Chapter 1

Introduction

Here we introduce some of the topics in this book—briefly, but we hope invitingly. The ideas will be developed more fully and their inter-relations more thoroughly examined in the chapters that follow.

This book has two over-arching themes. One is that different parts of mathematics can and do come together in surprising and illuminating ways: suggesting questions, providing tools, and generating examples. The other is the idea of a difference set—a special subset of a group. It exemplifies the first theme, since it belongs both to group theory and to combinatorics, and the study of difference sets uses tools from these areas as well as from geometry, number theory, and representation theory.

A group is often useful when it acts on a set or a structure. As we shall explain, a group contains a difference set if and only if it acts in a particular way on a nice structure called a symmetric design. Thus finding a difference set is equivalent to finding an interesting group action. Also, difference sets are of intrinsic interest because they yield applications in communications and other areas.

So what is a difference set? If a finite group G is written additively, a non-empty proper subset D of G is a (v, k, λ)-*difference set* if $|G| = v$, $|D| = k$ and there is an integer λ such that each non-identity element of G can be expressed in exactly λ ways as a difference $d_1 - d_2$ of elements of D. Equivalently, we require that each non-identity group element appears λ times in the *multiset*

$$\Delta = \{d_1 - d_2 \mid d_1, d_2 \in D, d_1 \neq d_2\}.$$

(The word "multiset" means that elements may be listed more than once.)

Example 1. Choose

$$G_1 = \mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\},$$

the additive group of integers modulo 7, and choose

$$D_1 = \{1, 2, 4\}.$$

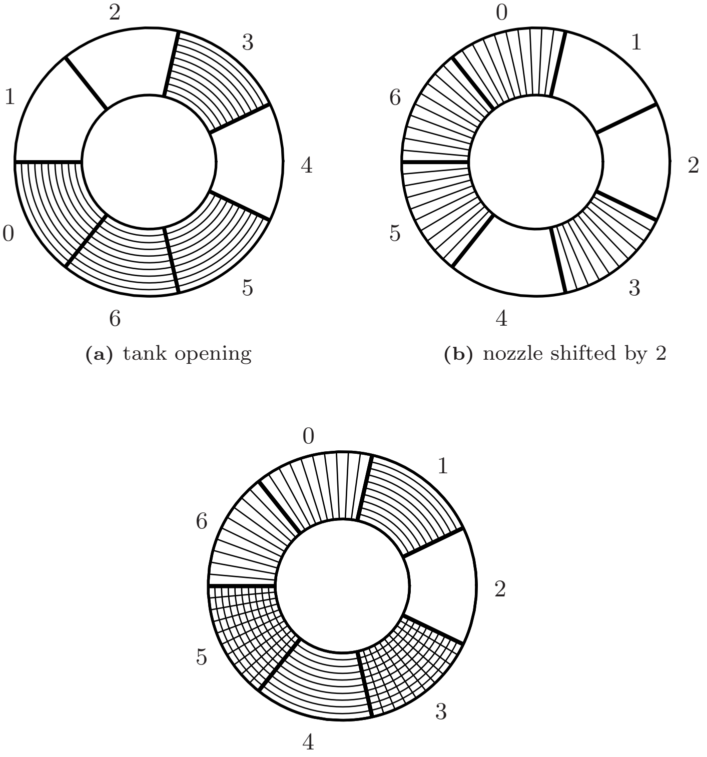
To check that D_1 is a $(7, 3, 1)$-difference set in G_1, it is convenient to organize our work in a table.

$-$	1	2	4
1	0	$-1 = 6$	$-3 = 4$
2	$2 - 1 = 1$	0	$-2 = 5$
4	$4 - 1 = 3$	$4 - 2 = 2$	0

Each of $1, 2, 3, 4, 5, 6$ appears exactly once in the table, confirming that D_1 is a $(7, 3, 1)$-difference set. ◇

We can use the difference set of Example 1 to glimpse one of the applications of difference sets. We might want to robotically align a cylindrical nozzle within a circular opening without deforming either the nozzle or the opening. Example 2 illustrates the general idea. We say more about this application in Chapter 13.

Example 2. The context here is refueling an airplane. Suppose that to optimize the refueling, the cylindrical nozzle on the fuel hose has to be aligned just right within the circular opening of the fuel tank. Imagine that the tank opening is surrounded by a circular ring divided into 7 cells numbered $0, 1, 2, \ldots, 6$. The cells numbered 1, 2 and 4 emit light and the others do not. A second similarly-patterned ring is on the nozzle, backed up by a light detector. The cells numbered 1, 2, 4 on the nozzle ring are transparent to light; the others are opaque. When the two rings are perfectly aligned, the maximum amount of light is detected. When they are out of alignment by as few as 1 or 2 cells, the amount of light detected is much less. In Figure 1.1, the ring in (a) surrounds the opening of the tank, and the ring in (b), on the nozzle, has been rotated clockwise by 2 cells. The ring in (c) shows the light reaching the detector on the nozzle. (See Figure 13.1 for a graph of the amount of light detected when the nozzle is in various positions.) A robot can adjust the nozzle to maximize the light reaching its detector and thereby position it correctly. ◇



(a) tank opening

(b) nozzle shifted by 2

(c) light detector

Figure 1.1. Alignment model for Example 2

Now we return to Example 1. Since $\mathbb{Z}_7$ is also a ring, we can multiply as well as add. Notice that the elements of D_1 are the nonzero squares in $\mathbb{Z}_7$. As we see later, this example can be generalized. We take a partial step toward that generalization, but first we need to do some counting.

Suppose D is a (v, k, λ)-difference set. There are $k(k-1)$ ordered pairs (d_1, d_2), with d_1, d_2 distinct elements of D, and therefore $k(k-1)$ differences $d_1 - d_2$ in the multiset Δ. However, because D is a difference set, each of the $v-1$ non-identity elements of G appears exactly λ times among the elements listed in Δ. We have proved the following theorem.

Theorem 1.1. *Assume D is a (v, k, λ)-difference set. Then*

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

We use this theorem to help us determine a necessary condition for the generalization of Example 1.

Theorem 1.2. *Let p be an odd prime, and let D be the set of nonzero squares in $\mathbb{Z}_p$. If D is a difference set in the additive group $\mathbb{Z}_p$, then $p \equiv 3$ (mod 4).*

Proof. Assume D is a difference set in $\mathbb{Z}_p$. We know $v = p$, and we want to determine $k = |D|$. Since p is prime, the $p-1$ nonzero elements of $\mathbb{Z}_p$ form a group under multiplication. We denote this multiplicative group by $\mathbb{Z}_p^*$. Consider the function mapping each element of $\mathbb{Z}_p^*$ to its square. This is a homomorphism onto D. Because p is an odd prime, $x^2 = 1$ implies $x = \pm 1$, so the kernel of this homomorphism has size 2. Therefore, there are exactly $(p-1)/2$ nonzero squares in $\mathbb{Z}_p$, and $k = (p-1)/2$. Now Theorem 1.1 tells us that $\lambda = k(k-1)/(v-1) = (p-3)/4$. But λ must be an integer, so $p \equiv 3$ (mod 4). □

The idea of a difference set first appeared in the 1938 paper, "A Theorem in Finite Projective Geometry and Some Applications to Number Theory," by James Singer [**62**]. Where is the geometry in our example of a $(7, 3, 1)$-difference set?

We create a geometry by specifying *points* and special sets of points called *blocks*. The points are the 7 elements of G_1, and the blocks are D_1 together with its 6 translates $a+D_1 = \{a+1, a+2, a+4\}$

for $a \in G_1$, $a \neq 0$. The 7 blocks are:

$$\{1,2,4\}\ \{2,3,5\}\ \{3,4,6\}\ \{4,5,0\}\ \{5,6,1\}\ \{6,0,2\}\ \{0,1,3\}.$$

Note that two distinct points appear together in exactly one block and that two distinct blocks have exactly one point in common. If we call blocks "lines," we say informally that two points determine a line and two lines determine a point; there are no parallel lines. This example meets the non-degeneracy conditions that there are at least three points in each block and at least two blocks. Thus we have an example of a non-Euclidean geometry called a finite *projective plane.*

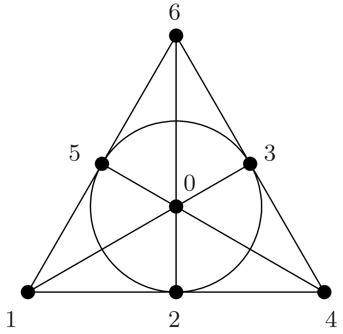


Figure 1.2. The Fano plane

More generally, a set of v *points* and v sets of points called *block*s form a *symmetric design* with parameters (v, k, λ) if every block contains k points, every point belongs to k blocks, two distinct points occur together in λ blocks, and two distinct blocks intersect in λ points. Our geometry is thus a symmetric design[1] with parameters $(7, 3, 1)$. This specific geometric structure is often called the *Fano plane*; see Figure 1.2 for a picture. In this picture, most blocks are represented by line segments; the block $\{2, 3, 5\}$ is represented by a circle.

Now we show how G_1 acts on this structure. Each element of the group G_1 can be regarded as a function taking points to points: the group element a takes the point b to the point $a + b$. Indeed, since

[1] We study designs, including symmetric designs, in Chapter 2.

distinct points go to distinct points, this function is a *permutation* of the points. This function can also be applied to blocks: it takes the block $B = m + D_1$ to the block $a + B = (a + m) + D_1$. Again, distinct blocks go to distinct blocks, so it is a permutation of the blocks. If point x is in block B, then the point $a + x$ is in the block $a + B$. This means that the elements of G_1 act as *automorphisms* of the geometry.

These permutations are special. We can see that G_1 acts *transitively* on the set of 7 points: given any two points b and c, there is a permutation (i.e., an element a of G_1) taking b to c, namely $a = c - b$. Similarly, G_1 acts transitively on the set of 7 blocks: given any two blocks $b + D_1$ and $c + D_1$, there is a permutation taking $b + D_1$ to $c + D_1$, namely $a = c - b$ again. Of course the identity $a = 0$ fixes every point and every block. But the converse is true too. If $a + b = b$ then a must be 0; and similarly (but less obviously) for blocks, if $a + B = B$ then $a = 0$.

We summarize these properties by saying G_1 acts as a *regular* group of automorphisms of the geometry we have defined. In fact, as we prove in Chapter 4, a finite group G contains a (v, k, λ)-difference set if and only if G acts as a regular group of automorphisms of a symmetric (v, k, λ) design.

We have used the group and the difference set to construct the design. How do symmetric designs arise "in nature"? Here is a construction that will take us back to the Fano plane. Choose the field $\mathbb{Z}_2 = \{0, 1\}$, with arithmetic modulo 2. Let V be the 3-dimensional vector space $(\mathbb{Z}_2)^3$. The vector space V contains exactly 2^3 vectors and thus 7 nonzero vectors. Since 1 is the only nonzero scalar, V also contains exactly 7 one-dimensional subspaces. Call these 1-spaces *points.*

Further consequences of the fact that 1 is the only nonzero scalar are

- distinct nonzero vectors are linearly independent, and
- a two-dimensional subspace of V contains exactly 3 nonzero vectors.

In particular, notice that for distinct nonzero vectors $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$, $\{\mathbf{0}, \mathbf{u}, \mathbf{v}, \mathbf{w}\}$ is a 2-space if and only if $\mathbf{u} + \mathbf{v} + \mathbf{w} = \mathbf{0}$. Call a triple of points contained in a single 2-space a *block*. Each block thus contains 3 points. There are exactly 7 2-spaces of V and therefore exactly 7 blocks. We list them below (writing xyz instead of (x, y, z) for each vector and omitting curly braces):

$$\begin{array}{c} 100,\ 010,\ 110 \\ 100,\ 001,\ 101 \\ 100,\ 111,\ 011 \\ 010,\ 001,\ 011 \\ 010,\ 111,\ 101 \\ 001,\ 111,\ 110 \\ 011,\ 110,\ 101. \end{array}$$

Consulting the preceding list we see that two distinct points appear together in exactly one block, and two distinct blocks intersect in exactly one point.

Where is the group? Consider the linear transformation $T : V \to V$ with matrix

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

with respect to the standard basis.[2] We write transformations on the left, so a vector $\mathbf{v}$ is written as a column in calculating $T(\mathbf{v}) = M\mathbf{v}$. The matrix M^7 is the identity matrix, so T^7 is the identity function fixing every vector in V. From linear algebra we know that invertible linear transformations map 1-spaces to 1-spaces and 2-spaces to 2-spaces. Thus the elements of the group

$$G_2 = \{T, T^2, T^3, T^4, T^5, T^6, T^7 = I\}$$

map points to points and blocks to blocks. Indeed we can check that G_2 acts regularly on the points and on the blocks.

Since we are writing the group operation multiplicatively, we replace the difference $d_i - d_j$ by $d_i d_j^{-1}$ in the definition of a difference set. Now we see that the subset

$$D_2 = \{T, T^2, T^4\}$$

[2] Admittedly, this transformation appears to come out of the blue. We motivate it when we discuss Singer's work in Chapter 8.

is a $(7, 3, 1)$-difference set in G_2. (In fact, the obvious group isomorphism from G_1 to G_2 takes D_1 to D_2.)

In his 1938 paper, Singer constructed symmetric designs slightly differently, identifying the vector space V with a finite field containing 8 elements. His construction and analysis generalize to finite projective geometries obtained from higher-dimensional vector spaces over arbitrary finite fields. Other constructions of difference sets require even more ideas from finite geometry, and we will explore them in Chapter 8.

Now we have seen the $(7, 3, 1)$-difference set twice.[3] But how would we find this difference set if we did not know it was there? Or, how could we prove a particular group does *not* contain a difference set? To glimpse one strategy, we rewrite the group of order 7 one more time, this time as a subgroup of the multiplicative group $\mathbb{C}^*$ of nonzero complex numbers,

$$G_3 = \{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6\}$$

for $\omega = \cos(2\pi/7) + i \sin(2\pi/7)$. We can add complex numbers, even though addition is not the group operation in this case. Observe what happens if we multiply the sum of the elements of the difference set

$$D_3 = \{\omega, \omega^2, \omega^4\}$$

by the sum of the inverses of those three elements in G_3:

$$\begin{aligned}
&(\omega + \omega^2 + \omega^4)(\omega^6 + \omega^5 + \omega^3)\\
&\quad = \quad 1 + \omega^6 + \omega^4 + \omega + 1 + \omega^5 + \omega^3 + \omega^2 + 1\\
&\quad = \quad (1 + \omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6) + 2 \cdot 1.
\end{aligned}$$

However, $1 + \omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6 = (1 - \omega^7)/(1 - \omega) = 0$, so we have

$$(\omega + \omega^2 + \omega^4)(\omega^6 + \omega^5 + \omega^3) = 2.$$

In other words, we have factored 2 in the ring $\mathbb{Z}[\omega]$ of integer linear combinations of powers of ω. Notice that $2 = k - \lambda$ in this example. This difference is important enough to get its own name. The quantity $n = k - \lambda$ is the *order* of a (v, k, λ)-difference set or symmetric design. Looking for factorizations of n in the ring $\mathbb{Z}[\eta]$ (where, in general, η

[3] Some of the ideas in this introduction appear in [**9**].

is an mth root of unity for some m dividing v) is a way to search for difference sets, or to prove they do not exist. However, $\mathbb{Z}[\eta]$ need not be a unique factorization domain, so this analysis requires some algebraic number theory. We develop these ideas in Chapter 12.

The group G_3 is actually the image of G_2 under the *representation* (i.e., group homomorphism) $\rho : G_2 \to \mathbb{C}^*$ defined by $\rho(T) = \omega$, and D_3 is the image of D_2. It is the representation ρ that gives us access to the factorization of n in $\mathbb{Z}[\omega]$. To pursue this line of investigation we need to study some representation theory. We offer a primer on representations and characters of finite groups in Chapters 10 and 11.

We now embark on our study, beginning first with designs, then moving on to difference sets. We hope this introduction has given some idea of the diversity and richness of the mathematical ideas we will encounter.

Chapter 2

Designs

In this chapter we introduce designs. Our ultimate goal is to study symmetric designs and their relationship to difference sets. Along the way we also introduce more general designs. Concepts of existence and equivalence that appear here will be mirrored in our study of difference sets.

Design theory is an area of combinatorics that was originally studied for its connections to statistics and the design of experiments. This study has found use in other areas of mathematics including geometry, coding theory, finite group theory, and difference sets. So the study of designs is a good place to start our exploration of the connections among these different algebraic and combinatorial structures.

2.1. Incidence structures

We start with the general notion of an incidence structure.

Definition. An incidence structure is an ordered triple $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ where

$\mathcal{P}$ is a set of points,

$\mathcal{B}$ is a set of blocks,

$\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$ is an incidence relation between $\mathcal{P}$ and $\mathcal{B}$.

If (p, B) is in $\mathcal{I}$, we say that p and B are incident.

2.3. Affine planes

Geometry—literally speaking—means "earth measure." Euclidean geometry with its infinite number of points and its definition of distance fits our literal interpretation of geometry. However, in this book we will look at different types of geometries. Most of our geometries will have finite numbers of points and lines, and we will drop any notion of a metric. What remains is a highly structured design with geometric points for its points, and lines or other substructures for its blocks. The structure is imposed on our geometries by a set of axioms. We are most interested in finite geometries that can be coordinatized.

In this section we define an affine plane and show that a finite coordinatized affine plane is a 2-design. In Section 5 we study finite projective geometries. These geometries provide a rich source for the symmetric designs we define in Section 4 and for constructing difference sets.

First we take the approach of synthetic geometry and define an affine plane as a set of points and lines that obey a set of axioms:

Definition. An affine plane is a non-empty set $\mathcal{P}$ of points and a non-empty set $\mathcal{L}$ of subsets of $\mathcal{P}$ called lines, so that

A1. Each pair of points is in a unique line.

A2. If ℓ is a line and P is a point not in ℓ, then there is a unique line ℓ' that contains P and does not intersect ℓ.

A3. There are at least two points in each line, and at least two lines in the plane.

We say that lines ℓ and ℓ' are parallel if either $\ell = \ell'$ or $\ell \cap \ell' = \emptyset$.

A1 is common to many geometries; it is often stated as "two points determine a line." A2 is one formulation of the parallel postulate, and is the key feature that distinguishes the Euclidean plane from infinite non-Euclidean planes. A3 eliminates trivial cases.

The well-known Euclidean plane is an example of an affine plane. The next example is the smallest affine plane allowed by our system of axioms.

Example 9. Let $\mathcal{P}$ be the set of points $\{A, B, C, D\}$ in Figure 2.1, and let $\mathcal{L}$ be the set of all 2-subsets of $\mathcal{P}$. The line segments connecting pairs of points represent the lines.

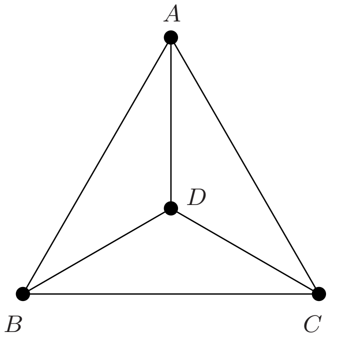


Figure 2.1. Affine plane with four points

If we label the columns A, B, C, D, then an incidence matrix for this affine plane is:

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

The rows correspond to the six lines in Figure 2.1. ◇

From this simple set of axioms it is possible to derive many properties of affine planes. While we will not pursue these results in detail, we list some of the numeric properties of finite affine planes derivable simply from these axioms. The parameter n in the theorem is the order of the affine plane. (See [**6**], p. 26, for a proof.)

Theorem 2.7. *Let $(\mathcal{P}, \mathcal{L})$ be a finite affine plane. Then for some integer $n \geq 2$:*

(i) *Each line has n points.*

(ii) *Each point is incident with $n + 1$ lines.*

(iii) *There are n^2 points.*

(iv) *There are $n(n + 1)$ lines.*

(v) *The lines form $n + 1$ classes, each with n mutually parallel lines.*

Often we identify the points of the Euclidean plane with ordered pairs from $\mathbb{R}\times\mathbb{R}$, and describe a line as a set of points (x, y) that obey a linear equation $ax + by = c$, where $a, b, c \in \mathbb{R}$ and a and b are not both 0. In this way we *coordinatize* the plane. This coordinate system gives us analytical tools to work with the plane. For instance, we can judge whether two lines are parallel by comparing their slopes. For two lines that are not parallel, we can find the point of intersection by finding the solution common to their two equations.

In a similar way we can coordinatize a finite affine plane.

Example 10. Consider the four-point affine plane, and label the points using coordinate pairs from $\mathbb{Z}_2 \times \mathbb{Z}_2$. The equations that determine the six lines are: $x = 0$, $x = 1$, $y = 0$, $y = 1$, $y = x$, and $y = x + 1 \bmod 2$. See Figure 2.2. ◇

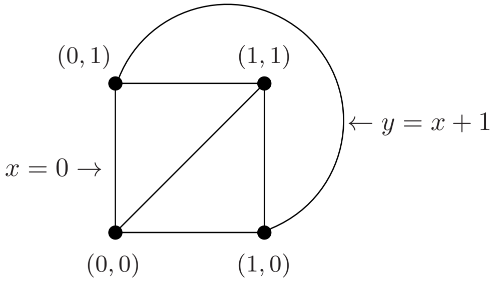


Figure 2.2. Coordinatized affine plane with four points

In general we start with any field $\mathbb{F}$ and use elements from $\mathbb{F}\times\mathbb{F}$ as coordinates of the points in an affine plane. We take as lines the solution sets of linear equations $ax + by = c$ for $a, b, c \in \mathbb{F}$ with a and

b not both zero. Notice that for any nonzero $u \in \mathbb{F}$, the equations $ax + by = c$ and $uax + uby = uc$ have the same solution set.

We define the slope of a line with equation $ax+by = c$ as follows. If $b = 0$, the slope is infinite (and the line is "vertical"). If $b \neq 0$, the slope is $m = -a/b \in \mathbb{F}$. Using algebra, we can verify that distinct lines with the same slope are parallel. Also suppose (x_1, y_1) and (x_2, y_2) are two points on a line. If $x_1 = x_2$, then the line has infinite slope. If $x_1 \neq x_2$, we calculate the slope as $m = (y_2 - y_1)/(x_2 - x_1)$.

This structure does indeed satisfy the axioms of an affine plane. We call this the coordinatized affine plane, denoted by $AG(2, \mathbb{F})$. If $\mathbb{F}$ has q elements, we denote this plane by $AG(2, q)$.

Theorem 2.8. *Let $\mathbb{F}$ be a field. Let $\mathcal{P} = \mathbb{F} \times \mathbb{F}$, and let $\mathcal{L}$ be the collection of lines defined as the solution sets to linear equations $ax + by = c$, for $a, b, c \in \mathbb{F}$, with a and b not both equal to 0. Then $(\mathcal{P}, \mathcal{L})$ is an affine plane.*

Proof. To show that two points determine a line, we consider the points (x_1, y_1) and (x_2, y_2). If $x_1 = x_2$, the line determined by these two points is the set of solutions to the equation $x = x_1$, a vertical line with infinite slope. If $x_1 \neq x_2$, then the line determined by the two points is the set of solutions to the equation $y - y_1 = m(x - x_1)$.

To show this line is unique, we suppose that (x_1, y_1) and (x_2, y_2) are solutions of both $ax+by = c$ and $a'x+b'y = c'$. We want to show there is a nonzero $u \in \mathbb{F}$ with $a' = ua, b' = bu, c' = cu$. We leave the two special cases $x_1 = x_2$ and $y_1 = y_2$ to the exercises and assume $x_1 \neq x_2$ and $y_1 \neq y_2$, so $m = (y_2 - y_1)/(x_2 - x_1) \neq 0$. Subtracting $ax_2 + by_2 = c$ from $ax_1 + by_1 = c$ we get $a(x_1 - x_2) = b(y_2 - y_1)$, from which it follows that both a and b must be nonzero and $a = b(-m)$. It follows that $c = b(y_1 - mx_1)$. Similarly, both a' and b' are nonzero, $a' = b'(-m)$ and $c' = b'(y_1 - mx_1)$. Now, choose $u = b'/b$ to see that $a' = ua$, $b' = ub$ and $c' = uc$, so the line is unique.

To prove axiom A2, the parallel postulate, we show that given a line ℓ and a point P not on ℓ, we can find a line parallel to ℓ and through P. Let P have coordinates (x_1, y_1). If ℓ has no slope (that is, if ℓ is a vertical line), its equation is of the form $x = x_0$ for some $x_0 \neq x_1$. Then the line with equation $x = x_1$ contains P and is parallel to ℓ. It is clearly unique. Otherwise let ℓ have slope m. Then the line through P and parallel to ℓ has equation $y - y_1 = m(x - x_1)$. We can rearrange this equation as $mx - y = mx_1 - y_1$, that is $a = m$, $b = -1$ and $c = mx_1 - y_1$. We see the ratio $a/b = m$, agreeing with the slope of ℓ. If $m = 0$ the equation is $by = c$ and we easily check that this line is unique. If $m \neq 0$ we can adapt the proof of uniqueness above for axiom A1.

Clearly if $\mathbb{F}$ is infinite, then the affine plane has infinitely many points and lines, and so satisfies axiom A3. We leave the finite case to the exercises. □

The above theorem guarantees the existence of a finite affine plane of order n for any n a prime power. It is not known whether other affine planes exist with other orders. It is relatively easy to show that we cannot construct an affine plane of order 6 using coordinates $\mathbb{Z}_6 \times \mathbb{Z}_6$. However, a proof that no order-6 affine plane exists cannot assume this coordinatization. It has now been shown that no affine planes of orders 6 or 10 exist [**42**]. The next open case is $n = 12$.

Finally we note the connection between affine planes and t-designs. Every finite affine plane is a t-design for $t = 2$ and $\lambda = 1$. This simply reflects the fact that any two points determine a line, and that every line contains the same number of points. Thus for any q a power of a prime, the coordinatized affine plane built on the field $GF(q)$ gives us a 2-$(q^2, q, 1)$ design.

Exercises

17. Consider the finite coordinatized plane $AG(2, 3)$.

(a) List the equations $ax + by = c$ corresponding to distinct solution sets by completing the following table. (The first row is done as a sample.)

a	b	c	slope	points
1	0	0	∞	$(0,0), (0,1), (0,2)$

(b) Draw the 3×3 array of points (x, y) where $x, y \in \mathbb{Z}_3$. Connect sets of points when they lie together on a line.

(c) How many lines are there? How many points per line? What is the order n of this plane? What are the parameters of this plane as a 2-design? Ⓢ

(d) What is $M^T M$? Explain its entries geometrically.

(e) What is MM^T? Explain its entries geometrically.

18. Show that distinct lines of $AG(2, \mathbb{F})$ with the same slope are parallel. Specifically, suppose a, b, a', b' are elements of $\mathbb{F}$ and $ax + by = c$ and $a'x + b'y = c'$ are distinct lines with the same slope. Show that these two lines have no points in common by considering these two cases.

(a) Suppose $b = b' = 0$ (i.e., both lines have infinite slope).

(b) Suppose $b \neq 0$, $b' \neq 0$, and $m = -a/b = -a'/b'$.

The next two exercises complete the proof of Theorem 2.8.

19. Consider the coordinatized plane $AG(2, \mathbb{F})$.

(a) Suppose that (x_1, y_1) and (x_2, y_2) are solutions of both $ax + by = c$ and $a'x + b'y = c'$, with $x_1 = x_2$ and $y_1 \neq y_2$. Show that the solution sets of these two linear equations are the same.

(b) Suppose that (x_1, y_1) and (x_2, y_2) are solutions of both $ax + by = c$ and $a'x + b'y = c'$, with $x_1 \neq x_2$ and $y_1 = y_2$. Show that the solution sets of these two linear equations are the same.

(c) Suppose ℓ is a line of slope 0 and $P = (x_1, y_1)$ is not on ℓ but is on the line with equation $by = c$. Show that this is the unique line of slope 0 containing P.

(d) Assume ℓ is a line of slope $m \neq 0$, and $P = (x_1, y_1)$ is a point not on ℓ. Show that $y - y_1 = m(x - x_1)$ is the unique line through P having slope m.

20. Let $\mathbb{F}$ be the finite field $GF(q)$ for $q = p^m$ where p is a prime and m is a positive integer.

(a) Calculate the numbers of points and lines in $AG(2, \mathbb{F})$.

(b) Calculate the number of points on a line in $AG(2, \mathbb{F})$.

21. For Example 9 compute $M^T M$. Use the result to show that this is a 2-design, and find its parameters. Now compute MM^T. Explain the diagonal elements. Then explain the 0's and 1's in the off-diagonal positions in terms of the geometry (using 'points' and 'lines').

22. It is known that there is no finite affine plane of order 6. If we try to coordinatize a 6×6 grid using $\mathbb{Z}_6$, several things go wrong. Using the definition of a line as the solution set to a linear equation, and calling two lines parallel if they have no points in common, show that there would be at least two lines through the point $(1, 3)$ and parallel to the line $y = 0$.

23. Show that the set of points $\mathbb{Z}_{12} \times \mathbb{Z}_{12}$, with lines defined as the solution sets to linear equations, is not an affine plane.

2.4. Symmetric designs

We have seen that for 2-designs, while $M^T M$ has a constant value λ in all the off-diagonal positions, the product MM^T may have different values in its off-diagonal positions. These products show that, while pairs of points are incident with a constant number of blocks, pairs of blocks can be incident with different numbers of points. Symmetric designs place more restrictions on the design to exclude this.

Definition. A symmetric (v, k, λ) design is an incidence structure $(\mathcal{P}, \mathcal{B}, I)$ in which $0 < k < v$ and the following hold:

(i) $|\mathcal{P}| = v$.

(ii) $|\mathcal{B}| = v$.

(iii) Each point is incident with k blocks.

(iv) Each block is incident with k points.

(v) Each pair of points is incident with λ blocks.

(vi) Each pair of blocks is incident with λ points.

To avoid problems with degenerate cases we require that $0 < k < v$. We will call symmetric designs with $\lambda = 0$ or $k - 1$ trivial symmetric designs.[6] The value $n = k - \lambda$ is called the order of the symmetric design.

These axioms are redundant. If a structure obeys axioms (i)–(iv), then (v) and (vi) are equivalent. (See Exercise 32.)

An immediate consequence of the definition is the following theorem.

Theorem 2.9. *Let A be a $v \times v$ matrix of 0's and 1's. Then A is the incidence matrix of a symmetric (v, k, λ) design if and only if*

$$AA^T \quad = \quad A^T A \quad = \quad nI + \lambda J.$$

Corollary 2.10. *The incidence matrix A of a symmetric design is invertible.*

Example 11. Consider a 4×4 board of squares. The 16 individual squares form the points of the design. The block T_j is the set of all squares in the row and the column of square j except the square j itself. Thus every block contains 6 squares. For instance, if we label the squares as shown in Figure 2.3, then block T_7 consists of squares 3, 5, 6, 8, 11, 15. This construction forms a symmetric $(16, 6, 2)$ design. ◇

Example 12. Let $p = 11$, and let $\mathcal{P} = \mathbb{Z}_{11}$. Let D be the set of all nonzero squares mod 11, and let $\mathcal{B}$ be the blocks $\{D,\ 1 + D,\ 2 + D, \cdots,\ 10 + D\}$, where addition is mod 11. Then these points and blocks form a symmetric design. The nonzero squares mod p are called the quadratic residues mod p. ◇

In Section 2.2 we saw relations among the parameters for t-designs. The following theorem shows how the parameters of a symmetric design are related.

Theorem 2.11. *For a symmetric (v, k, λ) design, $(v-1)\lambda = k(k-1)$.*

[6] Some authors define symmetric designs as special 2-designs, which would exclude what we call trivial symmetric designs. We retain trivial designs because they correspond to trivial difference sets.

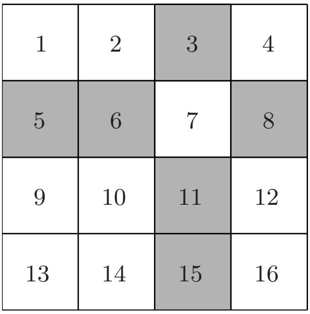


Figure 2.3. Design from 4×4 grid in Example 11; T_7 is shaded

As with t-designs, we define the complement of a symmetric design to have the same point set and to have blocks defined as the complements of the blocks in the original design.

Theorem 2.12. *The complement of a symmetric* (v, k, λ) *design is a symmetric design with parameters* $(v, v-k, v-2k+\lambda)$*.*

The following theorem generalizes Example 12 and the Fano plane example.

Theorem 2.13. *Let* p *be a prime such that* $p \equiv 3 \pmod 4$*, and let* $\mathcal{P} = \{0, 1, \ldots, p-1\}$*. Let* D *be the set of quadratic residues mod* p*, and let* $\mathcal{B} = \{i + D \mid i \in \mathcal{P}\}$*, where addition is mod* p*. Then* $(\mathcal{P}, \mathcal{B})$ *is a symmetric design.*

We explore examples of this construction in the exercises, and prove a more general result in Chapter 4.

A fundamental question is for which triples (v, k, λ) do symmetric (v, k, λ) designs exist. A partial answer comes from the infinite family of designs given in Theorem 2.13. We encounter other infinite families as we study projective geometries. The general existence question remains open.

There are many tantalizing questions about the triples of parameters for symmetric designs. According to Lander ([**43**], p. 44), “For each $\lambda > 1$, only finitely many symmetric (v, k, λ) designs are known.” Most nontrivial symmetric designs have $v \leq \lambda^2(\lambda+2)$. The only known exceptions are designs that have parameters $(37, 9, 2)$, $(56, 11, 2)$, $(79, 13, 2)$, and $(71, 15, 3)$. For each prime power λ, Lander gives a symmetric design that attains the bound $v = \lambda^2(\lambda + 2)$.

Exercises

24. Show that Example 11 is a symmetric $(16, 6, 2)$ design. Ⓢ

25. Show that Example 12 is a symmetric design and give its parameters.

26. Prove Theorem 2.11. Then compare this result with Corollary 2.3.

27. Prove Theorem 2.12: the complement of a symmetric (v, k, λ) design is a symmetric design. Explain why the parameters of the complement design are $(v, v - k, v - 2k + \lambda)$.

28. Using the construction in Theorem 2.13, what is the set D in $\mathbb{Z}_{19}$? What are the parameters for the symmetric design?

29. Show that the construction in Theorem 2.13 with $p = 5$ does not give a symmetric design. What goes wrong?

30. Nontrivial symmetric designs as 2-designs

(a) Which of the six axioms in the definition of a symmetric design are needed to make the structure a 2-design?

(b) Assume that an incidence structure is a 2-design with equal numbers of points and blocks. Prove that r, the number of blocks incident with a particular point, is equal to k.

31. Prove Corollary 2.10 as follows. Parts (b–d) assume a symmetric design with parameters (v, k, λ) and incidence matrix A.

(a) Let B be a $v \times v$ matrix with $B = aI + bJ$. Show that $\det B = (a + vb)a^{v-1}$ by finding $v - 1$ linearly independent eigenvectors for B with eigenvalue a and one independent of these with eigenvalue $a + vb$.

(b) Show that $\det(nI + \lambda J) = k^2 n^{v-1} \neq 0$.

(c) Explain why $AA^T = nI + \lambda J$.

(d) Prove that A is invertible.

32. Assume an incidence structure obeys axioms (i)–(iv) of a symmetric design, and let A be the incidence matrix for this structure.

(a) Show that $AJ = JA$.

(b) Assume axiom (vi) and deduce axiom (v). Ⓗ

(c) Assume axiom (v) and deduce axiom (vi).

2.5. Projective geometry

We return in this section to geometries—this time to projective geometries—to look for examples of symmetric designs. As with the affine planes of Section 3, we look first at the axiomatic definition of a projective plane. We then construct a coordinatized projective plane $PG(2, q)$ starting with a vector space over $GF(q)$. We also study projective geometries of dimension higher than two.

Definition. A projective plane is a non-empty set $\mathcal{P}$ of points and a non-empty set $\mathcal{L}$ of subsets of $\mathcal{P}$ called lines, so that

P1. Each pair of points is in a unique line.

P2. Each pair of lines intersects.

P3. Each line contains at least three points; the plane contains at least two lines.

Note that the parallel postulate from the definition of an affine plane is replaced by axiom P2 stating that any two lines intersect. Combining axioms P1 and P2 shows that any two lines intersect in exactly one point. From the axioms it is also possible to prove that each point is incident with at least three lines, and that the plane contains at least two points. An important property that comes from these axioms is that any true statement that can be derived from these axioms about points and lines remains true if the words "points" and "lines" are interchanged. This is known as the property of duality. We see this in the next theorem.

As with finite affine planes, the axioms for a projective plane give us enough information to prove that each line in a finite projective plane must have the same number of points. We can also prove other numerical results, as summarized in this theorem. (See [**6**], p. 4.)

Theorem 2.14. *Let $(\mathcal{P}, \mathcal{L})$ be a finite projective plane. Then for some integer $n \geq 2$*

(i) Each line has $n + 1$ points.

(ii) Each point is incident with $n + 1$ lines.

(iii) There are $n^2 + n + 1$ points.

(iv) There are $n^2 + n + 1$ lines.

The number n is called the order of the projective plane. The smallest finite projective plane is the order-2 Fano plane, with seven points and seven lines, each line containing three points. (See Figure 1.2 on page 5.)

So far we have talked about the synthetic approach. Just as we did with affine planes, we now restrict our attention to the class of coordinatized projective planes that are constructed starting with a vector space—in this case, a 3-dimensional vector space $\mathbb{F}^3$. Before we look at this construction in general, we introduce it using the field $\mathbb{R}$.

Example 13. Let $\mathbb{F} = \mathbb{R}$ and let $V = \mathbb{R}^3$, the familiar 3-space. The 1-spaces in V are the ordinary lines through the origin, and these will be our "points". The 2-spaces are the ordinary planes through the origin, and these will be our "lines". Then two 1-spaces ("points") span a unique 2-space ("line"). Two 2-spaces ("lines") meet in a 1-space ("point"). $\diamond$

Theorem 2.15. *Let $\mathbb{F}$ be a field and let V be a vector space of dimension three over $\mathbb{F}$. Let $\mathcal{P}$ be the collection of 1-spaces of V, and let $\mathcal{L}$ be the collection of 2-spaces of V. Then $(\mathcal{P}, \mathcal{L})$ is a projective plane.*

A projective plane constructed in this fashion is denoted $PG(2, \mathbb{F})$. When $\mathbb{F}$ has q elements, we write $PG(2, q)$.

Example 14. The finite projective plane $PG(2, 3)$ is constructed starting with the vector space $V = (\mathbb{Z}_3)^3$. There are $3^3 - 1 = 26$ nonzero vectors, with (x_1, x_2, x_3) and $2(x_1, x_2, x_3)$ in the same 1-space (together with the zero vector). So there are $26/2$ projective points. $\diamond$

We can define coordinates for $PG(2, \mathbb{F})$ and use analytical techniques to study these geometries. Clearly we cannot simply label a projective point with the components of a single vector in the related 1-space, since that would give several labels for one point. But since all the nonzero vectors in a 1-space are nonzero multiples of each other, we do something quite close to this.

On the set of nonzero ordered triples $(x, y, z) \in \mathbb{F}^3 \setminus (0, 0, 0)$ we define an equivalence relation $(x, y, z) \sim (x', y', z')$ if and only if $(x', y', z') = s(x, y, z)$ for some nonzero scalar s. We use square brackets for the equivalence class $[x, y, z]$ of all triples equivalent to (x, y, z), and we use these equivalence classes to label the projective points.

Any 2-space of V can be described as the solution set of a linear equation $ax + by + cz = 0$ with a, b, and c not all 0. Given this, the projective line identified with this 2-space can be described as the set of projective points $[x, y, z]$ so that $ax+by+cz = 0$. We note that any vector equivalent to (a, b, c) gives the same projective line. So we use an equivalence class $[a, b, c]$ to describe a particular projective line. We thus naturally call $PG(2, \mathbb{F})$ the coordinatized projective plane .

Example 15. Consider the projective plane $PG(2, 3)$. The points $[2, 1, 0]$ and $[1, 0, 1]$ are different since $(2, 1, 0) \not\sim (1, 0, 1)$. Given this, there must be a projective line through these points. This line must have coordinates $[a, b, c]$ so that $2a + b = 0$ and $a + c = 0$ in $\mathbb{Z}_3$. If we choose $a = 1$, then $b = -2 = 1$ and $c = -1 = 2$. Other choices for a will give other triples in the equivalence class $[1, 1, 2]$. $\diamond$

Projective spaces of higher dimensions. If we increase the dimension, there is enough room in projective space for lines that do not intersect. In the definition of a projective space we replace axiom P2 with one that basically says any two lines in a planar subspace must intersect.

Definition. A projective space is a non-empty set $\mathcal{P}$ of points and a non-empty set $\mathcal{L}$ of subsets of $\mathcal{P}$ called lines, so that

P1. Each pair of points is in a unique line. (We write $\ell(A, B)$ for the unique line on points A and B.)

P2$'$. (The Pasch Axiom) If A, B, C, and D are distinct points such that there is a point E in the intersection of lines $\ell(A, B)$ and $\ell(C, D)$, then there is a point F in the intersection of lines $\ell(A, C)$ and $\ell(B, D)$.

P3$'$. Each line contains at least three points; the projective space contains at least two lines.

Extending our construction to projective spaces of higher dimensions, we construct $PG(d, q)$ starting with the vector space $V = \mathbb{F}^{d+1}$ for $\mathbb{F}$ the field $GF(q)$. Again, the points of the projective space are the 1-spaces of V; the lines are the 2-spaces; the planes are the 3-spaces; and so forth.

In a finite projective space of dimension greater than two, there are not equal numbers of points and lines, so we cannot find a symmetric design using the lines as blocks. However there are equal numbers of 1-spaces and d-spaces in $V = \mathbb{F}^{d+1}$. We call these d-spaces hyperplanes, and we have the following theorem.

Theorem 2.16. *Let $\mathbb{F} = GF(q)$ and let V be a $(d+1)$-dimensional vector space over $\mathbb{F}$ for $d \geq 2$. Let $\mathcal{P}$ be the set of 1-spaces of V, and let $\mathcal{B}$ be the set of hyperplanes. Then $(\mathcal{P}, \mathcal{B})$ is a symmetric design with parameters*

$$v = \frac{q^{d+1} - 1}{q - 1}, \quad k = \frac{q^d - 1}{q - 1}, \quad \lambda = \frac{q^{d-1} - 1}{q - 1}.$$

Proof. We leave for the exercises the verification that v is the number of 1-spaces in V. Now we count the number of hyperplanes.[7] To

[7] It is true that the 1-spaces and hyperplanes of a finite-dimensional vector space are in a one-to-one correspondence. (See A.4.) For vector spaces over a finite field, a direct count of the hyperplanes is interesting.

begin, we count the number of ways to choose d linearly independent vectors in V. There are $q^{d+1}-1$ choices for the first nonzero vector. Then there are $q^{d+1}-q$ choices for a second vector independent of the first. Similarly there are $q^{d+1}-q^2$ ways to choose a third vector not in the span of the first two. Proceeding in this way, the total number of choices is

$$(q^{d+1}-1)(q^{d+1}-q)(q^{d+1}-q^2)\dots(q^{d+1}-q^{d-1}).$$

But a hyperplane has many bases. The number of bases of a fixed hyperplane (d-space) is $(q^d-1)(q^d-q)(q^d-q^2)\dots(q^d-q^{d-1})$. Therefore the number of hyperplanes is

$$\frac{(q^{d+1}-1)(q^{d+1}-q)(q^{d+1}-q^2)\dots(q^{d+1}-q^{d-1})}{(q^d-1)(q^d-q)(q^d-q^2)\dots(q^d-q^{d-1})}.$$

Factor a q from all but the first binomial in the numerator for a leading factor of q^{d-1}. Now factoring q^{d-1} from the last binomial in the denominator gives:

$$\frac{q^{d-1}(q^{d+1}-1)(q^d-1)(q^d-q)\dots(q^d-q^{d-2})}{q^{d-1}(q^d-1)(q^d-q)(q^d-q^2)\dots(q^d-q^{d-2})(q-1)}.$$

Cancel factors in common to get:

$$\frac{q^{d+1}-1}{q-1}.$$

We leave for the exercises the proof that k is also the number of 1-spaces in a hyperplane.

Next we show that the number r of hyperplanes containing a 1-space is independent of the particular 1-space. Suppose $\mathbf{u},\mathbf{w}\in V$ are two nonzero vectors. We can define an invertible linear transformation $T: V\to V$ with $T(\mathbf{u})=\mathbf{w}$. Then T permutes the hyperplanes of V, so H is a hyperplane containing $\mathbf{u}$ if and only if $T(H)$ is a hyperplane of V containing $\mathbf{w}$.

Finally, two hyperplanes meet in λ 1-spaces. □

Exercises

33. Let $\mathbb{F}=GF(5)$

(a) How many nonzero vectors are there in $\mathbb{F}^3$?

(b) Explain how to calculate the number of points and lines in $PG(2,5)$.

34. Prove Theorem 2.15. Be sure to verify axiom P3 in the finite case.

35. What goes wrong with the construction in Theorem 2.15 if we start with $V = \mathbb{Z}^3$?

36. Consider the projective plane $PG(2,5)$.

(a) Let [0,1,3] and [2,1,1] be two projective points. Find the coordinates for the line through these points. Ⓢ

(b) Let [0,1,3] and [2,1,1] be two projective lines. Find the coordinates for the point in the intersection of these two lines.

(c) Write a general statement about the principal of duality that you see in parts (a) and (b).

37. Let $V = \mathbb{Z}_5^4$, the vector space of dimension 4 over $\mathbb{Z}_5$. Find an equation for the hyperplane (here, a 3-space) containing vectors $(1,0,0,0)$, $(0,1,0,0)$, and $(1,1,1,1)$.

38. Consider the projective space $PG(3,5)$.

(a) Find the numbers of points, lines, and planes in this projective space.

(b) Show that the incidence structure with $\mathcal{P}$ the set of projective points and $\mathcal{B}$ the set of projective planes is a symmetric design. Find its parameters.

39. Complete the proof of Theorem 2.16 as follows:

(a) Show that v is the number of 1-spaces in V.

(b) Show that k is the number of 1-spaces in a hyperplane of V.

(c) Explain why $r = k$.

(d) Fix two hyperplanes. Show that λ is the number of 1-spaces in the intersection of the hyperplanes.

Coda

Design theory is mathematically rich and very useful. It belongs to combinatorics and is strongly linked to geometry and algebra. Designs arose in statistics as designs of experiments (and this statistical origin shows in the standard notation v for the number of points in a design). A statistics text that highlights designs is [**14**]; it is very applied but also imbued with the spirit of abstract designs. Another important application of designs is to coding theory. See for example [**12**]. Also see the section on codes in Chapter 13.

The treatment of designs in this chapter is somewhat more general than required for our study of difference sets, but we wanted to place the designs we need in a wider context. Our main focus is on symmetric designs because they are intimately connected to difference sets in finite groups. Chapter 3 introduces groups via automorphisms of designs, and Chapter 4 makes the explicit link between symmetric designs and difference sets.

Finite geometries often play a key role in constructions of difference sets. Here we have treated affine and projective geometries in two parallel sections (forgive the pun). In each section, we begin synthetically, with a list of axioms. Adding the assumption of finiteness to the axioms determines many parameters of the geometry. We then narrow our focus to the coordinatized geometries, since these are most useful to us.

Chapter 4

Introducing Difference Sets

As we noted in Chapter 1, many authors trace difference sets to the 1938 paper of Singer ([**62**]). Although Singer does formulate the definition of a difference set, his main theorem is about an automorphism of a design. Singer also frames the theorem's important consequences as descriptions of the points and blocks of the design. The systematic study of difference sets themselves goes back at least to Hall's work in the late 1940's. Ideas from combinatorics, geometry and algebra were ingredients in all of these early papers. The use of algebraic methods has grown steadily as the subject has developed.

In this chapter we introduce difference sets and some of the mathematical tools used to construct them and to explore their properties. We begin in Section 1 with the definition and examples. We describe in Section 2 how a difference set can be used to produce a symmetric design and thus how it provides a compact description of the design it yields. An important algebraic tool for the study of difference sets is the integral group ring, the topic of Section 3. Finally, in Section 4 we define what it means for two difference sets to be equivalent.

(b) How many group automorphisms does G have?

(c) Now find all the subsets of G that are equivalent to the difference set $D = \{1, 2, 4\}$. Ⓢ

39. Show that if $\mathbb{Z}_m$ contains an (m, k, λ)-difference set, then it contains an (m, k, λ)-difference set D with $0, 1 \in D$.

40. Let G be the abelian group $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $G = \langle\, a, b, c \mid a^4 = b^2 = c^2 = 1\rangle$. For this group Kibler [**40**] lists two difference sets: $D_6 = \{1, a, a^2, b, c, a^3bc\}$ and $D_7 = \{1, a, a^2, ab, ac, a^3bc\}$. Show that these are not equivalent. Ⓗ

41. Kibler [**40**] gives three difference sets in the group $\langle\, a, b \mid a^4 = b^4 = 1,\ ab = ba\,\rangle$. They are

$$\begin{aligned} D_3 &= \{1,\ a,\ a^2,\ b,\ ab^2,\ a^2b^3\}, \\ D_4 &= \{1,\ a,\ a^2,\ b,\ b^3,\ a^3b^2\}, \\ D_5 &= \{1,\ a,\ b,\ a^2b,\ ab^2,\ a^2b^2\}. \end{aligned}$$

Which of Kibler's three examples is equivalent to the difference set in $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ of Exercise 19 on page 58? How do you know?

42. Prove that in $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ the difference sets

$$\{1,\ a,\ b,\ c,\ d,\ abcd\} \quad \text{and} \quad \{a,\ b,\ c,\ d,\ ab,\ cd\}$$

are equivalent. (The first is in Kibler's paper [**40**]; the second is in Baumert ([**5**], p. 10).)

43. Show that up to equivalence there is only one $(16, 6, 2)$-difference set in $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Ⓗ

44. Prove Theorem 4.12.

Coda

The fundamental problem in the study of difference sets is the existence question:

Given a group, does it contain a difference set?

In particular, can we construct one? Can we prove one cannot exist?

Difference sets bridge group theory and design theory, since a group contains a difference set if and only if the group acts regularly on the points and on the blocks of a symmetric design. Groups, designs and existence are three of our mathematical threads. We describe briefly how these and others weave through the book.

The definition of a difference set is combinatorial, so it is natural that counting plays an important role. Counting leads immediately to the fundamental equation $\lambda(v-1) = k(k-1)$ satisfied by the parameters of a (v, k, λ)-difference set. This is the first necessary condition for existence. We will see other necessary conditions in Chapters 5–7.

Many of the examples of difference sets we have seen thus far come from number theory: squares, fourth powers, twin primes. We use methods from algebra, combinatorics and geometry to construct families of difference sets in Chapters 8 and 9.

We translate the criterion for being a difference set into an equation in the integral group ring $\mathbb{Z}G$. This group ring equation opens the door to the use of other algebraic tools to address the existence question, and we develop these topics in Chapters 10–12.

Chapter 5

Bruck-Ryser-Chowla Theorem

The Bruck-Ryser-Chowla Theorem (BRC) is one of the most important tools for proving that difference sets with particular parameters cannot exist. It gives necessary conditions on the parameters (v, k, λ) for the existence of a symmetric (v, k, λ) design. Since the development of a difference set is a symmetric design, this theorem places restrictions on the parameters of a difference set in a group of order v.

In Section 1 we present the BRC Theorem and look at a number of applications of the theorem. In Section 2 we look at the details of the proof. This will lead us through interesting arguments from number theory and from linear algebra. It will also explain how the existence of a solution to a diophantine equation could have any bearing on the existence of a symmetric design.

The Bruck-Ryser-Chowla Theorem gets its name from the work by Bruck and Ryser [**11**] and by Chowla and Ryser [**13**]. In the first paper the authors prove the theorem in the case $\lambda = 1$. The second paper extends the result to any positive integer λ. Ryser's later paper [**61**] gives a much simplified proof. We look at this proof in some detail in Section 2.

chapters we will explore other necessary conditions for the existence of difference sets.

Exercises

19. Verify that in Example 7 the parameters pass the BRC test, but fail the test in Theorem 5.12.

Coda

The centuries-long quest for a proof of Fermat's Last Theorem reminds us that proving non-existence is often very hard. The Bruck-Ryser-Chowla Theorem (BRC) can tell us when a (v, k, λ) design does not exist and thus when a (v, k, λ)-difference set does not exist.

The proof of BRC uses the incidence matrix N of the design. For v even, we only need the determinant of $N^T N$. For v odd, the argument is more intricate. Many proofs explicitly require background knowledge of quadratic forms. We have chosen a more elementary approach that uses matrix algebra. Even if you did not follow all the details of this long argument, you should work to appreciate the source of this surprising number-theoretic condition required for the existence of a symmetric design.

Chapter 7

Necessary Group Conditions

Chapters 5 and 6 introduced necessary conditions for the existence of difference sets with certain parameters and in certain groups. Here we continue this discussion with three results that depend on the structure of the group. There are two related topics in Section 1. The first concerns the distribution of the elements of a difference set among the cosets of a normal subgroup of G. The second considers homomorphic images of D in the setting of the integral group ring. In Section 2 we discuss Turyn's "exponent bound". In Section 3 we describe Dillon's "dihedral trick" linking the existence of a difference set in a generalized dihedral group of size $2n$ to a difference set in an abelian group of the same size.

7.1. Intersection numbers

Partitioning D. We start with a group G that contains a difference set D. When G has a normal subgroup N, the cosets mod N partition the elements of G and correspondingly lead to a partition of the elements of D. The main result of this section concerns the possible sizes of these subsets of D. This theorem can be used both to find difference sets and to rule out the existence of difference sets in certain groups.

Chapter 7

Necessary Group Conditions

Chapters 5 and 6 introduced necessary conditions for the existence of difference sets with certain parameters and in certain groups. Here we continue this discussion with three results that depend on the structure of the group. There are two related topics in Section 1. The first concerns the distribution of the elements of a difference set among the cosets of a normal subgroup of G. The second considers homomorphic images of D in the setting of the integral group ring. In Section 2 we discuss Turyn's "exponent bound". In Section 3 we describe Dillon's "dihedral trick" linking the existence of a difference set in a generalized dihedral group of size $2n$ to a difference set in an abelian group of the same size.

7.1. Intersection numbers

Partitioning D**.** We start with a group G that contains a difference set D. When G has a normal subgroup N, the cosets mod N partition the elements of G and correspondingly lead to a partition of the elements of D. The main result of this section concerns the possible sizes of these subsets of D. This theorem can be used both to find difference sets and to rule out the existence of difference sets in certain groups.

We start by looking at an example found in Kibler's list of difference sets.

Example 1. Let G be the elementary abelian 3-group of order 27 generated by a, b, and c, and consider the difference set from Kibler [**40**]

$$D = \{1, a, a^2, b, ab, b^2, c, ac, bc, ac^2, a^2bc^2, b^2c^2, a^2b^2c^2\}.$$

If we choose the subgroup $N = \langle a, b\rangle$, then $G = N \cup Nc \cup Nc^2$ and D is partitioned into $D = D_0 \cup D_1 \cup D_2$ where $D_i = D \cap Nc^i$. We find that $D_0 = \{1, a, a^2, b, ab, b^2\}$, $D_1 = \{c, ac, bc\}$, and $D_2 = \{ac^2, a^2bc^2, b^2c^2, a^2b^2c^2\}$. The numbers of elements in these D_i are (respectively) 6, 3, and 4. ◇

Example 2. Let G be the group $\mathbb{Z}_5 \oplus \mathbb{Z}_7$ and let D be the $(35, 17, 8)$-difference set based on the twin primes 5 and 7. (See Theorem 4.6.) Let $N_1 = \{(a, 0) \mid a \in \mathbb{Z}_5\}$ and let $N_2 = \{(0, b) \mid b \in \mathbb{Z}_7\}$. These are normal subgroups in G. Figure 7.1 shows the elements of D and their membership in the various cosets of these normal subgroups. For instance, the second column shows that coset $(0, 1) + N_1$ (denoted by $(*, 1)$ in the table) contains two elements of D, namely $(1, 1)$ and $(4, 1)$. ◇

	$(*,0)$	$(*,1)$	$(*,2)$	$(*,3)$	$(*,4)$	$(*,5)$	$(*,6)$	
$(0,*)$	$(0,0)$							1
$(1,*)$	$(1,0)$	$(1,1)$	$(1,2)$		$(1,4)$			4
$(2,*)$	$(2,0)$			$(2,3)$		$(2,5)$	$(2,6)$	4
$(3,*)$	$(3,0)$			$(3,3)$		$(3,5)$	$(3,6)$	4
$(4,*)$	$(4,0)$	$(4,1)$	$(4,2)$		$(4,4)$			4
	5	2	2	2	2	2	2	17

Figure 7.1. Array showing elements of the twin-prime difference set

The sizes of the intersections of a possible difference set D with the various cosets of a normal subgroup are useful in tackling the existence question.

Definition. Let G be a group and N a normal subgroup of index r. Let $\{g_1, \ldots, g_r\}$ be a complete set of coset representatives for N in G. If D is a difference set in G, then the numbers $n_i = |D \cap g_i N|$ are the intersection numbers for D with respect to N.

For short we sometimes call these the intersection numbers for D mod N. In Figure 7.1 the numbers at the ends of the columns are the intersection numbers mod N_1, and those at the ends of the rows are the intersection numbers mod N_2. It is clear that the sum of the intersection numbers mod N for a (v, k, λ)-difference set must be k. What is less obvious is that the sum of their squares is predictable.

Theorem 7.1. *Let D be a (v, k, λ)-difference set in the group G, and let N be a normal subgroup of index r in G with $|N| = s$. Let $\{g_1, \ldots, g_r\}$ be a complete set of coset representatives, and denote the intersection numbers for D with respect to N by $n_i = |D \cap g_i N|$. Then*

$$\begin{aligned} \sum_{i=1}^{r} n_i &= k \\ \sum_{i=1}^{r} (n_i)^2 &= n + \lambda s. \end{aligned}$$

As illustrations of this theorem, we look again at the examples above.

Example 3. In the $(27, 13, 6)$-difference set of Example 1, we have $s = |\langle a, b\rangle| = 9$, $n = 7$, and

$$6^2 + 3^2 + 4^2 = 61 = 7 + 6 \cdot 9.$$

In the $(35, 17, 8)$-difference set of Example 2, when $s = 5$ we have $n + \lambda s = 9 + 8 \cdot 5 = 49$. We check that $\sum n_i^2 = 5^2 + 6 \cdot 2^2 = 49$. When $s = 7$ we have $n + \lambda s = 9 + 8 \cdot 7 = 65$. We check that $\sum n_i^2 = 1^2 + 4 \cdot 4^2 = 65$. ◇

Our proof of Theorem 7.1 uses the integral group ring introduced in Chapter 4. Recall that if D is a (v, k, λ)-difference set in G, then in the integral group ring $\mathbb{Z}G$ we know that $DD^{(-1)} = n1_G + \lambda G$. Our proof involves summing the coefficients of elements of N on each side of this equation.

Proof. The right hand side of the equation $DD^{(-1)} = n1_G + \lambda G$ may be rewritten as $n1_G + \lambda N + \lambda(G \setminus N)$. So the sum of the coefficients of elements in N is $n + \lambda|N| = n + \lambda s$. For the left hand side we write $D = D_1 + D_2 + \cdots + D_r$ where r is the index of N in G and $D_i = D \cap g_i N$. Then

$$\begin{aligned} DD^{(-1)} &= \Big(D_1 + D_2 + \cdots + D_r\Big)\Big(D_1 + D_2 + \cdots + D_r\Big)^{(-1)} \\ &= \sum_{i \neq j} D_i\, D_j^{(-1)} \;+\; \sum_i D_i\, D_i^{(-1)}. \end{aligned}$$

The terms $D_i\, D_j^{(-1)}$ have nonzero coefficients for elements in the coset $g_i\, g_j^{-1} N$. These elements are in N if and only if $i = j$. So in the expression for $DD^{(-1)}$ the sum of the coefficients of elements in N is the sum of coefficients in $\sum_i D_i\, D_i^{(-1)}$, namely the sum of squares of the intersection numbers. We conclude that

$$\sum_{i=1}^{r} (n_i)^2 = n + \lambda s. \qquad \square$$

Next we look at how this theorem can be used to limit the search for a difference set in a particular group. If we suspect that a group G might have a (v, k, λ)-difference set, we could check each of the $\binom{v}{k}$ subsets of G. This is prohibitively time consuming even for quite small examples. If G contains such a difference set D, we could search for an equivalent difference set $g^{-1}D$ where $g \in D$. This guarantees that 1_G is in $g^{-1}D$, so we only need to examine k-subsets that include 1_G, cutting the brute force search down to $\binom{v-1}{k-1}$. In a similar fashion, if we know a supposed difference set in a group G with normal subgroup N must have certain intersection numbers, we can limit our search based on these numbers.

Example 4. Continuing with Example 1, let $G = \langle a, b, c \mid a^3 = b^3 = c^3 = 1\rangle$ and $N = \langle a, b\rangle$. If we have a $(27, 13, 6)$-difference set D in G, we can show that the only intersection numbers that obey Theorem 7.1 are 3, 4, 6 in some order. Further we can specify the assignment of these numbers to specific cosets by looking at difference sets equivalent to D. Let D be a difference set with intersection numbers $3, 4, 6$. By multiplying D by an appropriate power of c, we can find a difference set equivalent (by a shift) to one with $|D \cap N| = 6$. Similarly the mapping

$$a \mapsto a, \quad b \mapsto b, \quad c \mapsto c^2$$

is a homomorphism that keeps the coset N fixed and interchanges the cosets Nc and Nc^2. So using this mapping if necessary, we can find an equivalent difference set with $|D \cap Nc| = 4$ and $|D \cap Nc^2| = 3$. Thus, we can limit our search to sets with 6 elements in N, 4 in Nc, and 3 in Nc^2. So we have cut the brute force search from $\binom{27}{13} \approx 20$ million to $\binom{9}{6}\binom{9}{4}\binom{9}{3} = 889,056$. Of course this number is also large, but computers may be able to tackle the smaller search in reasonable time where the larger one may be intractable. ◇

Homomorphisms. To take advantage of the integral group ring as a tool for studying intersection numbers, we start with a group homomorphism $\varphi : G \to H$ and extend it to a mapping $\widehat{\varphi} : \mathbb{Z}G \to \mathbb{Z}H$. Let N be the kernel of φ, so $H = G/N$. Then this mapping $\widehat{\varphi}$ will give us a slightly different approach to a proof of Theorem 7.1, and will be useful in later chapters.

First we must prove that $\widehat{\varphi}$ is a ring homomorphism.

Theorem 7.2. *Assume G and H are groups and $\varphi : G \to H$ is a group homomorphism. Define $\widehat{\varphi} : \mathbb{Z}G \to \mathbb{Z}H$ by*

$$\widehat{\varphi}\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a_g \, \varphi(g).$$

Then $\widehat{\varphi}$ is a ring homomorphism.

Let us look at some examples.

Example 5. One case of interest is when G is a group, $H = \{1_G\}$, and $\varphi(g) = 1_G$ for all $g \in G$. So $N = G$. Then $\widehat{\varphi}(\sum a_g g) = \sum a_g 1_G$ which we identify with the integer $\sum a_g \in \mathbb{Z}$. By analogy to evaluating a polynomial $f(x) \in \mathbb{Z}[x]$ at $x = 1$, this is sometimes called the *evaluation map.* ◇

Example 6. Let $G = \langle a, b \mid a^7 = b^3 = 1, \ ba = a^2 b \rangle$, and $D = \{1, a, a^3, b, a^2 b^2\}$, a $(21, 5, 1)$-difference set. We define $H = \langle b \rangle$, and consider the homomorphism φ from G to H defined by $\varphi(a) = 1$, $\varphi(b) = b$. The kernel of φ is $N = \langle a \rangle$. Then $\widehat{\varphi} : \mathbb{Z}G \to \mathbb{Z}H$ with $\widehat{\varphi}(G) = 7H$ and $\widehat{\varphi}(D) = 3 \cdot 1_H + 1 \cdot b + 1 \cdot b^2$. Note that the coefficients in $\widehat{\varphi}(D)$ are the intersection numbers of D mod N. ◇

The following theorem shows the result of applying $\widehat{\varphi}$ to the integral group ring equation for a difference set. Note that it requires that the group homomorphism map G *onto* H.

Theorem 7.3. *Assume D is a (v, k, λ)-difference set in G and $\varphi : G \to H$ is an epimorphism of groups. Then the image $\widehat{D} = \widehat{\varphi}(D)$ satisfies the following equation in $\mathbb{Z}H$:*

$$\widehat{D}\widehat{D}^{(-1)} = n1_H + s\lambda H,$$

where s is the order of $N = Ker\varphi$.

Example 7. This example sets the stage for a slightly different proof of Theorem 7.1 (see Exercise 11). Suppose the group G contains a (v, k, λ)-difference set D. Suppose further that G contains a normal subgroup N and let $\varphi : G \to G/N = H$ be the natural homomorphism. Assume $\{g_1, \ldots, g_r\}$ is a complete set of coset representatives for N in G, and let $n_i = |D \cap g_i N|$. Write $h_i = \varphi(g_i)$. Then

$$\widehat{D} = \widehat{\varphi}(D) = \sum_{i=1}^{r} n_i h_i. \qquad \diamond$$

Difference lists. Motivated by Theorem 7.3, we have the following generalization of a difference set.

Definition. An element $E = \sum_h a_h h$ in the integral group ring $\mathbb{Z}H$ is called a <u>difference list</u> over H with parameters (r, k, s, λ) if s and k are positive integers, λ and the a_h are non-negative, $|H| = r$, $\sum_h a_h = k$, and $EE^{(-1)} = (k - \lambda)1_H + s\lambda H$.

Difference lists were introduced in [**2**]. In that paper, the authors interpreted E as a multiset of elements from H, with $a_h h$ regarded as a_h copies of the element h. In the special case when $s = 1$ and all the coefficients a_h are 0 or 1, E interpreted as a subset of elements of H is an (r, k, λ)-difference set.

Write the image of a group G under a group homomorphism as $H \simeq G/N$. It is then clear that the image of a difference set D

in $\mathbb{Z}G$ under the corresponding ring homomorphism is a difference list $E = \sum_h a_h h$ in $\mathbb{Z}H$. In this case the multiplicity a_h counts the number of elements of D in the coset mod N that corresponds to h. In ([**8**], p. 332) we find the remark that not all difference lists can be obtained in this way. We also find the following interesting theorem, due to Hall and Ryser for cyclic groups and Bruck for general groups ([**10**], p. 469).

Theorem 7.4. *Let E be an (r, k, s, λ)-difference list over H, where r is odd and $n = k - \lambda$. Then the equation*

$$x^2 = ny^2 + (-1)^{(r-1)/2} r z^2$$

has a nontrivial solution in integers x, y, z.

This result is similar to the powerful and useful Bruck-Ryser-Chowla Theorem for symmetric designs (and thereby for difference sets).

Example 8. Can a $(25, 9, 3)$-difference set exist? These parameters satisfy BRC because $x^2 = 6y^2 + 3z^2$ has the solution $x = 3$ and $y = z = 1$. It is a consequence of the class equation (A.10) that every group of order equal to the square of a prime is abelian. Therefore a group of order 25 has a normal subgroup of order 5. It follows that if a difference set with these parameters existed, then a $(5, 9, 5, 3)$-difference list would also exist. Then by Theorem 7.4 the equation $x^2 = 6y^2 + 5z^2$ would have a nontrivial solution. However, by Theorem 5.2, this is impossible. ◇

Exercises

1. Let D be the difference set in Example 1.

(a) Let N be the normal subgroup $\langle a \rangle$. Find the intersection numbers for D with respect to N, and verify that these numbers obey Theorem 7.1.

(b) Show that these nine intersection numbers form a subpartition of the intersection numbers with respect to $\langle a, b \rangle$.

2. Consider the non-abelian group $G = \langle a, b \mid a^9 = b^3 = 1,\ ba = a^4 b\rangle$ with $(27, 13, 6)$-difference set given by Kibler

$$D = \{1, a, a^2, a^4, a^5, a^7, b, ab, a^2b, a^5b, a^5b^2, a^6b^2, a^8b^2\}.$$

(a) Check whether the subgroups $\langle a\rangle$ and $\langle b\rangle$ are normal subgroups.

(b) For any normal subgroups found in part (a), find the corresponding intersection numbers and confirm that they satisfy the equations in Theorem 7.1. Ⓢ

3. In this exercise we return to Example 4 to verify the claim that the only intersection numbers for a $(27, 13, 6)$-difference set G satisfying the equations in Theorem 7.1 are $3, 4, 6$. Suppose the intersection numbers, in some order, are the non-negative integers x, y, z.

(a) Explain why, without loss of generality, we may assume $x \leq y \leq z \leq 7$.

(b) By examining cases, complete the verification.

4. In the proof of Theorem 7.1, where do we use the fact that N is a *normal* subgroup of G?

5. Consider the non-abelian group

$$G = \langle a, b \mid a^{19} = b^3 = 1,\ ba = a^7 b\rangle.$$

(a) Show that $N = \langle a\rangle$ is normal in G.

(b) Assume that there is a $(57, 8, 1)$-difference set D in G, and find all possible triples of intersection numbers using Theorem 7.1.

(c) Show that we can assume without loss of generality that $n_0 \geq n_1,\ n_2$, where $n_j = |D \cap b^j N|$.

(d) Show that there is no homomorphism of G that fixes N and interchanges the cosets bN and b^2N. (This means we cannot swap intersection numbers n_1 and n_2 without loss of generality.)

(e) Compare your results above to the two difference sets in G given in Kibler's list for this group [**40**]:

$D_2 = \{1,\ a,\ a^3,\ a^8,\ b,\ a^4b,\ a^{13}b,\ a^{18}b^2\}$,
$D_3 = \{1,\ a,\ a^3,\ a^8,\ b,\ a^5b^2,\ a^9b^2,\ a^{18}b^2\}$.

6. Let G be a group of order 39. First look back at Example 5.7 to see what we know so far about the existence of $(39, 19, 9)$-difference sets. Use Theorem 7.1 to show that G cannot contain a $(39, 19, 9)$-difference set. Ⓗ

7. Let G be as in Example 6. Map G onto $H = \langle b \rangle$ by $\varphi(a^i b^j) = b^j$.

(a) Verify that φ is a group homomorphism.

(b) Calculate $\widehat{\varphi}((a^2 + 3ab - 5a^2b)(2a^5 - b))$.

(c) Calculate $\widehat{\varphi}(a^2 + 3ab - 5a^2b)\widehat{\varphi}(2a^5 - b)$.

8. Prove Theorem 7.2.

9. Start with the $(40, 13, 4)$-difference set

$$D = \{1, a, a^2, b, a^3b, ab^2, a^3b^2, a^4b^2, ab^4, ab^5, a^2b^5, ab^6, a^4b^7\}$$

in the group $G = \langle a, b \mid a^5 = b^8 = 1, ba = a^4b \rangle$.

(a) Explain why $N = \langle a \rangle$ is a normal subgroup in G.

(b) Find a complete set of coset representatives of G modulo N.

(c) Let $\varphi : G \to G/N = H$ be the natural homomorphism. Find $\widehat{D} = \widehat{\varphi}(D)$.

(d) How do the coefficients of $\widehat{D}$ in $\mathbb{Z}H$ compare to the intersection numbers for D mod N?

10. Prove Theorem 7.3

11. Using the notation of Example 7, compare the coefficients of 1_H on each side of the $\mathbb{Z}H$ equation in Theorem 7.3 to give another proof of Theorem 7.1

12. Recall from Section 5.1 that no projective plane of order $n = 10$ exists. It follows that no symmetric $(111, 11, 1)$ design exists, even though these parameters satisfy BRC. This fact implies that no difference set with these parameters exists. Using Theorem 7.4, give a direct proof that no $(111, 11, 1)$-difference set exists. Ⓗ

13. This exercise concerns the parameters $(201, 25, 3)$.

(a) Show that these parameters satisfy BRC.

(b) Use Theorem 7.4 to show that no $(201, 25, 3)$-difference set exists.

7.2. Turyn's exponent bound

The aspect of the structure of a group G that is the focus of this section is the exponent[1] of a Sylow p-subgroup of G. We also restrict our attention to abelian groups. The first version of our main theorem further restricts our discussion to difference sets with parameters $(4p^{2a},\ 2p^{2a} - p^a,\ p^{2a} - p^a)$ for a prime p. While this may sound narrow, these difference sets are in the important "Hadamard family" with $v = 4n$. All of these difference sets can be shown to have parameters of the form $(4u^2, 2u^2 - u, u^2 - u)$. We study them in Section 9.3. The second version of Turyn's theorem is more general.

Turyn's paper [**69**] is important not only for his very useful exponent bound, but also for his innovative use of tools from character theory and from algebraic number theory. We give an elementary introduction to some of these methods in Chapters 11 and 12. Here is the first version of Turyn's theorem as it is often given in the literature (for example, in [**8**], p. 414).

Theorem 7.5. *(Turyn's exponent bound, first version) Let p be a prime and assume the existence of a difference set with parameters*

$$(4p^{2a},\ 2p^{2a} - p^a,\ p^{2a} - p^a)$$

[1] See A.8 for the definition of the exponent of a group.

(b) Write $G_1 = \langle a, b \mid a^{32} = b^2 = 1, ab = ba \rangle$. Give generators and relations for a *non-cyclic* subgroup H of index 2 in G_1.

(c) Specify generators and relations for a generalized dihedral extension G_2 of H that is not isomorphic to D_{32}.

(d) Show that G_2 cannot contain a $(64, 28, 12)$-difference set.

Coda

In this chapter we continue our focus on the existence question for difference sets. Here we ask if a group G contains a difference set D, what does that imply about the structure of G? This emphasis on group structure is in contrast to the emphasis on the parameters (v, k, λ) in the two preceding chapters.

In Section 1 we look at the distribution of elements of a difference set in the cosets of a normal subgroup. A useful strategy is to construct a sieve of smaller and smaller normal subgroups of G, leading to finer and finer constraints on the possible elements of a difference set. Sometimes this strategy by itself suffices to prove non-existence. Sometimes it restricts the possibilities enough to make tractable a computer search that either produces a difference set or shows that none can exist. In this way this sieve strategy is similar to the analysis of unions of orbits of multipliers in Chapter 6.

Section 2 concerns the exponent of the Sylow p-subgroup for a prime p. Turyn's exponent bound may prove non-existence, but it provides no help in constructing a difference set if one is possible. This section focuses on applying Turyn's theorem. The proof uses deep ideas from representation theory and algebraic number theory, and it is our culminating application of these tools in Chapter 12.

Dillon's "dihedral trick" in Section 3 links existence of a difference set in a generalized dihedral extension of an abelian group H to existence in an abelian extension of H. It can be used either to prove non-existence or to produce an abelian difference set if the non-abelian one is known.

Chapters 5–7 contain clear necessary conditions for existence, and the latter two provide methods to narrow the search for a difference set to the point where a computer search may be feasible. In contrast, the next two chapters give explicit constructions for difference sets.

Chapter 10

Representation Theory

Representation theory is an essential tool for the study of algebraic structures, especially groups. We use representations of finite groups to discover and explore difference sets. Recall that in Section 9.3 we mentioned Smith's surprising discovery of a non-abelian $(100, 45, 20)$-difference set. He made substantial use of group representations and characters in his work.

Representation theory has important applications to many areas of mathematics, and to physics and chemistry as well. Because the subject is so beautiful and so widely used, we decided against simply quoting the results we need. Instead, in this chapter and the next we offer a brief primer on representations of finite groups and their characters. As in the proof of the Bruck-Ryser-Chowla Theorem, many of the arguments in these two chapters display the power of linear algebra.

10.1. Definitions and examples

Recall from abstract algebra that $GL(m, \mathbb{K})$, the set of invertible $m \times m$ matrices with elements from the field $\mathbb{K}$, is a group under matrix multiplication. This is known as the general linear group. We may interpret these matrices as invertible linear transformations from $\mathbb{K}^m$ to $\mathbb{K}^m$, where for $A \in GL(m, \mathbb{K})$, each vector $\mathbf{x} \in \mathbb{K}^m$ is mapped to

Coda

Just as the primes are the (multiplicative) building blocks for the integers, irreducible representations are the (additive) building blocks for representations of finite groups. Maschke's Theorem is our key result. It says that every representation is expressible as a sum of irreducible representations. The proof of Maschke's Theorem is complicated. Running through many of the arguments is the potent idea of averaging (more generally, summing) over a group.

We work over the complex numbers. The powerful facts that the field $\mathbb{C}$ is algebraically closed and has characteristic 0 give us an efficient route to the proof of Maschke's Theorem—one exploiting the nice properties of inner products in complex vector spaces and of unitary transformations of those spaces.

This chapter concludes by linking representation theory to the existence question for difference sets. Extending a representation $\rho : G \to GL(m, \mathbb{C})$ to a ring homomorphism $\widetilde{\varphi} : \mathbb{Z}G \to \mathcal{M}(m, \mathbb{C})$ translates the existence question to one in algebraic number theory.

A more general version of Maschke's Theorem applies over arbitrary fields with characteristic 0 or p relatively prime to the order of the group. The proof of this version of the theorem uses projections onto subspaces. A source for the proof of this stronger theorem is Curtis and Reiner's classic monograph [**15**], Section 10.8.

It takes us well beyond the scope of our work, but a theory of representations of infinite groups does exist—part of what is called "harmonic analysis." Representations of infinite "Lie groups" are important in physics. Under suitable hypotheses, satisfied by Lie groups, finite sums over the group can be replaced by integrals. There is also a "modular theory" of representations of finite groups over fields of characteristic p dividing the group order. Modular representation theory played an important role in early work on the classification of the finite simple groups.