new mathematical monographs: 5

Combinatorics of Symmetric Designs

Yury J. Ionin and Mohan S. Shrikhande

CAMBRIDGE

CAMBRIDGE www.cambridge.org/9780521818339

This page intentionally left blank

Combinatorics of Symmetric Designs

The aim of this book is to provide a unified exposition of the theory of symmetric designs with emphasis on recent developments. The authors cover the combinatorial aspects of the theory giving particular attention to the construction of symmetric designs and related objects. The last five chapters of the book are devoted to balanced generalized weighing matrices, decomposable symmetric designs, subdesigns of symmetric designs, non-embeddable quasi-residual designs, and Ryser designs. Most results in these chapters have never previously appeared in book form. The book concludes with a comprehensive bibliography of over 400 entries.

Researchers in all areas of combinatorial designs, including coding theory and finite geometries, will find much of interest here. Detailed proofs and a large number of exercises make this book suitable as a text for an advanced course in combinatorial designs.

YURY J. IONIN is a professor of mathematics at Central Michigan University, USA.

MOHAN S. SHRIKHANDE is a professor of mathematics at Central Michigan University, USA.

New Mathematical Monographs

Combinatorics of Symmetric Designs

YURY J. IONIN and MOHAN S. SHRIKHANDE
Central Michigan University

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 2RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521818339

First published in print format 2006

ISBN-13 978-0-511-15922-0 eBook (Adobe Reader)
ISBN-10 0-511-15922-6 eBook (Adobe Reader)

ISBN-13 978-0-521-81833-9 hardback
ISBN-10 0-521-81833-8 hardback

To Irina, Tania, and Timur

To Neelima, Aditi, and Sean

Contents

Preface

Design theory is a well-established branch of combinatorial mathematics. The origins of the subject can be traced back to statistics in the pioneering works of R. A. Fisher, F. Yates, and R. C. Bose. From the very beginning, one of the central objects of design theory has been symmetric designs. The prototype of a symmetric design is a finite projective plane, and the theory of symmetric designs borrows its methods and ideas from finite geometries, group theory, number theory, and linear algebra.

It is notoriously difficult to construct an infinite family of symmetric designs or even a single symmetric design. However, in recent years new ideas in constructing symmetric designs have been discovered and new infinite families have been found. The central role in these constructions is played by balanced generalized weighing matrices. These matrices generalize the notion of a symmetric design but until recently they were often regarded as a rather obscure combinatorial object. Now they seem to be a useful tool in unifying different construction methods that have been developed since the 1950s.

This book is primarily a research monograph which aims to give a unifying exposition of the theory of symmetric designs with emphasis on these new developments. The book covers the combinatorial aspects of the theory with particular attention to constructing symmetric designs and related objects. Recent results that have never previously appeared in book format are developed mainly in the last five chapters. These chapters are devoted to balanced generalized weighing matrices, decomposable symmetric designs, subdesigns of symmetric designs, non-embeddable quasi-residual designs, and Ryser designs. The preceding chapters on finite geometries, Hadamard matrices, resolvable designs, t-designs, strongly regular graphs, and difference sets emphasize relations between these objects and symmetric designs.

We believe that this book can also be used as a text for a course in combinatorial designs. We begin with a brief introduction to combinatorial set theory,

including such beautiful results as Fisher's Inequality, the Ray-Chaudhuri–Wilson Inequality, and the Ryser–Woodall Theorem. The proofs of these theorems are elementary, but we hope they may be of interest even to the expert. Both Fisher's Inequality and the Ryser–Woodall Theorem allow us to introduce the notion of a symmetric design even before the formal definition is given in Chapter 2. Chapters 2–4 and 6–9 contain basic material on combinatorial designs, finite geometries, Hadamard matrices, strongly regular graphs, difference sets, and codes. We have included many examples and exercises and presented the proofs of many theorems in a manner suitable for graduate and advanced undergraduate students. Every chapter of the book is concluded by notes containing comments, references, and historical material. We suggest that the following chapters and sections could form a course in combinatorial designs: Chapter 1, Chapter 2 (without Sections 2.7 and 2.8), Chapter 3 (without Section 3.7), and also Sections 4.1, 4.2, 4.3, 6.1, 6.2, 6.3, 6.5, 7.1, 7.2, 9.1, and 9.2. A standard course of linear algebra and the basic notions of combinatorics and abstract algebra should form a sufficient background for this book.

The numbering of theorems, definitions, remarks, and examples is consecutive within each section and includes the chapter and section numbers, so, for instance, Theorem 3.7.10 can be found in Section 3.7. However, equations are numbered consecutively within each chapter. The last two sections of every chapter are **Exercises** and **Notes**. The **Appendix** contains the list of parameters of all known symmetric designs, which are combined into 23 series and 12 sporadic designs. We conclude the book with an extensive **References** section of over 400 entries, all of which are cited in the book.

We would like to acknowledge people and institutions who through their help, financial support, and hospitality made this work possible. Our particular thanks are due to Alphonse Baartmans, Dieter Jungnickel, Hadi Kharaghani, Vassili Mavron, Gary McGuire, Damaraju Raghavarao, Dijen Ray-Chaudhuri, S. S. Shrikhande, and Vladimir Tonchev for their comments and encouragement during various stages of preparation of this book.

We thank O. Abu Ghnaim, T. Al-Raqqad, J. R. Angelos, T. Ionin, D. Levi, A. Sarker, and K. W. Smith for help and comments and also the students of three classes at Central Michigan University who had to use imperfect drafts of the book as their textbooks.

Our own research that is included in this book, and the writing of the book were done at Central Michigan University, with extensive use of its facilities. The university has also supported us with sabbaticals and numerous travel grants. We are especially thankful to Central Michigan University for two Research Professorship grants awarded to each of us. We would also like to acknowledge the hospitality and financial support of the following

institutions: Mathematisches Forschungsinstitut, Oberwolfach, Germany; Michigan Technological University, Houghton, Michigan, USA; Ohio State University, Columbus, Ohio, USA; University of Lethbridge, Lethbridge, Alberta, Canada; Temple University, Philadelphia, Pennsylvania, USA; University of Wales, Aberystwyth, Wales, UK.

We thank Roger Astley and the staff of Cambridge University Press for their superb assistance during preparation and production of this book.

Finally, we would like to thank our wives for their unwavering support, patience, and understanding.

1

Combinatorics of finite sets

A number of advances in combinatorics originated in the following problem: given a finite set and a property of families of subsets of this set, estimate the size of a family with this property and then explore families of maximum or minimum size.

In this chapter we will discuss three problems of this kind:

(i) given a nonempty finite set V, estimate the size of a family $\mathcal{F}$ of subsets of V such that $|A \cap B|$ is the same for all distinct $A, B \in \mathcal{F}$;
(ii) given a nonempty finite set V and positive integers k and s, estimate the size of a family $\mathcal{F}$ of k-subsets of V such that $|A \cap B|$ takes at most s values for distinct $A, B \in \mathcal{F}$;
(iii) given a nonempty finite set V, estimate the size of a family $\mathcal{F}$ of subsets of V such that the cardinality of the symmetric difference of A and B is the same for all distinct $A, B \in \mathcal{F}$.

This discussion will lead us to *symmetric designs*, the central object of study in this book.

1.1. Fisher's Inequality

When we consider families of subsets of a finite set V of cardinality v, it is convenient to think of V as the set $\{1, 2, \ldots, v\}$ and associate with every subset X of V a (0, 1)-string $(x_1, x_2, \ldots, x_v)$ of length v where $x_i = 1$ if $i \in X$ and $x_i = 0$ if $i \notin X$.

We now introduce a simple but useful idea. In order to estimate the size of a family $\mathcal{F}$ of subsets of V, we will select a suitable finite-dimensional vector space P over the rationals and associate an element of P with each element of

$\mathcal{F}$. If the set of vectors associated with the elements of $\mathcal{F}$ is linearly independent, then the cardinality of $\mathcal{F}$ does not exceed the dimension of P.

As the first application of this idea, we take P to be the vector space of linear polynomials $a_0 + a_1x_1 + a_2x_2 + \cdots + a_vx_v$ in v variables with rational coefficients. Clearly, $\dim P = v + 1$. We will now give a proof of the following result:

Theorem 1.1.1 (Nonuniform Fisher's Inequality). *Let V be a nonempty finite set and $\mathcal{F}$ a family of subsets of V such that the cardinality of the intersection of any two distinct members of $\mathcal{F}$ is the same positive integer. Then $|\mathcal{F}| \leq |V|$.*

Proof. Let $\mathcal{F}$ be a family of subsets of the set $V = \{1, 2, \ldots, v\}$. Assume there exists a positive integer λ such that $|A \cap B| = \lambda$ for any distinct A and B in $\mathcal{F}$.

Suppose first that there exists $A \in \mathcal{F}$ such that $|A| \leq \lambda$. Then $|A| = \lambda$ and the intersection of any two distinct members of $\mathcal{F}$ is the set A. By subtracting A from each member of $\mathcal{F}$, we obtain a family of pairwise disjoint subsets of the set $V \setminus A$. Since the cardinality of such a family does not exceed $|V \setminus A| + 1$, we obtain that $|\mathcal{F}| \leq v - \lambda + 1 \leq v = |V|$.

From now on, we assume that $|A| > \lambda$ for any $A \in \mathcal{F}$. With each $A \in \mathcal{F}$, we associate the linear polynomial $f_A = \sum_{i \in A} x_i - \lambda$. Then $f_A(X) = |A \cap X| - \lambda$ for any $X \subseteq V$ (regarded as a (0, 1)-string). In particular, for any $A, B \in \mathcal{F}$,

$$f_A(B) = \begin{cases} 0 & \text{if } B \neq A, \\ |B| - \lambda & \text{if } B = A. \end{cases} \tag{1.1}$$

We claim that the subset $\{f_A \colon A \in \mathcal{F}\}$ of the vector space P is linearly independent. Indeed, if $\sum_{A \in \mathcal{F}} \alpha_A f_A = 0$ for some (rational) coefficients α_A, then, applying both sides of this equation to an arbitrary $B \in \mathcal{F}$ and using (1.1), we obtain that $\alpha_B(|B| - \lambda) = 0$, so $\alpha_B = 0$.

Suppose that the constant polynomial 1 is spanned by the polynomials f_A, $A \in \mathcal{F}$, i.e.,

$$1 = \sum_{A \in \mathcal{F}} \alpha_A f_A. \tag{1.2}$$

for some coefficients α_A. Then, applying both sides of (1.2) to $B \in \mathcal{F}$ and using (1.1), we obtain that $\alpha_B(|B| - \lambda) = 1$, so

$$1 = \sum_{A \in \mathcal{F}} \frac{1}{|A| - \lambda} f_A.$$

Applying both sides of this equation to the empty set, we obtain

$$1 = \sum_{A \in \mathcal{F}} \frac{-\lambda}{|A| - \lambda},$$

a contradiction, since the right-hand side of the last equation is negative.

Thus, the set $\{f_A : A \in \mathcal{F}\} \cup \{1\}$ of linear polynomials is linearly independent. Since $\dim P = v + 1$, we obtain that $|\mathcal{F}| + 1 \leq v + 1$, i.e., $|\mathcal{F}| \leq v = |V|$. □

The bound given by Fisher's Inequality is sharp. If $\mathcal{F}$ is the family of all $(v-1)$-subsets of the v-set V, then $|A \cap B| = v - 2$ for all distinct $A, B \in \mathcal{F}$ and $|\mathcal{F}| = v$.

1.2. The First Ray-Chaudhuri–Wilson Inequality

If A and B are distinct elements of a family $\mathcal{F}$ of subsets of a set V, the number $|A \cap B|$ is called an *intersection number* of $\mathcal{F}$. In the previous section, we considered families of subsets with one intersection number. In this section, we will consider families with s intersection numbers. To estimate the size of such a family, we will use the vector space P_s of multilinear polynomials of total degree s or less in v variables.

Definition 1.2.1. Let Q_s be the vector space of all polynomials in variables $x_1, x_2, \ldots, x_v$ of total degree $\leq s$ with rational coefficients. For each $I \subseteq \{1, 2, \ldots, v\}$, let $x_I = \prod_{i \in I} x_i$ (with the convention that $x_\varnothing = 1$). A polynomial $f \in Q_s$ is called *multilinear* if it can be represented as a linear combination of the polynomials x_I with $|I| \leq s$. For every polynomial f in variables $x_1, x_2, \ldots, x_v$, let f^* be the multilinear polynomial obtained by replacing each occurrence of x_i^k by x_i (for $k \geq 2$ and $i = 1, 2, \ldots, v$).

Multilinear polynomials form a subspace P_s of Q_s, and the polynomials x_I with $|I| \leq s$ form a basis of P_s. Therefore, $\dim P_s = \sum_{i=0}^{s} \binom{v}{i}$.

With every subset X of $\{1, 2, \ldots, v\}$, we again associate a $(0,1)$-string $(x_1, x_2, \ldots, x_v)$ of length v where $x_i = 1$ if $i \in X$ and $x_i = 0$ if $i \notin X$. Then, for any polynomial f in v variables, we have $f(X) = f^*(X)$.

Theorem 1.2.2 (The First Ray-Chaudhuri–Wilson Inequality). *Let $\mathcal{F}$ be a family of subsets of a set V of cardinality v. Let M be a set of non-negative integers, $|M| = s$. Suppose that $|A| = k$ is the same for all $A \in \mathcal{F}$, $|A \cap B| \in M$ for any distinct $A, B \in \mathcal{F}$, and $k > m$ for all $m \in M$. Then $|\mathcal{F}| \leq \binom{v}{s}$.*

Proof. Let $V = \{1, 2, \ldots, v\}$ and let $\mathcal{F}$ be a family of k-subsets of V satisfying the conditions of the theorem. With each $A \in \mathcal{F}$, we associate the polynomial

$$g_A = \prod_{m \in M} \Big(\sum_{i \in A} x_i - m\Big),$$

and the multilinear polynomial g_A^*. Then

$$g_A^*(X) = \prod_{m \in M} (|A \cap X| - m)$$

for any $X \subseteq V$, and $g_A^*(B) = 0$ for any distinct $A, B \in \mathcal{F}$. Note that $g_A^*(A) > 0$ for any $A \in \mathcal{F}$. We also put $h(x_1, x_2, \ldots, x_v) = \sum_{i=1}^{v} x_i - k$. Then $h(X) = |X| - k$ for any subset X of V, so $h(A) = 0$ for any $A \in \mathcal{F}$.

We claim that the set

$$\{g_A^* \colon A \in \mathcal{F}\} \cup \{(x_I h)^* \colon I \subseteq V, |I| \leq s-1\}$$

of multilinear polynomials is linearly independent. Since all these polynomials are in P_s, this would imply that

$$|\mathcal{F}| + \sum_{i=0}^{s-1} \binom{v}{i} \leq \dim P_s,$$

so $|\mathcal{F}| \leq \binom{v}{s}$.

Assume that

$$\sum_{A \in \mathcal{F}} \alpha_A g_A^* + \sum_{\substack{I \subseteq V \\ |I| \leq s-1}} \beta_I (x_I h)^* = 0,$$

for some rational coefficients α_A, β_I. Applying both sides of this equation to $B \in \mathcal{F}$, we obtain that $\alpha_B g_B^*(B) = 0$, so $\alpha_B = 0$. Therefore,

$$\sum_{\substack{I \subseteq V \\ |I| \leq s-1}} \beta_I (x_I h)^* = 0. \tag{1.3}$$

We will show by induction on $|I|$ that $\beta_I = 0$.

Note that for $J \subseteq V$, we have

$$x_I(J) = \begin{cases} 1 & \text{if } I \subseteq J, \\ 0 & \text{otherwise.} \end{cases} \tag{1.4}$$

Applying both sides of (1.3) to the empty set and using (1.4), we obtain $\beta_\varnothing = 0$. Let $1 \leq u \leq s-1$ and let $\beta_I = 0$ whenever $|I| \leq u-1$. Then we have

$$\sum_{\substack{I \subseteq V \\ u \leq |I| \leq s-1}} \beta_I (x_I h)^* = 0.$$

Applying both sides of this equality to a subset J of V of cardinality u and using (1.4), we obtain that $\beta_J = 0$. This completes the induction and the proof of the theorem. □

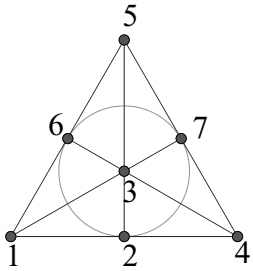

Figure 1.1 Fano Plane.

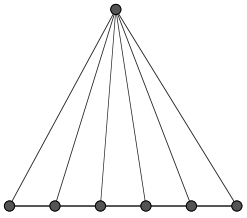

Figure 1.2 Pencil.

If $\mathcal{F}$ is the family of all s-subsets of the v-set V, then $|A \cap B| \in \{0, 1, \ldots, s-1\}$ for any distinct $A, B \in \mathcal{F}$ and $|\mathcal{F}| = \binom{v}{s}$, so the Ray-Chaudhuri–Wilson bound is sharp.

1.3. Symmetric designs and Ryser designs

By Fisher's Inequality (Theorem 1.1.1), the cardinality of a family of subsets of a v-set with one (nonzero) intersection number does not exceed v. In this section, we will consider families attaining this bound. The set of all $(v-1)$-subsets of a v-set is an example of such a family. We will give several less trivial examples.

Example 1.3.1. Let $V = \{1, 2, 3, 4, 5, 6, 7\}$ and let $\mathcal{F} = \{\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 7\}, \{5, 6, 1\}, \{6, 7, 2\}, \{7, 1, 3\}\}$. Then $|\mathcal{F}| = |V|$ and $|A \cap B| = 1$ for any distinct $A, B \in \mathcal{F}$. This configuration is known as the *Fano Plane*. In Fig. 1.1, triples of points on lines or on the circle represent elements of the family $\mathcal{F}$. All these triples are regarded as *lines* in the Fano Plane.

Example 1.3.2. Let V be a finite set. Fix $x \in V$ and define $\mathcal{F}$ to be the family consisting of the set $V \setminus \{x\}$ and all 2-subsets of V containing x. Then $|\mathcal{F}| = |V|$ and $|A \cap B| = 1$ for any distinct $A, B \in \mathcal{F}$. Such a configuration is called a *pencil* (Fig. 1.2).

Example 1.3.3. Arrange the elements of a set V of cardinality 16 in a 4×4 array. For each $x \in V$, define a subset B_x of size 6 by taking the elements of V, other than x, which occur in the same row or column as x. It is easy to see that $|B_x \cap B_y| = 2$ for any distinct $x, y \in V$.

Let $V = \{1, 2, \ldots, \mathrm{v}\}$ be a set of cardinality v. Let λ be a positive integer and let $\mathcal{F}$ be a family of subsets of V such that $|A \cap B| = \lambda$ for any distinct $A, B \in \mathcal{F}$. For each $A \in \mathcal{F}$, denote by f_A the linear polynomial

$$f_A = \sum_{i \in A} x_i - \lambda. \tag{1.5}$$

In the proof of Theorem 1.1.1, we have shown that the set $\{f_A : A \in \mathcal{F}\} \cup \{1\}$ is linearly independent in the vector space P of linear polynomials in variables $x_1, x_2, \ldots, x_v$ (over the rationals).

Suppose now that the family $\mathcal{F}$ is of maximum size, i.e., $|\mathcal{F}| = v$. Then this set of polynomials is a basis of P. By expanding monomials x_i in this basis we will attempt to extract information which can be used to obtain a crude classification of the extremal case. For the next theorem we introduce the notion of the *replication number* that will be used throughout the book.

Definition 1.3.4. Let $\mathcal{F}$ be a family of subsets of a finite set V. For any $x \in V$, the number of elements of $\mathcal{F}$ which contain x is called the *replication number of x in $\mathcal{F}$*.

Theorem 1.3.5 (The Ryser–Woodall Theorem). *Let v and λ be positive integers and let $\mathcal{F}$ be a family of v subsets of a v-set V such that $|A \cap B| = \lambda$ for any distinct $A, B \in \mathcal{F}$. Then either all elements of V have the same replication number or they have exactly two distinct replication numbers r and r^* and $r + r^* = v + 1$. In the latter case, $2 \leq r \leq v - 1$ and $2 \leq r^* \leq v - 1$.*

Proof. Let $V = \{1, 2, \ldots, v\}$. If there is $A \in \mathcal{F}$ such that $|A| \leq \lambda$, then $|A| = \lambda$ and $B \cap C = A$ for any distinct $B, C \in \mathcal{F}$. Therefore, each element of A has replication number $r = v$ and each element of $V \setminus A$ has replication number $r^* = 1$. Thus we have $r + r^* = v + 1$. From now on, we assume that $|A| > \lambda$ for each $A \in \mathcal{F}$. Then the set $\{f_A : A \in \mathcal{F}\} \cup \{1\}$ where the polynomials f_A are defined by (1.5), is a basis of the vector space P of linear polynomials in variables $x_1, x_2, \ldots, x_v$ over the rationals. We will expand the monomials x_i in this basis:

$$x_i = \sum_{A \in \mathcal{F}} \alpha_A^{(i)} f_A + \beta_i.$$

Applying both sides of this equation to $B \in \mathcal{F}$ and using (1.1), we obtain that $\alpha_B^{(i)} = (1 - \beta_i)/(|B| - \lambda)$ if $i \in B$ and $\alpha_B^{(i)} = -\beta_i/(|B| - \lambda)$ if $i \notin B$.

Therefore,

$$x_i = (1-\beta_i)\sum_{A\ni i}\frac{f_A}{|A|-\lambda} - \beta_i\sum_{A\not\ni i}\frac{f_A}{|A|-\lambda} + \beta_i. \tag{1.6}$$

Applying both side of (1.6) to the empty set and to the singleton $\{i\}$, we obtain:

$$0 = (1-\beta_i)(-\lambda)\sum_{A\ni i}\frac{1}{|A|-\lambda} - \beta_i(-\lambda)\sum_{A\not\ni i}\frac{1}{|A|-\lambda} + \beta_i, \tag{1.7}$$

$$1 = (1-\beta_i)(1-\lambda)\sum_{A\ni i}\frac{1}{|A|-\lambda} - \beta_i(-\lambda)\sum_{A\not\ni i}\frac{1}{|A|-\lambda} + \beta_i. \tag{1.8}$$

Subtract (1.7) from (1.8) to obtain that $\beta_i \neq 1$ and

$$\sum_{A\ni i}\frac{1}{|A|-\lambda} = \frac{1}{1-\beta_i}. \tag{1.9}$$

Equations (1.7) and (1.9) imply that $\beta_i \neq 0$ and

$$\sum_{A\not\ni i}\frac{1}{|A|-\lambda} = \frac{1}{\beta_i} - \frac{1}{\lambda}. \tag{1.10}$$

Adding (1.9) to (1.10) yields

$$\frac{1}{\lambda} + \sum_{A\in\mathcal{F}}\frac{1}{|A|-\lambda} = \frac{1}{\beta_i(1-\beta_i)}. \tag{1.11}$$

We can reduce (1.11) to a quadratic equation in β_i, whose coefficients do not depend on i. Therefore, β_i can have at most two distinct values, β and $\beta^* = 1-\beta$. If $\beta_i = \beta$, then applying both sides of (1.6) to the set V yields

$$1 = (1-\beta)r_i - \beta(v-r_i) + \beta,$$

where r_i is the replication number of i. This equation implies that $r_i = \beta(v-1)+1$. Similarly, if $\beta_i = \beta^*$, we obtain that $r_i = \beta^*(v-1)+1$. Thus, if all β_i are the same, then all points $i \in V$ have the same replication number. If β and β^* are the two distinct values of β_i, then the elements of V have two distinct replication numbers r and r^*. Since $\beta+\beta^* = 1$, we have $r + r^* = v+1$.

Since $r + r^* = v+1$, we have $r \geq 1$. If $r = 1$, then $r = \beta(v-1)+1$ implies $\beta = 0$ which is not the case. Therefore, if the family $\mathcal{F}$ has two replication numbers and $|A| > \lambda$ for all $A \in \mathcal{F}$, then the replication number of each element of V is greater than 1 and less than v. □

Let us now discuss the two possibilities that arise from the Ryser–Woodall Theorem.

Suppose first that $\mathcal{F}$ is a family of v subsets of a v-set V such that $|A \cap B| = \lambda$ for any distinct $A, B \in \mathcal{F}$ and all elements of V have the same replication number r. Fix $A \in \mathcal{F}$ and count in two ways pairs (x, B) with $B \in \mathcal{F}$, $B \neq A$, and $x \in A \cap B$. We obtain that $|A|(r-1) = \lambda(v-1)$. Therefore, if $\lambda > 0$, then all $A \in \mathcal{F}$ have the same cardinality. In this case, we will say that $(V, \mathcal{F})$ is a *symmetric* (v, k, λ)*-design*, where $k = |A|$ for all $A \in \mathcal{F}$. Counting in two ways pairs (x, A) with $A \in \mathcal{F}$ and $x \in A$ yields $k = r$. Examples 1.3.1 and 1.3.3 describe a symmetric $(7, 3, 1)$-design and a symmetric $(16, 6, 2)$-design, respectively. The precise definition and many other examples of symmetric designs will be given in the next chapter.

The second possibility arising from the Ryser–Woodall Theorem leads to the notion of a *Ryser design*.

Definition 1.3.6. Let v and λ be positive integers. A *Ryser design of index* λ *on* v *points* is a pair $(V, \mathcal{F})$ where V is a set of cardinality v and $\mathcal{F}$ is a family of v subsets of V (blocks) such that

(i) $|A \cap B| = \lambda$ for any distinct $A, B \in \mathcal{F}$;
(ii) $|A| > \lambda$ for all $A \in \mathcal{F}$;
(iii) there are blocks A and B such that $|A| \neq |B|$.

Example 1.3.2 describes a Ryser design of index 1 on v points. As will be shown in Section 14.1, pencils are the only possible Ryser designs of index 1 on v points.

1.4. Equidistant families of sets

We will now consider a distance function on the set of subsets of a finite set. It will measure how different two subsets are. The following definition introduces the famous *Hamming distance*.

Definition 1.4.1. Let V be a finite set. For any $X, Y \subseteq V$, define the Hamming distance $d(X, Y)$ to be the cardinality of the symmetric difference $X \triangle Y$ of X and Y.

The Hamming distance has the following properties that can be easily verified:

(i) $d(X, Y) \geq 0$; $d(X, Y) = 0$ if and only if $X = Y$;
(ii) $d(X, Y) = d(Y, X)$;
(iii) $d(X, Y) + d(Y, Z) \geq d(X, Z)$.

Definition 1.4.2. A family $\mathcal{F}$ of subsets of the set V is called *equidistant* if there exists a positive integer d such that $|A \triangle B| = d$ for any distinct A and B in $\mathcal{F}$.

In this section we will first find the maximum cardinality of an equidistant family of subsets of a v-set.

Theorem 1.4.3. *If $\mathcal{F}$ is an equidistant family of subsets of a finite set V of cardinality v, then $|\mathcal{F}| \leq v + 1$.*

Proof. Let $\mathcal{F}$ be an equidistant family of subsets of the set $V = \{1, 2, \ldots, v\}$, $|\mathcal{F}| \geq 2$, and let $d = |A \triangle B|$ for any distinct A and B in $\mathcal{F}$. With each $A \in \mathcal{F}$ we associate the following linear polynomial f_A in variables $x_1, x_2, \ldots, x_v$:

$$f_A = \sum_{i \notin A} x_i - \sum_{i \in A} x_i + |A| - d. \tag{1.12}$$

Then, for any subset X of V (regarded as a (0, 1)-string),

$$f_A(X) = |A \triangle X| - d. \tag{1.13}$$

This implies that for any $A, B \in \mathcal{F}$,

$$f_A(B) = \begin{cases} 0 & \text{if} \quad B \neq A, \\ -d & \text{if} \quad B = A. \end{cases} \tag{1.14}$$

We claim that the set $\{f_A : A \in \mathcal{F}\}$ of linear polynomials is linearly independent (over the rationals). Indeed, if $\sum_{A \in \mathcal{F}} \alpha_A f_A = 0$ for some rational coefficients α_A, then, applying both sides of this equality to $B \in \mathcal{F}$ and using (1.14), we obtain that $\alpha_B(-d) = 0$, so $\alpha_B = 0$. Since the dimension of the vector space of linear polynomials in the variables $x_1, x_2, \ldots, x_v$ equals $v + 1$, it follows that $|\mathcal{F}| \leq v + 1$. □

Hadamard matrices provide examples of maximum cardinality equidistant families.

Definition 1.4.4. A *Hadamard matrix* is a square matrix with all entries equal to ± 1 and with any two distinct rows orthogonal.

For example,

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

is a Hadamard matrix of order 4.

Hadamard matrices arise in different areas of combinatorics. The order of a Hadamard matrix is 1 or 2 or a multiple of 4. One of the most famous open conjectures in combinatorics is that there exists a Hadamard matrix of every order that is divisible by 4. We will discuss Hadamard matrices at length in Chapter 4.

Example 1.4.5. Let $V = \{1, 2, \ldots, v\}$, and let $H = [h_{ij}]$ be a Hadamard matrix of order $v + 1$ with all entries in the last column equal to 1. For $i = 1, 2, \ldots, v + 1$, let $A_i = \{j \in V : h_{ij} = 1\}$. Then the family $\mathcal{F} = \{A_i : 1 \leq i \leq v + 1\}$ is equidistant. It is called a *Hadamard family*.

We will now show that this is the only possible example of a maximum size equidistant family.

Theorem 1.4.6. *Let $\mathcal{F}$ be an equidistant family of subsets of a v-set V. If $|\mathcal{F}| = v + 1$, then $\mathcal{F}$ is a Hadamard family.*

Proof. Let $|\mathcal{F}| = v + 1$, $|A \triangle B| = d$ for any distinct $A, B \in \mathcal{F}$, and let polynomials f_A be defined by (1.12). It was shown in the proof of Theorem 1.4.3 that the set $\{f_A : A \in \mathcal{F}\}$ of linear polynomials is linearly independent. Since $|\mathcal{F}| = v + 1$, this set is a basis of the vector space P of linear polynomials in $x_1, x_2, \ldots, x_v$. Expand the constant polynomial 1 in this basis:

$$1 = \sum_{A \in \mathcal{F}} \alpha_A f_A$$

for some rational coefficients α_A. Applying both sides of this equality to $B \in \mathcal{F}$, we derive that $\alpha_B(-d) = 1$, so $\alpha_B = -1/d$ for any $B \in \mathcal{F}$. Therefore, we have

$$\sum_{A \in \mathcal{F}} f_A = -d. \tag{1.15}$$

Applying both sides of (1.15) to the empty set and the set V, we obtain:

$$\sum_{A \in \mathcal{F}} (|A| - d) = -d$$

and

$$\sum_{A \in \mathcal{F}} (v - |A| - d) = -d.$$

Adding these equalities yields $(v + 1)(v - 2d) = -2d$, which implies $d = \frac{v+1}{2}$. Let $\mathcal{F} = \{A_1, A_2, \ldots, A_{v+1}\}$. Define the following square matrix $H = [h_{ij}]$ of

order $v+1$:

$$h_{ij} = \begin{cases} 1 & \text{if} \quad j = v+1, \\ 1 & \text{if} \quad 1 \le j \le v \quad \text{and} \quad j \in A_i, \\ -1 & \text{if} \quad 1 \le j \le v \quad \text{and} \quad j \notin A_i. \end{cases} \tag{1.16}$$

Since $|A \triangle B| = d = \frac{v+1}{2}$ for any distinct A and B in $\mathcal{F}$, the inner product of any two distinct rows of H is equal to 0, i.e., H is a Hadamard matrix and therefore $\mathcal{F}$ is a Hadamard family. □

We will return to equidistant families of sets (regarded as binary equidistant codes) in Section 5.5.

Exercises

(1) Let $\mathcal{F}$ be a set of pairwise disjoint subsets of a v-set V.
   (a) Prove that $|\mathcal{F}| \le v+1$.
   (b) Prove that if $|\mathcal{F}| = v+1$, then $\mathcal{F}$ consists of the empty set and all singletons.

(2) For any positive integer n, $\pi(n)$ denotes the number of primes that do not exceed n. Let X be a subset of the set $\{1, 2, \ldots, n\}$ such that the product of all elements of any nonempty subset Y of X is not a square (in particular, no element of X is a square). Prove that $|X| \le \pi(n)$.

(3) Let $\mathcal{F}$ be a set of subsets of a v-set V such that for any distinct $A, B \in \mathcal{F}$, $A \cup B \ne V$. Prove that $|\mathcal{F}| \le 2^{v-1}$. Give an example of a set $\mathcal{F}$ of cardinality 2^{v-1} having this property.

(4) Let $\mathcal{F}$ be a set of subsets of a v-set V such that $A \cap B \ne \varnothing$ for all $A, B \in \mathcal{F}$. Prove that if $|\mathcal{F}| < 2^{v-1}$, then there exists $X \subseteq V$ such that $X \notin \mathcal{F}$ and $X \cap A \ne \varnothing$ for all $A \in \mathcal{F}$.

(5) Let V be a v-set with $v \ge 3$. Prove that there is a set $\mathcal{F}$ of subsets of V such that $A \cap B \ne \varnothing$ for all $A, B \in \mathcal{F}$, $|\mathcal{F}| = 2^{v-1}$, and $\bigcap_{A \in \mathcal{F}} A = \varnothing$.

(6) Let $V = \{1, 2, 3, 4, 5, 6, 7\}$ and

$$\mathcal{B} = \{\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 7\}, \{5, 6, 1\}, \{6, 7, 2\}, \{7, 1, 3\}\}.$$

   Let $\mathcal{F}$ be the set of all subsets of V which contain at least one member of $\mathcal{B}$.
   (a) Find $|\mathcal{F}|$.
   (b) Prove that $A \cap B \ne \varnothing$ for all $A, B \in \mathcal{F}$.

(7) Let $\mathcal{F}$ be a set of subsets of a finite set V such that $|A \cap B|$ is the same for all distinct $A, B \in \mathcal{F}$. Fix $C \in \mathcal{F}$ and define $\mathcal{G} = \{C\} \cup \{A \triangle C \colon A \in \mathcal{F}, A \ne C\}$. Prove that $|A \cap B|$ is the same for all distinct $A, B \in \mathcal{F}$.

(8) Let $(V, \mathcal{F})$ be a symmetric (v, k, λ)-design. Let X be a subset of V such that $|X \cap A|$ is the same for all $A \in \mathcal{F}$. Prove that $X = \varnothing$ or $X = V$.
   Hint: Expand the polynomial $\sum_{i \in X} x_i$ in the basis introduced in the proof of the Ryser–Woodall Theorem.

(9) Let $(V, \mathcal{F})$ be a Ryser design and let X be a subset of V such that $|X \cap A|$ is the same for all $A \in \mathcal{F}$. Prove that $X = \varnothing$.

(10) Let $(V, \mathcal{F})$ be a symmetric (v, k, λ)-design and let $A \in \mathcal{F}$ be a fixed block. Let X be a subset of V such that $|X \cap B|$ is the same for all $B \in \mathcal{F} \setminus \{A\}$. Prove that $X = \varnothing$ or $X = V$ or $X = A$ or $X = V \setminus A$.

(11) Let $(V, \mathcal{F})$ be a Ryser design and let $A \in \mathcal{F}$ be a fixed block. Let X be a subset of V such that $|X \cap B|$ is the same for all $B \in \mathcal{F} \setminus \{A\}$. Prove that $X = \varnothing$ or $X = A$ or $X \supseteq V \setminus A$. Give an example of a Ryser design, a block A, and a subset $X \supset V \setminus A$, $X \neq V \setminus A$ which satisfy the given conditions.

(12) Let $\mathcal{F}$ be an equidistant family of subsets of a v-set V. Let X be a subset of V. Prove that the family $\mathcal{F} \triangle X = \{A \triangle X \colon A \in \mathcal{F}\}$ is also equidistant.

(13) Show that the family of subsets introduced in Example 1.4.5 is equidistant.

(14) A *regular n-simplex* is a set S of $n+1$ points of the n-dimensional real vector space $\mathbb{R}^n$ such that the (Euclidean) distance between any two points of S is the same. Prove that the following two statements are equivalent:
   (a) the set of vertices of an n-dimensional cube contains a regular n-simplex;
   (b) there exists a Hadamard matrix of order $n+1$.

(15) Let $\mathcal{F}$ be an equidistant family of subsets of a v-set V. Suppose that $|\mathcal{F}| = v$. Define linear polynomials f_A, $A \in \mathcal{F}$, as in the proof of Theorem 1.4.3. Prove that if $v \geq 3$, then the set $\{f_A \colon A \in \mathcal{F}\} \cup \{1\}$ is linearly independent. Is this true for $v = 2$?

(16) For a positive integer n, let $k = 1 + \lfloor \frac{2^{n+1}}{n+1} \rfloor$ if there exists a Hadamard matrix of order $n+1$ and $k = 1 + \lfloor \frac{2^{n+1}}{n} \rfloor$ otherwise. Prove that among any k vertices of an n-dimensional cube there are three distinct vertices of an equilateral triangle.

(17) Let V be a set of cardinality v and $\mathcal{F}$ a family of subsets of V such that $|A \cap B|$ takes at most s values for distinct $A, B \in \mathcal{F}$. Prove that $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{v}{i}$.

(18) Let p be a prime and let $V = \{1, 2, , , , .4p\}$. Let $\mathcal{F}$ be a family of subsets of V such that $|A| = 2p$ for all $A \in \mathcal{F}$ and $|A \cap B| \neq p$ for all $A, B \in \mathcal{F}$. Prove that $|\mathcal{F}| \leq 2\binom{4p-1}{p-1}$.
   Hint: with each $A \in \mathcal{F}$, associate a multilinear polynomial f_A^* where $f_A = (\sum_{i \in A} x_i)^{p-1} - 1$ over the field of residue classes modulo p.

(19) Let X be a set of strings $(x_1, x_2, \ldots, x_v)$ of length v of elements of the set $\{0, 1, 2\}$. Suppose that for any distinct $(x_1, x_2, \ldots, x_v), (y_1, y_2, \ldots, y_v) \in X$, there is an index j such that $x_j - y_j \equiv 1 \pmod 3$. Prove that $|X| \leq 2^v$.

Notes

The topic of combinatorics of finite sets is also referred to as extremal set theory. See Bollobás (1986) and Anderson (1987) for an exposition of many famous results and methods in this area.

The technique of estimating the size of a given family of subsets of a finite set using suitable polynomials in a vector space is well known. This approach has been used, for example, by Koornwinder (1976), Delsarte, Goethals, and Seidel (1977), and more recently by Alon, Babai, and Suzuki (1991), Blokhuis (1993), Godsil (1993), Snevily (1994), and Ionin and M. S. Shrikhande (1996a) among others.

Nonuniform Fisher's Inequality was first proved in Majumdar (1953). It is a generalization of Fisher's Inequality for 2-designs considered in Section 2.3. Another proof is in Babai (1987). The proof given in Section 1.1. is adapted from Ionin and M. S. Shrikhande (1996a). The First Ray-Chaudhuri–Wilson Inequality is contained in the seminal paper by Ray-Chaudhuri and Wilson (1975). The proof given in Section 1.2. is due to Alon, Babai, and Suzuki (1991). The last paper also contains nonuniform versions of this inequality.

The Ryser–Woodall Theorem was independently proven by Ryser (1968) and Woodall (1970). The proof of this result given in Section 3 is due to Ionin and M. S. Shrikhande (1996a). The term *Ryser design* is taken from Stanton (1997). Ryser (1968) calls these structures λ-*designs* and Woodall (1970) uses the term λ-*linked designs* for a more general structure. We prefer to call these objects Ryser designs to avoid confusion with common usage of such terms as 2-design, t-design, etc. in design theory.

Theorem 1.4.6 was proven in Delsarte (1973b). Our proof follows that of Ionin and M. S. Shrikhande (1995b). Equidistant families of sets were also studied by Bose and S. S. Shrikhande (1959a) and Semakov and Zinoviev (1968).

For Exercise 17, see Alon, Babai and Suzuki (1991). The result of Exercise 18 is due to Frankl and Wilson (1981). For the polynomial proof of this result and for Exercise (19), see Blokhuis (1993).

2

Introduction to designs

Points and lines in Euclidean plane represent the oldest example of an *incidence structure*. Generally, an incidence structure can be described by two abstract sets (called the *point set* and the *block set*) and a binary relation between points and blocks. Imposing certain regularity conditions on a finite incidence structure leads to the concept of combinatorial designs that includes 2-*designs*, *symmetric designs*, and *graphs*.

2.1. Incidence structures

One of the most general notions in the theory of combinatorial designs is that of an *incidence structure*. It involves two finite sets and a binary relation between their elements.

Definition 2.1.1. A (finite) *incidence structure* is a triple $\mathbf{D} = (X, \mathcal{B}, I)$ where X and $\mathcal{B}$ are nonempty finite sets and $I \subseteq X \times \mathcal{B}$. The sets X and $\mathcal{B}$ are called the *point set* and the *block set* of $\mathbf{D}$, respectively, and their elements are called *points* and *blocks*. The set I is called the *incidence relation*. If $(x, B) \in I$, we will say that point x and block B are incident and that (x, B) is a *flag*.

The number of points incident with a block B is called the *size* or the *cardinality* of B and denoted by $|B|$. If $|B| = |X|$, the block B is said to be *complete*. The number of blocks incident with a point x is called the *replication number* of x (Fig. 2.1) and denoted by $r(x)$. For distinct points x and y, $\lambda(x, y)$ denotes the number of blocks incident with both x and y. An *incidence matrix* of $\mathbf{D}$ is a (0, 1)-matrix whose rows are indexed by the points of $\mathbf{D}$, columns are indexed by the blocks of $\mathbf{D}$, and the (x, B)-entry is equal to 1 if and only if $(x, B) \in I$.

Remark 2.1.2. When we have to actually form an incidence matrix of an incidence structure $\mathbf{D} = (X, \mathcal{B}, I)$ with v points and b blocks, we need

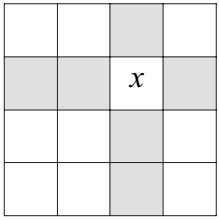

Figure 2.1 Block B_x.

to order the sets X and $\mathcal{B}$. To indicate the chosen ordering, we will write $X = \{x_1, x_2, \ldots, x_v\}$ and $\mathcal{B} = \{B_1, B_2, \ldots, B_b\}$ and refer to the (0, 1)-matrix $N = [n_{ij}]$ with $n_{ij} = 1$ if and only if $(x_i, B_j) \in I$ as the *corresponding incidence matrix* of $\mathbf{D}$.

If N is an incidence matrix of $\mathbf{D}$, then $|B|$ is the sum of the entries of the column of N indexed by B, $r(x)$ is the sum of the entries of the row of N indexed by x, and $\lambda(x, y)$ is the inner product of the rows of N indexed by x and y.

Definition 2.1.3. If an incidence structure $(X, \mathcal{B}, I)$ is such that $\mathcal{B}$ is a set of subsets of X, and $(x, B) \in I$ if and only if $x \in B$, then it will be denoted as $(X, \mathcal{B})$.

For any incidence structure $\mathbf{D} = (X, \mathcal{B}, I)$, we will associate with each block B the set of points incident with B. We will denote this set by the same letter B. With this notation, one should be aware that distinct blocks may have the same set of incident points. Nevertheless, it is convenient to use the set theory notation. For instance, if A and B are blocks of an incidence structure, then $A \cap B$ denotes the set of points incident with both A and B. In the same manner, we will interpret the union $A \cup B$, the difference $A \setminus B$, the symmetric difference $A \triangle B = (A \cup B) \setminus (A \cap B)$, etc. We will often use $x \in B$ or $B \ni x$ instead of $(x, B) \in I$. If Y is a set of points and B is a block, then $Y \subseteq B$ means that every point of Y is incident with B and $B \subseteq Y$ means that every point that is incident with B is in Y.

For an incidence structure $\mathbf{D} = (X, \mathcal{B}, I)$, counting flags in two ways yields the equation

$$\sum_{x \in X} r(x) = \sum_{B \in \mathcal{B}} |B|. \tag{2.1}$$

Fixing a point x and counting in two ways flags (y, B) with $y \neq x$ and $x, y \in B$,

we obtain another basic equation

$$\sum_{\substack{y\in X\\ y\neq x}} \lambda(x, y) = \sum_{\substack{B\in\mathcal{B}\\ B\ni x}} |B| - r(x). \tag{2.2}$$

The notion of a *substructure* of an incidence structure can be defined in a natural way.

Definition 2.1.4. Let $\mathbf{D} = (X, \mathcal{B}, I)$ be an incidence structure. Let X_0 be a nonempty subset of X and $\mathcal{B}_0$ a nonempty subset of $\mathcal{B}$. The incidence structure $\mathbf{D}(X_0, \mathcal{B}_0) = (X_0, \mathcal{B}_0, I \cap (X_0 \times \mathcal{B}_0))$ is said to be a *substructure* of $\mathbf{D}$. If $\mathcal{B}_0 = \mathcal{B}$, we will write $\mathbf{D}(X_0)$ instead of $\mathbf{D}(X_0, \mathcal{B})$.

If N is an incidence matrix of $\mathbf{D}$, then the submatrix of N formed by the rows with indices from X_0 and columns with indices from $\mathcal{B}_0$ is an incidence matrix of $\mathbf{D}(X_0, \mathcal{B}_0)$.

The following two kinds of substructures are of special interest.

Definition 2.1.5. Let $\mathbf{D} = (X, \mathcal{B}, I)$ be an incidence structure and let Y be a proper subset of X. Let $\mathcal{B}^Y = \{B \in \mathcal{B}\colon Y \not\subseteq B\}$ and $\mathcal{B}_Y = \{B \in \mathcal{B}\colon B \not\subseteq Y\}$. If $\mathcal{B}^Y \neq \varnothing$, then the substructure $\mathbf{D}^Y = \mathbf{D}(X \setminus Y, \mathcal{B}^Y)$ is called a *residual substructure* of $\mathbf{D}$. If $\mathcal{B}_Y \neq \varnothing$, then the substructure $\mathbf{D}_Y = \mathbf{D}(Y, \mathcal{B}_Y)$ is called a *derived substructure* of $\mathbf{D}$. If Y is the set of all points incident with a block B, then we write $\mathbf{D}^B$ and $\mathbf{D}_B$ instead of $\mathbf{D}^Y$ and $\mathbf{D}_Y$ and call these substructures *block-residual* and *block-derived*, respectively. If x is a point, then we put $\mathbf{D}^x = \mathbf{D}^{\{x\}}$ and $\mathbf{D}_x = \mathbf{D}_{X\setminus\{x\}}$ and call these substructures *point-residual* and *point-derived*, respectively.

The next proposition characterizing incidence matrices of residual and derived substructures is immediate. In this proposition we denote by J the all-one matrix of an appropriate size. The following is a list of notations that will be used throughout this book without further explanation.

I	the identity matrix
J	the all-one matrix
I_n	the identity matrix of order n
J_n	the all-one matrix of order n
$J_{m,n}$	the $m \times n$ all-one matrix
O	the zero matrix
$A^\top$	the transpose of matrix A
$\mathbf{a}, \mathbf{b}, \mathbf{x}$	column vectors
$\mathbf{0}$	the zero column vector
$\mathbf{j}$	the all-one column vector

Proposition 2.1.6. *Let* $\mathbf{D} = (X, \mathcal{B}, I)$ *be an incidence structure and let* Y *be a proper subset of* X. *A matrix* M^Y *is an incidence matrix of* $\mathbf{D}^Y$ *if and only if there is an incidence matrix* M *of* $\mathbf{D}$ *that can be represented as a block matrix*

$$M = \begin{bmatrix} M^Y \\ P \end{bmatrix} \text{ or } M = \begin{bmatrix} M^Y & Q \\ P & J \end{bmatrix}.$$

A matrix N_Y *is an incidence matrix of* $\mathbf{D}_Y$ *if and only if there is an incidence matrix* N *of* $\mathbf{D}$ *that can be represented as a block matrix*

$$N = \begin{bmatrix} R \\ N_Y \end{bmatrix} \text{ or } N = \begin{bmatrix} R & O \\ N_Y & S \end{bmatrix}.$$

From a given incidence structure $\mathbf{D}$, we can define the *s-fold multiple* of $\mathbf{D}$ by repeating every block s times, the *complementary* structure by replacing every block by its complement, and the *dual* incidence structure by interchanging points and blocks.

Definition 2.1.7. Let $\mathbf{D} = (X, \mathcal{B}, I)$ be an incidence structure and s a positive integer. Let $\mathcal{B} = \{B_1, B_2, \ldots, B_b\}$. The *s-fold multiple of* $\mathbf{D}$ is the incidence structure $s \times \mathbf{D} = (X, s \times \mathcal{B}, I_s)$, where $s \times \mathcal{B} = \{B_{ij} : 1 \leq i \leq b, 1 \leq j \leq s\}$ and $(x, B_{ij}) \in I_s$ if and only if $(x, B_i) \in I$.

Definition 2.1.8. Let $\mathbf{D} = (X, \mathcal{B}, I)$ be an incidence structure. The *complementary incidence structure* is $\mathbf{D}' = (X, \mathcal{B}, I')$ where $(x, B) \in I'$ if and only if $(x, B) \notin I$.

Definition 2.1.9. Let $\mathbf{D} = (X, \mathcal{B}, I)$ be an incidence structure. The *dual incidence structure* is $\mathbf{D}^\top = (\mathcal{B}, X, I^*)$ where $(B, x) \in I^*$ if and only if $(x, B) \in I$.

If N is an incidence matrix of $\mathbf{D}$, then $N^\top$ is an incidence matrix of $\mathbf{D}^\top$ and $J - N$ is an incidence matrix of $\mathbf{D}'$.

The same incidence structure may be described in several ways. In order to make this concept precise, we define *isomorphism* between incidence structures.

Definition 2.1.10. Incidence structures $\mathbf{D}_1 = (X_1, \mathcal{B}_1, I_1)$ and $\mathbf{D}_2 = (X_2, \mathcal{B}_2, I_2)$ are called *isomorphic* if there exists a pair of bijections $f : X_1 \to X_2$ and $g : \mathcal{B}_1 \to \mathcal{B}_2$ such that $(x, B) \in I_1$ if and only if $(f(x), g(B)) \in I_2$.

If an incidence structure admits a symmetric incidence matrix, it is isomorphic to its dual. Such an incidence structure is called *self-dual*.

Definition 2.1.11. An incidence structure $\mathbf{D}$ is called *self-dual* if $\mathbf{D}$ and $\mathbf{D}^\top$ are isomorphic incident structures.

The following example of isomorphic incidence structures is an immediate corollary of Proposition 2.1.6.

Proposition 2.1.12. *Let $\mathbf{D} = (X, \mathcal{B}, I)$ be an incidence structure and let $\mathbf{D}'$ be the complementary incidence structure. Let Y be a proper subset of X. If the residual substructure $\mathbf{D}^Y$ of $\mathbf{D}$ is defined, then the complementary structure $(\mathbf{D}^Y)'$ is isomorphic to the derived substructure $(\mathbf{D}')_{X\setminus Y}$ of $\mathbf{D}'$. If the derived substructure $\mathbf{D}_Y$ of $\mathbf{D}$ is defined, then the complementary structure $(\mathbf{D}_Y)'$ is isomorphic to the residual substructure $(\mathbf{D}')^{X\setminus Y}$ of $\mathbf{D}'$.*

Two (0, 1)-matrices N_1 and N_2 are incidence matrices of isomorphic incidence structures if and only if there exist permutation matrices P and Q such that $PN_1 = N_2Q$.

Proposition 2.1.13. *Let N_1 and N_2 be $v \times b$ incidence matrices of isomorphic incidence structures $\mathbf{D}_1 = (X_1, \mathcal{B}_1, I_1)$ and $\mathbf{D}_2 = (X_2, \mathcal{B}_2, I_2)$ and let bijections $f\colon X_1 \to X_2$ and $g\colon \mathcal{B}_1 \to \mathcal{B}_2$ be such that $(x, B) \in I_1$ if and only if $(f(x), g(B)) \in I_2$. For $k = 1$ and 2, for $i = 1, 2, \ldots, v$, and for $j = 1, 2, \ldots, b$, let x_i^k and B_j^k be the point and the block of X_k corresponding to the i^{th} row and to the j^{th} column of N_k, respectively. Let (0, 1)-matrices $P = [p_{ij}]$ of order v and $Q = [q_{ij}]$ of order b be defined by:*

$$p_{ij} = 1 \text{ if and only if } x_i^2 = f(x_j^1),$$
$$q_{ij} = 1 \text{ if and only if } B_i^2 = g(B_j^1).$$

Then $PN_1 = N_2Q$.

Proof. For $k = 1, 2$, let $N_k = [n_{ij}^{(k)}]$. For $i = 1, 2, \ldots, v$ and $j = 1, 2, \ldots, b$, the (i, j)-entry of PN_1 is equal to $n_{sj}^{(1)}$ with $x_i^2 = f(x_s^1)$, so it is equal to 1 if and only if $(x_i^2, g(B_j^1)) \in I_2$. Similarly, the (i, j)-entry of N_2Q is equal to $n_{it}^{(2)}$ with $B_t^2 = g(B_j^1)$, so it is equal to 1 if and only if $(x_i^2, g(B_j^1)) \in I_2$. Therefore, $PN_1 = N_2Q$. □

Remark 2.1.14. Note that the matrices P and Q defined in Proposition 2.1.13 are *permutation matrices*, that is, (0, 1)-matrices with exactly one entry equal to 1 in each row and each column.

Remark 2.1.15. The converse of Proposition 2.1.13 is also true. See Exercise 3

2.2. Graphs

The basic concepts of graph theory are used in many areas of combinatorics. A *graph* is determined by a set of points called *vertices* and a set of 2-subsets of the set of vertices called *edges*. All graphs under consideration are without multiple edges. Therefore, as incidence structures, they do not have repeated blocks.

Definition 2.2.1. A *graph* is a pair $\Gamma = (V, E)$ where V is a nonempty finite set (of *vertices*) and E is a set of 2-subsets of V (*edges*). If $\{x, y\}$ is an edge, then vertices x and y are said to be *adjacent*. The cardinality of V is called the *order* of Γ. For each vertex $x \in V$, $\Gamma(x)$ denotes the set of all vertices y such that $\{x, y\}$ is an edge. The cardinality of $\Gamma(x)$ is called the *degree* or *valency* of x. If all vertices of a graph are of the same degree k, then the graph is said to be *regular of degree* k.

Example 2.2.2. For $n \geq 3$, the graph C_n with vertices $x_1, x_2, \ldots, x_n$ and edges $\{x_i, x_{i+1}\}$, for $i = 1, \ldots, n-1$, and $\{x_n, x_1\}$ is called a *cycle of length* n. It is regular of degree 2.

Definition 2.2.3. A graph $\Gamma = (V, E)$ is called a *null graph* if $E = \varnothing$. A graph $\Gamma = (V, E)$ is called a *complete graph* if E is the set of all 2-subsets of V. The complete graph of order n is denoted by K_n. A graph $\Gamma = (V, E)$ is called *bipartite* if there is a partition of the vertex set V into two nonempty subsets such that no two vertices from the same partition set form an edge. A regular bipartite graph of degree 1 is called a *ladder graph*. A graph $\Gamma' = (V', E')$ is called a *subgraph* of a graph $\Gamma = (V, E)$ if $V' \subseteq V$ and $E' \subseteq E$. The subgraph Γ' is called an *induced subgraph* if E' is the set of all elements of E that are contained in V'. An induced subgraph Γ' of a graph Γ is called a *clique* if Γ' is a complete graph. An induced subgraph Γ' of a graph Γ is called a *coclique* if Γ' is a null graph. The set of vertices of a clique or a coclique is usually referred to by the same name.

With any incidence structure we associate a bipartite graph called the *Levi graph* of the structure.

Definition 2.2.4. Let $\mathbf{D} = (X, I, \mathcal{B})$ be an incidence structure with disjoint sets X and $\mathcal{B}$. The *Levi graph* of $\mathbf{D}$ is the graph with the vertex set $X \cup \mathcal{B}$ and all edges $\{x, B\}$ such that $(x, B) \in I$.

A graph $\Gamma = (V, E)$ can be regarded as a partition of the set of all 2-subsets of V into two sets: the set E of edges and the set of *non-edges*. Replacing the former set by the latter yields *the complement of the graph*.

Definition 2.2.5. The *complement* of a graph $\Gamma = (V, E)$ is the graph $\Gamma' = (V, E')$ where E' is the set of all 2-subsets of V that are not edges of Γ.

The next definition introduces some basic notions of graph theory.

Definition 2.2.6. A *walk* from a vertex x to a vertex y of a graph $\Gamma = (V, E)$ is a sequence $(x_0, x_1, \ldots, x_n)$ of vertices such that $x_0 = x$, $x_n = y$, and $\{x_{i-1}, x_i\}$ is an edge for $i = 1, 2, \ldots, n$. The number n is the *length* of the walk. The binary relation on V, given by $x \sim y$ if and only if $x = y$ or there is a walk from x to y, is an equivalence relation. If $V_1, V_2, \ldots, V_m$ are the equivalence classes, then the graphs $\Gamma_i = (V_i, E_i)$ where $E_i = \{e \in E : e \subseteq V_i\}$ are called *connected components of* Γ. A graph with only one connected component is called a *connected graph*.

We leave proof of the following proposition as an exercise.

Proposition 2.2.7. *If Γ' is the complement of a graph Γ, then at least one of these graphs is connected.*

Graphs with disjoint vertex sets can be combined into a larger graph.

Definition 2.2.8. Let $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$ be graphs with $V_1 \cap V_2 = \varnothing$. The graph $\Gamma = (V_1 \cup V_2, E_1 \cup E_2)$ is called the *disjoint union* of the graphs Γ_1 and Γ_2. For positive integers m and n, the disjoint union of m copies of K_n is denoted by $m \cdot K_n$; its complement is called a *complete multipartite graph* and denoted $K_{m,n}$.

A graph can be represented via its *adjacency matrix*.

Definition 2.2.9. If $V = \{x_1, x_2, \ldots, x_v\}$ is the vertex set of a graph Γ, then the *corresponding adjacency matrix* of Γ is the $v \times v$ matrix whose (i, j) entry is equal to 1 if $\{x_i, x_j\}$ is an edge of Γ, and is equal to 0 otherwise.

A (0, 1)-matrix is an adjacency matrix of a graph if and only if it is symmetric and has zero diagonal. The following proposition can be proved by straightforward induction.

Proposition 2.2.10. *Let Γ be a graph with the vertex set $V = \{x_1, x_2, \ldots, x_v\}$ and let A be the corresponding adjacency matrix. For any positive integer k, A^k is the matrix whose (i, j) entry is equal to the number of walks of length k from vertex x_i to vertex x_j.*

If A is an adjacency matrix of a graph Γ on v vertices and J is the all-one matrix of order v, then the (i, j)-entry of AJ is the valency of x_i and the

(i, j)-entry of JA is the valency of x_j. Therefore, Γ is regular if and only if $AJ = JA$. It is regular of degree k if and only if $AJ = kJ$.

If A and B are adjacency matrices of a graph Γ, then one can be obtained from the other by a suitable permutation of vertices of Γ, that is, there exists a permutation matrix P such that $B = P^\top AP$. Since permutation matrices are orthogonal, the matrices A and B have the same characteristic polynomial $\chi(\Gamma)$, which therefore can be called the *characteristic polynomial of the graph* Γ. If A is an adjacency matrix of Γ, then $\chi(\Gamma)(t) = \det(tI - A)$. The roots of $\chi(\Gamma)$ are *the eigenvalues of* Γ. The *spectrum of* Γ is the multiset of its eigenvalues taken with their respective multiplicities. Note that since adjacency matrices of graphs are symmetric matrices with zeros on the diagonal, the spectrum of any graph consists of real numbers whose sum is equal to 0. If a graph Γ has m connected components $\Gamma_1, \Gamma_2, \ldots, \Gamma_m$, then $\chi(\Gamma) = \chi(\Gamma_1)\chi(\Gamma_2)\cdots\chi(\Gamma_m)$.

Example 2.2.11. By Lemma 2.3.6, $\chi(K_n)(t) = (t - n + 1)(t + 1)^{n-1}$ and $\chi(m \cdot K_n)(t) = ((t - n + 1)(t + 1)^{n-1})^m$.

If A is an adjacency of a graph Γ, then s is an eigenvalue of Γ if and only if there exists a nonzero (column) vector $\mathbf{x}$ such that $A\mathbf{x} = s\mathbf{x}$. The vector $\mathbf{x}$ is called an *eigenvector of A corresponding to s*. All eigenvectors of A corresponding to s together with the zero vector $\mathbf{0}$ form the *eigenspace of A corresponding to s*.

The spectrum of a graph may provide useful information about the graph. For instance, the largest eigenvalue of a regular graph is the degree of the graph. In the proof of this and other results involving eigenvalues of graphs, we will use the following three results on symmetric matrices the first two of which can be found in standard linear algebra texts.

Proposition 2.2.12. *If A is a real symmetric matrix, then the dimension of the eigenspace of A corresponding to a given eigenvalue is equal to the multiplicity of this eigenvalue. If $\mathbf{x}$ and $\mathbf{y}$ are eigenvectors of A corresponding to two different eigenvalues, then $\mathbf{x}^\top\mathbf{y} = [0]$.*

Proposition 2.2.13. *If $A_1, A_2, \ldots, A_m$ are real symmetric matrices, any two of which commute, then there exists an orthogonal matrix C such that all matrices $C^\top A_i C$ $(i = 1, 2, \ldots, m)$ are diagonal matrices.*

Proposition 2.2.14. *For any matrix N, every nonzero eigenvalue of $NN^\top$ is also an eigenvalue of $N^\top N$ with the same multiplicity.*

Proof. Let s be a nonzero eigenvalue of NN^T, i.e., $NN^T\mathbf{x} = s\mathbf{x}$ for some nonzero vector $\mathbf{x}$. Then

$$N^\top\mathbf{x} \neq \mathbf{0} \quad \text{and} \quad (N^\top N)(N^\top\mathbf{x}) = s(N^\top\mathbf{x})$$

so s is an eigenvalue of N^TN with the nonzero eigenvector $N^\top\mathbf{x}$. The multiplicity of an eigenvalue of a symmetric matrix is equal to the dimension of the corresponding eigenspace. Let $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m$ be linearly independent eigenvectors corresponding to an eigenvalue $s \neq 0$ of NN^T. Then the corresponding eigenvectors $N^\top\mathbf{x}_1, N^\top\mathbf{x}_2, \ldots, N^\top\mathbf{x}_m$ of $N^\top N$ are also linearly independent. Indeed, if $\sum_{i=1}^m \alpha_i N^\top\mathbf{x}_i = \mathbf{0}$, then $\sum_{i=1}^m \alpha_i NN^T\mathbf{x}_i = \mathbf{0}$, so $\sum_{i=1}^m \alpha_i s\mathbf{x}_i = \mathbf{0}$, $\sum_{i=1}^m \alpha_i\mathbf{x}_i = \mathbf{0}$, and all α_i are equal to 0. Thus, each nonzero eigenvalue of NN^T is an eigenvalue of N^TN with at least the same multiplicity. By interchanging N and N^T, we complete the proof. □

Corollary 2.2.15. *If N is a $v \times b$ matrix with $v \leq b$, then the spectrum of $N^\top N$ can be obtained by adjoining $b - v$ zeros to the spectrum of $NN^\top$.*

If Γ is a regular graph of degree k and A is an adjacency matrix of Γ, then $AJ = kJ$, so k is an eigenvalue of Γ with an eigenvector $\mathbf{j}$. Proposition 2.2.12 implies that if $\mathbf{x}$ is an eigenvector of Γ corresponding to an eigenvalue other than k, then $J\mathbf{x} = \mathbf{0}$.

The following proposition gives a relation between eigenvalues of a regular graph and of its complement.

Proposition 2.2.16. *Let Γ be a regular graph of order v and degree k and let s be an eigenvalue of Γ other than k. Then $-s - 1$ is an eigenvalue of the complementary graph $\overline{\Gamma}$ and the multiplicity of s in Γ does not exceed the multiplicity of $-s - 1$ in $\overline{\Gamma}$. Furthermore, these multiplicities are the same if and only if $s \neq k - v$.*

Proof. Let A be an adjacency matrix of Γ and let $A\mathbf{x} = s\mathbf{x}$. Then $J - A - I$ is an adjacency matrix of $\overline{\Gamma}$ and $(J - A - I)\mathbf{x} = (-s - 1)\mathbf{x}$. Thus, $-s - 1$ is an eigenvalue of $\overline{\Gamma}$. Furthermore, the eigenspace U of A corresponding to s is contained in the eigenspace $\overline{U}$ of $J - A - I$ corresponding to the eigenvalue $-s - 1$ of $\overline{\Gamma}$. Therefore, the multiplicity of s in Γ does not exceed the multiplicity of $-s - 1$ in $\overline{\Gamma}$.

If $s = k - v$, then $-s - 1$ is the degree of $\overline{\Gamma}$, so $\mathbf{j} \in \overline{U}$ and $\dim(\overline{U}) > \dim(U)$. If $s \neq k - v$, then $-s - 1$ is an eigenvalue of $\overline{\Gamma}$ other than the degree of $\overline{\Gamma}$ and therefore, by the first part of the proof, $\dim(\overline{U}) \leq \dim(U)$, so the multiplicities of s and $-s - 1$ are the same. □

The degree of a regular graph is its largest eigenvalue.

Proposition 2.2.17. *If Γ is a regular graph of degree k with m connected components, then k is an eigenvalue of Γ of multiplicity m. If s is any eigenvalue of Γ, then $|s| \leq k$.*

Proof. First assume that $m = 1$, i.e., that Γ is a connected regular graph of degree k with the vertex set $\{x_1, x_2, \ldots, x_v\}$. Let A be the corresponding adjacency matrix of Γ. Then $AJ = kJ$ and therefore k is an eigenvalue of A with the all-one eigenvector $\mathbf{j}$.

Let $\mathbf{x} = [\alpha_1, \alpha_2, \ldots, \alpha_v]^\top$ be any nonzero vector such that $A\mathbf{x} = k\mathbf{x}$. Then (for $j = 1, 2, \ldots, v$) $k\alpha_j$ is the sum of all α_i such that x_i is adjacent to x_j. Let α_m be an entry of $\mathbf{x}$ with the largest absolute value. Then $\alpha_i = \alpha_m$ for all i such that x_i is adjacent to x_m. Since Γ is connected, this implies that all components of $\mathbf{x}$ are equal. Therefore, the eigenspace of A corresponding to k is one-dimensional and k is a simple eigenvalue of Γ.

Let s be any eigenvalue of Γ. Let $\mathbf{y}$ be an eigenvector corresponding to s and let β_m be a component of $\mathbf{y}$ with the largest absolute value. Since $A\mathbf{y} = s\mathbf{y}$, we obtain that $s\beta_m$ is the sum of k components of $\mathbf{y}$ and therefore $|s||\beta_m| \leq k|\beta_m|$, which implies $|s| \leq k$.

Suppose now that Γ has $m > 1$ connected components $\Gamma_1, \Gamma_2, \ldots, \Gamma_m$. Then each Γ_i is a connected graph of degree k. Therefore, k is a simple root of each polynomial $\chi(\Gamma_i)$, $i = 1, 2, \ldots, m$, and so it is a root of multiplicity m of $\chi(\Gamma)$. If s is another eigenvalue of Γ, then s is an eigenvalue of at least one Γ_i and therefore $|s| \leq k$. □

The following theorem gives some information on other eigenvalues of a regular graph.

Theorem 2.2.18. *Let A be an adjacency matrix of a connected regular graph of order v and degree k and let p be a polynomial with real coefficients. Then $p(A) = J$ if and only if $p(k) = v$ and $p(s) = 0$ for all eigenvalues s of Γ, other than k.*

Proof. Since $AJ = JA = kJ$, matrices A and J commute. Therefore, there exists an orthogonal matrix C such that $C^\top AC = D$ and $C^\top JC = E$ are diagonal matrices. Since the matrix J of order v has a simple eigenvalue v and an eigenvalue 0 of multiplicity $v - 1$, we assume without loss of generality that the $(1, 1)$-entry of E is v and all other entries are zeros.

Let $\mathbf{x} = C^\top \mathbf{j}$, so $C\mathbf{x} = \mathbf{j}$. Then $E\mathbf{x} = v\mathbf{x}$, which implies that $\mathbf{x} = [x_1, 0, \ldots, 0]^\top$. Since $D\mathbf{x} = k\mathbf{x}$, we obtain that the $(1, 1)$-entry of D is k.

Let p be a polynomial over the reals. Then $p(D) = C^\top p(A)C$. If $p(A) = J$, then $p(D) = E$, so $p(k) = v$ and $p(s) = 0$ for all eigenvalues s of Γ other than k.

Conversely, if $p(s) = 0$ for all these eigenvalues and $p(k) = v$, then $p(D) = E$, which implies $p(A) = J$. □

The next two propositions characterize graphs with one eigenvalue and regular graphs with two eigenvalues.

Proposition 2.2.19. *The only graphs with one eigenvalue are null graphs.*

Proof. If a graph Γ on v vertices with an adjacency matrix A has only one eigenvalue s, then $A\mathbf{x} = s\mathbf{x}$ for all vectors $x \in \mathbb{Q}^v$. In particular $A\mathbf{j} = s\mathbf{j}$, which implies that Γ is a regular graph of degree s. Now Proposition 2.2.17 implies that Γ has v connected components and therefore it is a null graph. □

Proposition 2.2.20. *A regular graph has two eigenvalues if and only if it is a K_n or a $m \cdot K_n$.*

Proof. As Example 2.2.11 shows, all graphs K_n and $m \cdot K_n$ have two eigenvalues.

Let Γ be a connected regular graph of order v and degree k with two eigenvalues, k and s. Let A be an adjacency matrix of Γ. By Proposition 2.2.17, k is a simple eigenvalue and then s is an eigenvalue of multiplicity $v - 1$. Therefore, we have $k + (v - 1)s = 0$. Let $p(t) = (s - t)/s$. Then $p(k) = v$ and $p(s) = 0$, and Theorem 2.2.18 implies that $p(A) = J$. Therefore, $A = s(I - J)$. Since A is a $(0, 1)$-matrix, we have $s = -1$ and $A = J - I$. Thus, $\Gamma = K_v$.

If Γ is a regular graph of order v with two eigenvalues, having $m > 1$ connected components, then each component is a complete graph. Therefore, $\Gamma = m \cdot K_{v/m}$. □

2.3. Basic properties of (v, b, r, k, λ)-designs

We will now impose certain regularity conditions on incidence structures.

Definition 2.3.1. A (v, b, r, k, λ)-design is an incidence structure $\mathbf{D} = (X, \mathcal{B}, I)$ satisfying the following conditions: (i) $|X| = v$; (ii) $|\mathcal{B}| = b$; (iii) $r(x) = r$ for all $x \in X$; (iv) $|B| = k$ for all $B \in \mathcal{B}$; (v) $\lambda(x, y) = \lambda$ for all distinct $x, y \in X$; (vi) if $I = \varnothing$ or $I = X \times \mathcal{B}$, then $v = b$.

Remark 2.3.2. Parameters v and b of a (v, b, r, k, λ)-design are positive integers; parameters r and k are nonnegative integers; if $v > 1$, then λ is a nonnegative integer; if $v = 1$, then λ is irrelevant. An incidence matrix of a (v, b, r, k, λ)-design is a $v \times b$ matrix with constant row sum r, constant column sum k, and constant inner product λ of distinct rows. If it is the all-zero

or all-one matrix, then (vi) implies that it is a square matrix. The designs with incidence matrices O and J have parameters $(v, v, 0, 0, 0)$ and (v, v, v, v, v), respectively. We will call these designs *trivial*. If $v = 1$, then condition (vi) of Definition 2.3.1 implies that $b = 1$.

We now give several examples of (v, b, r, k, λ)-designs.

Example 2.3.3. Let $v \geq k \geq 2$ and let $\mathbf{D} = (X, \mathcal{B})$, where X is a set of cardinality v and $\mathcal{B}$ is the set of all k-subsets of X. Then $\mathbf{D}$ is a $(v, \binom{v}{k}, \binom{v-1}{k-1}, k, \binom{v-2}{k-2})$-design. Such a design is called *complete*.

Example 2.3.4. Let $X = \{1, 2, 3, 4, 5, 6\}$ and $\mathcal{B} = \{\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 5\}, \{1, 4, 6\}, \{1, 5, 6\}, \{2, 3, 6\}, \{2, 4, 5\}, \{2, 5, 6\}, \{3, 4, 5\}, \{3, 4, 6\}\}$. Then $\mathbf{D} = (X, \mathcal{B})$ is a $(6, 10, 5, 3, 2)$-design.

Incidence structures introduced in Examples 1.3.1 and 1.3.3 are in fact a $(7, 7, 3, 3, 1)$-design and a $(16, 16, 6, 6, 2)$-design, respectively.

If N is an incidence matrix of a (v, b, r, k, λ)-design, then it is a $v \times b$ matrix and properties (iii) – (v) can be expressed in the form of matrix equations:

$$NJ = rJ,\ JN = kJ,\ NN^\top = (r - \lambda)I + \lambda J. \tag{2.3}$$

The complement and s-fold multiple of a (v, b, r, k, λ)-design are a $(v, b, b - r, v - k, b - 2r + \lambda)$ and a $(v, sb, sr, k, s\lambda)$-design, respectively.

Definition 2.3.5. The *order* of a (v, b, r, k, λ)-design with $v > 1$ is the non-negative integer $r - \lambda$.

Observe that a design and its complement have the same order.

If N is an incidence matrix of a (v, b, r, k, λ)-design, then the matrix $NN^\top$ is of the form $xI + yJ$. It is useful to know the determinant of such matrices.

Lemma 2.3.6. *For any real numbers x and y,* $\det(xI + yJ) = (x + ny)x^{n-1}$.

Proof. Let $A = xI + yJ$. We add to the first row of A all other rows to make all entries in the first row equal to $x + ny$. Factoring $x + ny$ out and then subtracting y times the first row from every other row yields a matrix with zeros below the diagonal and with the first diagonal entry equal to 1 and the other $n - 1$ diagonal entries equal to x. Therefore, $\det(xI + yJ) = (x + ny)x^{n-1}$. □

For a (v, b, r, k, λ)-design, equations (2.1) and (2.2) imply immediately the following result.

Proposition 2.3.7. *If $\mathbf{D} = (X, \mathcal{B}, I)$ is a (v, b, r, k, λ)-design, then*

$$vr = bk \tag{2.4}$$

and

$$\lambda(v-1) = r(k-1). \tag{2.5}$$

The following proposition introduces a simple but very useful counting technique known as *variance counting*.

Proposition 2.3.8. *Let* $\mathbf{D} = (X, \mathcal{B})$ *be a* (v, b, r, k, λ)*-design and let* $A \in \mathcal{B}$*. For* $i = 0, 1, \ldots, k$*, let* n_i *denote the number of blocks* $B \in \mathcal{B} \setminus \{A\}$ *such that* $|A \cap B| = i$*. Then*

$$\sum_{i=0}^{k} n_i = b - 1, \tag{2.6}$$

$$\sum_{i=0}^{k} i n_i = k(r-1), \tag{2.7}$$

and

$$\sum_{i=0}^{k} i(i-1) n_i = k(k-1)(\lambda - 1). \tag{2.8}$$

Proof. Eq. (2.6) is obvious. Counting in two ways pairs (x, B) with $B \in \mathcal{B} \setminus \{A\}$ and $x \in A \cap B$ yields (2.7). Counting in two ways triples (x, y, B) with $B \in \mathcal{B} \setminus \{A\}$, $x \neq y$, and $x, y \in A \cap B$ yields (2.8). □

Property (vi) of Definition 2.3.1 allows us to avoid exceptions in the following classical result.

Theorem 2.3.9 (Fisher's Inequality). *For any* (v, b, r, k, λ)*-design, the number of points does not exceed the number of blocks, i.e.,* $v \leq b$*.*

Proof. Let $\mathbf{D} = (X, \mathcal{B}, I)$ be a (v, b, r, k, λ)-design. For each $x \in X$, let $\mathcal{B}_x$ denote the set of all blocks $B \in \mathcal{B}$ incident with x. If $\mathcal{B}_x = \mathcal{B}_y$ for distinct points $x, y \in X$, then $\lambda = r$ and (2.5) implies that either $r = 0$ or $v = k$. Then $I = \varnothing$ or $I = X \times \mathcal{B}$, and therefore $v = b$. Thus, we may assume that $\mathcal{B}_x \neq \mathcal{B}_y$ for any distinct points $x, y \in X$. Condition (v) of Definition 2.3.1 implies that $|\mathcal{B}_x \cap \mathcal{B}_y| = \lambda$ for any distinct $x, y \in X$. If $\lambda = 0$ and $r \neq 0$, then (2.5) implies that $k = 1$, so sets $\mathcal{B}_x$ are distinct singletons, and then $v \leq b$. If $\lambda > 0$, then Non-Uniform Fisher's Inequality applied to the family $\{\mathcal{B}_x : x \in X\}$ of subsets of $\mathcal{B}$ yields $v \leq b$. □

Remark 2.3.10. Another proof of Fisher's Inequality is proposed in Exercise 26.

Remark 2.3.11. Equations (2.4) and (2.5) and Fisher's Inequality are not sufficient for the existence of a (v, b, r, k, λ)-design. For instance, there is no $(22, 22, 7, 7, 2)$-design (see Remark 2.4.11) or a $(15, 21, 7, 5, 2)$-design (Corollary 8.2.21). However, for $k \leq 5$, these conditions are sufficient with the only exception of the parameter set $(15, 21, 7, 5, 2)$. The smallest unresolved parameter set for (v, b, r, k, λ)-designs is $(46, 69, 9, 6, 1)$.

Equations (2.4) and (2.5) indicate that some of the conditions of Definition 2.3.1 may imply the other conditions. The following three propositions confirm it.

Proposition 2.3.12. *Let* $\mathbf{D} = (X, \mathcal{B}, I)$ *be an incidence structure satisfying conditions* (i), (iv), (v), *and* (vi) *of Definition 2.3.1. If* $k \geq 2$, *then* $\mathbf{D}$ *is a* (v, b, r, k, λ)*-design with* $r = \lambda(v-1)/(k-1)$ *and* $b = vr/k$.

Proof. For the incidence structure $\mathbf{D}$, equation (2.2) reads $\lambda(v-1) = r(x)(k-1)$. Therefore, $r(x) = r = \lambda(v-1)/(k-1)$ is the same for all $x \in X$, so $\mathbf{D}$ is a (v, b, r, k, λ)-design, and then (2.1) implies that $b = vr/k$. □

Proposition 2.3.13. *Let* $\mathbf{D} = (X, \mathcal{B}, I)$ *be an incidence structure satisfying conditions* (i), (ii), (iii), (v), *and* (vi) *of Definition 2.3.1. Suppose further that there exists a real number* k *satisfying equations* (2.4) *and* (2.5). *Then* $\mathbf{D}$ *is a* (v, b, r, k, λ)*-design.*

Proof. For the incidence structure $\mathbf{D}$, equations (2.2) and (2.5) imply that

$$\sum_{B \ni x} |B| = \lambda(v-1) + r = rk.$$

Since $\sum_{B \in \mathcal{B}} |B|^2 = \sum_{x \in X} \sum_{B \ni x} |B|$, equation (2.4) implies that

$$\sum_{B \in \mathcal{B}} |B|^2 = vrk = bk^2.$$

Since $\sum_{B \in \mathcal{B}} |B| = vr = bk$, we obtain that

$$\sum_{B \in \mathcal{B}} (|B| - k)^2 = bk^2 - 2bk^2 + bk^2 = 0,$$

and $|B| = k$ for all $B \in \mathcal{B}$. Therefore, $\mathbf{D}$ is a (v, b, r, k, λ)-design. □

Proposition 2.3.14. *Let* $\mathbf{D} = (X, \mathcal{B}, I)$ *be an incidence structure satisfying conditions* (i) – (iv) *and* (vi) *of Definition 2.3.1. Suppose further that there exists a nonnegative integer* λ *such that* $(v-1)\lambda = r(k-1)$ *and* (i) *any two points of* $\mathbf{D}$ *are incident with at most* λ *blocks or* (ii) *any two points of* $\mathbf{D}$ *are incident with at least* λ *blocks. Then* $\mathbf{D}$ *is a* (v, b, r, k, λ)*-design.*

Proof. Fixing a point $x \in X$ and counting flags (y, B) where x is incident with B yields either $(v-1)\lambda \geq r(k-1)$ or $(v-1)\lambda \leq r(k-1)$, respectively. Since, in fact, $(v-1)\lambda = r(k-1)$, we obtain that in either case there are exactly λ blocks containing $\{x, y\}$. Therefore, **D** is a (v, b, r, k, λ)-design. □

Proposition 2.3.12 allows us to give the following definition.

Definition 2.3.15. An incidence structure **D** satisfying conditions (i) – (v) of Definition 2.3.1 is called a 2-(v, k, λ) design if $k \geq 2$.

Remark 2.3.16. A more general notion of a t-(v, k, λ) design is considered in Section 6.1

Remark 2.3.17. Since two points of a block are contained in at least one block, we have $\lambda \geq 1$ for any 2-(v, k, λ) design.

2.4. Symmetric designs

Symmetric designs, the main subject of this book, were described informally in Chapter 1. We will now give a formal definition.

Definition 2.4.1. A *symmetric* (v, k, λ)*-design* is a (v, v, k, k, λ)-design.

Clearly, the complement of a symmetric (v, k, λ)-design is a symmetric $(v, v-k, v-2k+\lambda)$-design.

Proposition 2.3.7 yields the following basic relation for symmetric designs.

Proposition 2.4.2. *For any symmetric* (v, k, λ)*-design,*

$$\lambda(v-1) = k(k-1). \tag{2.9}$$

The Fano Plane (Example 1.3.1) is a symmetric $(7, 3, 1)$-design. Trivial designs (with incidence matrices O and J) are symmetric designs with parameters $(v, 0, 0)$ and (v, v, v), respectively. The block set of a symmetric $(v, 1, 0)$-design consists of all singletons of a v-set, and the block set of a symmetric $(v, v-1, v-2)$-design consists of all $(v-1)$-subsets of a v-set. Example 1.3.3 describes a symmetric $(16, 6, 2)$-design.

Example 2.4.3. Let a 6×6 array L contain each of the digits 1, 2, 3, 4, 5, and 6 in each row and in each column. (Such an array is called a *Latin square of order* 6.) Let $L(i, j)$ be the (i, j)-entry of L. Define the point set X to consist of the ordered pairs (i, j) with $i, j = 1, 2, 3, 4, 5, 6$. For each $x = (i, j) \in X$, define B_x to be the set of points (l, m), other than x, such that $l = i$ or $m = j$

or $L(l, m) = L(i, j)$. Let $\mathcal{B} = \{B_x : x \in X\}$. Then $\mathbf{D} = (X, \mathcal{B})$ is a symmetric (36, 15, 6)-design.

Example 2.4.4. Let $n \geq 2$ be an integer and let $\mathcal{P}$ be the set of all nonempty subsets of the set $\{1, 2, \ldots, n\}$. Consider the incidence structure $\mathbf{D} = (\mathcal{P}, \mathcal{P}, I)$ with $(X, Y) \in I$ if and only if the cardinality of the intersection $X \cap Y$ is even. Then $\mathbf{D}$ is a symmetric $(2^n - 1, 2^{n-1} - 1, 2^{n-2} - 1)$-design.

Incidence matrices of a (v, b, r, k, λ)-design satisfy the three equations (2.3). For symmetric designs, one equation suffices, as is shown by the following theorem.

Theorem 2.4.5. *A $(0, 1)$-matrix N of order v is an incidence matrix of a symmetric (v, k, λ)-design if and only if*

$$NN^\top = (k - \lambda)I + \lambda J, \tag{2.10}$$

where I is the identity matrix and J is the all-one matrix of order v.

Proof. If N is an incidence matrix of a symmetric (v, k, λ)-design, then (2.10) follows from (2.3).

Suppose N is a $(0, 1)$-matrix of order v satisfying (2.10). If $N = O$ or $N = J$, then (v, k, λ) are the parameters of a trivial symmetric design. Assume that $N \neq O$ and $N \neq J$. Then $v > 1$. Observe that the diagonal entries k and off-diagonal entries λ of $NN^\top$ represent the row sum and the inner product of two distinct rows of N, respectively. Therefore, $k > \lambda \geq 0$. By Lemma 2.3.6,

$$\det(NN^\top) = (\det N)^2 = (k + \lambda(v - 1))(k - \lambda)^{v-1}.$$

Therefore, N is nonsingular. Since the row sum of N is k, we have $NJ = kJ$, which implies $N^{-1}J = \frac{1}{k}J$. Therefore, multiplying (2.10) on the left by N^{-1} and on the right by N yields

$$N^\top N = (k - \lambda)I + \frac{\lambda}{k}JN.$$

Comparing (j, j)-entries on both sides of this equation yields

$$c_j = k - \lambda + \frac{\lambda}{k}c_j,$$

where c_j is the sum of the entries in the jth column of N. Therefore, $c_j = k$ for $j = 1, 2, \ldots, v$, and N is an incidence matrix of a symmetric (v, k, λ)-design. □

Remark 2.4.6. The proof of the above theorem shows in fact that if a (0, 1)-matrix N of order v satisfies (2.10), then

$$N^\top N = (k - \lambda)I + \lambda J,$$

i.e., the dual of a symmetric (v, k, λ)-design is a symmetric (v, k, λ)-design. This implies that any two distinct blocks of a symmetric (v, k, λ)-design meet in λ points. This also implies the following proposition.

Remark 2.4.7. If a symmetric (v, k, λ)-design $\mathbf{D}$ admits a symmetric incidence matrix, then, of course, the dual design $\mathbf{D}^\top$ is isomorphic to $\mathbf{D}$, i.e., $\mathbf{D}$ is self-dual. However, the converse is not true: there exists a self-dual symmetric (25, 9, 3)-design that does not admit a symmetric incidence matrix.

Proposition 2.4.8. *An incidence structure having v points and v blocks, constant block size k, and constant intersection size λ between any two distinct blocks is a symmetric (v, k, λ)-design.*

The next proposition gives another sufficient condition for an incidence structure to be a symmetric design.

Proposition 2.4.9. *Let λ and μ be positive integers and let $\mathbf{D} = (X, \mathcal{B}, I)$ be an incidence structure satisfying the following conditions*:

(i) $r(x) < |\mathcal{B}|$ *for all* $x \in X$;
(ii) $|B| < |X|$ *for all* $B \in \mathcal{B}$;
(iii) $\lambda(x, y) = \lambda$ *for any distinct* $x, y \in X$;
(iv) $|A \cap B| = \mu$ *for any distinct* $A, B \in \mathcal{B}$.

Then $\mathbf{D}$ *is either a symmetric design or a pencil.*

Proof. If $\mathbf{D}$ has distinct blocks A and B such that the set of points incident with A is the same as the set of points incident with B, then $|A| = |B| = \mu$ and, for any block C, every point incident with A is incident with C. However, this is not the case due to (i). Similarly, distinct points of $\mathbf{D}$ are incident with distinct sets of blocks. Therefore, we can consider the block set of $\mathbf{D}$ as a set of subsets of X and the block set of $\mathbf{D}^\top$ as a set of subsets of $\mathcal{B}$. Non-uniform Fisher's Inequality then implies that $|X| = |\mathcal{B}|$.

Suppose first that $\lambda > 1$. Let $A \in \mathcal{B}$ and $x \in A$. Counting in two ways flags (y, B) of $\mathbf{D}$ with $y \neq x$, $B \neq A$, $y \in A$, and $x \in B$ yields $(|A| - 1)(\lambda - 1) = (r(x) - 1)(\mu - 1)$. Therefore, $|A|$ is the same for all blocks A containing a given point x. Since any two blocks of $\mathbf{D}$ have a common point, all blocks have the same cardinality and $\mathbf{D}$ is a symmetric design. If $\mu > 1$, then, for similar reasons, $\mathbf{D}^\top$ is a symmetric design and so is $\mathbf{D}$.

Suppose now that $\lambda = \mu = 1$. If all blocks of $\mathbf{D}$ have the same cardinality or all points of $\mathbf{D}$ have the same replication number, then $\mathbf{D}$ is a symmetric design. Otherwise, by the Ryser–Woodall Theorem, applied to both $\mathbf{D}$ and $\mathbf{D}^\top$, the set X can be partitioned into nonempty subsets X_1 and X_2, and $\mathcal{B}$ can be partitioned into nonempty subsets $\mathcal{B}_1$ and $\mathcal{B}_2$ so that, for $i = 1$ and 2, all points of X_i have the same replication number r_i and all blocks of $\mathcal{B}_i$ have the same cardinality k_i. Let $A \in \mathcal{B}$ and $x \in X \setminus A$. Counting in two ways flags (y, B) of $\mathbf{D}$ with $y \in A$ and $x \in B$ yields $|A| = r(x)$. This means that every block A contains either X_1 or X_2 and, for each i, all blocks of $\mathcal{B}_i$ contain the same set X_j. Without loss of generality, we assume that the blocks of $\mathcal{B}_1$ contain X_1 and the blocks of $\mathcal{B}_2$ contain X_2. If $|\mathcal{B}_i| \geq 2$, then $|X_i| = 1$; similarly, if $|X_i| \geq 2$, then $|\mathcal{B}_i| = 1$. Therefore, we may assume that $|\mathcal{B}_1| = |X_2| = 1$. Let $\mathcal{B}_1 = \{A\}$ and $X_2 = \{x\}$. Then $A = X_1$ and therefore, every block of $\mathcal{B}_2$ contains x and one point of X_1. Thus, $\mathbf{D}$ is a pencil. □

If N is an incidence matrix of a symmetric (v, k, λ)-design, then $\det(NN^\top) = (k + \lambda(v-1))(k-\lambda)^{v-1} = k^2(k-\lambda)^{v-1}$. On the other hand, $\det(NN^\top) = (\det N)^2$ must be a perfect square. This gives the following necessary condition for the parameters of a symmetric design.

Proposition 2.4.10. *If (v, k, λ) are the parameters of a symmetric design and v is even, then $k - \lambda$ is a perfect square.*

Remark 2.4.11. This proposition shows that the necessary condition (2.9) for the parameters of a symmetric design is not sufficient. For instance, a symmetric $(22, 7, 2)$-design cannot exist even though its parameters satisfy (2.9). We now have two restrictions on the parameters of a symmetric (v, k, λ)-design with v even:

$$\lambda(v-1) = k(k-1), \quad k - \lambda \text{ is a perfect square.}$$

It is not known whether these conditions are sufficient for existence of a symmetric (v, k, λ)-design. The smallest unresolved parameter set is $(154, 18, 2)$.

In the next section, we will prove the Bruck–Ryser–Chowla Theorem that gives a necessary condition for the parameters of a symmetric (v, k, λ)-design with v odd.

Equation (2.9) implies bounds on the number of points of a symmetric design of a given order.

Proposition 2.4.12. *Let $\mathbf{D}$ be a symmetric (v, k, λ)-design of order $n = k - \lambda \geq 2$. Then*

$$4n - 1 \leq v \leq n^2 + n + 1.$$

Proof. Since $\mathbf{D}$ and its complement $\mathbf{D}'$ have the same order, we can assume without loss of generality that $v \geq 2k$. Equation (2.9) implies that λ and $v - 2n - \lambda = v - 2k + \lambda$ are the roots of the quadratic equation

$$x^2 - (v - 2n)x + n(n-1) = 0. \tag{2.11}$$

Since the discriminant of this equation is nonnegative, we have

$$(v - 2n)^2 \geq 4n(n-1) = (2n-1)^2 - 1.$$

Since $(2n-1)^2 - 1$ is not a perfect square for $n \geq 2$, we have $v - 2n \geq 2n - 1$, so $v \geq 4n - 1$.

Since the left-hand side of (2.11) is positive at $x = 0$ and since the roots of this equation are integers, it is nonnegative at $x = 1$. This implies that $v \leq n^2 + n + 1$. □

Symmetric designs meeting the bounds of Proposition 2.4.12 are projective planes and Hadamard 2-designs which will be considered in Chapters 3 and 4, respectively.

Given a symmetric design $\mathbf{D}$ with a fixed block, one can obtain the following two 2-designs as substructures of $\mathbf{D}$.

Definition 2.4.13. Let $\mathbf{D} = (X, \mathcal{B}, I)$ be a nontrivial symmetric design and let B be a block of $\mathbf{D}$. The substructures $\mathbf{D}^B$ and $\mathbf{D}_B$ are called a *residual design of* $\mathbf{D}$ and a *derived design of* $\mathbf{D}$, respectively.

The blocks of $\mathbf{D}^B$ and $\mathbf{D}_B$ can be regarded as sets $A \setminus B$ and $A \cap B$, respectively, where A is a block of $\mathbf{D}$ other than B. If N is an incidence matrix of $\mathbf{D}$ such that the last column of N corresponds to the block B, then

$$N = \begin{bmatrix} S & \mathbf{0} \\ T & \mathbf{j} \end{bmatrix}$$

where S is an incidence matrix of the residual design $\mathbf{D}^B$ and T is an incidence matrix of the derived design $\mathbf{D}_B$.

Remark 2.4.14. The residual and derived designs of a symmetric design with respect to the same block do not determine this symmetric design uniquely: there exist symmetric $(25, 9, 3)$-designs $\mathbf{D}$ and $\mathbf{E}$ and blocks A of $\mathbf{D}$ and B of $\mathbf{E}$ such that the residual designs $\mathbf{D}^A$ and $\mathbf{E}^B$ are isomorphic and the derived designs $\mathbf{D}_A$ and $\mathbf{E}_B$ are isomorphic, yet the designs $\mathbf{D}$ and $\mathbf{E}$ are not isomorphic.

The following proposition is straightforward.

Proposition 2.4.15. *Let* $\mathbf{D}$ *be a nontrivial symmetric* (v, k, λ)*-design with* $v > k \geq 2$ *and let* B *be a block of* $\mathbf{D}$*. Then* $\mathbf{D}^B$ *is a* $(v-k, v-1, k, k-\lambda, \lambda)$*-design and* $\mathbf{D}_B$ *is a* $(k, v-1, k-1, \lambda, \lambda-1)$*-design.*

Proposition 2.1.12 immediately implies the following result.

Proposition 2.4.16. *Let* $\mathbf{D} = (X, \mathcal{B})$ *be a symmetric* (v, k, λ)*-design with* $v > k \geq 2$ *and let* $\mathbf{D}'$ *be the complementary design. Then, for any block* B *of* $\mathbf{D}$*, the designs* $\mathbf{D}^B$ *and* $\mathbf{D}'_{X\setminus B}$ *are isomorphic as well as the designs* $\mathbf{D}_B$ *and* $(\mathbf{D}')^{X\setminus B}$*.*

Observe that if a (v, b, r, k, λ)-design is a residual of a symmetric design $\mathbf{D}$, then $r = k + \lambda$ and $\mathbf{D}$ is a symmetric $(v + r, r, \lambda)$-design.

Definition 2.4.17. Any (v, b, r, k, λ)-design $\mathbf{D}$ with $r = k + \lambda$ is called a *quasi-residual design*. If $\mathbf{D}$ is a residual of a symmetric $(v + r, r, \lambda)$-design, then it is said to be *embeddable*. Otherwise, $\mathbf{D}$ is said to be *non-embeddable*.

Example 2.4.18 (Bhattacharya's Example). The following incidence structure $\mathbf{D} = (X, \mathcal{B})$ is a $(16, 24, 9, 6, 3)$-design, so it is quasi-residual. Let $X = \{a, b, c, \ldots, o, p\}$ and let $\mathcal{B}$ be the following family of 6-subsets of X:

$abcdef$ $abcdgh$ $abijlm$ $acjklo$ $adimnp$ $aegjno$ $aegkmp$ $afhikn$
$afhlop$ $bcijkp$ $bdlmno$ $befiop$ $behkmo$ $bfgkln$ $bghjnp$ $cdknop$
$cefjmn$ $cehiln$ $cfglmp$ $cghimo$ $degikl$ $dehjlp$ $dfgijo$ $dfhjkm$

This design has blocks that meet in four points, for instance, the first two blocks. Therefore, $\mathbf{D}$ cannot be a residual of a symmetric $(25, 9, 3)$-design, i.e., $\mathbf{D}$ is a non-embeddable quasi-residual design.

Two symmetric designs with the same parameters do not have to be isomorphic (see Theorem 2.4.21). Sometimes, one can prove that two symmetric designs are not isomorphic by comparing the ranks of their incidence matrices over a finite field.

Definition 2.4.19. Let $\mathbf{D}$ be a symmetric (v, k, λ)-design and let N be an incidence matrix of $\mathbf{D}$. For any prime p, the *p-rank* of $\mathbf{D}$ is the rank of N regarded as a matrix over the field $GF(p)$ of residue classes modulo p. The p-rank of $\mathbf{D}$ is denoted as $rank_p(\mathbf{D})$.

Remark 2.4.20. Proposition 2.1.13 immediately implies that the p-rank of a symmetric design $\mathbf{D}$ is independent of the choice of an incidence matrix of the design.

The following theorem can be obtained using the 2-ranks. We leave its proof as an exercise.

Theorem 2.4.21. *There are exactly three nonisomorphic symmetric* (16, 6, 2)*-designs. Their* 2*-ranks are* 6*,* 7*, and* 8*.*

Another application of 2-ranks is given in Section 3.7 (Theorems 3.7.14 and 3.7.16.).

2.5. The Bruck–Ryser–Chowla Theorem

In this section we obtain a necessary condition on the parameters of a symmetric (v, k, λ)-design with v odd. We first develop some classical number-theoretical results related to the *Legendre symbol*. We then define the *Hilbert symbols* whose calculation uses the Legendre symbol. The Hilbert symbols are used to define the *Hasse invariants* for symmetric matrices over the integers.

Definition 2.5.1. For any odd prime p and for any integer $a \not\equiv 0 \pmod{p}$, the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined to be equal to 1 if there exists an integer x such that $a \equiv x^2 \pmod{p}$; $\left(\frac{a}{p}\right) = -1$ otherwise.

The following properties of the Legendre symbol can be found in standard Number Theory texts.

Theorem 2.5.2. *Let p and q be distinct odd primes and let a and b be integers not divisible by p. Then*

(i) *if* $a \equiv b \pmod{p}$, *then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;
(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;
(iii) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$;
(iv) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$;
(v) $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}$.

Remark 2.5.3. Property (v) of Theorem 2.5.2 is the celebrated *Quadratic Reciprocity Law*.

Properties (i) and (ii) of Theorem 2.5.2 almost uniquely define the Legendre symbol, as the next proposition shows.

Proposition 2.5.4. *Let p be an odd prime and let a function L from the set of all integers not divisible by p to the set $\{-1, 1\}$ have the following properties:*

(i) *if* $a \equiv b \pmod{p}$, *then* $L(a) = L(b)$;
(ii) $L(ab) = L(a)L(b)$ *for all* a *and* b.

Then either $L(a) = 1$ *for all* a *or* $L(a) = \left(\frac{a}{p}\right)$ *for all* a.

Proof. Property (i) allows us to regard L as a function from the multiplicative group G of residue classes $\bmod p$ to the group $\{-1, 1\}$ of order 2. Property (ii) implies that this function is a homomorphism. The kernel of this homomorphism is either the entire group G or a subgroup of index 2. In the former case, $L(a) = 1$ for all $a \in G$. In the latter case, since $L(a^2) = 1$ for all $a \in G$, the kernel is the subgroup of all squares. Therefore, in this case, $L(a) = \left(\frac{a}{p}\right)$ for all $a \in G$. □

The next theorem will allow us to define the *Hilbert symbols*.

Theorem 2.5.5. *For any odd prime* p, *there exists a unique function* $(a, b) \longrightarrow (a, b)_p$ *from* $\mathbb{Z}^* \times \mathbb{Z}^*$ *to* $\{-1, 1\}$ *that satisfies the following conditions:*

(H1) $(a, b)_p = (b, a)_p$, *for any* $a, b \in \mathbb{Z}^*$;
(H2) $(ab, c)_p = (a, c)_p(b, c)_p$, *for any* $a, b, c \in \mathbb{Z}^*$;
(H3) $(a, b)_p = 1$, *for any integers* $a, b \not\equiv 0 \pmod{p}$;
(H4) *if* $a \not\equiv 0 \pmod{p}$, *then* $(a, p)_p = \left(\frac{a}{p}\right)$;
(H5) $(-p, p)_p = 1$.

Proof. Let a function $(a, b) \longrightarrow (a, b)_p$ from $\mathbb{Z}^* \times \mathbb{Z}^*$ to $\{-1, 1\}$ satisfy conditions (H1) – (H5). Then $(p, p)_p = \left(\frac{-1}{p}\right)$ and therefore, for any nonnegative integers s and t, $(p^s, p^t)_p = \left(\frac{-1}{p}\right)^{st}$. Let $a, b \in \mathbb{Z}^*$ and let $a = p^s a_0$ and $b = p^t b_0$ where s and t are nonnegative integers and a_0 and b_0 are integers not divisible by p. Then

$$(a, b)_p = \left(\frac{-1}{p}\right)^{st} \left(\frac{a_0}{p}\right)^{t} \left(\frac{b_0}{p}\right)^{s}. \tag{2.12}$$

Conversely, if we define a function $(a, b) \longrightarrow (a, b)_p$ from $\mathbb{Z}^* \times \mathbb{Z}^*$ to $\{-1, 1\}$ by (2.12), then it is straightforward to verify that it satisfies (H1) – (H5). □

Definition 2.5.6. The functions $(a, b) \longrightarrow (a, b)_p$ from $\mathbb{Z}^* \times \mathbb{Z}^*$ to $\{-1, 1\}$ defined, for odd primes p, by (2.12) are called the *Hilbert symbols*.

The next proposition gives further properties of Hilbert symbols.

Proposition 2.5.7. *The Hilbert symbol* $(a, b)_p$ *satisfies the following properties for any nonzero integers* a *and* b *and odd prime* p:

(H6) $(a^2, b)_p = 1$;
(H7) *if* $a + b$ *is a square, then* $(a, b)_p = 1$;
(H8) $(a, -a)_p = 1$;
(H9) *if* $a + b \neq 0$, *then* $(a, b)_p = (a + b, -ab)_p$.

Proof. (H6) follows immediately from (H2).
(H7) If $a \not\equiv 0 \pmod{p}$ and $b \not\equiv 0 \pmod{p}$, then $(a, b)_p = 1$ by (H3).

Suppose that $a \not\equiv 0 \pmod{p}$ and $b \equiv 0 \pmod{p}$. Let $a + b = x^2$ and $b = p^t b_0$ where $b_0 \not\equiv 0 \pmod{p}$. Then $a \equiv x^2 \pmod{p}$, so, by (H2), (H3), and (H6), we obtain:

$$(a, b)_p = (a, b_0)_p (a, p)_p^t = (x^2, p)_p^t = 1.$$

Suppose that $a \equiv b \equiv 0 \pmod{p}$. Let $a = p^s a_0, b = p^t b_0$ where $a_0, b_0 \not\equiv 0 \pmod{p}$. Then

$$(a, b)_p = (a_0, b_0)_p (a_0, p)_p^t (b_0, p)_p^s (p, p)_p^{st}. \tag{2.13}$$

If s and t are even, then $(a, b)_p = 1$. Suppose that s is even and t is odd. Since $a + b = p^s a_0 + p^t b_0$ is a square and $s \neq t$, the smaller of the exponents s, t must be even, i.e., $s < t$. Then $a + b = p^s(a_0 + p^{t-s} b_0)$, so $a_0 + p^{t-s} b_0$ is a square. Therefore, $(a_0, p)_p = 1$ and (2.13) implies that $(a, b)_p = 1$. Suppose finally that both s and t are odd. If $s \neq t$, then the highest power of p dividing $a + b$ is odd, and $a + b$ cannot be a square. Therefore, $s = t$, and we have $a + b = p^s(a_0 + b_0)$. Since $a + b$ is a square and s is odd, $a_0 + b_0 \equiv 0 \pmod{p}$. Therefore, (2.13) implies that

$$\begin{aligned}(a, b)_p &= (a_0, p)_p (b_0, p)_p (p, p)_p = (a_0, p)_p (-a_0, p)_p (-1, p)_p (-p, p)_p \\ &= (a_0, p)_p^2 (-p, p)_p = 1.\end{aligned}$$

(H8) follows from (H7).
(H9) Since $a(a + b) + b(a + b) = (a + b)^2$, we apply (H7) to obtain that $(a(a + b), b(a + b))_p = 1$. Therefore,

$$\begin{gathered}(a, b)_p (a, a + b)_p (b, a + b)_p (a + b, a + b)_p = 1, \\ (a, b)_p (ab, a + b)_p (-1, a + b)_p (-(a + b), a + b)_p = 1, \\ (a, b)_p (-ab, a + b)_p = 1, (a, b)_p = (-ab, a + b)_p.\end{gathered}$$

□

We next use the Hilbert symbols to define the *Hasse invariants* of symmetric matrices over the integers.

Definition 2.5.8. Let A be a symmetric matrix of order n with integral entries. For $i = 1, 2, \cdots, n$, let $D_i(A)$ be the determinant of the submatrix formed by

the first i rows and the first i columns of A. Suppose that the determinants $D_1(A), D_2(A), \cdots, D_n(A)$ are not equal to zero. Let p be an odd prime. Then the product

$$c_p(A) = (-1, D_n(A))_p \prod_{i=1}^{n-1} (D_i(A), -D_{i+1}(A))_p$$

is called the *Hasse p-invariant of A*.

The following theorem is central to applications of Hasse invariants to designs. Its proof is beyond the scope of this book.

Theorem 2.5.9. *If N is a nonsingular matrix over the integers, then $c_p(NN^\top) = 1$, for every odd prime p.*

We are now ready to prove the Bruck–Ryser–Chowla Theorem, which gives a necessary condition on the parameters of a symmetric (v, k, λ)-design in case v is odd.

Theorem 2.5.10 (The Bruck–Ryser–Chowla Theorem). *If there exists a nontrivial symmetric (v, k, λ)-design with odd v, then $((-1)^{\frac{v-1}{2}}\lambda, k-\lambda)_p = 1$, for any odd prime p.*

Proof. Let N be the incidence matrix of a nontrivial symmetric (v, k, λ)-design and let $A = NN^\top$. Then $A = (k-\lambda)I + \lambda J$. For $i = 1, 2, \cdots, v$, let D_i be the determinant of the matrix formed by the first i rows and the first i columns of A. By Lemma 2.3.6, $D_i = a_i(k-\lambda)^{i-1}$ where $a_i = k + (i-1)\lambda$. Note that $a_v = k^2$, so $(-1, D_v)_p = 1$, for any odd prime p. By Theorem 2.5.9, $c_p(A) = 1$. Therefore, we have

$$\begin{aligned}
1 = c_p(A) &= \prod_{i=1}^{v-1} (D_i, -D_{i+1})_p = \prod_{i=1}^{\frac{v-1}{2}} (D_{2i-1}, -D_{2i})_p (D_{2i}, -D_{2i+1})_p \\
&= \prod_{i=1}^{\frac{v-1}{2}} (a_{2i-1}(k-\lambda)^{2i-2}, -a_{2i}(k-\lambda)^{2i-1})_p (a_{2i}(k-\lambda)^{2i-1}, \\
&\qquad -a_{2i+1}(k-\lambda)^{2i})_p \\
&= \prod_{i=1}^{\frac{v-1}{2}} (a_{2i-1}, -a_{2i}(k-\lambda))_p (a_{2i}(k-\lambda), -a_{2i+1})_p \\
&= \prod_{i=1}^{\frac{v-1}{2}} (a_{2i-1}, -a_{2i})_p (a_{2i-1}, k-\lambda)_p (a_{2i}, -a_{2i+1})_p (k-\lambda, -a_{2i+1})_p.
\end{aligned}$$

Note that $a_{2i-1} - a_{2i} = -\lambda$, and we apply (H9) to obtain that $(a_{2i-1}, -a_{2i})_p = (-\lambda, a_{2i-1}a_{2i})_p$ and $(a_{2i}, -a_{2i+1})_p = (-\lambda, a_{2i}a_{2i+1})_p$. Therefore,

$$\begin{aligned}
1 = c_p(A) &= \prod_{i=1}^{\frac{v-1}{2}} (-\lambda, a_{2i-1}a_{2i})_p (-\lambda, a_{2i}a_{2i+1})_p (k-\lambda, a_{2i-1}a_{2i+1})_p (k-\lambda, -1)_p \\
&= \left((-1)^{\frac{v-1}{2}}, k-\lambda\right)_p \prod_{i=1}^{\frac{v-1}{2}} \left(-\lambda, a_{2i-1}a_{2i}^2 a_{2i+1}\right)_p (k-\lambda, a_{2i-1}a_{2i+1})_p \\
&= \left((-1)^{\frac{v-1}{2}}, k-\lambda\right)_p \left(-\lambda(k-\lambda), \prod_{i=1}^{\frac{v-1}{2}} a_{2i-1}a_{2i+1}\right)_p \\
&= \left((-1)^{\frac{v-1}{2}}, k-\lambda\right)_p (-\lambda(k-\lambda), a_1 a_v)_p = \left((-1)^{\frac{v-1}{2}}, k-\lambda\right)_p (-\lambda(k-\lambda), k)_p.
\end{aligned}$$

By (H9), $(-\lambda(k-\lambda), k)_p = (\lambda, k-\lambda)_p$, and the proof is now complete. □

Example 2.5.11. If there exists a symmetric $(43, 7, 1)$-design, then $(-1, 6)_p = 1$ for any odd prime p. However, $(-1, 6)_3 = (-1, 3)_3 = \left(\frac{-1}{3}\right) = -1$. Therefore, there is no symmetric $(43, 7, 1)$-design.

Example 2.5.12. If there exists a symmetric $(29, 8, 2)$-design, then $(2, 6)_3 = 1$. On the other hand, $(2, 6)_3 = (2, 3)_3 = \left(\frac{2}{3}\right) = -1$. Therefore, there is no symmetric $(29, 8, 2)$-design.

Remark 2.5.13. The condition of the Bruck–Ryser–Chowla Theorem is not sufficient for the existence of symmetric designs. The only known counterexample is the parameter set $(111, 11, 1)$. It satisfies the condition of the Bruck–Ryser–Chowla Theorem (and the equation (2.9)). However, there is no symmetric $(111, 11, 1)$-design (Theorem 6.4.5). An unresolved parameter set for a symmetric design with the smallest number of points is $(81, 16, 3)$.

2.6. Automorphisms of symmetric designs

In Definition 2.1.10, we introduced the notion of isomorphic incidence structures. If $\mathbf{D}_1 = (X_1, \mathcal{B}_1)$ and $\mathbf{D}_2 = (X_2, \mathcal{B}_2)$ are nontrivial symmetric designs, we can regard $\mathcal{B}_1$ and $\mathcal{B}_2$ as sets of subsets of X_1 and X_2, respectively. An isomorphism of $\mathbf{D}_1$ and $\mathbf{D}_2$ in this case can be regarded as a bijection $f\colon X_1 \to X_2$ such that $f(B)$ is a block of $\mathbf{D}_2$ if and only if B is a block of $\mathbf{D}_1$. It is often convenient to assume that $X_1 = X_2$; then an isomorphism of $\mathbf{D}_1$ and $\mathbf{D}_2$ can be regarded as a permutation of the point set X_1 that maps blocks of $\mathbf{D}_1$ onto blocks of $\mathbf{D}_2$.