MATH3301

Graph Theory and Design Theory

Design Theory

2025

Acknowledgements

In addition to the other references cited in the text, extensive use of three books in particular has been made in preparing these notes. These are *The CRC Handbook of Combinatorial Designs* by Charles Colbourn and Jeff Dinitz [8], *Design Theory* by Curt Lindner and Chris Rodger [16], and *Combinatorial Designs: Constructions and Analysis* by Douglas Stinson [19]. Many of the included proofs and constructions are adapted from those in these books. Also, several factual claims made here are derived directly from these books, sometimes without direct reference to them.

Contents

Chapter 1

Introduction to Designs

“The evolution of combinatorial design theory has been one of remarkable successes, unanticipated applications, deep connections with fundamental mathematics, and the desire to produce order from chaos. While some of its celebrated successes date from the eighteenth and nineteenth centuries in the research of Euler, Kirkman, Cayley, Hamilton, Sylvester, Moore, and others, not until the twentieth century did the study of combinatorial designs emerge as an academic subject in its own right. When Fisher and his colleagues developed the mathematics of experimental design in the 1920s, combinatorial design theory was born as a field intimately linked to its applications. Beginning in the 1930s, Bose and his school laid the foundations, embedding the nascent field firmly as a mathematical discipline by developing deep connections with finite geometry, number theory, finite fields, and group theory; however, Bose accomplished much more. His foundation entwined deep mathematics with its applications in experimental design and in recreational problems and anticipated its fundamental importance in the theory of error-correcting codes. The rapid advances in design theory can be attributed in large degree to its impetus from applications in coding theory and communications and its continued deep interactions with geometry, algebra, and number theory. The last fifty years have witnessed not only the emergence of certain combinatorial designs (balanced incomplete block designs, Hadamard matrices, pairwise balanced designs, and orthogonal arrays, for example) as central, but also powerful combinatorial and computational techniques for their construction. Indeed the field grew so far and so fast that its historical connection to applications was strained. Yet, in the last twenty years, combinatorial design theory has emerged again as a field rich in current and practical applications. The fundamental connections with algebra, number theory, and finite geometry remain and flourish. The applications in experimental design and coding theory have developed a breadth and depth that defy brief explanation. Yet combinatorial design theory has matured into more than this through applications in cryptography, optical communications, storage system design, communications protocols, algorithm design and analysis, and wireless communications, to mention just a few areas.” Charles Colbourn (2003, [19])

Definition 1.0.1. A **design** is a pair $(V, \mathcal{B})$ where V is a set and $\mathcal{B}$ is a collection of subsets of V. The elements of V are the **points** of the design, and the elements of $\mathcal{B}$ are the **blocks**. If $(V, \mathcal{B})$ is a design, then $|V|$ is called the **order** of the design, and if $B \in \mathcal{B}$, then $|B|$ is called the **size** of the block B. □

Notice that $\mathcal{B}$ is a collection or multiset, rather than a set, which means that designs can have repeated blocks. A design having no repeated blocks is a **simple** design. In general we will enclose the blocks of designs in curly brackets $\{\ \}$, whether there are repeated blocks or not. If a point x is in a block B, then we say that x and B are **incident** and that B **covers** x. More generally, a set S of points is said to be **covered** r times by $\{B_1, B_2, \ldots, B_t\}$ if there are r values of $i \in \{1, 2, \ldots, t\}$ for which $S \subseteq B_i$.

Design theory is concerned with designs that are optimal or balanced in some sense. In the design of Example 1.0.2, each point occurs in exactly four blocks, and each pair of points occurs in exactly one block. The number of blocks in which a point x occurs is called the **replication number of x** and is usually denoted by r_x. If $r_x = r$ is a constant, independent of x, then r is called the **replication number** of the design. The number of blocks in which distinct points x and y both occur is denoted by λ_{xy}. If $\lambda_{xy} = \lambda$ is a constant, independent of x and y, then the design is said to be **balanced** and λ is called the **index** of the design.

Example 1.0.2. Let $V = \{1, 2, \ldots, 9\}$ and let

$$\begin{array}{rllllr}\mathcal{B} = \{ & \{1,2,3\}, & \{1,4,7\}, & \{1,5,9\}, & \{1,6,8\}, & \\ & \{4,5,6\}, & \{2,5,8\}, & \{2,6,7\}, & \{2,4,9\}, & \\ & \{7,8,9\}, & \{3,6,9\}, & \{3,4,8\}, & \{3,5,7\} & \}.\end{array}$$

□

Any graph is an example of a design. The vertices and edges of a graph form the points and blocks of a design, but most graphs are not very interesting from the point of view of design theory. It is worth mentioning that the design corresponding to an r-regular graph has replication number r. Most graphs are neither optimal nor balanced in any meaningful way. However, we shall see that graph theory can be very useful in understanding designs and their properties, and there is significant overlap between the two areas. In particular, there are strong connections between designs and **graph decompositions**.

Definition 1.0.3. A **decomposition** of a graph K is a set of subgraphs whose edge sets partition the edge set of K. A **G-decomposition** is a decomposition in which each subgraph is isomorphic to some fixed graph G. The subgraphs in a G-decomposition are called **G-blocks**. □

Definition 1.0.4. A **d-factor** of a graph is a spanning d-regular subgraph, and a **d-factorisation** is a decomposition into d-factors. □

The complete graph of order n and multiplicity λ is denoted by λK_n. It has n vertices and each distinct pair of vertices is joined by λ distinct edges. The notation K_n is used when $\lambda = 1$. Since the design in Example 1.0.2 covers each pair of points exactly once, it is equivalent to a K_3-decomposition of K_9. Here, the points of the design correspond to vertices, the blocks give the vertex sets of the subgraphs, and pairs of points are equivalent to edges.

Often there is some additional structure associated with a design. For example, the blocks of the design in Example 1.0.2 are partitioned into four columns such that each column covers each point exactly once. It is thus an example of a **resolvable** design.

Definition 1.0.5. A **resolution class** of a design is a subset of its blocks which covers each point exactly once. A design is **resolvable** if its blocks can be partitioned into resolution classes. □

The resolution classes of the design from Example 1.0.2 correspond to 2-factors in a 2-factorisation of K_9, where each 2-factor consists of three disjoint copies of K_3.

Additional structure associated with a design is sometimes considered part of the design itself, and included in its definition. For example, if we let $V = \{1, 2, \ldots, 8\}$ and let $\mathcal{B}$ be the set of all 2-element subsets of V, then $(V, \mathcal{B})$ is not very interesting on its own. However, in Example 1.0.6, the blocks of this design are resolved into seven resolution classes, the columns of blocks are the resolution classes. Such a design can be used to schedule a round-robin tournament involving eight teams. In the language of graph theory, this design corresponds to a 1-factorisation of K_8.

Example 1.0.6.

$$\begin{array}{ccccccc}
\{1,2\} & \{1,3\} & \{1,4\} & \{1,5\} & \{1,6\} & \{1,7\} & \{1,8\} \\
\{3,4\} & \{2,4\} & \{2,3\} & \{2,6\} & \{2,7\} & \{2,8\} & \{2,5\} \\
\{5,6\} & \{5,7\} & \{5,8\} & \{3,7\} & \{3,8\} & \{3,5\} & \{3,6\} \\
\{7,8\} & \{6,8\} & \{6,7\} & \{4,8\} & \{4,5\} & \{4,6\} & \{4,7\}
\end{array}$$

□

The design in Example 1.0.7 yields a Latin square of side 4; a 4 by 4 array of symbols where each symbol occurs exactly once in each row and exactly once in each column. If the points are partitioned into three sets $\{r_1, r_2, r_3, r_4\}$, $\{c_1, c_2, c_3, c_4\}$, and $\{s_1, s_2, s_3, s_4\}$, then each pair of points from distinct parts is covered by exactly one block, and each pair of points from the same part is covered by no block. Thus, we obtain a Latin square by placing symbol s_k in row i and column j where $\{r_i, c_j, s_k\}$ is the unique block containing the pair $\{r_i, c_j\}$.

Example 1.0.7. The Latin square on the right below corresponds to the design with point set $V = \{r_1, r_2, r_3, r_4, c_1, c_2, c_3, c_4, s_1, s_2, s_3, s_4\}$ and block set $\mathcal{B}$ given on the left below.

$$\begin{array}{llllll}
\mathcal{B} = \{ & \{r_1, c_1, s_1\}, & \{r_1, c_2, s_2\}, & \{r_1, c_3, s_3\}, & \{r_1, c_4, s_4\}, & \\
& \{r_2, c_1, s_2\}, & \{r_2, c_2, s_3\}, & \{r_2, c_3, s_4\}, & \{r_2, c_4, s_1\}, & \\
& \{r_3, c_1, s_3\}, & \{r_3, c_2, s_4\}, & \{r_3, c_3, s_1\}, & \{r_4, c_4, s_2\}, & \\
& \{r_4, c_1, s_4\}, & \{r_4, c_2, s_1\}, & \{r_4, c_3, s_2\}, & \{r_4, c_4, s_3\} & \}
\end{array}$$

s_1	s_2	s_3	s_4
s_2	s_3	s_4	s_1
s_3	s_4	s_1	s_2
s_4	s_1	s_2	s_3

□

A Latin square of side n is easily seen to be equivalent to a K_3-decomposition of the complete tripartite graph $K_{n,n,n}$; which has $3n$ vertices partitioned into three parts of size n and there is an edge joining vertices x and y if and only if x and y are from distinct parts.

Chapter 2

Balanced Incomplete Block Designs

A design is said to be a **block design** if the blocks are of uniform cardinality k, and is said to be **balanced** if each pair of points is covered by the same number of blocks. This number is called the **index** of the design and is usually denoted by λ. In a more general setting, this notion of balance is called **pairwise balance**. A **complete design** with v points and block size $k \leq v$ consists of the set of all k-sets of points. A block design with v points and block size k is called **incomplete** if $k < v$. In design theory, the usage of the terms complete and incomplete is somewhat inconsistent in that for $k < v$, a complete design with blocks size k is incomplete.

Definition 2.0.1. Let v, k, and λ be integers with $2 \leq k < v$. A design $(V, \mathcal{B})$ is a **balanced incomplete block design** with parameters (v, k, λ), or a **(v, k, λ)-design**, if it has v points, each block has k points, and each pair of distinct points is covered by exactly λ blocks. □

Example 2.0.2. If $V = \{0, 1, 2, 3, 4, \infty\}$ and $\mathcal{B} =$

$$\{\{\infty,0,1\},\{\infty,1,2\},\{\infty,2,3\},\{\infty,3,4\},\{\infty,4,0\},\{0,1,3\},\{1,2,4\},\{2,3,0\},\{3,4,1\},\{4,0,2\}\},$$

then $(V, \mathcal{B})$ is a $(6, 3, 2)$-design. □

Theorem 2.0.3. A (v, k, λ)-design has $b = \lambda\frac{v(v-1)}{k(k-1)}$ blocks and each point occurs in $r = \lambda\frac{v-1}{k-1}$ blocks.

Proof Let $(V, \mathcal{B})$ be a (v, k, λ)-design and let b be the number of blocks in $\mathcal{B}$. Since each 2-element subset of V occurs in exactly λ blocks, it follows that $b\frac{k(k-1)}{2} = \lambda\frac{v(v-1)}{2}$ and hence that $b = \lambda\frac{v(v-1)}{k(k-1)}$. Suppose a point x occurs in r_x blocks of $\mathcal{B}$. Then x occurs in blocks with $r_x(k-1)$ elements of V. But we know that x occurs with each of the other $v-1$ elements of V exactly λ times and so we have $r_x(k-1) = \lambda(v-1)$. So we see that $r_x = r = \lambda\frac{v-1}{k-1}$ is independent of x. □

The notation b for number of blocks and r for replication number is in common usage in design theory. Whenever b or r is used in the context a (v, k, λ)-design, it is understood that $b = \lambda\frac{v(v-1)}{k(k-1)}$ and $r = \lambda\frac{v-1}{k-1}$.

Theorem 2.0.3 yields two necessary conditions for the existence of a (v, k, λ)-design.

Theorem 2.0.4. If there exists a (v, k, λ)-design, then $b = \lambda\frac{v(v-1)}{k(k-1)}$ and $r = \lambda\frac{v-1}{k-1}$ are integers.

Proof The result is an immediate corollary of Theorem 2.0.3 because the number of blocks and the replication number of a design are integers. □

Definition 2.0.5. In the context of (v, k, λ)-designs, the integers v, k and λ are **admissible** if and only if $b = \lambda\frac{v(v-1)}{k(k-1)}$ and $r = \lambda\frac{v-1}{k-1}$ are integers. These conditions are called the **obvious necessary conditions** for the existence of a (v, k, λ)-design, and a (v, k, λ)-design is said to be **admissible** if its parameters v, k and λ are admissible. □

It is routine to check that if v, k and λ are admissible, then

$$vr = bk \qquad \text{and} \qquad \lambda(v-1) = r(k-1).$$

The notation (v, b, r, k, λ)-design or (v, b, r, k, λ)-BIBD (BIBD being an acronym for balanced incomplete block design) is often used instead of (v, k, λ)-design, but the values of b and r are uniquely determined from v, k and λ.

We now introduce a special family of (v, k, λ)-designs.

Definition 2.0.6. A (v, k, λ)-design is **symmetric** if it has v blocks. □

Example 2.0.7. Let $V = \{1, 2, \ldots, 16\}$ and let $\mathcal{B} = \{B_1, B_2, \ldots, B_{16}\}$ where for $i = 1, 2, \ldots, 16$ the block B_i is defined to contain the points other than i that are in the same row as i or in the same column as i in the array shown below.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

For example, $B_5 = \{1, 6, 7, 8, 9, 13\}$. It is easy to see that $(V, \mathcal{B})$ is a $(16, 6, 2)$-design. For example, the pair $\{2, 3\}$ occurs precisely in blocks B_1 and B_4 and the pair $\{2, 7\}$ occurs precisely in blocks B_3 and B_6. The design is symmetric because it has the same number of points as blocks, namely 16. □

Theorem 2.0.8. Let v, k and λ be integers with $2 \leq k < v$. If there exists a symmetric (v, k, λ)-design, then $\lambda(v-1) = k(k-1)$. Moreover, if $\lambda(v-1) = k(k-1)$, then v, k and λ are admissible and any (v, k, λ)-design satisfies $b = v$ and $r = k$.

Proof In a symmetric (v, k, λ)-design, the number b of blocks is given both by $b = v$ and by $b = \lambda\frac{v(v-1)}{k(k-1)}$. It follows immediately that $\lambda(v-1) = k(k-1)$. Also, if $\lambda(v-1) = k(k-1)$, then $b = \lambda\frac{v(v-1)}{k(k-1)} = v$ and $r = \lambda\frac{v-1}{k-1} = k$ are both integers. So v, k and λ are admissible and any (v, k, λ)-design satisfies $b = v$ and $r = k$. □

Definition 2.0.9. In the context of symmetric (v, k, λ)-designs, the integers v, k and λ are **admissible** if and only if $\lambda(v-1) = k(k-1)$. □

2.1 Some Existence Results

In this section we present some existence results for (v, k, λ)-designs, mostly for small values of k and with a focus on designs with index $\lambda = 1$. We will discuss some of the constructions used to prove these results in later sections.

A very important result on the existence of (v, k, λ)-designs was proved by Wilson in 1975 [24]. For given block size k and index λ, it solves the existence problem for (v, k, λ)-designs for all but a (large) finite number of values of v.

Theorem 2.1.1. (Wilson's Theorem, [24]) For all $k \geq 2$ and $\lambda \geq 1$ there exists a constant $C(k, \lambda)$ such that for all $v \geq C(k, \lambda)$, there exists a (v, k, λ)-design if and only if $k(k-1)$ divides $\lambda v(v-1)$ and $k-1$ divides $\lambda(v-1)$.

We now turn to the existence problem for small values of k. For $k \in \{3, 4, 5\}$ and for each $\lambda \geq 1$, it is known that there exists a (v, k, λ)-design whenever the obvious necessary conditions are satisfied; except that there is no $(15, 5, 2)$-design. For $k = 6$ and for each $\lambda \geq 2$ the situation is similar: it is known that there exists a (v, k, λ)-design whenever the obvious necessary conditions are satisfied; except that there is no $(21, 6, 2)$-design. For $k = 6$ and $\lambda = 1$, there are 29 unresolved values of v and four cases where the obvious necessary conditions are satisfied but no design exists. For larger values of k less in known, especially for $k \geq 10$. A comprehensive summary of results is given in [3]. For $k \leq \frac{v}{2}$ (see Theorem 2.2.3), the smallest, in terms of number of points, three designs whose existence is unknown are a $(39, 13, 6)$-design, a $(40, 14, 7)$-design and a $(40, 10, 3)$-design.

In the next four theorems, we state the relevant results for $k \in \{3, 4, 5, 6\}$. A $(v, 3, 1)$-design is called a Steiner triple system, and these were shown to exist if and only if $v \equiv 1, 3 \pmod 6$ by Kirkman in 1847 [14]. By 1975, the existence problem for (v, k, λ)-designs was completely settled for $k \in \{3, 4, 5\}$, and also for $k = 6$ with $\lambda \geq 2$ [12]. For $k = 6$ and $\lambda = 1$, the most recent new results were obtained in 2007 [1].

Theorem 2.1.2. Let $v > 3$ and $\lambda \geq 1$. There exists a $(v, 3, \lambda)$-design if and only if 3 divides $\lambda \frac{v(v-1)}{2}$ and $\lambda(v-1)$ is even. Equivalently,

- for $\lambda \equiv 1, 5 \pmod 6$, there exists a $(v, 3, \lambda)$-design if and only if $v \equiv 1, 3 \pmod 6$;
- for $\lambda \equiv 2, 4 \pmod 6$, there exists a $(v, 3, \lambda)$-design if and only if $v \equiv 0, 1 \pmod 3$;
- for $\lambda \equiv 3 \pmod 6$, there exists a $(v, 3, \lambda)$-design if and only if $v \equiv 1 \pmod 2$; and
- for $\lambda \equiv 0 \pmod 6$, there exists a $(v, 3, \lambda)$-design for all v.

Theorem 2.1.3. Let $v > 4$ and $\lambda \geq 1$. There exists a $(v, 4, \lambda)$-design if and only if 6 divides $\lambda \frac{v(v-1)}{2}$ and 3 divides $\lambda(v-1)$. Equivalently,

- for $\lambda \equiv 1, 5 \pmod 6$, there exists a $(v, 4, \lambda)$-design if and only if $v \equiv 1, 4 \pmod{12}$;
- for $\lambda \equiv 2, 4 \pmod 6$, there exists a $(v, 4, \lambda)$-design if and only if $v \equiv 1 \pmod 3$;

- for $\lambda \equiv 3 \pmod{6}$, there exists a $(v, 4, \lambda)$-design if and only if $v \equiv 0, 1 \pmod{4}$; and

- for $\lambda \equiv 0 \pmod{6}$, there exists a $(v, 4, \lambda)$-design for all v.

Theorem 2.1.4. Let $v > 5$ and $\lambda \geq 1$. There exists a $(v, 5, \lambda)$-design if and only if 10 divides $\lambda\frac{v(v-1)}{2}$ and 4 divides $\lambda(v-1)$, except that there is no $(15, 5, 2)$-design. Equivalently,

- for $\lambda \equiv 1, 3, 7, 9, 11, 13, 17, 19 \pmod{20}$, there exists a $(v, 5, \lambda)$-design if and only if $v \equiv 1, 5 \pmod{20}$;

- for $\lambda \equiv 2, 6, 14, 18 \pmod{20}$, there exists a $(v, 5, \lambda)$-design if and only if $v \equiv 1, 5 \pmod{10}$, except that there is no $(15, 5, 2)$-design;

- for $\lambda \equiv 4, 8, 12, 16 \pmod{20}$, there exists a $(v, 5, \lambda)$-design if and only if $v \equiv 0, 1 \pmod{5}$;

- for $\lambda \equiv 5, 15 \pmod{20}$, there exists a $(v, 5, \lambda)$-design if and only if $v \equiv 1 \pmod{4}$;

- for $\lambda \equiv 10 \pmod{20}$, there exists a $(v, 5, \lambda)$-design if and only if $v \equiv 1 \pmod{2}$; and

- for $\lambda \equiv 0 \pmod{20}$, there exists a $(v, 5, \lambda)$-design for all v.

Theorem 2.1.5. Let $v > 6$ and $\lambda \geq 1$. There exists a $(v, 6, \lambda)$-design if and only if 15 divides $\lambda\frac{v(v-1)}{2}$ and 5 divides $\lambda(v-1)$, except that there is no $(16, 6, 1)$-design, $(21, 6, 1)$-design, $(36, 6, 1)$-design, $(46, 6, 1)$-design, nor $(21, 6, 2)$-design, and except that it is unknown whether there exists a $(v, 6, 1)$-design when v is one of the 29 values listed below.

$$\begin{array}{cccccccccc}
51 & 61 & 81 & 166 & 226 & 231 & 256 & 261 & 286 & 316 \\
321 & 346 & 351 & 376 & 406 & 411 & 436 & 441 & 471 & 501 \\
561 & 591 & 616 & 646 & 651 & 676 & 771 & 796 & 801 &
\end{array}$$

Equivalently,

- for $\lambda \equiv 1, 2, 4, 7, 8, 11, 13, 14 \pmod{15}$, there exists a $(v, 6, \lambda)$-design if and only if $v \equiv 1, 6 \pmod{15}$ except that there is no $(16, 6, 1)$-design, $(21, 6, 1)$-design, $(36, 6, 1)$-design, $(46, 6, 1)$-design, nor $(21, 6, 2)$-design, and except that it is unknown whether there exists a $(v, 6, 1)$-design when v is one of the 29 values listed above;

- for $\lambda \equiv 3, 6, 9, 12 \pmod{15}$, there exists a $(v, 6, \lambda)$-design if and only if $v \equiv 1 \pmod{5}$;

- for $\lambda \equiv 5, 10 \pmod{15}$, there exists a $(v, 6, \lambda)$-design if and only if $v \equiv 0, 1 \pmod{3}$;

- for $\lambda \equiv 0 \pmod{15}$, there exists a $(v, 6, \lambda)$-design for all v.

2.2 Constructing New Designs from Existing Designs

We now examine some methods for constructing new designs from existing ones. If $(V, \mathcal{B}_1)$ is a (v, k, λ_1)-design and $(V, \mathcal{B}_2)$ is a (v, k, λ_2)-design, then obviously $(V, \mathcal{B}_1 \cup \mathcal{B}_2)$ is a $(v, k, \lambda_1 + \lambda_2)$-design. So given a (v, k, λ)-design, it is easy to construct a $(v, k, d\lambda)$-design for any positive integer d. The resulting design is called a **multiple** of the original.

Theorem 2.2.1. If there exists a (v, k, λ)-design, then there exists a $(v, k, d\lambda)$-design for each positive integer d.

We now give another method for constructing a new design from an existing one.

Definition 2.2.2. The **complement** of a design $(V, \mathcal{B})$ is the design $(V, \mathcal{B}^c)$ where $\mathcal{B}^c = \{V \setminus B : B \in \mathcal{B}\}$. □

Theorem 2.2.3. If $k \leq v-2$, then the complement of a (v, k, λ)-design is a $(v, v-k, b-2r+\lambda)$-design.

Proof Let $(V, \mathcal{B})$ be a (v, k, λ)-design and let $(V, \mathcal{B}^c)$ be its complement. Clearly the blocks of $(V, \mathcal{B}^c)$ have size $v - k$. Now let x and y be an arbitrary pair of points. The number of blocks of $\mathcal{B}^c$ containing both x and y is the number of blocks of $\mathcal{B}$ that contain neither x nor y. The number of blocks of $\mathcal{B}$ containing at least one of x and y is the number containing x plus the number containing y minus the number containing both x and y. That is, $2r - \lambda$. Thus, the number of blocks of $\mathcal{B}^c$ containing both x and y is $b - 2r + \lambda$ as required. □

Example 2.2.4. The complement of a $(7, 3, 1)$-design is a $(7, 4, 2)$-design.

$$\begin{array}{ccccccc}
\{0,1,3\} & \{1,2,4\} & \{2,3,5\} & \{3,4,6\} & \{4,5,0\} & \{5,6,1\} & \{6,0,2\} \\
\{2,4,5,6\} & \{3,5,6,0\} & \{4,6,0,1\} & \{5,0,1,2\} & \{6,1,2,3\} & \{0,2,3,4\} & \{1,3,4,5\}
\end{array}$$

□

There are two ways of constructing new designs from symmetric designs, and they are both based on the following result.

Theorem 2.2.5. In a symmetric (v, k, λ)-design, $r = k$ and each pair of distinct blocks intersects in exactly λ points.

Proof Putting $b = v$ in Theorem 2.0.3 tells us that in a symmetric design we have

$$r = k \qquad \text{and} \qquad \lambda(v-1) = k(k-1).$$

Let the blocks be $B_1, B_2, \ldots, B_v$ and for $i = 1, 2, \ldots, v-1$, let $x_i = |B_i \cap B_v|$. Now, $x_1 + x_2 + \cdots + x_{v-1}$ counts the number of points of intersection between B_v and the other $v - 1$ blocks. Since B_v has k points and each such point occurs in $r - 1$ of the other $v - 1$ blocks, we have

$$x_1 + x_2 + \cdots + x_{v-1} = k(r-1) = k(k-1) = \lambda(v-1).$$

Also, $\binom{x_1}{2}+\binom{x_2}{2}+\cdots+\binom{x_{v-1}}{2}$ counts the number two-point intersections between B_v and the other $v-1$ blocks. Since B_v has $\binom{k}{2}$ pairs of points and each such pair occurs in $\lambda-1$ of the other $v-1$ blocks, we have

$$\binom{x_1}{2}+\binom{x_2}{2}+\cdots+\binom{x_{v-1}}{2}=\binom{k}{2}(\lambda-1)=\tfrac{\lambda(v-1)}{2}(\lambda-1)=\binom{\lambda}{2}(v-1).$$

Using the two displayed equations we can evaluate $x_1^2+x_2^2+\cdots+x_{v-1}^2$ as follows.

$$\begin{array}{rrcl}
 & \binom{x_1}{2}+\binom{x_2}{2}+\cdots+\binom{x_{v-1}}{2} & = & \binom{\lambda}{2}(v-1)\\
\to & \frac{1}{2}(x_1^2-x_1+x_2^2-x_2+\cdots+x_{v-1}^2-x_{v-1}) & = & \frac{1}{2}\lambda(\lambda-1)(v-1)\\
\to & x_1^2+x_2^2+\cdots+x_{v-1}^2-(x_1+x_2+\cdots+x_{v-1}) & = & \lambda(\lambda-1)(v-1)\\
\to & x_1^2+x_2^2+\cdots+x_{v-1}^2-\lambda(v-1) & = & \lambda(\lambda-1)(v-1)\\
\to & x_1^2+x_2^2+\cdots+x_{v-1}^2 & = & \lambda(\lambda-1)(v-1)+\lambda(v-1)\\
\to & x_1^2+x_2^2+\cdots+x_{v-1}^2 & = & \lambda^2(v-1)
\end{array}$$

Now consider the sum $(x_1-\lambda)^2+(x_2-\lambda)^2+\cdots+(x_{v-1}-\lambda)^2$. We have

$$\begin{array}{rl}
 & (x_1-\lambda)^2+(x_2-\lambda)^2+\cdots+(x_{v-1}-\lambda)^2\\
= & (x_1^2-2\lambda x_1+\lambda^2)+(x_2^2-2\lambda x_2+\lambda^2)+\cdots+(x_{v-1}^2-2\lambda x_{v-1}+\lambda^2)\\
= & (x_1^2+x_2^2+\cdots+x_{v-1}^2)-2\lambda(x_1+x_2+\cdots+x_{v-1})+\lambda^2(v-1)\\
= & \lambda^2(v-1)-2\lambda\cdot\lambda(v-1)+\lambda^2(v-1)\\
= & 0
\end{array}$$

Thus each of the terms in the sum $(x_1-\lambda)^2+(x_2-\lambda)^2+\cdots+(x_{v-1}-\lambda)^2$ is zero. That is, $x_1=x_2=\cdots=x_{v-1}=\lambda$. The same argument holds for any block (not just B_v) and so we see that each pair of blocks intersects in exactly λ points. □

Definition 2.2.6. Let $(V,\mathcal{B})$ be a (v,k,λ)-design and let $B^*\in\mathcal{B}$. The **derived design** of (V,B) with respect to B^* is the design $(B^*,\{B\cap B^*:B\in\mathcal{B}\setminus B^*\})$. The **residual design** of (V,B) with respect to B^* is the design $(V\setminus B^*,\{B\setminus B^*:B\in\mathcal{B}\setminus B^*\})$. □

If $(V,\mathcal{B})$ is a design, then it is routine to check that the complement of $(V,\mathcal{B})$'s derived design with respect to B^* is the residual design with respect to $V\setminus\mathcal{B}^*$ of the complement of $(V,\mathcal{B})$.

Theorem 2.2.7. The derived design of a symmetric (v,k,λ)-design is a $(k,\lambda,\lambda-1)$-design.

Proof Clearly the derived design has k points, and since distinct blocks of a symmetric (v,k,λ)-design intersect in exactly λ points (see Theorem 2.2.5), the derived design has blocks of constant size λ. Let x and y be distinct points of the derived design. Since x and y occur together in exactly λ blocks of the original symmetric design, they occur together in exactly $\lambda-1$ blocks of the derived design. □

Theorem 2.2.8. The residual design of a symmetric (v,k,λ)-design is a $(v-k,k-\lambda,\lambda)$-design.

Proof Clearly the residual design has $v-k$ points, and since distinct blocks of a symmetric (v,k,λ)-design intersect in exactly λ points (see Theorem 2.2.5), the residual design has blocks of constant size $k-\lambda$. Let x and y be distinct points of the residual design. Since x and y occur together in exactly λ blocks of the original symmetric design, it is clear that they also occur together in exactly λ blocks of the residual design. □

Example 2.2.9. The derived and residual designs of a symmetric $(19,9,4)$-design are a $(9,4,3)$-design and a $(10,5,4)$-design respectively. Below we give the blocks of a $(19,9,4)$-design, the derived $(9,4,3)$-design and the residual $(10,5,4)$-design, both with respect to the block $\{0,3,4,5,6,8,10,15,16\}$.

0	3	4	5	6	8	10	15	16									
1	4	5	6	7	9	11	16	17	4	5	6	16	1	7	9	11	17
2	5	6	7	8	10	12	17	18	5	6	8	10	2	7	12	17	18
3	6	7	8	9	11	13	18	0	0	3	6	8	7	9	11	13	18
4	7	8	9	10	12	14	0	1	0	4	8	10	1	7	9	12	14
5	8	9	10	11	13	15	1	2	5	8	10	15	1	2	9	11	13
6	9	10	11	12	14	16	2	3	3	6	10	16	2	9	11	12	14
7	10	11	12	13	15	17	3	4	3	4	10	15	7	11	12	13	17
8	11	12	13	14	16	18	4	5	4	5	8	16	11	12	13	14	18
9	12	13	14	15	17	0	5	6	0	5	6	15	9	12	13	14	17
10	13	14	15	16	18	1	6	7	6	10	15	16	1	7	13	14	18
11	14	15	16	17	0	2	7	8	0	8	15	16	2	7	11	14	17
12	15	16	17	18	1	3	8	9	3	8	15	16	1	9	12	17	18
13	16	17	18	0	2	4	9	10	0	4	10	16	2	9	13	17	18
14	17	18	0	1	3	5	10	11	0	3	5	10	1	11	14	17	18
15	18	0	1	2	4	6	11	12	0	4	6	15	1	2	11	12	18
16	0	1	2	3	5	7	12	13	0	3	5	16	1	2	7	12	13
17	1	2	3	4	6	8	13	14	3	4	6	8	1	2	13	14	17
18	2	3	4	5	7	9	14	15	3	4	5	15	2	7	9	14	18

□

2.3 Affine and Projective Planes

In this section we give a brief introduction to two very important and closely related families of designs, namely affine and projective planes.

Theorem 2.3.1. If $q=p^\alpha$ where p is prime and α is a positive integer, then there exists a $(q^2,q,1)$-design.

Proof Let F be a field of order q and let $V=F\times F$. For each $m\in F$ and each $c\in F$, let

$$B_{m,c}=\{(x,y)\in F\times F : y=mx+c\},$$

let

$$B_{\infty,c} = \{(x,y) \in F \times F : x = c\},$$

and let

$$\mathcal{B} = \{B_{m,c} : m \in F \cup \{\infty\}, c \in F\}$$

We show that $(V, \mathcal{B})$ is a $(q^2, q, 1)$-design. The number of blocks in $\mathcal{B}$ is $q(q+1)$, which is the number of blocks in a $(q^2, q, 1)$-design. Thus, it suffices to show that arbitrary distinct points $(x_1, y_1), (x_2, y_2) \in F \times F$ are covered by a block. If $x_1 = x_2$, then $(x_1, y_1), (x_2, y_2) \in B_{\infty, x_1}$. For $x_1 \neq x_2$, we let $m = \frac{y_2 - y_1}{x_2 - x_1}$ and let $c = y_1 - mx_1$ so that $mx_1 + c = y_1$ and

$$mx_2 + c = mx_2 + (y_1 - mx_1) = m(x_2 - x_1) + y_1 = \frac{y_2 - y_1}{x_2 - x_1}(x_2 - x_1) + y_1 = y_2.$$

Thus, $(x_1, y_1), (x_2, y_2) \in B_{m,c}$. □

Definition 2.3.2. Let $k \geq 2$ be an integer. A $(k^2, k, 1)$-design is called an **affine plane of order k**.

Theorem 2.3.3. Any affine plane is resolvable.

Proof Let $(V, \mathcal{B})$ be an affine plane of order k. The number of blocks is $b = \frac{k^2(k^2-1)}{k(k-1)} = k(k+1)$, and the replication number is $r = \frac{k^2-1}{k-1} = k+1$. Let B be a block and let $x \notin B$ be a point. Since there are k points in B, there are exactly k blocks containing x that intersect B. This implies that x is in exactly 1 block that does not intersect B. It follows that there are exactly $k-1$ blocks that are disjoint from B, and any two of these are pairwise disjoint. Thus, any block is in a unique resolution class. Further, since there are k blocks in any resolution class and k points in each block, any block not in a resolution class contains exactly one point from each block of the resolution class. Thus, $(V, \mathcal{B})$ is resolvable. □

Definition 2.3.4. Let $k \geq 2$ be an integer. A $(k^2+k+1, k+1, 1)$-design is called an **projective plane of order k**.

Theorem 2.3.5. There exist an affine plane of order k if and only if there exists a projective plane of order k.

Proof If $(V, \mathcal{B})$ is a projective plane of order k, then the residual with respect to any block is an affine plane of order k. Conversely, if $(V, \mathcal{B})$ is an affine plane of order k, then $(V, \mathcal{B})$ is resolvable by Theorem 2.3.3. Let $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_{k+1}$ be a resolution of $\mathcal{B}$ and let $\infty_1, \infty_2, \ldots, \infty_{k+1} \notin V$ be $k+1$ new points. Then

$$\{B \cup \{\infty_i\} : B \in \mathcal{B}_i, i = 1, 2, \ldots, k+1\} \cup \{\{\infty_1, \infty_2, \ldots, \infty_{k+1}\}\}$$

is the block set of a projective plane of order k with point set $V \cup \{\infty_1, \infty_2, \ldots, \infty_{k+1}\}$. □

Combining Theorems 2.3.5 and 2.3.1 we have the following result.

Corollary 2.3.6. If $q = p^\alpha$ where p is prime and α is a positive integer, then there exists an affine plane of order q and a projective plane of order q.

2.4 Necessary Conditions for Existence

The **incidence matrix** of a (v, k, λ)-design is a v by b matrix A, defined as follows. Suppose the design has point set $\{1, 2, \ldots, v\}$ and blocks $B_1, B_2, \ldots, B_b$. For $i = 1, 2, \ldots, v$ and $j = 1, 2, \ldots, b$, there is a 1 in row i and column j if $i \in B_j$ and otherwise there is a 0 in row i and column j.

The following theorem, known as **Fisher's Inequality**, gives an additional necessary condition for the existence of a (v, k, λ)-design. It was first proved by Fisher [9] in 1940.

Theorem 2.4.1. **(Fisher's Inequality)** If there exists a (v, k, λ)-design, then $v \leq b$.

Proof Let A be the incidence matrix of the design. Consider the v by v matrix $B = AA^T$. Since each point is covered by exactly r blocks, each diagonal entry of B is r. Since any pair of distinct points is covered by exactly λ blocks, each off-diagonal entry of B is λ.

$$B = AA^T = \begin{pmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & & & \lambda \\ \vdots & & & & \vdots \\ \lambda & \lambda & & \cdots & r \end{pmatrix}$$

It is easy to calculate the determinant of B. Subtract the first column from each other column, and then add rows $2, 3, \ldots, v$ to the first row. The resulting matrix is

$$\begin{pmatrix} r + \lambda(v-1) & 0 & 0 & \cdots & 0 \\ \lambda & r - \lambda & 0 & \cdots & 0 \\ \vdots & 0 & & & \vdots \\ \vdots & \vdots & & & 0 \\ \lambda & 0 & & \cdots & r - \lambda \end{pmatrix}$$

and so we see that the determinant of B is

$$\det(B) = (r + \lambda(v-1))(r - \lambda)^{v-1}.$$

Since a (v, k, λ)-design satisfies $v > k$, it follows from $r = \lambda \frac{v-1}{k-1}$ that $r > \lambda$. Thus $\det(B) \neq 0$ and B has rank v. Since A has rank at most b, and since the rank of a product of matrices cannot exceed the rank of either factor, we have $v \leq b$. □

Example 2.4.2. There is no $(16, 6, 1)$-design. If such a design exists then we have $b = \frac{16 \cdot 15}{6 \cdot 5} = 8$ so $b < v$ which is impossible by Fisher's Inequality. □

The following theorem gives additional necessary conditions (to those given in Theorem 2.0.4) for the existence of a symmetric (v, k, λ)-design. It is known as the Bruck-Ryser-Chowla Theorem. The part of the theorem relating to the case v is even was proven independently by Schützenberger [17] and Shrikhande [18] in 1949 and 1950 respectively. The part relating to the case v is odd is a combination of the results of Bruck and Ryser [6] (1949) and Chowla and Ryser [7] (1950). We will only prove the part relating to v even, the proof of the other part of the theorem can be found in most textbooks on design theory.

Theorem 2.4.3. **(Bruck-Ryser-Chowla Theorem)** If there exists a symmetric (v, k, λ)-design, then

- for v even, $k - \lambda$ is a perfect square; and
- for v odd, the equation $z^2 = (k - \lambda)x^2 + (-1)^{\frac{v-1}{2}}\lambda y^2$ has a solution where x, y and z are integers and not all zero.

Proof (of the part relating to v even). In a symmetric design we have $v = b$ so the incidence matrix A of a symmetric (v, k, λ)-design is a square matrix. Thus, it follows from the evaluation of the determinant of $B = AA^T$ given in the proof of Theorem 2.4.1 that

$$(\det(A))^2 = \det(B) = (r + \lambda(v - 1))(r - \lambda)^{v-1}.$$

Since $r = k$ and $\lambda(v - 1) = k(k - 1)$ in a symmetric design, we have $r + \lambda(v - 1) = k^2$. So

$$(\det(A))^2 = \det(B) = k^2(k - \lambda)^{v-1}.$$

Since $\det(A)$ is clearly an integer, it follows immediately from this that $k - \lambda$ is a perfect square when v is even. □

The following corollary gives the parameters of some small designs whose existence is ruled out by the Bruck-Ryser-Chowla Theorem.

Corollary 2.4.4. The following designs do not exist.

- $(22, 7, 2)$-design
- $(29, 8, 2)$-design
- $(34, 12, 4)$-design
- $(43, 7, 1)$-design
- $(43, 15, 5)$-design
- $(46, 10, 2)$-design
- $(53, 13, 3)$-design

Example 2.4.5. There is no $(22, 7, 2)$-design. If such a design exists, then we have $b = 2\frac{22\cdot 21}{7\cdot 6} = 22 = v$ and the Bruck-Ryser-Chowla Theorem tells us that $7 - 2 = 5$ is a perfect square, which is false. □

Example 2.4.6. There is no $(43, 7, 1)$-design. Suppose such a design exists. Then we have $b = \frac{43\cdot 42}{7\cdot 6} = 43 = v$. Hence the Bruck-Ryser-Chowla Theorem tells us that the equation

$$z^2 = 6x^2 - y^2$$

has a solution where x, y and z are integers and not all zero. Since we can cancel out any common factor of x, y and z, we can assume that x, y and z have no common factor. Now consider the possible congruences of x, y, and z modulo 3. Since $y^2 + z^2 = 6x^2$ we have $y^2 + z^2 \equiv 0 \pmod 3$ and so we have either $y^2 \equiv z^2 \equiv 0 \pmod 3$ or, without loss of generality, $y^2 \equiv 1 \pmod 3$ and $z^2 \equiv 2 \pmod 3$. But $z^2 \equiv 2 \pmod 3$ is impossible (as $0^2 \equiv 0 \pmod 3$, $1^1 \equiv 1 \pmod 3$ and $2^2 \equiv 1 \pmod 3$) and so it must be that $y^2 \equiv z^2 \equiv 0 \pmod 3$. Let $y = 3\alpha$ and $z = 3\beta$. Then we have $6x^2 = 9\alpha^2 + 9\beta^2$, from which it follows that $2x^2 = 3(\alpha^2 + \beta^2)$. So we see that $x \equiv 0 \pmod 3$. Thus, 3 divides x, y and z, and we have a contradiction to the assumption that x, y and z have no common factor. □

The next theorem was proved by Hall and Connor in 1954 [11].

Theorem 2.4.7. **(Hall-Connor Theorem)** Let $k \geq 5$ be an integer. Any $\left(\binom{k-1}{2}, k-2, 2\right)$-design is the residual of a symmetric $\left(\binom{k}{2} + 1, k, 2\right)$-design.

Proof Omitted. □

For parameters v, k and λ satisfying the obvious necessary conditions given in Theorem 2.0.4, Fisher's Inequality, the Bruck-Ryser-Chowla Theorem, and the Hall-Connor Theorem are essentially the only theoretical tools we have for establishing non-existence of (v, k, λ)-designs. However, large computer searches have been used to establish non-existence in the following cases. The first result is from 1989, the second is from 2001, and the third is from 2007.

Theorem 2.4.8. ([15]) There is no $(111, 11, 1)$-design and no $(100, 10, 1)$-design.

Theorem 2.4.9. ([13]) There is no $(46, 6, 1)$-design.

Theorem 2.4.10. ([4]) There is no $(22, 8, 4)$-design.

Chapter 3

Steiner Triple Systems

Groups are often useful in the construction of designs. We use the following notation and definitions on several occasions in Chapters 3 and 4. Let $(G, +)$ be a group and let $B = \{x_1, x_2, \ldots, x_k\} \subseteq G$. The **orbit** of B under G, denoted $G(B)$, is given by

$$G(B) = \{\{x_1 + g, x_2 + g, \ldots, x_k + g\} : g \in G\}.$$

Further, for $\{x_1, x_2, \ldots, x_{k-1}\} \subseteq G$ and $\infty \notin G$, the **orbit** $G(B)$ of $B = \{x_1, x_2, \ldots, x_{k-1}, \infty\}$ under G is given by

$$G(B) = \{\{x_1 + g, x_2 + g, \ldots, x_{k-1} + g, \infty\} : g \in G\}.$$

Example 3.0.1. Let $G = \mathbb{Z}_7$. The orbit of $T = \{0, 1, 3\}$ under the action of $\mathbb{Z}_7$ is

$$G(T) = \{\{0, 1, 3\}, \{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{0, 4, 5\}, \{1, 5, 6\}, \{0, 2, 6\}\}$$

and forms a $(7, 3, 1)$-design. □

Example 3.0.2. The union of the orbits of $\{\infty, 0, 1\}$ and $\{0, 1, 3\}$ under $\mathbb{Z}_5$ is the block set of a $(6, 3, 2)$-design with points set $\mathbb{Z}_5 \cup \{\infty\}$, see Example 2.0.2. □

3.1 Existence of Steiner Triple Systems

A $(v, 3, 1)$-design is called a **Steiner triple system**, and its blocks are called **triples**. Steiner triple systems are probably the most studied family of designs, perhaps along with Latin squares. It is often convenient to discuss Steiner triple systems in terms of graph decompositions: a Steiner triple system $(V, \mathcal{B})$ is equivalent to a K_3-decomposition of the complete graph with vertex set V.

In MATH2302 you may have seen the Bose construction and Skolem construction for Steiner triple systems of order $3 \pmod 6$ and order $1 \pmod 6$, respectively. In the next two lemmas we present some different constructions of Steiner triple systems.

Lemma 3.1.1. Let $t \geq 3$ be odd, let

$$\mathcal{B}_0 = \{\{(x,0),(-x,0),(0,1)\} : x = 1,2,\ldots,\tfrac{t-1}{2}\}, \text{ let } \quad \mathcal{B}_1 = \{\{(0,0),(0,1),(0,2)\}\},$$

and let $\mathcal{B}$ be the union of the orbits of the triples of $B_0 \cup B_1$ under $\mathbb{Z}_t \times \mathbb{Z}_3$. Then $(\mathbb{Z}_t \times \mathbb{Z}_3, \mathcal{B})$ is a Steiner triple system of order $3t$.

Proof It is clear that $(\mathbb{Z}_t \times \mathbb{Z}_3, \mathcal{B})$ is a design with $3t$ points and blocks of size 3. To show that the design is a Steiner triple system, we need to show that arbitrary distinct points $(i,j),(k,l) \in \mathbb{Z}_t \times \mathbb{Z}_3$ are covered by exactly one triple. It can be seen that $|\mathcal{B}_0| = \frac{t-1}{2}$ and that the union of the orbits of the triples of $\mathcal{B}_0$ contains $(3t)\frac{t-1}{2}$ triples. Since the orbit of $\{(0,0),(0,1),(0,2)\}$ has t triples (and since these orbits are disjoint), we thus have $|\mathcal{B}| = (3t)\frac{t-1}{2} + t = \frac{3t(3t-1)}{6}$, which is the number of triples in a Steiner triple system of order $3t$. Thus, it suffices to show that (i,j) and (k,l) are covered by at least one triple.

If $i = k$, then (i,j) and (k,l) are covered by $\{(i,0),(i,1),(i,2)\}$.

Now suppose $j = l$. Observe that if we define $\frac{1}{2} = \frac{t+1}{2} \in \mathbb{Z}_t$, then (working modulo t) the equation $2z = a$ has unique solution $z = \frac{1}{2}a$. Since t is odd, either $i-k$ or $k-i$ is in $\{2,4,\ldots,t-1\}$. Without loss of generality, we can assume $i-k \in \{2,4,\ldots,t-1\}$. Thus, if we let $x = \frac{1}{2}(i-k)$, then $x \in \{1,2,\ldots,\frac{t-1}{2}\}$,

$$x + \frac{1}{2}(i+k) = \frac{1}{2}(i-k) + \frac{1}{2}(i+k) = i \qquad \text{and} \qquad -x + \frac{1}{2}(i+k) = -\frac{1}{2}(i-k) + \frac{1}{2}(i+k) = k,$$

and it follows that (i,j) and (k,l) are covered by a triple in the orbit of a triple from $\mathcal{B}_0$.

Finally, suppose $i \neq k$ and $j \neq l$. Since $j, l \in \mathbb{Z}_3$ (and $j \neq l$) we have either $j - l = 1$ or $l - j = 1$. Without loss of generality, we can assume $l - j = 1$. Since the points $(i-k,0)$ and $(0,1)$ are covered by a triple of $\mathcal{B}_0$, and since $(i-k,0)+(k,j) = (i,j)$ and $(0,1)+(k,j) = (k,l)$, the points (i,j) and (k,l) are covered by a triple in the orbit of a triple from $\mathcal{B}_0$. □

Lemma 3.1.2. There is a Steiner triple system of order v for all $v \equiv 1 \pmod{6}$.

Proof Let $t = \frac{v-1}{6}$ and let $n = 2t$. Take a decomposition $\mathcal{P}$ into Hamilton paths of the complete graph with vertex set S where $|S| = n$. For example, we can take $S = \mathbb{Z}_n$ and $\mathcal{P} = \{H_0, H_1, \ldots, H_{\frac{n}{2}-1}\}$ where for $i = 0,1,\ldots,\frac{n}{2}-1$,

$$E(H_i) = \{xy : x,y \in \mathbb{Z}_n, x \neq y, x+y \in \{2i, 2i+1\}\}.$$

Note that $|\mathcal{P}| = t$. The point set of our Steiner triple system will be $V = (S \times \mathbb{Z}_3) \cup \{\infty\}$. So $|V| = v$.

Let $P = v_1, v_2, \ldots, v_{2t}$ be a path in $\mathcal{P}$ and for each $j \in \mathbb{Z}_3$ let $\mathcal{T}_j^P$ be the set consisting of the following triples.

- $\{(v_i,j),(v_{i+1},j),(v_1,j+1)\}$ for $i = 1,3,\ldots,2t-1$,
- $\{(v_i,j),(v_{i+1},j),(v_{2t},j+1)\}$ for $i = 2,4,\ldots,2t-2$,
- $\{(v_1,j),(v_{2t},j+1),\infty\}$,

- $\{(v_{2t},0),(v_{2t},1),(v_{2t},2)\}$.

Then

$$\bigcup_{P\in\mathcal{P}} \mathcal{T}_0^P \cup \mathcal{T}_1^P \cup \mathcal{T}_2^P$$

is the block set of a Steiner triple system of order v. □

Theorem 3.1.3. There exists a Steiner triple system of order v if and only if $v \equiv 1, 3 \pmod 6$.

Proof If there exists a Steiner triple system of order v, then there is decomposition into triangles of K_v. At each vertex $v \in K_v$, the triangles containing v partition the edges incident with v into pairs. Thus, v is odd. If $v \equiv 5 \pmod 6$, then the number of edges in K_v is congruent to $1 \pmod 3$, and it is not possible to partition the edges of K_v into triangles. We have shown that if there is a Steiner triple system of order v, then $v \equiv 1, 3 \pmod 6$ and we now prove the converse.

Trivially, there exist Steiner triple systems of orders 1 and 3, so we assume $v \geq 7$. If $v \equiv 1 \pmod 6$, then there exists a Steiner triple system of order v by Lemma 3.1.2, and if $v \equiv 3 \pmod 6$, then there exists a Steiner triple system of order v by Lemma 3.1.1. □

3.2 Maximum Packings

Definition 3.2.1. A **partial Steiner triple system** is a design whose blocks, called triples, each contain three points and each pair of points occurs in at most one triple. The **underlying graph** of a partial Steiner triple system $(V, \mathcal{B})$ is the graph with vertex set V and edge set given by joining x to y if and only if x and y occur together in some triple of $\mathcal{B}$. The **leave** of a partial Steiner triple system $(V, \mathcal{B})$ is the graph with vertex set V and edge set given by joining x to y if and only if x and y occur together in no triple of $\mathcal{B}$. □

The leave of a partial Steiner triple system may contain isolated vertices, and for convenience these are sometimes ignored. For example, the leave of a partial Steiner triple system of order v may be described as being a 4-cycle, when it actually consists of a 4-cycle and $v-4$ isolated vertices.

Lemma 3.2.2. For all $v \equiv 5 \pmod 6$, there exists a partial Steiner triple system of order v with a K_5 leave.

Proof The result is trivial for $v = 5$, so assume $v \geq 11$. Let $t = \frac{v-2}{3}$. So $t \geq 3$ is odd. We modify the Steiner triple system of order $3t$ given by Lemma 3.1.1 as follows. First, delete each of the triples in the orbit of $\{(0,0),(0,1),(0,2)\}$. Then let π be the permutation $(0)(1\ 2\ \cdots\ t-1)$ and replace each triple of the form $\{(x,2),(y,2),(z,0)\}$ (that is, those having exactly two points in $\mathbb{Z}_t \times \{2\}$) with the triple $\{(x,2),(y,2),(\pi(z),0)\}$. The result is a partial Steiner triple system of order $v-2$ whose leave is a 2-factor consisting of a 3-cycle, namely $((0,0),(0,1),(0,2))$, and a $(v-5)$-cycle. Let the $(v-5)$-cycle be $(x_1, x_2, \ldots, x_{v-5})$ and note that $v-5$ is even. Now add two new points ∞_1 and ∞_2 and add the triples $\{\infty_1, x_i, x_{i+1}\}$ for $i = 1, 3, \ldots, v-6$, $\{\infty_2, x_i, x_{i+1}\}$ for $i = 2, 4, \ldots, v-7$, and $\{\infty_2, x_1, x_{v-5}\}$. This is the required partial Steiner triple system with the K_5 leave having vertex set $\{(0,0),(0,1),(0,2),\infty_1,\infty_2\}$. □

Definition 3.2.3. A **maximum partial Steiner triple system of order v** is a partial Steiner triple system of order v with the property that no partial Steiner triple system of order v has more triples. □

Theorem 3.2.4. A maximum partial Steiner triple system of order v has μ_v triples and leave L_v where

- $\mu_v = \frac{v(v-1)}{6}$ and $L_v \cong K_v^c$ when $v \equiv 1, 3 \pmod 6$,
- $\mu_v = \frac{v(v-1)-8}{6}$ and $L_v \cong C_4$ when $v \equiv 5 \pmod 6$,
- $\mu_v = \frac{v(v-2)}{6}$ and L_v is a 1-factor when $v \equiv 0, 2 \pmod 6$,
- $\mu_v = \frac{v(v-2)-2}{6}$ and L_v is a graph whose components are $\frac{v-4}{2}$ copies of K_2 and one copy $K_{1,3}$ when $v \equiv 4 \pmod 6$.

Proof We first show that partial Steiner triple systems as given in the theorem exist. The case $v \equiv 1, 3 \pmod 6$ follows immediately from Theorem 3.1.3. For $v \equiv 5 \pmod 6$ we take a partial Steiner triple system of order v with a K_5 leave, see Theorem 3.2.2, and add two further triples. For $v \equiv 0, 2 \pmod 6$ we take a Steiner triple system of order $v+1$ and delete a point and all the triples containing that point. For $v \equiv 4 \pmod 6$ we take a partial Steiner triple system of order $v+1$ with a C_4 leave and delete a point of the C_4 together with all the triples containing that point.

We now show that any partial Steiner triple system of order v with μ_v triples has a leave isomorphic to L_v. Clearly, the leave G of any partial Steiner triple system of order v with μ_v triples satisfies $|E(G)| = |E(L_v)|$. Moreover each vertex x of G satisfies $\deg_G(x) \equiv v - 1 \pmod 2$. It is routine to check that these conditions imply $G \cong L_v$.

Finally, we need to check that there is no partial Steiner triple system of order v with more than μ_v triples. Suppose there is such a system and let G be its leave. Then $|E(G)| \leq |E(L_v)| - 3$ and each vertex x of G satisfies $\deg_G(x) \equiv v - 1 \pmod 2$. It is routine to check that no such graph G exists, and hence no partial Steiner triple system of order v with more than μ_v triples exists. □

Chapter 4

Pairwise Balanced and Group Divisible Designs

Definition 4.0.1. A **pairwise balanced design**, or **PBD**, is a design $(V, \mathcal{B})$ in which any pair of distinct points is covered by exactly one block. A pairwise balanced design $(V, \mathcal{B})$ with $v = |V|$ is called a (v, K)-PBD if $\{|B| : B \in \mathcal{B}\} \subseteq K$. □

The definition of pairwise balanced designs can be generalised so that pairs of distinct points are covered by exactly λ blocks (rather than by exactly one block), but we shall be only concerned with the case $\lambda = 1$. Note that if $2 \leq k < v$ and $K = \{k\}$, then a (v, K)-PBD is a $(v, k, 1)$-design.

The next lemma follows immediately from Lemma 3.2.2.

Lemma 4.0.2. If $v \equiv 5 \pmod 6$, then there exists a $(v, \{3, 5\})$-PBD.

Partial Steiner triple systems yield examples of $(v, \{2, 3\})$-PBDs, by taking the blocks of size three from the partial Steiner triple system and every pair not covered by the blocks of the partial Steiner triple system as a block of size two.

If $(V, \mathcal{B})$ is a PBD and $x \in V$, then $(V \setminus \{x\}, \{B \setminus \{x\} : B \in \mathcal{B}\})$ is also a PBD, and is called the PBD obtained from $(V, \mathcal{B})$ by **deleting the point** x.

Definition 4.0.3. A **group divisible design** consists of a design $(V, \mathcal{B})$, together with a partition $\mathcal{G}$ of the points into **groups**, such that no block covers distinct points from the same group, and such that any two points from distinct groups are covered by exactly one block. A group divisible design is usually denoted by the triple $(V, \mathcal{G}, \mathcal{B})$. □

Like in the case of pairwise balanced designs, the definition of group divisible designs can be generalised so that pairs of points from distinct groups are covered by exactly λ blocks (rather than by exactly one block), but we shall be only concerned with the case $\lambda = 1$.

Definition 4.0.4. If $(V, \mathcal{G}, \mathcal{B})$ is a group divisible design and $K = \{|B| : B \in \mathcal{B}\}$, then $(V, \mathcal{G}, \mathcal{B})$ is called a ***K*-GDD**. If $K = \{k\}$ then ***k*-GDD** may be used rather than $\{k\}$-GDD. If $\{g_1, g_2, \ldots, g_t\}$ is the set of group sizes (that is $\{g_1, g_2, \ldots, g_t\} = \{|G| : G \in \mathcal{G}\}$), and α_i is the number of groups of size g_i for $i = 1, 2, \ldots, t$, then $(V, \mathcal{G}, \mathcal{B})$ is said to be of **type** $g_1^{\alpha_1} g_2^{\alpha_2} \cdots g_t^{\alpha_t}$. □

If $(V, \mathcal{G}, \mathcal{B})$ is a GDD, then $(V, \mathcal{B} \cup \mathcal{G})$ is a PBD. We noted above that if $(V, \mathcal{B})$ is a PBD, then we can obtain a new PBD from $(V, \mathcal{B})$ by deleting a point. In fact we can also obtain a GDD from $(V, \mathcal{B})$. If x is the deleted point, then $\{B \setminus \{x\} : B \in \mathcal{B}, x \in B\}$ is the group set, and $\{B : B \in \mathcal{B}, x \notin B\}$ is the block set. We shall refer to this GDD as the GDD obtained from $(V, \mathcal{B})$ by **deleting the point** x.

We can also delete points from GDDs. If $(V, \mathcal{G}, \mathcal{B})$ is a GDD and $x \in V$, then $(V \setminus \{x\}, \{G \setminus \{x\} : G \in \mathcal{G}\}, \{B \setminus \{x\} : B \in \mathcal{B}\})$ is a GDD. This new GDD and the PBD obtained from it by including the groups as blocks, will be called respectively the GDD and PBD obtained from $(V, \mathcal{G}, \mathcal{B})$ by **deleting the point** x. From a GDD we can also obtain a PBD as follows. If $(V, \mathcal{G}, \mathcal{B})$ is a GDD and $\infty \notin V$, then $(V \cup \{\infty\}, \mathcal{B} \cup \{G \cup \{\infty\} : G \in \mathcal{G}\})$ is a PBD. This PBD will be called the PBD obtained from $(V, \mathcal{G}, \mathcal{B})$ by **adjoining a point**.

Theorem 4.0.5. For all $x \geq 1$, there exists a 3-GDD of type 2^{3x}, a 3-GDD of type 2^{3x+1}, and a 3-GDD of type $2^{3x}4^1$.

Proof Let v be the number of points in the required GDD. By Theorem 3.1.3 and Lemma 4.0.2, there exists a $(v+1, \{3,5\})$-PBD where there is exactly 1 block of size 5 when $v + 1 \equiv 5 \pmod 6$ and no blocks of size 5 otherwise. Let x be a point of such a PBD, where x is a point in the block of size 5 when $v + 1 \equiv 5 \pmod 6$ and x is chosen arbitrarily otherwise. Deleting the point x gives the required GDD. □

4.1 Some 3-GDDs and 4-GDDs, and Wilson's Construction for GDDs

In this section we state a few of the known existence results for 3-GDDs and 4-GDDs, and then we present Wilson's construction for GDDs. References for the stated results on 3-GDDs and 4-GDDs can be found in [10]. Many of the methods used in the construction of GDDs make extensive use of Wilson's construction for GDDs, which is given at the end of this section.

Theorem 4.1.1. For $u \geq 2$ and $g \geq 1$, there exists a 3-GDD of type g^u if and only if

- $u \geq 3$;
- $g(u-1)$ is even; and
- 3 divides $g^2\binom{u}{2}$.

Theorem 4.1.2. For $u \geq 2$ and $g, h \geq 1$, there exists a 3-GDD of type $g^u h^1$ if and only if

- $u \geq 3$ or $g = h$;
- $h \leq g(u-1)$;
- $g(u-1) + h$ is even;

- gu is even; and
- 3 divides $g^2\binom{u}{2} + guh$.

Theorem 4.1.3. For $u \geq 2$ and $g \geq 1$, there exists a 4-GDD of type g^u if and only if

- $u \geq 4$;
- 3 divides $g(u-1)$; and
- 6 divides $g^2\binom{u}{2}$;

except that there is no 4-GDD of type 2^4 and there is no 4-GDD of type 6^4.

We note that k-GDDs of type g^k are called transversal designs, and these are discussed in Section 4.2, and in later sections. The non-existence of 4-GDDs of type 2^4 and 6^4 will come up again there.

In Theorem 4.0.2 we constructed $(v, \{3,5\})$-PBDs with at most one block of size 5 for all odd v. These PBDs consist almost entirely of blocks of size 3. An analogous result for PBDs consisting almost entirely of blocks of size 4 was proved by Brouwer [5]. Brouwer showed that there is a $(v, \{4,7\})$-PBD with exactly one block of size 7 if and only if $v \equiv 7, 10 \pmod{12}$; except that there is no such PBD for $v \in \{10, 19\}$.

We now present Wilson's construction for GDDs [22]. This construction is used extensively in many branches of design theory. It is known as Wilson's fundamental construction for group divisible designs.

Theorem 4.1.4. If there exists an K_0-GDD of type $g_1^{\alpha_1}, g_2^{\alpha_2}, \ldots, g_t^{\alpha_t}$ and a K-GDD of type w^k for each $k \in K_0$, then there exists a K-GDD of type $(wg_1)^{\alpha_1}, (wg_2)^{\alpha_2}, \ldots, (wg_t)^{\alpha_t}$.

Proof Let I be a set of cardinality w, let $(V, \mathcal{G}, \mathcal{A})$ be a K_0-GDD of type $g_1^{\alpha_1}, g_2^{\alpha_2}, \ldots, g_t^{\alpha_t}$, and for each $A \in \mathcal{A}$, let $(A \times I, \{x \times I : x \in A\}, \mathcal{B}_A)$ be a K-GDD of type $w^{|A|}$. Then

$$(V \times I, \{G \times I : G \in \mathcal{G}\}, \{B \in \mathcal{B}_A : A \in \mathcal{A}\})$$

is a K-GDD of type $(wg_1)^{\alpha_1}, (wg_2)^{\alpha_2}, \ldots, (wg_t)^{\alpha_t}$. To see this, observe that if (x,i) and (y,j) are points from distinct groups, then there is unique block $A \in \mathcal{A}$ that covers x and y, and thus a unique block in $\mathcal{B}_A$ that covers (x,i) and (y,j). □

The construction used in the proof of Theorem 4.1.4 shall be called **inflating $(V, \mathcal{G}, \mathcal{A})$ by a factor of w**. Since a (v, K_0)-PBD is a K_0-GDD of type 1^v, we can also apply Theorem 4.1.4 to obtain a K-GDD of type w^v from a (v, K_0)-PBD (when there exists a K-GDD of type w^k for each $k \in K_0$). This shall be called **inflating the (v, K_0)-PBD by a factor of w**.

4.2 Constructing some Transversal Designs

Definition 4.2.1. Let $k \geq 3$. A **transversal design TD(k, m)** is a k-GDD of type m^k. □

There is a straightforward equivalence between a TD$(3, m)$ and a Latin square of side m. In Chapter 5 we shall see a correspondence between a TD(k, m) and a set of $k - 2$ mutually orthogonal Latin squares.

Theorem 4.2.2. For all $m \geq 1$, there exists a TD$(3, m)$.

Proof Let $V = \mathbb{Z}_m \times \mathbb{Z}_3$, let $\mathcal{G} = \{G_0, G_1, G_2\}$ where $G_0 = \mathbb{Z}_m \times \{0\}$, $G_1 = \mathbb{Z}_m \times \{1\}$ and $G_2 = \mathbb{Z}_m \times \{2\}$, and let

$$\mathcal{B} = \{\{(i, 0), (j, 1), (i + j, 2)\} : i, j \in \mathbb{Z}_m\}.$$

Then $(V, \mathcal{G}, \mathcal{B})$ is a TD$(3, m)$. □

Theorem 4.2.3. If there exists a TD(k, m), then there exists a TD(k', m) for all $3 \leq k' \leq k$.

Proof Suppose $(V, \mathcal{G}, \mathcal{B})$ is a TD(k, m), $\mathcal{G} = \{G_1, G_2, \ldots, G_k\}$ and $3 \leq k' \leq k$. If we let $V' = G_1 \cup G_2 \cup \cdots \cup G_{k'}$, let $\mathcal{G}' = \{G_1, G_2, \ldots, G_{k'}\}$, and let $\mathcal{B}' = \{B \cap V' : B \in \mathcal{B}\}$, then $(V', \mathcal{G}', \mathcal{B}')$ is a TD(k', m). □

Theorem 4.2.4. For $m \geq 2$, if there exists a TD(k, m), then $k \leq m + 1$.

Proof Let $m \geq 2$, let $(V, \{G_1, G_2, \ldots, G_k\}, \mathcal{B})$ be a TD(k, m), let x and y be distinct points in G_k, and let B_y be a block containing y. The point x is in m blocks whose union is $\{x\} \cup G_1 \cup G_2 \cup \cdots \cup G_{k-1}$ and B_y contains at most one point from each of these m blocks. Thus, $k = |B_y| \leq m + 1$. □

Theorem 4.2.5. There exists a TD$(m + 1, m)$ if and only if there exists a projective plane of order m.

Proof If we take a TD$(m + 1, m)$, add a new point ∞, and a new block $\{\infty\} \cup G$ for each group G of the TD$(m + 1, m)$, then the result is a projective plane of order m. Conversely, if we delete a point from a projective plane of order m, then we get a TD$(m + 1, m)$. □

Theorem 4.2.6. If there exists a TD(k, m) and a TD(k, n), then there exists a TD(k, mn).

Proof When there exists a TD(k, n), we can inflate a TD(k, m) by a factor of n to obtain the required TD(k, mn). □

The following theorem has a Latin square analogue which is known as MacNeish's Theorem and is discussed in Section 5, see Theorem 5.3.5.

Theorem 4.2.7. Let $p_1, p_2, \ldots, p_t$ be distinct primes, let $a_1, a_2, \ldots, a_t$ be positive integers, and let $m = p_1^{a_1}, p_2^{a_2}, \ldots, p_t^{a_t}$. Then there exists a TD$(k, m)$ where $k = \min\{p_i^{a_i} + 1 : i = 1, 2, \ldots, t\}$.

Proof For $i = 1, 2, \dots, t$, there exists a projective plane of order $p_i^{a_i}$ and hence a $\mathrm{TD}(p_i^{a_i} + 1, p_i^{\alpha_i})$ by Theorem 4.2.5. Hence, for $i = 1, 2, \dots, t$ there exists a $\mathrm{TD}(k, p_i^{a_i})$ where $k = \min\{p_i^{a_i} + 1 : i = 1, 2, \dots, t\}$ by Theorem 4.2.3. Theorem 4.2.6 thus gives us the required $\mathrm{TD}(k, m)$. □

Theorem 4.2.7 gives us a powerful method for constructing transversal designs. The following theorem contains some, but not all, of the results we obtain from it for $k \in \{4, 5, 6\}$.

Theorem 4.2.8. The following transversal designs exist.

(1) a $\mathrm{TD}(4, m)$ for all $m \equiv 0, 1$ or $3 \pmod 4$;

(2) a $\mathrm{TD}(5, m)$ for all $m \equiv 1, 4, 5, 7, 8$ or $11 \pmod{12}$;

(3) a $\mathrm{TD}(6, m)$ for all $m \equiv 1, 5, 7$ or $11 \pmod{12}$.

Proof The required transversal designs exist by Theorem 4.2.7 because when $m \equiv 0, 1$ or $3 \pmod 4$ each $p_i^{a_i}$ in the prime factorisation of m is at least 3, when $m \equiv 1, 4, 5, 7, 8$ or $11 \pmod{12}$ each $p_i^{a_i}$ in the prime factorisation of m is at least 4, and when $m \equiv 1, 5, 7$ or $11 \pmod{12}$ each $p_i^{a_i}$ in the prime factorisation of m is at least 5. □

4.3 Existence of $(v, 4, 1)$-designs

In this section, we make use of group divisible and pairwise balanced designs to completely settle the existence problem for $(v, 4, 1)$-designs, thus proving Theorem 2.1.3 for the case $\lambda = 1$ (see Theorem 4.3.5). We begin by verifying the existence of a $(v, 4, 1)$-design for $v \in \{13, 16, 25, 28, 37\}$. These designs shall be used as **ingredients** in the constructions that follow.

Theorem 4.3.1. For each $v \in \{13, 16, 25, 28, 37\}$, there exists a $(v, 4, 1)$-design.

Proof For $v = 13$ and $v = 16$ we can use a projective plane of order 3 and an affine plane of order 4 respectively.

The union of the orbits of the following two blocks under the action of the group $\mathbb{Z}_5 \times \mathbb{Z}_5$ is the block set of a $(25, 4, 1)$-design with point set $\mathbb{Z}_5 \times \mathbb{Z}_5$.

$$\{(0,0), (0,1), (1,0), (2,2)\} \qquad \{(0,0), (1,1), (1,3), (3,1)\}$$

The union of the orbits of the following two blocks under the action of the group $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ is the block set of a 4-GDD of type 3^9 with point set $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ and group set $\{\{(x, y, 0), (x, y, 1), (x, y, 2)\} : x, y \in \mathbb{Z}_3\}$.

$$\{(0,0,0), (0,2,0), (1,1,1), (2,1,1)\} \qquad \{(0,0,0), (0,1,2), (1,0,2), (1,1,0)\}$$

Adjoining a point to this 4-GDD gives us a $(28, 4, 1)$-design.

The union of the orbits of the following three blocks under the action of the group $\mathbb{Z}_{37}$ is the block set of a $(37, 4, 1)$-design with point set $\mathbb{Z}_{37}$.

$$\{0, 1, 3, 24\} \qquad \{0, 4, 26, 32\} \qquad \{0, 8, 20, 27\}$$

□

Theorem 4.3.2. If there exists an $(n, \{4, 5, 8, 9, 12\})$-PBD for all $n \equiv 0, 1 \pmod 4$, then there exists a $(v, 4, 1)$-design for all $v \equiv 1, 4 \pmod{12}$.

Proof Deleting a point from a $(v, 4, 1)$-design yields a 4-GDD of type $3^{\frac{v-1}{3}}$. Thus, by Theorem 4.3.1 there exists a 4-GDD of type 3^t for each $t \in \{4, 5, 8, 9, 12\}$. We can thus inflate any $(n, \{4, 5, 8, 9, 12\})$-PBD by a factor of 3 (see Theorem 4.1.4) to obtain a 4-GDD of type 3^n. Adjoining a point to a 4-GDD of type 3^n yields a $(v, 4, 1)$-design with $v = 3n + 1$. Thus, if there exists an $(n, \{4, 5, 8, 9, 12\})$-PBD for all $n \equiv 0, 1 \pmod 4$, then there exists a $(v, 4, 1)$-design for all $v \equiv 1, 4 \pmod{12}$. □

In view of Theorem 4.3.2, we aim to construct an $(n, \{4, 5, 8, 9, 12\})$-PBD for all $n \equiv 0, 1 \pmod 4$. We begin with some examples for small values of n, and then prove the result by induction on n.

Theorem 4.3.3. For each $n \leq 49$ with $n \equiv 0$ or $1 \pmod 4$, there exists an $(n, \{4, 5, 8, 9, 12\})$-PBD.

Proof For $n \in \{4, 5, 8, 9, 12\}$ the required design contains only one block and is thus trivial to construct. For $n \in \{13, 16, 25, 28, 37\}$ we simply use an $(n, 4, 1)$-design from Theorem 4.3.1. This leaves us with the following values of n.

$$17, 20, 21, 24, 29, 32, 33, 36, 40, 41, 44, 45, 48, 49$$

In what follows, we deal with each of these by using various transversal designs which exist by Theorems 4.2.3, 4.2.5 and 4.2.8.

For $n = 17$ we adjoin a point to a TD$(4, 4)$ to obtain a $(17, \{4, 5\})$-PBD. A projective plane of order 4 is a $(21, \{5\})$-PBD, and by deleting a point we obtain a $(20, \{4, 5\})$-PBD. An affine plane of order 5 is a $(25, \{5\})$-PBD, and by deleting a point we obtain a $(24, \{4, 5\})$-PBD. For $n = 29$ we adjoin a point to a TD$(4, 7)$ to obtain a $(29, \{4, 8\})$-PBD. The blocks and groups of a TD$(4, 8)$ yield a $(32, \{4, 8\})$-PBD, and adjoining a point yields a $(33, \{4, 9\})$-PBD. The blocks and groups of a TD$(4, 9)$ yield a $(36, \{4, 9\})$-PBD.

The blocks and groups of a TD$(5, 8)$ yield a $(40, \{5, 8\})$-PBD, and adjoining a point yields a $(41, \{5, 9\})$-PBD. We construct a $(44, \{4, 5, 8, 9\})$-PBD by deleting a point from a TD$(5, 9)$, and the blocks and groups of the TD$(5, 9)$ itself give us a $(45, \{5, 9\})$-PBD. The blocks and groups of a TD$(4, 12)$ yield a $(48, \{4, 12\})$-PBD, and adjoining a point yields a $(49, \{4, 13\})$-PBD. Replacing each block B of size 13 in a $(49, \{4, 13\})$-PBD with the blocks of $(13, 4, 1)$-design having point set B yields a $(49, \{4\})$-PBD, in fact a $(49, 4, 1)$-design. □

Theorem 4.3.4. For all $n \equiv 0$ or $1 \pmod 4$, there exists an $(n, \{4, 5, 8, 9, 12\})$-PBD.

Proof The proof is by induction on n. Theorem 4.3.3 gives us an $(n, \{4, 5, 8, 9, 12\})$-PBD for all $n \le 49$ with $n \equiv 0$ or $1 \pmod 4$. So let $n \ge 52$ with $n \equiv 0$ or $1 \pmod 4$ and suppose we have constructed an $(n', \{4, 5, 8, 9, 12\})$-PBD for all $n' < n$ with $n' \equiv 0$ or $1 \pmod 4$.

Now, if there exists a TD$(5, t)$ where $t \equiv 0$ or $1 \pmod 4$ and $4t \le n \le 5t$, then we can construct an $(n, \{4, 5, 8, 9, 12\})$-PBD as follows. Delete $5t - n$ points from one group of a TD$(5, t)$ and let $(V, \mathcal{B})$ be the resulting $(n, \{4, 5, t, n - 4t\})$-PBD. If $n = 4t$ or $n = 4t + 1$ respectively, then $(V, \mathcal{B})$ is an $(n, \{4, t\})$-PBD or an $(n, \{4, 5, t\})$-PBD respectively. By induction, and since $t \equiv 0$ or $1 \pmod 4$ and $n \equiv 0$ or $1 \pmod 4$, there exists a $(t, \{4, 5, 8, 9, 12\})$-PBD and an $(n - 4t, \{4, 5, 8, 9, 12\})$-PBD. If we replace each block B of $\mathcal{B}$ that has size t with a $(t, \{4, 5, 8, 9, 12\})$-PBD on the point set B, and replace any block B' of $\mathcal{B}$ that has size $n - 4t$ (B' is present only when $n > 4t + 1$, and $|B'| = t$ if $n = 5t$) with an $(n - 4t, \{4, 5, 8, 9, 12\})$-PBD, then we obtain an $(n, \{4, 5, 8, 9, 12\})$-PBD.

Thus, we only need to show that there exists a TD$(5, t)$ for some t such that $t \equiv 0$ or $1 \pmod 4$ and $4t \le n \le 5t$. We choose $t \equiv 1, 4, 5$ or $8 \pmod{12}$, so that there exists a TD$(5, t)$ by Theorem 4.2.8. Using $n \ge 52$, it is routine to check that such a t exists. For example, $t = 13$ covers $52 \le n \le 65$, $t = 16$ covers $64 \le n \le 80$, $t = 17$ covers $68 \le n \le 85$, $t = 20$ covers $80 \le n \le 100$, $t = 25$ covers $100 \le n \le 125$, and so on. □

The above results give us the main result of this section.

Theorem 4.3.5. There exists a $(v, 4, 1)$-design if and only if $v \equiv 1$ or $4 \pmod{12}$.

Proof If there exists a $(v, 4, 1)$-design then by Theorem 2.0.4, we have 12 divides $v(v - 1)$ and $v \equiv 1 \pmod 3$, from which it follows that $v \equiv 1$ or $4 \pmod{12}$. Conversely, by Theorems 4.3.2 and 4.3.4 there exists a $(v, 4, 1)$-design for all $v \equiv 1$ or $4 \pmod{12}$. □

4.4 Wilson's Construction for Transversal Designs

The following theorem was proved by Wilson in 1974 [23]. It is known as Wilson's fundamental construction for transversal designs.

Theorem 4.4.1. If there exists a TD(k, m), a TD$(k, m + 1)$, a TD$(k + 1, t)$, and a TD(k, u), where $0 \le u \le t$, then there exists a TD$(k, mt + u)$.

Proof Delete $t - u$ points from a group of a TD$(k + 1, t)$ to obtain a $\{k, k + 1\}$-GDD of type t^k, u^1. Let this GDD be $(V, \mathcal{G}, \mathcal{A})$, let $\mathcal{G} = \{G_1, G_2, \ldots, G_{k+1}\}$ where G_{k+1} is the group of size u, let $\mathcal{A}_k = \{A \in \mathcal{A} : |A| = k\}$, and let $\mathcal{A}_{k+1} = \{A \in \mathcal{A} : |A| = k + 1\}$. So $\mathcal{A} = \mathcal{A}_k \cup \mathcal{A}_{k+1}$, $A \in \mathcal{A}_k$ when $A \cap G_{k+1} = \emptyset$, and $A \in \mathcal{A}_{k+1}$ otherwise. Let $M = \{1, 2, \ldots, m\}$. The group set of our TD$(k, mt + u)$ is $\{(G_i \times M) \cup (\{i\} \times G_{k+1}) : i = 1, 2, \ldots, k\}$ (and the point set is the union of the groups).

We now construct the block set. For each block $A \in \mathcal{A}_k$ let $(A \times M, \{x \times M : x \in A\}, \mathcal{B}_A)$ be a TD(k, m). For each block $A = \{a_1, a_2, \ldots, a_{k+1}\} \in \mathcal{A}_{k+1}$ where $a_i \in G_i$ for $i = 1, 2, \ldots, k + 1$, let $\mathcal{B}_A \cup (\{1, 2, \ldots, k\} \times \{a_{k+1}\})$ be the block set of a TD$(k, m + 1)$ with group set

$$\{(\{a_i\} \times M) \cup \{(i, a_{k+1})\} : i = 1, 2, \ldots, k\}.$$

Let $\mathcal{B}^*$ be the block set of a TD(k,u) with group set $\{\{i\} \times G_{k+1} : i = 1,2,\dots,k\}$.

It is routine to check that $\{B \in \mathcal{B}_A : A \in \mathcal{A}\} \cup \mathcal{B}^*$ is the block set of a TD$(k, mt+u)$ with points and groups as defined above. First check that the number of blocks is $(mt+u)^2$, and then check that each pair of points from distinct groups occurs in a block as follows. If (x,i) and (y,j) are points in $(G_1 \cup G_2 \cup \cdots \cup G_k) \times M$ from distinct groups, then (x,i) and (y,j) occur together in a block in $\mathcal{B}_A$ where A is the unique block in $\mathcal{A}_k$ or $\mathcal{A}_{k+1}$ that contains x and y. If $(x,i) \in (G_1 \cup G_2 \cup \cdots \cup G_k) \times M$, $(j,y) \in \{1,2,\dots,k\} \times G_{k+1}$, and $x \notin G_j$ (so that (x,i) and (j,y) are from distinct groups) then (x,i) and (j,y) occur together in a block in $\mathcal{B}_A$ where A is the unique block in $\mathcal{A}_{k+1}$ that contains x and y. Finally, if $(i,x),(j,y) \in \{1,2,\dots,k\} \times G_{k+1}$ with $i \neq j$ (so that (i,x) and (j,y) are from distinct groups), then (i,x) and (j,y) occur together in a block in $\mathcal{B}^*$. □

4.5 Transversal Designs with Block Size 4

Theorem 4.5.1. There exists a TD$(4,n)$ if and only if $n \notin \{2,6\}$.

Proof It is easy to see that there is no TD$(4,2)$, and indeed the existence of a TD$(4,2)$ is ruled out by Theorem 4.2.4. The non-existence of a TD$(4,6)$ has been verified by exhaustive search [20]. By Theorem 4.2.8, there exists a TD$(4,n)$ for all $n \equiv 0, 1$ or $3 \pmod 4$. So it remains to construct a TD$(4,n)$ when $n \geq 10$ and $n \equiv 2 \pmod 4$. To do this we use Theorem 4.4.1 with $k = 4$ and $m = 3$.

Write n as $36x+y$ where $2 \leq y \leq 34$, and define t and u as in the following table so that $n = mt+u$ where $m = 3$.

n	$36x+2$	$36x+6$	$36x+10$	$36x+14$	$36x+18$
$3t+u$	$3(12x-1)+5$	$3(12x+1)+3$	$3(12x+1)+7$	$3(12x+1)+11$	$3(12x+5)+3$

n	$36x+22$	$36x+26$	$36x+30$	$36x+34$
$3t+u$	$3(12x+5)+7$	$3(12x+7)+5$	$3(12x+7)+9$	$3(12x+7)+13$

There exists a TD$(4,3)$, a TD$(4,4)$, and we have defined t and u so that $t \equiv 1, 5, 7$ or $11 \pmod{12}$ and $u \in \{3,5,7,9,11,13\}$. Thus, by Theorem 4.2.8, there exists a TD$(5,t)$ and a TD$(4,u)$. Hence by Theorem 4.4.1, there exists a TD$(4,n)$ whenever $0 \leq u \leq t$. This leaves only $n \in \{10,14,22,30,34\}$.

In Section 5 we show that a TD$(4,n)$ is equivalent to a pair of orthogonal Latin squares of side n (two Latin squares are orthogonal if each ordered pair of symbols occurs exactly once when they are superimposed). Briefly, if I is the set of symbols occurring in the squares and we index (in the same order for each square) the rows and columns of each square with I so that the squares act as tables for two binary operations $*_1$ and $*_2$ defined on I, then

$$(I \times \{1,2,3,4\}, \mathcal{G}, \{\{(i,1),(j,2),(i *_1 j, 3),(i *_2 j, 4)\} : i,j \in I\})$$

where $\mathcal{G} = \{I \times \{1\}, I \times \{2\}, I \times \{3\}, I \times \{4\}\}$ is a TD$(4,n)$.

Shown below are a pair of orthogonal Latin squares of side 10, and a pair of orthogonal Latin squares of side 14. Thus, there exists a TD$(4,10)$ and a TD$(4,14)$.

0	*A*	1	*B*	2	*C*	3	6	5	4
4	1	*A*	2	*B*	3	*C*	0	6	5
C	5	2	*A*	3	*B*	4	1	0	6
5	*C*	6	3	*A*	4	*B*	2	1	0
B	6	*C*	0	4	*A*	5	3	2	1
6	*B*	0	*C*	1	5	*A*	4	3	2
A	0	*B*	1	*C*	2	6	5	4	3
1	2	3	4	5	6	0	*A*	*B*	*C*
2	3	4	5	6	0	1	*C*	*A*	*B*
3	4	5	6	0	1	2	*B*	*C*	*A*

0	4	*A*	5	*B*	6	*C*	1	2	3
C	1	5	*A*	6	*B*	0	2	3	4
1	*C*	2	6	*A*	0	*B*	3	4	5
B	2	*C*	3	0	*A*	1	4	5	6
2	*B*	3	*C*	4	1	*A*	5	6	0
A	3	*B*	4	*C*	5	2	6	0	1
3	*A*	4	*B*	5	*C*	6	0	1	2
6	0	1	2	3	4	5	*A*	*C*	*B*
5	6	0	1	2	3	4	*C*	*B*	*A*
4	5	6	0	1	2	3	*B*	*A*	*C*

0	4	6	*C*	1	3	5	2	9	*B*	*A*	8	7	*X*
A	1	5	7	*C*	2	4	6	3	*X*	*B*	9	8	0
B	*A*	2	6	8	*C*	3	5	7	4	0	*X*	9	1
1	*B*	*A*	3	7	9	*C*	4	6	8	5	0	*X*	2
6	2	*B*	*A*	4	8	*X*	*C*	5	7	9	1	0	3
X	7	3	*B*	*A*	5	9	0	*C*	6	8	2	1	4
9	0	8	4	*B*	*A*	6	*X*	1	*C*	7	3	2	5
8	*X*	1	9	5	*B*	*A*	7	0	2	*C*	4	3	6
C	9	0	2	*X*	6	*B*	*A*	8	1	3	5	4	7
4	*C*	*X*	1	3	0	7	*B*	*A*	9	2	6	5	8
3	5	*C*	0	2	4	1	8	*B*	*A*	*X*	7	6	9
7	8	9	*X*	0	1	2	3	4	5	6	*A*	*B*	*C*
5	6	7	8	9	*X*	0	1	2	3	4	*C*	*A*	*B*
2	3	4	5	6	7	8	9	*X*	0	1	*B*	*C*	*A*

0	A	B	1	6	X	9	8	C	4	3	7	5	2
4	1	A	B	2	7	0	X	9	C	5	8	6	3
6	5	2	A	B	3	8	1	0	X	C	9	7	4
C	7	6	3	A	B	4	9	2	1	0	X	8	5
1	C	8	7	4	A	B	5	X	3	2	0	9	6
3	2	C	9	8	5	A	B	6	0	4	1	X	7
5	4	3	C	X	9	6	A	B	7	1	2	0	8
2	6	5	4	C	0	X	7	A	B	8	3	1	9
9	3	7	6	5	C	1	0	8	A	B	4	2	X
B	X	4	8	7	6	C	2	1	9	A	5	3	0
A	B	0	5	9	8	7	C	3	2	X	6	4	1
8	9	X	0	1	2	3	4	5	6	7	A	C	B
7	8	9	X	0	1	2	3	4	5	6	C	B	A
X	0	1	2	3	4	5	6	7	8	9	B	A	C

For $n = 22$ we apply Theorem 4.4.1 with $k = 4$, $m = 3$, $t = 7$ and $u = 1$ using a TD$(4, 3)$, a TD$(4, 4)$, a TD$(5, 7)$ and a TD$(4, 1)$. For $n = 30$, we apply Theorem 4.4.1 with $k = 4$, $m = 3$, $t = 9$ and $u = 3$ using a TD$(4, 3)$, a TD$(4, 4)$, and a TD$(5, 9)$. Alternatively, we could obtain a TD$(4, 30)$ by applying Theorem 4.2.6 using a TD$(4, 3)$ and the TD$(4, 10)$ given above. For $n = 34$ we apply Theorem 4.4.1 with $k = 4$, $m = 3$, $t = 9$ and $u = 7$ using a TD$(4, 3)$, a TD$(4, 4)$, a TD$(5, 9)$ and a TD$(4, 7)$. □

Chapter 5

Orthogonal Arrays and Latin Squares

5.1 Orthogonal Arrays

We now introduce an alternative presentation of a TD(k, m).

Definition 5.1.1. Let $k \geq 2$ and $m \geq 1$ be integers. An **orthogonal array**, denoted OA(k, m), is an $m^2 \times k$ array A, with entries from a set X of size m such that within any two columns of A, every ordered pair of elements from X occurs in exactly one row. □

Example 5.1.2. An $OA(4, 3)$ with entries from the set $\{1, 2, 3\}$.

$$\begin{array}{cccc}
1 & 1 & 1 & 1 \\
1 & 2 & 2 & 2 \\
1 & 3 & 3 & 3 \\
2 & 1 & 2 & 3 \\
2 & 2 & 3 & 1 \\
2 & 3 & 1 & 2 \\
3 & 1 & 3 & 2 \\
3 & 2 & 1 & 3 \\
3 & 3 & 2 & 1
\end{array}$$

□

We often denote the symbol in row i and column j of the array A by $A(i, j)$. We observe that an $OA(2, m)$ exists trivially for all integers $m \geq 1$.

We now show that an OA(k, m) is equivalent to a TD(k, m). Let A be an OA(k, m) on symbol set $\{1, 2, \ldots, m\}$. Label the columns of A as $1, 2, \ldots, k$ and label the rows of A as $1, 2, \ldots, m^2$. Define

$$V = \{1, 2, \ldots, m\} \times \{1, 2, \ldots, k\}$$

and for each $i \in \{1, 2, \ldots, k\}$, define

$$G_i = \{1, 2, \ldots, m\} \times \{i\} \text{ and let } \mathcal{G} = \{G_i : 1 \leq i \leq k\}.$$

For each $r \in \{1, 2, \ldots, m^2\}$, define

$$B_r = \{(A(r, i), i) : 1 \leq i \leq k\}, \text{ and let } \mathcal{B} = \{B_r : 1 \leq r \leq m^2\}.$$

Then it is clear that $(V, \mathcal{G}, \mathcal{B})$ is a k-GDD of type m^k, that is a $\mathrm{TD}(k, m)$.

Example 5.1.3. Applying the above construction to the $\mathrm{OA}(4, 3)$ from Example 5.1.2 we obtain the following $\mathrm{TD}(4, 3)$. The groups are

$$G_i = \{(1, i), (2, i), (3, i)\} \text{ for } i = 1, 2, 3, 4$$

and the blocks are

$$\begin{aligned}
B_1 &= \{(1,1),(1,2),(1,3),(1,4)\}\\
B_2 &= \{(1,1),(2,2),(2,3),(2,4)\}\\
B_3 &= \{(1,1),(3,2),(3,3),(3,4)\}\\
B_4 &= \{(2,1),(1,2),(2,3),(3,4)\}\\
B_5 &= \{(2,1),(2,2),(3,3),(1,4)\}\\
B_6 &= \{(2,1),(3,2),(1,3),(2,4)\}\\
B_7 &= \{(3,1),(1,2),(3,3),(2,4)\}\\
B_8 &= \{(3,1),(2,2),(1,3),(3,4)\}\\
B_9 &= \{(3,1),(3,2),(2,3),(1,4)\}
\end{aligned}$$

□

This construction can be reversed. Given a $\mathrm{TD}(k, m)$, $(V, \mathcal{G}, \mathcal{B})$, relabel the points if necessary so that $V = \{1, 2, \ldots, m\} \times \{1, 2, \ldots, k\}$ and $\mathcal{G} = \{G_i : 1 \leq i \leq k\}$ where $G_i = \{1, 2, \ldots, m\} \times \{i\}$ for $i = 1, 2, \ldots, k$. For each block $B \in \mathcal{B}$ and for $i = 1, 2, \ldots, k$, let (b_i, i) be the unique point in $B \cap G_i$ (recall that each block intersects each group in a unique point). Then, for each $B \in \mathcal{B}$, form the k-tuple $(b_1, b_2, \ldots, b_k)$. Construct an array A whose rows consist of all these k-tuples. It is clear that A is an $\mathrm{OA}(k, m)$.

5.2 Latin Squares

The position in row i and column j of an array is called **cell** (i, j). The elements occurring in the cells of an array are called **symbols**. We will be typically dealing with arrays in which each cell contains a unique symbol, but will also discuss arrays which are **partially filled**. That is, arrays in which some cells are **filled** (contain a symbol) and some are **empty** (contain no symbol). In an array L, if cell (i, j) is filled, then the symbol occurring in it is denoted by $L(i, j)$.

Definition 5.2.1. Let N be an set of size n. A **Latin square of order** n is an n by n array in which each cell contains a unique element of N, each row contains every element of N exactly once, and each column contains every element of N exactly once. □

It is easy to construct a Latin square of order n for any positive integer n. For example, if $(\{g_1, g_2, \ldots, g_n\}, *)$ is any group, then we can define $M(i,j) = g_i * g_j$ for $1 \leq i,j \leq n$. Another way of constructing a Latin square of order n is to define $M(i,j) \equiv j - i \pmod{n}$ for $1 \leq i,j \leq n$. Notice that in general the elements of $\mathbb{Z}_n$ do not form a group under the binary operation $*$ defined by $x * y = y - x \pmod{n}$ (the operation $*$ is not associative).

Definition 5.2.2. A set Q together with a binary operation $*$ is a **quasigroup** $(Q, *)$ if and only if for all $a, b \in Q$, the equations $a * x = b$ and $x * a = b$ each have a unique solution $x \in Q$. □

It is easy to see that there are strong connections between the following.

A Latin square of order n.	A quasigroup of order n.
A transversal design $\mathrm{TD}(3,n)$.	An orthogonal array $\mathrm{OA}(3,n)$.
A K_3-decomposition of $K_{n,n,n}$.	A 1-factorisation of $K_{n,n}$.
A proper n-edge-colouring of $K_{n,n}$.	

5.3 Orthogonal Latin squares

Definition 5.3.1. If L and L' are Latin squares of order n, each with symbol set N, then L and L' are **orthogonal** if and only if

$$\{(L(i,j), L'(i,j)) : 1 \leq i,j \leq n\} = N \times N.$$

Latin squares $L_1, L_2, \ldots, L_k$ are **mutually orthogonal** if L_i is orthogonal to L_j for $1 \leq i < j \leq k$. □

Euler's famous 36 officers problem from 1782 asks for a pair of orthogonal Latin squares of order 6. Euler knew of the existence of a pair of orthogonal Latin squares of order n for each $n \in \{3,4,5,7,8,9\}$, and it is easy to see that there is no pair of orthogonal Latin squares of order 2. Euler correctly conjectured that there was no solution to his 36 officers problem, but incorrectly conjectured further that there is no pair of orthogonal Latin squares of order n for any $n \equiv 2 \pmod{4}$. We shall show in fact that there exists a pair of orthogonal Latin squares of order n for all n except $n = 2$ and $n = 6$.

First we describe an equivalence between mutually orthogonal Latin squares and orthogonal arrays. Suppose $L_1, L_2, \ldots, L_k$ are mutually orthogonal Latin squares of order n, each with symbol set $\{1, 2, \ldots, n\}$, and with rows and columns labelled $1, 2, \ldots, n$. We can construct an $\mathrm{OA}(k+2, n)$ from $L_1, L_2, \ldots, L_k$ as follows. For every $i, j \in \{1, 2, \ldots, n\}$, construct a $(k+2)$-tuple

$$(i, j, L_1(i,j), L_2(i,j), \ldots, L_k(i,j)).$$

Then the array A whose rows consist of these n^2 $(k+2)$-tuples is an $OA(k+2, n)$.

To show that A is an $OA(k+2, n)$, we need to show that every ordered pair from $\{1, 2, \ldots, n\}$ occurs in any two columns a and b where $1 \leq a < b \leq k+2$. Consider columns a and b.

1. If $a = 1$ and $b = 2$, then we get every ordered pair by the choice of $i, j \in \{1, 2, \ldots, n\}$.
2. If $a = 1$ and $b \geq 3$, then we get every ordered pair because each row of a Latin square contains each symbol exactly once.
3. If $a = 2$ and $b \geq 3$, then we get every ordered pair because each column of a Latin square contains each symbol exactly once.
4. If $a \geq 3$, then we get every ordered pair because every pair of Latin squares from $L_1, L_2, \ldots, L_k$ is orthogonal.

The process can be reversed: Given any orthogonal array $OA(k + 2, n)$, let the first column correspond to the row labels and the second column correspond to the column labels. The remaining k columns then give the entries for k mutually orthogonal Latin squares of order n.

In view of the equivalence just described, and noting that an $\mathrm{OA}(k, n)$ is equivalent to a $\mathrm{TD}(k, n)$, we have the following theorem.

Theorem 5.3.2. There exist k mutually orthogonal Latin squares of order n if and only if there exists a $\mathrm{TD}(k + 2, n)$.

Theorem 5.3.2 allows us to use existence results and constructions for transversal designs from Chapter 4 in the context of mutually orthogonal Latin squares. For example, since Theorem 4.2.4 says that if there exists a $\mathrm{TD}(k, n)$, then $k \leq n + 1$, we know that there is no set of more than $n - 1$ mutually orthogonal Latin squares of order n. A set of $n - 1$ mutually orthogonal Latin squares of order n is called a **complete set**. The existence of a complete set of mutually orthogonal Latin squares of order n is equivalent to the existence of a $\mathrm{TD}(n+1, n)$, and in view of Theorem 4.2.5, also equivalent to the existence of a projective plane of order n. We state these observations as a theorem.

Theorem 5.3.3. The following statements are equivalent.

- There exists a complete set of $n - 1$ mutually orthogonal Latin squares of order n.
- There exists an $\mathrm{OA}(n + 1, n)$.
- There exists a $\mathrm{TD}(n + 1, n)$.
- There exists a projective plane of order n.

The next two theorems are the analogues of Theorems 4.2.6 and 4.2.7. Theorem 5.3.5 is known as MacNeish's Theorem.

Theorem 5.3.4. If there exist k mutually orthogonal Latin squares of order m and k mutually orthogonal Latin squares of order n, then there exist k mutually orthogonal Latin squares of order mn.

Theorem 5.3.5. Let $p_1, p_2, \ldots, p_t$ be distinct primes, let $a_1, a_2, \ldots, a_t$ be positive integers, and let $n = p_1^{a_1}, p_2^{a_2}, \ldots, p_t^{a_t}$. Then there exist k mutually orthogonal Latin squares of order n where $k = \min\{p_i^{\alpha_i} - 1 : i = 1, 2, \ldots, t\}$.

The existence problem for transversal designs with block size 4 was settled in Section 4.5. In particular, Theorem 4.5.1 says that there exists a TD$(4, n)$ if and only if $n \notin \{2, 6\}$. Thus, we have the following result which completely resolves Euler's conjecture, showing that it is incorrect except when $n = 2$ and $n = 6$.

Theorem 5.3.6. There exists a pair of orthogonal Latin squares of order n if and only if $n \notin \{2, 6\}$.

Three mutually orthogonal Latin squares of order n have been constructed for all n except $n \in \{2, 3, 6, 10\}$. There do not exist three mutually orthogonal Latin squares of order 2, 3 or 6, but it is unknown whether there are three mutually orthogonal Latin squares of order 10. Four mutually orthogonal Latin squares of order n have been constructed for all n except $n \in \{2, 3, 4, 6, 10, 14, 18, 22\}$. There do not exist four mutually orthogonal Latin squares of order 2, 3, 4 or 6, but it is unknown whether there are four mutually orthogonal Latin squares of order 10, 14, 18 or 22. The following table gives the best currently known lower bound on the maximum number of mutually orthogonal Latin squares of order n for $n < 100$. Additional results on mutually orthogonal Latin squares can be found in [2]. The existence of 4 mutually orthogonal Latin squares of order 14 was proven Todorov in 2012 [21]

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$0-19$	∞	∞	1	2	3	4	1	6	7	8	2	10	5	12	4	4	15	16	3	18
$20-39$	4	5	3	22	7	24	4	26	5	28	4	30	31	5	4	5	8	36	4	5
$40-59$	7	40	5	42	5	6	4	46	8	48	6	5	5	52	5	6	7	7	5	58
$60-79$	4	60	5	6	63	7	5	66	5	6	6	70	7	72	5	7	6	6	6	78
$80-99$	9	80	8	82	6	6	6	6	7	88	6	7	6	6	6	6	7	96	6	8

5.4 Transversals in Latin squares

Suppose L and L' are orthogonal Latin squares of order n, and consider the n cells of L' that contain an arbitrary symbol x. These cells occur in n distinct rows and n distinct columns, and in L they contain n distinct symbols. Such a set of cells is called a **transversal**.

Definition 5.4.1. A **transversal** in a Latin square of order n is a set of n cells, one from each row, one from each column, and one containing each symbol. □

Clearly, if L' is orthogonal to L, then L' induces a partition of L into n disjoint transversals. It is interesting to ask which Latin squares have transversals. In 1967, Ryser conjectured that every Latin square of odd order has a transversal, and this conjecture remains open. On the other hand, the following theorem shows that for every even n, there is a Latin square of order n having no transversal. In this theorem, the rows and columns are indexed by $\mathbb{Z}_n$, rather than the usual $\{1, 2, \ldots, n\}$.

Theorem 5.4.2. If n is even, then the Latin square L with symbol set $\mathbb{Z}_n$ given by $L(i, j) \equiv i + j \pmod{n}$ for $0 \leq i, j \leq n - 1$ has no transversal.

Proof For a contradiction, suppose $\{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\}$ is a transversal, and for $i = 1, 2, \ldots, n$, let $z_i = L(x_i, y_i)$. Thus, $x_i + y_i - z_i \equiv 0 \pmod{n}$ for $i = 1, 2, \ldots, n$, and it follows that modulo n we have

$$\begin{aligned} 0 &\equiv \textstyle\sum_{i=1}^{n}(x_i + y_i - z_i) \\ &\equiv \textstyle\sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i - \sum_{i=1}^{n} z_i \\ &\equiv (0 + 1 + \cdots + n - 1) + (0 + 1 + \cdots + n - 1) - (0 + 1 + \cdots + n - 1) \\ &\equiv (0 + 1 + \cdots + n - 1) \\ &\equiv \tfrac{n}{2} \end{aligned}$$

which is a contradiction. □

Definition 5.4.3. A **partial transversal of size** k in a Latin square is a set of k cells, at most one from each row, at most one from each column, and at most one containing each symbol. □

An open conjecture of Brualdi states that every Latin square of order n has a partial transversal of size $n - 1$.

Bibliography

[1] R. J. R. Abel, I. Bluskov, M. Greig and J. de Heer, Pair covering and other designs with block size 6, *J. Combin. Des.*, **15** (2007) 511–533.

[2] R. J. R. Abel, C. J. Colbourn and J. H. Dinitz, Mutually orthogonal Latin squares (MOLS), in *The CRC Handbook of Combinatorial Designs, 2nd edition* (Eds. C. J. Colbourn, J. H. Dinitz), CRC Press, Boca Raton (2007), 160–193.

[3] R. J. R. Abel and M. Greig, BIBDs with Small Block Size, in *The CRC Handbook of Combinatorial Designs, 2nd edition* (Eds. C. J. Colbourn, J. H. Dinitz), CRC Press, Boca Raton (2007), 72–79.

[4] R. Bilous, C. W. H. Lam, L. H. Thiel, P. C. Li, G. H. J. van Rees, S. P. Radziszowski, W. H. Holzmann, H. Kharaghani, There is no 2-$(22, 8, 4)$ block design, *J. Combin. Des.*, **15** (2007) 262–267.

[5] A. E. Brouwer, Optimal packings of K_4's into a K_v, *J. Combin. Theory Ser. A*, **26** (1979) 278–297.

[6] R. H. Bruck and H. J. Ryser, The nonexistence of certain finite projective planes, *Canadian Journal of Mathematics*, **1** (1949), 88–93.

[7] S. Chowla and H. J. Ryser, Combinatorial Problems, *Canadian Journal of Mathematics*, **2** (1950), 93–99.

[8] C. J. Colbourn and J. H. Dinitz (Editors), Handbook of Combinatorial Designs (Second Edition), CRC Press, 2007.

[9] R. A. Fisher, An examination of the different possible solutions of a problem in incomplete blocks, *Annals of Eugenics*, **10** (1940), 52–75.

[10] G. Ge, Group Divisible Designs, in *The CRC Handbook of Combinatorial Designs, 2nd edition* (Eds. C. J. Colbourn, J. H. Dinitz), CRC Press, Boca Raton (2007), 255–260.

[11] M. Hall and W. S. Connor, An embedding theorem for balanced incomplete block designs, *Canad. J. Math.*, **6** (1954), 35–41.

[12] H. Hanani, Balanced incomplete block designs and related designs, *Discrete Math.*, **11** (1975) 255–369.

[13] S. K. Houghten, L. H. Thiel, J. Janssen and C. W. H. Lam, There is no $(46, 6, 1)$ block design, *J. Combin. Des.*, **9** (2001) 60–71.

[14] T. P. Kirkman, On a problem in combinations, *Cambridge and Dublin Math. J.*, **2** (1847), 191–204.

[15] C. W. H. Lam, L. Thiel and S. Swiercz, The non-existence of finite projective planes of order 10, *Canad. J. Math.*, **41** (1989) 1117–1123.

[16] C. C. Lindner and C. A. Rodger, Design Thoery (Second Edition), CRC Press, 2008.

[17] M. P. Schützenberger, A non-existence theorem for an infinite family of symmetrical block designs, *Annals of Eugenics*, **14** (1949), 286–287.

[18] S. S. Shrikhande, The impossibility of certain symmetrical balanced incomplete block designs, *Ann. Math. Stat.*, **21** (1950), 106–111.

[19] D. R. Stinson, Combinatorial designs : constructions and analysis, Springer, 2004.

[20] G. Tarry, Le probleme des 36 officiers, *C. R. Assoc. France Av. Sci.*, **29** (1900) 170–203.

[21] D. T. Todorov, Four Mutually Orthogonal Latin Squares of Order 14, *J. Combin. Des.*, **20** (2012) 363–367.

[22] R. M. Wilson, An existence theory for pairwise balanced designs I - Composition theorems and morphisms, *J. Combin. Theory Ser. A*, **13** (1972) 220–245.

[23] R. M. Wilson, Concerning the number of mutually orthogonal Latin squares, *Discrete Math.*, **9** (1974) 181–198.

[24] R. M. Wilson, An existence theory for pairwise balanced designs III: a proof of the existence conjectures, *J. Combin. Theory Ser. A*, **18** (1975) 71–79.