CHAPTER 1

Overview

1.1. What is a combinatorial design?

An experimental scientist, statistician, or engineer often studies variables that depend on several factors. Usually the experimenter has specific goals. She may wish to eliminate (as far as possible) the effect of one factor, or to gauge the effects of certain factors on the response variable. An experimental design is a schedule for a series of measurements that efficiently meets these needs. For example, it may be necessary to measure the weights of samples using a beam balance, or to compare the yields of strains of a crop. In the former case, the estimates are most accurate if the objects are weighed in combinations prescribed by a 'weighing matrix'. In the latter case, one can use a 'balanced incomplete block design'.

These and other efficient designs obey simple combinatorial rules determined by the setting. For example, a weighing matrix $\mathrm{W}(n, k)$ is an $n \times n$ matrix of 0s, 1s, and -1s such that

- each row and column contains exactly k non-zero entries,
- each pair of distinct rows has inner product equal to zero.

Also, a balanced incomplete block design $\mathrm{BIBD}(v, b, r, k, \lambda)$ is a $v \times b$ matrix of 0s and 1s such that

- each row contains exactly r 1s,
- each column contains exactly k 1s,
- each pair of distinct rows has inner product equal to λ.

The realization that an optimal experimental design corresponds to a schedule satisfying combinatorial rules, and that these designs may be used to save time and money, led to the development of combinatorial design theory: the field of mathematics concerned with finite objects, called combinatorial designs, obeying specified combinatorial rules. The field grows apace. It now has major interactions with coding theory, the study of sequences with autocorrelation properties, extremal graph theory, and finite geometry. In this book, we focus on *pairwise* combinatorial designs, each of which can be displayed as a square array whose rows taken pairwise obey a combinatorial rule. These seem to be the most pervasive sort of design.

1.2. What is Algebraic Design Theory?

This book is about the emerging area that we call *algebraic design theory*: the application of algebra and algebraic modes of reasoning in design theory.

The unresolved problems for pairwise combinatorial designs are not so easily categorized. It seems that these problems are algebraic, and some of them may be classed as a modern kind of Diophantine problem. In the situations where a design corresponds to a solution of a group ring (or norm) equation, this judgment is obviously correct; however, current algebraic techniques have not succeeded in answering vital questions. Thus, we sometimes fall back on constructions that supply us with examples and insights, but bypass the issue of extending current techniques to the point where they can answer our questions.

1.3. What is in this book?

Chapters 3–16 and Chapter 20 establish a general abstract framework for pairwise combinatorial designs. Chapters 2, 17, 18, 19, 21, 22, and 23 are case studies.

1.3.1. Theory.

Algebraic essentials. Chapter 3 collects together basic algebraic definitions and results. Parts of this chapter could be skipped by a reader with sufficient algebraic background. More algebra is filled in as we proceed through the book.

Orthogonality. Chapter 2 introduces the notions of orthogonality set Λ and pairwise combinatorial design $\mathrm{PCD}(\Lambda)$. We give many examples of familiar designs that are $\mathrm{PCD}(\Lambda)$s. Then Chapter 4 treats orthogonality in design theory at greater length. A natural and important problem is to determine, for each orthogonality set Λ, the maximum number of rows that are pairwise Λ-orthogonal. After discussing this problem, we show how the lattice of orthogonality sets with a given *alphabet* $\mathcal{A}$ may be studied using dual maps λ and δ between orthogonality sets and *design sets*. We further show how Λ determines a range of Λ-*equivalence* operations. These make up the group $\Pi_\Lambda = \langle \Pi_\Lambda^{\mathrm{row}}, \Pi_\Lambda^{\mathrm{col}} \rangle$ of row and column equivalence operations, and the group Φ_Λ incorporating Π_Λ and the global equivalence operations. We calculate Π_Λ and Φ_Λ for all the designs from Chapter 2.

Ambient rings. Chapter 5 constructs several rings for the necessary matrix algebra with designs. Let Λ be an orthogonality set with alphabet $\mathcal{A}$. At the very least, an *ambient ring* for Λ is just a ring containing $\mathcal{A}$. More productively, it is an involutory ring that also contains a *row group* $R \cong \Pi_\Lambda^{\mathrm{row}}$ and a *column group* $C \cong \Pi_\Lambda^{\mathrm{col}}$ in its group of units. This kind of ambient ring has a *matrix algebra model for* Λ-*equivalence*. Section 5.2 constructs such a ring for any Λ. Later, in Chapter 13, we show that a *central group* $Z \cong \Pi_\Lambda^{\mathrm{row}} \cap \Pi_\Lambda^{\mathrm{col}}$ may always be included in $R \cap C$. This extra structure is needed to model cocyclic development.

In Chapter 6 we consider Λ-orthogonality as a 'Gram Property': a $(0, \mathcal{A})$-array D is a $\mathrm{PCD}(\Lambda)$ if and only if the Gram matrix DD^* over an ambient ring $\mathcal{R}$ with involution $*$ lies in a prescribed set $\mathrm{Gram}_{\mathcal{R}}(\Lambda)$. Thus, although we start from a definition of orthogonality shorn of algebra, we can in fact think of each $\mathrm{PCD}(\Lambda)$ as a solution to a matrix ring equation.

Transposability. When does Λ-orthogonality, a pairwise condition on the rows of an array, impose a pairwise condition on the array's columns? In Chapter 7 we prove a theorem that answers this question for orthogonality sets like those in Chapter 2, as well as the new case of generalized weighing matrices over a non-abelian group. We also describe transposable orthogonality sets outside the scope of our theorem.

Composition and transference. Chapter 8 discusses the construction of new designs from other (generally smaller) designs. This is an old and recurring theme. The chapter divides into two sections: one on *composition*, the other on *transference*. These ideas have some overlap, but it is convenient to have both at our disposal.

Designs may be composed by means of a *substitution scheme*, which consists of a template array and a set of *plug-in matrices* that satisfy relations determined by the ambient ring for the template array. Since there is more than one choice of ring, a single template array can be employed in different compositions.

Transference (a term of our coinage) is a vehicle for another recurring theme in design theory. Here, existence of one kind of design implies the existence of another kind of design. The connections can be quite unexpected, and, to our eyes, exhibit no discernible common pattern. In Chapter 8 we give examples of transference. These depend on special properties of the alphabet.

The automorphism group. Let $\mathcal{R}$ be any ambient ring with row group $R \cong \Pi_\Lambda^{\mathrm{row}}$ and column group $C \cong \Pi_\Lambda^{\mathrm{col}}$. The ordered pair (P, Q) of monomial matrices $P \in \mathrm{Mon}(v, R)$ and $Q \in \mathrm{Mon}(v, C)$ is an *automorphism* of a PCD(Λ), D, if

$$PDQ^* = D.$$

Then $\mathrm{Aut}(D)$ consists of all automorphisms of D. This group is independent of the choice of ambient ring $\mathcal{R}$.

In Chapter 9 we show that Λ-orthogonality bounds the size of $\mathrm{Aut}(D)$. As an example, we find the automorphism groups for a class of generalized Hadamard matrices. We show that, in this case, the bound is nearly sharp. We then find the automorphism groups of some familiar orthogonal designs. Chapter 9 also presents a simple depth-first backtrack algorithm for computing $\mathrm{Aut}(D)$.

Expanded and associated designs. Chapter 9 introduces the *expanded design* and *associated design* of a pairwise combinatorial design. The associated design of a balanced generalized weighing matrix is a group divisible design. If D is a PCD(Λ) with ambient ring $\mathcal{R}$, then the expanded design of D is the block matrix

$$\mathcal{E}(D) = [rDc]_{r \in R, c \in C}$$

(the multiplication being done over $\mathcal{R}$). The expanded design $\mathcal{E}(D)$ is used to compute the automorphism group of D, and it figures prominently in the theory of cocyclic development.

Group-developed arrays. Chapter 10 is about a host of concepts: regular actions on square arrays, group development, associates, and group ring equations. The $(0, \mathcal{A})$-array A is group-developed modulo a group G if its rows and columns can be labeled with the elements of G so that, for some map $h : G \to \{0\} \cup \mathcal{A}$,

$$A = [h(xy)]_{x,y \in G}.$$

This is equivalent to G acting regularly on A. For each such h we get an element

$$\sum_{x \in G} h(x)x$$

of the group ring $\mathcal{R}[G]$ of G over an ambient ring $\mathcal{R}$, called a *G-associate* of A.

Associates and group ring equations. In Chapter 10 we show how each G-associate corresponds to a solution of a group ring equation with $(0, \mathcal{A})$-coefficients. The particulars of the group ring equation depend on the orthogonality set Λ. So the enumeration of group-developed PCD(Λ)s is equivalent to solving a group ring equation. The connection is akin to that between pairwise combinatorial designs and the Gram Property.

Associates and regular subgroups. We also show that the G-associates of an array correspond to the conjugacy classes of regular subgroups in the automorphism group of the array. We thereby gain a practical method to find all G-associates of a PCD(Λ).

Associates and difference sets. Finally, in Chapter 10 we see how the G-associates of designs give rise to (relative) difference sets.

Origins of cocyclic development. Chapter 11 elucidates the origins of cocyclic design theory. We give two derivations, both of which begin with the notion of an f-developed array

$$[f(x,y)(g(xy))]_{x,y\in G},$$

where $f : G \times G \to \mathrm{Sym}(\mathcal{A} \cup \{0\})$ is a map fixing 0. The first derivation is in the context of higher-dimensional designs. The second derivation springs from the fact that a group-developed array $A = [g(xy)]_{x,y\in G}$ is equivalent, via row and column permutations, to the array $[g(axy)]_{x,y\in G}$ obtained by developing the ath row of A for any a. If one requires that an f-developed array is Λ-equivalent to the array obtained by 'f-developing' the ath row of A, then f must be a 2-cocycle.

Cocycles. Let G and Z be groups, where Z is abelian. A map $f : G \times G \to Z$ such that

$$f(a,b)f(ab,c) = f(b,c)f(a,bc) \qquad \forall\, a,b,c \in G$$

is a 2-*cocycle*. Chapter 12 contains an elementary exposition of 2-cocycles. The discussion revolves around central short exact sequences

$$1 \longrightarrow Z \stackrel{\iota}{\longrightarrow} E \stackrel{\pi}{\longrightarrow} G \longrightarrow 1.$$

Each map (apart from the first) is a group homomorphism whose kernel is the image of the preceding homomorphism, and ι maps into the center of the extension group E. We define a cocycle $f_{\iota,\tau} : G \times G \to Z$ for each 'transversal map' $\tau : G \to E$; moreover, every cocycle $f : G \times G \to Z$ arises in this way. Chapter 12 discusses cocycles of product groups, cocycles calculated by collection within a polycyclic group, and monomial representations from a cocycle.

Cocyclic pairwise combinatorial designs. Chapter 13 formulates the theory of cocyclic designs in terms of matrix algebra.

Let D be a $\mathrm{PCD}(\Lambda)$, where Λ has ambient ring $\mathcal{R}$ containing the row group R, column group C, and central group Z. Then D is *cocyclic* if for some cocycle $f : G \times G \to Z$ there are monomial matrices $P \in \mathrm{Mon}(v, R)$, $Q \in \mathrm{Mon}(v, C)$ and a map $g : G \to \{0\} \cup \mathcal{A}$ such that

$$D = P[f(x,y)g(xy)]_{x,y\in G}Q$$

over $\mathcal{R}$. We say that f is a *cocycle of* D with *indexing group* G, and that f is a Λ-*cocycle*. Any extension group for f is an *extension group* of D. Chapter 13 asks

1.3.1. Question. *Given a* $\mathrm{PCD}(\Lambda)$*,* D*, what are all the cocycles of* D*?*

1.3.2. Question. *Given an orthogonality set* Λ *and a cocycle* $f : G \times G \to Z$*, is there a* $\mathrm{PCD}(\Lambda)$ *with cocycle* f*?*

Four approaches to cocyclic designs are proposed.

1.3.3. For a given orthogonality set Λ,

(1) study the cocycles of known highly-structured $\mathrm{PCD}(\Lambda)$s;
(2) determine Λ-cocycles via the extension group;
(3) determine Λ-cocycles via the indexing group;
(4) use composition to prove existence of $\mathrm{PCD}(\Lambda)$s.

All these approaches are taken in the book.

Centrally regular actions, cocyclic associates, and group ring equations. Chapters 14 and 15 set out more theory of cocyclic designs. We describe relationships between cocyclic development, actions on the expanded design, cocyclic associates, and group ring equations. Taken together, Chapters 14 and 15 are analogous to Chapter 10.

Chapter 15 contains deeper material: an application of character theory to the existence question for circulant complex Hadamard matrices, and Ito's striking results on allowable extension groups of cocyclic Hadamard matrices (in line with part (2) of 1.3.3).

Cocyclic development tables. A *development table* displays all the ways in which a cocyclic PCD(Λ) with indexing group G may be f-developed for some cocycle $f : G \times G \to Z$. Chapter 20 explains how to compute development tables when G is solvable.

The theory for familiar classes of designs. Chapter 16 is a 'bridging' chapter. It refreshes some of the preceding theory in the book, with particular regard to (complex) Hadamard matrices, balanced weighing matrices, and orthogonal designs. Theoretical results needed for the case studies are here.

1.3.2. Practice.

Many pairwise combinatorial designs. In Chapter 2 we prove basic results about familiar PCD(Λ)s, and state what is done in the book concerning those designs.

Paley matrices. The automorphism groups and all the regular actions for the Paley conference and Hadamard matrices are described in Chapter 17. This case study is extremely rich, yet it is tractable enough that we can answer Question 1.3.1 and carry out part (1) of the agenda 1.3.3.

A large family of cocyclic Hadamard matrices. Chapter 18 is a nice example of part (4) of 1.3.3. Beginning with Paley matrices and applying plug-in techniques, we obtain a large family of cocyclic Hadamard matrices, and thus many maximal-sized relative difference sets with central forbidden subgroup of size 2.

Substitution schemes. Chapter 19 considers the cocyclic Hadamard matrices with cocycle $f : G \times G \to \langle -1 \rangle$ obtained from a central short exact sequence

$$1 \longrightarrow \langle -1 \rangle \longrightarrow E = L \ltimes N \stackrel{\pi}{\longrightarrow} G = K \ltimes N \longrightarrow 1,$$

where $|K| = 4$, π is the identity on N, and $\pi(L) = K$ (this includes the atomic case $|G| = 4p,\ p > 3$ prime). All such Hadamard matrices are defined by a substitution scheme that, among other things, generalizes the Williamson construction. This study is an instance of part (3) of 1.3.3.

Cocyclic Hadamard matrices and elementary abelian groups. A primary aim in the study of cocyclic Hadamard matrices is to answer Question 1.3.2 for a given group G. For most G this problem breaks up into a practicable algebraic component and a difficult combinatorial component. However, if G is an elementary abelian 2-group then we show in Chapter 21 that the problem can be solved algebraically: here, nearly every cocycle is a cocycle of a Sylvester Hadamard matrix. Chapter 21 is a good example of parts (2) and (3) of the agenda 1.3.3.

Systems of cocyclic orthogonal designs. Chapter 22 gives a complete algebraic solution of the problem of classifying *concordant* systems $\{D_1, \ldots, D_r\}$ of cocyclic orthogonal designs, where in each D_i every relevant indeterminate appears exactly once in each row and column. The approach is via the extension group, and there is a strong reliance on Chapter 21.

Asymptotic existence of cocyclic Hadamard matrices. In the final chapter we present a proof of the best known (to date) asymptotic existence result for cocyclic Hadamard matrices. Our proof combines knowledge about the existence of complex complementary sequences with ideas from Chapters 21 and 22.