB^t \otimes S^t + BA^t \otimes S + BB^t \otimes SS^t \\ &= mI_m \otimes I_n + (-\varepsilon BA^t) \otimes (\varepsilon S) + BA^t \otimes S + mI_m \otimes (n-1)I_n \\ &= mI_{mn} + m(n-1)I_{mn} \\ &= mnI_{mn}, \end{aligned}$$

and the result is complete. *Q.E.D.*

Proposition 4.4. If $q \equiv 1 \bmod 4$, and if n is the order of a Hadamard matrix, then there is a Hadamard matrix of order $n(q+1)$.

PROOF. Let $q \equiv 1 \bmod 4$ be a prime power. We have shown already that there is a conference matrix of order $q+1$, say W. Let H be a Hadamard matrix of order n. Define $U = I_{n/2} \otimes \left[\begin{smallmatrix} 0 & 1 \\ - & 0 \end{smallmatrix}\right]$ and $K = UH$. Observe:

$$\begin{aligned} KK^t &= nI_n, \\ HK^t &= -nU, \text{ and} \\ KH^t &= nU. \end{aligned}$$

Then W, H, and K satisfy the conditions of the previous lemma. *Q.E.D.*

The Kronecker product can be generalized in the following way. Let B be some matrix over an arbitrary ring, and let $A = [a_{ij}]$ be a matrix over some group acting on the rows, columns, or entries of A. Then $A \otimes B = [a_{ij}B]$, where $a_{ij}B$ denotes the action of a_{ij} on B. We pursue this further in the following section.

4.2 Structurally Interesting BGW Matrices

In order to apply the Kronecker product to the construction of BGW matrices, we will need to employ specific groups acting on the smaller blocks. To this end, we introduce the so-called *groups of symmetries*.

Definition. Let G be some finite group, and let $\mathcal{M}$ be a non-empty set of $(0, G)$-matrices of the same size. A set S of bijections $\mathcal{M} \to \mathcal{M}$ will be called a *group of symmetries* if the following are satisfied.

i. $(\sigma X)(\sigma Y)^* = XY^*$, for every $\sigma \in S$ and $X, Y \in \mathcal{M}$, and

ii. for every $X \in \mathcal{M}$, there is a $g \in \mathbb{Z}[G]$ such that $\sum_\sigma \sigma X = gJ$.

In general, it is difficult to find groups of symmetries; however, there are some simple, useful examples. For instance, any transitive group acting on the columns of a matrix is easily seen to be a group of symmetries for any set of $(0, G)$-matrices (say $\mathcal{M}$) such that $XJ = gJ$, for $X \in \mathcal{M}$ and some $g \in \mathbb{Z}G$. If the group G is cyclic, then we can be more general.

Proposition 4.5. Let $G = \langle \omega \rangle$ be a cyclic group, and let $\mathcal{M}$ be the set of all BGW$(v, k, \lambda; G)$ matrices. Let ϱ be the ω-circulant matrix of order v with first row $(0, 1, 0, \ldots, 0)$. Then $S = \langle \varrho \rangle$ is a group of symmetries of $\mathcal{M}$ when acting on the right by multiplication.

Proof. Let $X, Y \in \mathcal{M}$. Clearly, then, $(X\varrho^k)(Y\varrho^k)^* = X\varrho^k(\varrho^k)^*Y^* = XY^*$. Since $|\varrho| = v|\omega|$, we see that

$$\sum_{i=0}^{v|\omega|-1} X\varrho^k = \sum_{i=0}^{v-1}\sum_{j=0}^{|\omega|-1} (X\varrho^i)\omega^j = \sum_{i=0}^{v-1}(X\varrho^i)G = kGJ.$$

It follows that S is a group of symmetries of $\mathcal{M}$. *Q.E.D.*

Before moving on, we provide one further simple example of a group of symmetries in the case of GH matrices.

Proposition 4.6. Let G and S be finite groups, and let $\mathcal{M}$ be the set of GH$(G; \lambda)$, for some $\lambda > 0$. Let $f : S \to G$ be an epimorphism, and for each $\sigma \in S$, define $\sigma X = Xf(\sigma)$. Then S is a group of symmetries of $\mathcal{M}$.

Proof. By simple calculation, we have that $(\sigma X)(\sigma Y)^* = Xf(\sigma)f^*(\sigma)Y^* = XY^*$ and $\sum_\sigma \sigma X = X\sum_\sigma f(\sigma) = |S|XG/|G| = |S|GJ/|G|$; hence, S is as claimed. *Q.E.D.*

Usually, if the objects to which we are applying the group of symmetries have particular parameters associated to them, then a successful application

of the group is predicated on particular parametric conditions. An important example for us is the application of groups of symmetries to GBRD matrices.

Theorem 4.7. Let $\mathcal{M}$ be the set of GBRD$(v, b, r, k, \lambda; G)$s over some finite group G, and let $X \in \mathcal{M}$. Further, let S be a group of symmetries of $\mathcal{M}$ such that $\alpha_X = \alpha G$, for $\alpha \in \mathbb{Z}_+$ and every $X \in \mathcal{M}$. If there is a BGW$(w, l, \mu; S)$ such that $kr\mu = v\lambda l$ (say $W = [w_{ij}]$), then the block matrix $W \otimes X$ is a GBRD$(vw, bw, rl, kl, \lambda l; G)$.

Proof. Define $P_{ij} = \sum_{h=1}^{w}(w_{ih}X)(w_{jh}X)^*$. Then, if $\sigma_1, \sigma_2, \ldots \sigma_l \in S$, we have

$$\begin{aligned} P_{ii} &= \sum_{h=1}^{w}(w_{ih}X)(x_{ih}X)^* \\ &= \sum_{h=1}^{l}(\sigma_h X)(\sigma_h X)^* \\ &= \sum_{h=1}^{l} XX^* \\ &= rlI + \frac{\lambda l}{|G|}G(J - I). \end{aligned}$$

In the case that $i \neq j$, we have

$$\begin{aligned} P_{ij} &= \sum_{h=1}^{w}(w_{ih}X)(w_{jh}X)^* \\ &= \sum_{h=1}^{w}(w_{jh}^{-1}w_{ih}X)X^* \\ &= \frac{\mu}{|S|}\left(\sum_{\sigma}\sigma X\right)X^* \\ &= \frac{\mu\alpha}{|S|}GJX^* \\ &= \frac{\mu\alpha r}{|S|}GJ. \end{aligned}$$

Now, multiply both sides of $\sum_\sigma \sigma X = \alpha GJ$ on the left by GJ^t to obtain

$$\begin{aligned} \sum_{\sigma} GJ^t(\sigma X) &= \alpha(GJ^t)(GJ) \\ \sum_{\sigma} kGJ_b &= \alpha v|G|GJ_b \\ k|S|GJ_b &= \alpha v|G|GJ_b. \end{aligned}$$

Therefore, $\alpha = \frac{k|S|}{v|G|}$, and $\frac{\mu\alpha r}{|S|} = \frac{\mu k r}{v|G|} = \frac{\lambda l}{|G|}$. *Q.E.D.*

We have shown already the existence of a $\mathrm{GH}(q, 1)$ whenever q is a prime power. The identity automorphism satisfies the conditions of Proposition 4.6, so by the previous Theorem, we have the following.

Corollary 4.8. Let q be a prime power. For every positive n, there is a $\mathrm{GH}(q, q^{n-1})$.

We are now ready to construct families of BGW matrices over cyclic groups with classical parameters such that the matrix is either skew-symmetric or symmetric, given particular parametric conditions. These will be of fundamental use in the construction of new orthogonal designs.

Theorem 4.9. Let $G = \langle\omega\rangle$ be a cyclic group of order g, and let q be a prime power such that g divides $q - 1$. For every positive integer n, there exists a BGW over G with parameters

$$\left(\frac{q^{2n} - 1}{q - 1}, q^{2n-1}, q^{2n-1} - q^{2n-2}\right). \tag{4.1}$$

Moreover, if $q(q-1)/g \equiv 0 \bmod 2$, then the BGW is symmetric with zero diagonal; while if $g \equiv 0 \bmod 2$ and $(q-1)/g \equiv 1 \bmod 2$, then the BGW is skew-symmetric.

Proof. Proposition 3.18 provides the base case for the result. Now, let $v = (q^{n+1} - 1)/(q - 1)$, let $k = q^n$, and let $\lambda = q^n - q^{n-1}$. Let $\mathcal{M}$ be the set of all ω-circulant $\mathrm{BGW}(v, k, \lambda; G)$s, and let R be the back identity matrix. For any $X \in \mathcal{M}$, we have that XR is back ω-circulant, symmetric BGW with the same parameters. Let $\mathcal{M}' = \{XR \mid X \in \mathcal{M}\}$, and let $S = \langle\varrho\rangle$ be the group of symmetries generated by the ω-shift matrix given in Proposition 4.5. We now show the general case.

First, suppose that $q(q-1)/g$ is even. Since $q^{n+1} - 1$ is a multiple of gv, and since $q^{n+1}(q^{n+1} - 1)/gv$ is even, we have, by Proposition 3.18, there is a symmetric generalized conference matrix (say W) over S of order $q^{n+1} - 1$. Let $X \in \mathcal{M}'$. By Theorem 4.7, $W \otimes X$, is a BGW with the required parameters, as since both W and X are symmetric, it follows that $W \otimes X$ is symmetric with zero diagonal.

Suppose now that $(q-1)/g$ is odd and q is even. Then G is signable with unique element of order two given by $\omega^{\frac{n}{2}}$. Again, using Proposition 3.18, since $q^{n+1} - 1$ is a multiple of gv, and since gv is even while $(q^{n+1} - 1)/gv$ is odd, there is a skew-symmetric generalized conference matrix (say W) over S of order q^{n+1}. Let $X \in \mathcal{M}'$; then $W \otimes X$ is a BGW with the required parameters. By construction, $\varrho^{\frac{n}{2}} = \omega^{\frac{n}{2}} I$; whence, $(W \otimes X)^t = W^t \otimes X^t = \varrho^{\frac{n}{2}} W \otimes X = \omega^{\frac{n}{2}}(W \otimes X)$. This completes the proof. *Q.E.D.*

Example 4.10. Define the following weighing matrices.

$$W = \begin{bmatrix} 0&1&1&1&1&1&1&1&1&1 \\ 1&0&-&1&-&1&-&1&-&1 \\ 1&-&0&1&1&1&-&-&1&- \\ 1&1&1&0&-&-&-&1&1&- \\ 1&-&1&-&0&1&1&1&-&- \\ 1&1&1&-&1&0&-&-&-&1 \\ 1&-&-&-&1&-&0&1&1&1 \\ 1&1&-&1&1&-&1&0&-&- \\ 1&-&1&1&-&-&1&-&0&1 \\ 1&1&-&-&-&1&1&-&1&0 \end{bmatrix}, \text{ and}$$

$$X = \begin{bmatrix} 1&0&1&- \\ 0&1&-&- \\ 1&-&-&0 \\ -&-&0&- \end{bmatrix}.$$

Then W is a symmetric conference matrix, and X is a back (-1)-circulant conference matrix. It follows that the matrix $W \otimes X$, shown below, is a symmetrix $\mathrm{W}(40, 27)$ with zero diagonal that is also balanced.

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

4.3 Applications to BIBDs and GBRDs

In this section we will apply BGW matrices to the construction of BIBDs and GBRDs using the Kronecker product. To begin, we note that in the case of classical parameter BGW matrices and quasi-residual designs, the parametric condition of Theorem 4.7 reduces to $q = r$. It remains to find quasi-residual designs with an applicable group of symmytries. We will initially turn to resolvability.

To begin, note that if one has a resolvable BIBD, then one may cyclically permute the blocks of each resolution class. The group just defined has order the least common multiple of the cardinalities of the resolution classes. Since this group is a cyclic group acting on the columns of a BIBD, it follows that it is a group of symmetries for the set of all such designs. Moreover, if r is a prime power, and if the least common multiple of the cardinalities of the resolution classes of the design divides $r-1$, then there is a BGW with classical parameteres over the above group. In this way, we can apply the construction of the previous section with the trivial group to obtain a class of larger BIBDs.

The above discussion is sufficient for the following result.

Theorem 4.11. Suppose the existence of a quasi-residual BIBD(v, b, r, k, λ) admitting a resolution such that the cardinality of each resolution class divides $r-1$. If r is a prime power, then there is a quasi-residual design with parameters

$$\left(\frac{v(r^n-1)}{r-1}, \frac{b(r^n-1)}{r-1}, r^n, kr^{n-1}, \lambda r^{n-1}\right),$$

for every $n > 1$.

Corollary 4.12. Let q be a prime power, and let $n > 1$. If $r = (q^n-1)/(q-1)$ is a prime power, then there is a quasi-residual design with parameters

$$\left(\frac{q^n(r^m-1)}{r-1}, \frac{qr(r^m-1)}{r-1}, r^m, q^{n-1}r^{m-1}, \frac{(q^{n-1}-1)r^{m-1}}{q-1}\right),$$

for every $m > 1$.

Proof. It is well known that every $\mathrm{AG}_{n-1}(n, q)$ is affine resolvable. We remind the reader that the parameters of $\mathrm{AG}_{n-1}(n, q)$ are given by

$$\left(q^n, \frac{q(q^n-1)}{q-1}, \frac{q^n-1}{q-1}, q^{n-1}, \frac{q^{n-1}-1}{q-1}\right);$$

whence, by Theorem 1.14, we have that the cardinality of each resolution class is q. Let G be the cyclic group of order q acting on the resolution

classes of $\mathrm{AG}_{n-1}(n,q)$. By assumption, $r = (q^n-1)/(q-1)$ is a prime power, and moreover, since $r-1 = \sum_{i=1}^{n-1} q^i$, we have that q divides $r-1$; therefore, there is a $\mathrm{BGW}((r^m-1)/(r-1), r^{m-1}, r^{m-1}-r^{m-2}; G)$, for every $m > 1$ (say W). If X is the incidence matrix of $\mathrm{AG}_{n-1}(n,q)$, then $W \otimes X$ is the required design. *Q.E.D.*

Note that we may assume the columns of $\mathrm{AG}_{n-1}(n,q)$ are partitioned into the resolution classes, each of size q. If g is the circulant matrix of order q with first row $(0,1,0,\ldots,0)$, then define $\varrho = I_r \otimes g$, with $r = (q^n-1)/(q-1)$. We may then take $G = \langle \varrho \rangle$ in the above construction. This idea will be important for what is to follow. For the moment, however, we will move on to develop a group of symmetries for another family of designs.

Consider the quasi-residual block designs with the parameters

$$\left(r+1, 2r, r, \frac{r+1}{2}, \frac{r-1}{2} \right). \tag{4.2}$$

Let X be the incidence matrix of one such design. Then $J-X$ has the same parameters. Take $\mathcal{M} = \{X, J-X\}$, and let $\sigma Y = J - Y$, for each $Y \in \mathcal{M}$. Since the parameters are invariant under complementation, we have that $(\sigma Y)(\sigma Y)^t = YY^t$. Also, $Y(J-Y)^t = \frac{r+1}{2}(J-I) = (J-Y)Y^t$. Therefore, $(\sigma Y)(\sigma Z)^t = YZ^t$ for every $Y, Z \in \mathcal{M}$. Finally, $Y + (J-Y) = J$; whence, we have shown that $\langle \sigma \rangle$ is a group of symmetries on $\mathcal{M}$. We then have the following result.

Theorem 4.13. If there is a BIBD with parameters (4.2) such that r is an odd prime power, then there is a BIBD with parameters

$$\left(\frac{(r+1)(r^n-1)}{r-1}, \frac{2r(r^n-1)}{r-1}, r^n, \frac{(r+1)r^{n-1}}{2}, \frac{(r-1)r^{m-1}}{2} \right).$$

A Hadamard matrix of order $4n$ is equivalent to the existence of a symmetric $\mathrm{BIBD}(4n-1, 2n-1, n-1)$. The residuals of these designs have the parameters (4.2), with $r = 2n-1$. Particular families of Hadamard matrices are readily applicable to the construction.

Corollary 4.14. Let q be any odd prime power. Then there is a BIBD with the parameters

$$\left(\frac{(q+1)(q^n-1)}{q-1}, \frac{2q(q^n-1)}{q-1}, q^n, \frac{q^{n-1}(q+1)}{2}, \frac{q^{n-1}(q-1)}{2} \right),$$

for every $n > 0$.

PROOF. The constructions of Paley and Sylvester, together with Proposition 4.4, imply the existence of a Hadamard matrix of order $2(q+1)$, whenever

q is an odd prime power. These are equivalent to symmetric BIBD$(2q+1, q, (q-1)/2)$s, whose residual designs have the parameters

$$\left(q+1, 2q, q, \frac{q+1}{2}, \frac{q-1}{2}\right).$$

Apply the result to these designs. *Q.E.D.*

Corollary 4.15. Let $q \equiv -1 \bmod 4$ such that $r = (q-1)/2$ is an odd prime power. Then there is a BIBD with the parameters

$$\left(\frac{(q+1)(r^n-1)}{2(r-1)}, \frac{(q-1)(r^n-1)}{r-1}, \frac{(q-1)r^{n-1}}{2}, \frac{(q+1)r^{n-1}}{4}, \frac{(q-3)r^{n-1}}{4}\right),$$

for every $n > 0$.

Proof. By Theorem 2.7, there is a Hadamard matrix of order $q+1$ whenever $q \equiv -1 \bmod 4$ is a prime power. These are equivalent to the existence of symmetric BIBD$(q, (q-1)/2, (q-3)/4)$s, whose residual designs have parameters

$$\left(\frac{q+1}{2}, q-1, \frac{q-1}{2}, \frac{q+1}{4}, \frac{q-3}{4}\right).$$

We apply the result to these designs. *Q.E.D.*

At this point, it is natural to ask whether or not the quasi-residual designs constructed in this section are, in fact, embeddable. The following construction answers this question in the affirmative, at least in the case of those constructed from affine geometries.

Theorem 4.16. Let q and $p = q+1$ be prime powers, and let $n > 1$. Then there is a symmetric BIBD$(p(p^n-1)+1, p^n, p^{n-1})$.

Proof. Let A be the incidence matrix for the $\mathrm{AG}_1(2, q)$. Since $p = q+1$ is a prime power, there is a BGW$((p^n-1)/(p-1), p^{n-1}, p^{n-1}-p^{n-2})$, for $n > 1$, over the cyclic group acting on the parallel classes of A, say $W = [w_{ij}]$. Then $W \otimes A$ is a quasi-residual BIBD with parameters

$$\left((p-1)(p^n-1), p(p^n-1), p^n, p^{n-1}(p-1), p^{n-1}\right).$$

Let B be the incidence matrix of $\mathrm{AG}_{n-1}(n, p)$. Then $B \otimes \mathbf{j}_q^t$ is a BIBD with parameters

$$\left(p^n, p(p^n-1), p^n-1, p^{n-1}, p^{n-1}-1\right).$$

We claim that

$$\begin{bmatrix} \mathbf{0} & W \otimes A \\ \mathbf{j} & B \otimes \mathbf{j}_q^t \end{bmatrix}$$

is the required design. Note that it suffices to show that $(W \otimes A)(B \otimes \mathbf{j}_q^t)^t = p^{n-1}J$. To this end, we assume that B is partitioned into its parallel classes as $B = [B_1, B_2, \ldots, B_k]$, where $k = (p^n - 1)/(p - 1)$; and moreover, the entry decomposition of each parallel class will be given as $B_i = [b_{uv}^{(i)}]$. Since, for every u, there is precisely one v such that $b_{uv}^{(i)} = 1$, we have that $(w_{st}A)(B_i \otimes \mathbf{j}_q^t)^t = J$ after noting that the parallel classes of $w_{st}A$ are positioned above the block columns of $B_i \otimes \mathbf{j}_q^t$. There are p^{n-1} non-zero blocks in every row of W; whence, $(W \otimes A)(B \otimes \mathbf{j}_q^t)^t = p^{n-1}J$. *Q.E.D.*

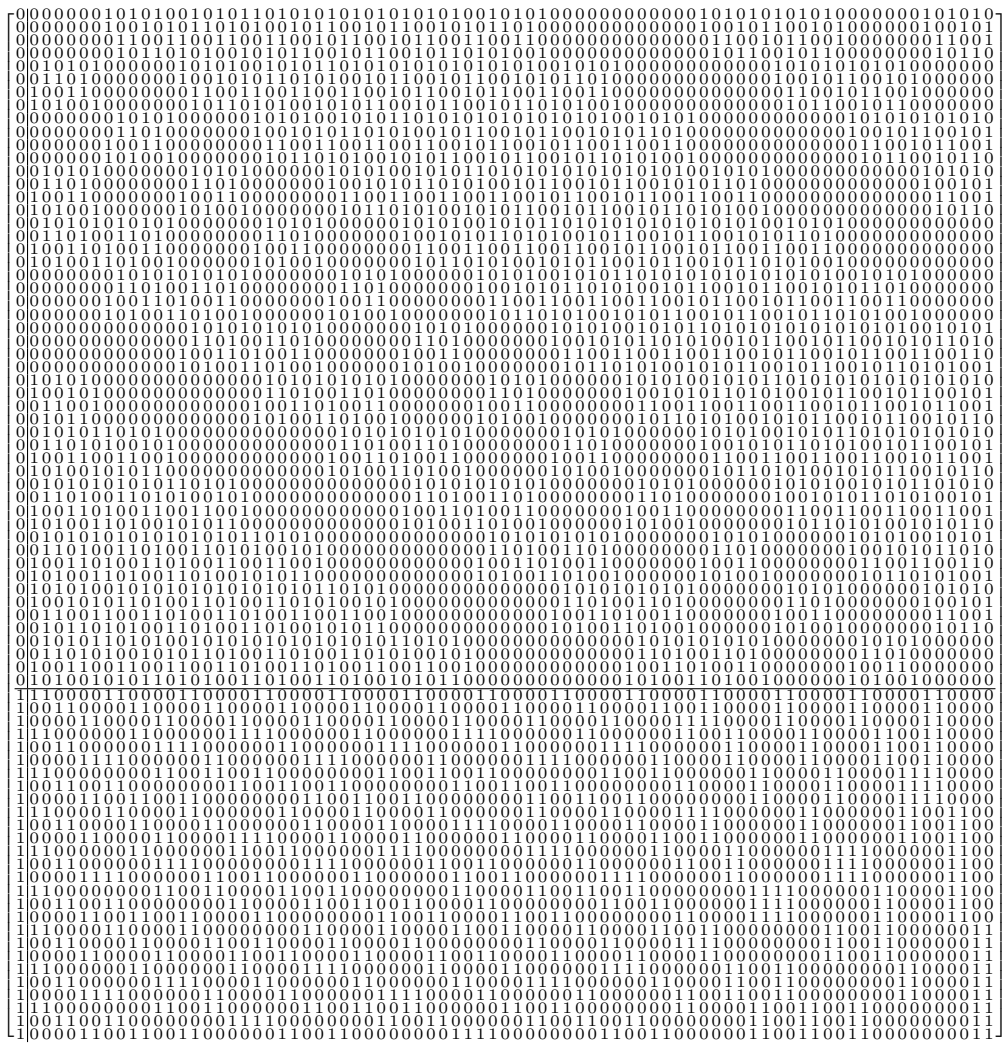
Example 4.17. An $\mathrm{AG}_1(2, 2)$

$$\begin{bmatrix} 1\,0\,1\,0\,1\,0 \\ 1\,0\,0\,1\,0\,1 \\ 0\,1\,1\,0\,0\,1 \\ 0\,1\,0\,1\,1\,0 \end{bmatrix},$$

and an $\mathrm{AG}_2(3, 3)$

$$\begin{bmatrix}
1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0 \\
0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0 \\
0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0 \\
1\,0\,0\,0\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0\,1\,0\,0\,1\,0\,0\,1\,0\,1\,0\,0 \\
0\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,1\,0\,1\,0\,0 \\
0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,1\,0\,0 \\
1\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0 \\
0\,1\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,0\,0\,0\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0 \\
0\,0\,1\,0\,1\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,0\,0\,0\,1\,0\,0\,1\,1\,0\,0 \\
1\,0\,0\,1\,0\,0\,1\,0\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,0\,1\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,1\,0 \\
0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,0\,1\,0\,0\,1\,1\,0\,0\,1\,0\,0\,1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,1\,0 \\
0\,0\,1\,0\,0\,1\,0\,0\,1\,1\,0\,0\,1\,0\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,1\,0 \\
1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0 \\
0\,1\,0\,0\,0\,1\,1\,0\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0 \\
0\,0\,1\,1\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,1\,1\,0\,0\,0\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0 \\
1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,1\,0 \\
0\,1\,0\,1\,0\,0\,0\,0\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,1\,0 \\
0\,0\,1\,0\,1\,0\,1\,0\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,1\,0 \\
1\,0\,0\,1\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1 \\
0\,1\,0\,0\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,1\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1 \\
0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1 \\
1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0\,1\,0\,0\,0\,0\,1 \\
0\,1\,0\,0\,0\,1\,1\,0\,0\,1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,1\,0\,1\,0\,0\,0\,0\,1 \\
0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,1\,1\,0\,0\,1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,1\,0\,1\,0\,0\,0\,0\,1 \\
1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,0\,1\,0\,0\,0\,0\,1\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,0\,1\,0\,1\,0\,0\,0\,0\,1 \\
0\,1\,0\,1\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,0\,0\,0\,1 \\
0\,0\,1\,0\,1\,0\,1\,0\,0\,0\,1\,0\,1\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,0\,1\,0\,1\,0\,0\,0\,0\,1
\end{bmatrix}.$$

Using a BGW(13,9,6;Z_2), we construct a symmetric BIBD(79,27,9).



The constructions of the section are given to include those designs that have intra-positional balance, namely, generalized Bhaskar Rao designs. To employ these constructions to obtain a novel famly of GBRD matrices, we give an important example.

Example 4.18. A BGW(15,7,3;Z_3).

$$\begin{bmatrix}
3&3&1&0&2&0&0&0&3&2&0&1&0&0&0\\
3&0&3&1&0&2&0&0&0&3&2&0&1&0&0\\
3&0&0&3&1&0&2&0&0&0&3&2&0&1&0\\
3&0&0&0&3&1&0&2&0&0&0&3&2&0&1\\
3&2&0&0&0&3&1&0&1&0&0&0&3&2&0\\
3&0&2&0&0&0&3&1&0&1&0&0&0&3&2\\
3&1&0&2&0&0&0&3&2&0&1&0&0&0&3\\
0&3&3&3&3&3&3&3&0&0&0&0&0&0&0\\
0&3&2&0&1&0&0&0&0&0&2&0&2&2&3\\
0&0&3&2&0&1&0&0&3&0&0&2&0&2&2\\
0&0&0&3&2&0&1&0&2&3&0&0&2&0&2\\
0&0&0&0&3&2&0&1&2&2&3&0&0&2&0\\
0&1&0&0&0&3&2&0&0&2&2&3&0&0&2\\
0&0&1&0&0&0&3&2&2&0&2&2&3&0&0\\
0&2&0&1&0&0&0&3&0&2&0&2&2&3&0
\end{bmatrix}.$$

The residual part of this matrix is a GBRD(8,14,7,4,3;Z_3) shown below.

$$A = \begin{bmatrix}
3&3&3&3&3&3&3&0&0&0&0&0&0&0\\
3&2&0&1&0&0&0&0&0&2&0&2&2&3\\
0&3&2&0&1&0&0&3&0&0&2&0&2&2\\
0&0&3&2&0&1&0&2&3&0&0&2&0&2\\
0&0&0&3&2&0&1&2&2&3&0&0&2&0\\
1&0&0&0&3&2&0&0&2&2&3&0&0&2\\
0&1&0&0&0&3&2&2&0&2&2&3&0&0\\
2&0&1&0&0&0&3&0&2&0&2&2&3&0
\end{bmatrix}.$$

Note that the residual GBRD A has the form

$$\begin{bmatrix} 3 & \dots & 3 & 0 & \dots & 0 \\ & A_1 & & & A_2 & \end{bmatrix},$$

where $A_1 = J - A_2$ after changing the non-zero entries to unity. If $Z_3 = \langle\omega\rangle$, then we define $G = \langle \left[\begin{smallmatrix} 0 & 1 \\ \omega & 0 \end{smallmatrix}\right] \otimes R_7 \rangle$, where R_7 is the back identity matrix of order seven. In much the same way as before, one sees that G is a group of symmetries on the orbit of A under the action of its generator. Since $|G| = 6$, and since the replication number of A is seven, we have shown the following.

Proposition 4.19. Let $n > 1$. There is a quasi-residual GBRD over Z_3 with parameters

$$\left(\frac{4}{3}(7^n - 1), \frac{7}{3}(7^n - 1), 7^n, 4 \cdot 7^{n-1}, 3 \cdot 7^{n-1}\right).$$

PROOF. Form the matrix $W \otimes A$, where W is a BGW$((7^n-1)/6, 7^{n-1}, 7^{n-1}-7^{n-2}; G)$. *Q.E.D.*

Of course, there is still the question of the embeddability of the family of GBRDs just given. Evidently, they are not embedabble by any of the standard methods. Thus, we see that the added condition of intra-positional balance forces these objects to be much more difficult to work with.

4.4 Notes

The Kronecker product is an important function of linear algebra, and so, it appears quite naturally in the theory of combinatorial matrices. Paley [Pal33] used this product quite successfully, as we've already seen. Lemma 4.3 and Proposition 4.4 are generalizations of Paley's constructions and appear in Hall [Hal86].

The symmetric BGW matrices with zero diagonal constructed in §4.2 first appeared in Kharaghani [Kha03]. Ionin, Kharaghani[IK03b] used these symmetric BGW matrices to construct new families of strongly regular graphs (see Ionin, Shrikhande[IS06] and Brouwer *et al* [BCN89]). The skew-symmetric BGW matrices of the same section appeared in Ionin, Kharaghani [IK03a], where they were used to construct new families of the so-called doubly regular, asymmetric digraphs. The presentation given here is taken from [IS06]. Theorem 4.7 is a generalization of that given in Ionin [Ion01, IS06].

Theorems 4.11 and 4.13 and their corollaries first appeared in [Ion01], and they are addressed in [IS06] in greater detail. Theorem 4.16 presents a novel construction of the Rajkundlia designs [Raj83], which are also contained in the larger class of Ionin type designs found in [Ion01]. The generalized Bhaskar Rao designs of Proposition 4.19 appear to be new.

Chapter 5

Hadamard Matrices

5.1 Quaternary Unit Hadamard Matrices

Recall that a unit Hadamard matrix is a matrix of order n (say H) with unimodular complex entries such that $HH^* = nI$. In Chapter 2 we considered several subsets of such matrices, that is, those whose entries are roots of unity. In this section, we will focus on another subset of unit Hadamard matrices, namely, those matrices satisfying the equation $HH^* = nI$, whose entries are from the field extension $\mathbb{Q}[\sqrt{q}, \sqrt{q+1}, i]$.

Definition. Let H be a square matrix of order n, with entries from the set $\left\{\frac{\pm 1 \pm i\sqrt{m}}{\sqrt{m+1}}, \frac{\pm i \pm \sqrt{m}}{\sqrt{m+1}}\right\}$, such that $HH^* = nI$. We say that H is a *quaternary unit Hadamard matrix of order* n, and we denote this as QUH(n).

To motivate the results of this chapter, we will need the following idea.

Definition. Let $S = \{A_1, A_2, \ldots, A_s; B_1, B_2, \ldots, B_t\}$ be a family of matrices, each of order n, such that $\sum A_i A_i^* + q \sum B_j B_j^* = fI$, for some prime power q. Then we say that S is a *$q_{(s,t)}$-suitable family of matrices.* If $s = t$, then we write $q_{(s)}$-suitable for simplicity. We call f the *ordinate of suitability.*

q-suitability is interesting in that it provides a method for recursively building families of such matrices. In what follows, Q will be the Paley matrix of order q.

Proposition 5.1. Let q be an odd prime power, and let $\{A; B\}$ be a $q_{(1)}$-suitable family of matrices of order n. Define A_m and B_m for every non-

negative integer m thus.

$$A_m = \begin{cases} A & \text{if } m = 0, \text{ and} \\ J_q \otimes B_{m-1} & \text{otherwise.} \end{cases}$$

$$B_m = \begin{cases} B & \text{if } m = 0, \text{ and} \\ I_q \otimes A_{m-1} + \varepsilon Q \otimes B_{m-1} & \text{otherwise.} \end{cases}$$

We have the following.

i. Let $AB^* - BA^* = 0$. Then $\{A_m; B_m\}$ is an amicable $q_{(1)}$-suitable family of matrices in each of the following two cases. First, $q \equiv -1 \bmod 4$ and $\varepsilon = 1$. Second, $q \equiv 1 \bmod 4$ and $\varepsilon = i$.

ii. Let $AB^* + BA^* = 0$. Then $\{A_m; B_m\}$ is an anti-amicable $q_{(1)}$-suitable family of matrices in each of the following two cases. First, $q \equiv -1 \bmod 4$ and $\varepsilon = i$. Second, $q \equiv 1 \bmod 4$ and $\varepsilon = 1$.

Moreover, in every case, the ordinate of suitability is given by $q^m f$.

PROOF. We will prove the case where $q \equiv 1 \bmod 4$, $\varepsilon = 1$, and (A, B) is an anti-amicable pair, all other cases being similar. Assume, for $m - 1 > 0$, we have that $A_{m-1}A_{m-1}^* + qB_{m-1}B_{m-1}^* = q^{m-1} f I_{nq^{m-1}}$ and $A_{m-1}B_{m-1}^* + B_{m-1}A_{m-1}^* = 0$. Observe:

$$\begin{aligned} A_m A_m^* + qB_m B_m^* &= (J \otimes B_{m-1})(J \otimes B_{m-1})^* + \\ &\quad q(I \otimes A_{m-1} + Q \otimes B_{m-1})(I \otimes A_{m-1} + Q \otimes B_{m-1})^* \\ &= qJ \otimes B_{m-1}B_{m-1}^* + \\ &\quad q(I \otimes A_{m-1}A_{m-1}^* + Q \otimes A_{m-1}B_{m-1}^* + Q \otimes B_{m-1}A_{m-1}^* + \\ &\qquad QQ^* \otimes B_{m-1}B_{m-1}^*) \\ &= qJ \otimes B_{m-1}B_{m-1}^* + q(I \otimes A_{m-1}A_{m-1}^* + (qI - J) \otimes B_{m-1}B_{m-1}^*) \\ &= qI \otimes (A_{m-1}A_{m-1}^* + qB_{m-1}B_{m-1}^*) \\ &= q^m f I_{nq^m}. \end{aligned}$$

Therefore, $\{A_m; B_m\}$ is a $q_{(1)}$-suitable family of matrices. Finally,

$$\begin{aligned} A_m B_m^* &= (J \otimes B_{m-1})(I \otimes A_{m-1} + A \otimes B_{m-1})^* \\ &= J \otimes B_{m-1}A_{m-1}^* \\ &= -J \otimes A_{m-1}B_{m-1}^* \\ &= -B_m A_m^*; \end{aligned}$$

whence, (A_m, B_m) is an anti-amicable pair. *Q.E.D.*

Evidently, q-suitability can be exploited to construct families of matrices with pairwise orthogonal rows.

Proposition 5.2. Let q be an odd prime power, and let $\{A; B\}$ be a q-suitable family of matrices of order n. Define

$$X = \begin{bmatrix} 0 & \mathbf{j}^t \\ (-1)^{\frac{q+1}{2}}\mathbf{j} & Q \end{bmatrix} \otimes B + \varepsilon \begin{bmatrix} -1 & 0 \\ 0 & I_q \end{bmatrix} \otimes A.$$

We have the following.

i. Let $AB^* - BA^* = 0$. If $q \equiv -1 \bmod 4$ and $\varepsilon = 1$, or if $q \equiv 1 \bmod 4$ and $\varepsilon = i$, then $XX^* = fI_{n(q+1)}$.

ii. Let $AB^* + BA^* = 0$. If $q \equiv -1 \bmod 4$ and $\varepsilon = i$, or if $q \equiv 1 \bmod 4$ and $\varepsilon = 1$, then $XX^* = fI_{n(q+1)}$.

PROOF. We prove the case that (A, B) is an anti-amicable pair, $q \equiv 1 \bmod 4$, and $\varepsilon = 1$. We have

$$X = \begin{bmatrix} 0 & \mathrm{j}^t \\ -\mathbf{j} & Q \end{bmatrix} \otimes B + \begin{bmatrix} - & 0 \\ 0 & I_q \end{bmatrix} \otimes A.$$

Hence,

$$\begin{aligned} XX^* &= qI_{q+1} \otimes BB^* + \begin{bmatrix} 0 & \mathbf{j}^t \\ \mathbf{j} & Q \end{bmatrix} \otimes BA^* + \\ &\qquad \begin{bmatrix} 0 & \mathbf{j}^t \\ \mathbf{j} & Q \end{bmatrix} \otimes AB^* + I_{q+1} \otimes AA^t \\ &= I_{q+1} \otimes (AA^* + qBB^*) \\ &= fI_{n(q+1)}. \end{aligned}$$

Thus, X is as claimed. *Q.E.D.*

Taking $A = B = [1]$ yields the skew-type Hadamard matrices of Paley; however, we can do more.

Corollary 5.3. Let $q \equiv 1 \bmod 4$ be a prime power. There is an $\mathrm{H}(2q^n(q+1))$ for every $n \geq 0$.

PROOF. Take $A = \left[\begin{smallmatrix} 1 & - \\ 1 & 1 \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} 1 & 1 \\ - & 1 \end{smallmatrix}\right]$. Then (A, B) is an anti-ammicable pair of Hadamard matrices; whence, they are q-suitable with ordinate of suitability 2. Apply the recursion of Proposition 5.1. *Q.E.D.*

Corollary 5.4. Let q be any odd prime power. There is a $\mathrm{CH}(q^n(q+1))$, for every $n \geq 0$.

PROOF. Take $A = [1]$ and $B = [i]$. Apply the recursion of Proposition 5.1. *Q.E.D.*

We are ready to construct some families of QUH matrices, but first we extend the definition of QUH matrices in the following way. Let $\{1, i, j, k\}$ be the usual group of quaternions. Then a QUH(n) is a matrix (say H) whose entries are from the set $\left\{\frac{\pm\varepsilon_1 \pm \varepsilon_2\sqrt{q}}{\sqrt{q+1}} \mid \varepsilon_1, \varepsilon_2 = 1, i, j, k; \varepsilon_1 \neq \varepsilon_2\right\}$ such that $HH^* = nI$.

Theorem 5.5. Let q be an odd prime power, and let $\{A; B\}$ be an amicable family of $q_{(1)}$-suitable $(-1, 1)$-matrices of order n with ordinate of suitability $n(q + 1)$. Then

$$\frac{1}{\sqrt{q+1}}A + i\frac{\sqrt{q}}{\sqrt{q+1}}B, \text{ and}$$
$$\frac{i}{\sqrt{q+1}}A + \frac{\sqrt{q}}{\sqrt{q+1}}B$$

are QUH(n)s. If $\{A; B\}$ is an amicable family of $q_{(1)}$-suitable $(\pm 1, \pm i)$-matrices of order n with ordinate $n(q + 1)$. Then

$$\frac{1}{\sqrt{q+1}}A + j\frac{\sqrt{q}}{\sqrt{q+1}}B, \text{ and}$$
$$\frac{j}{\sqrt{q+1}}A + \frac{\sqrt{q}}{\sqrt{q+1}}B$$

are QUH(n)s.

Proof. We show the case that A and B are (-1,1)-matrices and $X = (A + i\sqrt{q}B)/\sqrt{q+1}$. We have $XX^* = (AA^* + qBB^*)/(q+1) = nI$. *Q.E.D.*

Corollary 5.6. For every odd prime power q, there is a QUH(q^n), for every $n > 0$.

Proof. Take $A = B = [1]$ and apply the recursion of Proposition 5.1. *Q.E.D.*

Of course, one can ask if we can have strictly complex QUH matrices in the case that $q \equiv 1 \bmod 4$. Evidently we can; though, it comes at the expense of a greater complexity of the underlying $q_{(1)}$-suitable matrices. We will say that two $(\pm 1, \pm i)$-matrices are *complex complimentary* if one has ± 1 whenever the other has $\pm i$, and conversely. We then have the following result, whose proof is similar to that of Theorem 5.5 and is, therefore, omitted.

Theorem 5.7. Let q be a prime power, and let $\{A; B\}$ be an anti-amicable, $q_{(1)}$-suitable, complex complementary family of matrices of order n, with ordinate $n(q + 1)$. Then

$$X = \frac{1}{\sqrt{q+1}}A + \frac{\sqrt{q}}{\sqrt{q+1}}B$$

is a QUH(n).

Corollary 5.8. Let $p \equiv 1 \bmod 4$ be a prime power. There is a QUH($p+1$).

PROOF. We have shown the existence of a symmetric conference matrix of order $p+1$ whenever $p \equiv 1 \bmod 4$, say W. Then $W + iI$ and $iW - I$ form an anti-amicable, complex complementary pair of CH($p+1$)s. Thus, they are trivially a family of $q_{(1)}$-suitable matrices of for every odd prime power q. Moreover, they have ordinate of suitability $(q+1)(p+1)$. The result follows. *Q.E.D.*

Corollary 5.9. If there is an H(n), then there is a QUH(n).

PROOF. If H is a H(n), then H and iH are the required matrices. *Q.E.D.*

5.2 Morphisms of QUH Matrices

In this section, we will introduce a kind of morphism from the set of quaternary unit Hadamard matrices to the set of complex Hadamard matrices. We must, however, introduce the following.

The Hadamard matrices constructed as a result of Proposition 2.7, for those prime powers $q \equiv -1 \bmod 4$, have the form $H = I + W$, where W is a skew-symmetric conference matrix. More generally, any matrix (say X) with constant diagonal such that $X = xI + P$, where $P^* = -P$, will be called *skew-type*.

Let $\alpha_m = \frac{1+i\sqrt{m}}{\sqrt{m+1}}$, and let $\beta_m = \frac{\sqrt{m}+i}{\sqrt{m+1}}$. In the next result, we will need the following two polynomials over $\mathbb{Q}[x]$.

$$p_{\alpha_m}(x) = x^4 + \frac{2(m-1)}{m+1}x^2 + 1 \qquad p_{\beta_m}(x) = x^4 - \frac{2(m-1)}{m+1}x^2 + 1$$

We have the following result.

Proposition 5.10. Let H be any skew-type Hadamard matrix of order $m+1$, such that $m+1$ is non-square. Then $\mathbb{Q}(\alpha_m, \beta_m) \simeq \mathbb{Q}\left(\frac{1}{\sqrt{m+1}}H, i\right)$.

PROOF. It can be checked that β_m is a root of $p_{\beta_m}(x)$. Then $-\beta_m$ and $\pm\beta_m^*$ are also roots of $p_{\beta_m}(x)$. Therefore, $p_{\beta_m}(x) = (x-\beta_m)(x+\beta_m)(x-\beta_m^*)(x+\beta_m^*)$ over $\mathbb{C}[x]$. Since β_m and β_m^* are not in $\mathbb{Q}$, it follows that $p_{\beta_m}(x)$ is irreducible over $\mathbb{Q}$. Moreover, since $\beta_m^{-1} = \beta_m^*$, it follows that $\mathbb{Q}(\beta_m)$ is the splitting field of $p_{\beta_m}(x)$. It is a straighforward calculation to show that $\frac{i}{\sqrt{m+1}}H$ is a root of $p_{\beta_m}(x)$, and so it is the minimal polynomial of this matrix. We have shown

$$\frac{\mathbb{Q}[x]}{(p_{\beta_m}(x))} \simeq \mathbb{Q}(\beta_m) \simeq \mathbb{Q}\left(\frac{i}{\sqrt{m+1}}H\right).$$

The case of $p_{\alpha_m}(x)$ and $\frac{1}{\sqrt{m+1}}H$ is similar. *Q.E.D.*

We note that in the case $m+1$ is a square, it follows that the polynomials $p_{\alpha_m}(x)$ and $p_{\beta_m}(x)$ factor into two irreducible quadradics, corresponding to the minimal polynomials of $\pm\alpha_m$ and $\pm\beta_m$, respectively. Then the minimal polynomials of α_m and $\frac{1}{\sqrt{m+1}}H$, $-\alpha_m$ and $\frac{-1}{\sqrt{m+1}}H^t$, β_m and $\frac{i}{\sqrt{m+1}}H$, $-\beta_m$ and $\frac{-i}{\sqrt{m+1}}H^t$, respectively, correspond. The next result also holds in the case that $m+1$ is a perfect square with minor modifications.

Proposition 5.11. If there exists a properly complex QUH(n) with entries from the set $\left\{\frac{\pm1\pm i\sqrt{m}}{\sqrt{m}}, \frac{\pm i\pm\sqrt{m}}{\sqrt{m+1}}\right\}$, and if there is a skew-type CH($m+1$), then there is a CH($nm+n$).

Proof. Let H be a skew-type CH($m+1$), and let $K=[k_{ij}]$ be a properly complex QUH(n). Define φ by $\frac{1+i\sqrt{m}}{\sqrt{m+1}} \mapsto \frac{1}{\sqrt{m+1}}H$ and $\frac{i+\sqrt{m}}{\sqrt{m+1}} \mapsto \frac{i}{\sqrt{m+1}}H$. If we take $\varphi|_{\mathbb{Q}}$ as $\mathbb{Q} \to \mathbb{Q}I$, then φ extends uniquely to an isomomorphism $\mathbb{Q}(\alpha_m,\beta_m) \to \mathbb{Q}(H/\sqrt{m+1}, i)$. Define K^φ by $k_{ij} \mapsto \varphi(k_{ij})$. Observe:

$$\begin{aligned}(m+1)\sum_h \varphi(k_{ih})\varphi(k_{jh})^* &= (m+1)\varphi\left(\sum_h k_{ih}k_{jh}^*\right)\\ &= (m+1)\varphi(n\delta_i^j)\\ &= (nm+n)I_n.\end{aligned}$$

Therefore, $\sqrt{m+1}K^\varphi$ is a CH($nm+n$). *Q.E.D.*

Finding morphisms for QUH matrices with quaternions is, in general, more difficult. We may, however, derive certain constructions in specific cases as the following example shows.

Example 5.12. The matrices $A=J_5$ and $B=I_5+iQ_5$ form an amicable family of $5_{(1)}$-suitable matrices. Then

$$X=\frac{1}{\sqrt{6}}A+j\frac{\sqrt{5}}{\sqrt{6}}B$$

is a QUH(5) with entries $\frac{1+j\sqrt{5}}{\sqrt{6}}$ and $\frac{1\pm k\sqrt{5}}{\sqrt{6}}$. Let W be a symmetric conference matrix of order 6. Apply the map $\frac{1+j\sqrt{5}}{\sqrt{6}} \mapsto I+jW$ and $\frac{1+k\sqrt{5}}{\sqrt{6}} \mapsto I+kW$, to obtain a *quaternion Hadamard matrix* of order thirty.

Note that the unimodular numbers $\frac{\pm i\pm j\sqrt{m}}{\sqrt{m+1}}$ and $\frac{\pm i\pm k\sqrt{m}}{\sqrt{m+1}}$ have minimal polynomial x^2+1 over $\mathbb{Q}$; hence, we need Hermitian Hadamard matrices, but their form remains elusive.

5.3 Notes

Properly complex quaternary unit Hadamard matrices were originally introduced in Fender *et al* [FKS18]. There the results of Propositions 5.1, 5.2, and 5.5 regarding amicable families of q-suitable matrices were shown. The parallel developments for those families of anti-amicable q-suitable matrices followed over the course of the preparation of this thesis. Theorem 5.7 also followed during this preparation.

Using the notation of §5.2, the morphisms $\alpha_m \mapsto H/\sqrt{m+1}$, for some skew-type Hadamard matrix of order $m+1$, were first shown in Heikoop *et al* [HPOCP20]. The elegance of the method presented there struck the authors, and it highlights a beautiful connectivity between otherwise seemingly disparate objects. Their method is most useful when employing q-suitable matrices for $q \equiv -1 \bmod 4$. The extension of this development to include the element β_m and the more general quaternion forms, along with the cases of complex complementary matrices, arose in an effort to employ those famlies of q-suitable matrices where $q \equiv 1 \bmod 4$. At the completion of this treatise, morphisms involving Hermitian Hadamard matrices is still not solved; however, it would seem to be a more tractable problem.

Chapter 6

Orthogonal Designs and Constant Weight Codes

6.1 Main Constructions

Let W be some skew-symmetric weighing matrix of weight k, and let (A, B) be an amicable pair of orthogonal design. Clearly, $W \otimes B$ is also an OD; however, because of the anti-symmetry of W, we can also form the block matrix $X = I \otimes A + W \otimes B$. Then $XX^* = (I \otimes A + W \otimes B)(I \otimes A^* - W \otimes B^*) = I \otimes AA^* + WW^* \otimes BB^* = I \otimes (AA^* + kBB^*)$. Therefore, X is an OD. For the case that W is symmetric, we follow the same construction using A and iB. It follows that if A, B, and W are real, then this construction can only give a real OD in the case that W is skew-symmetric. One may ask if the construction can be expanded to give real ODs in cases that the simple method would fail to yield. We can, in fact, provide a positive answer to this question in certain cases.

Recall the existence of a BGW$((q^{2d}-1)/(q-1), q^{2d-1}, q^{2d-1}-q^{2d-2}; G)$, where q is any prime power, and where G is any cyclic group of order n such that $q-1$ is a multiple of n. If $n \equiv 0 \bmod 2$, and if $(q-1)/n \equiv 1 \bmod 2$, then we have shown that W is skew-symmetric. Therefore, if $G = \langle -1 \rangle$, then W will be skew-symmetric precisely when $q \equiv -1 \bmod 4$. In this cases, we can form the matrix $I \otimes A + W \otimes B$. Note that W will be symmetric over this group, however, if $q \equiv 1 \bmod 4$. To expand this construction to those prime powers $q \equiv 1 \bmod 4$, we must use a different group in the BGW.

Define $g = \left[\begin{smallmatrix} 0 & 1 \\ - & 0 \end{smallmatrix}\right] \otimes I_m$, and let $G = \langle g \rangle$. Then $|g| = 4$, and $(q-1)/4 \equiv 1 \bmod 2$ precisely when $q \equiv 5 \bmod 8$. In the next result, we will need the following block arrays.

$$\alpha = \begin{bmatrix} A & B \\ -B & A \end{bmatrix}, \text{ and } \quad \beta = \begin{bmatrix} C & D \\ D & -C \end{bmatrix}.$$

We will further take $W = [w_{ij}]$ to be the BGW with parameters 4.1 over

the group $G = \langle g \rangle$ just defined. The following result provides an answer to our question.

Theorem 6.1. Let $q \equiv 1 \bmod 4$ be a prime power, and let $\{A, B; C, D\}$ be an amicable $q_{(2)}^{2d-1}$-suitable family of matrices of order n, with entries from the set $\{0, \pm x_1, \ldots, \pm x_\rho\}$, and with ordinate of suitability $f = \sum s_i x_i^2$. Define

$$X = I \otimes \alpha + \varepsilon W \otimes \beta,$$

where $\varepsilon \in \{1, i\}$. Then:

i. If $q \equiv 5 \bmod 8$, and if $\varepsilon = 1$, then X is an $\mathrm{OD}(v; s_1, s_2, \ldots, s_\rho)$; and

ii. if $q \equiv 1 \bmod 8$, and if $\varepsilon = i$, then X is a $\mathrm{COD}(v; s_1, s_2, \ldots, s_\rho)$;

where $v = 2n(q^{2d} - 1)/(q - 1)$.

Proof. Recall $|g| = 4$, and let $\xi = (q-1)/4$. Since the set of matrices $\{A, B; C, D\}$ is pairwise amicable, it follows that α and β are amicable. Moreover, $\beta\beta^t$ is constant block diagonal; whence, $g\beta\beta^t = \beta\beta^t g$. Further, note that $\alpha\beta^t = \left[\begin{smallmatrix} X & Y \\ Y & -X \end{smallmatrix}\right]$ so that $g^k\alpha\beta^t = \alpha\beta^t(g^k)^t$.

i. Assume $q \equiv 5 \bmod 8$ and $\varepsilon = 1$. Then $\xi \equiv 1 \bmod 2$; whence, $w_{ij} = -w_{ij}$. Let r_i and r_j be any two block rows of X. If $i = j$, then

$$\begin{aligned} r_i r_j^t &= \alpha\alpha^t + \sum_{k=1}^{q^{2d-1}} g^k\beta(g^k\beta)^t \\ &= \alpha\alpha^t + \sum_{k=1}^{q^{2d-1}} g^k\beta\beta^t(g^k)^t \\ &= \alpha\alpha^t + \sum_{k=1}^{q^{2d-1}} \beta\beta^t g^k(g^k)^t \\ &= \alpha\alpha^t + q^{2d-1}\beta\beta^t \\ &= \left(\sum_{k=1}^{\rho} s_k x_k^2\right) I_{2n}. \end{aligned}$$

If $i \neq j$, then there are two cases to consider. First, if $w_{ij} \neq 0$, then

$$\begin{aligned} r_i r_j^t &= -\alpha(g^m\beta)^t + g^m\beta\alpha^t + q^{2d-1}\xi\sum_{k=0}^{3} g^k \\ &= -\alpha\beta^t(g^m)^t + g^m\alpha\beta^t \\ &= -\alpha\beta^t(g^m)^t + \alpha\beta^t(g^m)^t \\ &= 0, \end{aligned}$$

where $m = \log w_{ij}$. The second case, in which $w_{ij} = 0$, is immediate.

ii. Assume $q \equiv 1 \bmod 8$ and $\varepsilon = i$. Then $\xi \equiv 0 \bmod 2$; whence, $w_{ij} = w_{ji}$. As in i., it follows, *mutatis mutandis*, that $r_i r_j^* = (\sum s_k x_k^2) I_{2n} \delta_i^j$.

In any case, we have, therefore, that $XX^* = (\sum s_k x_k^2) I_v$. *Q.E.D.*

Of course, if α and β are any $q_{(1)}$-suitable (not an AOD as assumed at the start of this section), then $I \otimes \alpha + W \otimes \beta$ will be a design in the case that W is skew-symmetric.

The block matrices α and β used in the previous result may be replaced with other suitable arrays. For example, if we instead take

$$\alpha = \begin{bmatrix} -A & A \\ A & A \end{bmatrix}, \text{ and } \begin{bmatrix} B & B \\ B & -B \end{bmatrix},$$

then one may obtain a similar result. First, let $W = [w_{ij}]$ be as before, and let $R = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right] \otimes I_n$. Define $\tilde{W} = [w_{ij} R]$. We then have the following.

Theorem 6.2. Let q be any odd prime power, and let $\{A; B\}$ be any family of $q_{(1)}^{2d-1}$-suitable matrices, whose entries are in the set $\{0, \pm x_1, \ldots, \pm x_\rho\}$, and with ordinate of suitability $f = \sum s_i x_i^2$. Further, let the group over which $\tilde{W}$ is defined be chosen to reflect the value of q modulo 4. Define

$$X = I \otimes \alpha + \tilde{W} \otimes \beta.$$

Then:

i. If $q \equiv 5 \bmod 8$ or $q \equiv 3 \bmod 4$, and if $AB^t - BA^t = 0$, then X is an $\mathrm{OD}(v; 2s_1, 2s_2, \ldots, 2s_\rho)$; and

ii. if $q \equiv 1 \bmod 8$, and if $AB^t + BA^t = 0$, then X is an $\mathrm{OD}(v; 2s_1, 2s_1, \ldots, 2s_\rho)$;

where $v = 2n(q^{2d} - 1)/(q - 1)$.

Proof. Note that $\alpha\beta^t = \left[\begin{smallmatrix} 0 & -2AB^t \\ 2AB^t & 0 \end{smallmatrix}\right]$. Then one may verify that AB^t and $g^k R$ anti-commute for $k \in \{0, 1, 2, 3\}$. The remainder of the proof is similar to that of Theorem 6.1, and is therefore omitted. *Q.E.D.*

The follow proposition is simply a collection of immediate corollaries of the results we have thusfar obtained.

Proposition 6.3. Let $d \in \mathbb{Z}_+$, and let $v = (q^{2d} - 1)/(q - 1)$. Further, let q be any odd prime power, and let $\{A, B; C, D\}$ be a family of pairwise amicable $q_{(2)}^{2d-1}$-suitable matrices. Then:

i. If B ,C, and D are symmetric, while A is skew-type, then the resulting design will be skew-type.

ii. If A, B, C, and D have no zero entries, and if $d = 1$, then the resulting design will be full.

iii. There is a skew-type design of order $2v$ and type $(1, 1, q^{2d-1}, q^{2d-1})$.

iv. If n is the order of a pair of amicable Hadamard matrices (see Seberry, Yamada [SY92]), then there is a skew-type design of order 2nv and type $(1, n-1, n, nq^{2d-1}, nq^{2d-1})$.

v. For every odd q, there is a design of order $2q^{2d-1}v$ and type (q^{4d-2}, q^{4d-2}); and for $q \equiv 1 \bmod 4$, there is a design of the same order with type $(q^{2d-1}(q^{2d-1}+1), q^{2d-1}(q^{2d-1}+1))$.

vi. If there are two families of $q_{(1)}^{2d-1}$-suitable matrices of order n such that each pair is amicable, then there is an anti-amicable pair of designs of order $2nv$.

PROOF. i., ii., and iv. are obvious. iii. follows from the AOD$(2; (1,1); (1,1))$ given by $\left[\begin{smallmatrix} a & b \\ \bar{b} & a \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} c & d \\ d & \bar{c} \end{smallmatrix}\right]$.

To show v., let Q be the Paley matrix of order q. Then we take $A = aJ$, $B = bJ$, $C = aQ$, and $D = bQ$ in the first case; and we take $A = aJ$, $B = bJ$, $C = bI + aQ$, and $D = bQ - aI$ in the second case.

To show vi., we let $\{\tilde{A}; \tilde{B}\}$ and $\{\tilde{C}; \tilde{D}\}$ be our two families of $q_{(1)}^{2d-1}$-suitable matrices such that each pair is amicable. We then take $\tilde{W}$ as above and define the following.

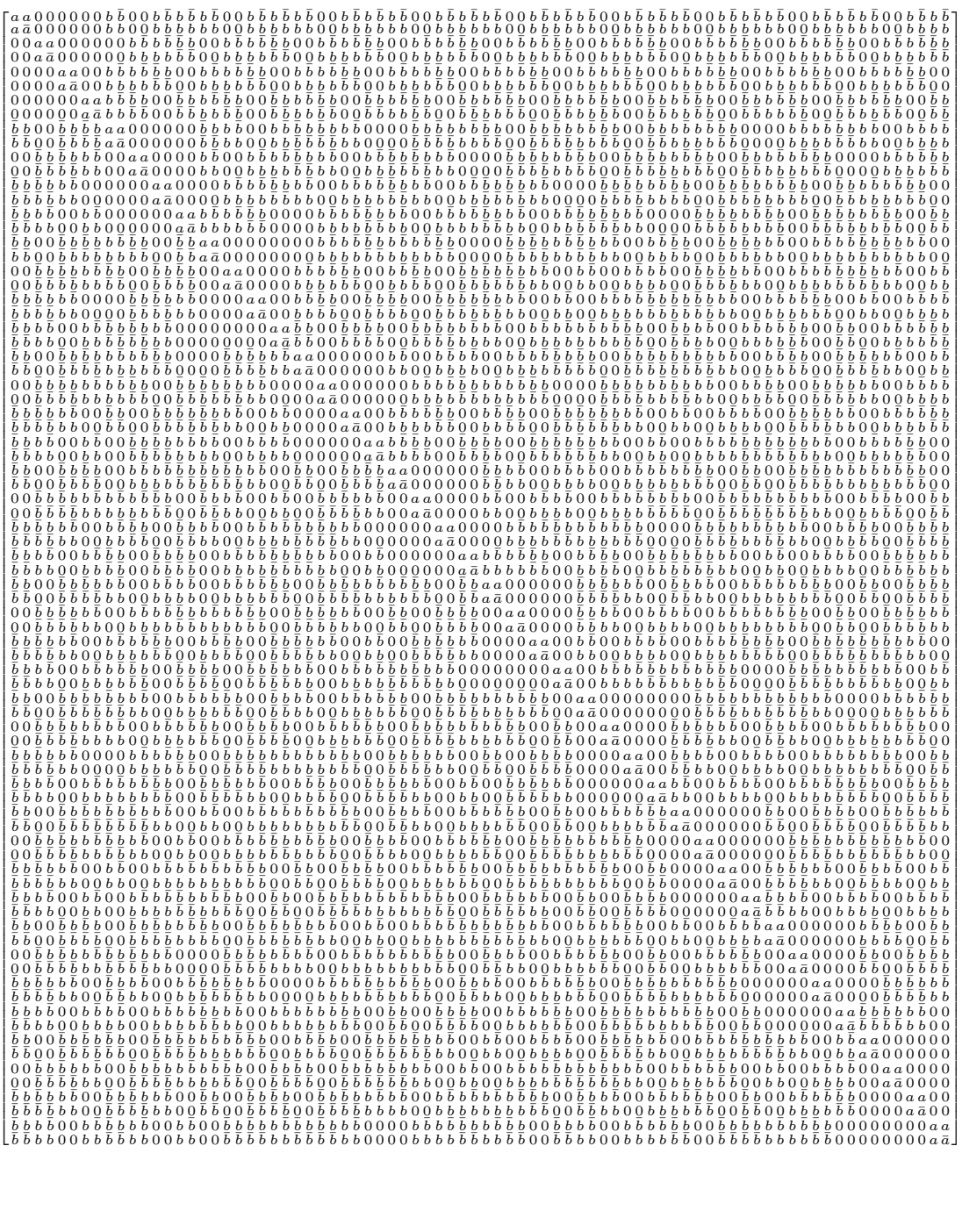
$$\alpha = \begin{bmatrix} \tilde{A} & \tilde{A} \\ \tilde{A} & -\tilde{A} \end{bmatrix} \quad \beta = \begin{bmatrix} \tilde{B} & \tilde{B} \\ \tilde{B} & -\tilde{B} \end{bmatrix}$$
$$\gamma = \begin{bmatrix} -\tilde{C} & \tilde{C} \\ \tilde{C} & \tilde{C} \end{bmatrix} \quad \eta = \begin{bmatrix} -\tilde{D} & \tilde{D} \\ \tilde{D} & \tilde{D} \end{bmatrix}$$

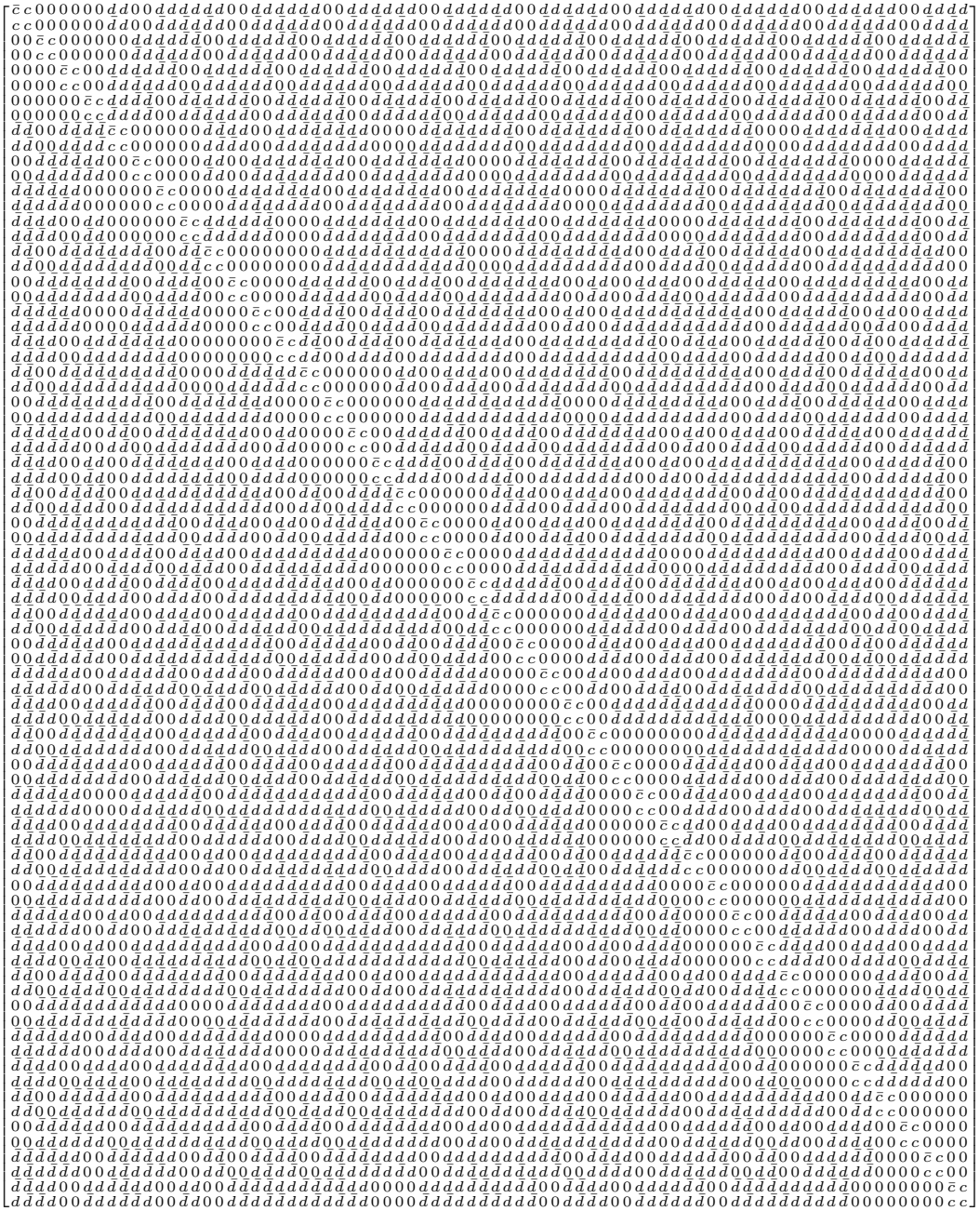
Then the designs $X = I \otimes \alpha + \tilde{W} \otimes \beta$ and $Y = I \otimes \gamma + \tilde{W} \otimes \eta$ can be verified to be anti-amicable by routine calculation. *Q.E.D.*

Example 6.4. i. From amicable Hadamard matrices of order 4, a skew-type OD(24;1,1,2,10,10).

$$\begin{bmatrix}
e & a & b & \bar{b} & c & c & d & \bar{d} & c & \bar{c} & d & \bar{d} & c & \bar{c} & d & \bar{d} & c & \bar{c} & d & \bar{d} \\
\bar{a} & e & b & \bar{b} & c & \bar{c} & d & \bar{d} & c & \bar{c} & d & \bar{d} & c & \bar{c} & d & \bar{d} & c & \bar{c} & d & \bar{d} \\
\bar{b} & \bar{b} & e & a & d & d & \bar{c} & \bar{c} & d & d & \bar{c} & \bar{c} & d & d & \bar{c} & \bar{c} & d & d & \bar{c} & \bar{c} \\
\bar{b} & b & \bar{a} & e & d & \bar{d} & \bar{c} & c & d & \bar{d} & \bar{c} & c & d & \bar{d} & \bar{c} & c & d & \bar{d} & \bar{c} & c \\
\bar{c} & \bar{c} & \bar{d} & \bar{d} & e & a & b & b & d & d & \bar{c} & \bar{c} & \bar{c} & \bar{d} & \bar{d} & \bar{d} & c & c & c & d & d \\
\bar{c} & c & \bar{d} & d & \bar{a} & e & b & \bar{b} & d & \bar{d} & \bar{c} & c & \bar{c} & \bar{d} & d & \bar{d} & c & \bar{c} & c & \bar{d} & \bar{d} \\
\bar{d} & \bar{d} & c & c & \bar{b} & \bar{b} & e & a & \bar{c} & \bar{c} & \bar{d} & \bar{d} & \bar{d} & c & c & c & c & d & d & d & \bar{c} & \bar{c} \\
\bar{d} & d & c & \bar{c} & \bar{b} & b & \bar{a} & e & \bar{c} & c & \bar{d} & d & \bar{d} & c & \bar{c} & c & \bar{c} & d & \bar{d} & d & \bar{c} & c \\
\bar{c} & \bar{c} & \bar{d} & \bar{d} & \bar{d} & \bar{d} & c & c & e & a & b & b & d & d & \bar{c} & \bar{c} & c & c & d & d & \bar{c} & \bar{c} & \bar{d} & \bar{d} \\
\bar{c} & c & \bar{d} & d & \bar{d} & d & c & \bar{c} & \bar{a} & e & b & \bar{b} & d & \bar{d} & \bar{c} & c & c & \bar{c} & d & \bar{d} & \bar{c} & c & \bar{d} & d \\
\bar{d} & \bar{d} & c & c & c & c & d & d & \bar{b} & \bar{b} & e & a & \bar{c} & \bar{c} & \bar{d} & \bar{d} & d & d & \bar{c} & \bar{c} & \bar{d} & \bar{d} & c & c \\
\bar{d} & d & c & \bar{c} & c & \bar{c} & d & \bar{d} & \bar{b} & b & \bar{a} & e & \bar{c} & c & \bar{d} & d & d & \bar{d} & \bar{c} & c & \bar{d} & d & c & \bar{c} \\
\bar{c} & \bar{c} & \bar{d} & \bar{d} & c & c & d & d & \bar{d} & \bar{d} & c & c & e & a & b & b & \bar{c} & \bar{c} & \bar{d} & \bar{d} & d & d & \bar{c} & \bar{c} \\
\bar{c} & c & \bar{d} & d & c & \bar{c} & d & \bar{d} & \bar{d} & d & c & \bar{c} & \bar{a} & e & b & \bar{b} & \bar{c} & c & \bar{d} & d & d & \bar{d} & \bar{c} & c \\
\bar{d} & \bar{d} & c & c & d & d & \bar{c} & \bar{c} & c & c & d & d & \bar{b} & \bar{b} & e & a & \bar{d} & \bar{d} & c & c & \bar{c} & \bar{c} & \bar{d} & \bar{d} \\
\bar{d} & d & c & \bar{c} & d & \bar{d} & \bar{c} & c & c & \bar{c} & d & \bar{d} & \bar{b} & b & \bar{a} & e & \bar{d} & d & c & \bar{c} & \bar{c} & c & \bar{d} & d \\
\bar{c} & \bar{c} & \bar{d} & \bar{d} & d & d & \bar{c} & \bar{c} & \bar{c} & \bar{d} & \bar{d} & c & c & d & d & e & a & b & b & \bar{d} & \bar{d} & c & c \\
\bar{c} & c & \bar{d} & d & d & \bar{d} & \bar{c} & c & \bar{c} & c & \bar{d} & d & c & \bar{c} & d & \bar{d} & \bar{a} & e & b & \bar{b} & \bar{d} & d & c & \bar{c} \\
\bar{d} & \bar{d} & c & c & \bar{c} & \bar{c} & \bar{d} & \bar{d} & \bar{d} & \bar{d} & c & c & d & d & \bar{c} & \bar{c} & \bar{b} & \bar{b} & e & a & c & c & d & d \\
\bar{d} & d & c & \bar{c} & \bar{c} & c & \bar{d} & d & \bar{d} & d & c & \bar{c} & d & \bar{d} & \bar{c} & c & \bar{b} & b & \bar{a} & e & c & \bar{c} & d & \bar{d} \\
\bar{c} & \bar{c} & \bar{d} & \bar{d} & \bar{c} & \bar{c} & \bar{d} & \bar{d} & c & c & d & d & \bar{d} & \bar{d} & c & c & d & d & \bar{c} & \bar{c} & e & a & b & b \\
\bar{c} & c & \bar{d} & d & \bar{c} & c & \bar{d} & d & c & \bar{c} & d & \bar{d} & \bar{d} & d & c & \bar{c} & d & \bar{d} & \bar{c} & c & \bar{a} & e & b & \bar{b} \\
\bar{d} & \bar{d} & c & c & \bar{d} & \bar{d} & c & c & d & d & \bar{c} & \bar{c} & c & c & d & d & \bar{c} & \bar{c} & \bar{d} & \bar{d} & \bar{b} & \bar{b} & e & a \\
\bar{d} & d & c & \bar{c} & \bar{d} & d & c & \bar{c} & d & \bar{d} & \bar{c} & c & c & \bar{c} & d & \bar{d} & \bar{c} & c & \bar{d} & d & \bar{b} & b & \bar{a} & e
\end{bmatrix}$$

ii. An AAOD(80; (2,54); (2,54)).





The structure of the BGWs W and $\tilde{W}$ can be exploited in other ways as well. To this end, we note that W and $\tilde{W}$ are, in fact, disjoint weighing matrices. The proof of the following result comes by straightforward calculations.

Proposition 6.5. Let W and $\tilde{W}$ be as above, and let $v = (q^{2d}-1)/(q-1)$. Then:

i. If A is an OD$(m; s_1, s_2, \ldots, s_\rho)$, then $X = W \otimes A$ is an OD$(mv; q^{2d-1}s_1, q^{2d-1}s_2, \ldots, q^{2d-1}s_\rho)$; and

ii. if (A, B) is an AAOD$(m; (s_1, s_2, \ldots, s_\rho); (t_1, t_2, \ldots, t_\sigma))$, then , understand W and $\tilde{W}$ as weighing matrices only, $X = W \otimes A + \tilde{W} \otimes B$ is a design order kv and type $(q^{2d-1}s_1, \ldots, q^{2d-1}s_\rho, q^{2d-1}t_1, \ldots, q^{2d-1}t_\sigma)$.

Example 6.6. The matrix A given by

$$A = \begin{bmatrix} \bar{b} & b & a & 0 & b & b \\ b & a & \bar{b} & b & 0 & b \\ a & \bar{b} & b & b & b & 0 \\ 0 & b & b & b & \bar{b} & \bar{a} \\ b & 0 & b & \bar{b} & \bar{a} & b \\ b & b & 0 & \bar{a} & b & \bar{b} \end{bmatrix}$$

is a symmetric OD(6; 1, 4). Using i. of the Proposition, for $q = 5$ and $d = 1$, we find that we have a skew-symmetric OD(36; 5, 20), say X. However, since X is skew-symmetric, $cI + X$ is a skew-type OD$(36; 1, 5, 20)$.

$$
\left[\begin{array}{cccccccccccccccccccccccccccccccccccc}
c&0&0&0&0&0&\bar{b}&b&a&0&b&b&\bar{b}&b&a&0&b&b&\bar{b}&b&a&0&b&b&\bar{b}&b&a&0&b&b&\bar{b}&b&a&0&b&b\\
0&c&0&0&0&0&b&a&\bar{b}&b&0&b&b&a&\bar{b}&b&0&b&b&a&\bar{b}&b&0&b&b&a&\bar{b}&b&0&b&b&a&\bar{b}&b&0&b\\
0&0&c&0&0&0&a&\bar{b}&b&b&b&0&a&\bar{b}&b&b&b&0&a&\bar{b}&b&b&b&0&a&\bar{b}&b&b&b&0&a&\bar{b}&b&b&b&0\\
0&0&0&c&0&0&0&b&b&b&\bar{b}&\bar{a}&0&b&b&b&\bar{b}&\bar{a}&0&b&b&b&\bar{b}&\bar{a}&0&b&b&b&\bar{b}&\bar{a}&0&b&b&b&\bar{b}&\bar{a}\\
0&0&0&0&c&0&b&0&b&\bar{b}&\bar{a}&b&b&0&b&\bar{b}&\bar{a}&b&b&0&b&\bar{b}&\bar{a}&b&b&0&b&\bar{b}&\bar{a}&b&b&0&b&\bar{b}&\bar{a}&b\\
0&0&0&0&0&c&b&b&0&\bar{a}&b&\bar{b}&b&b&0&\bar{a}&b&\bar{b}&b&b&0&\bar{a}&b&\bar{b}&b&b&0&\bar{a}&b&\bar{b}&b&b&0&\bar{a}&b&\bar{b}\\
b&\bar{b}&\bar{a}&0&\bar{b}&\bar{b}&c&0&0&0&0&0&0&b&b&b&\bar{b}&\bar{a}&b&\bar{b}&\bar{a}&0&\bar{b}&\bar{b}&0&\bar{b}&\bar{b}&\bar{b}&b&a&\bar{b}&b&a&0&b&b\\
\bar{b}&\bar{a}&b&\bar{b}&0&\bar{b}&0&c&0&0&0&0&b&0&b&\bar{b}&\bar{a}&b&\bar{b}&\bar{a}&b&\bar{b}&0&\bar{b}&\bar{b}&0&\bar{b}&b&a&\bar{b}&b&a&\bar{b}&b&0&b\\
\bar{a}&b&\bar{b}&\bar{b}&\bar{b}&0&0&0&c&0&0&0&b&b&0&\bar{a}&b&\bar{b}&\bar{a}&b&\bar{b}&\bar{b}&\bar{b}&0&\bar{b}&\bar{b}&0&a&\bar{b}&b&a&\bar{b}&b&b&b&0\\
0&\bar{b}&\bar{b}&\bar{b}&b&a&0&0&0&c&0&0&b&\bar{b}&\bar{a}&0&\bar{b}&\bar{b}&0&\bar{b}&\bar{b}&\bar{b}&b&a&\bar{b}&b&a&0&b&b&0&b&b&b&\bar{b}&\bar{a}\\
\bar{b}&0&\bar{b}&b&a&\bar{b}&0&0&0&0&c&0&\bar{b}&\bar{a}&b&\bar{b}&0&\bar{b}&\bar{b}&0&\bar{b}&b&a&\bar{b}&b&a&\bar{b}&b&0&b&b&0&b&\bar{b}&\bar{a}&b\\
\bar{b}&\bar{b}&0&a&\bar{b}&b&0&0&0&0&0&c&\bar{a}&b&\bar{b}&\bar{b}&\bar{b}&0&\bar{b}&\bar{b}&0&a&\bar{b}&b&a&\bar{b}&b&b&b&0&b&b&0&\bar{a}&b&\bar{b}\\
b&\bar{b}&\bar{a}&0&\bar{b}&\bar{b}&0&\bar{b}&\bar{b}&\bar{b}&b&a&c&0&0&0&0&0&0&b&b&b&\bar{b}&\bar{a}&\bar{b}&b&a&0&b&b&b&\bar{b}&\bar{a}&0&\bar{b}&\bar{b}\\
\bar{b}&\bar{a}&b&\bar{b}&0&\bar{b}&\bar{b}&0&\bar{b}&b&a&\bar{b}&0&c&0&0&0&0&b&0&b&\bar{b}&\bar{a}&b&b&a&\bar{b}&b&0&b&\bar{b}&\bar{a}&b&\bar{b}&0&\bar{b}\\
\bar{a}&b&\bar{b}&\bar{b}&\bar{b}&0&\bar{b}&\bar{b}&0&a&\bar{b}&b&0&0&c&0&0&0&b&b&0&\bar{a}&b&\bar{b}&a&\bar{b}&b&b&b&0&\bar{a}&b&\bar{b}&\bar{b}&\bar{b}&0\\
0&\bar{b}&\bar{b}&\bar{b}&b&a&\bar{b}&b&a&0&b&b&0&0&0&c&0&0&b&\bar{b}&\bar{a}&0&\bar{b}&\bar{b}&0&b&b&b&\bar{b}&\bar{a}&0&\bar{b}&\bar{b}&\bar{b}&b&a\\
\bar{b}&0&\bar{b}&b&a&\bar{b}&b&a&\bar{b}&b&0&b&0&0&0&0&c&0&\bar{b}&\bar{a}&b&\bar{b}&0&\bar{b}&b&0&b&\bar{b}&\bar{a}&b&\bar{b}&0&\bar{b}&b&a&\bar{b}\\
\bar{b}&\bar{b}&0&a&\bar{b}&b&a&\bar{b}&b&b&b&0&0&0&0&0&0&c&\bar{a}&b&\bar{b}&\bar{b}&\bar{b}&0&b&b&0&\bar{a}&b&\bar{b}&\bar{b}&\bar{b}&0&a&\bar{b}&b\\
b&\bar{b}&\bar{a}&0&\bar{b}&\bar{b}&\bar{b}&b&a&0&b&b&0&\bar{b}&\bar{b}&\bar{b}&b&a&c&0&0&0&0&0&b&\bar{b}&\bar{a}&0&\bar{b}&\bar{b}&0&b&b&b&\bar{b}&\bar{a}\\
\bar{b}&\bar{a}&b&\bar{b}&0&\bar{b}&b&a&\bar{b}&b&0&b&\bar{b}&0&\bar{b}&b&a&\bar{b}&0&c&0&0&0&0&\bar{b}&\bar{a}&b&\bar{b}&0&\bar{b}&b&0&b&\bar{b}&\bar{a}&b\\
\bar{a}&b&\bar{b}&\bar{b}&\bar{b}&0&a&\bar{b}&b&b&b&0&\bar{b}&\bar{b}&0&a&\bar{b}&b&0&0&c&0&0&0&\bar{a}&b&\bar{b}&\bar{b}&\bar{b}&0&b&b&0&\bar{a}&b&\bar{b}\\
0&\bar{b}&\bar{b}&\bar{b}&b&a&0&b&b&b&\bar{b}&\bar{a}&\bar{b}&b&a&0&b&b&0&0&0&c&0&0&0&\bar{b}&\bar{b}&\bar{b}&b&a&b&\bar{b}&\bar{a}&0&\bar{b}&\bar{b}\\
\bar{b}&0&\bar{b}&b&a&\bar{b}&b&0&b&\bar{b}&\bar{a}&b&b&a&\bar{b}&b&0&b&0&0&0&0&c&0&\bar{b}&0&\bar{b}&b&a&\bar{b}&\bar{b}&\bar{a}&b&\bar{b}&0&\bar{b}\\
\bar{b}&\bar{b}&0&a&\bar{b}&b&b&b&0&\bar{a}&b&\bar{b}&a&\bar{b}&b&b&b&0&0&0&0&0&0&c&\bar{b}&\bar{b}&0&a&\bar{b}&b&\bar{a}&b&\bar{b}&\bar{b}&\bar{b}&0\\
b&\bar{b}&\bar{a}&0&\bar{b}&\bar{b}&0&b&b&b&\bar{b}&\bar{a}&b&\bar{b}&\bar{a}&0&\bar{b}&\bar{b}&\bar{b}&b&a&0&b&b&c&0&0&0&0&0&0&\bar{b}&\bar{b}&\bar{b}&b&a\\
\bar{b}&\bar{a}&b&\bar{b}&0&\bar{b}&b&0&b&\bar{b}&\bar{a}&b&\bar{b}&\bar{a}&b&\bar{b}&0&\bar{b}&b&a&\bar{b}&b&0&b&0&c&0&0&0&0&\bar{b}&0&\bar{b}&b&a&\bar{b}\\
\bar{a}&b&\bar{b}&\bar{b}&\bar{b}&0&b&b&0&\bar{a}&b&\bar{b}&\bar{a}&b&\bar{b}&\bar{b}&\bar{b}&0&a&\bar{b}&b&b&b&0&0&0&c&0&0&0&\bar{b}&\bar{b}&0&a&\bar{b}&b\\
0&\bar{b}&\bar{b}&\bar{b}&b&a&b&\bar{b}&\bar{a}&0&\bar{b}&\bar{b}&0&\bar{b}&\bar{b}&\bar{b}&b&a&0&b&b&b&\bar{b}&\bar{a}&0&0&0&c&0&0&\bar{b}&b&a&0&b&b\\
\bar{b}&0&\bar{b}&b&a&\bar{b}&\bar{b}&\bar{a}&b&\bar{b}&0&\bar{b}&\bar{b}&0&\bar{b}&b&a&\bar{b}&b&0&b&\bar{b}&\bar{a}&b&0&0&0&0&c&0&b&a&\bar{b}&b&0&b\\
\bar{b}&\bar{b}&0&a&\bar{b}&b&\bar{a}&b&\bar{b}&\bar{b}&\bar{b}&0&\bar{b}&\bar{b}&0&a&\bar{b}&b&b&b&0&\bar{a}&b&\bar{b}&0&0&0&0&0&c&a&\bar{b}&b&b&b&0\\
b&\bar{b}&\bar{a}&0&\bar{b}&\bar{b}&b&\bar{b}&\bar{a}&0&\bar{b}&\bar{b}&\bar{b}&b&a&0&b&b&0&\bar{b}&\bar{b}&\bar{b}&b&a&0&b&b&b&\bar{b}&\bar{a}&c&0&0&0&0&0\\
\bar{b}&\bar{a}&b&\bar{b}&0&\bar{b}&\bar{b}&\bar{a}&b&\bar{b}&0&\bar{b}&b&a&\bar{b}&b&0&b&\bar{b}&0&\bar{b}&b&a&\bar{b}&b&0&b&\bar{b}&\bar{a}&b&0&c&0&0&0&0\\
\bar{a}&b&\bar{b}&\bar{b}&\bar{b}&0&\bar{a}&b&\bar{b}&\bar{b}&\bar{b}&0&a&\bar{b}&b&b&b&0&\bar{b}&\bar{b}&0&a&\bar{b}&b&b&b&0&\bar{a}&b&\bar{b}&0&0&c&0&0&0\\
0&\bar{b}&\bar{b}&\bar{b}&b&a&0&\bar{b}&\bar{b}&\bar{b}&b&a&0&b&b&b&\bar{b}&\bar{a}&\bar{b}&b&a&0&b&b&b&\bar{b}&\bar{a}&0&\bar{b}&\bar{b}&0&0&0&c&0&0\\
\bar{b}&0&\bar{b}&b&a&\bar{b}&\bar{b}&0&\bar{b}&b&a&\bar{b}&b&0&b&\bar{b}&\bar{a}&b&b&a&\bar{b}&b&0&b&\bar{b}&\bar{a}&b&\bar{b}&0&\bar{b}&0&0&0&0&c&0\\
\bar{b}&\bar{b}&0&a&\bar{b}&b&\bar{b}&\bar{b}&0&a&\bar{b}&b&b&b&0&\bar{a}&b&\bar{b}&a&\bar{b}&b&b&b&0&\bar{a}&b&\bar{b}&\bar{b}&\bar{b}&0&0&0&0&0&0&c
\end{array}\right]
$$

6.2 A Recursive Method

In this section, we will apply the recursive constructions employed in the previous chapter. To this end, note that every $q_{(1)}$-suitable family of matrices is also $q_{(k)}$-suitable, for any k. We observe the following immediate results.

Proposition 6.7. Let $q =\equiv 5 \bmod 8$ be a prime power. Then, for every non-negative m and n, there is a AACOD$(2q^m(q^{2n}-1)/(q-1); (2q^m, 2q^{2n+m-1}); (2q^m, 2q^{2n+m-1}))$.

Proof. Using the recursion of Proposition 5.1 to define A_m and B_m with base case $A_0 = B_0 = [1]$, and taking $\tilde{A} = aA_m$, $\tilde{B} = bB_m$, $\tilde{C} = cA_m$, and

$\tilde{D} = dB_m$ in Proposition 6.5(vi), we arrive at the required pair of matrices. *Q.E.D.*

Proposition 6.8. Let q be an odd prime power. If $q \equiv -1 \bmod 4$, then, for every non-negative m and n, there is an $\mathrm{OD}(2q^m(q^{2n}-1)/(q-1); q^m, q^m, q^{2n+m-1}, q^{2n+m-1})$; while if $q \equiv 1 \bmod 4$, the design is complex.

PROOF. Use the recursion of Proposition 5.1 to define A_m and B_m with base case $A_0 = B_0 = [1]$, and taking $A = aA_m$, $B = bA_m$, $C = cB_m$, and $D = dB_m$ in Theorem 6.1. *Q.E.D.*

The following is an immediate consequence of Proposition 5.1 and Theorem 6.1.

Proposition 6.9. Let q and p be odd prime powers where $q \equiv 5 \bmod 8$, and let m, n, and d be non-negative. Then there is a $\mathrm{CW}(2p^n q^m(q^{2d}-1)/(q-1))$.

For the following result, assume the conditions of Theorem 6.1.

Theorem 6.10. Let $q \equiv 1 \bmod 4$ be a prime power, and let $\{X; Y\}$ be an amicable $q_{(1)}^{2d-1}$-suitable family of matrices of order n, with entries from the set $\{0, \pm x_1, \ldots, \pm x_\rho\}$, and with ordinate of suitability $\sum s_i x_i^2$. Then, for every non-negative m, there is a $\mathrm{COD}(2nq^m(q^{2d}-1)/(q-1); 2q^m s_1, 2q^m s_2, \ldots, 2q^m s_\rho)$.

PROOF. Define A_m and B_m using the recursion of Proposition 5.1 with base case $A_0 = X$ and $B_0 = Y$. Then take $A = B = A_m$ and $C = D = B_m$ in Theorem 6.1. The result follows. *Q.E.D.*

Corollary 6.11. Let (A, B) be an $\mathrm{AOD}(n; (s_1, s_2, \ldots, s_\rho); (t_1, t_2, \ldots, t_\sigma))$. Then, for every non-negative m and d, there is a $\mathrm{COD}(2nq^m(q^{2d}-1)/(q-1); 2q^m s_1, \ldots, 2q^m s_\rho, 2q^{2d+m-1} t_1, \ldots, 2q^{2d+m-1} t_\sigma)$.

PROOF. Take $X = A$ and $Y = B$ in the theorem. *Q.E.D.*

We can obtain a result analogous to Theorem 6.10 as follows.

Theorem 6.12. Let $q \equiv 1 \bmod 8$ be a prime power, and let $\{X; Y\}$ be a $q_{(1)}^{2d-1}$-suitable family of anti-amicable matrices of order n, with entries from the set $\{0, \pm x_1, \ldots, \pm x_\rho\}$, and with ordinate $\sum s_i x_i^2$. Then, for every non-negative m, there is an $\mathrm{OD}(2nq^m(q^{2d}-1)/(q-1); 2q^m s_1, 2q^m s_2, \ldots, 2q^m s_\rho)$.

PROOF. Define A_m and B_m using the recursion of Proposition 5.1 with base case $A_0 = X$ and $B_0 = Y$. Then take $A = A_m$ and $B = B_m$ in Theorem 6.2. *Q.E.D.*

Corollary 6.13. Let (A, B) be any AAOD$(n; (s_1, s_2, \ldots, s_\rho); (t_1, t_2, \ldots, t_\sigma))$, and let $q \equiv 1 \bmod 8$ be a prime power. Then there is an OD$(2nq^m(q^{2d} - 1)/(q-1); 2q^m s_1, \ldots, 2q^m s_\rho, 2q^{2d+m-1}t_1, \ldots, 2q^{2d+m-1}t_\sigma)$, for every non-negative m.

PROOF. Take $X = A$ and $Y = B$ in the theorem. *Q.E.D.*

Corollary 6.14. Let $q \equiv 1 \bmod 8$ and $p \equiv 5 \bmod 8$ be prime powers. Then, for every non-negative n, m, s, and t there is a COD$(4p^m q^n (p^{2s} - 1)(q^{2t} - 1)/(p-1)(q-1); 4q^n p^m, 4q^n p^{2s+m-1}, 4q^{2t+n-1}p^m, 4q^{2t+n-1}p^{2s+m-1})$.

PROOF. The result follows immediatly using Proposition 6.7. *Q.E.D.*

Using the results of this and the previous chapter, after running searches on the derived parameters, we arrive at new orders of real Hadamard matrices. Note that the order of each Hadamard matrix can be written in the form $2^t n$, where $t \geq 2$ and $n \equiv 1 \bmod 2$. We will adopted the convention of writing this order as $n(t)$. The new orders of Hadamard matrices are shown below.

933(3)	1169(3)	1437(3)	1981(3)
2429(3)	2513(3)	2589(3)	2973(3)
3093(3)	3101(3)	3117(3)	3173(3)
3303(3)	3401(3)	3437(3)	3629(3)
3669(3)	3957(3)	4193(3)	4237(3)
4317(3)	4353(3)	4413(3)	4461(3)
4677(3)	4713(3)	4769(3)	4989(3)
5001(3)	5033(3)	5171(3)	5349(3)
5361(3)	5433(3)	5549(3)	5613(3)
5761(3)	5847(3)	5909(3)	5921(3)
5961(3)	6009(3)	6013(3)	6041(3)
6117(3)	6159(3)	6181(3)	6209(3)
6297(3)	6351(3)	6377(3)	6433(3)
6495(3)	6692(3)	6707(3)	6717(3)
6797(3)	6801(3)	6819(3)	6881(3)
6913(3)	6985(3)	6995(3)	7113(3)
7133(3)	7167(3)	7197(3)	7273(3)
7441(3)	7593(3)	7721(3)	7861(3)
8061(3)	8309(3)	8417(3)	8529(3)
8561(3)	8637(3)	8781(3)	8889(3)
8913(3)	8997(3)	9037(3)	9101(3)
9121(3)	9249(3)	9253(3)	9329(3)
9489(3)	9641(3)	9741(3)	9937(3)
9989(3)			

Similarly, candidates for new orders of complex Hadamard matrices are shown below.

35(2)	47(4)	65(4)	67(5)	71(2)	77(2)	103(3)
111(2)	119(2)	131(2)	133(2)	143(4)	151(5)	155(2)
161(2)	163(3)	165(2)	167(4)	171(2)	179(8)	183(2)
185(6)	203(2)	207(2)	209(2)	213(2)	215(2)	219(2)
221(6)	223(3)	227(4)	235(3)	237(2)	239(4)	245(4)
247(2)	249(2)	251(6)	259(2)	263(2)	267(2)	269(8)
273(2)	275(2)	287(2)	291(2)	295(5)	299(4)	303(2)
305(8)	319(3)	323(2)	329(2)	333(3)	341(2)	343(2)
345(2)	357(2)	359(4)	369(4)	371(2)	383(2)	391(5)
393(2)	395(2)	403(2)	407(2)	413(2)	417(2)	419(4)
425(2)	431(6)	437(2)	443(6)	445(3)	447(2)	453(2)
455(2)	463(7)	467(2)	475(2)	483(4)	485(4)	487(5)
493(7)	495(2)	497(2)	501(2)	503(2)	513(2)	519(2)
523(7)	527(2)	533(2)	537(2)	539(4)	551(2)	553(2)
563(4)	567(2)	571(3)	573(2)	575(2)	581(2)	583(3)
585(2)	587(6)	589(2)	595(3)	603(2)	605(2)	611(6)
621(2)	623(2)	633(2)	635(2)	637(2)	655(5)	657(5)
665(2)	669(2)	671(2)	679(2)	683(2)	693(2)	695(2)
697(5)	699(2)	707(2)	711(2)	713(2)	719(4)	721(2)
723(2)	725(6)	743(4)	749(2)	751(3)	753(2)	755(2)
763(2)	765(2)	767(2)	771(2)	779(2)	781(3)	783(2)
787(5)	789(2)	791(2)	793(3)	795(2)	813(2)	815(2)
817(2)	825(2)	827(2)	831(2)	833(4)	837(2)	853(3)
857(4)	859(3)	863(4)	869(2)	873(3)	875(2)	887(6)
891(2)	893(2)	897(5)	899(2)	903(4)	905(4)	907(5)
909(4)	911(2)	915(2)	917(2)	919(3)	921(2)	923(4)
927(4)	933(2)	935(2)	941(6)	947(6)	949(3)	955(5)
959(2)	963(3)	965(4)	969(2)	971(6)	973(2)	979(5)
981(2)	983(4)	985(3)	989(4)	991(3)	993(2)	995(2)

6.3 Constant Weight Codes

We remind the reader that a code over a finite alphabet $\mathcal{A}$, including the symbol 0, is a subset $C \subseteq \mathcal{A}$. The reader is referred back to §2.3 for the relavent definitions. In this section, we will consider those codes in which the alphabet $\mathcal{A}$ is $G \cup \{0\}$, where G is some finite cyclic group. A code C is called *constant weight*, if there is some k such that $\mathrm{wt}(\mathbf{x}) = k$, for every $\mathbf{x} \in C$. The simplex codes used to construct the BGW matrices in §3.3 are an example of a constant weight code. We apply BGW matrices to these codes in the following result.

Theorem 6.15. Let q be a prime power, and let $S = \langle \omega \rangle$ be a finite cyclic group such that $|S|$ divides $q - 1$. Let g be the ω-circulant matrix with first row $(0, 1, 0, \ldots, 0)$ of order n, and let $G = \langle g \rangle$. Take W to be any $\mathrm{BGW}(v, k, \lambda; G)$. Then the rows of W form a constant weight (vn, vn, d)-code where the following hold.

i. $\mathrm{wt}(\mathbf{x}) = k$, and

ii. $d = \min\left\{2k, 2(k-\lambda) + \frac{\lambda(|S|-1)}{n|S|}\right\}$.

Proof. Let X be the matrix obtained from W by setting all of the non-zero

entries equal to 1. Then

$$XX^* = k + \frac{\lambda}{n}(J - I). \tag{6.1}$$

Consider W as an $nv \times nv$ matrix, and let x and y be any two distinct rows of W. If x and y are from the same block row of the BGW W, then clearly $d(x, y) = 2k$. Otherwise, consider the concatenation $\left[\frac{x}{y}\right]$. It follows that

$$\begin{array}{l} 0\;0\;1\;0\;\omega \ldots \omega^{|\omega|-1}\quad 0\quad \overbrace{1\;\omega\ldots\omega^{|\omega|-1}\;\;1\ldots 1\;\;\omega\ldots\omega\;\ldots\omega^{|\omega|-1}\ldots\omega^{|\omega|-1}}^{\frac{\lambda}{n}} \\ 0\;1\;0\;\omega\;0\ldots\quad 0\quad \omega^{|\omega|-1}\;\;1\;\omega\ldots\omega^{|\omega|-1}\;\;\underbrace{\omega\ldots\omega^{|\omega|-1}\;\;1\ldots\omega^{|\omega|-1}\ldots 1\ldots\omega^{|\omega|-2}}_{\frac{\lambda(|\omega|-1)}{n|\omega|}} \end{array}$$

The result follows immediately. *Q.E.D.*

Corollary 6.16. Let $\langle\omega\rangle = \mathbb{F}_p^\times$, and let W be a BGW$((q^{d+1} - 1)/(q - 1), q^d, q^d - q^{d-1})$ over $\mathbb{F}_q^*$ such that $n(p-1) \mid q-1$. Taking $v = (q^{d+1} - 1)/(q-1)$, there is a constant weight (nv, nv, d)-linear code, where:

(i) $w = q^d$, and

(ii) $d = \min\left\{2q^d, 2\left(q^d - \frac{q^d - q^{d-1}}{n}\right) + \frac{(q^d - q^{d-1})(p-2)}{n(p-1)}\right\}$.

Proof. We have used the fact that there are BGW's with parameters $(q^{d+1} - 1)/(q-1), q^d, q^d - q^{q-1})$ over a cyclic group of order $q - 1$ for every prime power q. Since $\sum_{i=0}^{|\omega|-1} g^i = 0$, it follows that $WW^* = kI$; whence, W is invertible. *Q.E.D.*

A cyclic code C is a code in which the cyclic shift of every code word is also in C. As a final application, we have the following.

Theorem 6.17. If there is a cyclic $(n-1, d)$-code over an alphabet of cardinality s, where n is a prime power, then there is a constant weight $(n^m - 1, d')$-code of weight $(n-1)n^{m-1}$ over an alphabet of cardinality $s + 1$, where $d' \geq 2(n-1)n^{m-2}$, for any positive integer $m \geq 2$.

Proof. The automorphism group of a cyclic $(n-1, d)$-code admits a cyclic subgroup of order $n - 1$ acting on the code by shifting the coordinate positions. Assume the alphabet is given by the set $\{1, 2, \ldots, s\}$. Since n is a prime power, there is a BGW$((n^m - 1)/(n-1), n^{m-1}, n^{m-1} - n^{m-2})$, say $W = [w_{ij}]$, over this cyclic subgroup. Then the matrix $[w_{ij}C]$ can be regarded as a code with the required parameters over the alphabet $\{0, 1, 2, \ldots, s\}$. *Q.E.D.*

Theorem 6.15, in the case of binary, constant weight codes produces the following interesting reproductions.

Example 6.18. The following minimum bounds were reproduced for small parameter constant weight, binary codes using the above theorem, where we have used $\mathrm{A}(n, w, d)$ to denote the maximum number of words in an $(n, d)_2$-code of constant weight w:

$$\begin{aligned}
\mathrm{A}(8,3,4) &\geq 8 & \mathrm{A}(24,7,10) &\geq 24\\
\mathrm{A}(12,5,6) &\geq 12 & \mathrm{A}(40,9,14) &\geq 40\\
\mathrm{A}(15,4,6) &\geq 15 & \mathrm{A}(48,7,12) &\geq 48\\
\mathrm{A}(16,7,8) &\geq 16 & \mathrm{A}(63,8,14) &\geq 63\\
\mathrm{A}(20,9,10) &\geq 20 & \mathrm{A}(80,9,16) &\geq 80\\
\mathrm{A}(24,5,8) &\geq 24
\end{aligned}$$

6.4 Notes

The results of this section were all novel constructions. In determining the new orders of real Hadamard matrices, the derived parameters were compared with the tables found in Craigen, Kharaghani [CK07]. The putative orders for new complex Hadamard matrices displayed in the previous section were compared to the tables found in Seberry, Yamada [SY92].

The values for $\mathrm{A}(n, w, d)$, reproduced in §6.3, are found in Brouwer [Bro].

Bibliography

[AKP07] Sarah Spence Adams, Nathaniel Karst, and Jonathan Pollack. The minimum decoding delay of maximum rate complex orthogonal space-time block codes. *IEEE Trans. Inform. Theory*, 53(8):2677–2684, 2007.

[Bat97] Lynn Margaret Batten. *Combinatorics of finite geometries.* Cambridge University Press, Cambridge, second edition, 1997.

[BCN89] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-regular graphs*, volume 18 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)].* Springer-Verlag, Berlin, 1989.

[Ber78] Gerald Berman. Families of generalized weighing matrices. *Canadian J. Math.*, 30(5):1016–1028, 1978.

[BJL99a] Thomas Beth, Dieter Jungnickel, and Hanfried Lenz. *Design theory. Vol. I*, volume 69 of *Encyclopedia of Mathematics and its Applications.* Cambridge University Press, Cambridge, second edition, 1999.

[BJL99b] Thomas Beth, Dieter Jungnickel, and Hanfried Lenz. *Design theory. Vol. II*, volume 78 of *Encyclopedia of Mathematics and its Applications.* Cambridge University Press, Cambridge, second edition, 1999.

[Bro] A. E. Brouwer. *Homepage.* https://www.win.tue.nl/ aeb/.

[But62] A. T. Butson. Generalized Hadamard matrices. *Proc. Amer. Math. Soc.*, 13:894–898, 1962.

[But63] A. T. Butson. Relations among generalized Hadamard matrices, relative difference sets, and maximal length linear recurring sequences. *Canadian J. Math.*, 15:42–48, 1963.

[Cam94] Peter J. Cameron. *Combinatorics: topics, techniques, algorithms.* Cambridge University Press, Cambridge, 1994.

[CK07] Robert Craigen and Hadi Kharaghani. Hadamard matrices and hadamard designs. *Handbook of Combinatorial Designs*, pages 273–280, 2007.

[CvL91] P. J. Cameron and J. H. van Lint. *Designs, graphs, codes and their links*, volume 22 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.

[DEBŻ10] Thomas Durt, Berthold-Georg Englert, Ingemar Bengtsson, and Karol Życzkowski. On mutually unbiased bases. *International journal of quantum information*, 8(04):535–640, 2010.

[Del68] P. Delsarte. Orthogonal matrices over a group and related tactical configurations. *M.B.L.E. Report R90*, 1968.

[Dem97] Peter Dembowski. *Finite geometries*. Classics in Mathematics. Springer-Verlag, Berlin, 1997. Reprint of the 1968 original.

[DGS71] P. Delsarte, J.-M. Goethals, and J. J. Seidel. Orthogonal matrices with zero diagonal. II. *Canadian J. Math.*, 23:816–832, 1971.

[Dra79] David A. Drake. Partial λ-geometries and generalized Hadamard matrices over groups. *Canadian J. Math.*, 31(3):617–627, 1979.

[Fis40] R. A. Fisher. An examination of the different possible solutions of a problem in incomplete blocks. *Ann. Eugenics*, 10:52–75, 1940.

[FKS18] Kai Fender, Hadi Kharaghani, and Sho Suda. On a class of quaternary complex Hadamard matrices. *Discrete Math.*, 341(2):421–426, 2018.

[Had93] J. Hadamard. Resolution d'une question relative aux determinants. *Bull. des Sciences Math.*, 2:240–246, 1893.

[Hal86] Marshall Hall, Jr. *Combinatorial theory*. Wiley-Interscience Series in Discrete Mathematics. John Wiley & Sons, Inc., New York, second edition, 1986. A Wiley-Interscience Publication.

[Hor07] K. J. Horadam. *Hadamard matrices and their applications*. Princeton University Press, Princeton, NJ, 2007.

[Hot44] Harold Hotelling. Some improvements in weighing and other experimental techniques. *Ann. Math. Statistics*, 15:297–306, 1944.

[HPOCP20] Philip Heikoop, Guillermo Nuñez Ponasso, Padraig Ó Catháin, and John Pugmire. Morphisms of skew Hadamard matrices. *Bull. Inst. Combin. Appl.*, 90:50–62, 2020.

[Hur22] A. Hurwitz. Über die Komposition der quadratischen Formen. *Math. Ann.*, 88(1-2):1–25, 1922.

[IK03a] Yury J. Ionin and Hadi Kharaghani. Doubly regular digraphs and symmetric designs. *J. Combin. Theory Ser. A*, 101(1):35–48, 2003.

[IK03b] Yury J. Ionin and Hadi Kharaghani. New families of strongly regular graphs. *J. Combin. Des.*, 11(3):208–217, 2003.

[Ion01] Yury J. Ionin. Applying balanced generalized weighing matrices to construct block designs. *Electron. J. Combin.*, 8(1):Research Paper 12, 15, 2001.

[IS06] Yury J. Ionin and Mohan S. Shrikhande. *Combinatorics of symmetric designs*, volume 5 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006.

[JK04] Dieter Jungnickel and H. Kharaghani. Balanced generalized weighing matrices and their applications. *Matematiche (Catania)*, 59(1-2):225–261 (2006), 2004.

[JT99] Dieter Jungnickel and Vladimir D. Tonchev. Perfect codes and balanced generalized weighing matrices. *Finite Fields Appl.*, 5(3):294–300, 1999.

[JT02] Dieter Jungnickel and Vladimir D. Tonchev. Perfect codes and balanced generalized weighing matrices. II. *Finite Fields Appl.*, 8(2):155–165, 2002.

[Kha03] H. Kharaghani. On a class of symmetric balanced generalized weighing matrices. *Des. Codes Cryptogr.*, 30(2):139–149, 2003.

[Lev61] V. I. Levenshtein. Application of hadamard matrices on coding problem. *Problems of Cybernetica*, 5:123–136, 1961.

[Maj53] Kulendra N. Majumdar. On some theorems in combinatorics relating to incomplete block designs. *Ann. Math. Statistics*, 24:377–389, 1953.

[Mit13] M. Mitrouli. Sylvester Hadamard matrices revisited. *Spec. Matrices*, 1:120–124, 2013.

[MS77a] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. I.* North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. North-Holland Mathematical Library, Vol. 16.

[MS77b] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. II.* North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. North-Holland Mathematical Library, Vol. 16.

[Pal33] R. E. A. C. Paley. On orthogonal matrices. *Journal of Mathematics and Physics*, 12(1-4):311–320, 1933.

[Rad22] J. Radon. Lineare Scharen orthogonaler Matrizen. *Abh. Math. Sem. Univ. Hamburg*, 1(1):1–14, 1922.

[Raj83] Dinesh P. Rajkundlia. Some techniques for constructing infinite families of BIBDs. *Discrete Math.*, 44(1):61–96, 1983.

[Ros00] Kenneth H. Rosen. *Elementary number theory and its applications*. Addison-Wesley, Reading, MA, fourth edition, 2000.

[Sah13] Prasanna Sahoo. Probability and mathematical statistics. *University of Louisville*, 2013.

[Seb17] Jennifer Seberry. *Orthogonal designs*. Springer, Cham, 2017. Hadamard matrices, quadratic forms and algebras, Revised and updated edition of the 1979 original [MR0534614].

[Shr64] S. S. Shrikhande. Generalized Hadamard matrices and orthogonal arrays of strength two. *Canadian J. Math.*, 16:736–740, 1964.

[Shr76] S. S. Shrikhande. Affine resolvable balanced incomplete block designs: a survey. *Aequationes Math.*, 14(3):251–269, 1976.

[Sti04] Douglas R. Stinson. *Combinatorial designs*. Springer-Verlag, New York, 2004. Constructions and analysis, With a foreword by Charles J. Colbourn.

[SY92] Jennifer Seberry and Mieko Yamada. Hadamard matrices, sequences, and block designs. In *Contemporary design theory*, Wiley-Intersci. Ser. Discrete Math. Optim., pages 431–560. Wiley, New York, 1992.

[Syl67] J.J. Sylvester. Lx. thoughts on inverse orthogonal matrices, simultaneous signsuccessions, and tessellated pavements in two

or more colours, with applications to newton's rule, ornamental tile-work, and the theory of numbers. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 34(232):461–475, 1867.

[Ton09] Vladimir D. Tonchev. Generalized weighing matrices and self-orthogonal codes. *Discrete Math.*, 309(14):4697–4699, 2009.

[vL99] J. H. van Lint. *Introduction to coding theory*, volume 86 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, third edition, 1999.

Index of Terms

Index of Notations

Standard Set Notations

$\mathbb{Z}$: The ring of integers.
$\mathbb{Q}$: The field of rational numbers.
$\mathbb{R}$: The field of real numbers.
$\mathbb{C}$: The field of complex numbers.
$\mathbb{T}$: The multiplicative group of unimodular complex numbers.
$S_+ = \{s \in S \mid s > 0\}$, for $S \subseteq \mathbb{R}$.
$S_- = \{s \in S \mid s < 0\}$, for $S \subseteq \mathbb{R}$.
Z_n is the cyclic group of order n.

Matrices and Vectors

I: The multiplicative identity for a ring of square matrices.
J: The matrix whose entries are either a group identity or the multiplicative identity of some ring.
R: The back identity; the matrix whose anti-diagonal consists of unity, and whose off-diagonal entries are 0.
$\mathbf{0}$: The vector whose entries are all 0.
$\mathbf{j}$: The vector whose entries consist of either a group identity or the multiplicative identity of some ring.

Binary Operations

$\_ \otimes \_$: The Kronecker product.
$\_ * \_$: The Hadamard product.