WEIGHING MATRICES: GENERALIZATIONS, RELATED CONFIGURATIONS

THOMAS PENDER
BACHELOR OF SCIENCE, UNIVERSITY OF LETHBRIDGE, 2020

A thesis submitted
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

in

MATHEMATICS

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

WEIGHING MATRICES: GENERALIZATIONS, RELATED CONFIGURATIONS

THOMAS PENDER

Date of Defence:

Dr. H. Kharaghani Thesis Supervisor	Professor	Ph.D.
Dr. W. Holzmann Thesis Examination Committee Member	Professor	Ph.D.
Dr. M. Walton Thesis Examination Committee Member	Professor	Ph.D.

DEDICATION

To my wife and son who changed everything.

ABSTRACT

It is the purpose of this thesis to explore the relationships that exist between weighing matrices, including their generalizations, and various other combinatorial configurations.

Principally, it will be shown that any balanced generalized weighing matrix with entries from a finite abelian group is equivalent to the existence of families of commutative association schemes.

Additionally, novel constructions of related combinatorial configurations are presented such as balancedly splittable orthogonal designs and new families of balanced weighing matrices.

PREFACE

ACKNOWLEDGEMENTS

I would like to thank Dr. H. Kharaghani for his remarkable teaching prowess and his singular patience. There can be no doubt that if I have found any success during my studies, it is precisely because of my teacher, Hadi.

Furthermore, thanks are owed to Dr. S. Suda who, with an abundance of charity, agreed to include me in his collaboration with Dr. H. Kharaghani.

Finally, I would like to recognize the Department of Mathematics and Computer Science of the University of Lethbridge. Truly, here is a group of talented individuals with a passion for teaching and sharing their expertise.

Contents

LIST OF SYMBOLS

$\mathbf{N}$	The additive semigroup of natural numbers $\{0, 1, 2 \dots\}$.
$\mathbf{Z}$	The ring of integers $\{0, \pm 1, \pm 2, \dots\}$.
$\mathbf{Q}$	The rational number field $\{\frac{n}{m} : n, m \in \mathbf{Z}\}$.
$\mathbf{R}$	The real number field.
$\mathbf{C}$	The complex number field $\{x + y\sqrt{-1} : x, y \in \mathbf{R}\}$.
$\mathbf{Z}/n\mathbf{Z}$	The integers modulo n $\{\overline{0}, \dots, \overline{n-1}\}$.
GF(q)	The Galois field of q elements.
$\mathbf{D} = (X, \mathscr{B})$	A balanced incomplete block design with point set X and block set $\mathscr{B}$.
BIBD(v, k, λ)	A balanced incomplete block design with associated parameters.
$\mathfrak{C}(\mathbf{D})$	Complementary design of $\mathbf{D}$.
$\mathfrak{R}(\mathbf{D})$	Residual design of $\mathbf{D}$.
$\mathfrak{D}(\mathbf{D})$	Derived design of $\mathbf{D}$.
$A(\mathbf{D})$	Incidence matrix of the design $\mathbf{D}$.
GDD$(m, n, k, \lambda_1, \lambda_2)$	A group divisible design with associated parameters.
DS(v, k, λ)	A difference set of size k on a group of order v with index λ.
Dev(D)	The development of the set D.
D(m, q)	Singer difference set.
RDS(m, n, k, λ)	A relative difference set of size k, on a group of order mn, with index λ, and relative to a normal subgroup of order n.
P(m, q)	The projective space of dimension m.
$[n, k, d, w]_q$-code	A linear code in GF(q^n) of dimension k, minimum distance d, and minimum weight w.
$(n, M, d, w)_q$-code	A nonlinear code in an alphabet of q letters of length n, with M codewords, minimum distance d, and minimum weight w.
A$_q(n, d, w)$	The maximum size of any $(n, M, d, w)_q$-code, i.e. $M \leq \mathrm{A}_q(n, d, w)$.
W(v, k)	A weighing matrix of order v and weight k.
BW$(v, k; n)$	A Butson weighing matrix of order v and weight k over the n-th roots of unity.
GW$(v, k; G)$	A generalized weighing matrix of order v and weight k over the finite group G.
GBRD$(v, k, \lambda; G)$	A generalized Bhaskar Rao design over the finite group G with associated parameters.

BGW$(v, k, \lambda; G)$	A balanced generalized weighing matrix of order v, weight k, and index $\lambda/\lvert G\rvert$, over the finite group G.
SRG(v, k, λ, μ)	A strongly regular graph with associated parameters.
$A(\Gamma)$	The adjacency matrix of the graph Γ.
$\mathfrak{X} = (X, \mathscr{R})$	An association scheme with point set X and relations $\mathscr{R}$.
$\tau(A)$	The sum of the elements of the matrix A.
Tr(A)	The sum of the diagonal elements of the matrix A.
$\mathscr{S}_{q,n}$	A generalized simplex code.
$\mathscr{H}_{q,n}$	A generalized Hamming code.
$A \otimes B$	The Kronecker product of A by B.

Part I

Preliminaries

1

A Study of Incidence: Block designs, error-correcting codes

This first preliminary chapter introduces incidence in the context of two different but related objects. The first section will discuss the fundamental incidence structure underlying our constructions, namely, the balanced incomplete block designs. The second and final section moves on to consider in brief error-correcting codes.

§1. Balanced Incomplete Block Designs

This section presents some basic definitions and results about block designs that will be used throughout this work. Particular emphasis will be placed on matrix representations of such objects.

* * *

1.1. Definition and Necessary Parametric Conditions. Consider the following example (see MacWilliams and Sloane, 1977, §2.5). From a group of individuals, we must choose a number of committees, each of identical size, such that the appearances of each of the individuals among the various committees are equinumerous, as are the appearances of each of the t-subsets of the individuals. To be concrete, given eight individuals, can we arrange them into some number of committees of size four such that each individual is replicated the same number of times, and such that each triple of individuals is replicated precisely once.

This problem is solved by the following configuration where $\{a, b, c, d, e, f, g, h\}$ is our collection of individuals. The groups, or committees, are given by the following.

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

This configuration is an example of a so-called t-design. The case that $t = 2$ is the case with which we will concern ourselves. In what follows, we use $\binom{X}{k}$ to denote the k-subsets of a set X.

1.1. Definition. Let X be a set of order v, called the set of varieties; and let $\mathscr{B} \subset \binom{X}{k}$, called the set of blocks, have order b. The ordered pair $\mathbf{D} = (X, \mathscr{B})$ is a *balanced incomplete block design* (henceforth BIBD) if there is a positive integer λ such that each 2-subset of varieties appears in λ blocks of $\mathscr{B}$.

The conditions placed on a finite set and a collection of its subsets in order to form a BIBD are quite strong, and we have at once the following result.

1.2. Proposition. Let $\mathbf{D} = (X, \mathscr{B})$ be a BIBD with $|X| = v$, and $\mathscr{B} \subset \binom{X}{k}$ for which $|\mathscr{B}| = b$. Then:

(1.2.a) Every point of X occurs in $r = \frac{\lambda(v-1)}{k-1}$ blocks, and

(1.2.b) there are $b = \frac{vr}{k} = \frac{\lambda v(v-1)}{k(k-1)}$ blocks in $\mathscr{B}$.

Proof. Let $x \in X$, and take $r_x = \#\{B \in \mathscr{B} : B \ni x\}$. We count in two ways the number of ordered pairs (y, B) such that $y \in X \backslash \{x\}$, $B \in \mathscr{B}$, and $\{x, y\} \in B$.

To begin, there are $v - 1$ ways to choose y different from x. For each choice of y, there are λ blocks B which contain both x and y. On the other hand, there are r_x ways to choose B, and there are $k - 1$ remaining points in B different from x.

We have just shown that $r_x(k - 1) = \lambda(v - 1)$. Since this argument was independent of the choice of x, this shows (1.2.a).

Recall $b = |\mathscr{B}|$. As above, we will employ double counting; we will count the number of ordered pairs (x, B) such that $x \in X$, $B \in \mathscr{B}$ and $x \in B$.

First, there are b blocks, and, for each block, there are k points in this block. Second, there are v points, and, for each point, we have already shown that there are r blocks containing this point. All this shows that $bk = vr$. Substituting (1.2.a) into this result yields the final equality in (1.2.b). ∎

Since these parameters are integers, we have the following immediate consequence.

1.3. Corollary. For the parameters v, k, λ of a BIBD, it must hold that

(1.3.a) $\lambda(v - 1) \equiv 0 \bmod (k - 1)$, and

(1.3.b) $\lambda v(v - 1) \equiv 0 \bmod k(k - 1)$.

If $\mathbf{D} = (X, \mathscr{B})$ is a BIBD with the parameters shown above, then we denote this property as BIBD(v, b, r, k, λ). As we have seen, however, the parameters b and r are expressible in terms of v, k, and λ; hence, we will usually shorten the denotation to BIBD(v, k, λ) whenever no confusion will arise.

Corollary 1.3 imposes some necessary conditions on the parameters of a BIBD. Our next result, due to Fisher (1940), is a strong necessary condition relating the number of points to the number of blocks of a BIBD, and it has far reaching consequences in the applications of designs to fields like statistics.

1.4. Fisher's Inequality. Let $\mathbf{D} = (X, \mathscr{B})$ be a BIBD(v, b, r, k, λ). It follows that

(1.4.a) $b \geq v$.

Proof. We will apply the technique of variance counting[1]) as given in Cameron (1994). Let $B \in \mathscr{B}$, and, for $i \in \{0, \ldots, k\}$, let

$$n_i = \#\{B' \in \mathscr{B} : B' \neq B \text{ and } |B \cap B'| = i\}.$$

Since there are $b - 1$ blocks distinct from B, we have immediately that $\sum_i n_i = b - 1$.

We next count pairs (x, B') where $x \in X$, $B' \in \mathscr{B}$ with $B' \neq B$, and $x \in B' \cap B$. First, there are k points x in B, and there are $r - 1$ remaining blocks B' that contain x. Second, there are n_i blocks B' for which there are x points in $B \cap B'$. This establishes the equality $\sum_i i n_i = k(r - 1)$.

Counting triples (x_1, x_2, B') where $x_1 \neq x_2$, $B' \neq B$, and $x_1, x_2 \in B \cap B'$, we see that there are k choices for x_1, $k - 1$ choices for x_2, and $\lambda - 1$ blocks B' different from B that contain both points. Second, if $|B \cap B'| = i$, then there are i choices for x_1, $i - 1$ choices for x_2, and there are n_i such blocks B'. Hence, we have $\sum_i i(i-1)n_i = k(k-1)(\lambda-1)$.

Using the equalities just derived, we find that $\sum_{i=0}^{k} i^2 n_i = k(r-1) + k(k-1)(\lambda-1)$, hence

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

for some variable z. From the left-hand side, it follows that the quadratic is positive semi-definite; so, the discriminant of the right-hand side is non-positive, that is,

$$k^2(r-1)^2 - (b-1)k[(r-1) + (k-1)(\lambda-1)] \leq 0.$$

Using (1.2.a) and (1.2.b), and multiplying by $v-1$, the above equality becomes

$$k^2(r-1)^2(v-1) - (vr-k)(r-k)(v-1) - (vr-k)r(k-1)^2 \leq 0.$$

This simplifies to $(k-r)r(v-k)^2 \leq 0$; and, since $r > 0$ and $(v-k)^2 > 0$, it follows that $k \leq r$. Again using (1.2.b), it must be that $v \leq b$, as desired. ∎

The extremal case of Fisher's inequality is naturally very interesting and important. We single this case out thus.

1.5. Definition. Let $\mathbf{D} = (X, \mathscr{B})$ be some BIBD(v, b, r, k, λ). If $v = b$ (equiv. $k = r$), then we say that $\mathbf{D}$ is a *symmetric* balanced incomplete block design, or simply symmetric.

1.6. Example. Take $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$, and let $\mathscr{B}$ be the collection of blocks given by

$\{1, 2, 8, 13\}$,	$\{2, 7, 9, 10\}$,	$\{1, 3, 4, 7\}$,
$\{4, 8, 10, 11\}$,	$\{2, 4, 5, 6\}$,	$\{6, 7, 8, 12\}$,

$$\{5,7,11,13\}, \qquad \{3,5,8,9\}, \qquad \{1,6,9,11\},$$
$$\{1,5,10,12\}, \qquad \{2,3,11,12\}, \qquad \{4,9,12,13\},$$
$$\{3,6,10,13\}.$$

Then $\mathbf{D} = (X, \mathscr{B})$ is a symmetric BIBD$(13, 4, 1)$; in fact, it is a projective plane of order 3 (see §1.3).

* * *

1.2. Related Configurations. Thus far, we have been thinking of designs strictly as subsets of some finite set. We can, however, broaden our view to include the following tool, and in so doing the theory of linear algebra can be brought to bear on the subject.

1.7. Definition. Let $\mathbf{D} = (\{x_0, \ldots, x_{v-1}\}, \{B_0, \ldots, B_{b-1}\})$ be a BIBD(v, b, r, k, λ), and let A be a $v \times b$ $(0,1)$-matrix defined by

(1.7.a) $A_{ij} = \begin{cases} 1 & \text{if } x_i \in B_j, \text{ and} \\ 0 & \text{if } x_i \notin B_j. \end{cases}$

We call A the *incidence matrix* of the design.

The next result is immediate. Note that we use I_n and J_n to denote the identity matrix and the all ones matrix, respectively, of n rows and n columns. Similarly, $\mathbf{1}_n$ and $\mathbf{0}_n$ will denote the column with n ones and the column with n zeros. For simplicity, the indices will at times be omitted.

1.8. Proposition. Let $\mathbf{D} = (\{x_0, \ldots, x_{v-1}\}, \{B_0, \ldots, B_{b-1}\})$ be a BIBD(v, b, r, k, λ), and let A be a $v \times b$ $(0,1)$-matrix. Then A is the incidence matrix of the design if and only if the following hold.

(1.8.a) $AA^t = rI_v + \lambda(J_v - I_v)$, and

(1.8.b) $\mathbf{1}_v^t A = k\mathbf{1}_b^t$.

Proof. To show sufficiency, assume that A is the incidence matrix of a BIBD(v, b, r, k, λ) with rows indexed as $r_0, \ldots, r_{v-1}$. Then $r_i r_i^t = \sum_k A_{ik}^2 = \sum_k A_{ik}$. Since there are r blocks containing the point x_i, it follows that there are r indices k for which $A_{ik} = 1$; hence, $r_i r_i^t = r$.

Similarly, for $i \neq j$, we have $r_i r_j^t = \sum_k A_{ik} A_{jk}$. Since there are λ blocks containing the 2-subset $\{x_i, x_j\}$, it follows that there are λ indices k such that $A_{ik} = A_{jk} = 1$. We have, then, $r_i r_j^t = \lambda$, and (1.8.a) holds.

Finally, (1.8.b) is clear since there are k points in every block. Necessity follows by simply transposing the above argument. ∎

To show the utility of the incidence matrices, we will give a necessary and sufficient condition under which a design can be symmetric (see Cameron and van Lint, 1991, Theorem 1.14).

1.9. Proposition. For a BIBD(v, b, r, k, λ) with $k < v$, the following are equivalent.

(1.9.a) $b = v$;

(1.9.b) $r = k$;

(1.9.c) any two blocks intersect at λ points; and

(1.9.d) any two blocks intersect at a constant number of points.

Proof. That (1.9.a) $\Leftrightarrow$ (1.9.b) is clear. To show (1.9.b) $\Rightarrow$ (1.9.c), let A be the incidence matrix of the design. Then Proposition 1.8 shows that $A^t J = J A^t = kJ$, hence A^t commutes with $rI + \lambda(J - I)$ and with $[rI + \lambda(J - I)](A^t)^{-1} = A$. Therefore, $A^t A = rI + \lambda(J - I)$, which demonstrates the implication.

Since (1.9.c) $\Rightarrow$ (1.9.d) is trivial, it remains to show (1.9.d) $\Rightarrow$ (1.9.a). To do this, we will need the concept of a dual design: If $(X, \mathscr{B})$ is a BIBD, then its dual is the pair $(X^t, \mathscr{B}^t)$ where $X^t = \mathscr{B}$ and $\mathscr{B}^t = \{\beta_x : x \in X\}$, with $\beta_x = \{B \in B : B \ni x\}$.

Clearly, the dual structure is again a design if and only if (1.9.d) holds. An application of (1.4.a) then yields (1.9.a). ∎

As balanced incomplete block designs can more generally be regarded as finite incidence structures[2]), there can be related a number of further such structures. For our purposes, we will be interested in the following.

1.10. Definition. Let $\mathbf{D} = (X, \mathscr{B})$ be a BIBD, and let $B \in \mathscr{B}$. Then the *complement design* $\mathfrak{C}(\mathbf{D})$ is the pair $(X, \binom{X}{k} \backslash \mathscr{B})$. If $\mathbf{D}$ is symmetric, we have that the *derived design* $\mathfrak{D}(\mathbf{D})$ is the pair $(B_0, \{B \cap B_0 : B \in \mathscr{B}$ and $B \neq B_0\})$, and the *residual design* $\mathfrak{R}(\mathbf{D})$ is the pair $(X \backslash B_0, \{B - B_0 : B \in \mathscr{B}$ and $B \neq B_0\})$. When convenient, we will simply denote the complement, derived, and residual designs as $\mathfrak{C}$, $\mathfrak{D}$, and $\mathfrak{R}$, respectively.

The next result is immediate.

1.11. Proposition. Let $\mathbf{D} = (X, \mathscr{B})$ be a BIBD(v, b, r, k, λ). Then

(1.11.a) $\mathfrak{C}$ is a BIBD$(v, b, b-r, v-k, b-2r+\lambda)$.

If $\mathbf{D}$ is symmetric, then we further have that

(1.11.b) $\mathfrak{D}$ is a BIBD$(k, b-1, k-1, \lambda, \lambda-1)$, and

(1.11.c) $\mathfrak{R}$ is a BIBD$(v-k, b-1, k, k-\lambda, \lambda)$.

Proof. The result is most easily seen using incidence matrices. To that effect, assume $\mathbf{D}$ is symmetric, let A be its incidence matrix, and note that by permuting the rows and columns, we may assume (see §1.4) that it has the form

$$A = \begin{pmatrix} \mathbf{0}_{v-k} & A_1 \\ \mathbf{1}_k & A_2 \end{pmatrix}.$$

Then A_1 and A_2 are the incidence matrices of the derived and residual designs of $\mathbf{D}$. (1.11.b) and (1.11.c) now follow.

It remains to note that $\mathfrak{C}$ has the incidence matrix $J - A$ (where the design is not assumed to be symmetric here), and (1.11.a) follows. ∎

Notice that for $\mathfrak{R}$, $r = \lambda + k$; and for $\mathfrak{D}$, $k = \lambda + 1$. Conversely, if there is a BIBD(v, b, r, k, λ) satisfying $r = k + \lambda$, then we say that it is *quasi-residual*; if instead $k = \lambda + 1$, then we say that it is *quasi-derived*.

* * *

1.3. Difference Set Construction I. To present a unifying thread of the material in these preliminary chapters, we will introduce the concept of a difference set. We first look to the following example given in Hall (1986).

Consider the subset $D = \{\overline{1}, \overline{5}, \overline{6}, \overline{8}\}$ of $\mathbf{Z}/13\mathbf{Z}$. We examine the possible differences between distinct elements of D.

$$\begin{aligned}
\overline{1} &= \overline{6} - \overline{5}, & \overline{7} &= \overline{8} - \overline{1},\\
\overline{2} &= \overline{8} - \overline{6}, & \overline{8} &= \overline{1} - \overline{6},\\
\overline{3} &= \overline{8} - \overline{5}, & \overline{9} &= \overline{1} - \overline{5},\\
\overline{4} &= \overline{5} - \overline{1}, & \overline{10} &= \overline{5} - \overline{8},\\
\overline{5} &= \overline{6} - \overline{1}, & \overline{11} &= \overline{6} - \overline{8},\\
\overline{6} &= \overline{1} - \overline{8}, & \overline{12} &= \overline{5} - \overline{6}.
\end{aligned}$$

We see that each element of $(\mathbf{Z}/13\mathbf{Z})\backslash\{\overline{0}\} = \{\overline{1}, \ldots, \overline{12}\}$ appears precisely once as a difference of elements of D. To see the significance of such a configuration, consider now the translates $B_x = \overline{x} + D$, for $\overline{x} \in \mathbf{Z}/13\mathbf{Z}$. In ascending order,

$$B_0 = \{\overline{1}, \overline{5}, \overline{6}, \overline{8}\}, \qquad B_7 = \{\overline{0}, \overline{2}, \overline{8}, \overline{12}\},$$

$$B_1 = \{\overline{2}, \overline{6}, \overline{7}, \overline{9}\}, \qquad B_8 = \{\overline{0}, \overline{1}, \overline{3}, \overline{9}\},$$

$$B_2 = \{\overline{3}, \overline{7}, \overline{8}, \overline{10}\}, \qquad B_9 = \{\overline{1}, \overline{2}, \overline{4}, \overline{10}\},$$

$$B_3 = \{\overline{4}, \overline{8}, \overline{9}, \overline{11}\}, \qquad B_{10} = \{\overline{2}, \overline{3}, \overline{5}, \overline{11}\},$$

$$B_4 = \{\overline{5}, \overline{9}, \overline{10}, \overline{12}\}, \qquad B_{11} = \{\overline{3}, \overline{4}, \overline{6}, \overline{12}\},$$

$$B_5 = \{\overline{0}, \overline{6}, \overline{10}, \overline{11}\}, \qquad B_{12} = \{\overline{0}, \overline{4}, \overline{5}, \overline{7}\}.$$

$$B_6 = \{\overline{1}, \overline{7}, \overline{11}, \overline{12}\},$$

Examining these translates, we see that they are distinct, each group element appears in 4 sets, and each pair of distinct points appears in 1 block; that is, we see that these blocks together with $\mathbf{Z}/13\mathbf{Z}$ form a symmetric BIBD$(13, 4, 1)$.

This construction also shows that the maps $i \mapsto i + j$, for each $j \in \mathbf{Z}/13\mathbf{Z}$, are each an automorphism of the design; in particular, the group of automorphisms (see Definition 1.15) of the design has a subgroup isomorphic to $\mathbf{Z}/13\mathbf{Z}$ which acts sharpely transitively[3]) on the design.

All this motivates the following definition.

1.12. Definition. Let G be an additive finite abelian group of order v. Let $D \in \binom{G}{k}$, for $k < v$. Following Beth et al. (1999), we define $\Delta(D)$ to be the multiset of differences between distinct elements of D. We say that D is a *difference set* if

(1.12.a) $\Delta(D) = \lambda(G \backslash \{0\})$, for some $\lambda \in \mathbf{N}$.

We write D is a DS(v, k, λ) in the group G. The collection of all the translates $g + D$, for $g \in G$, is called the *development* Dev(D) of D.

The importance of these objects to designs is encapsulated in the following result, which we do not pause to prove (see Hall, 1986, Theorem 11.1.2).

1.13. Theorem. A k-subset D of a group G is a DS(v, k, λ) if and only if Dev(D) is a symmetric BIBD(v, k, λ).

1.14. Corollary. A symmetric design $\mathbf{D} = (X, \mathscr{B})$ is the development of a difference set in a group G if and only if the group of automorphism of $\mathbf{D}$ has a sharpely transitive subgroup isomorphic to G.

We will need the following ideas from finite geometry. Let q be a prime power. If $K = \mathrm{GF}(q)$, then recall that the extention field $F = \mathrm{GF}(q^{m+1})$ can be regarded as an $(m+1)$-dimensional vector space over K.

The m-dimensional projective space $\mathrm{P}(m, q)$ has points given by the non-trivial 1-dimensional subspaces of which there are $(q^{m+1}-1)/(q-1)$. If x is a projective point, and if $V \subseteq F$ is a linear subspace, then either $x \subseteq V$ or $x \cap V = \emptyset$. If V has dimension $d+1$, then the collection of all projective points $x \subseteq V$ forms a d-dimensional projective subspace of cardinality $(q^{d+1}-1)/(q-1)$.

The projective points, lines, planes, and hyperplanes are the 0-, 1-, 2-, and $(m-1)$-dimensional projective subspaces, respectively. More generally, the d-dimensional projective subspaces are called d-flats.

It isn't difficult to show that any two distinct points are contained in precisely $(q^{m-1}-1)/(q-1)$ hyperplanes. Evidently, then, the points and hyperplanes of $\mathrm{P}(m, q)$ form a square BIBD with parameters

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

It is well-known[4]) that the points of the space $\mathrm{P}(m, q)$ can be represented by the cyclic coset space $G = F^*/K^*$. If $\pi : F^* \to F^*/K^*$ is the natural projection, and if H is any hyperplane of $\mathrm{P}(m, q)$, then it follows by the comments above that $\pi(H)$ is a difference set in G with parameters given above. The difference sets so constructed are the so-called Singer difference sets (Singer, 1938).

If D is a $\mathrm{DS}(v, k, \lambda)$ in a group G, then $D^c = G \backslash D$ is clearly a $\mathrm{DS}(v, v-k, 2-2k+\lambda)$. It follows that the complement of a Singer difference set in $\mathrm{P}(m, q)$

is a difference set with parameters

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

We will follow Arasu et al. (1995) in labelling this difference set $\mathrm{D}(m, q)$. It is custumary to call such difference sets Singer difference sets as well, and we choose to follow this this pattern.

* * *

1.4. Isomorphisms of Designs. We conclude this section by briefly discussing isomorphisms of designs.

1.15. Definition. Let $\mathbf{D}_1 = (X_1, \mathscr{B}_1)$ and $\mathbf{D}_2 = (X_2, \mathscr{B}_2)$ be two BIBDs with the same parameters, and let $f : X_1 \to X_2$ be some bijection. If $f(\mathscr{B}_1) = f(\mathscr{B}_2)$, then we say that f is an *isomorphism* and that the two designs are *isomporhic*. For the case in which $\mathbf{D}_1 = \mathbf{D}_2$, we say that f is an *automorphism*. The collection of all automorphisms of a design $\mathbf{D}$ forms a group under composition called the *automorphism group* of the design.

In practice, one is usually concerned with the actions of isomorphisms on the incidence matrices of designs. In particular, two $\mathrm{BIBD}(v, b, r, k, \lambda)$s with incidence matrices A_1 and A_2 are isomorphic if and only if there is a permutation matrix P of order v and a permutation matrix Q of order b such that

(1.15.a) $PA_1Q = A_2.^{5)}$

1.16. Definition. As nothing essential is changed under the action of an isomorphism, one can then assume that the incidence matrix of a square design has the following form

$$
\text{(1.16.a)} \quad \begin{pmatrix} \mathbf{0}_{v-k} & A_1 \\ \mathbf{1}_k & A_2 \end{pmatrix}.
$$

We will say that such an incidence matrix is in *normal form*.

1.17. Example. The projective plane of order 3 in Example 1.6 has the incidence matrix

$$
\text{(1.17.a)} \quad \begin{pmatrix}
1&1&0&0&1&0&0&0&0&0&0&1&0\\
0&1&0&0&0&1&0&0&1&0&1&0&0\\
0&1&1&0&0&0&0&1&0&0&0&0&1\\
0&1&0&1&0&0&1&0&0&1&0&0&0\\
0&0&0&0&1&0&0&0&1&1&0&0&1\\
0&0&1&1&1&1&0&0&0&0&0&0&0\\
0&0&0&0&1&0&1&1&0&0&1&0&0\\
0&0&0&1&0&0&0&1&1&0&0&1&0\\
1&0&1&0&0&0&1&0&1&0&0&0&0\\
1&0&0&0&0&1&0&1&0&1&0&0&0\\
1&0&0&1&0&0&0&0&0&0&1&0&1\\
0&0&1&0&0&0&0&0&0&1&1&1&0\\
0&0&0&0&0&1&1&0&0&0&0&1&1
\end{pmatrix}
$$

It can be rearranged, however, so that it has the incidence matrix

$$
\text{(1.17.b)} \quad \begin{pmatrix}
0&1&0&0&0&1&0&0&1&0&1&0&0\\
0&1&1&0&0&0&0&1&0&0&0&0&1\\
0&1&0&1&0&0&1&0&0&1&0&0&0\\
0&0&0&0&1&0&0&0&1&1&0&0&1\\
0&0&1&1&1&1&0&0&0&0&0&0&0\\
0&0&0&0&1&0&1&1&0&0&1&0&0\\
0&0&0&1&0&0&0&1&1&0&0&1&0\\
0&0&1&0&0&0&0&0&0&1&1&1&0\\
0&0&0&0&0&1&1&0&0&0&0&1&1\\
1&1&0&0&1&0&0&0&0&0&0&1&0\\
1&0&1&0&0&0&1&0&1&0&0&0&0\\
1&0&0&0&0&1&0&1&0&1&0&0&0\\
1&0&0&1&0&0&0&0&0&0&1&0&1
\end{pmatrix},
$$

where the residual and derived designs are easily seen. The residual is the affine plane of order 3.

§2. Error-Correcting Codes

In this section, the definitions of linear error-correcting codes will be given. We then move on to consider the famous generalized Hamming and simplex codes. As these are the only family of codes that we require, this section will be brief. The interested reader is refered to the standard references of Huffman and Pless (2003) and MacWilliams and Sloane (1977) for a greater exposition of the subject.

* * *

2.1. Linear Codes. In elementary physics, we learn of the principal of superposition while studying oscillation theory; we learn how energy passing through a medium in the form of a wave can *interfere* with other such waves to create a new wave, the sum of the waves. This persists until these bursts of energy have passed.

The modern theories of commumincation and information seak to pass information via electrical signals (waves) passing through some channel (media). As information in the form of signals passes through the channel, it will invariably come into contact with other signals, whether latent or otherwise. The signal will then change, and there is no guaruntee that the signal received will be the signal sent; whence, one of the fundamental problems of digital communication is exposed. It becomes necessary, then, to attempt a solution. Hill (1986) provides the following instructive example.

Imagine there are two possible messages that we would like to send: `YES` and `NO`. And suppose further that `YES` is encoded as `0` and `NO` as `1`. If we had sent the message `0`, there is the possibility of the single bit being flipped, i.e. `1` is received instead of `0`, the initial message. The receiver would then have an incorrect message. It isn't difficult to envisage senarios in which such an error would have a terrible impact.

Instead, we will encode `YES` as `00000` and `NO` as `11111`. If we sent `00000` through the channel, and if the receiver got `01000`, then it would be reasonable to assume[6]) that the message intended was `YES`, a correct assumption. Since a single bit was all that was necessary to convey our minimal lexicon {`YES, NO`}, we see that the remaining 4 bits are *redundant*; however, we also see that these redundancies allowed us to correct the message in the case that any single bit was flipped. Similarly, if any two bits had been flipped, then we also would have correctly interpreted the message. If, however, we sent `00000` and received `00111`, then we would have interpreted this message as `11111`, clearly incorrect. So we see that there is a limitation of our ability to correct errors in transmition, but this is hardely unexpected. In any event, the ability to detect and correct errors is a remarkable property whose importance cannot be overstated in today's digital world.

The process of appending to `0` and `1` the redundant strings of bits `0000` and `1111`, respectively, is called *encoding*, and we now introduce such a method.

Suppose we had the binary string $x = x_0x_1 \cdots x_{n-1}$, where the first k bits $x_0x_1 \cdots x_{k-1}$ are the message we desire to preserve upon sending through some channel. We choose the remaining *check bits* $x_kx_{k+1} \cdots x_{n-1}$ (the redundancies) in such a way that

$$Hx^t = 0 \qquad (\text{mod } 2),$$

where H is the binary $(n-k) \times n$ matrix called the *parity check matrix* of the code. Moreover, by our assumptions on x, H can be assumed to have the form

$$H = (A \mid I_{n-k}),$$

for some binary matrix A.

More generally, we may take x and H to be over any field GF(q). We have the following definition.

2.1. Definition. Let $H = (A \mid I_{n-k})$ be an $(n-k) \times n$ matrix over GF(q). The *linear code* $\mathscr{C}$ with parity check matrix H is given by $\mathscr{C} = \text{Null}(H) = \{x \in \text{GF}(q^n) : Hx^t = 0\}$, where the extension GF$(q^n)$ is interpreted here as a linear space over GF(q). We say that $\mathscr{C}$ is a linear $[n,k]_q$-code, where clearly $\dim(\mathscr{C}) = k$.

2.2. Example. The repitition code over GF$(q) = \{0, a_1, \ldots, a_{q-1}\}$ of length n is given by

$$\text{(2.2.a)} \qquad \begin{array}{c} \overbrace{\begin{array}{cccc} 0 & 0 & \cdots & 0 \\ a_1 & a_1 & \cdots & a_1 \\ \vdots & \vdots & & \vdots \\ a_{q-1} & a_{q-1} & \cdots & a_{q-1} \end{array}}^{n} \end{array}$$

and has parity check matrix $H = (\mathbf{1}_{n-1} \mid I_{n-1})$.

We have defined a linear code by its parity check matrix. An equivalent definition is to use the so-called *generator matrix* G. If $H = (A \mid I_{n-k})$ is the parity check matrix of the code, then $G = (I_k \mid -A^t)$. The code is then given by the linear span of the rows of G. Note that by construction, it follows that $GH^t = HG^t = O$.

2.3. Example. The repitition code of the previous example has the generator matrix $\mathbf{1}_n^t$.

The dual of a linear code $\mathscr{C}$ is given in the usual way by $\mathscr{C}^\perp = \{x \in \text{GF}(q^n) : xy^t = 0$, for every $y \in \mathscr{C}\}$. If H and G are the parity check and generator matrices of $\mathscr{C}$, then G and H are the parity check and generator matrices of $\mathscr{C}^\perp$, respectively.

In Definition 2.1, there are two parameters explicitly given of a code, namely, the length n of the codewords and the dimension k of the linear space consisting of the codewords. Two more fundamental parameters for us are the minimum distance and the minimum weight defined thus.

2.4. Definition. Let $\mathscr{C}$ be a linear $[n,k]_q$-code. Then the *Hamming weight* of a codeword $x = x_0x_1\cdots x_{n-1} \in \mathscr{C}$ is given by

(2.4.a) $\mathrm{wt}(x) = \#\{i : x_i \neq 0\}$.

If $y = y_0y_1\cdots y_{n-1} \in \mathscr{C}$ is any other codeword, then the *Hamming distance* between x and y is defined as

(2.4.b) $\mathrm{dist}(x,y) = \#\{i : x_i \neq y_i\}$.

We then have that the minimum weight of the code and the minimum distance of the code are

(2.4.c) $\mathrm{wt}(\mathscr{C}) = \min_{x\in\mathscr{C}\setminus\{0\}} \mathrm{wt}(x)$ and

(2.4.d) $\mathrm{dist}(\mathscr{C}) = \min_{\substack{x,y\in\mathscr{C}\\ x\neq y}} \mathrm{dist}(x,y)$.

If we wish to emphasize the distance $d = \mathrm{dist}(\mathscr{C})$ of a code, we write $[n,k,d]_q$-code; and to emphasize the weight $w = \mathrm{wt}(\mathscr{C})$ of a code as well, $[n,k,d,w]_q$-code.

The Hamming distance can easily be seen to form a metric[7)] on $\mathrm{GF}(q^n)$. The next result is then clear (see Hill, 1986, Theorem 1.9).

2.5. Proposition. If $\mathscr{C}$ is any $[n,k,d]_q$-code, then the following hold.

(2.5.a) The code can detect s errors if $\mathrm{dist}(\mathscr{C}) \geq s+1$;

(2.5.b) the code can correct up to t errors if $\mathrm{dist}(\mathscr{C}) \geq 2t+1$; and

(2.5.c) for every $x,y \in \mathscr{C}$, it holds that $\mathrm{dist}(x,y) = \mathrm{wt}(x-y)$, hence $\mathrm{dist}(\mathscr{C}) = \mathrm{wt}(\mathscr{C})$.

We note that in the case the code is nonlinear, the condition (2.5.c) fails to hold in general.

We give one final result in this subsection relating the parity check matrix and the minimum distance.

2.6. Proposition. Let $\mathbf{C}$ be a linear $[n,k]_q$-code with parity check matrix H. Then $\mathscr{C}$ has dist$(\mathscr{C}) \geq d$ if and only if every $d-1$ columns of H are linearly independent.

Proof. To show necessity, let $x \in \mathscr{C}$ and $w = \text{wt}(x)$. Since $Hx^t = 0$, H has at least w linearly dependent columns; hence, if if any $d-1$ columns of H are linearly independent, then, by an application of (2.5.c), $\mathscr{C}$ cannot have a codeword of weight $d-1$ or less.

Towards sufficiency, assume that H has $d-1$ linearly independent columns. If $c_0, \ldots, c_{n-1}$ are the columns of H, then there is a dependence relation $a_0c_0 + \cdots + a_{n-1}c_{n-1} = 0$ ($a_0, \ldots, a_{n-1} \in$ GF(q)) for which at most $d-1$ of the a_is are nonzero. Then the codeword $x = a_0a_2 \cdots a_{n-1}$ has weight less than d, thereupon dist$(\mathscr{C}) \leq d$. ∎

* * *

2.2. The Hamming and Simplex Codes. The theory of error-correcting codes began with the seminal paper of Richard W. Hamming (1950) who introduced redundancy for the purpose of error correction. In this paper, he also constructed a most useful family of codes, aptly called the *Hamming codes*. The codes constructed by Hamming were binary; however, it is a simple matter to extend the construction to an arbitrary finite field.

2.7. Definition. Let H be the $n \times (q^n - 1)/(q-1)$ matrix over GF(q) whose columns are representatives of the nonzero 1-dimensional subspaces of the extension field GF(q^n) over GF(q). The linear code $\mathscr{H}_{q,n}$ whose parity check matrix is H is called a *Hamming code*. The linear code $\mathscr{S}_{q,n}$ whose generator matrix is H is called a *simplex code*.

2.8. Example. The following is a simplex code in GF(9) over GF$(3) \simeq \mathbf{Z}/3\mathbf{Z}$.

$$\text{(2.8.a)}\quad \begin{pmatrix} \overline{1}\,\overline{1}\,\overline{2}\,\overline{0} \\ \overline{2}\,\overline{1}\,\overline{0}\,\overline{2} \\ \overline{0}\,\overline{1}\,\overline{1}\,\overline{1} \\ \overline{1}\,\overline{2}\,\overline{0}\,\overline{1} \\ \overline{2}\,\overline{2}\,\overline{1}\,\overline{0} \\ \overline{0}\,\overline{2}\,\overline{2}\,\overline{2} \\ \overline{1}\,\overline{0}\,\overline{1}\,\overline{2} \\ \overline{2}\,\overline{0}\,\overline{2}\,\overline{1} \\ \overline{0}\,\overline{0}\,\overline{0}\,\overline{0} \end{pmatrix}.$$

The following result is immediate.

2.9. Proposition. Let q be a prime power, $n > 1$, and let $v = (q^n - 1)/(q - 1)$. Then:

(2.9.a) $\mathscr{S}_{q,n}$ is a linear $[v, n]_q$-code, and

(2.9.b) $\mathscr{H}_{q,n}$ is a linear $[v, v - n]_q$-code.

Using Proposition 2.6, we see that $\mathscr{H}_{q,n}$ is a linear single-error correcting code. In what follows, however, the simplex code will play a central role. Due to it's importance, then, we work through the rather lengthy proof of the following characterizing result (see Ionin and Shrikhande, 2006, Theorem 3.9.27).

2.10. Theorem. Let q be a prime power, $n > 1$, and let $v = (q^n - 1)/(q - 1)$. Then a linear $[v, n]_q$-code $\mathscr{C}$ is a $\mathscr{S}_{q,n}$ code if and only if $\mathrm{wt}(x) = q^{n-1}$, for every $x \in \mathscr{C}$.

Proof. Let $\mathscr{C}$ be a linear $[v, n]$-code in GF(q^v), and let $W = \begin{pmatrix} \overline{x_0} \\ \vdots \\ \overline{x_{v-1}} \end{pmatrix}$, where the x_i are representatives of the nonzero 1-dimensional subspaces of $\mathscr{C}$. Without loss of generality, assume that the first n rows of W form a generator matrix H for the code $\mathscr{C}$. Let $y_0, \ldots, y_{v-1}$ be the columns of W and let $Y = \langle y_0, \ldots, y_{v-1} \rangle$. Then $\dim(Y) = \operatorname{rank}(W) = \dim(\mathscr{C}) = n$. For $i \in \{0, \ldots, v-1\}$, let U_i be the hyperplane generated by all strings with the i-th position 0.

If $\mathscr{C}$ is a $\mathscr{S}_{q,n}$, then the columns of H are representatives of all the distinct 1-dimensional subspaces of a linear n-dimensional space over GF(q). By extension, then, $y_0, \ldots, y_{v-1}$ are representatives of the distinct 1-dimensional subspaces of Y. If $Y \subseteq U_i$, then $x_i = 0$, a contradiction. Therefore, $\dim(Y \cap U_i) = n-1$ so that $Y \cap U_i$ has $(q^{n-1}-1)/(q-1)$ 1-dimensional subspaces. It follows that wt$(x_i) = v - (q^{n-1}-1)/(q-1) = q^{n-1}$, but every string in $\mathscr{C}$ is a scalar multiple of some x_i, hence wt$(x) = q^{n-1}$, for every $x \in \mathscr{C}$.

Towards necessity, assume that wt$(x) = q^{n-1}$, for every $x \in \mathscr{C}$. As the code $\mathscr{C}$ is linear, it follows that it is equidistant with $d(\mathscr{C}) = q^{n-1}$.

If $Y \cap U_i = Y \cap U_j$, then x_i and x_j have zeros in the same $(q^{n-1}-1)/(q-1)$ positions. Then, if $W_{ih} \neq 0$, $W_{jh} \neq 0$ and $W_{ih} = \alpha W_{jh}$ for some $\alpha \in$ GF$(q)^*$. It follows that

$$\text{dist}(x_i, \alpha x_j) \leq v - \frac{q^{n-1}-1}{q-1} - 1 < q^{n-1},$$

a contradiction. Since $x_i \neq \alpha x_j$, we have $Y \cap U_i \neq Y \cap U_j$. Then $\mathrm{Y} \cap \mathrm{U_i} \cap \mathrm{U_j} = n-2$ so that there are $(q^{n-2}-1)/(q-1)$ indices h for which $W_{ih} = W_{jh} = 0$. If N is the matrix obtained from W by replacing the nonzero entries with 1, then our discussion shows that two distinct rows of N have inner product

$$v - 2\frac{q^{n-1}-1}{q-1} + \frac{q^{n-2}-1}{q-1} = q^{n-1} - q^{n-2};$$

hence, N is the incidence matrix of a square BIBD$(v, q^{n-1}, q^{n-1} - q^{n-2})$. By Proposition 1.9, no two columns of N are proportional, thereupon no two columns of W are proportional.

It remains to show that the columns of H represent all the distinct 1-dimensional subspaces of an n-dimensional linear space over GF(q). Let $z_0, \ldots, z_{v-1}$ be the columns of H. Suppose there are distinct $i, j \in \{0, \ldots, v-1\}$ and an $\alpha \in \text{GF}(q)^*$ such that $z_i = \alpha z_j$. Then $W_{hi} = \alpha W_{hj}$, for all $h \in \{0, \ldots, n-1\}$. Since $\{x_0, \ldots, x_{n-1}\}$ is a basis for $\mathscr{C}$, it follows that there are $\beta_0, \ldots, \beta_{n-1} \in \text{GF}(q)$ such that $x_\ell = \sum_k \beta_k x_k$. Thus,

$$W_{\ell i} = \sum_k \beta_k W_{ki} = \alpha \sum_k \beta_k W_{kj} = \alpha W_{\ell j},$$

from which it would follow that $y_i = \alpha y_j$, which cannot happen. Then H is a generator matrix of $\mathscr{C}$, and $\mathscr{C}$ is a $\mathscr{S}_{q,n}$. ∎

The fact that $\mathscr{S}_{q,n}$ is constant weight—and hence equidistant—will be used to great effect in Part II of this essay.

Notes

1. This technique is famously used in the justification of Hoffman's co-clique bound (see Brouwer et al., 1989, Proposition 1.3.2). In Cameron (1994) and Cameron and van Lint (1991), it is used to great effect in the context of designs.

2. By an incidence structure is meant a triple $S = (X, \mathscr{B}, I)$, where $I \subseteq X \times \mathscr{B}$. We say that X is the point set, $\mathscr{B}$ the block set, and I the set of flags. If $(x, B) \in I$, then the point x and block B are said to be incident. See Batten (1997) and Dembowski (1997) for a standard treatment of incidence. See Beth et al. (1999) for study of incidence in the context of design theory.

3. Recall that a group G is said to act on a set Ω if there is a map $\mu : \Omega \times G \to \Omega$ satisfying (a) $\mu(\mu(\alpha, g), h) = \mu(\alpha, gh)$, for all $\alpha \in \Omega$ and $g, h \in G$; and (b) $\mu(\alpha, 1) = \alpha$ for all $\alpha \in \Omega$. In particular, G is isomorphic to a subgroup of S_Ω, the symmetric group of Ω. The action is sharpely transitive if, for all $\alpha, \beta \in \Omega$, there is a unique $g \in G$ such that $\mu(\alpha, g) = \beta$. Cameron (1999) is a standard reference on permutation groups offering a wealth of explanation. Beth et al. (1999) studies the applications of transitive groups to designs.

4. What follows is given in the derivation of Theorem 9.2.1 of Ionin and Shrikhande (2006). If $\pi :$ GF$(q^{m+1})^* \to$ GF$(q^{m+1})^*/$GF$(q)^*$ is the natural projection, and if α is a primitive element of GF(q^{m+1}), then $x = \pi(\alpha)$ is a generator of the cyclic coset space GF$(q^{m+1})^*/$GF$(q)^*$. We have at once that the cosets x^n are given by all the nonzero elements of the 1-dimensional linear space spanned by α^n of the extension GF$(q^{m+1})/$GF(q).

5. This is more generaly given as the orbits of the action of $S_v \times S_b$ on the set of binary $v \times b$ matrices defined by $\mu(A, (P, Q)) = P^t AQ$, where the transposition is necessary in order to properly define

a right action.

6. This technique is known as nearest neighbour decoding (see MacWilliams and Sloane, 1977).

7. Recall that a metric space is a pair (X, ϱ), where X is a nonempty set, and where $\varrho : X \to \mathbf{R}_{\geq 0}$ is a map satisfying, for all $x, y, z \in X$, (a) $\varrho(x, y) \geq 0$ with equality iff $x = y$; (b) $\varrho(x, y) = \varrho(y, x)$; and (c) $\varrho(x, y) \leq \varrho(x, z) + \varrho(z, y)$. We then say that ϱ is a metric.

2

Weighing Matrices and Their Generalizations

This chapter focuses on a third combinatorial configuration, namely, weighing matrices, and their generalizations. We begin with a brief look at weighing matrices themselves, before moving onto to consider two generalizations. The first generalization is allowing the entries of a weighing matrix to be chosen from a finite group. This idea is then synthesized with the ideas of §1. Finally, we allow the entries of a weighing matrix to be taken from sets of indeterminants and consider the utility of such an approach.

§3. Weighing Matrices

In this section, we study weighing matrices. Apart from having numerous applications, these objects are of significant theoretical interest. Though we will be focusing on certain generalizations of these objects, it is worthwhile to consider their simplest case.

* * *

3.1. Definitions. Imagine, for a moment, the simple senario in which you need to weigh several objects, say, four objects (see MacWilliams and Sloane, 1977, Chapter 2). Imagine further that you are using a simple balance with two pans that makes an error ϵ everytime that it is used, where ϵ is random with mean 0 and variance σ^2.

Assume the actual weights are a, b, c, and d. If we weigh them seperately with measurements y_1, y_2, y_3, and y_4, and if the errors are $\epsilon_1, \epsilon_2, \epsilon_3$, and ϵ_4, then we obtain the four equations

$$a = y_1 + \epsilon_1, \qquad b = y_2 + \epsilon_2, \qquad c = y_3 + \epsilon_3, \qquad d = y_4 + \epsilon_4.$$

The estimates of the weights are then

$$\hat{a} = y_1 = a - \epsilon_1, \quad \hat{b} = y_2 = b - \epsilon_2, \quad \hat{c} = y_3 = c - \epsilon_3, \quad \hat{d} = y_4 = d - \epsilon_4,$$

each having variance σ^2.

Now, we will weigh the objects together in the following way.

$$a + b + c + d = y_1 + \epsilon_1,$$
$$a - b + c - d = y_2 + \epsilon_2,$$
$$a + b - d - d = y_3 + \epsilon_3,$$
$$a - b - c + d = y_4 + \epsilon_4,$$

where we have used $+1$ to indicate being placed on the right pan, and we have used -1 to indicate being placed on the left pan.

One can see that the coefficient matrix for the weighing configuration is non-singular. As such, we can solve for the variables; for example, we show the estimate for a:

$$\hat{a} = \frac{y_1 + y_2 + y_3 + y_4}{4}.$$

From this, we can see that the variance of $\hat{a}$ is given by $\sigma^2/4$, a large improvement from the initial configuration in which each weight was weighed independently.

In general, if there are n weights, and if there is a non-singular ternary (-1,0,1)-matrix of order n with a constant number of non-zero entries in each row, then that matrix can be used as a weighing configuration for the collection of objects in which the variance of the errors can be reduced.

All this motivates the following definition.

3.1. Definition. Let W be a $(-1, 0, 1)$-matrix of order n. W is a *weighing matrix* of *order* n and *weight* k if

(3.1.a) $WW^t = kI_n$.

If $n = k$, then we say that W is a *Hadamard matrix*. If $n - 1 = k$, then we say that W is a *conference matrix*. In any event, we write $\mathrm{W}(n, k)$ to denote this property.

3.2. Example. The following can be verified directly to be a $\mathrm{W}(13, 9)$ (NB: We have used $-$ in place of -1 and $+$ in place of $+1$)

$$\text{(3.2.a)} \quad \begin{pmatrix}
0 & 0 & - & + & 0 & + & - & - & - & - & - & 0 & - \\
+ & 0 & + & + & + & 0 & - & + & 0 & - & 0 & - & + \\
+ & 0 & 0 & - & + & + & + & 0 & - & + & - & - & 0 \\
- & 0 & + & 0 & - & + & 0 & + & - & 0 & - & + & + \\
- & - & - & + & 0 & + & + & + & 0 & 0 & + & - & 0 \\
- & - & 0 & 0 & 0 & 0 & - & - & + & + & - & - & + \\
+ & + & - & + & 0 & + & 0 & 0 & + & + & 0 & + & + \\
+ & - & + & 0 & - & + & - & 0 & 0 & + & + & 0 & - \\
0 & + & 0 & + & - & - & 0 & + & 0 & + & - & - & - \\
0 & + & - & - & - & 0 & - & 0 & - & 0 & + & - & + \\
0 & + & + & 0 & - & + & + & - & + & - & 0 & - & 0 \\
- & + & 0 & - & + & + & - & + & + & 0 & 0 & 0 & - \\
+ & - & - & - & - & 0 & 0 & + & + & - & - & 0 & 0
\end{pmatrix}.$$

The weighing matrix of the previous example is indicative of a more general construction that uses relative difference sets (see §3.4). Note that upon changing the nonzero entries of (3.2.a), one obtains the incidence matrix of the complement design of (1.17.a).

* * *

3.2. Necessary Conditions on Existence. The conditions placed on a matrix in order for it to be a weighing matrix are none too restrictive: One only needs orthogonality of the rows, a constant number of nonzero entries in every row, and the non-zero entries to have absolute value 1. Usually, in order to construct these objects one must assume some further combinatorial and/or algebraic properties. So-called cocyclic matrices, for example, are studied extensively in Horadam (2007) and de Launey and Flannery (2011). Nevertheless, we can say a few things at the outset.

By Cauchy's property of the determinant[8], $\det(W)^2 = k^n I_n$, for any $\mathrm{W}(n,k)$. In particular, if $n \equiv 1 \pmod 2$, then k is a square. This leaves the case that $n \equiv 0 \pmod 2$. It turns out, though we will not show it here, that if $n \equiv 2 \pmod 4$, then it must be the case that $k = a^2 + b^2$, for some $a, b \in \mathbf{Z}$[9]. Much is not known about the case $n \equiv 0 \pmod 4$, though Seberry (2017) conjectures that a $\mathrm{W}(4n, k)$ exists for every n and $k \leq 4n$.

Considering the weights, if $k = n - 1$, then it is clear that $n \equiv 0 \pmod 2$; for otherwise, if n is odd, then there will be $n - 2$ instances of $\binom{+}{+}$, $\binom{+}{-}$, or their negatives, in the product between any two distinct rows. Therefore, the product will resolve to a sum of $n - 2$ terms each consisting of ± 1. Since $n - 2 \equiv 1 \pmod 2$, this can never be zero.

In the case that $n = k$, we can assume (see §3.5) the first three rows have the following form.

$$
\overbrace{\begin{matrix} + & \ldots & + \\ + & \ldots & + \\ + & \ldots & + \end{matrix}}^{a}
\quad
\overbrace{\begin{matrix} + & \ldots & + \\ + & \ldots & + \\ - & \ldots & - \end{matrix}}^{b}
\quad
\overbrace{\begin{matrix} + & \ldots & + \\ - & \ldots & - \\ + & \ldots & + \end{matrix}}^{c}
\quad
\overbrace{\begin{matrix} + & \ldots & + \\ - & \ldots & - \\ - & \ldots & - \end{matrix}}^{d}
$$

Evidently, this configuration yields the following linear system.

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

whose solution is $a = b = c = d = n/4$. As these are integers, it must be the case, outside of the trivial cases $n = 1$ or 2, that $n \equiv 0 \pmod 4$ whenever $n = k$.

Finally, it follows by the definition and the above remarks that W is non-singular with $W^{-1} = k^{-1}W^t$, hence $W^tW = kI_n$. We record these result below.

3.3. Proposition. If there exists a $\mathrm{W}(n, k)$, say W, then the following must hold.

(3.3.a) If $n - 1 = k$, then n is even;

(3.3.b) if $n = k$, then n is 1, 2, or a multiple of 4;

(3.3.c) if n is odd, then k is a square;

(3.3.d) if 2 exactly divides n, then k is the sum of two squares; and

(3.3.e) W is non-singular and $WW^t = W^tW = kI_n$.

* * *

3.3. Complex Weighing Matrices. There are many useful generalizations of weighing matrices. We will take this up generally in the next section, but for now we note the following special case, where we use A^* to denote the conjugate (Hermitian) transpose of a complex matrix A.

3.4. Definition. Let $G = \{\exp(\frac{2\pi i m}{p}) : 0 \leq m < p\}$, and let W be a $(0, G)$-matrix of order v. We say that W is a *Butson weighing matrix* of *order* v and *weight* k if

(3.4.a) $WW^* = kI_n$,

and we write BW$(v, k; p)$ to denote this property.

3.5. Example. Let $\xi = \exp(\frac{2\pi i}{7})$, and let H, for $0 \leq i, j < 7$, be defined by $H_{ij} = \xi^{ij}$. It follows easily that H is a Butson weighing matrix (see Davis, 1979, §2.5); in fact, it is a Butson Hadamard matrix as $n = k$. To be concrete, the following is a BW$(7, 7; 7)$

(3.5.a) $$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \xi & \xi^2 & \xi^3 & \xi^4 & \xi^5 & \xi^6 \\ 1 & \xi^2 & \xi^4 & \xi^6 & \xi & \xi^3 & \xi^5 \\ 1 & \xi^3 & \xi^6 & \xi^2 & \xi^5 & \xi & \xi^4 \\ 1 & \xi^4 & \xi & \xi^5 & \xi^2 & \xi^6 & \xi^3 \\ 1 & \xi^5 & \xi^3 & \xi & \xi^6 & \xi^4 & \xi^2 \\ 1 & \xi^6 & \xi^5 & \xi^4 & \xi^3 & \xi^2 & \xi \end{pmatrix}.$$

The next result can be found in Lam and Leung (2000).

3.6. Lemma. Let p be a prime, and let ξ be a primitive complex p-th root of unity. Then $\sum_{i=0}^{n} a_i \xi^i = 0$ for some $n < p$ and $a_i \in \mathbf{N}$ if and only if $n = p - 1$ and $a_0 = \cdots = a_n$.

Proof. Let $f(x) = \sum_{i=0}^{n} a_i \xi^i \in \mathbf{Z}[x]$. The minimal polynomial of ξ over $\mathbf{Q}$ is the p-th cyclotomic polynomial $h(x) = 1 + x + \cdots + x^{p-1}$. Therefore, since the degree of f is at most p, we conclude that if $f(\xi) = 0$, then it must be an integer multiple of h. ∎

* * *

3.4. Difference Set Construction II. Let G be some additive, finite group. In Definition 1.12, a subset $D \in \binom{G}{k}$ was said to be a difference set if $\Delta(D)$ contained each element of $G\backslash\{0\}$ a constant number of times. Of course, we needn't restrict ourselves to omitting only the identity element; in fact, if we omit elements from a proper normal subgroup, we are left with a most useful object.

3.7. Definition. Let G be an additive, finite group for which $|G| = mn$, $N \subset G$ a normal subgroup of order n, and let $R \in \binom{G}{k}$ with $k < mn$. We say that R is a *relative difference set* in G with *forbidden subgroup* N if

(3.7.a) If $\Delta(R) = \lambda(G\backslash N)$, for some $\lambda \in \mathbf{N}$.

If N is a direct factor of G, then we call R a *splitting* relative difference set. In any case, we write R is an RDS(m, n, k, λ) in G relative to N.

3.8. Example. The set $R = \{\overline{1}, \overline{2}, \overline{4}, \overline{8}\}$ is an RDS$(5, 3, 4, 1)$ in $\mathbf{Z}/15\mathbf{Z}$ relative to $\{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}\}$.

3.9. Example. Let G be the direct product of $\mathbf{Z}/13\mathbf{Z}$ and S_3, and let $a = (1, 2)$ and $b = (1, 2, 3)$. Then $R = \{\overline{1}a, \overline{2}, \overline{3}ab, \overline{5}, \overline{6}, \overline{7}ab^2, \overline{8}a, \overline{9}ab^2, \overline{11}ab\}$ is an RDS$(13, 6, 9, 1)$ in G relative to S_3.

Though we do not show it here, just as difference sets are equivalent to square designs admitting a sharpely transitive automorphism group, relative difference sets can be shown to be equivalent to group divisible designs admitting a sharpely transitive automorphism group in which each element either fixes all or no point classes (see Jungnickel, 1982).

For our purposes, however, we are interested in the application of differences sets to weighing matrices and their generalizations. By far the most important family of such relative difference sets are found in the next result which is Theorem 9.6.12 of Ionin and Shrikhande (2006), and are called the *classical* relative difference sets.

3.10. Proposition. Let q be a prime power and $n > 1$. Let $f : \mathrm{GF}(q^n) \to \mathrm{GF}(q)$ be some nondegenerate linear map over $\mathrm{GF}(q)$. Then

(3.10.a) $R = \{x \in \mathrm{GF}(q^n) : f(x) = 1\}$ is an RDS in $\mathrm{GF}(q^n)^*$ relative to $\mathrm{GF}(q^*)$.

Moreover, the parameters of R are given by

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

Proof. Since f is nondegenerate, the Rank–Nullity Theorem[10]) implies that the dimension of $\ker(f)$ is $n-1$.

Suppose, for $x, y \in R$, that $xy^{-1} \in \mathrm{GF}(q)$. Then $1 = f(x) = af(y) = a$, hence $\mathrm{GF}(q)^* \cap \Delta(R) = \{1\}$.

It remains to verify that $\Delta(R) = q^{n-2}(\mathrm{GF}(q^n)^* \backslash \mathrm{GF}(q)^*)$. Let $t \in \mathrm{GF}(q^n)^* \backslash \mathrm{GF}(q)^*$, and define $g : \mathrm{GF}(q^n) \to \mathrm{GF}(q)$ by $g(y) = f(ty)$. It then suffices to show that there are q^{n-2} elements $y \in \mathrm{GF}(q^n)^*$ such that $f(y) = g(y) = 1$.

Since g is a nondegenerate linear map, the set $Y = g^{-1}(1)$ is an $(n-1)$-dimensional space over $\mathrm{GF}(q)$. Now, $\ker(g) = t^{-1}\ker(f)$, and, since $t \notin \mathrm{GF}(q)$, $\ker(g) \neq \ker(f)$. Therefore, $\dim(R \cap Y) = n-2$, and we're done. ∎

3.11. Example. Take $K = \mathrm{GF}(3)$ and $F = \mathrm{GF}(27)$ with the usual polynomial representation, and let $\mathrm{Tr} : F \to K$ be the absolute trace function[11]). By Proposition (3.10.a),

(3.11.a) $R = \{x \in F : \mathrm{Tr}(x) = 1\} = \{2x^2+x+2, 2x^2+2, 2x^2, 2x^2+x, 2x^2+2x+2, 2x^2+x+1, 2x^2+2x, 2x^2+2x+1, 2x^2+1\}$.

is an RDS$(13, 2, 9, 3)$ in F^* relative to K^*.

The following result is standard, and we do not pause to prove it (see Elliott and Butson, 1966).

3.12. Proposition. Let R be an RDS(m, n, k, λ) in a group G relative to a normal subgroup N, and let $\varphi : G \to H$ be a group epimorphism. Take $U = \ker(\varphi)$ and $|U| = u$. If $U \subseteq N$, then $\varphi(R)$ is an RDS$(m, n/u, k, \lambda u)$ in H relative to $\varphi(N)$. In particular, if $U = N$, then $f(R)$ is a DS$(m, k, \lambda u)$ in H.

We now present a construction of weighing matrices using relative difference sets. This construction is a special case of a more general result to be proven later, so we omit the proof.

3.13. Theorem. Let R be an RDS$(m, 2, k, \lambda)$ in a group G relative to a normal subgroup $N = \{1, t\}$. Let $g_0, \ldots, g_{m-1}$ be distinct coset representatives of N in G. Let W be a $(-1, 0, 1)$-matrix of order m defined by

$$\text{(3.13.a)}\quad W_{ij} = \begin{cases} 1 & \text{if } g_i g_j^{-1} \in R; \\ -1 & \text{if } t g_i g_j^{-1} \in R; \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

Then W is a W(m, k).

Speaking of the relative difference sets (3.10.a) for odd q, we see that the forbidden subgroup is cyclic of even order, hence it has a unique normal subgroup of order 2. Proposition 3.12 and Theorem 3.13 then imply the existence of a $W((q^n - 1)/(q - 1), q^{n-1})$ for every $n > 1$. We record this result as a corollary.

3.14. Corollary. For every odd prime power q, there is a $W((q^n - 1)/(q - 1), q^{n-1})$, for every $n > 1$.

The case in which q is even, Arasu et al. (2001) showed that there is a $W((q^n - 1)/(q-1), q^{n-1})$ whenever n is odd.

3.15. Example. Let R be as in (3.11.a). Using the coset representatives $1, 2x^2 + 2x, 2x^2+2x+1, x^2+x+1, x^2+2x, x^2+2x+2, 2x^2+x+2, 2x^2, 2x, 2x+1, 2x$ of GF$(3)^*$ in GF$(27)^*$, we can construct the weighing matrix in (3.2.a).

We will require one further result. Due to its length, we omit the proof; but the interested reader is refered to Chapter 9 of Ionin and Shrikhande (2006).

3.16. Proposition. Let q be a prime power, α a primitve element of GF(q^2), and $G = \{g_0, \ldots, g_{q-1}\}$ a group of order q. Let $C_i = \{a\alpha^i : a \in \text{GF}(q)^*\}$, for each $i \in \{0, \ldots, q\}$. Define

(3.16.a) $R = \{(0, 1_g)\} \cup \{(a, 1_g) : a \in C_0\} \cup \bigcup_{i=1}^{q} \{(a, g_{i-1}) : a \in C_i\}.$

Then R is an RDS(q^2, q, q^2, q) in GF$(q^2)^+ \times G$ relative to $\{0\} \times G$.

Proposition 3.12 then yields the following.

3.17. Corollary. Let p be a prime, and let $m \leq n$ be positive integers. Let $A =$ GF$(q^{2m})^+$, and let G be any group of order p^n. Then there is an RDS$(p^{2m}, p^n, p^{2m}, p^{2m-n})$ in $A \times G$ relative to $\{0\} \times G$.

* * *

3.5. Isomorphisms of Weighing Matrices. Let W be some W(v, k), and let P and Q be signed permutation matrices of order v. It is then clear that PWQ is again a W(v, k). We have the following.

3.18. Definition. Two weighing matrices W_1 and W_2 are *Hadamard equivalent* if there are two signed permutation matrices P and Q such that

(3.18.a) $PW_1Q = W_2.$[12])

3.19. Example. The weighing matrix (3.2.a) is Hadamard equivalent to the following.

$$\text{(3.19.a)}\quad \begin{pmatrix} 0&0&+&+&0&+&+&+&+&+&+&0&+\\ 0&+&0&+&-&-&0&-&0&-&+&-&+\\ 0&+&+&-&-&0&+&0&+&0&-&-&-\\ 0&+&-&0&-&+&-&+&-&+&0&-&0\\ +&0&-&+&+&0&+&-&0&+&0&-&-\\ +&0&0&-&+&+&-&0&+&-&+&-&0\\ +&0&+&0&+&-&0&+&-&0&-&-&+\\ +&+&-&-&0&-&+&+&0&0&+&+&0\\ +&+&0&0&0&0&-&-&+&+&-&+&+\\ +&+&+&+&0&+&0&0&-&-&0&+&-\\ +&-&-&0&-&+&+&0&0&-&-&0&+\\ +&-&0&+&-&-&-&+&+&0&0&0&-\\ +&-&+&-&-&0&0&-&-&+&+&0&0 \end{pmatrix}$$

The above example motivates the following definition.

3.20. Definition. A $\mathrm{W}(v,k)$ is said to be in *normal form* if it has the form

$$\text{(3.20.a)}\quad \begin{pmatrix} \mathbf{0}_{v-k} & A_1 \\ \mathbf{1}_k & A_2 \end{pmatrix}.$$

Similar to designs, we call A_1 the *residual part* and A_2 the *derived part* of the weighing matrix.

As a consequence of (3.20.a), we have

(3.20.b) $A_1 A_1^t = kI_{v-k}$ and

(3.20.c) $A_2 A_2^t = kI_k - J_k$.

§4. Balanced Generalized Weighing Matrices

We come now to the central object of our study, namely, the so-called balanced generalized weighing matrices. These objects are intriguing in their own right as we shall see, but they also have interesting applications in the construction of other configurations.

* * *

4.1. Generalized weighing matrices. In the previous section, we defined a weighing matrix as a square matrix over $\{-1, 0, 1\}$. We then extended this definition to include those matrices over 0 together with the complex p-th roots of unity. More generally, we can have weighing matrices over any finite group.

Before we can do this, however, we need to extend the conjugate transpose to group matrices. To accomplish this, let A be some matrix over a finite group G, and define $\overline{A}$ by $\overline{A}_{ij} = A_{ij}^{-1}$, that is, the matrix obtained by taking the group inverse of the nonzero entries of A. Finally, define $A^* = \overline{A}^t$. We then have the following.

4.1. Definition. Let G be some finite group not containing the symbol 0, and let W be a $(0, G)$-matrix of order v. If $WW^* = kI_n$ modulo the ideal $\mathbf{Z}G$, then we say that W is a generalized weighing matrix of order v and weight k. We write $\mathrm{GW}(v, k; G)$ to denote this property.[13])

4.2. Example. A real $\mathrm{W}(v, k)$ is a $\mathrm{GW}(v, k; C_2)$, and a $\mathrm{BW}(v, k; p)$ is a $\mathrm{GW}(v, k; C_p)$, were C_p denotes the cyclic group of prime order p.

4.3. Example. In the case that one has $\mathrm{BW}(v, k; C_n)$, where n is composite, one does not in general have a generalized weighing matrix. Consider the $\mathrm{BW}(6, 6; 4)$ given by

$$\text{(4.3.a)} \quad \begin{pmatrix} i & + & + & + & + & + \\ + & i & - & + & - & + \\ + & - & i & - & + & + \\ + & + & - & i & + & - \\ + & - & + & + & i & - \\ + & + & + & - & - & i \end{pmatrix}.$$

Clearly, this is a Hadamard matrix; however, $\pm i$ each appear only once in the conjugate inner product between distinct rows, hence it is not a generalized weighing matrix.

4.4. Example. The following is a $\mathrm{GW}(15,7;C_3)$, where the nonzero elements are the logarithms of a generator of C_3.

$$\text{(4.4.a)}\quad \begin{pmatrix}
0&3&3&3&3&3&3&3&0&0&0&0&0&0&0\\
0&3&2&0&1&0&0&0&0&0&2&0&2&2&3\\
0&0&3&2&0&1&0&0&3&0&0&2&0&2&2\\
0&0&0&3&2&0&1&0&2&3&0&0&2&0&2\\
0&0&0&0&3&2&0&1&2&2&3&0&0&2&0\\
0&1&0&0&0&3&2&0&0&2&2&3&0&0&2\\
0&0&1&0&0&0&3&2&2&0&2&2&3&0&0\\
0&2&0&1&0&0&0&3&0&2&0&2&2&3&0\\
3&3&1&0&2&0&0&0&3&2&0&1&0&0&0\\
3&0&3&1&0&2&0&0&0&3&2&0&1&0&0\\
3&0&0&3&1&0&2&0&0&0&3&2&0&1&0\\
3&0&0&0&3&1&0&2&0&0&0&3&2&0&1\\
3&2&0&0&0&3&1&0&1&0&0&0&3&2&0\\
3&0&2&0&0&0&3&1&0&1&0&0&0&3&2\\
3&1&0&2&0&0&0&3&2&0&1&0&0&0&3
\end{pmatrix}$$

* * *

4.2. Generalized Bhaskar Rao Designs. Our goal in introducing weighing matrices over arbitrary finite groups is to synthesize the ideas of weighing matrices and balanced incomplete block designs. We combine these concepts thus.

4.5. Definition. Let G be some finite group, and let A be a $v \times b$ $(0,G)$-matrix such that

$$\text{(4.5.a)}\quad AA^* = rI_v + \frac{\lambda}{|G|}\left(\sum_{g\in G} g\right)(J_v - I_v),$$

for some positive integers r and λ, and such that there are k non-zero entries in every column. We then say that A is a *generalized Bhaskar Rao design* (henceforth GBRD), and we write $\mathrm{GBRD}(v,k,\lambda;G)$ to denote this property. If we need to stress the remaining parameters, then we write GBRD$(v, b, r, k, \lambda; G)$.

Often it is helpful to give a combinatorial definition of GBRDs that is equivalent to the one just given. Again let A be a $v \times b$ $(0, G)$-matrix that has k nonzero entries in every column. If the multisets $\{A_{i\ell}A_{j\ell}^{-1} : A_{i\ell} \neq 0 \neq A_{j\ell}$ and $0 \leq \ell < b\}$, for $i, j \in \{0, \ldots, v-1\}$, $i \neq j$, have $\lambda/|G|$ copies of every group element in G, then we say that A is a GBRD$(v, k, \lambda; G)$.

A few things are rather immediate. If $\check{A}$ denotes the matrix obtained from A by changing each non-zero entry to 1, then condition (4.5.a) implies that $\check{A}$ is a BIBD. Conversely, a BIBD is a GBRD over the trivial group $\{1\}$.

Evidently, Fisher's inequality applies, hence $b \geq v$. We single out the extremal case of Fisher's inequality again.

4.6. Definition. A *balanced generalized weighing matrix* is a GBRD$(v, b, r, k, \lambda; G)$ in which $v = b$ (equiv. $k = r$). We use the denotation BGW$(v, k, \lambda; G)$. A BGW$(v, k, \lambda; G)$ in which $v = k$ is called a *generalized Hadamard matrix*, and we denote this as GH(G, λ) where $\lambda = v/|G|$. If $G = \mathrm{EA}(q)$, the elementary abelian group[14]) of order q, then we write GH(q, λ) instead.

4.7. Example. The generalized weighing matrix (4.4.a) is a BGW$(15, 7, 3; C_3)$.

4.8. Example. Let $G = \langle \alpha, \beta : \alpha^2 = \beta^2 = 1, \alpha\beta = \beta\alpha \rangle$. Then

$$\text{(4.8.a)} \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \alpha & \beta & \alpha\beta \\ 1 & \beta & \alpha\beta & \alpha \\ 1 & \alpha\beta & \alpha & \beta \end{pmatrix}$$

is a GH$(4, 1)$.

4.9. Example. A BGW$(v, k, \lambda; \{-1, 1\})$ is a *balanced weighing matrix*. The weighing matrix (3.2.a) is balanced.

* * *

4.3. Properties and Simple Constructions. Since A GBRD ultimately yields a BIBD, it follow that the necessary conditions of Proposition 1.2 also hold for the parameters of GBRDs. However, since we are now dealing with group matrices that are balanced with respect to the group, the next result is clear.

4.10. Proposition. Let A be a GBRD$(v, k, \lambda; G)$, and let $\phi : G \to H$ be some group epimorphism. Then $(\phi(A_{ij}))$ is a GBRD(v, k, λ) over H with the same parameters.

Our work from the previous section, namely, Lemma 3.6 yields the following.

4.11. Proposition. A Butson weighing matrix W over the p-th roots of unity, where p is a prime, is a BGW if and only if $(|W_{ij}|)$ is a BIBD.

The remainder of this section will focus on BGW matrices and will closely follow Chapter 10 of Ionin and Shrikhande (2006). We first present a few simple constructions.

4.12. Proposition. Let GF$(q) = \{a_0, \ldots, a_{q-1}\}$, and define H of order q by $H_{ij} = a_i a_j$. Then H is a GH$(q, 1)$.

Proof. Let H be so defined, and let $i, j \in \{0, \ldots, q-1\}$, $i \neq j$. Observe $\sum_k (a_i a_k - a_j a_k) = (a_i - a_j) \sum_k a_k$, hence each group element appears precisely once in $\{H_{ik} H_{jk}^{-1} : 0 \leq k < q\}$. ∎

4.13. Example. The GH$(4, 1)$ (4.8.a) was constructed using Proposition 4.12.

4.14. Proposition. Let GF$(q) = \{a_0, \ldots, a_{q-1}\}$, and define W of order $q+1$ by

$$(4.14.a)\quad W_{ij} = \begin{cases} 0 & \text{if } i = j = 0; \\ 1 & \text{if } i = 0 \text{ or } j = 0, \text{ but } i \neq j; \text{ and} \\ a_{i-1} - a_{j-1} & \text{otherwise.} \end{cases}$$

Then W is a BGW$(q+1, q, q-1; \mathrm{GF}(q)^*)$.

Proof. Let $i, j \in \{1, \ldots, q\}$, $i \neq j$. Then, for $\ell \neq j$,

$$W_{i\ell} W_{j\ell}^{-1} = \frac{a_{i-1} - a_{\ell-1}}{a_{j-1} - a_{\ell-1}} = \frac{a_{i-1} - a_{j-1}}{a_{j-1} - a_{\ell-1}} + 1.$$

As ℓ ranges over $\{1, \ldots, q\} \backslash \{j\}$, the difference $a_{j-1} - a_{\ell-1}$ ranges over $\mathrm{GF}(q)^*$. Since $W_{i0} = W_{j0} = 1$, the multiset $\{W_{i\ell} W_{j\ell}^{-1} : W_{i\ell} \neq 0 \neq W_{j\ell}$ and $0 \leq \ell < q+1\}$ contains each element of $\mathrm{GF}(q)^*$ once. The remaining cases in which $i = 0$ or $j = 0$ are trivial. ∎

4.15. Example. A BGW$(8, 7, 6; \mathrm{GF}(7)^*)$ formed from Proposition 4.14 is given by

$$\text{(4.15.a)} \quad \begin{pmatrix} 0&6&6&6&6&6&6&6 \\ 3&0&1&2&3&4&5&6 \\ 3&4&0&3&1&6&2&5 \\ 3&5&6&0&4&2&1&3 \\ 3&6&4&1&0&5&3&2 \\ 3&1&3&5&2&0&6&4 \\ 3&2&5&4&6&3&0&1 \\ 3&3&2&6&5&1&4&0 \end{pmatrix},$$

where the nonzero elements are the logarithms of some generator of $\mathrm{GF}(7)^*$. One can see that the matrix is skew-symmetric.

We present a construction due to Jungnickel and Tonchev (2002), which we do not prove here, that yields what are called the classical family of BGWs; more than that, however, the matrices so constructed are what is termed ω-circulant, a simple generalization of cirulant matrices.

4.16. Definition. Let $G = \langle \omega \rangle$ be a finite cyclic group, and let W be a matrix over $\mathbf{Z}[G]$ with first row $(\alpha_0, \ldots, \alpha_{n-1})$. W is ω-circulant if $W_{ij} = \alpha_{j-i}$ if $i \leq j$ and $W_{ij} = \omega \alpha_{j-i}$ if $i > j$, where the indices are calculated modulo n.

Finally, we are ready to present this simple and elegant construction.

4.17. Proposition. Let q be a prime power, and let β be a primitive element of the extension of order d of the field GF(q). Further, take $m = (q^d - 1)/(q - 1)$, and define $\omega = \beta^{-m} \in$ GF(q), i.e. the norm of β. Finally, we claim that the ω-circulant matrix with first row $(\mathrm{Tr}(\beta^k))_{k=0}^{m-1}$ is a BGW$(m, q^{d-1}, q^{d-1} - q^{d-2};$ GF$(q)^*)$.[15])

4.18. Example. The matrix

$$\begin{pmatrix}
0&2&2&2&0&1&2&2&1&2&0&2&0\\
0&0&2&2&2&0&1&2&2&1&2&0&2\\
1&0&0&2&2&2&0&1&2&2&1&2&0\\
0&1&0&0&2&2&2&0&1&2&2&1&2\\
1&0&1&0&0&2&2&2&0&1&2&2&1\\
2&1&0&1&0&0&2&2&2&0&1&2&2\\
1&2&1&0&1&0&0&2&2&2&0&1&2\\
1&1&2&1&0&1&0&0&2&2&2&0&1\\
2&1&1&2&1&0&1&0&0&2&2&2&0\\
0&2&1&1&2&1&0&1&0&0&2&2&2\\
1&0&2&1&1&2&1&0&1&0&0&2&2\\
1&1&0&2&1&1&2&1&0&1&0&0&2\\
1&1&1&0&2&1&1&2&1&0&1&0&0
\end{pmatrix} \tag{4.18.a}$$

is an ω-circulant BGW$(13, 9, 6;$ GF$(4)^*)$, where the nonzero elements are the logarithms of some generator of GF$(4)^*$.

We present a few brief remarks on the conjugate transpose and similar operations on BGWs.

4.19. Proposition. If W is a BGW$(v, k, \lambda; G)$, then W^* is also a BGW$(v, k, \lambda; G)$.

Proof. Consider W as a matrix over the ring $\mathbf{Q}[G]$ so that it satisfies (4.5.a) over $\mathbf{Q}[G]$. Let $\pi : \mathbf{Q}[G] \to \mathbf{Q}[G]/\mathbf{Q}G$ be the natural ring epimorphism. If πW denotes the matrix $(\pi(W_{ij}))$, then (4.5.a) becomes $(\pi W)(\pi W^*) = kI_v$, and hence $(\pi W)^{-1} = k^{-1}(\pi W^*)$. Therefore, $(\pi W^*)(\pi W) = kI_v$ so that $W^*W = kI_v + A$ for some $A = (a_{ij}\sum_{g\in G} g)$ over the ideal $\mathbf{Q}G$. Moreover, since $\check{W}^t$ is a BIBD, there exist integers a_g such that, for $i \neq j$, $\sum\limits_k w_{ki}w_{kj}^{-1} = \sum\limits_{g\in G} a_g g$ where $\sum\limits_{g\in G} a_g = \lambda$. Evidently, then, $A = \frac{\lambda}{|G|}(\sum\limits_{g\in G} g)(J_v - I_v)$, and the result follows. ▮

4.20. Corollary. If W is a BGW$(v, k, \lambda; G)$ where G is abelian, then $\overline{W}$ and W^t are also BGW$(v, k, \lambda; G)$s.

Proof. Since the group is abelian, the map $g \mapsto g^{-1}$ is an automorphism; hence, by Proposition 4.10, $\overline{W}$ is also a BGW$(v, k, \lambda; G)$. Then, by the proposition, $(\overline{W})^* = W^t$ is also a BGW$(v, k, \lambda; G)$. ▮

* * *

4.4. Difference Set Construction III. In §3.4, we introduced relative difference sets, and (3.13.a) then uses a difference set relative to a normal subgroup of order 2 in order to construct a weighing matrix. We saw how the classical relative difference sets with parameters (3.10.b), together with Proposition 3.12, whenever q is odd, can be used to construct the so-called classical weighing matrices. It so happens that this construction is a special case of something more general (see Ionin and Shrikhande, 2006, Theorem 10.3.1).

4.21. Theorem. Let R be an RDS(m, n, k, λ) in a group G relative to a normal subgroup N. Let $g_0, \ldots, g_{m-1}$ be all of the distinct coset representatives of N. Let W be a $(0, N)$-matrix of order m such that, for each $h \in N$, $W_{ij} = \alpha$ if and only if $g_iN \cap Rg_j = \{g_i\alpha\}$. Then W is a BGW$(m, k, \lambda n; N)$.

Proof. To begin, we first need that $|g_i \cap Rg_j| \leq 1$, for each $i, j \in \{0, \ldots .m-1\}$. To that end, let $a, b \in g_iN \cap Rg_j$; then $a = g_i\alpha = tg_j$ and $b = g_i\beta = ug_j$, for $t, u \in R$ and $\alpha, \beta \in N$. Then $t = g_i\alpha g_j^{-1}$ and $u = g_i\beta g_j^{-1}$, hence $tu^{-1} = g_i\alpha\beta^{-1}g_i^{-1}$. It follows that $tu^{-1} \in N$, as N is normal; thus, $t = u$ so that $a = b$.

For each $j \in \{0, \dots, m-1\}$, we have

$$k = |Rg_j| = \left| \bigcup_{i=0}^{m-1} g_i N \cap Rg_j \right| = \sum_{i=0}^{m-1} |g_i N \cap Rg_j|,$$

so we obtain that every column of W has k nonzero entries.

Now, let $i, h \in \{0, \dots, m-1\}$, with $\neq h$, and let $\gamma \in N$. First, assume that $\gamma = W_{ij}\overline{W_{hj}}$ for some j. Then there are unique $t, u \in R$ such that $tg_j = g_i W_{ij}$ and $ug_j = g_h W_{hj}$. It follows that $tu^{-1} = g_i \gamma g_h^{-1}$.

On the other hand, suppose that $g_i \gamma g_h^{-1} = tu^{-1}$, for some $t, u \in R$. Then there is a unique j such that $u^{-1}g_h \in g_j N$, that is, $u^{-1}g_h = g_j \beta$, for some $\beta \in N$. Then $ug_j = g_h \beta^{-1}$ and $tg_j = tu^{-1}g_h\beta^{-1} = g_i\gamma\beta^{-1}$ with $\gamma\beta^{-1} \in N$. Thus, $W_{ij} = \gamma\beta^{-1}$, $W_{hj} = \beta^{-1}$, and $\gamma = w_{ij}\overline{W_{hj}}$.

It follows that the number of indices j such that $\gamma = W_{ij}\overline{W_{hj}}$ is equal to the number of ordered pairs (t, u) of elements of R such that $tu^{-1} = g_i\gamma g_h^{-1}$. Since $g_i\gamma g_h^{-1} \notin N$, there are exactly λ such pairs. Therefore, W is a BGW$(m, k, \lambda n; N)$, and the proof is complete. ∎

Using the Theorem and the relative difference sets (3.16.a), yields the following.

4.22. Corollary. Let G be an arbitrary group of order p^n. Then there is a GH$(G; p^{2m-n})$, for every $m \geq n$.

4.23. Example. Using the relative difference sets (3.16.a), we construct a GH$(C_4, 4)$

over $C_4 \simeq \langle \left(\begin{smallmatrix} 0 & + \\ - & 0 \end{smallmatrix}\right) \rangle$ given by

$$
(4.23.a)\quad \begin{pmatrix}
+ & 0 & - & 0 & 0 & + & + & 0 & 0 & - & - & 0 & - & 0 & - & 0 & + & 0 & - & 0 & 0 & - & - & 0 & 0 & + & 0 & + & 0 & + & 0 & - \\
0 & + & 0 & - & - & 0 & 0 & + & + & 0 & 0 & - & 0 & - & 0 & - & 0 & + & 0 & - & + & 0 & 0 & - & - & 0 & - & 0 & - & 0 & + & 0 \\
- & 0 & + & 0 & - & 0 & 0 & + & - & 0 & 0 & - & - & 0 & 0 & + & + & 0 & 0 & + & 0 & - & - & 0 & - & 0 & 0 & - & + & 0 & 0 & + \\
0 & - & 0 & + & 0 & - & - & 0 & 0 & - & + & 0 & 0 & - & - & 0 & 0 & + & - & 0 & + & 0 & 0 & - & 0 & - & + & 0 & 0 & + & - & 0 \\
0 & - & + & 0 & + & 0 & - & 0 & - & 0 & - & 0 & - & 0 & 0 & - & - & 0 & - & 0 & - & 0 & 0 & - & 0 & + & 0 & - & - & 0 & + & 0 \\
+ & 0 & 0 & + & 0 & + & 0 & - & 0 & - & 0 & - & 0 & - & + & 0 & 0 & - & 0 & - & 0 & - & + & 0 & - & 0 & + & 0 & 0 & - & 0 & + \\
- & 0 & 0 & - & - & 0 & + & 0 & 0 & - & 0 & + & 0 & - & + & 0 & + & 0 & - & 0 & - & 0 & + & 0 & + & 0 & 0 & - & - & 0 & - & 0 \\
0 & - & + & 0 & 0 & - & 0 & + & + & 0 & - & 0 & + & 0 & 0 & + & 0 & + & 0 & - & 0 & - & 0 & + & 0 & + & + & 0 & 0 & - & 0 & - \\
0 & + & + & 0 & - & 0 & 0 & - & + & 0 & 0 & + & 0 & + & + & 0 & - & 0 & - & 0 & + & 0 & - & 0 & 0 & + & + & 0 & 0 & + & 0 & + \\
- & 0 & 0 & + & 0 & - & + & 0 & 0 & + & - & 0 & - & 0 & 0 & + & 0 & - & 0 & - & 0 & + & 0 & - & - & 0 & 0 & + & - & 0 & - & 0 \\
- & 0 & 0 & - & + & 0 & 0 & - & 0 & - & + & 0 & - & 0 & 0 & + & - & 0 & - & 0 & + & 0 & 0 & + & - & 0 & - & 0 & 0 & - & 0 & - \\
0 & - & + & 0 & 0 & + & + & 0 & + & 0 & 0 & + & 0 & - & - & 0 & 0 & - & 0 & - & 0 & + & - & 0 & 0 & - & 0 & - & + & 0 & + & 0 \\
- & 0 & - & 0 & + & 0 & 0 & + & 0 & - & - & 0 & + & 0 & + & 0 & 0 & - & 0 & + & + & 0 & - & 0 & 0 & - & + & 0 & - & 0 & + & 0 \\
0 & - & 0 & - & 0 & + & - & 0 & + & 0 & 0 & - & 0 & + & 0 & + & + & 0 & - & 0 & 0 & + & 0 & - & + & 0 & 0 & + & 0 & - & 0 & + \\
+ & 0 & 0 & - & 0 & - & + & 0 & + & 0 & 0 & - & - & 0 & + & 0 & - & 0 & 0 & + & - & 0 & 0 & - & 0 & - & + & 0 & + & 0 & 0 & - \\
0 & + & + & 0 & + & 0 & 0 & + & 0 & + & + & 0 & 0 & - & 0 & + & 0 & - & - & 0 & 0 & - & + & 0 & + & 0 & 0 & + & 0 & + & + & 0 \\
+ & 0 & + & 0 & + & 0 & - & 0 & + & 0 & - & 0 & 0 & - & + & 0 & + & 0 & 0 & + & 0 & + & 0 & + & - & 0 & - & 0 & 0 & + & - & 0 \\
0 & + & 0 & + & 0 & + & 0 & - & 0 & + & 0 & - & + & 0 & 0 & + & 0 & + & - & 0 & - & 0 & - & 0 & 0 & - & 0 & - & - & 0 & 0 & - \\
+ & 0 & 0 & - & - & 0 & - & 0 & - & 0 & + & 0 & 0 & - & 0 & + & 0 & - & + & 0 & 0 & + & - & 0 & 0 & + & + & 0 & - & 0 & 0 & - \\
0 & + & + & 0 & 0 & - & 0 & - & 0 & - & 0 & + & + & 0 & - & 0 & + & 0 & 0 & + & - & 0 & 0 & - & - & 0 & 0 & + & 0 & - & + & 0 \\
0 & + & 0 & + & - & 0 & - & 0 & + & 0 & - & 0 & - & 0 & - & 0 & 0 & - & 0 & + & + & 0 & + & 0 & + & 0 & 0 & - & 0 & - & 0 & - \\
- & 0 & - & 0 & 0 & - & 0 & - & 0 & + & 0 & - & 0 & - & 0 & - & + & 0 & - & 0 & 0 & + & 0 & + & 0 & + & + & 0 & + & 0 & + & 0 \\
- & 0 & - & 0 & 0 & + & - & 0 & + & 0 & 0 & + & - & 0 & 0 & + & 0 & + & + & 0 & - & 0 & + & 0 & - & 0 & + & 0 & 0 & + & + & 0 \\
0 & - & 0 & - & - & 0 & 0 & - & 0 & + & - & 0 & 0 & - & - & 0 & - & 0 & 0 & + & 0 & - & 0 & + & 0 & - & 0 & + & - & 0 & 0 & + \\
0 & + & - & 0 & 0 & - & - & 0 & 0 & - & - & 0 & 0 & - & 0 & + & - & 0 & 0 & - & - & 0 & - & 0 & + & 0 & - & 0 & + & 0 & 0 & + \\
- & 0 & 0 & - & + & 0 & 0 & - & + & 0 & 0 & - & + & 0 & - & 0 & 0 & - & + & 0 & 0 & - & 0 & - & 0 & + & 0 & - & 0 & + & - & 0 \\
0 & + & 0 & - & 0 & + & 0 & + & - & 0 & - & 0 & + & 0 & - & 0 & - & 0 & - & 0 & 0 & + & + & 0 & - & 0 & + & 0 & + & 0 & - & 0 \\
- & 0 & + & 0 & - & 0 & - & 0 & 0 & - & 0 & - & 0 & + & 0 & - & 0 & - & 0 & - & - & 0 & 0 & + & 0 & - & 0 & + & 0 & + & 0 & - \\
0 & - & - & 0 & - & 0 & - & 0 & 0 & + & 0 & + & + & 0 & + & 0 & 0 & - & - & 0 & 0 & - & 0 & - & - & 0 & - & 0 & + & 0 & 0 & - \\
+ & 0 & 0 & - & 0 & - & 0 & - & - & 0 & - & 0 & 0 & + & 0 & + & + & 0 & 0 & - & + & 0 & + & 0 & 0 & - & 0 & - & 0 & + & + & 0 \\
0 & - & 0 & + & - & 0 & + & 0 & 0 & - & 0 & - & + & 0 & 0 & + & - & 0 & 0 & + & 0 & + & + & 0 & 0 & + & - & 0 & 0 & + & + & 0 \\
+ & 0 & - & 0 & 0 & - & 0 & + & + & 0 & + & 0 & 0 & + & - & 0 & 0 & - & - & 0 & - & 0 & 0 & + & - & 0 & 0 & - & - & 0 & 0 & +
\end{pmatrix}
$$

* * *

4.5. Monomial Equivalence. As before, we can impose an equivalence on the set of all $v \times b$ $(0, G)$-matrices, which will play an important part in what is to come.

4.24. Definition. Two $v \times b$ $(0, G)$-matrices A_1 and A_2 are said to be *monomially equivalent* if there are monomial $(0, G)$-matrices P and Q of orders v and b, respectively, such that

(4.24.a) $PA_1Q = A_2$.[16)]

In order to extend (1.15.a) and (3.18.a) to BGW matrices, we begin by altering somewhat Definition 4.5 as in Part V of Colbourn and Dinitz (2007).

4.25. Definition. let G be some finite group, and let A be a $v \times b$ $(0, G)$-matrix. If A has k non-zero entries in every column, and if there is an element $c \in (\frac{\lambda}{|G|}G)\backslash\{1\} \subset \mathbf{Z}[G]$ such that

(4.25.a) $AA^* = rI_v + c(J_v - I_v)$,

then we say that A is a c-GBRD$(v, k, \lambda - 1; G)$, or a c-GBRD$(v, b, r, k, \lambda - 1; G)$ if more precision required.

We can now properly extend the idea of normality to BGW matrices.

4.26. Definition. A BGW$(v, k, \lambda; G)$ is said to be in *normal form* if it has the form

(4.26.a) $\begin{pmatrix} \mathbf{0}_{v-k} & A_1 \\ \mathbf{1}_k & A_2 \end{pmatrix}.$

Note that of necessity, A_1 is a GBRD$(v - k, v - 1, k, k - \lambda, \lambda; G)$ and A_2 is a c-GBRD$(k, v - 1, k - 1, \lambda, \lambda - 1; G)$. These have the parameters of the residual and derived designs of a square BIBD(v, k, λ), hence we call them, respectively, a residual GBRD and a derived c-GBRD.

§5. Orthogonal Designs

In the previous section, we covered one generalization of weighing matrices, namely, we allowed the nonzero enetries to come from a finite group. In this section, we pursue another generalization in a different direction. In particular, instead of allowing the nonzero entries to come from some group, we will take the nonzero entries to be indeterminants—real, complex, or quaternary[17]).

* * *

5.1. Definitions. We begin with the case of real indeterminants.

5.1. Definition. Let $x_1, \ldots, x_u$ be real, commuting indeterminants, and let X be an $n \times n$ matrix with entries from $\{0, \pm x_1, \ldots, \pm x_u\}$. We say that X is an *orthogonal design* if

(5.1.a) $XX^t = \left(\sum_i s_i x_i^2\right) I_n.$

We say that the orthogonal design is of order n and type $(s_1, \ldots, s_u)$, and we write X is an OD$(n; s_1, \ldots, s_u)$. If $\sum_i s_i = n$, then we say that the OD is *full*.

5.2. Example. The following are examples of full ODs of types $(1,1)$, $(1,1,1,1)$, and $(1,1,1,1,1,1,1,1)$, respectively,

(5.2.a) $$\begin{pmatrix} a & b \\ \overline{b} & a \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ \overline{b} & a & \overline{d} & c \\ \overline{c} & d & a & \overline{b} \\ \overline{d} & \overline{c} & b & a \end{pmatrix}, \begin{pmatrix} a & b & c & d & e & f & g & h \\ \overline{b} & a & d & \overline{c} & f & \overline{e} & \overline{h} & g \\ \overline{c} & \overline{d} & a & b & g & h & \overline{e} & \overline{f} \\ \overline{d} & c & \overline{b} & a & h & \overline{g} & f & \overline{e} \\ \overline{e} & \overline{f} & \overline{g} & \overline{h} & a & b & c & d \\ \overline{f} & e & \overline{h} & g & \overline{b} & a & \overline{d} & c \\ \overline{g} & h & e & \overline{f} & \overline{c} & d & a & \overline{b} \\ \overline{h} & \overline{g} & f & e & \overline{d} & \overline{c} & b & a \end{pmatrix},$$

where we have used $\overline{x}$ to stand for $-x$. We do not have space to pursue these remarkable matrices here, but the interested reader is refered to Seberry (2017) and the references cited therein for details.

We now extend Definition 5.1 to the case of complex and quaternary numbers.

5.3. Definition. Let $z_1, \ldots, z_u$ be complex (resp. quaternary), commuting indeterminants, and let X be a matrix of order n with entries from $\{0, \varepsilon_1 z_1, \ldots, \varepsilon_u z_u\}$ and $\{\varepsilon_1 z_1^*, \ldots, \varepsilon_u z_u^*\}$, where each $\varepsilon_t \in \{\pm 1, \pm i\}$ (resp. $\varepsilon_t \in \{\pm 1, \pm i, \pm j, \pm k\}$). In the event that

(5.3.a) $XX^* = \left(\sum_i s_i |z_i|^2\right) I_n,$

then we say that X is a *complex* (resp. *quaternary*) orthogonal design of type $(s_1, \ldots, s_u)$. We write X is a COD$(n; s_1, \ldots, s_u)$ (resp. QOD$(n; s_1, \ldots, s_u)$).

5.4. Example. The matrix

(5.4.a) $$\begin{pmatrix} ia & b \\ b & ia \end{pmatrix},$$

where a and b are real commuting indeterminants, is a $\mathrm{COD}(2;1,1)$.

5.5. Example. The matrix

$$\text{(5.5.a)}\quad \begin{pmatrix} \overline{a} & \overline{b} & ic & ic \\ b & \overline{a} & ic & i\overline{c} \\ j\overline{c} & j\overline{c} & ka & kb \\ j\overline{c} & jc & k\overline{b} & ka \end{pmatrix},$$

where a, b, and c are real indeterminants, is a $\mathrm{QOD}(4;1,1,2)$.

* * *

5.2. Sequences and Circulants. Let A be an $n \times n$ matrix with first row $(a_0, \ldots, a_{n-1})$. Recall that A is *circulant* if $A_{ij} = a_{j-i}$, where the indices are calculated modulo n. In this way, the entire matrix is determined by its first row; moreover, if A and B are two circulants of the same dimension, then A^t, $A+B$, and AB are also circulant matrices. Therefore, to effect a study of circulant matrices, we can profitably study sequences.

What we are particularly interested with here is the following.

5.6. Definition. Let $\mathcal{A} = \{A_i\}$ be a finite collection of circulant matrices of the same dimension over a commutative ring R endowed with an involution $\cdot^*$. The collection $\mathcal{A}$ is said to be *complementary* if

$$\text{(5.6.a)}\quad \sum_i A_i A_i^* = aI, \text{ for some } a \in R,$$

where, as usual, $(m_{ij})^* = (m_{ji}^*)$.

Note, however, that we can state this in terms of sequences. First, a definition.

5.7. Definition. Let $a_0 = (a_{0,0}, \ldots, a_{0,n-1})$ be a sequence in a commutative ring R with the involution $\cdot^*$. The *j-th aperiodic* and *j-th periodic autocorrelations* of the sequence a are given respectively by

(5.7.a) $N_j(a) = \sum_{i=0}^{n-j-1} a_{0,i}a^*_{0,i+j}$, and

(5.7.b) $P_j(a) = \sum_{i=0}^{n-1} a_{0,i}a^*_{0,i+j}$, indices calculated modulo n.

If $a_1 = (a_{1,0}, \ldots, a_{1,n-1}), \ldots, a_m = (a_{m,1}, \ldots, a_{m,n-1})$ are any other sequence in R, then $a_0, \ldots, a_m$ are *complementary* if

(5.7.c) $\sum_i P_j(a_i) = 0$, for every $j \in \{1, \ldots, n-1\}$.

For the case in which $m = 1$, we say that we have a *Golay pair*.

We see immediately that $P_j(a) = N_j(a) + N_{n-j}(a)^*$; hence, if $N_j(a) + N_j(b) = 0$, for every $j \in \{1, \ldots, n-1\}$, then a and b are complementary. However, vanishing periodic autocorrelations does not in general imply vanishing aperiodic autocorrelations.

The importance of the periodic correlation is given by the fact that if the first row of the circulant A continues to be $a = (a_0, \ldots, a_{n-1})$, then the first row of AA^* is given by $(\sum_i |a_i|^2, P_{n-1}(a), \ldots, P_1(a))$. So we see that complementary circulants and complementary sequences are one and the same.

Complementary sequences and orthogonal designs are connected in an intimate way; in fact, complementary sequences offer many elegant constructions of ODs. To make the connection precise, we need to allow sequence elements to be indeterminants whether real, complex, or quaternary, and where the involution is taken to be conjugation.

5.8. Proposition. Let $\{z_1, \ldots, z_u\}$ be commuting quaternary indeterminants, and let $a = (a_0, \ldots, a_{n-1})$ and $b = (b_0, \ldots, b_{n-1})$ be complementary sequences with entries from $\{0, \varepsilon_0 z_0, \ldots, \varepsilon_u z_u\}$, where $\varepsilon_t \in \{\pm 1, \pm i, \pm j, \pm k\}$, such that

$\sum_i(|a_i|^2 + |b_i|^2) = \sum_i s_i x_i^2$. Then

(5.8.a) $\begin{pmatrix} A & B \\ -B^* & A^* \end{pmatrix}$

is a QOD$(2n; s_1, \ldots, s_u)$, where A and B are the circulants with first rows a and b, respectively.

Proof. A restatement of (5.7.c). ∎

The matrix (5.8.a) will feature as a submatrix in our later work where the sequences will be composed of matrices. We will need one further idea before we proceed.

5.9. Definition. Let $a = (a_0, \ldots, a_{n-1})$ and $b = (b_0, \ldots, b_{n-1})$ be two sequences over a ring with involution $\cdot^*$. The *j-th cross-correlation* of a by b is given by

(5.9.a) $C_j(a, b) = \sum_{i=0}^{n-1} a_i b_{i+j}^*$, for each $j \in \{1, \ldots, n-1\}$.

If A has first row $a = (a_0, \ldots, a_{n-1})$, and if B has first row $b = (b_0, \ldots, b_{n-1})$, then the first row of the circulant AB^* is $(\sum_i a_i b_i^*, C_{n-1}(a, b), \ldots, C_1(a, b))$. Note, however, that $C_j(a, b)$ is not in general equal to $C_j(b, a)$. So, care must be taken in extending Proposition 5.8 since amicability is required in maintaining orthogonality when substituting into an OD.

Much more can be said about this most useful topic. The interested reader is may consult Seberry (2017) and Seberry and Yamada (1992) for a wealth of material.

Notes

8. Cauchy's determinant property states that if $\{A_i\}$ is a finite set of square matrices of the same order, then $\det(\prod_i A_i) = \prod_i \det(A_i)$.

9. This is a consequences of the Hasse-Minkowski Theory, more specifically, the Bruck-Ryser-Chowla Theorem. There are a number of references that treat this result. The interested reader is asked to consult Hall (1986) and Stinson (2004).

10. Let V and W be two linear spaces, and let $T : V \to W$ be a linear epimorphism. Recall that $W \simeq V/\ker(T)$. In the case that the spaces are finite-dimensional, we have $\dim(V) = \mathrm{rank}(T) + \mathrm{null}(T)$.

11. Let $K = \mathrm{GF}(q)$ and $F = \mathrm{GF}(q^n)$. The *relative trace function* $\mathrm{Tr}_{F/K} : F \to K$ is defined by $\mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}$. In the case that K is prime, $\mathrm{Tr}_{F/K}$ is the *absolute* trace function. Similarly, the relative norm $\mathrm{N}_{F/K} : F \to K$ is defined by $\mathrm{N}(\alpha) = \alpha^{1+q+\cdots+q^{n-1}} = \alpha^{\frac{q^n-1}{q-1}}$. See Lidl and Niederreiter (1994) for details.

12. Let H and $G \leq S_v$ be finite groups. Recall that the wreath product $H \wr G$ is the semi direct product $H^v \rtimes G$ where $g(h_0, \ldots, h_{v-1})g^{-1} = (h_{g^{-1}0}, \ldots, h_{g^{-1}(v-1)})$. Let $H = \{-1, 1\}$, and let $G = H \wr S_v$. We define an action of $G \times G$ on the set of (-1,0,1)-matrices by $\mu(W, (P, Q)) = P^t W Q$. The Hadamard equivalent weighing matrices reside in the same orbits of this action.

13. Here, we are doing arithmetic over the group ring $\mathbf{Z}[G]$, and $\mathbf{Z}G$, as is custumary, denotes the integer multiples of $\sum_{g \in G} g$.

14. If $q = p^n$, for some prime p, then $\mathrm{EA}(q) \simeq \underbrace{C_p \times \cdots \times C_p}_{n}$.

15. By note 12, it follows that the ω of Proposition 4.17 is the multiplicative inverse of the relative norm of the primitve element β.

16. Let $H_1 = G \wr S_v$, let $H_2 = G \wr S_b$, and let $H = H_1 \times H_2$. We define an action of H on the set of all $v \times b$ $(0, G)$-matrices by $\mu(A, (P, Q)) = P^* A Q$. The monomially equivalent matrices are composed precisely by the orbits of this action.

17. Recall that the quaternion group $\{\pm 1, \pm i, \pm j, \pm k\}$ is defined with anticommutative multiplication given by $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j$. We then take the quaternion algebra to be the $\mathbf{R}$-algebra $\{a_1 + a_i i + a_j j + a_k k : a_1, a_i, a_j, a_k \in \mathbf{R}\}$. Conjugation is extended to the quaternion algebra by $(a_1 + a_i i + a_j j + a_k k)^* = a_1 - a_i i - a_j j - a_k k$.

3

Association Schemes

This third and final preliminary chapter briefly touches on association schemes, a fundamental abstract object used as a unifying tool across the otherwise disparate fields of combinatorics. It is composed of two sections. The first will introduce the basic ideas via strongly regular graphs, the simplest nontrivial example of an association scheme. The second moves on to consider these objects in general. Only enough theory is developed in order to be applied in later chapters.

§6. Strongly Regular Graphs

This section introduces the so-called strongly regular graphs. Much attention has been given to these objects, both in excogitating their properties as well as answering existence and classification problems. Many of the resuts of this section will be generalized in the next section.

* * *

6.1. Definition and Elementary Properties. A *graph*, similar to a balanced incomplete block design, is simply an ordered pair $\Gamma = (V, E)$ where V is a finite set of v points, called *vertices*, and where $E \subset \binom{V}{2}$, called the *edges*.[18])

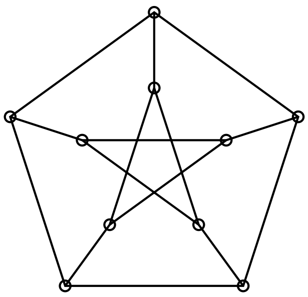
If $x, y \in V$ are distinct, and if $\{x, y\} \in E$, then we say that x and y are *adjacent*, and we write $x \sim y$. If there is a sequence of vertices $x = v_0, v_1, \ldots, v_{n-1} = y$ such that $v_{i-1} \sim v_i$, for $i \in \{1, \ldots, n-1\}$, then we say that x and y are *connected*. Connectedness is easily seen to be an equivalence relation of the vertex set V.

The *degree* of vertex x is defined as the number of vertices that are adjacent to x. If every vertex has the same degree, say, k, then we say that the graph is *regular* with degree k.

The *complement* of a graph $\Gamma = (V, E)$ is given by $\overline{\Gamma} = (V, \binom{V}{2} \backslash E)$.

6.1. Example. The following is a graph on 10 vertices called the *Petersen graph*, where the vertices are the nodes, and where the line segments represent adjacencies. One can see that each pair of distinct vertices are connected.

(6.1.a)



This graph evinces further interesting properties, namely, the graph is regular with degree 3, each pair of adjacenct vertices have 0 common neighbours, and each pair of non-adjacenct vertices have 1 common neighbour.

The above example motivates the following definition.

6.2. Definition. Let $\Gamma = (V, E)$ be a graph with $|V| = v$. Γ is said to be *strongly regular* if the following are satisfied.

(6.2.a) The graph is regular with degree k,

(6.2.b) each pair of adjacenct vertices have λ common neighbours, and

(6.2.c) each pair of non-adjacenct vertices have μ common neighbours.

In such a case we write Γ is an SRG(v, k, λ, μ).

6.3. Example. The Petersen graph of Example 6.1 is an SRG$(10, 3, 0, 1)$.

6.4. Example. Let $[m] = \{0, \ldots, m-1\}$, for $m > 2$, and take $V = \binom{[m]}{2}$. Define adjacencies by $x \sim y$ iff $|x \cap y| = 1$. The ensuing structure is called the T(m) graph. Clearly, the graph is regular of degree $k = 2(m-2)$. The vertices adjacent to both $\{a, c\}$ and $\{b, c\}$ are given by those $\{c, d\}$, where $d \neq a, b, c$, and $\{a, b\}$. Hence, $\lambda = m - 2$. Finally, the number of vertices adjacent to the nonadjacent vertices $\{a, b\}$ and $\{c, d\}$ is given by $\{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}$; hence, $\mu = 4$. We have shown that T(m) is strongly regular with parameters $(m(m-1)/2, 2(m-2), m-2, 4)$.

6.5. Proposition. The parameters of an SRG(v, k, λ, μ) satisfy

(6.5.a) $k(k - \lambda - 1) = \mu(v - k - 1)$.

Proof. Let $\Gamma = (V, E)$ be an SRG(v, k, λ, μ), and fix a vertex $x \in V$. Count in two ways the edges $\{y, z\} \in E$ such that $x \sim y$, $x \not\sim z$, and $z \neq x$. First, there are k choices for y and $k - \lambda - 1$ choices for z. On the other hand, there are $v - k - 1$ choices for z and μ choices for y. ∎

With graphs, as with BIBDs, we can represent these objects with matrices.

6.6. Definition. Let $\Gamma = (\{x_0, \ldots, x_{v-1}\}, E)$ be some graph. The *adjacency matrix* $A = A(\Gamma)$ of Γ is the $(0, 1)$-matrix of order v defined by

(6.6.a) $A_{ij} = \begin{cases} 1 & \text{if } x_i \sim x_j \text{, and} \\ 0 & \text{otherwise.} \end{cases}$

From the definition, we can se that $A(\Gamma)$ is symmetric and has zero diagonal. Furthermore, $A(\overline{\Gamma}) = J - I - A(\Gamma)$.

Using the adjacency matrix, it turns out that SRGs are completely characterized by a simple matrix equation.

6.7. Proposition. A graph Γ with adjacency matrix $A = A(\Gamma)$ is strongly regular with parameters (v, k, λ, μ) if and only if

(6.7.a) $A^2 = kI + \lambda A + \mu(J - I - A)$.

Proof. Restatement of Definition 6.2. ∎

6.8. Corollary. The complement of an SRG(v, k, λ, μ) is an SRG$(v, v - k - 1, v - 2k + \mu - 2, v - 2k + \lambda)$.

We conclude this subsection with one further result. Its justification is rather immediate, and as such, it is omitted (see Ionin and Shrikhande, 2006, Proposition 7.1.6).

6.9. Proposition. Let Γ be an SRG(v, k, λ, μ). Then the following are equivalent.

(6.9.a) $\mu = 0$;

(6.9.b) $k = \lambda + 1$;

(6.9.c) Γ is not connected; and

(6.9.d) Γ is the disjoint union of v/k copies of K_k.

The above proposition shows that the interesting SRGs are those which are connected. We will assume this to be the case unless otherwise stated.

* * *

6.2. Eigenvalues. This subsection will closely follow §1.2 of Bannai et al. (2021).

Let Γ be an SRG(v, k, λ, μ) with adjacency matrix $A = A(\Gamma)$. Since Γ is regular of degree k, it follows that $AJ = JA = kJ$. Since A and J are then symmetric matrices which commute, they are simultaneously orthogonally diagonalizable[19]).

The rank of J is one, and its eigenvalues are v and 0 with multiplicities 1 and $v - 1$, respectively.

Since Γ is regular of degree k, it has eigenvalue k with multiplicity given by the number of connected components of the graph (see Bannai and Ito, 1984, Theorem 1.5). Since we are assuming that Γ is connected, the eigenvalue k has multiplicity 1. Moreover, by (6.7.a), it follows that $k^2 = k + \lambda k + \mu(v - k - 1)$, which shows again (6.5.a).

Since Tr$(A) = 0$, it follows that there is at least one further eigenvalue. If there is only one further eigenvalue, say ϱ, then $k + (v - 1)\varrho = 0$; hence, $\varrho = -\frac{k}{v-1}$ is a rational integer. But this would imply that $\Gamma = K_v$, the complete graph on v vertices[20]). We therefore assume that Γ has more than two eigenvalues.

If ϱ is any other eigenvalue of A, then $\varrho^2 = k - \mu + (\lambda - \mu)\varrho$; hence, there are precisely three eigenvalues of A given by k, r, and s, where

$$r = (\lambda - \mu + \sqrt{(\lambda - \mu)^2 + 4(k - \mu)})/2, \text{ and}$$
$$s = (\lambda - \mu - \sqrt{(\lambda - \mu)^2 + 4(k - \mu)})/2.$$

Furthermore, if the multiplicities of r and s are f and g, respectively, then

$v = 1 + f + g$ and $k + fr + gs = 0$. Solving this system yields

$$f = (v - 1 + [(\mu - \lambda)(v - 1) - 2k]/\sqrt{(\lambda - \mu)^2 + 4(k - \mu)})/2, \text{ and}$$
$$g = (v - 1 - [(\mu - \lambda)(v - 1) - 2k]/\sqrt{(\lambda - \mu)^2 + 4(k - \mu)})/2.$$

We have shown the following result.

6.10. Theorem. Let Γ be a connected, noncomplete SRG(v, k, λ, μ) with adjacency matrix $A = A(\Gamma)$. Then A has eigenvalues

(6.10.a) k of multiplicity 1,

(6.10.b) $r = \frac{1}{2}(\lambda - \mu + \sqrt{(\lambda - \mu)^2 + 4(k - \mu)})$ of multiplicity $f = \frac{1}{2}\left(v - 1 + \frac{(\mu-\lambda)(v-1)-2k}{\sqrt{(\lambda-\mu)^2+4(k-\mu)}}\right)$, and

(6.10.c) $s = \frac{1}{2}(\lambda - \mu - \sqrt{(\lambda - \mu)^2 + 4(k - \mu)})$ of multiplicity $g = \frac{1}{2}\left(v - 1 - \frac{(\mu-\lambda)(v-1)-2k}{\sqrt{(\lambda-\mu)^2+4(k-\mu)}}\right)$.

Moreover, we have that

(6.10.d) $\lambda = k + r + s + rs$, and

(6.10.e) $\mu = k + rs$.

* * *

6.3. Generated Matrix Algebra. Let Mat$_v(\mathbf{C})$ be the algebra of $v \times v$ matrices with entries from $\mathbf{C}$. Let Γ be an SRG, and let $A = A(\Gamma)$ and $\overline{A} = A(\overline{\Gamma})$. Since $A + \overline{A} = J - I$, it follows that I, A and $\overline{A}$ are $\mathbf{C}$-linearly independent and, therefore, span a 3-dimensional linear subspace of Mat$_v(\mathbf{C})$, say, $\mathfrak{U}$.

If we use $\cdot \circ \cdot$ to denote Schur multiplication[21]), then we see at once that $X \circ X = X$, for each $X \in \{I, A, \overline{A}\}$. Therefore, $\mathfrak{U}$ is closed under Schur multiplication. We denote this algebra as $\hat{\mathfrak{U}}$ and call I, A, and $\overline{A}$ the *Schur idempotents* of $\hat{\mathfrak{U}}$.

It turns out that $\mathfrak{U}$ also has an algebra structure with respect to matrix multiplication.

6.11. Proposition. Let Γ be an SRG, and let $A = A(\Gamma)$. Then $\mathfrak{U} = \langle I, A, \overline{A} \rangle$ is a commutative matrix algebra.

Proof. By (6.7.a), we have that $J - I = \mu^{-1}[A^2 + A(\mu - \lambda) - kI]$. Therefore, $\overline{A} = \mu^{-1}A^2 + A[\mu^{-1}(\mu - \lambda) - 1] - \mu^{-1}kI$; so, $\overline{A}$ is a polynomial in A, whence it commutes with A. Then

$$\begin{aligned}\overline{A}A = A\overline{A} &= A(J - I - A) = kJ - A - A^2 \\ &= kJ - A - kI - \lambda A - \mu\overline{A} \\ &= k(I + A + \overline{A}) - A - kI - \lambda A - \mu\overline{A} \\ &= (k - \lambda - 1)A + (k - \mu)\overline{A},\end{aligned}$$

and $A\overline{A} = \overline{A}A \in \mathfrak{U}$. By (6.7.a), we see that $A^2, \overline{A}^2 \in \mathfrak{U}$. We therefore have that $\mathfrak{U}$ is closed under standard matrix multiplication. ∎

Since I, A, and $\overline{A}$ are symmetric, pairwise commuting matrices, they are simultaneously diagonalizable; hence, $\mathfrak{U}$ is semisimple (see Lang, 2002). It follows that there are matrices $E_0, E_1, E_2 \in \mathfrak{U}$ such that (a) $\mathfrak{U} = \langle E_0, E_1, E_2 \rangle$, (b) $E_0 + E_1 + E_2 = I$, and (c) $E_iE_j = \delta_{i,j}E_j$.

§7. Association Schemes

Here we generailze some the concepts of the previous section, and we will mostly draw from Chapter 2 of Bannai and Ito (1984), the standard reference on the subject.

* * *

7.1. Definitions. We begin with the following definition.

7.1. Definition. Let X be a finite set of v elements, and let $\mathscr{R} = \{R_0, \ldots, R_d\}$ be a collection of relations on X. We say that the ordered pair $\mathfrak{X} = (X, \mathscr{R})$ is an *association scheme* with d *classes* whenever the following are satisfied.

(7.1.a) $R_0 = \{(x,x) : x \in X\}$;

(7.1.b) $R_i \cap R_j = \emptyset$ and $X \times X$ is the disjoint union of $R_0, \ldots, R_d$;

(7.1.c) $R_i^t = R_{i'}$ for some $i' \in \{0, \ldots, d\}$, where $R_i^t = \{(x,y) : (y,x) \in R_i\}$; and

(7.1.d) Given $(x,y) \in R_k$, the number of $z \in X$ such that $(x,z) \in R_i$ and $(z,y) \in R_j$ is a constant p_{ij}^k. We call the p_{ij}^k, the *intersection numbers* of the scheme.

The scheme $\mathfrak{X}$ is *commutative* if

(7.1.e) $p_{ij}^k = p_{ji}^k$, for all $i, j, k \in \{0, \ldots, d\}$.

The scheme is *symmetric* if

(7.1.f) $i = i'$, for every $i \in \{0, \ldots, d\}$.

We denote p_{ii}^0 as k_i, the *valency* of the relation R_i.

We present a few classical examples.

7.2. Example. Let G be a transitive permutation group on a set X, and let $\mathscr{R}$ be the collection of orbits of G on $X \times X$. Then $\mathfrak{X} = (X, \mathscr{R})$ is an association scheme (see Higman, 1975, 1976). In general $\mathfrak{X}$ is non-commutative; however, the scheme is commutative if and only if the Hecke algebra is commutative (see Wielandt, 1964). $\mathfrak{X}$ is symmetric if and only if the group is generously transitive[22]).

7.3. Example. Recall The definition of a q-ary code. Let $\mathcal{A}$ be our q-ary alphabet, and take $X = \underbrace{\mathcal{A} \times \cdots \times \mathcal{A}}_{n}$. We partition $X \times X$ in the following way. We take $(x, y) \in R_i$ if and only if $\text{dist}(x, y) = i$. Since the wreath product $S_q \wr S_n$ acts transitively on each R_i, we have that $\mathfrak{X} = (X, \mathscr{R})$ is a symmetric association scheme on n classes called the *Hamming scheme*.

7.4. Example. Let V be a set of order v, and take $X = \binom{V}{k}$, where $k \leq v/2$. Partition $X \times X$ by $(x, y) \in R_i$ if and only if $|x \cap y| = k - i$. The symmetric group S_v acts transitively on each R_i, hence $\mathfrak{X} = (X, \mathscr{R})$ is a symmetric association scheme of k classes called the *Johnson scheme*.

Unless otherwise stated, we will assume that the association schemes we are working with are commutative.

* * *

7.2. Adjacency Algebras. The importance of association schemes resides in the following definition.

7.5. Definition. Let $\mathfrak{X} = (X, \mathscr{R})$ be a d-class assocation scheme. For $i \in \{0, \ldots, d\}$, define the $v \times v$ $(0, 1)$-matrix A_i with rows and columns indexed by elements of X by $(A_i)_{xy} = 1$ if and only if $(x, y) \in R_i$. We call A_i the *adjacency matrix* of the relation R_i. Then Definition 7.1 is equivalent to the following.

(7.5.a) $A_0 = I$;

(7.5.b) $A_0 + \cdots + A_d = J$;

(7.5.c) $A_i^t = A_{i'}$ for some $i' \in \{0, \ldots, d\}$; and

(7.5.d) $A_i A_j = \sum_k p_{ij}^k A_k$, for every $i, j \in \{0, \ldots d\}$.

If $\mathfrak{X}$ is commutative, then

(7.5.e) $A_iA_j = A_jA_i$, for each $i, j \in \{0, \ldots, d\}$.

If $\mathfrak{X}$ is symmetric, then

(7.5.f) $A_i^t = A_i$, for every $i \in \{0, \ldots, d\}$.

By (7.5.b), the adjacency matrices of the scheme are $\mathbf{C}$-linearly independent and generate a subspace $\mathfrak{U}$ of $\mathrm{Mat}_v(\mathbf{C})$ of dimension $d+1$. By (7.5.d), $\mathfrak{U}$ is closed under standard matrix multiplication. We call $\mathfrak{U}$ the *adjacency algebra* of the association scheme $\mathfrak{X}$.

We further have that $A_i \circ A_j = \delta_{ij}A_i$. Therefore, $A_0, \ldots, A_d$ also generate a commutative algebra $\hat{\mathfrak{U}}$ with Schur multiplication for which they are primitive idempotents[23]). We therefore also call the adjacency matrices the *Schur idempotents* of the scheme.

Assume an ordering of $X = \{x_0, \ldots, x_{v-1}\}$, and take e_{x_i} to be the standard vector with i-th position equal to 1 and 0 elsewhere. Take V to be the Hermitian space with the standard orthonormal basis $\{e_x : x \in X\}$.

Since we are assuming commutativity, the adjacency matrices $A_0, \ldots, A_d$ are pairwise commuting, normal matrices. So, they share an eigenbasis, and by the Spectral Theorem for normal matrices, $V = \bigoplus_{i=1}^r V_i$, where the V_i are maximal common eigenspaces.

Since $J = \sum_i A_i$, we find the eigenspace corresponding to the eigenvalue v is spanned by $\mathbf{1}_v$, i.e. it is 1-dimensional and hence maximal. It follows that this space is equal to V_i for some i. We can assume, then, that $i = 0$.

If we take E_i to be the orthogonal projection $V \to V_i$ with respect to the basis $\{e_x : x \in X\}$, then we can assume that $E_0 = |X|^{-1}J$, and we have $E_0 + \cdots + E_d = I$. Moreover, there is a unitary matrix Λ such that $\Lambda^* E_i \Lambda = \mathrm{diag}(0, \ldots, 0, \underbrace{1, \ldots, 1}_{m_i}, 0, \ldots, 0)$, where we have used m_i to denote $\dim(V_i)$. The numbers m_i, for $i \in \{0, \ldots, d\}$, are called the *multiplicities* of the scheme.

It can be shown (see Bannai and Ito, 1984, Theorem 3.1) that the projection matrices $E_0, \ldots, E_d$ are primitive idempotents of $\mathfrak{U}$ and form a dual basis of $\mathfrak{U}$. It follows that there are constants P_{ij} and Q_{ij}, for $i, j \in \{0, \ldots, d\}$, called the *eigenvalues* and *dual-eigenvalues* of the scheme, such that $A_j = \sum_i P_{ij} E_i$ and $E_j = |X|^{-1} \sum_i Q_{ij} A_i$. Using these constants, we form the matrices P and Q with (i, j)-th entry given by P_{ij} and Q_{ij}, respectively, and we call these matrices the *first* and *second character tables* of the scheme. By what has been said, we have at once that $PQ = QP = vI$.

7.6. Example. Using the notation of the previous section, we see that a strongly regular graph has first and second character tables

$$\text{(7.6.a)} \quad \begin{pmatrix} 1 & k & v-k-1 \\ 1 & r & -r-1 \\ 1 & s & -s-1 \end{pmatrix}, \frac{1}{r-s} \begin{pmatrix} r-s & -k-(v-1)s & k+(v-1)r \\ r-s & v-k-s & k-v-r \\ r-s & s-k & k-r \end{pmatrix},$$

respectively.

* * *

7.3. Parameters. As we have seen, there are numerous parameters related to a given assocation scheme. The regular structure of a scheme allows us to relate these parameters together in a number of interesting ways.

To begin, we have a few immediate properties of the intersection numbers.

7.7. Proposition.

(7.7.a) $p^k_{0j} = \delta_{jk}$,

(7.7.b) $p^k_{i0} = \delta_{ik}$,

(7.7.c) $p^0_{ij} = k_i \delta_{ij'}$,

(7.7.d) $p^k_{ij} = p^{k'}_{i'j'}$,

(7.7.e) $\sum_{j=0}^{d} p^k_{ij} = k_i$,

(7.7.f) $k_\gamma p^\gamma_{\alpha\beta} = k_\beta p^\beta_{\alpha'\gamma} = k_\alpha p^\alpha_{\gamma\beta'}$, and

(7.7.g) $\displaystyle\sum_{\alpha=0}^{d} p^\alpha_{ij} p^\ell_{k\alpha} = \sum_{\beta=0}^{d} p^\beta_{ki} p^\ell_{\beta j}$.

Proof. (7.7.a-d) are a restatment of the definitions. To show (7.7.e), fix a pair $(x, y) \in R_k$ and count the points $z \in X$ such that $(x, z) \in R_i$. For (7.7.f), count the triangles (x, y, z) such that $(x, y) \in R_\gamma$, $(x, z) \in R_\alpha$, and $(z, y) \in R_\beta$. Finally, we show (7.7.g) in the following way. Fix a pair $(x, y) \in R_\ell$ and count the pairs (z, w) such that $(x, z) \in R_k$, $(z, w) \in R_i$, and $(w, y) \in R_j$. ∎

Regarding the bases, we have the following, where $\tau(C) = \sum_{i,j} C_{ij}$ is the sum of the elements of the matrix C.

7.8. Proposition.

(7.8.a) $\mathrm{Tr}(A_i) = \delta_{i0}|X|$,

(7.8.b) $\tau(A_i) = |X|k_i$,

(7.8.c) $\mathrm{Tr}(E_i) = m_i$, and

(7.8.d) $\tau(E_i) = \delta_{i0}|X|$.

Proof. Trivial. ∎

Regarding the character tables of the scheme, we have the following two propositions.

7.9. Proposition. For each $i \in \{0, \ldots, d\}$,

(7.9.a) $P_{i0} = 1$,

(7.9.b) $P_{0i} = k_i$,

(7.9.c) $Q_{i0} = 1$, and

(7.9.d) $Q_{0i} = m_i$.

Proof. To show (7.9.a), compare coefficients in $\sum_i E_i = A_0 = I = \sum_i P_{i0} E_i$. To show (7.9.b), apply the functional τ to $A_i = \sum_j P_{ji} E_j$. Comparing coefficients in $E_0 = |X|^{-1} J = |X|^{-1} \sum_i A_i$ yields (7.9.c). Finally, taking the trace of $E_i = |X|^{-1} \sum_j Q_{ji} A_j$ gives (7.9.d). ∎

7.10. Proposition. For each $i, j \in \{0, \ldots, d\}$,

(7.10.a) $Q_{ij}/m_j = \overline{P_{ij}}/k_i$,

(7.10.b) $\sum_{\nu=0}^{d} k_\nu^{-1} P_{i\nu} \overline{P_{j\nu}} = \delta_{ij} |X|/m_i$, and

(7.10.c) $\sum_{\nu=0}^{d} m_\nu P_{\nu i} \overline{P_{\nu j}} = \delta_{ij} |X| k_i$.

It is custumary to refer to (7.10.b) and (7.10.c) as the *first* and *second orthogonality relations of association schemes*.

Proof. To show (7.10.a), note that $E_j \circ A_i = |X|^{-1} Q_{ij} A_i$; hence,

$$\begin{aligned} \tau(E_j \circ A_i) &= \mathrm{Tr}(E_j A_i^t) \\ &= \mathrm{Tr}(E_j A_{i'}) \\ &= \mathrm{Tr}(P_{ji'} E_j) \\ &= P_{ji'} m_j \\ &= m_j \overline{P_{ji}}. \end{aligned}$$

Similarly, $\tau(|X|^{-1}Q_{ij}A_i) = Q_{ij}k_i$. The remaining points follow by writing $PQ = |X|I$ and $QP = |X|$ entrywise. ∎

Much more can be said of this most intersting topic, but we do not have the space to pursue it here. It suffices to say that the character tables of a scheme in a sense characterize the scheme. In order to derive these character tables, however, we will often try to employ a further object, namely, the intersection matrices of the scheme.

* * *

7.4. Intersection Matrices. If we regard left multiplication of $\mathfrak{U}$ as linear transformations of $\mathfrak{U}$ and express them in terms of the basis $\{A_0, \ldots, A_d\}$, then we have an algebra homomorphism $\mathfrak{U} \to \mathrm{Mat}_v(\mathbf{C})$ called the *left regular representation of* $\mathfrak{U}$ with respect to $\{A_0, \ldots, A_d\}$.

For $i \in \{0, \ldots, d\}$, define the matrix B_i by $(B_i)_{jk} = p^k_{ij}$, called the *i-th intersection matrix*. It then follows by (7.5.d) that the image of A_i under the above homomorphism is B_i^t, whence $A_i \leftrightarrow B_i^t$ is an isomorphism. Since, however, we are assuming that our schemes are commutative, transposition is an isomorphism; thus, $A_i \leftrightarrow B_i$ is an isomorphism. If we denote $\mathfrak{B} = \langle B_0, \ldots, B_d \rangle$, then we have shown $\mathfrak{U} \simeq \mathfrak{B}$.

That the intersection matrices and the isomorphism given above are important for us is shown in the next result. First, however, we say that a vector is in *standard form* if the first entry is 1.

7.11. Theorem. Let $\mathfrak{X} = (X, \mathscr{R})$ be a commutative association scheme with d classes. Let $v_i = (P_{i0}, \ldots, P_{id})$ and $u_i = (\overline{P_{i0}}/k_0, \ldots, \overline{P_{id}}/k_d)$ be the row vectors obtained by standardizing the first row and column of P and Q, respectively. Then u_i is the unique standardized common left eigenvector u of the matrices B_j such that $uB_j = P_{ij}u$. Similarly, v_i^t is the common right eigenvector v^t of the matrices B_j such that $B_jv^t = P_{ij}v^t$.

Proof. We consider the left regular representation of the adjacency algebra $\mathfrak{U}$ of $\mathfrak{X}$. With respect to the basis $\{A_0, \ldots, A_d\}$, the image of A_j is B_j^t. With respect to the basis $\{E_0, \ldots, E_d\}$, the image of A_j is $\text{diag}(P_{0j}, \ldots, P_{dj})$. Since $E_jP = A_j$, we have that $B_j^t = P^{-1}\text{diag}(P_{0j}, \ldots, P_{dj})P$, hence $B_jP^t = P^t\text{diag}(P_{0j}, \ldots, P_{dj})$. Thus, the i-th column v_i^t of P^t is a right eigenvector of B_j belonging to the eigenvalue P_{ij}.

Multiplying by Q^t on the right and left, $Q^tB_j = \text{diag}(P_{0j}, \ldots, P_{dj})Q^t$. So, the i-th row vector $(Q_{0i}, \ldots, Q_{di})$ of Q^t is a left eigenvector of B_j belonging to the eigenvalue P_{ij}. By (7.10.a), $m_i^{-1}(Q_{0i}, \ldots, Q_{di}) = u_i$.

Let u be a common left eigenvector of B_j such that $uB_j = P_{ij}u$, for all j. By the linear independence of $\{u_k\}$, we can write $u = \sum_k \lambda_k u_k$. Applying B_j, $P_{ij}\sum_k \lambda_k u_k = \sum_k \lambda_k P_{kj}u_k$, hence $\lambda_k P_{ij} = \lambda_k P_{kj}$, for every j. If $\lambda_k \neq 0$, then $P_{ij} = P_{kj}$ so that $i = k$ as $\det(P) \neq 0$. Therefore, u is a multiple of u_i

v_i^t is similarly characterized. ∎

As stated in Bannai and Ito (1984), by virture of this result, one can conceivably derive the character tables P and Q from the intersection matrices. In particular, if the algebra $\mathfrak{B}$ is generated by a single B_j, we can use the single matrix B_j to calculate the character tables. Following Lemma 2.2.1 of Brouwer et al. (1989), the authors go on to point out that if some B_j has $d + 1$ distinct eigenvalues, then we can similarly use this intersection matrix. Of course, if $\mathfrak{B}$ is cyclic, then this property is satisfied by the generator matrix.

Notes

18. NB: Our definition of a graph given here precludes the case of loops, that is, it is assumed that $x \sim x$ can never happen. Moreover, the graph is undirected: If $x \sim y$, then $y \sim x$, and we do not differentiate these two cases. To use the standard nomenclature, this is a simple, undirected graph.

19. More generally, if $\{A_i\}$ is a finite collection of pairwise commuting, diagonalizable matrices, then they share an eigenbasis; hence, there is a matrix Λ such that $\Lambda^* A_i \Lambda$ is diagonal, for each i.

20. Note that $A(K_n) = J - I$; so, K_n has eigenvalue $n-1$ with eigenvector $\mathbf{1}$. Next, $A+I$ has rank 1 so that there are $n-1$ linearly independent eigenvectors for the eigenvalue -1. By transposing the argument, we get the converese.

21. Let A and B be two matrices of the same dimension over some commutative ring. Then $(A \circ B)_{ij} = A_{ij} B_{ij}$, i.e. componentwise multiplication.

22. Let $\mu : \Omega \times G \to \Omega$ be an action of G on Ω. The action is *generously transitive* if, for each pair of points α and β in Ω, there is an element $g \in G$ such that $\mu(\alpha, g) = \beta$ and $\mu(\beta, g) = \alpha$. The terminology is due to Neumann (1975).

23. The algebra $\hat{\mathfrak{U}}$ is in many senses the dual of the algebra $\mathfrak{U}$. This is explored in Bannai and Ito (1984), Bannai et al. (2021), and Delsarte (1973).

Part II

Results

4

Balancedly Splittable Orthogonal Designs

This is the first chapter constituting the novel results of this work. Here balancedly splittable orthogonal designs are defined and various constructions are presented. These most interesting objects are connected to several objects such as frames and pairs of unbiased orthogonal designs.

§8. Balancedly Splittable Hadamard Matrices

Most of the results of this section are due to Kharaghani and Suda (2019). We include this material here to evince the fact that the concept of a balancedly splittable orthogonal design is a generalization of previous work.

* * *

8.1. Definition. Recall that a Hadamard matrix is a weighing matrix $\mathrm{W}(n, n)$ (see §3). These elusive objects have vexed combinatorialists for over a century now. Ever more clever techniques from ever more branches of mathematics are needed in order to construct these objects.

We will consider one such construction in preparation for our study of orthogonal designs. The matrices we will study are the so-called balancedly splittable Hadamard matrices. First, an example.

8.1. Example. Consider a Hadamard matrix of order 4 shown below

$$\text{(8.1.a)} \quad \begin{pmatrix} +&+&+&+ \\ +&+&-&- \\ +&-&+&- \\ +&-&-&+ \end{pmatrix}.$$

Label the rows h_0, h_1, h_2, and h_3. We then form the block matrix with (i,j)-th entry given by $h_j^t h_i$.

$$\text{(8.1.b)} \quad \begin{pmatrix}
\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+} \\
\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{-}&\mathbf{-}&\mathbf{-}&\mathbf{-}&\mathbf{-}&\mathbf{-}&\mathbf{-}&\mathbf{-} \\
\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{-}&\mathbf{-}&\mathbf{-}&\mathbf{-}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{-}&\mathbf{-}&\mathbf{-}&\mathbf{-} \\
\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{-}&\mathbf{-}&\mathbf{-}&\mathbf{-}&\mathbf{-}&\mathbf{-}&\mathbf{-}&\mathbf{-}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+} \\
+&+&-&-&+&+&-&-&+&+&-&-&+&+&-&- \\
+&+&-&-&+&+&-&-&-&-&+&+&-&-&+&+ \\
+&+&-&-&-&-&+&+&+&+&-&-&-&-&+&+ \\
+&+&-&-&-&-&+&+&-&-&+&+&+&+&-&- \\
+&-&+&-&+&-&+&-&+&-&+&-&+&-&+&- \\
+&-&+&-&+&-&+&-&-&+&-&+&-&+&-&+ \\
+&-&+&-&-&+&-&+&+&-&+&-&-&+&-&+ \\
+&-&+&-&-&+&-&+&-&+&-&+&+&-&+&- \\
+&-&-&+&+&-&-&+&+&-&-&+&+&-&-&+ \\
+&-&-&+&+&-&-&+&-&+&+&-&-&+&+&- \\
+&-&-&+&-&+&+&-&+&-&-&+&-&+&+&- \\
+&-&-&+&-&+&+&-&-&+&+&-&+&-&-&+
\end{pmatrix}.$$

The matrix (8.1.b) has the submatrix H_1 which we have shown in bold above. This submatrix has the property that $H_1^t H_1 = 4I + 4A$, for some symmetric $(0,1)$-matrix A with zero diagonal. In particular, there are only two angles that exist between the columns of H_1.

The above example motivates the following definition.

8.2. Definition. A Hadamard Matrix H of order n is *balancedly splittable* with parameters (n, ℓ, a, b) if H has an $\ell \times n$ submatrix H_1 such that

(8.2.a) $H_1^t H_1 = \ell I + aA + b(J - I - A)$,

for some binary $(0,1)$-matrix A with zero diagonal.

This definition and the previous example are suggestive. Notably, a connection to sets of biangular lines is inherent in the definition. These connections will be taken up in the following subsections.

* * *

8.2. Equiangular Lines. In the previous subsection, it was intimated that balancedly splittable Hadamard matrices were related to collections of biangular lines. By a set of *lines*, we mean a collection of vectors in $\mathbf{R}^\ell$, for some ℓ. Given a collection $\mathscr{L}$ of lines in $\mathbf{R}^\ell$, define $\Xi = \{|\langle u, v\rangle| : u, v \in \mathscr{L} \text{ and } u \neq v\}$. If $|\Xi| = 2$, then we say that $\mathscr{L}$ is a set of *biangular lines*; while if $|\Xi| = 1$, then we say that $\mathscr{L}$ is a set of *equiangular lines*[24]).

Clearly, if H is balancedly splittable with respect to the $\ell \times n$ submatrix H_1, then Definition 8.2 implies that the columns of H_1 are at most biangular. They are equiangular precisely in the case that $b = -a$.

We will require the following proposition due to Delsarte et al. (1977).

8.3. Proposition. Let $\mathscr{L} \subset \mathbf{R}^\ell$ be a set of lines (vectors) such that $|\langle u, v\rangle| = a$, for every pair of distinct lines u and v in $\mathscr{L}$. If $\ell < a^{-2}$, then

(8.3.a) $|\mathscr{L}| \leq \ell(1 - a^2)/(1 - \ell a^2)$.

Using balancedly splittable Hadamard matrices, we can construct optimal sets of equiangular lines.

8.4. Theorem. If there exists a balancedly splittable Hadamard matrix with parameters $(n, \ell, a, -a)$, then there is an optimal set of equiangular lines in $\mathbf{R}^\ell$.

Proof. Suppose that H is a balancedly splittable Hadamard matrix with respect to the $\ell \times n$ submatrix H_1 with parameters $(n, \ell, a, -a)$. Take $\mathscr{L}$ to be the collection of normalized columns of H_1. Note that $a^2\ell^2 = \ell(n-\ell)/(n-1)$; then the absolute value of the inner product between distinct lines in $\mathscr{L}$ is given by $a = \sqrt{n-\ell}/\sqrt{\ell(n-1)}$; moreover, $\ell \le a$. The right-hand side of (8.3.a) reduces to n. We have, therefore, exhibited an optimal set of equiangular lines. ∎

In §10, we will pursue this topic again in the more restricted setting of frames.

* * *

8.3. Constructions. For the sake of completeness, we make Example 8.1 general.

8.5. Proposition. If there exists a Hadamard matrix of order n, then there exists a balancedly splittable Hadamard matrix with parameters $(n^2, n, n, 0)$.

Proof. Let H be a normalized Hadamard matrix of order n, and label the rows $h_0 = \mathbf{1}, \dots, h_{n-1}$. Take M to be the block matrix defined by $M_{ij} = h_j^t h_i$. Then $M_{ij}M_{kj}^t = (h_j^t h_i)(h_j^t h_k)^t = h_j^t(h_i h_k^t)h_j = O$ whenever $i \ne k$, hence M is a Hadamard matrix of order n^2 (cf Kharaghani, 1986). Take M_1 to be the first block row of M. Then

$$M_1^t M_1 = \begin{pmatrix} J \\ \mathbf{1}^t h_1 \\ \vdots \\ \mathbf{1}^t h_{n-1} \end{pmatrix} \begin{pmatrix} J & h_2^t \mathbf{1} & \dots & h_{n-1}^t \mathbf{1} \end{pmatrix} = mI \otimes J,$$

and the proof is complete. ∎

There are many more constructions presented in Kharaghani and Suda (2019) that the interested reader may consult. For our purposes, however, we present a novel construction. Consider the following example.

8.6. Example. Consider the Hadamard matrix of order 2

(8.6.a) $\begin{pmatrix} + & + \\ + & - \end{pmatrix}$,

and label the rows h_0 and h_1. Form the matrices $c_i = h_i^t h_i$, the so-called *auxiliary matrices*, shown in order below.

(8.6.b) $c_0 = \begin{pmatrix} + & + \\ + & + \end{pmatrix}, c_1 = \begin{pmatrix} + & - \\ - & + \end{pmatrix}$.

Take $K = H \otimes H$, labelling the rows as k_0, k_1, k_2, and k_3. Form the block circulant matrices A and B with first rows (c_0, c_1, c_1) and $(c_0, c_1, -c_1)$, shown below.

(8.6.c) $A = \begin{pmatrix} + & + & + & - & + & - \\ + & + & - & + & - & + \\ + & - & + & + & + & - \\ - & + & + & + & - & + \\ + & - & + & - & + & + \\ - & + & - & + & + & + \end{pmatrix}, B = \begin{pmatrix} + & + & + & - & - & + \\ + & + & - & + & + & - \\ - & + & + & + & + & - \\ + & - & + & + & - & + \\ + & - & - & + & + & + \\ - & + & + & - & + & + \end{pmatrix}$.

Now, form the block matrix $F = \left(\begin{smallmatrix} F_1 & \cdots & F_7 \end{smallmatrix} \right)$ by defining $F_i = k_i^t h_0$

(8.6.d) $F = \begin{pmatrix} + & + & + & + & + & + \\ - & - & + & + & - & - \\ + & + & - & - & - & - \\ - & - & - & - & + & + \end{pmatrix}$.

Finally, take $E = F^t$. We then form the block matrix $X = \left(\begin{smallmatrix} J & F & -F \\ E & A & B \\ -E & B & A \end{smallmatrix} \right)$

$$(8.6.e)\quad X = \begin{pmatrix}
+&+&+&+&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&-&-&-&-&-&-\\
+&+&+&+&\mathbf{-}&\mathbf{-}&\mathbf{+}&\mathbf{+}&\mathbf{-}&\mathbf{-}&+&+&-&-&+&+\\
+&+&+&+&\mathbf{+}&\mathbf{+}&\mathbf{-}&\mathbf{-}&\mathbf{-}&\mathbf{-}&-&-&+&+&+&+\\
+&+&+&+&\mathbf{-}&\mathbf{-}&\mathbf{-}&\mathbf{-}&\mathbf{+}&\mathbf{+}&+&+&+&+&-&-\\
+&-&+&-&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{-}&\mathbf{+}&\mathbf{-}&+&+&+&-&-&+\\
+&-&+&-&\mathbf{+}&\mathbf{+}&\mathbf{-}&\mathbf{+}&\mathbf{-}&\mathbf{+}&+&+&-&+&+&-\\
+&+&-&-&\mathbf{+}&\mathbf{-}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{-}&-&+&+&+&+&-\\
+&+&-&-&\mathbf{-}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{-}&\mathbf{+}&+&-&+&+&-&+\\
+&-&-&+&\mathbf{+}&\mathbf{-}&\mathbf{+}&\mathbf{-}&\mathbf{+}&\mathbf{+}&+&-&-&+&+&+\\
+&-&-&+&\mathbf{-}&\mathbf{+}&\mathbf{-}&\mathbf{+}&\mathbf{+}&\mathbf{+}&-&+&+&-&+&+\\
-&+&-&+&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{-}&\mathbf{-}&\mathbf{+}&+&+&+&-&+&-\\
-&+&-&+&\mathbf{+}&\mathbf{+}&\mathbf{-}&\mathbf{+}&\mathbf{+}&\mathbf{-}&+&+&-&+&-&+\\
-&-&+&+&\mathbf{-}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{+}&\mathbf{-}&+&-&+&+&+&-\\
-&-&+&+&\mathbf{+}&\mathbf{-}&\mathbf{+}&\mathbf{+}&\mathbf{-}&\mathbf{+}&-&+&+&+&-&+\\
-&+&+&-&\mathbf{+}&\mathbf{-}&\mathbf{-}&\mathbf{+}&\mathbf{+}&\mathbf{+}&+&-&+&-&+&+\\
-&+&+&-&\mathbf{-}&\mathbf{+}&\mathbf{+}&\mathbf{-}&\mathbf{+}&\mathbf{+}&-&+&-&+&+&+
\end{pmatrix}.$$

The matrix X is a Hadamard matrix of order 16, and evidently, it is balancedly splittable. Indeed, the submatrix shown in bold above can be used to form a balanced split. Due to the form of X, however, any one of the following can be used to form a balanced split

$$(8.6.f)\quad \begin{pmatrix} F \\ A \\ B \end{pmatrix}, \begin{pmatrix} -F \\ B \\ A \end{pmatrix}, \begin{pmatrix} E & A & B \end{pmatrix}, \begin{pmatrix} -E & B & A \end{pmatrix}.$$

In any event, the parameters of the splits are $(16, 6, 2, -2)$. Therefore, we have optimal sets of equiangular lines.

This construction can be made perfectly general. Since this result is ultimately a special case of Theorem 9.13, we will not show it explicitly.

8.7. Theorem. There is a balancedly splittable Hadamard matrix of order $4n^2$ with parameters $(4n^2, 2n^2 - n, n, -n)$ whenever there is a Hadamard matrix of order n.

8.8. Corollary. If there is a Hadamard matrix of order n, then there is an optimal set of equiangular lines in $\mathbf{R}^{2n^2-n}$.

We mention in passing that Kharaghani and Suda (2019) showed that balancedly splittable Hadamard matrices can be used to construct various association schemes. As nothing essentially new about association schemes has been added in our study of orthogonal designs, we will not pursue this topic here and simply refer the reader to the aforementioned article.

§9. Balancedly Splittable Orthogonal Designs

In this and the following section, the new results of Kharaghani et al. (2021) are presented. Here we define balanced splittability of orthogonal designs and give several constructions. To avoid obfuscation, we given the constructions in terms of real and complex ODs; however, the results are perfectly valid for the more general QODs.

* * *

9.1. Definition. Generalizing balanced splittability to orthogonal designs presents several difficulties. The various cases are encapsulated in the next definition.

9.1. Definition. Let X be a full QOD$(n; s_1, \ldots, s_u)$. X is *balancedly splittable* if there is an $\ell \times n$ submatrix X_1 where one of the following conditions holds. In what follows $\alpha, \beta \in \{a + ib + jc + kd : a, b, c, d \in \mathbf{R}\}$.

(9.1.a) The off-diagonal entries of $X_1^* X_1$ are in the set

$$\{\pm \varepsilon c x_1^{m_1} \cdots x_u^{m_u} x_1^{*m_1'} \cdots x_u^{*m_u'} : m_i, m_i' \in \mathbf{N}, \varepsilon \in \{1, i, j, k\}, c \in \{\alpha, \alpha^*, \beta, \beta^*\}\}.$$

(9.1.b) The off-diagonal entries of $X_1^* X_1$ are in the set

$$\left\{\sum_{i=1}^{u} t_i |x_i|^2 : t_i \in \mathbf{N}, \sum_{i=0}^{u} t_i = m\right\}$$

or in the set

$$\{\pm\varepsilon c x_1^{m_1}\cdots x_u^{m_u} x_1^{*m_1'}\cdots x_u^{*m_u'} : m_i, m_i' \in \mathbf{N}, \varepsilon \in \{1,i,j,k\}, c \in \{\alpha,\alpha^*,\beta,\beta^*\}\}.$$

(9.1.c) The off-diagonal entries of $X_1^* X_1$ are in the set

$$\{\pm\varepsilon c\sigma : \varepsilon \in \{1,i,j,k\}, c \in \{\alpha,\alpha^*,\beta,\beta^*\}\},$$

where $\sigma = \sum_i s_i |x_i|^2$ (cf. (5.3.a)).

In the first case, the split is *unstable*; in the second, the split is *unfaithfully unstable*; and in the third, the split is *stable*. The term *faithful* is used to describe the first and third cases.

From the definition, we see that if α and β are the same in absolute value, the split corresponds to a set of equiangular lines. Interestingly, we will see that both conditions in (9.1.b) can hold simultaneously.

The next two subsections will present constructions for both the unfaithful, and the faithful case.

* * *

9.2. Unfaithful Constructions. The constructions of this section are similar to those presented in Fender et al. (2018) and Pender (2020), and are applicable to real and complex orthogonal designs.

To begin, if W is a skew-symmetric $\mathrm{W}(q+1,q)$, then we take Q to be its core, i.e. the submatrix obtaind by deleting the first row and column. Further, we can assume that $W = \left(\begin{smallmatrix} 0 & \mathbf{1}^t \\ -\mathbf{1} & Q \end{smallmatrix}\right)$, hence $JQ = QJ = O$ and $Q^2 = J - qI$. We recursively define the following family of matrices.

$$\mathcal{J}_m = \begin{cases} aJ_1 & \text{if } m = 0, \text{ and} \\ J_q \otimes \mathcal{A}_{m-1} & \text{if } m > 0; \end{cases}$$

$$\mathcal{A}_m = \begin{cases} bJ_1 & \text{if } m = 0, \text{ and} \\ I_q \otimes \mathcal{J}_{m-1} + Q \otimes \mathcal{A}_{m-1} & \text{if } m > 0; \end{cases}$$

where a and b are commuting indeterminants.

We require the following lemma.

9.2. Lemma.

(9.2.a) $\mathcal{J}_m \mathcal{A}_m^t = \mathcal{A}_m \mathcal{J}_m^t$;

(9.2.b) $\mathcal{J}_m \mathcal{J}_m^t + q\mathcal{A}_m \mathcal{A}_m^t = (q^m a^2 + q^{m+1} b^2)I$; and

(9.2.c) $\mathcal{J}_1^t \mathcal{J}_1 = qa^2 J, \mathcal{A}_1^t \mathcal{A}_1 = a^2 I + b^2(qI - J)$, and $\mathcal{A}_1^t \mathcal{J}_1 = \mathcal{J}_1^t \mathcal{A}_1 = abJ$.

Proof. We have $\mathcal{J}_0 \mathcal{A}_0^t = ab = ba = \mathcal{A}_0 \mathcal{J}_0^t$. Assume $\mathcal{J}_{m-1} \mathcal{A}_{m-1}^t = \mathcal{A}_{m-1} \mathcal{J}_{m-1}^t$. Then

$$\begin{aligned} \mathcal{J}_m \mathcal{A}_m^t &= (J \otimes \mathcal{A}_{m-1})(I \otimes \mathcal{J}_{m-1} + Q \otimes \mathcal{A}_{m-1})^t \\ &= J \otimes \mathcal{A}_{m-1} \mathcal{J}_{m-1}^t + JQ^t \otimes \mathcal{A}_{m-1} \mathcal{A}_{m-1}^t \\ &= J \otimes \mathcal{J}_{m-1} \mathcal{A}_{m-1}^t + QJ \otimes \mathcal{A}_{m-1} \mathcal{A}_{m-1}^t \\ &= (I \otimes \mathcal{J}_{m-1} + Q \otimes \mathcal{A}_{m-1})(J \otimes \mathcal{A}_{m-1})^t, \end{aligned}$$

and (9.2.a) has been shown.

Clearly, $\mathcal{J}_0 \mathcal{J}_0^t + q\mathcal{A}_0 \mathcal{A}_0^t = a^2 + qb^2$; so, assume $\mathcal{J}_{m-1} \mathcal{J}_{m-1}^t + q\mathcal{A}_{m-1} \mathcal{A}_{m-1}^t = (a^2 + qb^2)I$. Then

$$\mathcal{J}_m \mathcal{J}_m^t + q\mathcal{A}_m \mathcal{A}_m^t = qJ \otimes \mathcal{A}_{m-1} \mathcal{A}_{m-1}^t + q(I \otimes \mathcal{J}_{m-1} \mathcal{J}_{m-1}^t - Q^2 \otimes \mathcal{A}_{m-1} \mathcal{A}_{m-1}^t)$$

$$\begin{aligned} &= qI \otimes (\mathcal{J}_{m-1}\mathcal{J}_{m-1}^t + q\mathcal{A}_{m-1}\mathcal{A}_{m-1}^t) \\ &= qI \otimes (q^{m-1}q^2 + q^m b^2)I \\ &= (q^m a^2 + q^{m+1}b^2)I, \end{aligned}$$

and (9.2.b) is proven.

Finally, (9.2.c) is simply a restatement of the definitions of $\mathcal{J}_m$ and $\mathcal{A}_m$. ∎

We can now present the first construction of the novel balancedly splittable ODs.

9.3. Theorem. Let W, $\mathcal{A}_m$, and $\mathcal{J}_m$ be as above. Define $X_m = I \otimes \mathcal{J}_m + W \otimes \mathcal{A}_m$. Then:

(9.3.a) X_m is an OD$(q^m(q+1); q^m, q^{m+1})$, and

(9.3.b) The matrix X_1 is an unfaithful balancedly splittable OD$(q(q+1); q, q^2)$.

Proof. X_m has entries from $\{\pm a, \pm b\}$. Observe:

$$\begin{aligned} X_m X_m^t &= (I \otimes \mathcal{J}_m + W \otimes \mathcal{A}_m)(I \otimes \mathcal{J}_m + W \otimes \mathcal{A}_m)^t \\ &= I \otimes \mathcal{J}_m\mathcal{J}_m^t + WW^t \otimes \mathcal{A}_m\mathcal{A}_m^t \\ &= I \otimes \mathcal{J}_m\mathcal{J}_m^t + qI \otimes \mathcal{A}_m\mathcal{A}_m^t \\ &= I \otimes (\mathcal{J}_m\mathcal{J}_m^t + q\mathcal{A}_m\mathcal{A}_m^t) \\ &= I \otimes (q^m a^2 + q^{m+1}b^2)I \\ &= (q^m a^2 + q^{m+1}b^2)I, \end{aligned}$$

which shows that X_m is an OD$(q^m(q+1); q^m; q^{m+1})$. It remains to prove the balanced splittability of the base case.

Take $Y = (\,\mathcal{J}_1\ \mathcal{A}_1\ \dots\ \mathcal{A}_1\,)$, the first block row of X_1. Then

$$Y^tY = \begin{pmatrix} \mathcal{J}_1^t\mathcal{J}_1 & \mathbf{1}^t \otimes \mathcal{J}_1^t\mathcal{A}_1 \\ \mathbf{1} \otimes \mathcal{A}_1^t\mathcal{J}_1 & J \otimes \mathcal{A}_1^t\mathcal{A}_1 \end{pmatrix}$$
$$= \begin{pmatrix} qa^2J & ab\mathbf{1}^t \otimes J \\ ab\mathbf{1} \otimes J & J \otimes [(a^2-b^2)J + qb^2I] \end{pmatrix}.$$

Hence, X_1 admits an unfaithfully balanced split. ∎

9.4. Corollary. For every prime power $q \equiv -1 \pmod 4$, and for every integer $m > 0$, there is an OD$(q^m(q+1); q^m, q^{m+1})$

Proof. By Propositions 4.14 and 4.10, there is a skew-symmetric W$(q+1, q)$. Apply the theorem to this matrix. ∎

9.5. Corollary. For every prime power $q \equiv -1 \pmod 4$, there is an unfaithful balancedly splittable OD$(q(q+1); q, q^2)$.

9.6. Example. Using the skew-symmetric Paley weighing matrix[25]) $W(4,3)$ given by

$$\text{(9.6.a)}\quad \begin{pmatrix} 0 & + & + & + \\ - & 0 & + & - \\ - & - & 0 & + \\ - & + & - & 0 \end{pmatrix},$$

we construct the smallest case of an OD$(12; 3, 9)$ given by the theorem

$$
(9.6.b)\qquad
\begin{pmatrix}
\mathbf{b} & \mathbf{b} & \mathbf{b} & \mathbf{a} & \mathbf{b} & \overline{\mathbf{b}} & \mathbf{a} & \mathbf{b} & \overline{\mathbf{b}} & \mathbf{a} & \mathbf{b} & \overline{\mathbf{b}} \\
\mathbf{b} & \mathbf{b} & \mathbf{b} & \overline{\mathbf{b}} & \mathbf{a} & \mathbf{b} & \overline{\mathbf{b}} & \mathbf{a} & \mathbf{b} & \overline{\mathbf{b}} & \mathbf{a} & \mathbf{b} \\
\mathbf{b} & \mathbf{b} & \mathbf{b} & \mathbf{b} & \overline{\mathbf{b}} & \mathbf{a} & \mathbf{b} & \overline{\mathbf{b}} & \mathbf{a} & \mathbf{b} & \overline{\mathbf{b}} & \mathbf{a} \\
\overline{\mathbf{a}} & \overline{\mathbf{b}} & \mathbf{b} & \mathbf{b} & \mathbf{b} & \mathbf{b} & \mathbf{a} & \mathbf{b} & \overline{\mathbf{b}} & \overline{\mathbf{a}} & \overline{\mathbf{b}} & \mathbf{b} \\
b & \overline{a} & \overline{b} & b & b & b & \overline{b} & a & b & b & \overline{a} & \overline{b} \\
\overline{b} & b & \overline{a} & b & b & b & b & \overline{b} & a & \overline{b} & b & \overline{a} \\
\overline{a} & \overline{b} & b & \overline{a} & \overline{b} & b & b & b & b & a & b & \overline{b} \\
b & \overline{a} & \overline{b} & b & \overline{a} & \overline{b} & b & b & b & \overline{b} & a & b \\
\overline{b} & b & \overline{a} & \overline{b} & b & \overline{a} & b & b & b & b & \overline{b} & a \\
\overline{a} & \overline{b} & b & a & b & \overline{b} & \overline{a} & \overline{b} & b & b & b & b \\
b & \overline{a} & \overline{b} & \overline{b} & a & b & b & \overline{a} & \overline{b} & b & b & b \\
\overline{b} & b & \overline{a} & b & \overline{b} & a & \overline{b} & b & \overline{a} & b & b & b
\end{pmatrix},
$$

where the unfaithful split is shown in bold.

Our first construction yields real ODs and is applicable in the case that we have a prime power $q \equiv -1 \pmod 4$. Of course, since $(q-1)/2$ is odd, we can apply the results of §4 to construct a weighing matrix that is skew-symmetric, a property essential to the construction. If $q \equiv 1 \pmod 4$, then $(q-1)/2$ is even and the ensuing weighing matrix is symmetric. In this event, we need to appeal to complex ODs in order apply the construction.

To apply the complex units, we make the following recursive definitions where $W = \left(\begin{smallmatrix} 0 & \mathbf{1}^t \\ \mathbf{1} & Q \end{smallmatrix}\right)$ is a $\mathrm{W}(q+1, q)$ with $Q^t = Q$.

$$
\mathcal{C}_m = \begin{cases} aJ_1 & \text{if } m = 0, \text{ and} \\ J_q \otimes \mathcal{D}_{m-1} & \text{if } m > 0; \end{cases}
$$

$$
\mathcal{D}_m = \begin{cases} bJ_1 & \text{if } m = 0, \text{ and} \\ I_q \otimes \mathcal{C}_{m-1} + iQ \otimes \mathcal{D}_{m-1} & \text{if } m > 0; \end{cases}
$$

where again a and b are real commuting indeterminants. As above, we have the following lemma that is shown in precisely the same way as before, save one replaces transposition with conjugate transposition.

9.7. Lemma.

(9.7.a) $\mathcal{C}_m\mathcal{D}_m^* = \mathcal{D}_m\mathcal{C}_m^*$;

(9.7.b) $\mathcal{C}_m\mathcal{C}_m^* + q\mathcal{D}_m\mathcal{D}_m^* = (q^m a^2 + q^{m+1}b^2)I$; and

(9.7.c) $\mathcal{C}_1^*\mathcal{C}_1 = qa^2J, \mathcal{D}_1^*\mathcal{D}_1 = a^2I + b^2(qI - J)$, and $\mathcal{D}_1^*\mathcal{C}_1 = \mathcal{C}_1^*\mathcal{D}_1 = abJ.$

9.8. Theorem. Let W, $\mathcal{C}_m$, and $\mathcal{D}_m$ be as above, and define $Y_m = iI \otimes \mathcal{C}_m + W \otimes \mathcal{D}_m$. Then:

(9.8.a) The matrix Y_m is a COD$(q^m(q+1); q^m, q^{m+1})$, and

(9.8.b) Y_1 admits an unfaithfully balanced split.

9.9. Corollary. For every prime power $q \equiv 1 \pmod 4$, and for every integer $m > 0$, there is a COD$(q^m(q+1); q^m, q^{m+1})$.

9.10. Corollary. For every prime power $q \equiv 1 \pmod 4$, there is an unfaithful balancedly splittable COD$(q(q+1); q, q^2)$.

We again explore the smallest case.

9.11. Example. Take $q = 5$ and consider the symmetric Paley weighing matrix W$(6,5)$ given by

$$\text{(9.11.a)} \quad \begin{pmatrix} 0 & + & + & + & + & + \\ + & 0 & + & - & - & + \\ + & + & 0 & + & - & - \\ + & - & + & 0 & + & - \\ + & - & - & + & 0 & + \\ + & + & - & - & + & 0 \end{pmatrix}.$$

Applying the construction, we obtain

$$
\begin{pmatrix}
\mathbf{ib} & \mathbf{ib} & \mathbf{ib} & \mathbf{ib} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} \\
\mathbf{ib} & \mathbf{ib} & \mathbf{ib} & \mathbf{ib} & \mathbf{ib} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} \\
\mathbf{ib} & \mathbf{ib} & \mathbf{ib} & \mathbf{ib} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} \\
\mathbf{ib} & \mathbf{ib} & \mathbf{ib} & \mathbf{ib} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} \\
\mathbf{ib} & \mathbf{ib} & \mathbf{ib} & \mathbf{ib} & \mathbf{ib} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} & \mathbf{ib} & \mathbf{i\overline{b}} & \mathbf{i\overline{b}} & \mathbf{ib} & \mathbf{a} \\
a & ib & i\overline{b} & i\overline{b} & ib & ib & ib & ib & ib & ib & a & ib & i\overline{b} & i\overline{b} & ib & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & a & ib & i\overline{b} & i\overline{b} & ib \\
ib & a & ib & i\overline{b} & i\overline{b} & ib & ib & ib & ib & ib & ib & a & ib & i\overline{b} & i\overline{b} & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & ib & a & ib & i\overline{b} & i\overline{b} \\
i\overline{b} & ib & a & ib & i\overline{b} & ib & ib & ib & ib & ib & i\overline{b} & ib & a & ib & i\overline{b} & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & i\overline{b} & ib & a & ib & i\overline{b} \\
i\overline{b} & i\overline{b} & ib & a & ib & ib & ib & ib & ib & ib & i\overline{b} & i\overline{b} & ib & a & ib & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & i\overline{b} & i\overline{b} & ib & a & ib \\
ib & i\overline{b} & i\overline{b} & ib & a & ib & ib & ib & ib & ib & ib & i\overline{b} & i\overline{b} & ib & a & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & ib & i\overline{b} & i\overline{b} & ib & a \\
a & ib & i\overline{b} & i\overline{b} & ib & a & ib & i\overline{b} & i\overline{b} & ib & ib & ib & ib & ib & ib & a & ib & i\overline{b} & i\overline{b} & ib & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} \\
ib & a & ib & i\overline{b} & i\overline{b} & ib & a & ib & i\overline{b} & i\overline{b} & ib & ib & ib & ib & ib & ib & a & ib & i\overline{b} & i\overline{b} & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib \\
i\overline{b} & ib & a & ib & i\overline{b} & i\overline{b} & ib & a & ib & i\overline{b} & ib & ib & ib & ib & ib & i\overline{b} & ib & a & ib & i\overline{b} & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib \\
i\overline{b} & i\overline{b} & ib & a & ib & i\overline{b} & i\overline{b} & ib & a & ib & ib & ib & ib & ib & ib & i\overline{b} & i\overline{b} & ib & a & ib & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} \\
ib & i\overline{b} & i\overline{b} & ib & a & ib & i\overline{b} & i\overline{b} & ib & a & ib & ib & ib & ib & ib & ib & i\overline{b} & i\overline{b} & ib & a & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} \\
a & ib & i\overline{b} & i\overline{b} & ib & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & a & ib & i\overline{b} & i\overline{b} & ib & ib & ib & ib & ib & ib & a & ib & i\overline{b} & i\overline{b} & ib & \overline{a} & i\overline{b} & ib & ib & i\overline{b} \\
ib & a & ib & i\overline{b} & i\overline{b} & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & ib & a & ib & i\overline{b} & i\overline{b} & ib & ib & ib & ib & ib & ib & a & ib & i\overline{b} & i\overline{b} & i\overline{b} & \overline{a} & i\overline{b} & ib & ib \\
i\overline{b} & ib & a & ib & i\overline{b} & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & i\overline{b} & ib & a & ib & i\overline{b} & ib & ib & ib & ib & ib & i\overline{b} & ib & a & ib & i\overline{b} & ib & i\overline{b} & \overline{a} & i\overline{b} & ib \\
i\overline{b} & i\overline{b} & ib & a & ib & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & i\overline{b} & i\overline{b} & ib & a & ib & ib & ib & ib & ib & ib & i\overline{b} & i\overline{b} & ib & a & ib & ib & ib & i\overline{b} & \overline{a} & i\overline{b} \\
ib & i\overline{b} & i\overline{b} & ib & a & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & ib & i\overline{b} & i\overline{b} & ib & a & ib & ib & ib & ib & ib & ib & i\overline{b} & i\overline{b} & ib & a & i\overline{b} & ib & ib & i\overline{b} & \overline{a} \\
a & ib & i\overline{b} & i\overline{b} & ib & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & a & ib & i\overline{b} & i\overline{b} & ib & ib & ib & ib & ib & ib & a & ib & i\overline{b} & i\overline{b} & ib \\
ib & a & ib & i\overline{b} & i\overline{b} & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & ib & a & ib & i\overline{b} & i\overline{b} & ib & ib & ib & ib & ib & ib & a & ib & i\overline{b} & i\overline{b} \\
i\overline{b} & ib & a & ib & i\overline{b} & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & i\overline{b} & ib & a & ib & i\overline{b} & ib & ib & ib & ib & ib & i\overline{b} & ib & a & ib & i\overline{b} \\
i\overline{b} & i\overline{b} & ib & a & ib & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & i\overline{b} & i\overline{b} & ib & a & ib & ib & ib & ib & ib & ib & i\overline{b} & i\overline{b} & ib & a & ib \\
ib & i\overline{b} & i\overline{b} & ib & a & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & ib & i\overline{b} & i\overline{b} & ib & a & ib & ib & ib & ib & ib & ib & i\overline{b} & i\overline{b} & ib & a \\
a & ib & i\overline{b} & i\overline{b} & ib & a & ib & i\overline{b} & i\overline{b} & ib & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & a & ib & i\overline{b} & i\overline{b} & ib & ib & ib & ib & ib & ib \\
ib & a & ib & i\overline{b} & i\overline{b} & ib & a & ib & i\overline{b} & i\overline{b} & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & ib & a & ib & i\overline{b} & i\overline{b} & ib & ib & ib & ib & ib \\
i\overline{b} & ib & a & ib & i\overline{b} & i\overline{b} & ib & a & ib & i\overline{b} & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & i\overline{b} & ib & a & ib & i\overline{b} & ib & ib & ib & ib & ib \\
i\overline{b} & i\overline{b} & ib & a & ib & i\overline{b} & i\overline{b} & ib & a & ib & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & i\overline{b} & i\overline{b} & ib & a & ib & ib & ib & ib & ib & ib \\
ib & i\overline{b} & i\overline{b} & ib & a & ib & i\overline{b} & i\overline{b} & ib & a & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & i\overline{b} & ib & ib & i\overline{b} & \overline{a} & ib & i\overline{b} & i\overline{b} & ib & a & ib & ib & ib & ib & ib
\end{pmatrix}, \tag{9.11.b}
$$

a $\mathrm{COD}(30; 5, 25)$, where the unfaithful split is shown in bold.

* * *

9.3. Faithful Construction. Here we will introduce a most useful construction of orthogonal designs admitting a faithful split. We will see later how we can use these constructed matrices in constructing other objects.

To begin, we assume the existence of a full $\mathrm{OD}(n; s_1, \ldots, s_u)$, say X, and label the rows of X as $x_0, \ldots, x_{n-1}$. Further, assume that the coefficients of the indeterminants of the first row and column are $+1$. We need to extend the idea of an auxiliary matrix given in Example 8.6. To do this, we will follow Kharaghani and Suda (2018) in defining the auxiliary matrix of an OD thus: Let H be the Hadamard matrix obtained by setting each indeterminant of X to $+1$, and label the rows of H as $h_0, \ldots, h_{n-1}$. Then the auxiliary matrices[26]) of X are given by $c_i = h_i^t x_i$. We have the following result.

9.12. Lemma. Let $c_i = h_i^t x_i$, for $i \in \{0, \ldots, n-1\}$, be the auxiliary matrices of an $\mathrm{OD}(n; s_1, \ldots, s_u)$ X where $XX^t = \sigma I$. Then:

(9.12.a) $\sum_i c_i c_i^t = n\sigma I_n$, and

(9.12.b) $c_i c_j^t = \delta_{ij}\sigma h_i^t h_i$.

We need the simple fact that if (a,b) denotes the concatination of sequences a and b, then (a,b) and $(a,-b)$ is a Golay pair (see §5). Continuing to let $c_0,\ldots,c_{n-1}$ be the auxiliary matrices of the OD$(n;s_1,\ldots,s_u)$ X, then $a=(c_0,c_1,\ldots,c_{n-1},c_{n-1},\ldots,c_1)$ and $b=(c_0,c_1,\ldots,c_{n-1},-c_{n-1},\ldots,-c_1)$ form a complementary pair. Let A and B be the block-circulant matrices with first rows a and b, respectively.

Now, take $\tilde{X}=\left(\begin{smallmatrix}+&+\\+&-\end{smallmatrix}\right)\otimes X$ and $\tilde{H}=\left(\begin{smallmatrix}+&+\\+&-\end{smallmatrix}\right)\otimes H$, and label the block rows $\tilde{x}_0,\ldots,\tilde{x}_{2n-1}$ and $\tilde{h}_0,\ldots,\tilde{h}_{2n-1}$. Define $G=\tilde{h}_0^t\tilde{x}_0$, and define the block matrices $E^t=\left(\begin{smallmatrix}E_1^t & \cdots & E_{2n-1}^t\end{smallmatrix}\right)^t$ and $F=\left(\begin{smallmatrix}F_1 & \cdots & F_{2n-1}\end{smallmatrix}\right)$ by $E_i=h_0^t\tilde{x}_i$ and $F_i=\tilde{h}_i^t x_0$.

As before, we then take $Z=\left(\begin{smallmatrix}G & F & -F\\ E & A & B\\ -E & B & A\end{smallmatrix}\right)$. The next result then follows.

9.13. Theorem. If there is an OD$(n;s_1,\ldots,s_u)$, then the block matrix Z is an OD$(4n^2;4ns_1,\ldots,4ns_u)$.

Proof. The proof amounts to checking the block entries of ZZ^t.

To begin, $GE_i^t=(\tilde{h}_0^t\tilde{x}_0)(h_0^t\tilde{x}_i)^t=\tilde{h}_0^t(\tilde{x}_0\tilde{x}_i^t)h_0=O$, hence $GE^t=EG^t=O$. Then $F_ic_j^t=(\tilde{h}_i^t x_0)(h_j^t x_j)^t=\tilde{h}_i^t(x_0x_j^t)h_j=\delta_{0j}\sigma\tilde{h}_i^t h_0$ so that

$$FA^t=FB^t=\sigma\begin{pmatrix}\tilde{h}_1\\ \vdots\\ \tilde{h}_{2n-1}\end{pmatrix}^t(\mathbf{1}_{2n-1}\otimes h_0).$$

We have, therefore, that $FA^t-FB^t=O$. Then the inner product between the first and second, and the first and third, block rows of Z vanish.

Next, $E_iE_j^t=(h_0^t\tilde{x}_i)(h_0^t\tilde{x}_j)^t=h_0^t(\tilde{x}_i\tilde{x}_j^t)h_0=\delta_{ij}2\sigma J_n$. It follows that $EE^t=(E_iE_j^t)=(\delta_{ij}2\sigma J_n)=2\sigma(I_{2n-1}\otimes J_n)$.

We need to examine the product AB^t and in order to do that, we need to examine the cross-product correlations (see §5). To begin, the product between the first block row and column of A and B^t is given by $c_0c_0^t + \sum_{i=1}^{n-1} c_ic_i^t - \sum_{i=1}^{n-1} c_ic_i^t = \sigma J_n$. Next, let a and b be two sequences of length $2n-1$ defined by

$$a_i = \begin{cases} c_i & \text{if } 0 \le i < n, \text{ and} \\ c_{2n-i-1} & \text{if } n \le i < 2n-1, \end{cases}$$

$$b_i = \begin{cases} c_0 & \text{if } i = 0, \\ -c_i & \text{if } 0 < i < n, \text{ and} \\ c_{2n-i-1} & \text{if } n \le i < 2n-1. \end{cases}$$

For $j \in \{1, \ldots 2n-2\}$, we have $C_j(a,b) = \sum_{i=0}^{2n-2} a_ib_{i+j}^t = \sum_{i=0}^{n-1} a_ib_{i+j}^t + \sum_{i=n}^{2n-2} a_ib_{i+j}^t$, where precisely one of the right-hand sums is nonzero by (9.12.b). For $j \in \{1, \ldots, n-1\}$, we have that

$$\begin{aligned} \sum_{i=0}^{n-1} a_ib_{i+j}^t &= a_0b_j^t + \sum_{i=1}^{n-j-1} a_ib_{i+j}^t + \sum_{i=n-j}^{n-1} a_ib_{i+j}^t \\ &= c_0c_j^t - \sum_{i=1}^{n-j-1} c_ic_{i+j}^t + \sum_{i=n-j}^{n-1} c_ic_{2n-j-i-1}^t \\ &= \sum_{i=0}^{j-1} c_{n-j+i}c_{n-i-1}^t, \end{aligned}$$

and

$$\begin{aligned} \sum_{i=n}^{2n-2} a_ib_{i+j}^t &= \sum_{i=n}^{2n-j-2} a_ib_{i+j}^t + \sum_{i=2n-j-1}^{2n-2} a_ib_{i+j}^t \\ &= \sum_{i=0}^{n-j-2} c_{n-i-1}c_{n-j-i-1}^t + c_jc_0^t - \sum_{i=1}^{j-1} c_{j-i}c_i^t \end{aligned}$$

$$= -\sum_{i=1}^{j-1} c_{j-i}c_i^t.$$

We have shown that, for $j \in \{1, \ldots, n-1\}$,

$$\begin{aligned} C_j(a,b) &= \sum_{i=0}^{j-1} c_{n-j+i}c_{n-i-1}^t - \sum_{i=1}^{j-1} c_{j-i}c_i^t \\ &= \begin{cases} \sigma h_{n-i-1}^t h_{n-i-1} & \text{if } j-1 = 2i, \text{ for some } i; \text{ and} \\ -\sigma h_i^t h_i & \text{if } j = 2i, \text{ for some } i \end{cases} \end{aligned}$$

Similarly, we find that $C_{2n-j-1}(a,b) = -C_j(a,b)$, for $j \in \{1, \ldots, n-1\}$, and $C_j(b,a) = -C_j(a,b)$, for all $j \in \{1, \ldots, 2n-2\}$.

Putting things together, we have shown that

$$\begin{aligned} AB^t &= \operatorname{circ}(\sigma J, C_{2n-2}(a,b), \ldots, C_1(a,b)) \\ &= \operatorname{circ}(\sigma J, -C_1(a,b), \ldots, -C_{n-1}(a,b), C_{n-1}(a,b), \ldots, C_1(a,b)) \\ &= \sigma\operatorname{circ}(J, -h_{n-1}^t h_{n-1}, \ldots, -h_{n/2}^t h_{n/2}, \\ &\qquad\qquad h_{n/2}^t h_{n/2}, \ldots, h_{n-1}^t h_{n-1}), \text{ and} \\ BA^t &= \sigma\operatorname{circ}(J, h_{n-1}^t h_{n-1}, \ldots, h_{n/2}^t h_{n/2}, \\ &\qquad\qquad - h_{n/2}^t h_{n/2}, \ldots, -h_{n-1}^t h_{n-1}). \end{aligned}$$

It follows that the product between the second and third block rows vanishes, i.e. $-EE^t + AB^t + BA^t = O$.

It remains to evaluate the block diagonal entries of ZZ^t. The first block row gives

$$GG^t + 2\sum_{i=1}^{2n-1} F_iF_i^t = 2\sigma J + 2\sigma \sum_{i=1}^{2n-1} \tilde{h}_i^t\tilde{h}_i$$

$$= 2\sigma J + 2\sigma \left(\sum_{i=0}^{2n-1} \tilde{h}_i^t \tilde{h}_i - \tilde{h}_0^t \tilde{h}_0 \right)$$

$$= 2\sigma J + 2\sigma (2nI - J)$$

$$= 4n\sigma I.$$

By a similar argument about the sequences a and b given above, we find that

$$\begin{aligned} AA^t &= \sigma\mathrm{circ}(2nI - J, h_{n-1}^t h_{n-1}, \dots, h_{n/2}^t h_{n/2}, \\ &\qquad\qquad h_{n/2}^t h_{n/2}, \dots, h_{n-1}^t h_{n-1}), \text{ and} \\ BB^t &= \sigma\mathrm{circ}(2nI - J, -h_{n-1}^t h_{n-1}, \dots, -h_{n/2}^t h_{n/2}, \\ &\qquad\qquad - h_{n/2}^t h_{n/2}, \dots, -h_{n-1}^t h_{n-1}). \end{aligned}$$

Thus, $EE^t + AA^t + BB^t = 4\sigma I$. The proof is complete. ∎

We have shown that Z is an OD. It remains to show that Z admits a faithful split. This is accomplished with the next result.

9.14. Theorem. Assume the OD Z of the previous theorem. Then:

(9.14.a) The submatrices $\begin{pmatrix} F \\ A \\ B \end{pmatrix}$ and $\begin{pmatrix} -F \\ B \\ A \end{pmatrix}$ yield stable splits, and

(9.14.b) The submatrices $\begin{pmatrix} E & A & B \end{pmatrix}$ and $\begin{pmatrix} -E & B & A \end{pmatrix}$ yield unstable splits.

Proof. It suffices to show the result for one matrix of each class. Note that

$$\begin{pmatrix} F \\ A \\ B \end{pmatrix} \begin{pmatrix} F^t & A^t & B^t \end{pmatrix} = \begin{pmatrix} FF^t & FA^t & FB^t \\ AF^t & AA^t & AB^t \\ BF^t & BA^t & BB^t \end{pmatrix}.$$

It follows by the proof of the previous theorem that

$$FF^t = 2n\sigma I - \sigma J,$$

$$
\begin{aligned}
FA^t &= FB^t = \sigma \sum_{i=1}^{2n-1} \tilde{h}_i^t h_0, \\
AA^t &= \sigma \mathrm{circ}(2nI - J, h_{n-1}^t h_{n-1}, \ldots, h_{n/2}^t h_{n/2}, \\
&\qquad\qquad\qquad h_{n/2}^t h_{n/2}, \ldots, h_{n-1}^t h_{n-1}), \text{ and} \\
BB^t &= \sigma \mathrm{circ}(2nI - J, -h_{n-1}^t h_{n-1}, \ldots, -h_{n/2}^t h_{n/2}, \\
&\qquad\qquad\qquad - h_{n/2}^t h_{n/2}, \ldots, -h_{n-1}^t h_{n-1}).
\end{aligned}
$$

Therefore, the product between distinct rows is $\pm\sigma$, which shows (9.14.a).

Next,

$$
\begin{pmatrix} E^t \\ A^t \\ B^t \end{pmatrix} \begin{pmatrix} E \; A \; B \end{pmatrix} = \begin{pmatrix} E^tE \; E^tA \; E^tB \\ A^tE \; A^tA \; A^tB \\ B^tE \; B^tA \; B^tB \end{pmatrix}.
$$

However, $E^tE = n\sum_{i=1}^{2n-1} \tilde{x}_i^t \tilde{x}_0$ has off-diagonal entries in the set

$$
\{\pm x_1^{m_1} \cdots x_u^{m_u} x_1^{*m'_1} \cdots x_u^{*m'_u} : m_i, m'_i \in \mathbf{N}\},
$$

which shows (9.14.b). ∎

9.15. Example. Applying the construction to the OD$(2;1,1)$

(9.15.a) $\begin{pmatrix} a \; b \\ b \; \overline{a} \end{pmatrix}$,

we obtain the balancedly splittble OD$(16;8,8)$

$$
(9.15.\text{b}) \quad
\begin{pmatrix}
a & b & a & b & \mathbf{a} & \mathbf{b} & \mathbf{a} & \mathbf{b} & \mathbf{a} & \mathbf{b} & \bar{a} & \bar{b} & \bar{a} & \bar{b} & \bar{a} & \bar{b} \\
a & b & a & b & \overline{\mathbf{a}} & \overline{\mathbf{b}} & \mathbf{a} & \mathbf{b} & \overline{\mathbf{a}} & \overline{\mathbf{b}} & a & b & \bar{a} & \bar{b} & a & b \\
a & b & a & b & \mathbf{a} & \mathbf{b} & \overline{\mathbf{a}} & \overline{\mathbf{b}} & \overline{\mathbf{a}} & \overline{\mathbf{b}} & \bar{a} & \bar{b} & a & b & a & b \\
a & b & a & b & \overline{\mathbf{a}} & \overline{\mathbf{b}} & \overline{\mathbf{a}} & \overline{\mathbf{b}} & \mathbf{a} & \mathbf{b} & a & b & a & b & \bar{a} & \bar{b} \\
b & \bar{a} & b & \bar{a} & \mathbf{a} & \mathbf{b} & \mathbf{b} & \overline{\mathbf{a}} & \mathbf{b} & \overline{\mathbf{a}} & a & b & b & \bar{a} & \bar{b} & a \\
b & \bar{a} & b & \bar{a} & \mathbf{a} & \mathbf{b} & \overline{\mathbf{b}} & \mathbf{a} & \overline{\mathbf{b}} & \mathbf{a} & a & b & \bar{b} & a & b & \bar{a} \\
a & b & \bar{a} & \bar{b} & \mathbf{b} & \overline{\mathbf{a}} & \mathbf{a} & \mathbf{b} & \mathbf{b} & \overline{\mathbf{a}} & \bar{b} & a & a & b & b & \bar{a} \\
a & b & \bar{a} & \bar{b} & \overline{\mathbf{b}} & \mathbf{a} & \mathbf{a} & \mathbf{b} & \overline{\mathbf{b}} & \mathbf{a} & b & \bar{a} & a & b & \bar{b} & a \\
b & \bar{a} & \bar{b} & a & \mathbf{b} & \overline{\mathbf{a}} & \mathbf{b} & \overline{\mathbf{a}} & \mathbf{a} & \mathbf{b} & b & \bar{a} & \bar{b} & a & a & b \\
b & \bar{a} & \bar{b} & a & \overline{\mathbf{b}} & \mathbf{a} & \overline{\mathbf{b}} & \mathbf{a} & \mathbf{a} & \mathbf{b} & \bar{b} & a & b & \bar{a} & a & b \\
\bar{b} & a & \bar{b} & a & \mathbf{a} & \mathbf{b} & \mathbf{b} & \overline{\mathbf{a}} & \overline{\mathbf{b}} & \mathbf{a} & a & b & b & \bar{a} & b & \bar{a} \\
\bar{b} & a & \bar{b} & a & \mathbf{a} & \mathbf{b} & \overline{\mathbf{b}} & \mathbf{a} & \mathbf{b} & \overline{\mathbf{a}} & a & b & \bar{b} & a & \bar{b} & a \\
\bar{a} & \bar{b} & a & b & \overline{\mathbf{b}} & \mathbf{a} & \mathbf{a} & \mathbf{b} & \mathbf{b} & \overline{\mathbf{a}} & b & \bar{a} & a & b & b & \bar{a} \\
\bar{a} & \bar{b} & a & b & \mathbf{b} & \overline{\mathbf{a}} & \mathbf{a} & \mathbf{b} & \overline{\mathbf{b}} & \mathbf{a} & \bar{b} & a & a & b & \bar{b} & a \\
\bar{b} & a & b & \bar{a} & \mathbf{b} & \overline{\mathbf{a}} & \overline{\mathbf{b}} & \mathbf{a} & \mathbf{a} & \mathbf{b} & b & \bar{a} & b & \bar{a} & a & b \\
\bar{b} & a & b & \bar{a} & \overline{\mathbf{b}} & \mathbf{a} & \mathbf{b} & \overline{\mathbf{a}} & \mathbf{a} & \mathbf{b} & \bar{b} & a & \bar{b} & a & a & b
\end{pmatrix},
$$

where a stable vertical split is shown in bold.

Finally, we see at once how Theorem 8.7 is a consequence of Theorem 9.13 as we can simply set the indeterminants to $+1$ to obtain the result.

§10. Related Configurations

In this section, the balancedly splittable orthogonal designs of the previous section are applied in the construction of related objects. We will explore quasi-symmetric balanced incomplete block designs, equiangular tight frames, and unbiased orthogonal designs.

* * *

10.1. Quasi-Symmetric BIBDs. Symmetric designs are characterized by the fact that the blocks of the design intersect in a constant number of points. The "next best" designs are those which have two cardinalities for the intersections between distinct blocks.

10.1. Definition. A balanced incomplete block design is *quasi-symmetric* if there exist two cardinalities that exist for the intersections between pairs of distinct blocks. The cardinalities of the intersections are called the *intersection numbers* of the design.[27])

These beautiful objects are studied extensively in Shrikhande and Sane (1991). Ionin and Shrikhande (2006) also contains a study of these objects, especially as it pertains to SRGs and association schemes.

10.2. Example. The following is the incidence matrix of a quasi-symmetric BIBD$(6, 15, 5, 2, 1)$

$$\begin{pmatrix} 0&1&0&0&0&1&0&0&1&0&0&0&1&0&1 \\ 0&1&0&0&0&0&1&1&0&0&0&1&0&1&0 \\ 1&0&0&0&1&0&0&1&0&0&1&0&0&0&1 \\ 1&0&0&1&0&0&0&0&1&1&0&0&0&1&0 \\ 0&0&1&1&0&0&1&0&0&0&1&0&1&0&0 \\ 0&0&1&0&1&1&0&0&0&1&0&1&0&0&0 \end{pmatrix} \tag{10.2.a}$$

with block intersection numbers 0 and 2.

Using the balancedly splittable Hadamard matrices constructed in Theorem 9.13, we can constuct quasi-symmetric BIBDs. For the proposition, we assume the notations of §8.3.

10.3. Proposition. If there is a Hadamard matrix of order n, there is a quasi-symmetric BIBD$(2n^2-n, 4n^2-1, 2n^2-n-1, n^2-n, n^2-n-1)$ with intersection numbers $(n^2-n)/2$ and $(n^2-2n)/2$.

Proof. If there exists a normalized Hadamard matrix of order n, there exists a balancedly splittable Hadamard matrix of order $4n^2$ by Theorem 8.7 (or by Theorem 9.13 upon setting the indeterminants to unity if there is a full OD of order n). It suffices to show the result for one of the four splits obtained by the theorem; in particular, we will show the result for the submatrix $X = \left(\begin{smallmatrix} -F \\ B \\ A \end{smallmatrix}\right)$. Form the matrix $\tilde{Y} = (1/2)(J - X)$, and take Y to be the matrix formed by omitting the first row of $\tilde{Y}$ consisting of all zeros.

Since H is assumed to be normalized, each row of H and $\left(\begin{smallmatrix} + & + \\ + & - \end{smallmatrix}\right) \otimes H$, other than the first, of course, contain $n/2$ and $n^2/2$ -1s, respectively. By construction, then, the first row of F consists of all ones, while the remaining rows have $n^2 - n$ $+1$s; thus, the same rows of $-F$ have $n^2 - n$ -1s. Similarly, A and B have $n(2n-2)/2 = n^2 - n$ -1s in each row. It also follows that there must be $2n^2 - 2n + n - 1 = 2n^2 - n - 1$ -1s in each column of X.

Finally, the index of the design follows by considering the Menon design[28]) induced by the regular Hadamard matrix of the construction.

It remains to consider the block intersection numbers of the design. Consider the first row of X along with any other two distinct rows. Without loss of generality, we can assume the following situation.

$$\begin{array}{cccc}
\overbrace{- \ \cdots \ -}^{a} & \overbrace{- \ \cdots \ -}^{b} & \overbrace{- \ \cdots \ -}^{c} & \overbrace{- \ \cdots \ -}^{d} \\
+ \ \cdots \ + & + \ \cdots \ + & - \ \cdots \ - & - \ \cdots \ - \\
+ \ \cdots \ + & - \ \cdots \ - & + \ \cdots \ + & - \ \cdots \ -
\end{array}$$

This yields the two linear systems of equations

$$\begin{aligned}
a + b + c + d &= 2n^2 - n, \\
-a - b + c + d &= -n, \\
-a + b - c + d &= -n, \text{ and} \\
a - b - c + d &= \pm n.
\end{aligned}$$

Solving for d gives $2d = n^2 - n$ or $n^2 - 2n$, which proves the result. ∎

10.4. Example. The quasi-symmetric BIBD$(6, 15, 5, 2, 1)$ given by (10.2.a) is obtained by the splittable Hadamard matrix (8.6.e).

The quasi-symmetric designs of the previous result are not new, however. They represent a subset of the designs obtained in Bracken et al. (2006) viz. McGuire (1997).

* * *

10.2. Equiangular Tight Frames. In our earliest collegiate education, we learn that given some linear space, the "nice" bases are those which are orthonormal. As Han et al. (2007) points out, however, the property of orthonormality can be too restrictive in many applications. For instance, if a signal is interferred with in transmission, then the lost information cannot be recovered.

By contrast, a frame is an overdetermined[29]) spanning set of vectors. In this way, calculations and applications involving these objects can at times be simplified and data loss deterred. Frames have theoretical applications as well, as shown in the seminal paper of Paley and Wiener (1987) using different language, however.

We will not have the opportunity to explore the theory of frames in any depth; rather, we direct the reader to the standard references of Christensen (2016), Waldron (2018), and Young (2001).

10.5. Definition. Let H be a Hilbert space[30]) with inner product $\langle\cdot,\cdot\rangle$, and let $\{f_i\} \subset H$. Then $\{f_i\}$ is a *frame* if there exists two constants A and B such that

(10.5.a) $$A\|f\|^2 \leq \sum_i |\langle f, f_i\rangle|^2 \leq B\|f\|^2, \text{ for all } f \in H.$$

A and B are called frame bounds. If $\#\{f_i\} < \infty$, it is a *finite frame*. If $A = B$, the frame is said to be *tight*. If $A = B = 1$, then $\{f_i\}$ is said to be a *Parseval frame*.

The frame bounds of a frame are not unique. The *optimal upper frame bound* is the infimum of the collection of all upper bounds of the frame. Similarly, the *optimal lower frame bound* is the supremum of the collection of all lower bounds of the frame.

It also follows from the definition that $\overline{\text{span}}\{f_i\} = H$.

10.6. Example. If $\{e_i\}$ is an orthonormal basis, then $\{e_0, e_0, e_1, e_1, \dots\}$, where each element is repeated twice, is a tight frame with $A = 2$.

10.7. Example. If $\{e_i\}$ is an orthonormal basis, then $\{e_0, 2^{-\frac{1}{2}}e_1, 2^{-\frac{1}{2}}e_1, 3^{-\frac{1}{2}}e_2, 3^{-\frac{1}{2}}e_2, 3^{-\frac{1}{2}}e_2\}$, where the element $(n+1)^{-\frac{1}{2}}e_n$ is repeated $n+1$ times, is a frame with $A = 1$.

From this point on, we will assume that we are working with a finite dimensional Hilbert space of dimension k. Our frames will, therefore, always be finite, say of order n. Just as for the standard bases of a space, we can relate matrices to finite frames.

10.8. Definition. Let $\{f_0, \dots, f_{n-1}\}$ be a finite frame in a finite dimensional Hilbert space H. The matrix $\Theta = \begin{pmatrix} f_0^* \\ \vdots \\ f_{n-1}^* \end{pmatrix}$ is the *analysis operator* of the frame, and Θ^* is called the *synthesis operator* of the frame.

The following is then a restatement of the definitions.

10.9. Proposition. Let $x_0, \dots, x_{n-1}$ be vectos in a Hilbert space H of dimension n, and define the $k \times n$ matrix $T = \left(\begin{smallmatrix} x_0 & \cdots & x_{n-1} \end{smallmatrix} \right)$. Then:

(10.9.a) $\{x_0, \dots, x_{n-1}\}$ is a frame if and only if $\operatorname{rank}(T) = n$,

(10.9.b) $\{x_0, \dots, x_{n-1}\}$ is a tight frame with bound A if and only if $TT^* = \sqrt{A}I$.

In what follows, we will take $\mathbf{H} = \{a_1 + a_i i + a_j j + a_k k : a_1, a_i, a_j, a_k \in \mathbf{R}\}$, i.e. the $\mathbf{R}$-algebra of quaternions[31]), and we will consider frames over $\mathbf{H}^k$. Furthermore, for $q = z + wj$ where $z, w \in \mathbf{C}$, we define $\mathrm{Co}_1(q) = z$ and $\mathrm{Co}_2(q) = w^*$. Finally, define $[\cdot]_{\mathbf{C}} : \mathbf{H}^d \to \mathbf{C}^{2d}$ by $[q]_{\mathbf{C}} = \begin{pmatrix} \mathrm{Co}_1(q) \\ \mathrm{Co}_2(q) \end{pmatrix} = \left(\begin{smallmatrix} z \\ w^* \end{smallmatrix} \right)$.

The following is Theorem 3.2 of Waldron (2020).

10.10. Theorem. (10.10.a) Tight frames for $\mathbf{C}^{2k}$ correspond to tight frames for $\mathbf{H}^k$, and

(10.10.b) Tight frames for $\mathbf{H}^k$ correspond to tight frames for $\mathbf{C}^k$ if and only if

$$\sum_{i,j} |\mathrm{Co}_1(\langle f_i, f_j\rangle)|^2 = \sum_{i,j} |\mathrm{Co}_2(\langle f_i, f_j\rangle)|^2.$$

In light of this result, it is of interest to find frames over $\mathbf{H}^k$ for which they are not equivalent to frames over $\mathbf{C}^{2d}$, i.e. there can be no reduction in the ring of scalars. We present two examples of such frames.

10.11. Example. The following is a QOD$(2; 1, 1)$

$$\text{(10.11.a)} \quad \begin{pmatrix} \bar{a} & bi \\ \bar{b}j & ak \end{pmatrix},$$

where a and b are real variables. We then arrive at the following QOD$(16; 8, 8)$

$$\text{(10.11.b)} \quad \begin{pmatrix}
\bar{a} & bi & \bar{a} & bi & \bar{a} & bi & \bar{a} & bi & \bar{a} & bi & a & \bar{b}i & a & \bar{b}i & a & \bar{b}i \\
\bar{a} & bi & \bar{a} & bi & a & \bar{b}i & \bar{a} & bi & a & \bar{b}i & \bar{a} & bi & a & \bar{b}i & \bar{a} & bi \\
\bar{a} & bi & \bar{a} & bi & \bar{a} & bi & a & \bar{b}i & a & \bar{b}i & a & \bar{b}i & \bar{a} & bi & \bar{a} & bi \\
\bar{a} & bi & \bar{a} & bi & a & \bar{b}i & a & \bar{b}i & \bar{a} & bi & \bar{a} & bi & \bar{a} & bi & a & \bar{b}i \\
\bar{\mathbf{b}}\mathbf{j} & \mathbf{ak} & \bar{\mathbf{b}}\mathbf{j} & \mathbf{ak} & \bar{\mathbf{a}} & \mathbf{bi} & \bar{\mathbf{b}}\mathbf{j} & \mathbf{ak} & \bar{\mathbf{b}}\mathbf{j} & \mathbf{ak} & \bar{\mathbf{a}} & \mathbf{bi} & \bar{\mathbf{b}}\mathbf{j} & \mathbf{ak} & \mathbf{bj} & \bar{\mathbf{a}}\mathbf{k} \\
\bar{\mathbf{b}}\mathbf{j} & \mathbf{ak} & \bar{\mathbf{b}}\mathbf{j} & \mathbf{ak} & \bar{\mathbf{a}} & \mathbf{bi} & \mathbf{bj} & \bar{\mathbf{a}}\mathbf{k} & \mathbf{bj} & \bar{\mathbf{a}}\mathbf{k} & \bar{\mathbf{a}} & \mathbf{bi} & \mathbf{bj} & \bar{\mathbf{a}}\mathbf{k} & \bar{\mathbf{b}}\mathbf{j} & \mathbf{ak} \\
\bar{\mathbf{a}} & \mathbf{bi} & \mathbf{a} & \bar{\mathbf{b}}\mathbf{i} & \bar{\mathbf{b}}\mathbf{j} & \mathbf{ak} & \bar{\mathbf{a}} & \mathbf{bi} & \bar{\mathbf{b}}\mathbf{j} & \mathbf{ak} & \mathbf{bj} & \bar{\mathbf{a}}\mathbf{k} & \bar{\mathbf{a}} & \mathbf{bi} & \bar{\mathbf{b}}\mathbf{j} & \mathbf{ak} \\
\bar{\mathbf{a}} & \mathbf{bi} & \mathbf{a} & \bar{\mathbf{b}}\mathbf{i} & \mathbf{bj} & \bar{\mathbf{a}}\mathbf{k} & \bar{\mathbf{a}} & \mathbf{bi} & \mathbf{bj} & \bar{\mathbf{a}}\mathbf{k} & \bar{\mathbf{b}}\mathbf{j} & \mathbf{ak} & \bar{\mathbf{a}} & \mathbf{bi} & \mathbf{bj} & \bar{\mathbf{a}}\mathbf{k} \\
\bar{\mathbf{b}}\mathbf{j} & \mathbf{ak} & \mathbf{bj} & \bar{\mathbf{a}}\mathbf{k} & \bar{\mathbf{b}}\mathbf{j} & \mathbf{ak} & \bar{\mathbf{b}}\mathbf{j} & \mathbf{ak} & \bar{\mathbf{a}} & \mathbf{bi} & \bar{\mathbf{b}}\mathbf{j} & \mathbf{ak} & \mathbf{bj} & \bar{\mathbf{a}}\mathbf{k} & \bar{\mathbf{a}} & \mathbf{bi} \\
\bar{\mathbf{b}}\mathbf{j} & \mathbf{ak} & \mathbf{bj} & \bar{\mathbf{a}}\mathbf{k} & \mathbf{bj} & \bar{\mathbf{a}}\mathbf{k} & \mathbf{bj} & \bar{\mathbf{a}}\mathbf{k} & \bar{\mathbf{a}} & \mathbf{bi} & \mathbf{bj} & \bar{\mathbf{a}}\mathbf{k} & \bar{\mathbf{b}}\mathbf{j} & \mathbf{ak} & \bar{\mathbf{a}} & \mathbf{bi} \\
bj & \bar{a}k & bj & \bar{a}k & \bar{a} & bi & \bar{b}j & ak & bj & \bar{a}k & \bar{a} & bi & \bar{b}j & ak & \bar{b}j & ak \\
bj & \bar{a}k & bj & \bar{a}k & \bar{a} & bi & bj & \bar{a}k & \bar{b}j & ak & \bar{a} & bi & bj & \bar{a}k & bj & \bar{a}k \\
a & \bar{b}i & \bar{a} & bi & bj & \bar{a}k & \bar{a} & bi & \bar{b}j & ak & \bar{b}j & ak & \bar{a} & bi & \bar{b}j & ak \\
a & \bar{b}i & \bar{a} & bi & \bar{b}j & ak & \bar{a} & bi & bj & \bar{a}k & bj & \bar{a}k & \bar{a} & bi & bj & \bar{a}k \\
bj & \bar{a}k & \bar{b}j & ak & \bar{b}j & ak & bj & \bar{a}k & \bar{a} & bi & \bar{b}j & ak & \bar{b}j & ak & \bar{a} & bi \\
bj & \bar{a}k & \bar{b}j & ak & bj & \bar{a}k & \bar{b}j & ak & \bar{a} & bi & bj & \bar{a}k & bj & \bar{a}k & \bar{a} & bi
\end{pmatrix}.$$

Taking the horizontal frame shown in bold as the synthesis operator of a frame over $\mathbf{H}^6$ after setting $a = b = 1$, we find that $(1/2)H^*H$ is given by

$$(10.11.c)\qquad \begin{pmatrix}
3 & i & - & i & \bar{j} & \bar{k} & 1 & \bar{i} & \bar{j} & \bar{k} & \bar{j} & \bar{k} & 1 & \bar{i} & \bar{j} & \bar{k} \\
\bar{i} & 3 & \bar{i} & - & k & \bar{j} & i & 1 & k & \bar{j} & k & \bar{j} & i & 1 & k & \bar{j} \\
- & i & 3 & i & \bar{j} & \bar{k} & - & i & j & k & \bar{j} & \bar{k} & - & i & j & k \\
\bar{i} & - & \bar{i} & 3 & k & \bar{j} & \bar{i} & - & \bar{k} & j & k & \bar{j} & \bar{i} & - & \bar{k} & j \\
j & \bar{k} & j & \bar{k} & 3 & i & 1 & i & 1 & i & 1 & \bar{i} & - & \bar{i} & 1 & i \\
k & j & k & j & \bar{i} & 3 & \bar{i} & 1 & \bar{i} & 1 & i & 1 & i & - & \bar{i} & 1 \\
1 & \bar{i} & - & i & 1 & i & 3 & i & 1 & i & 1 & i & 1 & \bar{i} & - & \bar{i} \\
i & 1 & \bar{i} & - & \bar{i} & 1 & \bar{i} & 3 & \bar{i} & 1 & \bar{i} & 1 & i & 1 & i & - \\
j & \bar{k} & \bar{j} & k & 1 & i & 1 & i & 3 & i & - & \bar{i} & 1 & i & 1 & \bar{i} \\
k & j & \bar{k} & \bar{j} & \bar{i} & 1 & \bar{i} & 1 & \bar{i} & 3 & i & - & \bar{i} & 1 & i & 1 \\
j & \bar{k} & j & \bar{k} & 1 & \bar{i} & 1 & i & - & \bar{i} & 3 & i & - & \bar{i} & - & \bar{i} \\
k & j & k & j & i & 1 & \bar{i} & 1 & i & - & \bar{i} & 3 & i & - & i & - \\
1 & \bar{i} & - & i & - & \bar{i} & 1 & \bar{i} & 1 & i & - & \bar{i} & 3 & i & - & \bar{i} \\
i & 1 & \bar{i} & - & i & - & i & 1 & \bar{i} & 1 & i & - & \bar{i} & 3 & i & - \\
j & \bar{k} & \bar{j} & k & 1 & i & - & \bar{i} & 1 & \bar{i} & - & \bar{i} & - & \bar{i} & 3 & i \\
k & j & \bar{k} & \bar{j} & \bar{i} & 1 & i & - & i & 1 & i & - & i & - & \bar{i} & 3
\end{pmatrix}.$$

It follows that $320 = \sum_{i,j} |\mathrm{Co}_1(\langle f_i, f_j\rangle)|^2 \neq \sum_{i,j} |\mathrm{Co}_2(\langle f_i, f_j\rangle)|^2 = 64$ so that the frame is not reducible to a frame over $\mathbf{C}^{12}$.

10.12. Example. Beginning with the QOD$(6; 1, 5)$

$$(10.12.a)\qquad \begin{pmatrix}
a & b & b & b & b & b \\
b & \overline{a} & bk & \overline{bk} & \overline{bk} & bk \\
b & bk & \overline{a} & bk & \overline{bk} & \overline{bk} \\
b & \overline{bk} & bk & \overline{a} & bk & \overline{bk} \\
b & \overline{bk} & \overline{bk} & bk & \overline{a} & bk \\
b & bk & \overline{bk} & \overline{bk} & bk & \overline{a}
\end{pmatrix},$$

we apply the construction to obtain a QOD$(144; 24, 120)$. Taking H to again be the first horizontal frame of the splittable QOD, we find that $29056 = \sum_{i,j} |\mathrm{Co}_1(\langle f_i, f_j\rangle)|^2 \neq \sum_{i,j} |\mathrm{Co}_2(\langle f_i, f_j\rangle)|^2 = 8960$. It follows that we have constructed another quaternion frame not reducible to a complex frame.

* * *

10.3. Unbiased Orthogonal Designs. Let A and B be two orthonormal bases of the Hilbert space $\mathbf{C}^k$. The bases are said to be *mutually unbiased* in the event that $|\langle a, b\rangle| = k^{-\frac{1}{2}}$, for every $a \in A$ and $b \in B$, and where $\langle a, b\rangle$ denotes the usual sesquilinear inner product between a and b.

The reader will recognize unbiased bases as a subtype of equiangular lines (see §8.2). These objects are fundamental in many applications such as quantum key distribution (see Boykin et al., 2005).

Unitary Hadamard matrices, i.e. a matrices with entries from the unit circle in the complex plane whose rows are pairwise orthogonal, have received much attention with their connection to unbiased bases. Two unitary Hadamard matrices H and K of order n are *unbiased* if $HK^* = \sqrt{n}L$, for some unitary Hadamard matrix L. Recently, these ideas where studied for the case of unitary weighing matrices[32]) in Best et al. (2015). The case of unbiased real Hadamard matrices were studied in Holzmann et al. (2010), and the case of unbiased quaternary complex Hadamard in Best and Kharaghani (2010).

We have seen that extending concepts from matrices of concrete values to matrices of indeterminants usually presents us with subtle difficulties, and extending unbiasedness is no different. In Kharaghani and Suda (2018), unbiased orthogonal designs are presented thus.

10.13. Definition. Let X_1 and X_2 be two instances of an $\mathrm{OD}(n; s_1, \dots, s_u)$ in the indeterminants $x_1, \dots, x_u$. Then X_1 and X_1 are *unbiased* with parameter $\alpha \in \mathbf{R}_+$ if there is a $(-1, 0, 1)$-matrix W such that

$$X_1 X_2^t = \left(\alpha^{-\frac{1}{2}} \sum_i s_i x_i^t\right) W. \tag{10.13.a}$$

We use the stable construction presented in the previous section to construct pairs of unbiased orthogonal designs. Note that this is essentially a generalization of a method presented in Kharaghani and Suda (2019). In what follows, we take Z to be as in §9.3.

10.14. Proposition. Let

$$V = \begin{pmatrix} -F \\ B \\ A \end{pmatrix}, \text{ and } U = \begin{pmatrix} G & F \\ E & A \\ -E & B \end{pmatrix}$$

so that $Z = \begin{pmatrix} U & V \end{pmatrix}$, and take $Y = \begin{pmatrix} U & -V \end{pmatrix}$. Then Y is an OD of the same order and type as Z. In particular, $ZY^t = 2\sigma K$, where K is a Hadamard matrix.

Proof. That Y is also an OD is clear. Then $ZY^t = (UU^t - VV^t)$. We claim that $K = (1/2\sigma)(UU^t - VV^t)$ is a Hadamard matrix. Indeed, since the vertical frames of Z constitute a stable split, and since Z is an OD, we find that K has entries from the set $\{-1, 1\}$. Furthermore,

$$\begin{aligned} KK^t &= \frac{1}{4\sigma^2}(UU^tUU^t + VV^tVV^t) \\ &= \frac{n}{\sigma}(UU^t + VV^t) \\ &= 4n^2 I, \end{aligned}$$

and the proof is complete. ∎

Notes

24. Recall the angle between two vectors in $\mathbf{R}^\ell$ is given by $\alpha = \arccos(\langle u, v\rangle/\|u\|\|v\|)$. It follows that we only need to consider $|\langle u, v\rangle|$ whenever we want to deduce the number of angles that exist between a collection of vectors in $\mathbf{R}^\ell$.

25. The classic construction due to Paley goes as follows. Let q be odd, and take GF(q) $= \{a_0 = 0, a_1, \ldots, a_{q-1}\}$. If η is the quadratic character on GF(q), define Q by $Q_{ij} = \eta(a_j - a_i)$. Finally, form the matrix $W = \begin{pmatrix} 0 & \mathbf{1}^t \\ (-1)^{(q-1)/2}\mathbf{1} & Q \end{pmatrix}$. Then W is a W($q+1, q$). If $q \equiv -1 \pmod 4$, then $W^t = -W$; while if $q \equiv 1 \pmod 4$, then $W^t = W$. See Hall (1986) for more detail.

26. In defining the auxiliary matrix of a full OD, we limit ourselves to using the Hadamard matrix obtained from the OD by setting the indeterminants equal to $+1$. This is done that the formation of the auxiliary matrices is unique.

27. Quasi-symmetric designs are often studied in the more general context of t-designs (see §1.1). This is the approach taken in Ionin and Shrikhande (2006) and Shrikhande and Sane (1991).

28. It isn't difficult to see that a regular Hadamard matrix H must have square order $4u^2$. Moreover, it follows that $(1/2)(J - H)$ is a symmetric BIBD$(4u^2, 2h^2 - h, h^2 - h)$. The converse can also seen to be true. The reader may consult Stinson (2004) for a standard treatment of these objects. Ionin and Shrikhande (2006) studies these objects and their applications in constructing other configurations.

29. Note the similarity to the redundance introduced in constructing the error-correcting codes of §2.

30. Recall that a Hilbert space is a complete normed linear space where the norm is induced by an inner

product. Halmos (1982) and Halmos (1998) are standard references on the subject of Hilbert spaces.

31. There is some ambiguity in defining frames over $\mathbf{H}^k$. As $\mathbf{H}$ is a skew-field, we can take $\mathbf{H}^k$ to be either a left- or right-module. This discussion is taken up in detail in Waldron (2020), where the right-module is always used.

32. There are different ways of defining unbiased weighing matrices. Classically, two unitary weighing matrices $\mathrm{W}(n,k)$, say H and K, are *unbiased* if $HK^* = \sqrt{k}L$, for some unitary weighing matrix L of weight k. In Nozaki and Suda (2015), the weighing matrices H and K above are *quasi-unbiased* with parameters (n,k,ℓ,a) if $a^{-\frac{1}{2}}HK^*$ is a $\mathrm{W}(n,\ell)$. It is this idea of quasi-unbiasedness that is most easily extended to orthogonal designs.

5

A New Family of Balanced Weighing Matrices and Association Schemes

This chapter serves as a particular application of a more general construction to be given in the following chapter. Here a new family of balanced weighing matrices are constructed, and an equivalence to certain association schemes is developed. The work shown here is a result of Kharaghani et al. (2022).

§11. Generalized Kronecker Product

In this section, we briefly review the Kronecker product and a few of its properties and applications, namely, we will see its applications to regular Hadamard matrices. Following this, we will consider a simple generalization of the Kronecker product in order to allow particular bijections to act on a matrix.

* * *

11.1. Definitions. Let A be an $n \times m$ matrix, and let B be an $s \times t$ matrix, each with entries from some field. The *Kronecker product* of A by B is the $ns \times mt$ matrix given by $A \otimes B = (A_{ij}B)$. This noncommutative matrix product has the following immediate properties wherever the sizes of the matrices make sense.

11.1. Lemma. Let A, B, C and D be matrices over some field F, and let $\lambda \in F$. Then:

(11.1.a) $\lambda A \otimes B = A \otimes \lambda B = \lambda(A \otimes B)$,

(11.1.b) $A \otimes B = (A \times I)(I \otimes B) = (I \otimes B)(A \otimes I)$,

(11.1.c) $(A + B) \otimes C = (A \otimes C) + (B \otimes C)$,

(11.1.d) $A \otimes (B + C) = (A \otimes B) + (A \otimes C)$,

(11.1.e) $(A \otimes B)(C \otimes D) = AC \otimes BD$,

(11.1.f) $(A \otimes B)^t = A^t \otimes B^t$, and

(11.1.g) if A is $n \times n$ and B is $m \times m$, then $\det(A \otimes B) = [\det(A)]^m[\det(B)]^n$.

There are a number of immediate applications of the Kronecker product to what we have done so far. For instance, if H is a W(n_1, k_1) and K a W(n_2, k_2), then $H \otimes K$ is a W$(n_1 n_2, k_1 k_2)$.

11.2. Example. Let H be the Hadamard matrix of order 4 given by

$$\text{(11.2.a)} \quad \begin{pmatrix} - + + + \\ + - + + \\ + + - + \\ + + + - \end{pmatrix}.$$

Then $H \otimes H$ is the Hadamard matrix of 16 given by

$$
\text{(11.2.b)} \quad \begin{pmatrix}
+&-&-&-&-&+&+&+&-&+&+&+&-&+&+&+\\
-&+&-&-&+&-&+&+&+&-&+&+&+&-&+&+\\
-&-&+&-&+&+&-&+&+&+&-&+&+&+&-&+\\
-&-&-&+&+&+&+&-&+&+&+&-&+&+&+&-\\
-&+&+&+&+&-&-&-&-&+&+&+&-&+&+&+\\
+&-&+&+&-&+&-&-&+&-&+&+&+&-&+&+\\
+&+&-&+&-&-&+&-&+&+&-&+&+&+&-&+\\
+&+&+&-&-&-&-&+&+&+&+&-&+&+&+&-\\
-&+&+&+&-&+&+&+&+&-&-&-&-&+&+&+\\
+&-&+&+&+&-&+&+&-&+&-&-&+&-&+&+\\
+&+&-&+&+&+&-&+&-&-&+&-&+&+&-&+\\
+&+&+&-&+&+&+&-&-&-&-&+&+&+&+&-\\
-&+&+&+&-&+&+&+&-&+&+&+&+&-&-&-\\
+&-&+&+&+&-&+&+&+&-&+&+&-&+&-&-\\
+&+&-&+&+&+&-&+&+&+&-&+&-&-&+&-\\
+&+&+&-&+&+&+&-&+&+&+&-&-&-&-&+
\end{pmatrix},
$$

where the block structure is evident[33]).

As one further application of the standard Kronecker product before we move on, we will consider regular Hadamard matrices.

11.3. Definition. A Hadamard matrix is *row regular* (or *column regular*) if it's rows (resp. columns) have a constant sum. A Hadamard matrix is *regular* if it is both row and column regular.

It isn't difficult to see that a Hadamard matrix is row regular or column regular if and only if it is regular. Moreover, if the constant row (column) sum is s, then the order of the matrix is s^2 (see Stinson, 2004, Chapter 4). By the definition of the standard Kronecker product, we also see that if H and K are regular Hadamard matrices, then so is $H \otimes K$.

Example 11.2 has evinced the existence of a regular $\mathrm{W}(4, 4)$. It is also known that there is a regular $\mathrm{W}(36, 36)$ (see Stinson, 2004, Chapter 4). Also, if there is a Hadamard matrix of order n, then there is a symmetric, regular, Hadamard matrix with constant block diagonal of order n^2 (see Colbourn and Dinitz, 2007, Part V). We then have the following result.

11.4. Proposition. If there exist Hadamard matrices of orders $n_1, \ldots, n_k$, then there is a regular Hadamard matrix of order $4^a 9^b n_1^2 \cdots n_k^2$, for $a, b \in \mathbf{Z}_+$ and $a \geq b$.

Having convinced ourselves of the utility of the standard Kronecker product, we generalize in the following way. Let $\mathcal{M}$ be a collection of $n \times m$ matrices with entries from some commutative ring R, and let Ξ be an $s \times t$ matrix over the collection of endofunctions of $\mathcal{M}$. For each $A \in \mathcal{M}$, the $ns \times mt$ matrix $\Xi \otimes A$ over R is defined as $(\Xi_{ij}(A))$. If certain properties of A are left invariant under the elements of Ξ, then these properties will be reflected in the block structure of $\Xi \otimes A$.

With the above ideas in mind, if we have a collection $\mathcal{M}$ of objects, we desire a subset of the collection of endofunctions of $\mathcal{M}$ that are property preserving. If $\mathcal{M}$ is a collection of incidence structures, then a set of bijections of $\mathcal{M}$ that preserve incidence is called a *group of symmetries* of $\mathcal{M}$. If Ξ is a BGW over a group of symmetries, then $\Xi \otimes A$ has both inter-block regularites and intra-block regularities.

* * *

11.2. A First Application: Block designs. In the previous subsection, we began a brief discussion of groups of symmetries of incidence structures. As an example, let $\mathbf{D} = (X, \mathscr{B})$ be a BIBD(v, b, r, k, λ), and let $\mathscr{B} = \bigcup_{i=1}^m \mathscr{B}_i$ be a partition of the blocks of $\mathbf{D}$. If G_i acts on $\mathscr{B}_i$, then, $(X, \bigcup_{i=1}^m \mathscr{B}_i g_i)$, for $g_i \in G_i$, is again a BIBD(v, b, r, k, λ). Let $A = A(\mathbf{D})$ be the incidence matrix of $\mathbf{D}$, and assume that $A = \left(A(X,\mathscr{B}_1) \cdots A(X,\mathscr{B}_m) \right)$. Then $G = \prod_i G_i$ acts naturally on the columns of A. If in addition G_i is sharpley transitive on $\mathscr{B}_i$, and if each point $x \in X$ appears r_i times in $\mathscr{B}_i$, then

$$|G|^{-1} \sum_{g \in G} Ag = \left(r_1 b_1^{-1} J_{v \times b_1} \cdots r_m b_m^{-1} J_{v \times b_m} \right),$$

where $b_i = |\mathscr{B}_i|$. Therefore, if $r_i b_j = r_j b_i$, for all $i, j \in \{1, \ldots, m\}$, then $\sum_{g \in G} Ag$ is an integer multiple of $J_{v \times b}$ since $b_i \mid |G|$. Since G acts on the columns of A, we also have that $Xg(Yg)^t = XY^t$, for each $X, Y \in AG$.

This motivates the following. If G is a group of symmetries of a collection $\mathcal{M}$ of BIBD(v, b, r, k, λ)s such that $\sum_{g \in G} Xg = \alpha_X J$, for some $\alpha_X \in \mathbf{N}$ and all $X \in \mathcal{M}$; and if $Xg(Yg)^t = XY^t$, for all $X, Y \in \mathcal{M}$; then we say that G is an *admissible* group of symmetries of $\mathbf{D}$. We then have the following.

11.5. Theorem. Let $\mathcal{M}$ be a collection of BIBD(v, b, r, k, λ)s, and let G be an admissible group of symmetries of $\mathcal{M}$. If Ξ is a BGW$(w, \ell, \mu; G)$ such that $kr\mu = v\lambda\ell$, then $\Xi \otimes X$ is a BIBD$(vw, bw, r\ell, k\ell, \lambda\ell)$, for any $X \in \mathcal{M}$.

Proof. Straightforward calculation. See Theorem 2.4 of Ionin (2001) for details. ∎

11.6. Corollary. If X is quasi-residual, then so is $\Xi \otimes X$.

11.7. Example. Let $q = p^n$ be a prime power, and let H be a GH$(q, 1)$ over EA(q) where the elements have the usual representation of $(0, 1)$-matrices. Then it isn't difficult to see that $A = \left(I_q \otimes \mathbf{1}_q \; H \right)$ is a BIBD$(q^2, q + q^2, 1 + q, q, 1)$. Importantly, the columns are placed into $1 + q$ consecutive disjoint groups of q columns each such that each point appears precisely once in every group[34]). Let G be the group which cyclically permutes the blocks in each group so that $|G| = q$.

If $1 + q$ is a prime power, then there is a BGW$(2 + q, 1 + q, q; C_q)$, say Ξ, where the group elements cyclically permute the blocks of each parition class in the above design. The parametric conditions of the theorem are met, hence $\Xi \otimes A$ is a BIBD$(q^2(2 + q), (q + q^2)(2 + q), (1 + q)^2, q(1 + q), 1 + q)$. More generally, we can take Ξ to be any BGW$((p^{n+1} - 1)/(p - 1), p^n, p^n - p^{n-1}; C_q)$, where $p = 1 + q$.

* * *

11.3. A Second Application: Bkaskar Rao designs. It isn't difficult to extend the ideas of Theorem 11.5 to the more general Bhaskar Rao designs. In order to accomplish this, however, we need to extend the idea of admissible groups of symmetries.

Let $\mathcal{M}$ be a collection of GBRD$(v, b, r, k, \lambda; H)$s. Then a group of bijections G of $\mathcal{M}$ is an admissible group of symmetries if (a) $\sum_{g \in G} Xg = \alpha_X HJ$, for some $\alpha_X \in \mathbf{N}$ and every $X \in \mathcal{M}$, and (b) $Xg(Yg)^* = XY^*$, for every $X, Y \in \mathcal{M}$.

The following is then a simple generalization of Theorem 11.5

11.8. Theorem. Let $\mathcal{M}$ be a collection of GBRD$(v, b, r, k, \lambda; H)$s, and let G be an admissible group of symmetries of $\mathcal{M}$. If Ξ is a BGW$(w, \ell, \mu; G)$ such that $kr\mu = v\lambda\ell$, then $\Xi \otimes X$ is a GBRD$(vw, bw, r\ell, k\ell, \lambda\ell; H)$, for any $X \in \mathcal{M}$.

11.9. Example. The following example was noted in Pender (2020). The following BGW$(15, 7, 3; C_3)$ was found by computational means in Gibbons and Mathon (1987)

$$\begin{pmatrix}
0&3&3&3&3&3&3&3&0&0&0&0&0&0&0\\
0&3&2&0&1&0&0&0&0&0&2&0&2&2&3\\
0&0&3&2&0&1&0&0&3&0&0&2&0&2&2\\
0&0&0&3&2&0&1&0&2&3&0&0&2&0&2\\
0&0&0&0&3&2&0&1&2&2&3&0&0&2&0\\
0&1&0&0&0&3&2&0&0&2&2&3&0&0&2\\
0&0&1&0&0&0&3&2&2&0&2&2&3&0&0\\
0&2&0&1&0&0&0&3&0&2&0&2&2&3&0\\
3&3&1&0&2&0&0&0&3&2&0&1&0&0&0\\
3&0&3&1&0&2&0&0&0&3&2&0&1&0&0\\
3&0&0&3&1&0&2&0&0&0&3&2&0&1&0\\
3&0&0&0&3&1&0&2&0&0&0&3&2&0&1\\
3&2&0&0&0&3&1&0&1&0&0&0&3&2&0\\
3&0&2&0&0&0&3&1&0&1&0&0&0&3&2\\
3&1&0&2&0&0&0&3&2&0&1&0&0&0&3
\end{pmatrix}, \tag{11.9.a}$$

where the nonzero entries are logarithms of some generator of C_3. Note that the core of (11.9.a) is composed of 4 circulant matrices. Taking R to be the residual part of (11.9.a), and letting $g = \left(\begin{smallmatrix} O & I_7 \\ \omega I_7 & O \end{smallmatrix}\right)$, we see that $G = \langle g \rangle$ forms an admissible group of symmetries for R. For any $n \in N$, there is a BGW$((7^{n+1}-1)/6, 7^n, 6 \cdot 7^{n-1}; G)$ which satisfy the parametric conditions of Theorem 11.8. Therefore, for any $n > 0$, there is a GBRD$(4(7^{n+1}-1)/3, 2 \cdot 7^{n+1}, 7^{n+1}, 4 \cdot 7^n, 3 \cdot 7^n; C_3)$.[35])

This concludes our introduction to the generalized Kronecker product.

§12. A New Family of Balanced Weighing Matrices

Here the generalized Kronecker product of the previous subsection will be put to use in constructing a new family of balanced weighing matrices. Additionally, the simplex codes appear again and are applied in the construction. The construction presented here is indicative of a general method to be presented in the following chapter.

* * *

12.1. Lemmata. In §2.2, we introduced the linear simplex code $\mathscr{S}_{q,n}$. There it was shown that the code had constant weight q^{n-1}; in particular, it follows that it is equidistant with constant Hamming distance q^{n-1} since the code is linear.

In Rajkundlia (1983), and later reproduced in Ionin (2001) using the language of BGW matrices, generalized Hadamard matrices GH(q, q^{n-1}) were used recursively in conjunction with the classical parameter BGW$((q^n-1)/(q-1), q^{n-1}, q^{n-1}-q^{n-2}; \mathrm{GF}(q)^*)$s in order to construct certain designs. It turns out out that the GH(q, q^{n-1}) used in the construction can be replaced by $\mathscr{S}_{q,n}$, and so simplify the construction.

In order to apply the linear code $\mathscr{S}_{q,n}$, we will require the following lemma.

12.1. Lemma. Let GF$(q) = \{a_0 = 0, a_1, \ldots, a_{q-1}\}$, and let $n > 1$. Then there exist disjoint $(0,1)$-matrices $A_{a_1}, \ldots, A_{a_{q-1}}$ of dimensions $q^n \times (q^n-1)/(q-1)$

such that $\mathscr{S}_{q,n} = \sum_{\alpha \in \mathrm{GF}(q)^*} \alpha A_\alpha$. If we define $A_0 = J - \sum_{\alpha \in \mathrm{GF}(q)^*} A_\alpha$, then the following hold.

(12.1.a) $\sum_{\alpha \in \mathrm{GF}(q)} A_\alpha A_\alpha^t = \frac{q^{n-1}-1}{q-1} J + q^{n-1} I$, and

(12.1.b) $\sum_{\substack{\alpha,\beta \in \mathrm{GF}(q)\\ \alpha \neq \beta}} A_\alpha A_\beta^t = q^{n-1}(J - I)$.

Proof. Labeling the rows of $\mathscr{S}_{q,n}$ by $r_0, \ldots, r_{q^n-1}$, and taking $A = \mathscr{S}_{q,n}$, we then have that

$$\begin{aligned}
(\sum_{\alpha \in \mathrm{GF}(q)} A_\alpha A_\alpha^t)_{ij} &= \sum_{\alpha \in \mathrm{GF}(q)} (A_\alpha A_\alpha^t)_{ij} \\
&= \sum_{\alpha \in \mathrm{GF}(q)} \sum_{\ell=0}^{\frac{q(q^{n-1}-1)}{q-1}} (A_\alpha)_{i\ell} (A_\alpha)_{j\ell} \\
&= \sum_{\alpha \in \mathrm{GF}(q)} \#\{\ell \in \{0, \ldots, \frac{q(q^{n-1}-1)}{q-1}\} : A_{i\ell} = A_{j\ell} = \alpha\} \\
&= \#\{\ell \in \{0, \ldots, \frac{q(q^{n-1}-1)}{q-1}\} : A_{i\ell} = A_{j\ell}\} \\
&= \frac{q^n - 1}{q-1} - \mathrm{dist}(r_i, r_j),
\end{aligned}$$

which shows (12.1.a).

Since $\sum_{\alpha \in \mathrm{GF}(q)} A_\alpha = J$, it follows that $\sum_{\alpha,\beta} A_\alpha A_\beta^t = (\sum_\alpha A_\alpha)(\sum_\beta A_\beta)^t = \frac{q^n-1}{q-1} J$, and (12.1.b) has been proven. ∎

If W is a BGW$(v, k, \lambda; C_n)$ over some cyclic group $C_n = \{1, g, \ldots, g^{n-1}\}$ of order n, then there are n disjoint $(0,1)$-matrices $W_0, \ldots, W_{n-1}$ such that $W = W_0 + gW_1 + \cdots + g^{n-1} W_{n-1}$. We call W_0 and W_1 the *decomposition matrices* of the weighing matrix. Because W is a BGW matrix, we have the following lemma.

12.2. Lemma.

(12.2.a) $\displaystyle\sum_{i,j} g^{i-j} W_i W_j^t = \sum_{i,j} g^{i-j} W_j^t W_i = kI + \tfrac{\lambda}{n}(\sum_i g_i)(J-I),$

(12.2.b) $\displaystyle\sum_i W_i W_i^t = \sum_i W_i^t W_i = kI + \tfrac{\lambda}{n}(J-I)$, and

(12.2.c) $\displaystyle\sum_i W_i W_{i+j}^t = \sum_i W_{i+j}^t W_i = \tfrac{\lambda}{n}(J-I)$, for $j \in \{1,\ldots,n-1\}$.

Proof. (12.2.a) is simply a restatment of the fact that both W and W^* are BGW$(v,k,\lambda;C_n)$s (see Proposition 4.19). (12.2.b) follows by noting that there are k nonzero entries in every row of W, and that 1 appears λ/n times in the conjugate inner product between distinct rows. Similarly, (12.2.c) follows by noting that each nonidentity element of the group appears λ/n times in the conjugate inner product between distinct rows of W, and that $i \neq i+j$, for each i whenever $j \not\equiv 0 \pmod{n}$. ∎

Now, consider the balanced W$(19,9)$ shown to exist by computational means in de Launey and Sarvate (1984).

$$W_{19} = \begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&+&+&+&+&+&+&+&+&+\\
0&-&0&0&+&0&+&+&+&0&0&0&0&+&0&-&+&-&0\\
0&0&-&0&+&+&0&0&+&+&0&0&0&-&+&0&0&+&-\\
0&0&0&-&0&+&+&+&0&+&0&0&0&0&-&+&-&0&+\\
0&+&+&0&-&0&0&+&0&+&+&-&0&0&0&0&+&0&-\\
0&0&+&+&0&-&0&+&+&0&0&+&-&0&0&0&-&+&0\\
0&+&0&+&0&0&-&0&+&+&-&0&+&0&0&0&0&-&+\\
0&+&0&+&+&+&0&-&0&0&+&0&-&+&-&0&0&0&0\\
0&+&+&0&0&+&+&0&-&0&-&+&0&0&+&-&0&0&0\\
0&0&+&+&+&0&+&0&0&-&0&-&+&-&0&+&0&0&0\\
+&0&0&0&+&0&-&+&-&0&0&-&-&0&+&0&0&0&+\\
+&0&0&0&-&+&0&0&+&-&-&0&-&0&0&+&+&0&0\\
+&0&0&0&0&-&+&-&0&+&-&-&0&+&0&0&0&+&0\\
+&+&-&0&0&0&0&+&0&-&0&0&+&0&-&-&0&+&0\\
+&0&+&-&0&0&0&-&+&0&+&0&0&-&0&-&0&0&+\\
+&-&0&+&0&0&0&0&-&+&0&+&0&-&-&0&+&0&0\\
+&+&0&-&+&-&0&0&0&0&0&+&0&0&0&+&0&-&-\\
+&-&+&0&0&+&-&0&0&0&0&0&+&+&0&0&-&0&-\\
+&0&-&+&-&0&+&0&0&0&+&0&0&0&+&0&-&-&0
\end{pmatrix}.$$

Take R_1 and D to be the residual and derived parts, respectively, of W_{19}. Define the matrix $|R_1|$ by $|R_1|_{ij} = |R_{1_{ij}}|$. Then $|R_1|$ is the incidence matrix of a residual BIBD$(10, 18, 9, 5, 4)$, hence $|R_2| = J - |R_1|$ is a BIBD with the same parameters. Moreover, $|R_2|$ is residual since $|R_2|$ together with $|D|$ also forms a symmetric design. We therefore seek a signing of $|R_2|$ over $\{-1, 1\}$. This search was conducted via Maple, and the following signing was produced.

$$R_2 = \begin{pmatrix}
+ & + & + & + & + & + & + & + & + & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & - & - & 0 & + & 0 & 0 & 0 & + & - & + & + & 0 & + & 0 & 0 & 0 & + \\
- & 0 & - & 0 & 0 & + & + & 0 & 0 & + & - & + & 0 & 0 & + & + & 0 & 0 \\
- & - & 0 & + & 0 & 0 & 0 & + & 0 & + & + & - & + & 0 & 0 & 0 & + & 0 \\
0 & 0 & + & 0 & - & - & 0 & + & 0 & 0 & 0 & + & - & + & + & 0 & + & 0 \\
+ & 0 & 0 & - & 0 & - & 0 & 0 & + & + & 0 & 0 & + & - & + & 0 & 0 & + \\
0 & + & 0 & - & - & 0 & + & 0 & 0 & 0 & + & 0 & + & + & - & + & 0 & 0 \\
0 & + & 0 & 0 & 0 & + & 0 & - & - & 0 & + & 0 & 0 & 0 & + & - & + & + \\
0 & 0 & + & + & 0 & 0 & - & 0 & - & 0 & 0 & + & + & 0 & 0 & + & - & + \\
+ & 0 & 0 & 0 & + & 0 & - & - & 0 & + & 0 & 0 & 0 & + & 0 & + & + & -
\end{pmatrix}.$$

Remarkably, R_2 together with D also forms a balanced W$(19, 9)$. The matrices R_1, R_2, and D then satisfy several properties.

12.3. Lemma.

(12.3.a) $R_1R_1^t = R_2R_2^t = I$, $R_1R_2^t = R_2R_1^t$;

(12.3.b) $DD^t = 9I - J$;

(12.3.c) $R_1D^t = R_2D^t = O$;

(12.3.d) $|R_1||R_1|^t = |R_2||R_2|^t = 5I + 4J$, $|R_1||R_2|^t = |R_2||R_1|^t = 5(J - I)$; and

(12.3.e) $|D||D|^t = 5I + 3J$, $|R_1||D|^t = |R_2||D^t| = 4J$.

Proof. Restatement of the facts that R_1, R_2, and D form balanced W$(19, 4)$ weighing matrices. ∎

* * *

12.2. Construction. Having the lemmata of the previous subsection at our disposal, we are ready to present the construction of a new family of balanced weighing matrices. We desire to apply BGWs in the construction of these matrices, so we need an admissible group of symmetries. Take $\mathcal{M} = \{R_1, R_2\}$; then it isn't difficult to see that $-R_2 \mapsto -R_1 \mapsto R_2 \mapsto R_1 \mapsto -R_2$ is an admissible cyclic group of symmetries of order 4 for $\mathcal{M}$—though, this will be derived explicitly below.

Let $n > 1$, and take Ξ to be a BGW$((9^n - 1)/8, 9^{n-1}, 9^{n-1} - 9^{n-2}; C_4)$. We claim that $\Xi \otimes R_1$ is the residual part of a balanced W$([9(9^n-1)/4]+1, 9^n)$. Note there are disjoint $(0,1)$-matrices $\Xi_0, \Xi_1, \Xi_2, \Xi_3$ such that $\Xi = \Xi_0 + g\Xi_1 + g^2\Xi_2 + g^3\Xi_3$ if $C_4 = \{e, g, g^2, g^3\}$. Then $\Xi \otimes R_1 = \Xi_0 \otimes R_1 - \Xi_1 \otimes R_2 - \Xi_2 \otimes R_1 + \Xi_3 \otimes R_2$.

Next, let $\mathscr{S}_{9,n} = \sum_{\alpha \in \mathrm{GF}(9)^*} \alpha A_\alpha$, and define $A_0 = J - \sum_{\alpha \in \mathrm{GF}(9)^*} A_\alpha$. Finally, take $\Theta = \sum_{\alpha \in \mathrm{GF}(9)} A_\alpha \otimes D$. It will be shown that Θ is the derived part of a balanced $W([9(9^n-1)/4]+1, 9^n)$.

We require the following lemma.

12.4. Lemma.

(12.4.a) $(\Xi \otimes R_1)(\Xi \otimes R_1)^t = 9^n I$;

(12.4.b) $\Theta\Theta^* = 9^n I - J$;

(12.4.c) $(\Xi \otimes R_1)\Theta^t = \Theta(\Xi \otimes R_1)^t = O$;

(12.4.d) $|\Xi \otimes R_1||\Xi \otimes R_1|^t = 5 \cdot 9^n I + 4 \cdot 9^n J$;

(12.4.e) $|\Theta||\Theta|^t = 5 \cdot 9^n I + (4 \cdot 9^n - 1)J$; and

(12.4.f) $|\Xi \otimes R_1||\Theta|^t = |\Theta||\Xi \otimes R_1|^t = 4 \cdot 9^n J$.

Proof. By Lemma 12.2 and (12.3.a),

$$
\begin{aligned}
(\Xi \otimes R_1)(\Xi \otimes R_1) &= 9\Xi_0\Xi_0^t \otimes I - \Xi_0\Xi_1^t \otimes R_1R_2^t - 9\Xi_0\Xi_2^t \otimes I + \Xi_0\Xi_3^t \otimes R_1R_2^t \\
&\quad - \Xi_1\Xi_0^t \otimes R_2R_1^t + 9\Xi_1\Xi_1^t \otimes I + \Xi_1\Xi_2^t \otimes R_2R_1^t - 9\Xi_1\Xi_3^t \otimes I \\
&\quad - 9\Xi_2\Xi_0^t \otimes I + \Xi_2\Xi_1^t \otimes R_1R_2^t + 9\Xi_2\Xi_2^t \otimes I - \Xi_2\Xi_3^t \otimes R_1R_2^t \\
&\quad + \Xi_3\Xi_0^t \otimes R_2R_1^t - 9\Xi_3\Xi_1^t \otimes I - \Xi_3\Xi_2^t \otimes R_2R_1^t + 9\Xi_3\Xi_3^t \otimes I \\
&= 9\sum_i (\Xi_i\Xi_i^t - \Xi_i\Xi_{i+2}^t) \otimes I - \sum_i (\Xi_i\Xi_{i+1} - \Xi_i\Xi_{i+3}) \otimes R_1R_2^t \\
&= 9^n I,
\end{aligned}
$$

and (12.4.a) is shown.

Next, by Lemma 12.1 and (12.3.b), and upon indexing the rows of D by elements of GF(9),

$$
\begin{aligned}
\Theta\Theta^t &= \sum_{\alpha,\beta \in \mathrm{GF}(9)} A_\alpha A_\beta^t \otimes r_\alpha r_\beta^t \\
&= \sum_{\alpha \in \mathrm{GF}(9)} A_\alpha A_\alpha^t \otimes r_\alpha r_\alpha^t + \sum_{\alpha \neq \beta} A_\alpha A_\beta^t \otimes r_\alpha r_\beta^t \\
&= 8 \sum_{\alpha \in \mathrm{GF}(9)} A_\alpha A_\alpha^t - \sum_{\alpha \neq \beta} A_\alpha A_\beta^t \\
&= (9^{n-1} - 1)J + 8 \cdot 9^{n-1} I - 9^{n-1}(J - I) \\
&= 9^n I - J,
\end{aligned}
$$

which shows (12.4.b).

By Lemma (12.3.c),

$$
\begin{aligned}
(\Xi \otimes R_1)\Theta^t &= \sum_{\alpha \in \mathrm{GF}(9)} (\Xi_0 A_\alpha^t \otimes R_1 r_\alpha^t - \Xi_1 A_\alpha^t \otimes R_2 r_\alpha^t - \Xi_2 A_\alpha^t \otimes R_2 r_\alpha^t + \Xi_3 A_\alpha^t \otimes R_2 r_\alpha^t) \\
&= O,
\end{aligned}
$$

and (12.4.c) has been shown.

Since $|\Xi \otimes R_1| = (\Xi_0 + \Xi_2) \otimes |R_1| + (\Xi_1 + \Xi_3) \otimes |R_2|$, (12.4.d) is shown similarly to (12.4.a).

(12.4.e) is shown just as (12.4.b) after noting that $|\Theta| = \sum_{\alpha \in \mathrm{GF}(9)} A_\alpha \otimes |r_\alpha|$.

Finally, (12.4.f) is shown precisely as in (12.4.c). ∎

We are now ready to present the main construction.

12.5. Theorem. Given $\Xi \otimes R_1$ and Θ defined above,

$$\text{(12.5.a)} \quad \begin{pmatrix} \mathbf{0} & \Xi \otimes R_1 \\ \mathbf{1} & \Theta \end{pmatrix}$$

is a balanced W$([9(9^n - 1)/4] + 1, 9^n)$.

Proof. By the lemma, $(\Xi \otimes R_1)(\Xi \otimes R_1)^t = 9^n I$, $\Theta\Theta^t = 9^n I - J$, and $(\Xi \otimes R_1)\Theta^t = O$; thus, (12.5.a) is a weighing matrix with the appropriate parameters. It remains to show it is balanced. But the lemma again gives $|\Xi \otimes R_1||\Xi \otimes R_1|^t = 5 \cdot 9^n I + 4 \cdot 9^n J$, $|\Theta||\Theta|^t = 5 \cdot 9^n I + (4 \cdot 9^n - 1)J$, and $|\Xi \otimes R_1|\Theta^t = 4 \cdot 9^n J$. We have then shown that (12.5.a) is balanced, and the proof is complete. ∎

§13. Weighing Matrices and Association Schemes

In Brouwer et al. (1989) it is shown that symmetric designs are equivalent to certain 3-class association schemes. It is a natural question to ask whether or not a balanced weighing matrix could be related to this scheme, particularly an augmentation. This is the goal of this subsection.

* * *

13.1. Adjacency Matrices. Assume the existence of a balanced $\mathrm{W}(v,k)$, say $W = W_0 - W_1$, where W_0 and W_1 are disjoint $(0,1)$-matrices, and define the following matrices where $P = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

$$
\begin{aligned}
A_0 &= I_{4v},\\
A_1 &= I_2 \otimes P \otimes I_v,\\
A_2 &= I_2 \otimes J_2 \otimes (J_v - I_v),\\
A_3 &= \begin{pmatrix} O & I_2 \otimes W_0 + P \otimes W_1 \\ I_2 \otimes W_0^t + P \otimes W_1^t & O \end{pmatrix},\\
A_4 &= \begin{pmatrix} O & I_2 \otimes W_1 + P \otimes W_0 \\ I_2 \otimes W_1^t + P \otimes W_0^t & O \end{pmatrix},\\
A_5 &= \begin{pmatrix} O & J_2 \otimes (J_v - W_0 - W_1) \\ J_2 \otimes (J_v - W_0^t - W_1^t) & O \end{pmatrix}.
\end{aligned}
$$

We claim that $\{A_0, A_1, A_2, A_3, A_4, A_5\}$ form a 5-class symmetric association scheme. Clearly, (7.5.a), (7.5.b), and (7.5.f) are satisfied. It remains to show closure under multiplication.

First, $A_1^2 = (I_2 \otimes P \otimes I_v)^2 = I_2 \otimes P^2 \otimes I_v = I = A_0$. Next, since

$$
\begin{aligned}
[J_2 \otimes (J_v - I_v)]^2 &= 2J_2 \otimes [(v-1)I_v + (v-2)(J_v - I_v)]\\
&= 2(v-1)J_2 \otimes I_v + 2(v-2)J_2 \otimes (J_v - I_v)\\
&= 2(v-1)(I_2 + P) \otimes I_v + 2(v-2)J_2 \otimes (J_v - I_v),
\end{aligned}
$$

it follows that $A_2^2 = 2(v-1)(A_0 + A_1) + 2(v-2)A_2$. By (12.2.b) and (12.2.c), we find

$$\begin{aligned}(I_2 \otimes W_0 + P \otimes W_1)(I_2 \otimes W_0^t + P \otimes W_1^t) &= I_2 \otimes (W_0 W_0^t + W_1 W_1^t) \\ &\quad + P \otimes (W_0 W_1^t + W_1 W_0^t) \\ &= I_2 \otimes [kI_v + \frac{\lambda}{2}(J_v - I_v)] + P \otimes \frac{\lambda}{2}(J_v - I_v) \\ &= kI_{2v} + \frac{\lambda}{2} J_2 \otimes (J_v - I_v),\end{aligned}$$

where $\lambda = k(k-1)/(v-1)$. Therefore, $A_3^3 = A_4^2 = kA_0 + \frac{\lambda}{2}A_2$. Finally,

$$\begin{aligned}J_2^2 \otimes [J_v - W_0 - W_1)(J_v - W_0^t - W_1^t) &= J_2^2 \otimes (J_v^2 - 2J_v(W_0 + W_1) \\ &\quad + W_0 W_0^t + W_1 W_1^t + W_0 W_1^t + W_1 W_0^t] \\ &= J_2 \otimes [2(v-k)I_v + 2(v - 2k + \lambda)(J_v - I_v)],\end{aligned}$$

hence $A_5^2 = 2(v-k)(A_0 + A_1) + 2(v - 2k + \lambda)A_1$. We next show that $A_i A_j \in \langle A_0, \ldots, A_5 \rangle$ whenever $i \neq j$.

Note $(P \otimes I_v)[J_2 \otimes (J_v - I_v)] = J_2 \otimes (J_v - I_v)$ so that $A_1 A_2 = A_2 A_1 = A_2$. Then

$$\begin{aligned}(I_2 \otimes W_0 + P \otimes W_1)(I_2 \otimes W_1^t + P \otimes W_0^t) &= I_2 \otimes (W_0 W_1^t + W_1 W_0^t) + P \otimes (W_0 W_0^t + W_1 W_1^t) \\ &= I_2 \otimes \frac{\lambda}{2}(J_v - I_v) + P \otimes [kI_v + \frac{\lambda}{2}(J_v - I_v)] \\ &= \frac{\lambda}{2} J_2 \otimes (J_v - I_v) + kP \otimes I_v\end{aligned}$$

so that $A_3 A_4 = A_4 A_3 = kA_1 + \frac{\lambda}{2}A_2$. Next, $(P \otimes I_v)(I_2 \otimes W_0 + P \otimes W_1) = I_2 \otimes W_1 + P \otimes W_0$, hence $A_1 A_3 = A_3 A_1 = A_4$; and similary, $A_1 A_4 = A_4 A_1 = A_3$. Then $(P \otimes I_v)[J_2 \otimes (J_v - W_0 - W_1)] = J_2 \otimes (J_v - W_0 - W_1)$ and $A_1 A_5 = A_5 A_1 = A_5$. Now,

$$\begin{aligned}(I_2 \otimes W_0 + P \otimes W_1)[J_2 \otimes (J_v - W_0^t - W_1^t)] &= J_2 \otimes [(W_0 + W_1)(J_v - (W_0 + W_1)^t)] \\ &= (k - \lambda) J_2 \otimes (J_v - I_v)\end{aligned}$$

so that $A_3A_5 = A_5A_3 = (k-\lambda)A_2$. Similarly, $A_4A_5 = A_5A_4 = (k-\lambda)A_2$. Since

$$\begin{aligned}[J_2 \otimes (J_v - I_v)](I_2 \otimes W_0 + P \otimes W_1 &= J_2 \otimes (J_v - I_v)(W_0 + W_1) \\ &= (k-1)J_2 \otimes J_v + J_2 \otimes (J_v - W_0 - W_1),\end{aligned}$$

it follows that $A_2A_3 = A_3A_2 = (k-1)(A_3 + A_4 + A_5) + kA_5$. Similarly, $A_2A_4 = A_4A_2 = (k-1)(A_3 + A_4 + A_5) + kA_5$. Finally,

$$[J_2 \otimes (J_v - I_v)][J_2 \otimes (J_v - W_0 - W_1)] = J_2 \otimes [2(v-k)J_v - 2(J_v - W_0 - W_1)],$$

and $A_2A_5 = A_5A_2 = 2(v-k)(A_3 + A_4 + A_5) - 2A_5$.

We have shown the following result.

13.1. Theorem. If there is a balanced $\mathrm{W}(v,k)$, then there is a 5-class symmetric association scheme.

* * *

13.2. Character Tables. Our work from the previous subsection shows that the third intersection matrix is given by

$$B_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & k-1 & k-1 & k \\ k & 0 & \frac{k(k-1)}{2(v-1)} & 0 & 0 & 0 \\ 0 & k & \frac{k(k-1)}{2(v-1)} & 0 & 0 & 0 \\ 0 & 0 & \frac{k(v-k)}{v-1} & 0 & 0 & 0 \end{pmatrix}.$$

It can be shown that B_3^t has the six distinct eigenvalues $\pm k$, $\pm\sqrt{k}$, and $\pm\sqrt{k(v-k)/(v-1)}$ with corresponding eigenvectors

$$\mathbf{1}_6, \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 0 \\ \frac{1}{\sqrt{k}} \\ -\frac{1}{\sqrt{k}} \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 0 \\ -\frac{1}{\sqrt{k}} \\ \frac{1}{\sqrt{k}} \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ \frac{-1}{v-1} \\ \frac{v-k}{\sqrt{k(v-1)(v-k)}} \\ \sqrt{\frac{v-k}{k(v-1)}} \\ \frac{-k}{\sqrt{k(v-1)(v-k)}} \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ \frac{-1}{v-1} \\ \frac{k-v}{\sqrt{k(v-1)(v-k)}} \\ -\sqrt{\frac{v-k}{k(v-1)}} \\ \frac{k}{\sqrt{k(v-1)(v-k)}} \end{pmatrix}.$$

The valencies of the scheme are $k_0 = k_1 = 1$, $k_2 = 2(v-1)$, $k_3 = k_4 = k$, and $k_5 = 2(v-k)$. Define $\Delta_k = \mathrm{diag}(k_0, \ldots, k_5)$. Then $v_i^t = (\Delta_k u_i)^t$ are the standardized left eigenvectors of B_3^t. The vectors v_i^t form the rows of the first character table P.

Next, the multiplicities of the scheme are given by $m_i = 4v/\langle u_i, v_i\rangle$ and evaluate to $1, 1, v, v, v-1$, and $v-1$. Then $m_i u_i$ are the columns of the second character table Q.

Summing up, we have the following result.

13.2. Theorem. The 5-class symmetric association scheme of Theorem 13.1 has the character tables

$$P = \begin{array}{c} \\ E_0 \\ E_1 \\ E_2 \\ E_3 \\ E_4 \\ E_5 \end{array} \begin{array}{c} \begin{array}{cccccc} A_0 & A_1 & A_2 & A_3 & A_4 & A_5 \end{array} \\ \begin{pmatrix} 1 & 1 & 2(v-1) & k & k & 2(v-k) \\ 1 & -1 & 0 & \sqrt{k} & -\sqrt{k} & 0 \\ 1 & -1 & 0 & -\sqrt{k} & \sqrt{k} & 0 \\ 1 & 1 & 2(v-1) & -k & -k & 2(k-v) \\ 1 & 1 & -2 & -\sqrt{\frac{k(v-k)}{v-1}} & -\sqrt{\frac{k(v-k)}{v-1}} & 2\sqrt{\frac{k(v-k)}{v-1}} \\ 1 & 1 & -2 & \sqrt{\frac{k(v-k)}{v-1}} & \sqrt{\frac{k(v-k)}{v-1}} & -2\sqrt{\frac{k(v-k)}{v-1}} \end{pmatrix} \end{array},$$

$$Q = \begin{array}{c} \\ A_0 \\ A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \end{array} \begin{array}{c} \begin{array}{cccccc} E_0 & E_1 & E_2 & E_3 & E_4 & E_5 \end{array} \\ \begin{pmatrix} 1 & v & v & 1 & v-1 & v-1 \\ 1 & -v & -v & 1 & v-1 & v-1 \\ 1 & 0 & 0 & 1 & -1 & -1 \\ 1 & \frac{v}{\sqrt{k}} & -\frac{v}{\sqrt{k}} & -1 & -\sqrt{\frac{(v-1)(v-k)}{k}} & \sqrt{\frac{(v-1)(v-k)}{k}} \\ 1 & -\frac{v}{\sqrt{k}} & \frac{v}{\sqrt{k}} & -1 & -\sqrt{\frac{(v-1)(v-k)}{k}} & \sqrt{\frac{(v-1)(v-k)}{k}} \\ 1 & 0 & 0 & -1 & \sqrt{\frac{k(v-1)}{v-k}} & -\sqrt{\frac{k(v-1)}{v-k}} \end{pmatrix} \end{array}.$$

Interestingly, the converse holds as well.

13.3. Theorem. If there is a 5-class symmetric association scheme with the character tables given in the statement of Theorem 13.2, then there is a balanced $\mathrm{W}(v,k)$.

Proof. Let $\tilde{A}_0, \ldots, \tilde{A}_5$ be the adjacency matrices of the scheme. Then $\tilde{A}_1 + \tilde{A}_2$ has eigenvalues $2v-1$ and -1 with multiplicities 2 and $4v-2$, respectively. It follows (see note 21) that $\tilde{A}_1 + \tilde{A}_2 \sim I_2 \otimes A(K_{2v})$. By the eigenvalues of $\tilde{A}_1$, it is the adjacency matrix of $2v$ disjoint 2-cliques, hence $\tilde{A}_1 \sim I_2 \otimes P \otimes I_v$ and $\tilde{A}_2 \sim I_2 \otimes J_2 \otimes (J_v - I_v)$.

It follows that

$$A_3 = \begin{pmatrix} O & O & X_1 & X_2 \\ O & O & X_3 & X_4 \\ X_1^t & X_3^t & O & O \\ X_2^t & X_4^t & O & O \end{pmatrix} \text{ and } A_4 = \begin{pmatrix} O & O & Y_1 & Y_2 \\ O & O & Y_3 & Y_4 \\ Y_1^t & Y_3^t & O & O \\ Y_2^t & Y_4^t & O & O \end{pmatrix}.$$

It can be shown (see Bannai and Ito, 1984, Theorem 3.6.2, for example) that the eigenvalues of the scheme imply that $A_1 A_3 = A_4$ so that

$$\begin{pmatrix} O & O & X_3 & X_4 \\ O & O & X_1 & X_2 \\ X_2^t & X_4^t & O & O \\ X_1^t & X_3^t & O & O \end{pmatrix} = \begin{pmatrix} O & O & Y_1 & Y_2 \\ O & O & Y_3 & Y_4 \\ Y_1^t & Y_3^t & O & O \\ Y_2^t & Y_4^t & O & O \end{pmatrix}.$$

Therefore, there are $(0, 1)$-matrices W_0 and W_1 such that

$$A_3 = \begin{pmatrix} O & O & W_0 & W_1 \\ O & O & W_1 & W_0 \\ W_0^t & W_1^t & O & O \\ W_1^t & W_0^t & O & O \end{pmatrix} \text{ and } A_4 = \begin{pmatrix} O & O & W_1 & W_0 \\ O & O & W_0 & W_1 \\ W_1^t & W_0^t & O & O \\ W_0^t & W_1^t & O & O \end{pmatrix}.$$

Appealing to the character tables again, it can be shown that

$$\begin{aligned} A_3^2 &= kA_0 + \frac{k(k-1)}{2(v-1)}A_2, \\ A_3A_4 = A_4A_3 &= kA_1 + \frac{k(k-1)}{2(v-1)}A_2, \text{ and} \\ A_4^2 &= kA_0 + \frac{k(k-1)}{2(v-1)}A_2. \end{aligned}$$

Therefore, $(A_3-A_4)^2 = 2k(A_0-A_1)$ and $(A_3+A_4)^2 = 2k(A_0+A_1)+\frac{2k(k-1)}{v-1}A_2$, from which it follows that

$$\begin{aligned} &(W_0 - W_1)(W_0 - W_1)^t = kI, \text{ and} \\ &(W_0 + W_1)(W_0 + W_1)^t = kI + \lambda(J - I), \end{aligned}$$

where $\lambda = k(k-1)/(v-1)$.

We then have that $W_0 - W_1$ is the required matrix. ∎

In light of the equivalence, we make the following definition.

13.4. Definition. A symmetric 5-class association scheme is a *weighing scheme* if it has the character tables given in Theorem 13.2.

Notes

33. Seberry (2017), Seberry and Yamada (1992), and Wallis et al. (1972) all contain a wealth of constructions for weighing matrices and orthogonal designs using the Kronecker product.

34. Such a decomposition of the block set is called a *parallelism*. Beth et al. (1999) studies partitions of the blocks of an incidence structure in great detail.

35. The author and Prof. Kharaghani have tried several different groups acting of the residual part of the $\mathrm{BGW}(15, 7, 3; C_3)$ for which the derived part of the design can be embedded into a larger BGW. So far, we have been unsuccessful.

6

A Unified Construction of Weighing Matrices

In this final chapter of results, we present a general method to construct certain configurations using classical parameter BGW matrices and the generalized simplex codes. This method is similar to that given by Rajkundlia (1983) and Ionin (2001), but it can be seen that it is much simpler to apply than the recursive methods of the aforementioned seminal articles. Following the presentation of this construction technique, we find an equivalence between arbitrary BGW matrices over a finite abelian group and certain commutative association schemes. This result generalizes that obtained over the course of the previous chapter.

§14. A General Method

In this section, the general method intimated above is derived and used in the construction of weighing matrices and symmetric designs. Resulting parameters of configurations so constructible are then tabulated.

* * *

14.1. A First Application: Weighing matrices. It is a peculiarity of the constuction that the application of the method to weighing matrices is predicated upon the weight of the matrix being a prime power. Indeed, as in the previous chapter, the generalized simplex codes are applied to the derived part of the matrix by substituting the rows of the derived part for the letters of the code. The simplex code, as the reader may remember, has a prime power number of letters.

To begin, let $W = \left(\begin{smallmatrix} \mathbf{0} & R \\ \mathbf{1} & D \end{smallmatrix}\right)$ be a W(v, q) weighing matrix in normal form, where q is some prime power. Then it is easy to see that $RR^t = kI$ and $DD^t = kI - J$. We say that W is the *seed matrix* of the construction.

Let $\mathscr{S}_{q,n} = \sum_{\alpha \in \mathrm{GF}(q)^*} \alpha A_\alpha$, and define $A_0 = J - \sum_{\alpha \in \mathrm{GF}(q)^*} A_\alpha$. Index the rows of D by the elements of GF(q), and take $\mathcal{D} = \sum_{\alpha \in \mathrm{GF}(q)} A_\alpha \otimes r_\alpha$. Next, by our previous work, there is a W$((q^n - 1)/(q-1), q^{n-1})$, say H, for every $n > 1$. We define $\mathcal{R} = H \otimes R$.

We claim that $\mathcal{W} = \left(\begin{smallmatrix} \mathbf{0} & \mathcal{R} \\ \mathbf{1} & \mathcal{D} \end{smallmatrix}\right)$ is again a weighing matrix. Indeed, $\mathcal{R}\mathcal{R}^t = (H \otimes R)(H \otimes R)^t = HH^t \otimes RR^t = q^n I$. Further, by Lemma 12.1,

$$\begin{aligned}
\mathcal{D}\mathcal{D}^t &= \left(\sum_\alpha A_\alpha \otimes r_\alpha\right)\left(\sum_\alpha A_\alpha \otimes r_\alpha\right) \\
&= \sum_\alpha A_\alpha A_\alpha^t \otimes r_\alpha r_\alpha^t + \sum_{\alpha \neq \beta} A_\alpha A_\beta^t \otimes r_\alpha r_\beta^t \\
&= (q-1)\sum_\alpha A_\alpha A_\alpha^t - \sum_{\alpha \neq \beta} A_\alpha A_\beta^t \\
&= (q-1)\left(\frac{q^{n-1}-1}{q-1} J + q^{n-1} I\right) - q^{n-1}(J - I) \\
&= q^n I - J.
\end{aligned}$$

Finally,

$$\begin{aligned}\mathcal{R}\mathcal{D}^t &= (H \otimes R)\left(\sum_\alpha A_\alpha \otimes r_\alpha\right)^t \\ &= \sum_\alpha HA_\alpha^t \otimes Rr_\alpha^t \\ &= \sum_\alpha HA_\alpha^t \otimes O \\ &= O.\end{aligned}$$

It follows that $\mathcal{W}$ is a weighing matrix. We record this result below.

14.1. Theorem. If there exists a $\mathrm{W}(v, q)$ weighing matrix of prime power weight, then there is a weighing matrix with parameters

$$\left(\frac{(v-1)(q^n-1)}{q-1} + 1, q^n\right). \tag{14.1.a}$$

14.2. Example. Take as a seed matrix the $\mathrm{W}(8, 5)$ shown below

$$\begin{pmatrix} 0 & + & 0 & 0 & - & - & + & + \\ 0 & 0 & + & 0 & - & + & - & + \\ 0 & 0 & 0 & + & - & + & + & - \\ + & + & + & + & + & 0 & 0 & 0 \\ + & + & - & - & 0 & + & 0 & 0 \\ + & - & + & - & 0 & 0 & + & 0 \\ + & - & - & + & 0 & 0 & 0 & + \\ + & 0 & 0 & 0 & - & - & - & - \end{pmatrix}. \tag{14.2.a}$$

Applying the construction, we find a $\mathrm{W}(43, 25)$

$$
\left(\begin{array}{*{43}{c}}
0&0&0&0&0&0&0&0&+&0&0&-&-&+&+&+&0&0&-&-&+&+&+&0&0&-&-&+&+&+&0&0&-&-&+&+&+&0&0&-&-&+&+ \\
0&0&0&0&0&0&0&0&0&+&0&-&+&-&+&0&+&0&-&+&-&+&0&+&0&-&+&-&+&0&+&0&-&+&-&+&0&+&0&-&+&-&+ \\
0&0&0&0&0&0&0&0&0&0&+&-&+&+&-&0&0&+&-&+&+&-&0&0&+&-&+&+&-&0&0&+&-&+&+&-&0&0&+&-&+&+&- \\
0&+&0&0&-&-&+&+&0&0&0&0&0&0&0&-&0&0&+&+&-&-&+&0&0&-&-&+&+&-&0&0&+&+&-&-&+&0&0&-&-&+&+ \\
0&0&+&0&-&+&-&+&0&0&0&0&0&0&0&0&-&0&+&-&+&-&0&+&0&-&+&-&+&0&-&0&+&-&+&-&0&+&0&-&+&-&+ \\
0&0&0&+&-&+&+&-&0&0&0&0&0&0&0&0&0&-&+&-&-&+&0&0&+&-&+&+&-&0&0&-&+&-&-&+&0&0&+&-&+&+&- \\
0&+&0&0&-&-&+&+&-&0&0&+&+&-&-&0&0&0&0&0&0&0&-&0&0&+&+&-&-&+&0&0&-&-&+&+&+&0&0&-&-&+&+ \\
0&0&+&0&-&+&-&+&0&-&0&+&-&+&-&0&0&0&0&0&0&0&0&-&0&+&-&+&-&0&+&0&-&+&-&+&0&+&0&-&+&-&+ \\
0&0&0&+&-&+&+&-&0&0&-&+&-&-&+&0&0&0&0&0&0&0&0&0&-&+&-&-&+&0&0&+&-&+&+&-&0&0&+&-&+&+&- \\
0&+&0&0&-&-&+&+&+&0&0&-&-&+&+&-&0&0&+&+&-&-&0&0&0&0&0&0&0&+&0&0&-&-&+&+&-&0&0&+&+&-&- \\
0&0&+&0&-&+&-&+&0&+&0&-&+&-&+&0&-&0&+&-&+&-&0&0&0&0&0&0&0&0&+&0&-&+&-&+&0&-&0&+&-&+&- \\
0&0&0&+&-&+&+&-&0&0&+&-&+&+&-&0&0&-&+&-&-&+&0&0&0&0&0&0&0&0&0&+&-&+&+&-&0&0&-&+&-&-&+ \\
0&+&0&0&-&-&+&+&-&0&0&+&+&-&-&+&0&0&-&-&+&+&+&0&0&-&-&+&+&0&0&0&0&0&0&0&-&0&0&+&+&-&- \\
0&0&+&0&-&+&-&+&0&-&0&+&-&+&-&0&+&0&-&+&-&+&0&+&0&-&+&-&+&0&0&0&0&0&0&0&0&-&0&+&-&+&- \\
0&0&0&+&-&+&+&-&0&0&-&+&-&-&+&0&0&+&-&+&+&-&0&0&+&-&+&+&-&0&0&0&0&0&0&0&0&0&-&+&-&-&+ \\
0&+&0&0&-&-&+&+&+&0&0&-&-&+&+&+&0&0&-&-&+&+&-&0&0&+&+&-&-&-&0&0&+&+&-&-&0&0&0&0&0&0&0 \\
0&0&+&0&-&+&-&+&0&+&0&-&+&-&+&0&+&0&-&+&-&+&0&-&0&+&-&+&-&0&-&0&+&-&+&-&0&0&0&0&0&0&0 \\
0&0&0&+&-&+&+&-&0&0&+&-&+&+&-&0&0&+&-&+&+&-&0&0&-&+&-&-&+&0&0&-&+&-&-&+&0&0&0&0&0&0&0 \\
+&+&-&-&0&+&0&0&+&-&-&0&+&0&0&-&+&-&0&0&+&0&0&0&0&-&-&-&-&+&+&+&+&0&0&0&-&-&+&0&0&0&+ \\
+&-&+&-&0&0&+&0&+&-&-&0&+&0&0&0&0&0&-&-&-&-&+&+&+&+&0&0&0&-&-&+&0&0&0&+&-&+&-&0&0&+&0 \\
+&-&-&+&0&0&0&+&+&-&-&0&+&0&0&+&+&+&+&0&0&0&-&-&+&0&0&0&+&-&+&-&0&0&+&0&0&0&0&-&-&-&- \\
+&0&0&0&-&-&-&-&+&-&-&0&+&0&0&-&-&+&0&0&0&+&-&+&-&0&0&+&0&0&0&0&-&-&-&-&+&+&+&+&0&0&0 \\
+&+&+&+&+&0&0&0&+&-&-&0&+&0&0&+&-&-&0&+&0&0&+&-&-&0&+&0&0&+&-&-&0&+&0&0&+&-&-&0&+&0&0 \\
+&+&-&-&0&+&0&0&-&+&-&0&0&+&0&0&0&0&-&-&-&-&-&-&+&0&0&0&+&+&-&-&0&+&0&0&+&+&+&+&0&0&0 \\
+&-&+&-&0&0&+&0&-&+&-&0&0&+&0&-&-&+&0&0&0&+&+&-&-&0&+&0&0&+&+&+&+&0&0&0&0&0&0&-&-&-&- \\
+&-&-&+&0&0&0&+&-&+&-&0&0&+&0&+&-&-&0&+&0&0&+&+&+&+&0&0&0&0&0&0&-&-&-&-&-&-&+&0&0&0&+ \\
+&0&0&0&-&-&-&-&-&+&-&0&0&+&0&+&+&+&+&0&0&0&0&0&0&-&-&-&-&-&-&+&0&0&0&+&+&-&-&0&+&0&0 \\
+&+&+&+&+&0&0&0&-&+&-&0&0&+&0&-&+&-&0&0&+&0&-&+&-&0&0&+&0&-&+&-&0&0&+&0&-&+&-&0&0&+&0 \\
+&+&-&-&0&+&0&0&-&-&+&0&0&0&+&+&+&+&+&0&0&0&+&-&-&0&+&0&0&0&0&0&-&-&-&-&-&+&-&0&0&+&0 \\
+&-&+&-&0&0&+&0&-&-&+&0&0&0&+&+&-&-&0&+&0&0&0&0&0&-&-&-&-&-&+&-&0&0&+&0&+&+&+&+&0&0&0 \\
+&-&-&+&0&0&0&+&-&-&+&0&0&0&+&0&0&0&-&-&-&-&-&+&-&0&0&+&0&+&+&+&+&0&0&0&+&-&-&0&+&0&0 \\
+&0&0&0&-&-&-&-&-&-&+&0&0&0&+&-&+&-&0&0&+&0&+&+&+&+&0&0&0&+&-&-&0&+&0&0&0&0&0&-&-&-&- \\
+&+&+&+&+&0&0&0&-&-&+&0&0&0&+&-&-&+&0&0&0&+&-&-&+&0&0&0&+&-&-&+&0&0&0&+&-&-&+&0&0&0&+ \\
+&+&-&-&0&+&0&0&0&0&0&-&-&-&-&-&-&+&0&0&0&+&+&+&+&+&0&0&0&-&+&-&0&0&+&0&+&-&-&0&+&0&0 \\
+&-&+&-&0&0&+&0&0&0&0&-&-&-&-&+&+&+&+&0&0&0&-&+&-&0&0&+&0&+&-&-&0&+&0&0&-&-&+&0&0&0&+ \\
+&-&-&+&0&0&0&+&0&0&0&-&-&-&-&-&+&-&0&0&+&0&+&-&-&0&+&0&0&-&-&+&0&0&0&+&+&+&+&+&0&0&0 \\
+&0&0&0&-&-&-&-&0&0&0&-&-&-&-&+&-&-&0&+&0&0&-&-&+&0&0&0&+&+&+&+&+&0&0&0&-&+&-&0&0&+&0 \\
+&+&+&+&+&0&0&0&0&0&0&-&-&-&-&0&0&0&-&-&-&-&0&0&0&-&-&-&-&0&0&0&-&-&-&-&0&0&0&-&-&-&- \\
+&+&-&-&0&+&0&0&+&+&+&+&0&0&0&+&-&-&0&+&0&0&-&+&-&0&0&+&0&-&-&+&0&0&0&+&0&0&0&-&-&-&- \\
+&-&+&-&0&0&+&0&+&+&+&+&0&0&0&-&+&-&0&0&+&0&-&-&+&0&0&0&+&0&0&0&-&-&-&-&+&-&-&0&+&0&0 \\
+&-&-&+&0&0&0&+&+&+&+&+&0&0&0&-&-&+&0&0&0&+&0&0&0&-&-&-&-&+&-&-&0&+&0&0&-&+&-&0&0&+&0 \\
+&0&0&0&-&-&-&-&+&+&+&+&0&0&0&0&0&0&-&-&-&-&+&-&-&0&+&0&0&-&+&-&0&0&+&0&-&-&+&0&0&0&+ \\
+&+&+&+&+&0&0&0&+&+&+&+&0&0&0&+&+&+&+&0&0&0&+&+&+&+&0&0&0&+&+&+&+&0&0&0&+&+&+&+&0&0&0
\end{array}\right). \tag{14.2.b}
$$

Evidently, this resolves the question of existence of a $\mathrm{W}(43, 25)$ given in Part V of Colbourn and Dinitz (2007).

To further evince the utility of the method, we include a table of constructible parameters given a seed weighing matrix known to exist.

Table 6.1: Small parameter consequential order/weight pairs.

Seed (v, k)	*Succident* (v', k')	*Seed* (v, k)	*Succident* (v', k')
$(6, 5)^{\ddagger}$:	$(31, 25)$‡, $(156, 125)$‡, $(781, 625)$‡	$(16, 3)$:	$(69, 9)$, $(196, 27)$, $(601, 81)$
$(8, 5)$:	$(43, 25)^{\dagger}$, $(218, 125)$	$(16, 5)$:	$(91, 25)$, $(466, 125)$
$(8, 7)^{\ddagger}$:	$(57, 49)^{\ddagger}$, $(400, 343)^{\ddagger}$	$(16, 7)$:	$(121, 49)$, $(856, 343)$
$(10, 5)$:	$(55, 25)$, $(280, 125)$	$(16, 9)$:	$(151, 81)$
$(10, 9)^{\ddagger}$:	$(91, 81)^{\ddagger}$, $(820, 729)^{\ddagger}$	$(16, 11)$:	$(181, 121)^{\dagger}$
$(12, 5)$:	$(67, 25)$, $(342, 125)$	$(16, 13)$:	$(211, 169)$
$(12, 7)$:	$(89, 49)^{\dagger}$, $(628, 343)$	$(18, 13)$:	$(239, 169)$

Continuation of Table 6.1.

Seed (v, k)	Succident (v', k')	*Seed* (v, k)	Succident (v', k')
$(12, 9)$:	$(111, 81)^{\dagger}$	$(19, 9)^{\ddagger}$:	$(181, 81)^{*}$
$(13, 9)^{\ddagger}$:	$(121, 81)$	$(20, 7)$:	$(153, 49)$
$(14, 9)$:	$(131, 81)$	$(20, 13)$:	$(267, 169)^{\dagger}$
$(14, 13)^{\ddagger}$:	$(183, 169)^{\ddagger}$		

* Note that the $\mathrm{W}(181, 81)$ constructible from the balanced seed $\mathrm{W}(19, 9)$ can be made to be balanced as shown in the previous chapter. It is not, however, a consequence of the construction of this chapter that the succident matrix is balanced.

† Denotes previously unknown order weight pairs.

‡ Denotes a balanced weighing matrix.

* * *

14.2. A Second Application: Block designs. The construction is perfectly amenable to certain symmetric designs. For precisely the same reasoning given in the previous subsection, we require that the design have a prime power block size. Furthermore, we require that the parameters of the residual of the design be invariant under complementation. Explicitly, if $A = \left(\begin{smallmatrix} \mathbf{0} & R \\ \mathbf{1} & D \end{smallmatrix}\right)$ is the incidence matrix of the given design, then $J - R$ must have the same parameters as R.

As shown in Hall (1986), there is a $\mathrm{W}(2q + 2, 2q + 2)$ if and only if there is a symmetric $\mathrm{BIBD}(2q + 1, q, (q - 1)/2)$, called a *Hadamard design* [36]). Accordingly, the residual of this design is a $\mathrm{BIBD}(q + 1, 2q, q, (q + 1)/2, (q - 1)/2)$, the parameters of which are invariant under complementation. Also, the derived design is a $\mathrm{BIBD}(q, 2q, q - 1, (q - 1)/2, (q - 3)/2)$.

Let $H = H_0 - H_1$ be a balanced $\mathrm{W}((q^n - 1)/(q - 1), q^{n-1})$, and let $\{A_\alpha\}_{\alpha \in \mathrm{GF}(q)}$ be as above. If $A = \left(\begin{smallmatrix} \mathbf{0} & R \\ \mathbf{1} & D \end{smallmatrix}\right)$ is a Hadamard design with parameters $(2q + 1, q, (q - 1)/2)$, then we form $\mathcal{R} = H_0 \otimes R + H_1 \otimes (J - R)$. Indexing the rows of D by the elements of GF(q), we then form $\mathcal{D} = \sum_{\alpha \in \mathrm{GF}(q)} A_\alpha \otimes r_\alpha$.

We claim that $\mathcal{A} = \left(\begin{smallmatrix} \mathbf{0} & \mathcal{R} \\ \mathbf{1} & \mathcal{D} \end{smallmatrix}\right)$ is a symmetric design. To show this, we proceed as before. Using Lemma 12.2, we find

$$\begin{aligned}
\mathcal{R}\mathcal{R}^t &= [H_0 \otimes R + H_1 \otimes (J_{q+1,2q} - R)][H_0 \otimes R + H_1 \otimes (J_{q+1,2q} - R)]^t \\
&= (H_0 H_0^t + H_1 H_1^t) \otimes \left(\frac{q+1}{2} I_{q+1} + \frac{q-1}{2} J_{q+1}\right) \\
&\qquad\qquad + \frac{q+1}{2}(H_0 H_1^t + H_1 H_0^t) \otimes (J_{q+1} - I_{q+1}) \\
&= \frac{q^{n-2}}{4}[(q+1) I_{\frac{q^{n-1}}{q-1}} + (q-1) J_{\frac{q^{n-1}}{q-1}}] \otimes [(q+1) I_{q+1} + (q-1) J_{q+1}] \\
&\qquad\qquad + \frac{q^{n-2}(q^2-1)}{4}(J_{\frac{q^{n-1}}{q-1}} - I_{\frac{q^{n-1}}{q-1}}) \otimes (J_{q+1} - I_{q+1}) \\
&= \frac{q^{n-2}}{4}\left[2q(q+1) I_{\frac{(q+1)(q^n-1)}{q-1}} + 2q(q-1) J_{\frac{(q+1)(q^n-1)}{q-1}}\right] \\
&= q^n I_{\frac{(q+1)(q^n-1)}{q-1}} + \frac{q^n - q^{n-1}}{2}(J_{\frac{(q+1)(q^n-1)}{q-1}} - I_{\frac{(q+1)(q^n-1)}{q-1}}),
\end{aligned}$$

whence $\mathcal{R}$ is a quasi-residual BIBD with parameters

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

Next, by Lemma 12.1

$$\begin{aligned}
\mathcal{D}\mathcal{D}^t &= \left(\sum_\alpha A_\alpha \otimes r_\alpha\right)\left(\sum_\alpha A_\alpha \otimes r_\alpha\right)^t \\
&= \sum_\alpha A_\alpha A_\alpha^t \otimes r_\alpha r_\alpha^t + \sum_{\alpha \neq \beta} A_\alpha A_\beta^t \otimes r_\alpha r_\beta^t \\
&= (q-1)\sum_\alpha A_\alpha A_\alpha^t + \frac{q-3}{2}\sum_{\alpha \neq \beta} A_\alpha A_\beta^t \\
&= (q-1)\left(\frac{q^{n-1}-1}{q-1} J - q^{n-1} I\right) + \frac{q^{n-1}(q-3)}{2}(J - I) \\
&= (q^n - 1) I + \frac{q^n - q^{n-1} - 2}{2}(J - I),
\end{aligned}$$

and $\mathcal{D}$ is a quasi-derived BIBD with parameters

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

Finally,

$$\begin{aligned}
\mathcal{R}\mathcal{D}^t &= [H_0 \otimes R + H_1 \otimes (J-R)]\left(\sum_\alpha A_\alpha \otimes r_\alpha\right)^t \\
&= \sum_\alpha H_0 A_\alpha^t \otimes R r_\alpha^t + \sum_\alpha H_1 A_\alpha^t \otimes (J-R) r_\alpha^t \\
&= \frac{q-1}{2}\sum_\alpha H_0 A_\alpha^t \otimes \mathbf{1} + \frac{q-1}{2}\sum_\alpha H_1 A_\alpha^t \otimes \mathbf{1} \\
&= \frac{q-1}{2}(H_0+H_1)\sum_\alpha A_\alpha^t \otimes \mathbf{1} \\
&= \frac{q-1}{2}(H_0+H_1)J \\
&= \frac{q^n-q^{n-1}}{2}J.
\end{aligned}$$

We have shown that $\mathcal{A} = \left(\begin{smallmatrix} \mathbf{0} & \mathcal{R} \\ \mathbf{1} & \mathcal{D} \end{smallmatrix}\right)$ is a symmetric BIBD. We record this result below.

14.3. Theorem. If there is a symmetric BIBD$(2q+1, q, (q-1)/2)$, then there is a symmetric BIBD with parameters

$$\text{(14.3.a)} \quad \left(\frac{2q^{n+1}-2q}{q-1}+1, q^n, \frac{q^n-q^{n-1}}{2}\right).$$

14.4. Example. Consider the Hadamard design

$$\text{(14.4.a)} \quad \begin{pmatrix}
0&1&1&0&1&0&0\\
0&0&1&1&0&1&0\\
0&0&0&1&1&0&1\\
1&0&0&0&1&1&0\\
0&1&0&0&0&1&1\\
1&0&1&0&0&0&1\\
1&1&0&1&0&0&0
\end{pmatrix}$$

with parameters $(7,3,1)$. The result of the first iteration of the construction is the symmetric BIBD$(25, 9, 3)$

$$\tag{14.4.b} \begin{pmatrix}
0&0&0&0&0&0&0&1&1&0&1&0&0&1&1&0&1&0&0&1&1&0&1&0&0\\
0&0&0&0&0&0&0&0&1&1&0&1&0&0&1&1&0&1&0&0&1&1&0&1&0\\
0&0&0&0&0&0&0&0&0&1&1&0&1&0&0&1&1&0&1&0&0&1&1&0&1\\
0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&1&1&0&0&0&1&1\\
0&0&0&1&0&1&1&0&0&0&0&0&0&0&0&1&0&1&1&1&1&0&1&0&0\\
0&1&0&0&1&0&1&0&0&0&0&0&0&1&0&0&1&0&1&0&1&1&0&1&0\\
0&1&1&0&0&1&0&0&0&0&0&0&0&1&1&0&0&1&0&0&0&1&1&0&1\\
0&0&1&1&1&0&0&0&0&0&0&0&0&0&1&1&1&0&0&1&0&0&0&1&1\\
0&0&0&1&0&1&1&1&1&0&1&0&0&0&0&0&0&0&0&0&0&1&0&1&1\\
0&1&0&0&1&0&1&0&1&1&0&1&0&0&0&0&0&0&0&1&0&0&1&0&1\\
0&1&1&0&0&1&0&0&0&1&1&0&1&0&0&0&0&0&0&1&1&0&0&1&0\\
0&0&1&1&1&0&0&1&0&0&0&1&1&0&0&0&0&0&0&0&1&1&1&0&0\\
0&0&0&1&0&1&1&0&0&1&0&1&1&1&1&0&1&0&0&0&0&0&0&0&0\\
0&1&0&0&1&0&1&1&0&0&1&0&1&0&1&1&0&1&0&0&0&0&0&0&0\\
0&1&1&0&0&1&0&1&1&0&0&1&0&0&0&1&1&0&1&0&0&0&0&0&0\\
0&0&1&1&1&0&0&0&1&1&1&0&0&1&0&0&0&1&1&0&0&0&0&0&0\\
1&0&1&0&0&0&1&0&1&0&0&0&1&1&0&1&0&0&0&0&0&0&1&1&0\\
1&1&0&1&0&0&0&0&1&0&0&0&1&0&0&0&1&1&0&1&0&1&0&0&0\\
1&0&0&0&1&1&0&0&1&0&0&0&1&0&1&0&0&0&1&0&1&0&0&0&1\\
1&0&1&0&0&0&1&1&0&1&0&0&0&0&0&0&1&1&0&0&1&0&0&0&1\\
1&1&0&1&0&0&0&1&0&1&0&0&0&0&1&0&0&0&1&0&0&0&1&1&0\\
1&0&0&0&1&1&0&1&0&1&0&0&0&1&0&1&0&0&0&1&0&1&0&0&0\\
1&0&1&0&0&0&1&0&0&0&1&1&0&0&1&0&0&0&1&1&0&1&0&0&0\\
1&1&0&1&0&0&0&0&0&0&1&1&0&1&0&1&0&0&0&0&1&0&0&0&1\\
1&0&0&0&1&1&0&0&0&0&1&1&0&0&0&0&1&1&0&0&0&0&1&1&0
\end{pmatrix}.$$

§15. BGW Matrices and Association Schemes

In this section we present perhaps the most striking result of this essay. Here the equivalence between BGW matrices and commutative association schemes is described in detail.

* * *

15.1. Adjacency Matrices. We must first extend Lemma 12.2 to the case of arbitrary BGW matrices. Let $G = \{g_0 = 1, g_1, \dots, g_{n-1}\}$ be an abelian group, and let $W = \sum_{g\in G} gW_g$ be a $\mathrm{BGW}(v, k, \lambda; G)$. We then have the following.

15.1. Lemma.

$$\tag{15.1.a} \sum_{g,h} gh^{-1}W_gW_h^t = \sum_{g,h} h^{-1}gW_h^tW_g = kI + \tfrac{\lambda}{n}\left(\sum_g g\right)(J - I),$$

(15.1.b) $\sum_g W_g W_g^t = \sum_g W_g^t W_g = kI + \frac{\lambda}{n}(J - I)$, and

(15.1.c) $\sum_g W_g W_{gh^{-1}}^t = \sum_g W_{gh^{-1}}^t W_g = \frac{\lambda}{n}(J - I)$ whenever $h \neq 1$.

Proof. Restatement of the fact that $W = \sum_g gW_g$ is a BGW$(v, k, \lambda; G)$. ∎

Let $\{U_g : g \in G\}$ be the usual regular linear representation of G, that is, $U_g = (\delta(g_i^{-1} g g_j))$ where $\delta(h) = 1$ if $h = 1$ and 0 otherwise. Consider the following family of matrices.

$$A_{0,g} = I_2 \otimes U_g \otimes I_v, \text{ for } g \in G,$$

$$A_1 = I_2 \otimes J_n \otimes (J_v - I_v),$$

$$A_{2,g} = \begin{pmatrix} O & \sum_{h \in G}(U_h \otimes W_{gh}) \\ \sum_{h \in G}(U_h \otimes W_{g^{-1}h^{-1}}^t) & O \end{pmatrix}, \text{ for } g \in G, \text{ and}$$

$$A_3 = \begin{pmatrix} O & J_n \otimes (J_v - \sum_{h \in G} W_h) \\ J_n \otimes (J_v - \sum_{h \in G} W_h^t) & O \end{pmatrix}.$$

In showing that $\{A_1, A_3\} \cup \{A_{0,g}, A_{2,g} : g \in G\}$ is an association scheme, we proceed precisely as before. First, $A_1 + A_3 + \sum_{g \in G}(A_{0,g} + A_{2,g}) = J$. Second, $A_{0,g}^t = A_{0,g^{-1}}$, $A_1^t = A_1$, $A_{2,g}^t = A_{2,g^{-1}}$, and $A_3^t = A_3$.

We next show closure under multiplication. We have $A_{0,g}A_{0,h} = A_{0,gh} = A_{0,hg} = A_{0,h}A_{0,g}$. Then $A_{0,g}A_1 = A_1 A_{0,g} = A_1$ and $A_{0,g}A_3 = A_3 A_{0,g} = A_3$. Since $\sum_j (U_{gj} \otimes W_{hj}) = \sum_j (U_j \otimes W_{g^{-1}hj})$, it follows that $A_{0,g}A_{2,h} = A_{2,h}A_{0,g} = A_{2,g^{-1}h}$. As $[J_n \otimes (J_v - I_v)]^2 = n(v-1)\sum_g (U_g \otimes I_v) + n(v -$

$2)J_n \otimes (J_v - I_v)$, we have $A_1^2 = n(v-1)\sum_g A_{0,g} + n(v-2)A_1$. Next,

$$\begin{aligned}[J_n \otimes (J_v - I_v)]\sum_h (U_h \otimes W_{gh}) &= J_n \otimes (J_v - I_v)\sum_h W_h \\ &= (k-1)J_n \otimes J_v + J_n \otimes (J_v - \sum_h W_h),\end{aligned}$$

hence $A_1 A_{2,g} = A_{2,g}A_1 = (k-1)\sum_{g\in G} A_{2,g} + kA_3$. We have

$$\begin{aligned}[J_n \otimes (J_v - I_v)]\left[J_n \otimes (J_v - \sum_h W_h)\right] &= nJ_n \otimes (J_v - I_v)\left(J_v - \sum_h W_h\right) \\ &= n(v-k)J_n \otimes J_v - nJ_n \otimes \left(J_v - \sum_h W_h\right)\end{aligned}$$

so that $A_1 A_3 = A_3 A_1 = n(v-k)\sum_{g\in G} A_{2,g} + n(v-k-1)A_3$. Then

$$\begin{aligned}\sum_h (U_h \otimes W_{gh})\left[J_n \otimes (J_v - \sum_j W_j^t)\right] &= J_n \otimes \left(\sum_h W_h J_v - \sum_{h,j} W_h W_j^t\right) \\ &= (k-\lambda)J_n \otimes (J_v - I_v),\end{aligned}$$

and $A_{2,g}A_3 = A_3 A_{2,g} = (k-\lambda)A_1$. Since

$$\begin{aligned}\left(J_v - \sum_{h\in G} W_h\right)\left(J_v - \sum_{g\in G} W_g^t\right) &= vJ_v - 2kJ_v + kI_v + \lambda(J_v - I_v) \\ &= (v-2k+\lambda)(J_v - I_v) + (v-k)I_v,\end{aligned}$$

one finds that $A_3^2 = n(v-2k+\lambda)A_1 + n(v-k)\sum_{g\in G} A_{0,g}$. Finally, for fixed $g, h \in G$, we note that

$$\sum_{\alpha,\beta}(U_{\alpha\beta} \otimes W_{g\alpha}W_{h^{-1}\beta^{-1}}^t) = \sum_\gamma \left(U_\gamma \otimes \sum_{\alpha\beta=\gamma} W_{g\alpha}W_{h^{-1}\beta^{-1}}^t\right)$$

$$
\begin{aligned}
&= \sum_{\gamma \neq g^{-1}h^{-1}} \left(U_\gamma \otimes \sum_{\alpha\beta=\gamma} W_{g\alpha} W^t_{h^{-1}\beta^{-1}} \right) \\
&\qquad\qquad + U_{g^{-1}h^{-1}} \otimes \sum_\gamma W_\gamma W^t_\gamma \\
&= \sum_{\gamma \neq g^{-1}h^{-1}} \left[U_\gamma \otimes \frac{\lambda}{n}(J_v - I_v) \right] \\
&\qquad\qquad + U_{g^{-1}h^{-1}} \otimes \left[kI_v + \frac{\lambda}{n}(J_v - I_v) \right] \\
&= \frac{\lambda}{n} J_n \otimes (J_v - I_v) + kU_{g^{-1}h^{-1}} \otimes I_v
\end{aligned}
$$

so that $A_{2,g}A_{2,h} = A_{2,h}A_{2,g} = \frac{\lambda}{n}A_1 + kA_{0,g^{-1}h^{-1}}$.

We have shown the following result.

15.2. Theorem. If G is a finite abelian group, and if there is a BGW$(v, k, \lambda; G)$, then there is either a commutative $2n$- or $(2n+1)$-class association scheme predicated upon whether or not $v = k$.

* * *

15.2. Character Tables. As before, we desire to give explicitly the character tables of the scheme. The difference between the schemes arising from an arbitrary BGW vs. a balanced weighing matrix, is that the number of classes is no longer fixed. Therefore, we desire to exhibit a general form for the primitive idempotents of the scheme in terms of the adjacency matrices.

To this end, let $\hat{G} = \{\chi_g : g \in G\}$ be the collection of irreducible characters[37]) of the group G, i.e. the dual group of G. Following Kharaghani and Suda (2021), we make the following definitions for each $g \in G$:

$$
F_{0,g} = \sum_{h \in G} \chi_g(h) A_{0,h}, \qquad \text{and} \qquad F_{2,g} = \sum_{h \in G} \chi_g(h) A_{2,h}.
$$

Using the intersection numbers derived above, and using the generalized orthogonality relation of characters (see Isaacs, 2006, Theorem 2.13), we have the following lemma.

15.3. Lemma.

(15.3.a) $F_{0,g}F_{0,h} = n\delta_{gh}F_{0,g}$,

(15.3.b) $F_{0,g}F_{2,h} = F_{2,h}F_{0,g} = n\delta_{g^{-1}h}F_{2,h}$, and

(15.3.c) $F_{2,g}F_{2,h} = n\lambda\delta_{gh}\delta_{g1}A_1 + nk\delta_{gh}F_{0,g^{-1}}$.

Proof. We have

$$\begin{aligned}
F_{0,g}F_{0,h} &= \sum_{\alpha,\beta} \chi_g(\alpha)\chi_h(\beta)A_{0,\alpha\beta} \\
&= n\sum_{\gamma}\left(\sum_{\alpha\beta=\gamma}\chi_g(\alpha)\chi_h(\beta)\right)A_{0,\gamma} \\
&= n\sum_{\gamma}\left(\sum_{\beta}\chi_g(\beta^{-1}\gamma)\chi_h(\beta)\right)A_{0,\gamma} \\
&= n\delta_{gh}\sum_{\gamma}\chi_g(\gamma)A_{0,\gamma} \\
&= n\delta_{gh}F_{0,g},
\end{aligned}$$

which shows (15.3.a). Next,

$$\begin{aligned}
F_{0,g}F_{2,h} &= \sum_{\alpha,\beta} \chi_g(\alpha)\chi_h(\beta)A_{0,g}A_{2,h} \\
&= n\sum_{\gamma}\left(\sum_{\alpha\beta=\gamma}\chi_{g^{-1}}(\alpha)\chi_h(\beta)\right)A_{2,\gamma} \\
&= n\delta_{g^{-1}h}\sum_{\gamma}\chi_h(\gamma)A_{2,\gamma}
\end{aligned}$$

$$= n\delta_{g^{-1}h}F_{2,h}.$$

Since the scheme is commutative, $F_{2,h}F_{0,g} = F_{0,g}F_{2,h}$, which shows (15.3.b). Finally,

$$\begin{aligned}
F_{2,g}F_{2,h} &= \sum_{\alpha,\beta}\chi_g(\alpha)\chi_h(\beta)\left(\frac{\lambda}{n}A_1 + kA_{0,\alpha^{-1}\beta^{-1}}\right) \\
&= n\sum_{\gamma}\left(\sum_{\alpha\beta=\gamma}\chi_{g^{-1}}(\alpha)\chi_{h^{-1}}(\beta)\right)\left(\frac{\lambda}{n}A_1 + kA_{0,\gamma}\right) \\
&= n\sum_{\gamma}\left(\sum_{\beta}\chi_{g^{-1}}(\beta^{-1}\gamma)\chi_{h^{-1}}(\beta)\right)\left(\frac{\lambda}{n}A_1 + kA_{0,\gamma}\right) \\
&= n\delta_{gh}\sum_{\gamma}\chi_{g^{-1}}(\gamma)\left(\frac{\lambda}{n}A_1 + kA_{0,\gamma}\right) \\
&= n\lambda\delta_{gh}\delta_{g1}A_1 + nk\delta_{gh}F_{0,g^{-1}},
\end{aligned}$$

showing (15.3.c). This completes the proof. ∎

We are now ready to give the idempotents of the scheme. There are two cases two consider, namely, whether or not $v = k$. In the latter case, we have

$$\begin{aligned}
E_0 &= \frac{1}{2nv}(F_{0,0} + F_{2,0} + A_1 + A_3), \\
E_1 &= \frac{1}{2nv}\left(F_{0,0} - F_{2,0} + A_1 - A_3\right), \\
E_{2,1} &= \frac{1}{2nv}\left((v-1)F_{0,0} + \sqrt{\frac{(v-1)(v-k)}{k}}F_{2,0} - A_1 - \sqrt{\frac{k(v-1)}{v-k}}A_3\right), \\
E_{2,2} &= \frac{1}{2nv}\left((v-1)F_{0,0} - \sqrt{\frac{(v-1)(v-k)}{k}}F_{2,0} - A_1 + \sqrt{\frac{k(v-1)}{v-k}}A_3\right), \\
E_{3,g} &= \frac{1}{2nv}\left(vF_{0,g} + \frac{v}{\sqrt{k}}F_{2,g}\right), \text{ for } g \in G/\{1\}, \text{ and} \\
E_{4,g} &= \frac{1}{2nv}\left(vF_{0,g} - \frac{v}{\sqrt{k}}F_{2,g}\right), \text{ for } g \in G/\{1\}.
\end{aligned}$$

In the case that $v = k$, then $A_3 = O$ and we replace $E_{2,1}$ and $E_{2,2}$ with $E_2 = E_{2,1} + E_{2,2}$. The following lemma is immediate.

15.4. Lemma. Let $\mathcal{E} = \{E_0, E_1, E_{2,1}, E_{2,2}, E_{3,g}, E_{4,g} : g \in G/\{1\}\}$. Then:

(15.4.a) $EF = \delta_{EF} E$, for all $E, F \in \mathcal{E}$;

(15.4.b) $I = \sum_{E \in \mathcal{E}} E$; and

(15.4.c) $E^* \in \mathcal{E}$, for each $E \in \mathcal{E}$.

Proof. Straightforward but tedious calculation. ∎

Using these lemmata, we have the following result.

15.5. Theorem. The commutative association scheme given in Theorem 15.2 has the first and second character tables

$$P = \begin{array}{c} \\ E_0 \\ E_1 \\ E_2 \\ E_{3,g} \\ E_{4,g} \end{array} \begin{array}{c} \begin{array}{ccc} A_{0,h} & A_1 & A_{2,h} \end{array} \\ \begin{pmatrix} 1 & n(v-1) & k \\ 1 & n(v-1) & -k \\ -n & 0 & \\ \chi_{g^{-1}}(h) & 0 & \sqrt{k}\chi_{g^{-1}}(h) \\ \chi_{g^{-1}}(h) & 0 & \chi_{g^{-1}}(h) \end{pmatrix} \end{array},$$

$$Q = \begin{array}{c} \\ A_{0,h} \\ A_1 \\ A_{2,h} \end{array} \begin{array}{c} \begin{array}{ccccc} E_0 & E_1 & E_2 & E_{3,g} & E_{4,g} \end{array} \\ \begin{pmatrix} 1 & 1 & 2(v-1) & v\chi_g(h) & v\chi_g(h) \\ 1 & 1 & -2 & 0 & 0 \\ 1 & -1 & 0 & \frac{v}{\sqrt{k}}\chi_g(h) & -\frac{v}{\sqrt{k}}\chi_g(h) \end{pmatrix} \end{array}$$

in the case that $v = k$ and

$$P = \begin{array}{c} \\ E_0 \\ E_1 \\ E_{2,1} \\ E_{2,2} \\ E_{3,g} \\ E_{3,g} \end{array} \begin{array}{c} \begin{array}{cccc} A_{0,h} & A_1 & A_{2,h} & A_3 \end{array} \\ \begin{pmatrix} 1 & n(v-1) & k & n(v-k) \\ 1 & n(v-1) & -k & n(k-v) \\ 1 & -n & \sqrt{\frac{k(v-k)}{v-1}} & -n\sqrt{\frac{k(v-k)}{v-1}} \\ 1 & -n & -\sqrt{\frac{k(v-k)}{v-1}} & n\sqrt{\frac{k(v-k)}{v-1}} \\ -\chi_{g^{-1}}(h) & 0 & \sqrt{k}\chi_{g^{-1}}(h) & 0 \\ \chi_{g^{-1}}(h) & 0 & -\sqrt{k}\chi_{g^{-1}}(h) & 0 \end{pmatrix} \end{array},$$

$$Q = \begin{array}{c} \\ A_{0,h} \\ A_1 \\ A_{2,h} \\ A_3 \end{array} \begin{array}{c} \begin{array}{cccccc} E_0 & E_1 & E_{2,1} & E_{2,2} & E_{3,g} & E_{4,g} \end{array} \\ \begin{pmatrix} 1 & 1 & v-1 & v-1 & v\chi_g(h) & v\chi_g(h) \\ 1 & 1 & -1 & -1 & 0 & 0 \\ 1 & -1 & \sqrt{\frac{(v-1)(v-k)}{v-k}} & -\sqrt{\frac{(v-1)(v-k)}{v-k}} & \frac{v}{\sqrt{k}}\chi_g(h) & -\frac{v}{\sqrt{k}}\chi_g(h) \\ 1 & 1 & -\sqrt{\frac{k(v-1)}{v-k}} & \sqrt{\frac{k(v-1)}{v-k}} & 0 & 0 \end{pmatrix} \end{array}$$

in the case that $v > k$.

As before, the converse also holds.

15.6. Theorem. If there is a commutative scheme with the character tables given in Theorem 15.5, then there is a BGW$(v, k, \lambda; G)$, where G is an abelian group isomorphic to $\{\chi_g\}$.

Proof. The derivation of this fact is the same mutatis mutandis as that for Theorem 13.3 and is, therefore, omitted. ∎

In light of this equivalence, we make the following final definition.

15.7. Definition. The commutaive association schemes with character tables given in Theorem 15.5 are called *generalized weighing schemes*.

Since the largest—indeed, the most important—families of generalized matrices are those over a group which is either cyclic or elementary abelian, it would be benificial to conclude with a brief discussion of the irreducible characters of these groups in an effort to make the preceeding results more concrete.

To this end, recall the irreducible characters of the cyclic group $C_p \simeq \{1, g, \ldots, g^{p-1}\}$ of order p are given by $\chi_{g^i}(g^j) = e^{\frac{2\pi\sqrt{-1}ij}{p}}$. This suffices for the case in which the group is cyclic.

Let p be a prime, and let C_p be as above. If $q = p^n$, then $\mathrm{EA}(q) \simeq \underbrace{C_p \otimes \cdots \otimes C_p}_{n} = \{g^{m_0} \otimes \cdots \otimes g^{m_{n-1}} : 0 \leq m_0, \ldots, m_{n-1} < p\}$. By Theorem 4.21 of Isaacs (2006), it follows that

$$\begin{aligned}
\chi_{g^{m_0} \otimes \cdots \otimes g^{m_{n-1}}}(g^{k_0} \otimes \cdots \otimes g^{k_{n-1}}) &= \prod_i \chi_{g^{m_i}}(g^{k_i}) \\
&= \prod_i e^{\frac{2\pi\sqrt{-1}m_i k_i}{p}} \\
&= e^{\frac{2\pi\sqrt{-1}}{p}\sum_i m_i k_i}.
\end{aligned}$$

This concludes our study of weighing matrices and related configurations.

Notes

36. Let C be the matrix obtained upon deleting the first row and column of a normalized Hadamard matrix of order $4n$. Then $(1/2)(J + C)$ is a symmetric BIBD$(4n-1, 2n-1, n-1)$. See Hall (1986) for a proof of this resut and related discussions.

37. Recall that a linear representation of a group G is a homomorphism $\varrho : G \to \mathrm{GL}(V)$, where V is some linear space. The character of the representation is then $\chi(g) = \mathrm{Tr}(\varrho(g))$, for each $g \in G$. Isaacs (2006) is the classical reference for the character theory of finite groups.

Bibliography

Arasu, K. T., Dillon, J. F., Jungnickel, D., and Pott, A. (1995). The solution of the Waterloo problem. *J. Combin. Theory Ser. A*, 71(2):316–331.

Arasu, K. T., Dillon, J. F., Leung, K. H., and Ma, S. L. (2001). Cyclic relative difference sets with classical parameters. *J. Combin. Theory Ser. A*, 94(1):118–126.

Bannai, E., Bannai, E., Ito, T., and Tanaka, R. (2021). *Algebraic combinatorics*. De Gruyter.

Bannai, E. and Ito, T. (1984). *Algebraic combinatorics. I.* The Benjamin/Cummings Publishing Co., Inc., Menlo Park, CA. Association schemes.

Batten, L. M. (1997). *Combinatorics of finite geometries*. Cambridge University Press, Cambridge, second edition.

Best, D. and Kharaghani, H. (2010). Unbiased complex Hadamard matrices and bases. *Cryptogr. Commun.*, 2(2):199–209.

Best, D., Kharaghani, H., and Ramp, H. (2015). Mutually unbiased weighing matrices. *Des. Codes Cryptogr.*, 76(2):237–256.

Beth, T., Jungnickel, D., and Lenz, H. (1999). *Design theory. Vols. I and II*, volume 69 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition.

Boykin, O. P., Sitharam, M., Tarifi, M., and Wocjan, P. (2005). Real mutually unbiased bases.

Bracken, C., McGuire, G., and Ward, H. (2006). New quasi-symmetric designs constructed using mutually orthogonal Latin squares and Hadamard matrices. *Des. Codes Cryptogr.*, 41(2):195–198.

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

Cameron, P. J. (1994). *Combinatorics: topics, techniques, algorithms*. Cambridge University Press, Cambridge.

Cameron, P. J. (1999). *Permutation groups*, volume 45 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge.

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

Christensen, O. (2016). *An introduction to frames and Riesz bases*. Applied and Numerical Harmonic Analysis. Birkhäuser/Springer, [Cham], second edition.

Colbourn, C. J. and Dinitz, J. H., editors (2007). *Handbook of combinatorial designs*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition.

Davis, P. J. (1979). *Circulant matrices*. A Wiley-Interscience Publication. John Wiley & Sons, New York-Chichester-Brisbane.

de Launey, W. and Flannery, D. (2011). *Algebraic design theory*, volume 175 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI.

de Launey, W. and Sarvate, D. G. (1984). Nonexistence of certain GBRDs. *Ars Combin.*, 18:5–20.

Delsarte, P. (1973). An algebraic approach to the association schemes of coding theory. *Philips Res. Rep. Suppl.*, (10):vi+97.

Delsarte, P., Goethals, J. M., and Seidel, J. J. (1977). Spherical codes and designs. *Geometriae Dedicata*, 6(3):363–388.

Dembowski, P. (1997). *Finite geometries*. Classics in Mathematics. Springer-Verlag, Berlin. Reprint of the 1968 original.

Elliott, J. E. H. and Butson, A. T. (1966). Relative difference sets. *Illinois J. Math.*, 10:517–531.

Fender, K., Kharaghani, H., and Suda, S. (2018). On a class of quaternary complex Hadamard matrices. *Discrete Math.*, 341(2):421–426.

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

Gibbons, P. B. and Mathon, R. A. (1987). Group signings of symmetric balanced incomplete block designs. In *Proceedings of the Singapore conference on combinatorial mathematics and computing (Singapore, 1986)*, volume 23, pages 123–134.

Goethals, J.-M. and Seidel, J. J. (1970). A skew Hadamard matrix of order 36. *J. Austral. Math. Soc.*, 11:343–344.

Hall, Jr., M. (1986). *Combinatorial theory*. Wiley-Interscience Series in Discrete Mathematics. John Wiley & Sons, Inc., New York, second edition. A Wiley-Interscience Publication.

Halmos, P. R. (1982). *A Hilbert space problem book*, volume 17 of *Encyclopedia of Mathematics and its Applications*. Springer-Verlag, New York-Berlin, second edition.

Halmos, P. R. (1998). *Introduction to Hilbert space and the theory of spectral multiplicity*. AMS Chelsea Publishing, Providence, RI. Reprint of the second (1957) edition.

Hamming, R. W. (1950). Error detecting and error correcting codes. *Bell System Tech. J.*, 29:147–160.

Han, D., Kornelson, K., Larson, D., and Weber, E. (2007). *Frames for undergraduates*, volume 40 of *Student Mathematical Library*. American Mathematical Society, Providence, RI.

Higman, D. G. (1975). Coherent configurations. I. Ordinary representation theory. *Geometriae Dedicata*, 4(1):1–32.

Higman, D. G. (1976). Coherent configurations. II. Weights. *Geometriae Dedicata*, 5(4):413–424.

Hill, R. (1986). *A first course in coding theory*. Oxford Applied Mathematics and Computing Science Series. The Clarendon Press, Oxford University Press, New York.

Holzmann, W. H., Kharaghani, H., and Orrick, W. (2010). On the real unbiased Hadamard matrices. In *Combinatorics and graphs*, volume 531 of *Contemp. Math.*, pages 243–250. Amer. Math. Soc., Providence, RI.

Horadam, K. J. (2007). *Hadamard matrices and their applications*. Princeton University Press, Princeton, NJ.

Huffman, W. C. and Pless, V. (2003). *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge.

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

Ionin, Y. J. and Shrikhande, M. S. (2006). *Combinatorics of symmetric designs*, volume 5 of *New Mathematical Monographs*. Cambridge University Press, Cambridge.

Isaacs, I. M. (2006). *Character theory of finite groups*. AMS Chelsea Publishing, Providence, RI. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423].

Jungnickel, D. (1982). On automorphism groups of divisible designs. *Canadian J. Math.*, 34(2):257–297.

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

Kharaghani, H. (1986). A new class of symmetric weighing matrices. *J. Austral. Math. Soc. Ser. A*, 41(1):44–46.

Kharaghani, H., Pender, T., and Suda, S. (2021). Balancedly splittable orthogonal designs and equiangular tight frames. *Des. Codes Cryptogr.*, 89(9):2033–2050.

Kharaghani, H., Pender, T., and Suda, S. (2022). A family of balanced generalized weighing matrices. *Combinatorica, to appear*.

Kharaghani, H. and Suda, S. (2018). Unbiased orthogonal designs. *Des. Codes Cryptogr.*, 86(7):1573–1588.

Kharaghani, H. and Suda, S. (2019). Balancedly splittable Hadamard matrices. *Discrete Math.*, 342(2):546–561.

Kharaghani, H. and Suda, S. (2021). Divisible design digraphs and association schemes. *Finite Fields Appl.*, 69:Paper No. 101763, 17.

Lam, T. Y. and Leung, K. H. (2000). On vanishing sums of roots of unity. *J. Algebra*, 224(1):91–109.

Lang, S. (2002). *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition.

Lidl, R. and Niederreiter, H. (1994). *Introduction to finite fields and their applications*. Cambridge University Press, Cambridge, first edition.

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

McGuire, G. (1997). Quasi-symmetric designs and codes meeting the Grey-Rankin bound. *J. Combin. Theory Ser. A*, 78(2):280–291.

Neumann, P. M. (1975). Generosity and characters of multiply transitive permutation groups. *Proc. London Math. Soc. (3)*, 31(4):457–481.

Nozaki, H. and Suda, S. (2015). Weighing matrices and spherical codes. *J. Algebraic Combin.*, 42(1):283–291.

Paley, R. E. A. C. and Wiener, N. (1987). *Fourier transforms in the complex domain*, volume 19 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI. Reprint of the 1934 original.

Pender, T. S. (2020). Balanced group matrices. honors thesis.

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

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

Seberry, J. and Yamada, M. (1992). Hadamard matrices, sequences, and block designs. In *Contemporary design theory*, Wiley-Intersci. Ser. Discrete Math. Optim., pages 431–560. Wiley, New York.

Shrikhande, M. S. and Sane, S. S. (1991). *Quasi-symmetric designs*, volume 164 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge.

Singer, J. (1938). A theorem in finite projective geometry and some applications to number theory. *Trans. Amer. Math. Soc.*, 43(3):377–385.

Stinson, D. R. (2004). *Combinatorial designs*. Springer-Verlag, New York. Constructions and analysis, With a foreword by Charles J. Colbourn.

Waldron, S. (2020). Tight frames over the quaternions and equiangular lines.

Waldron, S. F. D. (2018). *An introduction to finite tight frames*. Applied and Numerical Harmonic Analysis. Birkhäuser/Springer, New York.

Wallis, W. D., Street, A. P., and Wallis, J. S. (1972). *Combinatorics: Room squares, sum-free sets, Hadamard matrices*. Lecture Notes in Mathematics, Vol. 292. Springer-Verlag, Berlin-New York.

Wielandt, H. (1964). *Finite permutation groups*. Academic Press, New York-London. Translated from the German by R. Bercov.

Young, R. M. (2001). *An introduction to nonharmonic Fourier series*. Academic Press, Inc., San Diego, CA, first edition.

Index