MATH4306

Topics in Combinatorics

2023

Contents

Chapter 1

Preliminaries

1.1 Basics of Group Theory

Recall that a **group** consists of a nonempty set G together with a binary operation $\cdot$ on G satisfying

Associativity	For all $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
Identity	There exists $e \in G$ such that $e \cdot a = a = a \cdot e$ for every $a \in G$.
Inverses	For every $a \in G$ there exists $a^{-1} \in G$ such that $a \cdot a^{-1} = e = a^{-1} \cdot a$.

The notation 1_G is used to denote the identity of a group G, but the identity may also be denoted by 1 or e. We often write just ab rather than $a \cdot b$. The group with just one element is called the **trivial group**. We may use G to denote either the set of elements in the group, or the group together with its binary operation. The **order** of a group G is the cardinality of its underlying set of elements.

Definition 1.1.1. A group $(G, \cdot)$ is **abelian** or **commutative** if its binary operation is commutative, that is if $xy = yx$ for all $x, y \in G$.

Theorem 1.1.2. Let G be a group, let $a, b, c \in G$, and let $m, n \in \mathbb{Z}$.

(a) If $ab = ac$, then $b = c$ (left cancellation). If $ba = ca$, then $b = c$ (right cancellation).

(b) $a^m a^n = a^{m+n}$.

(c) $(a^m)^n = a^{mn}$.

(d) $(ab)^{-1} = b^{-1} a^{-1}$

(e) If G is abelian, then $(ab)^n = a^n b^n$.

Definition 1.1.3. Let $(G, *)$ and $(H, \circ)$ be groups. The **direct product** $G \times H$ of G and H is the group with binary operation $\odot$ defined by

$$(g_1, h_1) \odot (g_2, h_2) = (g_1 * g_2,\ h_1 \circ h_2).$$

Definition 1.1.4. Let G be a group. If H is a non-empty subset of G such that

(a) For all x, $y \in H$, $xy \in H$;

(b) $1 \in H$; and

(c) For all $x \in H$, $x^{-1} \in H$;

then H is a **subgroup** of G. If H is a subgroup of G, then we write $H \leq G$.

Definition 1.1.5. In a group G, the **order** of an element $a \in G$ is the smallest positive integer n such that $a^n = 1$; if no such n exists then a has infinite order.

If $a \in G$ has order n, then $\{1, a, a^2, \ldots, a^{n-1}\}$ is a subgroup of G. A group of the form $G = \{a^n : n \in \mathbb{Z}\}$ is called the **group generated by** a and is a **cyclic** group. Up to isomorphism (see below for definition of isomorphism), for each positive integer n there is only one cyclic group of order n, namely $\{1, a, a^2, \ldots, a^{n-1}\}$.

Example 1.1.6. Let n be a positive integer. Two integers a and b are said to be equivalent modulo n if n divides $a-b$. This is an equivalence relation with n equivalence classes $[0], [1], \ldots, [n-1]$. The set $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$ forms a group under the binary operation $+$ where $[a] + [b]$ is given by $[a] + [b] = [a + b]$. We usually abbreviate $[a]$ to a.

The group $(\mathbb{Z}_n, +)$ is the cyclic group of order n.

Permutions and the Symmetric Group:

Let π be a permutation of a set S. For each $x \in S$, the image of x under π may be denoted by either $\pi(x)$ or $x\pi$, whichever is more convenient. If π is a permutation and $\pi(x) = x$, then x is called a **fixed point** of π and we say that π **fixes** x. A convenient way to describe and work with permutations is by using their **cycle representation**, which we now define and use hereafter.

Let A be a non-empty finite set and let π be a permutation of A. Since A is finite and since π is a permutation, for any $a \in A$, there is a smallest positive integer k such that $\pi^k(a) = a$. Moreover, a, $\pi(a)$, $\pi^2(a)$, $\ldots$, $\pi^{k-1}(a)$ are pairwise distinct elements of A. Thus, the elements of A can be partitioned into cycles where each cycle $(a_0\ a_1\ \ldots\ a_{k-1})$ satisfies

$$a_0 \mapsto a_1 \mapsto a_2 \mapsto \cdots \mapsto a_{k-1} \mapsto a_0.$$

A cycle $(a_0\ a_1\ \ldots\ a_{k-1})$ is said to have **length** k. A **cycle representation** for a permutation is given by listing all its cycles in this manner. The **cycle structure** of a permutation is the sequence of the lengths of its cycles (in non-increasing order).

If a is a fixed point of π, then the cycle of π containing a is (a), and has length 1. Sometimes cycles of length 1 are omitted from a cycle representation of a permutation, with the understanding that any elements of A not appearing in the cycle representation of π are fixed points of π (however, any cycles of length 1 must still be counted in the cycle structure of π). The notation $()$ or (1) may be used to represent the identity permutation.

As an example, the permutation π of $\{1, 2, 3, 4, 5, 6\}$ given by

$$1 \mapsto 4,\ 2 \mapsto 6,\ 3 \mapsto 2,\ 4 \mapsto 1,\ 5 \mapsto 5,\ 6 \mapsto 3$$

has cycle representation $\pi = (1\ 4)(2\ 6\ 3)(5)$ or just $\pi = (1\ 4)(2\ 6\ 3)$. The cycles of a cycle representation of a permutation can be written in any order, and the elements within each cycle can be cyclically permuted, with any one of the elements of the cycle appearing first. So, if the cycle of length 1 is omitted, then there are twelve different equivalent ways of writing a cycle representation of the permutation π given above, namely

$$\begin{array}{cccccc} (1\ 4)(2\ 6\ 3), & (1\ 4)(6\ 3\ 2), & (1\ 4)(3\ 2\ 6), & (4\ 1)(2\ 6\ 3), & (4\ 1)(6\ 3\ 2), & (4\ 1)(3\ 2\ 6), \\ (2\ 6\ 3)(1\ 4), & (6\ 3\ 2)(1\ 4), & (3\ 2\ 6)(1\ 4), & (2\ 6\ 3)(4\ 1), & (6\ 3\ 2)(4\ 1), & (3\ 2\ 6)(4\ 1). \end{array}$$

It should be clear that the cycle structure of a permutation is independent of which particular cycle representation is used. The partition given by the cycles is also unique to the permutation.

Note that if $\pi = (x_1\ x_2\ \cdots\ x_k)(y_1\ y_2\ \cdots\ y_\ell)$, then π is equal to the composition

$$\pi = (x_1\ x_2\ \cdots\ x_k) \circ (y_1\ y_2\ \cdots\ y_\ell)$$

of the two permutations having cycle representations $(x_1\ x_2\ \cdots\ x_k)$ and $(y_1\ y_2\ \cdots\ y_\ell)$. Thus, each cycle within any given cycle representation, may be thought of as a permutation in its own right, and the cycle representation may be thought of as a composition of the permutations corresponding to the individual cycles.

When composing cycle representations, or indeed any mappings, consideration must be given to whether the mappings are written on the left or the right of the argument; that is, whether the image of x under the map f is written as $f(x)$ or xf. If written on the left, then the image of x under fg is $(fg)(x) = f(g(x))$ – which means that g acts first followed by f. However, if written on the right, then the image of x under fg is $x(fg) = (xf)g$ – which means that f acts first followed by g.

For example, when using the convention of writing permutations on the left, we have

$$(1\ 2\ 3) \circ (1\ 4\ 5)(2\ 3) = (1\ 4\ 5\ 2),$$

whereas when using the convention of writing permutations on the right, we have

$$(1\ 2\ 3) \circ (1\ 4\ 5)(2\ 3) = (1\ 3\ 4\ 5),$$

However, if $(a_1\ a_2\ \cdots\ a_k)$ and $(b_1\ b_2\ \cdots\ b_\ell)$ are disjoint cycles (that is, $\{a_1, a_2, \ldots, a_k\} \cap \{b_1, b_2, \ldots, b_\ell\} = \emptyset$), then $(a_1\ a_2\ \cdots\ a_k) \circ (b_1\ b_2\ \cdots\ b_\ell) = (b_1\ b_2\ \cdots\ b_\ell) \circ (a_1\ a_2\ \cdots\ a_k)$. This is why the order of the cycles in a cycle representation of a permutation does not matter.

Note that there are two subtly different meanings of the term permutation in common usage. First, a permutation of A is a bijective function from A to itself, and this is the definition that we will be using. The second is that a permutation is simply a listing of the elements of A in some order.

Definition 1.1.7. For a set S, the set of all permutations of S is denoted by $\mathrm{Sym}(S)$. Under function composition, $\mathrm{Sym}(S)$ forms a group, called the **symmetric group acting on S**, and the notation $\mathrm{Sym}(S)$ is also used to denote this group. The group $\mathrm{Sym}(\{1, 2, \ldots, n\})$ may be denoted by $\mathrm{Sym}(n)$, and the notation S_n is used to denote any group that is isomorphic to $\mathrm{Sym}(n)$.

Definition 1.1.8. For each $n \geq 3$, the **dihedral group** D_n is the subgroup of $\mathrm{Sym}(n)$ given by

$$D_n = \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \ldots, \sigma^{n-1}\tau\}$$

where $\sigma = (1\ 2\ \cdots\ n)$, $\tau = (1)(2\ n)(3\ n-1)(4\ n-2)\cdots(\frac{n}{2}\ \frac{n}{2}+2)(\frac{n}{2}+1)$ if n is even, and $\tau = (1)(2\ n)(3\ n-1)(4\ n-2)\cdots(\frac{n+1}{2}\ \frac{n+3}{2})$ if n is odd.

The dihedral group D_n is a non-abelian group with $2n$ elements, and is the group of symmetries of a regular n-gon. The elements $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ correspond to rotations of the n-gon, and the elements $\tau, \sigma\tau, \sigma^2\tau, \ldots, \sigma^{n-1}\tau$ correspond to reflections of the n-gon.

Definition 1.1.9. Let $g \in S_n$ and define $c(g)$ to be the number of cycles, including any cycles of length 1, in any cycle representation of g (this equals the number of terms in the cycle structure of g). The **parity** of g is defined to be the parity, odd or even, of the integer $n - c(g)$.

A permutation of odd parity is called an **odd permutation** and a permutation of even parity is called an **even permutation**. The parity of a permutation is considered an element $\mathbb{Z}_2$. So even permutations have parity $0 \in \mathbb{Z}_2$, and odd permutations have parity $1 \in \mathbb{Z}_2$.

Theorem 1.1.10. The composition of any two even permutations is even, the composition of any two odd permutations is even, and the composition of any even permutation and any odd permutation is odd.

Definition 1.1.11. A **transposition** is a permutation that interchanges two elements and fixes every other element.

Theorem 1.1.12. Any element of S_n is a product of transpositions.

Theorem 1.1.13. For pairwise distinct $x_1, x_2, \ldots, x_m$, the permutation $(x_1\ x_2\ \cdots\ x_m)$ is an even permutation if m is odd, and is an odd permutation if m is even.

Theorem 1.1.14. Let $n \geq 2$ be an integer. The even permutations of S_n form a normal subgroup of index 2.

Definition 1.1.15. Let $n \geq 2$ be an integer. The group consisting of the even permutations of S_n is called the **alternating group of degree** n and is denoted by A_n.

Homomorphisms, Quotients, Normal Subgroups, Simple Groups:

Definition 1.1.16. Let $(G, *)$ and $(H, \circ)$ be two groups. A **(group) homomorphism** from G to H is a function $f : G \to H$ satisfying

$$f(x * y) = f(x) \circ f(y) \qquad \text{for all } x, y \in G.$$

Theorem 1.1.17. Let $(G, *)$ and $(H, \circ)$ be groups, and let $f : G \to H$ be a homomorphism. Then

(a) $f(1_G) = 1_H$ (homomorphisms preserve the identity); and

(b) $f(x^{-1}) = f(x)^{-1}$ (homomorphisms preserve inverses).

Definition 1.1.18. Let $f : G \to H$ be a homomorphism. The **kernel** of f is the set

$$\ker f = \{g \in G : f(g) = 1_H\}.$$

The **image** of f is the set

$$\operatorname{Im} f = \{f(g) : g \in G\}.$$

Definition 1.1.19. An **isomorphism** is a bijective group homomorphism. If there exists an isomorphism $f : G \to H$ we say that G is **isomorphic** to H, and write $G \cong H$.

Definition 1.1.20. An isomorphism from G to itself is called an **automorphism** of G.

Theorem 1.1.21. If $f : G \to H$ is a homomorphism, then $\ker f = \{1_G\}$ if and only if f is injective.

Definition 1.1.22. Let G be a group, H a subgroup of G and $a \in G$. The **left coset** aH is the subset of G given by

$$aH = \{ah : h \in H\}.$$

The collection of all left cosets of H is denoted G/H.

The **right coset** Ha is the set $Ha = \{ha : h \in H\}$, but we will not be dealing with right cosets. Thus, we usually refer to left cosets simply as **cosets**.

Theorem 1.1.23. Let G be a group, let H be a subgroup of G, and let $a, b, c \in G$.

(a) $aH = bH$ if and only if $a^{-1}b \in H$.

(b) $aH = bH$ if and only if $b \in aH$.

(c) $aH = bH$ if and only if $caH = cbH$.

(d) $a \in bH$ if and only if $ca \in cbH$.

(e) G/H is a partition of G.

(f) If G is finite then any two left cosets of H have the same number of elements, equal to the number of elements in H.

Theorem 1.1.24. [Lagrange's Theorem] Let G be a finite group, and let H be a subgroup of G. Then the order of H divides the order of G.

Definition 1.1.25. A subgroup H of G is said to be **normal** if for every g in G and $h \in H$, we have $g^{-1}hg \in H$. We write

$$H \trianglelefteq G$$

to mean H is a normal subgroup of G.

Given a group G and a subgroup H, there is a natural way to try to define a binary operation on the set G/H of cosets, namely

$$(aH)(bH) = (ab)H.$$

However, this "definition" is only well-defined if H is a normal subgroup of G. If H is not normal, then we sometimes get different evaluations of $(aH)(bH)$ depending on which representatives are used for the cosets. That is, we have $a_1H = a_2H$ and $b_1H = b_2H$, but $(a_1b_1)H \neq (a_2b_2)H$. If $H \trianglelefteq G$, then the binary operation $(aH)(bH) = (ab)H$ on G/H is well-defined.

Theorem 1.1.26. If $H \trianglelefteq G$, then under the binary operation $(aH)(bH) = (ab)H$, G/H is a group.

Definition 1.1.27. If $H \trianglelefteq G$, then G/H under the binary operation $(aH)(bH) = (ab)H$ is called the **quotient group**, or **factor group**, of G by H.

Theorem 1.1.28. Let G be a group.

(a) $\{1_G\} \trianglelefteq G$ and $G/\{1_G\} \simeq G$.

(b) $G \trianglelefteq G$ and G/G is the trivial group.

(c) If G is abelian and $H \leq G$, then $H \trianglelefteq G$.

Theorem 1.1.29. [First Isomorphism Theorem] Let G and H be groups and let $f : G \to H$ be a homomorphism. Then

(a) $\ker f \trianglelefteq G$;

(b) $\operatorname{Im} f \leq H$; and

(c) $G/\ker f \simeq \operatorname{Im} f$.

Definition 1.1.30. A group is **simple** if it is non-trivial and its only normal subgroups are the trivial subgroup and the whole group.

1.2 Permutation Groups

Definition 1.2.1. A subgroup of $\mathrm{Sym}(S)$ is a **permutation group acting on S**. The **degree** of a permutation group acting on S is $|S|$.

Definition 1.2.2. Let S be a set and let G be a group. An **action of G on S** is a homomorphism from G into $\mathrm{Sym}(S)$. When we have an action ϕ of G on S, we say that **G acts on S**, and we write $g(x)$ to denote the image of x under the permutation $\phi(g) \in \mathrm{Sym}(S)$.

Observe that when G acts on S, for all $g_1, g_2 \in G$ and all $x \in S$ we have

$$(g_1g_2)(x) = g_1(g_2(x)).$$

Also, the image $\operatorname{Im} \phi = \{\phi(g) : g \in G\}$ of an action $\phi : G \to \mathrm{Sym}(S)$ is a permutation group acting on S.

Definition 1.2.3. An action of G on S is **faithful** if its kernel is the trivial group.

Let G and S be finite and let ϕ be an action of G on S. Observe that by the First Isomorphism Theorem (for groups), the action ϕ is faithful if and only if the permutation group $\operatorname{Im}\phi$ is isomorphic to G.

Definition 1.2.4. Let G be a permutation group acting on a finite set S and $T \subseteq S$. For each $g \in G$, we define the notation $g(T)$ by

$$g(T) = \{g(x) : x \in T\}$$

and refer to this as the induced action of G on subsets of S. Similarly, if $(x_1, x_2, \ldots, x_t)$ is any ordered t-tuple of of elements of S, then we define $g((x_1, x_2, \ldots, x_t))$ by

$$g((x_1, x_2, \ldots, x_t)) = (g(x_1), g(x_2), \ldots, g(x_t))$$

and refer to this as the induced action of G on t-tuples of elements of S.

It is not too difficult to verify that the notation in the above definition actually defines a homomorphism from the permutation group G acting on S to a permutation group acting on a set of subsets, or on a set of t-tuples. Thus, it makes sense to refer to these as induced actions of G.

Definition 1.2.5. If G is a permutation group acting on a set S, then the equivalence classes of the relation $\sim$ on S given by $x \sim y$ if and only if there exists a $g \in G$ such that $g(x) = y$ are called the **orbits** of G.

Definition 1.2.6. The subgroup $G_T = \{g \in G : g(x) = x \text{ for all } x \in T\}$ of G is called the **pointwise stabilizer** of T. The subgroup $G_{\{T\}} = \{g \in G : g(T) = T\}$ of G is called the **setwise stabilizer** of T. The notation G_x may be used instead of $G_{\{x\}}$.

Theorem 1.2.7. Let G be a permutation group. If x and y are in the same orbit, then $\{g \in G : g(x) = y\}$ is a left coset of G_x. Conversely, any two elements from the same left coset of G_x map x to the same point of S.

Proof If x and y are in the same orbit, then there exists $g^* \in G$ such that $g^*(x) = y$. We show that $\{g \in G : g(x) = y\}$ is the coset g^*G_x. An arbitrary element of g^*G_x can be written as g^*g' for some $g' \in G_x$, and then we have $(g^*g')(x) = g^*(g'(x)) = g^*(x) = y$. Thus, $g^*G_x \subseteq \{g \in G : g(x) = y\}$. If $g'' \in \{g \in G : g(x) = y\}$, then $((g^*)^{-1}g'')(x) = (g^*)^{-1}(g''(x)) = (g^*)^{-1}(y) = x$. Thus, $(g^*)^{-1}g'' \in G_x$, which is equivalent to $g'' \in g^*G_x$, and so we also have $\{g \in G : g(x) = y\} \subseteq g^*G_x$.

Now, conversely, let h_1, h_2 be two elements from the same left coset of G_x. Then $h_2^{-1}h_1 \in G_x$ and so $x = (h_2^{-1}h_1)(x) = h_2^{-1}(h_1(x))$. Thus, $h_1(x) = h_2(x)$. □

The following result is called the **Orbit-Stabilizer Theorem**.

Theorem 1.2.8. If G is a permutation group acting on a finite set S and $x \in S$, then

$$|G| = |G_x||\mathcal{O}(x)|$$

where $\mathcal{O}(x)$ denotes the orbit containing x.

Proof Let $\mathcal{O}(x) = \{g_1(x), g_2(x), \ldots, g_r(x)\}$. By Theorem 1.2.7, $g_1G_x, g_2G_x, \ldots, g_rG_x$ are the cosets of G_x. So $|\mathcal{O}(x)|$ is the number of cosets of G_x. Since the cosets of a subgroup partition the group into parts of equal cardinality, we have $|G| = |G_x||\mathcal{O}(x)|$. □

Definition 1.2.9. A permutation group is **transitive** if it has a single orbit.

If G is a transitive permutation group acting on S, then we may say **G acts transitively on S** or **G has a transitive action on S**.

Definition 1.2.10. A permutation group G acting on a finite set S is **regular** if for all $x, y \in S$, there is a unique $g \in G$ such that $g(x) = y$.

If G is a regular permutation group acting on S, then we may say **G acts regularly on S** or **G has a regular action on S**. Note that a regular group is transitive, but not every transitive group is regular.

Theorem 1.2.11. If G is a transitive permutation group acting on a finite set S, then the following are equivalent.

- G is regular.
- If $g \in G$ and there exists an $x \in S$ such that $g(x) = x$, then g is the identity.
- $|G| = |S|$.

Definition 1.2.12. Let G be a permutation group acting on S and let t be a positive integer with $t \leq |S|$. Then G is (sharply) **t-transitive** if for any two t-tuples $(x_1, x_2, \ldots, x_t)$ and $(y_1, y_2, \ldots, y_t)$, each containing pairwise distinct elements of S, there exists a (unique) $g \in G$ such that $g(x_i) = y_i$ for $i = 1, 2, \ldots, t$.

Thus, if G is t-transitive, then it is t'-transitive for $1 \leq t' \leq t$, 1-transitive is equivalent to transitive, and a group is t-transitive if and only if it acts transitively on t-tuples of distinct elements.

1.3 Some Exceptional Objects

There are some "exceptional" algebraic/combinatorial objects that we will encounter several times, and we mention these here. See `https://en.wikipedia.org/wiki/Exceptional_object`.

Convex Regular Polytopes.

The 2-dimensional convex regular polytopes are the regular n-gons for $n \geq 3$, and the 3-dimensional convex regular polytopes are the five Platonic solids: the tetrahadron, the cube, the octahedron, the icosahedron and the dodecahedron. There are six 4-dimensional convex regular polytopes. These are the **n-cells** for $n \in \{5, 8, 16, 24, 120, 600\}$.

The 5-cell, 8-cell, and 16-cell are 4-dimensional versions of the tetrahadron, the cube, and the octahedron, respectively. And for each $n \geq 5$, there also is an n-dimensional version of the tetrahadron, the cube, and the octahedron. However, these are the only convex regular polytopes of dimension $n \geq 5$. So we see that the icosahedron, dodecahedron, 24-cell, 120-cell and 600-cell are exceptional cases that fall outside the infinite families. These are known as the **exceptional convex regular polytopes**.

The Outer Automorphisms of S_6.

An **automorphism** of a group G is a map $\phi : G \to G$ satisfying $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$. The set of all automorphisms of G forms a group called the **automorphism group** of G and denoted by $\mathrm{Aut}(G)$. If G is a group and $g \in G$, then the map $\phi_g : G \to G$ given by

$$\phi_g(x) = g^{-1}xg \text{ for all } x \in G$$

is called **conjugation** by g. Conjugation is an automorphism of G and is called an **inner automorphism**.

An automorphism of G that is not an inner automorphism is called an **outer automorphism**. A remarkable fact is that S_6 is the only symmetric group S_n with an outer automorphism. See `https://cameroncounts.wordpress.com/2010/05/11/the-symmetric-group-3/` for a proof of this result.

Theorem 1.3.1. The symmetric group S_n has an outer automorphism if and only if $n = 6$.

The Mathieu groups.

Simple Groups:

Simple groups play a fundamental role in group theory. In the second half of the twentieth century (and with some small corrections/omissions made later), a program to classify all the finite simple groups was successfully undertaken. Up to isomorphism, the finite simple groups are

(a) $\mathbb{Z}_p$ where p is prime.

(b) A_n where $n \geq 5$.

(c) The so-called "groups of Lie type", which form an infinite family.

(d) 26 "sporadic groups".

Five of the ten smallest sporadic groups are the "Mathieu groups"

$$M_{11}, \qquad M_{12}, \qquad M_{22}, \qquad M_{23} \qquad \text{and} \qquad M_{24}$$

which have orders

$$7,920, \qquad 95,040, \qquad 443,520, \qquad 10,200,960 \qquad \text{and} \qquad 244,823,040$$

respectively. The largest sporadic group, the "Monster group", has order

$$808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000.$$

Multiply Transitive Groups:

The only t-transitive group actions with $t \geq 4$ are as follows. The proof of this fact uses the classification of finite simple groups.

- The symmetric group S_n is sharply n-transitive on n points.
- The alternating group A_n is sharply $(n-2)$-transitive on n points.
- The Mathieu group M_{11} is sharply 4-transitive on 11 points.
- The Mathieu group M_{12} is sharply 5-transitive on 12 points.
- The Mathieu group M_{23} is 4-transitive on 23 points.
- The Mathieu group M_{24} is 5-transitive on 24 points.

The Steiner Systems $S(5,6,12)$ and $S(5,8,24)$:

A (combinatorial) **design** consists a set V and a collection $\mathcal{B}$ of subsets of V. The elements of V are the **points** of the design, and the subsets in $\mathcal{B}$ are called **blocks**. An **automorphism** of a design is a permutation of V that preserves the blocks. More precisely, a permutation π of V is an automorphism of a design $(V, \mathcal{B})$ if $\mathcal{B}\pi = \mathcal{B}$, where $\mathcal{B}\pi = \{B\pi : B \in \mathcal{B}\}$ and $B\pi = \{x\pi : x \in B\}$.

A **Steiner system** $S(t,k,v)$ is a design with v points such that each block has cardinality k, and such that each t-subset of the points is a subset of exactly one block. The are only finitely many known non-trivial (non-trivial means $t < k < v$) Steiner systems with $t \geq 4$. All have $t \in \{4,5\}$, and two of the smallest with $t = 5$ are $S(5,6,12)$ and $S(5,8,24)$. The $S(5,6,12)$ and $S(5,8,24)$ are unique up to isomorphism. The automorphism group of $S(5,6,12)$ is M_{12} and the automorphism group of $S(5,8,24)$ is M_{24}.

For a long time, it was unknown whether there exist infinitely many non-trivial $S(t,k,v)$ systems with $t = 4$ or $t = 5$, and whether there are any non-trivial $S(t,k,v)$ systems with $t \geq 6$. However, in early 2014 Keevash [37] proved the existence of infinitely many $S(t,k,v)$ for all t. The proof of Keevash's Theorem is **non-constructive**, and uses the **Probabilistic Method**. A $t-(v,k,\lambda)$**-design** is a generalisation of an $S(t,k,v)$ system where each t-subset of the points is a subset of exactly λ blocks.

Theorem 1.3.2. (Keevash, [37]) For all $t \geq 1$, $k \geq t$ and $\lambda \geq 1$, there is a constant $C(t,k,\lambda)$ such that for all $v \geq C(t,k,\lambda)$, there exists a $t-(v,k,\lambda)$-design if and only if $\binom{k-s}{t-s}$ divides $\lambda\binom{v-s}{t-s}$ for $0 \leq s \leq t$.

Chapter 2

Combinatorial and Finite Geometry

2.1 Polygons and Pick's Theorem

In graph theory, a **tree** is a connected graph with no cycles. It is easy to prove that a tree with n vertices has $n-1$ edges. A subgraph H of a graph G is **spanning** if $V(H) = V(G)$. A spanning cycle is called a **Hamilton cycle** and a spanning path is called a **Hamilton path**. A graph is **planar** if it can be drawn or embedded in the plane (or equivalently on the surface of a sphere) without any edge crossings. A **plane graph** is a particular embedding of a planar graph. We will be using **Euler's formula** which gives a relation between the number of vertices, edges and faces in a connected plane graph. Euler's formula does not hold for disconnected graphs.

Theorem 2.1.1. If a connected plane graph has n vertices, e edges and f faces, then

$$n - e + f = 2.$$

Proof Suppose for a contradiction that the theorem is false and let G be a counter-example with the smallest number of edges. Since trees have exactly one face, the theorem holds for trees and G is not a tree. This means that G contains a cycle, and in particular an edge xy whose removal leaves a connected graph G'. If G has n vertices, e edges and f faces, then G' has n vertices, $e-1$ edges and $f-1$ faces (the faces on either side of xy are distinct in G). Since G' has fewer edges than G, it satifies Euler's formula. That is, $n-(e-1)+(f-1) = 2$, from which it follows that $n-e+f = 2$ contradicting the assumption that G is a counter-example. □

A **polygon** is a 2-dimensional region whose boundary is a simple closed curve which consists of straight line segments. These line segments are the polygon's **sides** or **edges**, and their endpoints are the polygon's **vertices**. A polygon with n sides, and hence also n vertices, is called an **n-gon**. Since a polygon's boundary is simple, any two sides are either disjoint or intersect at a vertex. Two vertices are **adjacent** if they are the endpoints of a single side, and two sides are **adjacent** if they share a common vertex.

A polygon is the union of two disjoint sets of points: its **boundary** (which is the union of its sides) and its **interior**. A **diagonal** of a polygon is a line segment xy where x and y are distinct non-adjacent vertices of the polygon. An **interior diagonal** of polygon P is a diagonal xy such that $xy \subseteq P$.

Theorem 2.1.2. For $n \geq 4$, every n-gon has an interior diagonal.

Proof Let P be a polygon. We begin by showing that every polygon has a vertex at which the interior angle is less than π. Since P is finite, there exists a line l such that $l \cap P = \emptyset$ and l is not parallel to any side or diagonal of P. It follows that there is a line l' such that l' is parallel to l, $l' \cap P = \{x\}$ where x is a vertex, and the interior angle of P at x is less than π.

Let y and z be the two vertices adjacent to x in P. Since $n \geq 4$, yz is a diagonal (not a side) of P. If yz is an interior diagonal of P then we are finished, so suppose otherwise. This means that the triangle xyz contains (perhaps only on its boundary) at least one vertex of P other than x, y and z. Thus, there is a triangle $xy'z'$ such that $y' \in xy$, $z' \in xz$, there is a vertex $w \in P \setminus \{y, z\}$ on $y'z'$, and there are no vertices of P in the interior of $xy'z'$. The triangle $xy'z'$ can be found by sweeping a line parallel to yz from x to yz until the first vertex of P (other than x) is encountered. The diagonal wx is an interior diagonal of P. $\square$

Theorem 2.1.3. The sum of the interior angles of an n-gon is $(n-2)\pi$.

Proof Using Theorem 2.1.2, the result can be proved by induction on n. For a triangle xyz, it is easily shown that the interior angles sum to π by considering a line through x that is parallel to yz. So let $n \geq 4$, let P be an n-gon, and assume that the result holds for polygons with fewer than n sides. By Theorem 2.1.2, P has an interior diagonal, and this diagonal partitions P into an n'-gon P' and an n''-gon P'' where $3 \leq n', n'' \leq n-1$ and $n' + n'' = n + 2$. By induction, the interior angles of P' and P'' sum to $(n'-2)\pi$ and $(n''-2)\pi$ respectively. But the sum of the interior angles of P' and P'' is the same as the sum of the interior angles of P. Thus, the sum of the interior angles of P is $(n'-2)\pi + (n''-2)\pi = (n-2)\pi$. $\square$

A **triangulation** of a polygon P is a set $\mathcal{T}$ of triangles such that

- $\bigcup_{T \in \mathcal{T}} T = P$,
- for all distinct $T_1, T_2 \in \mathcal{T}$, $T_1 \cap T_2$ is either empty, or is a side or vertex of both T_1 and T_2.

Any triangulation $\mathcal{T}$ of a polygon has a corresponding graph $G = G_{\mathcal{T}}$ where the vertices and edges of G are the vertices and sides of the triangles in $\mathcal{T}$.

Theorem 2.1.4. Every polygon has a triangulation in which the vertices of the triangles are vertices of the polygon.

Proof Let $n \geq 3$ and let P be an n-gon. The proof is by induction on n, and is clearly true for $n = 3$. So assume $n \geq 4$ and that the result holds for polygons with fewer than n vertices. By Theorem 2.1.2, P has an interior diagonal. Any interior diagonal of P divides P into an n'-gon P' and a n''-gon P'' where $3 \leq n', n'' \leq n-1$. By our inductive hypothesis, both P' and P'' have triangulations in which the vertices of the triangles are the vertices of P' or P'', and the union of these triangulations is the required triangulation of P. $\square$

A point in the plane is a **lattice point** if its coordinates are integers. A polygon P is a **lattice polygon** if all of its vertices are lattice points. A lattice polygon containing no lattice points other than its vertices is called **fundamental**, and a triangulation consisting entirely of fundamental triangles is a called a **fundamental triangulation**.

Theorem 2.1.5. Every lattice polygon has a fundamental triangulation.

Proof Given any lattice polygon, Theorem 2.1.4 guarantees the existence of a triangulation $\mathcal{T}$ consisting of lattice triangles. If there is a triangle T of $\mathcal{T}$ which is not fundamental, then there is a lattice point $x \in T$ which is not a vertex of T. If x is on the boundary of T, then join x to the opposite vertex of each triangle of $\mathcal{T}$ that contains x. Otherwise, x is in the interior of T, and is joined to the three vertices of T. The result of this process is a new triangulation consisting of lattice triangles. Moreover, it is clear that we can repeat this process until a triangulation is obtained in which every triangle is fundamental. $\square$

Theorem 2.1.6. The number of triangles in a fundamental triangulation of a lattice polygon P is $b + 2i - 2$ where b is the number of lattice points on the boundary of P and i is the number of lattice points in the interior of P.

Proof Let x be the number of triangles in an arbitrary triangulation of P into fundamental triangles. There is an obvious correspondence between the triangulation of P and a plane graph G. The vertices of G are the lattice points in P, the edges of G are the sides of the triangles in the triangulation, and the faces of G are the triangles and the exterior of P. The sum over all faces of G of the number of edges on the boundary of each face is $3x + b$. But this sum is also $2e$ where e is the number of edges in G. So G has $b + i$ vertices, $\frac{3x+b}{2}$ edges, and $x + 1$ faces. Thus, by Euler's formula we have $(b + i) - (\frac{3x+b}{2}) + (x + 1) = 2$, and it follows from this that $x = b + 2i - 2$. $\square$

Theorem 2.1.7. The area of a fundamental triangle is $\frac{1}{2}$.

Proof Any lattice triangle can be translated (without changing its area) to a lattice triangle in which one of the vertices is $(0, 0)$. The area of a triangle with coordinates $(0, 0)$, (w, x) and (y, z) is

$$\pm\frac{1}{2}\det\begin{pmatrix} w & y \\ x & z \end{pmatrix}.$$

(Under a matrix transformation, the area of the image of the unit square is the absolute value of the determinant.) Since the area is non-zero and the determinant is an integer, the area of any lattice triangle is at least $\frac{1}{2}$.

Now, let T be an arbitrary fundamental triangle. Then T can be embedded in a lattice 4-gon R having sides parallel to the x and y axes as follows. The two sides of R parallel to the x-axis pass through a vertex of T with largest y coordinate and a vertex of T with smallest y coordinate. The two sides of R parallel to the y-axis pass through a vertex of T with largest x coordinate and a vertex of T with smallest x coordinate. The rectangle R is partitioned into lattice polygons, one of which is T, and if we take an arbitrary fundamential triangulation of each of these polygons, then we obtain a fundamental triangulation of R which contains T.

However, R can also be partitioned into fundamental squares (in an obvious way), and each of these squares can be divided into two fundamental triangles (by a diagonal of the square). If R has sides of lengths a and b, then it has area ab and this fundamental triangulation of R contains $2ab$ triangles. Since every fundamental triangulation of R has the same number of triangles (see Theorem 2.1.6), the fundamental triangulation of R containing T also has $2ab$ triangles. We have shown that fundamental triangles have area at least $\frac{1}{2}$, and it follows that every triangle in the fundamental triangulation of R containing T has area $\frac{1}{2}$. In particular, T has area $\frac{1}{2}$. □

Theorem 2.1.8. (**Pick's Theorem**, 1899) If a lattice polygon has b lattice points on its boundary and i lattice points in its interior, then its area is $\frac{1}{2}b + i - 1$.

Proof Let P be a lattice polygon having b lattice points on its boundary and i lattice points in its interior. By Theorem 2.1.5, P has a fundamental triangulation, and by Theorem 2.1.6, the number of triangles is $b + 2i - 2$. Since each fundamental triangle has area $\frac{1}{2}$ (Theorem 2.1.7), the area of P is $\frac{1}{2}b + i - 1$. □

There is no higher dimensional direct analogue of Pick's Theorem. To see this, consider the **Reeve tetrahedron** R which has vertex coordinates $(0, 0, 0)$, $(1, 0, 0)$, $(0, 1, 0)$ and $(1, 1, h)$ where h is a positive integer. The only lattice points in R are its four vertices, but the volume of R is $\frac{1}{6}h$.

2.2 Sperner's Lemma

Let $\mathcal{T}$ be a triangulation of a triangle T, let $G = G_{\mathcal{T}}$ be the corresponding graph, and let $f : V(G) \mapsto \{1, 2, 3\}$ be a labeling of the vertices of G. We can equivalently think of f as a labeling of the corners of the triangles in $\mathcal{T}$. The labeling f is said to be a **Sperner labeling** if the corners of T are assigned three distinct labels, and exactly two distinct labels occur on each side of T. Thus, in a Sperner labeling all the vertices on the side of T that joins corners labeled i and j are labeled either i or j.

Theorem 2.2.1. (**Sperner's Lemma**, 1928) In any Sperner labeling of any triangulation $\mathcal{T}$ of a triangle T, there exists a $T^* \in \mathcal{T}$ such that the corners of T^* are assigned three distinct labels.

Proof We prove the stronger result that the number of triangles having corners with three distinct labels is odd. Let G be the graph corresponding to $\mathcal{T}$. Define a new graph H as follows. The vertices of H are the faces of G, and two vertices are adjacent if and only if their corresponding faces are adjacent and separated by an edge with endpoints labeled 1 and 2.

Let $x \in V(H)$ correspond to an internal face R of G. Then x has degree 1 if and only if the set of labels on the corners of R is $\{1, 2, 3\}$, x has degree 2 if and only if the set of labels on the corners of R is $\{1, 2\}$, and x has degree 0 otherwise.

The vertex corresponding to the external region of G has degree equal to the number of 12-edges on the side of T with corners labeled 1 and 2 (where a 12-edge is an edge whose endpoints are labeled 1 and 2). It is easy to that this number is odd. Since the number of vertices of odd degree in a graph is even, the number of triangles in $\mathcal{T}$ having corners with three distinct labels is odd. □

Sperner's Lemma can be generalised to higher dimensions using an induction proof. Indeed, we used the 1-dimensional version in our above proof of the 2-dimensional case. An interesting application of Sperner's Lemma is in proving the **Brouwer Fixed-Point Theorem** which states that any continuous function f from the closed n-dimensional unit ball to itself has a fixed point (an x such that $f(x) = x$). We now outline the proof in the 2-dimensional case.

It is sufficient to prove that any countinuous function f from a triangle T to itself has a fixed point (because a triangle is homeomorphic to the unit disc). For a contradiction suppose f has no fixed points. Let v_1, v_2 and v_3 be vectors for the corners of T, and express each point $a \in T$ as a triple (a_1, a_2, a_3) where a_1, a_2 and a_3 are given by $a = a_1v_1 + a_2v_2 + a_3v_3$, $a_1 + a_2 + a_3 = 1$ and $a_1, a_2, a_3 \geq 0$. Note that the expressions for v_1, v_2 and v_3 are $(1, 0, 0)$, $(0, 1, 0)$ and $(0, 0, 1)$ respectively, and that the points on the opposite side of T to v_i have i-th coordinate 0.

For each point $(a_1, a_2, a_3) \in T$ we denote $f((a_1, a_2, a_3))$ by (a'_1, a'_2, a'_3), and we assign a label from $\{1, 2, 3\}$ to each point as follows.

- (a_1, a_2, a_3) gets label 1 if $a_1 > a'_1$;
- (a_1, a_2, a_3) gets label 2 if $a_1 \leq a'_1$ and $a_2 > a'_2$;
- (a_1, a_2, a_3) gets label 3 if $a_1 \leq a'_1$, $a_2 \leq a'_2$, and $a_3 > a'_3$.

If a point remains unlabeled, then we have $a_1 \leq a'_1$, $a_2 \leq a'_2$ and $a_3 \leq a'_3$, which implies $a_1 = a'_1$, $a_2 = a'_2$ and $a_3 = a'_3$ (because $a_1 + a_2 + a_3 = a'_1 + a'_2 + a'_3 = 1$). But this means we have a fixed point and we conclude that every point of T is labeled.

Notice that v_i gets label i, and that the points on the opposite side of T to v_i do not get label i. Thus, our labeling induces a Sperner labeling of any triangulation of T, and Sperner's Lemma guarantees that in any such triangulation, there is a triangle whose corners are assigned three distinct labels. Call such triangles **rainbow triangles**. By taking a sequence of triangulations with increasingly smaller diameter (the diameter of a triangle is the length of its longest side, and the diameter of a triangulation is the maximum diameter of its triangles), we can generate a sequence of increasingly smaller rainbow triangles.

Using the **Bolzano-Weierstauss Theorem** (every bounded sequence in $\mathbb{R}^n$ has a convergent subsequence), we obtain a convergent sequence of points with label 1 which are contained in rainbow triangles. The sequence of points labeled 2 in these rainbow triangles also has a convergent subsequence, which yields a sequence of rainbow triangles in which the sequence of points labeled 1 converges and the sequence of points labeled 2 converges. By the same process, we obtain a sequence of rainbow triangles in which the sequence of points labeled i converges for each $i \in \{1, 2, 3\}$. Moreover, these rainbow triangles have diameter approaching zero. It follows that the limits of the three sequences are the same. Let this limit point be (A_1, A_2, A_3), and let $(A'_1, A'_2, A'_3) = f((A_1, A_2, A_3))$.

Now, for each $i \in \{1, 2, 3\}$ the ith coordinate a_i of each point in the sequence of points labeled i satisfies $a_i > a'_i$, and so it follows from the continuity of f that $A_i \geq A'_i$. Since $A_1 + A_2 + A_3 = A'_1 + A'_2 + A'_3 = 1$, this implies $A_i = A'_i$ for $i \in \{1, 2, 3\}$. Thus, (A_1, A_2, A_3) is a fixed point and we have the required contradiction.

2.3 Regular Polytopes

The term **polytope** has been defined in several different ways, only some of them equivalent. For our purposes, the following definition suffices. An **n-dimensional polytope**, or just **n-polytope** is a finite region of $\mathbb{R}^n$ that is enclosed by a finite number of hyperplanes (here, hyperplane means any translation of an $(n-1)$-dimensional subspace of $\mathbb{R}^n$).

A convenient way to think about polytopes is as the generalisation to higher dimensions of the well-known 2-polytopes and 3-polytopes – the polygons and polyhedra. We are only going to be interested in polytopes that are **convex** (the straight line joining any two points of the polytope is contained within the polytope) and **regular**. There are also several different definitions of what it means for a polytope to be **regular**, we will return to this shortly.

Polygons is the usual name for 2-polytopes, and there is a unique (up to scaling, rotation, and translation) convex regular polygon with n vertices for each $n \geq 3$, the **regular n-gon**. In a regular polygon, the sides all have the same length, and the angles at the vertices are equal. Moreover, the symmetry (automorphism) group of the polygon acts transitively on the **flags** of the polygon. A flag of a polygon consists of an edge e and a vertex v of e. The symmetry group of the regular n-gon is the dihedral group D_n.

Polyhedra is the usual name for 3-polytopes. A polyhedron is bounded by polygons, which are called the **faces** of the poyhedron. A flag of polyhedron consists of a face f (which is a polygon), an edge e of f, and a vertex v of e. A polyhedron is **regular** if its symmetry group acts transitively on its flags. The convex regular 3-polytopes are precisely the **Platonic solids** – the **tetrahedron**, **cube**, **octahedron**, **icosahedron**, and **dodecahedron**.

Theorem 2.3.1. A polyhedron satisfies Euler's formula

$$v - e + f = 2$$

where v is the number of vertices, e is the number of edges, and f is the number of faces.

The **dual** of an polyhedron is obtained by placing a vertex at the centre of each face, and joining two such vertices by an edge precisely when the corresponding faces share an edge. The octahedron is the dual of the cube, the dodecahedron is the dual of the icosahedron, and the tetrahedron is self-dual (the dual of itself). The dual of a polyhedron has the same symmetry group.

The (full) symmetry group of a polyhedron includes both rotations and reflections. The group of rotations is a subgroup of the full symmetry group, which includes the reflections. The table below lists the rotational and full symmetry groups, and their orders in parentheses, for each the five Platonic solids.

Solid	Group of rotations	Full symmetry group
Tetrahedron	A_4 (12)	S_4 (24)
Cube	S_4 (24)	$S_4 \times \mathbb{Z}_2$ (48)
Octahedron	S_4 (24)	$S_4 \times \mathbb{Z}_2$ (48)
Icosahedron	A_5 (60)	$A_5 \times \mathbb{Z}_2$ (120)
Dodecahedron	A_5 (60)	$A_5 \times \mathbb{Z}_2$ (120)

For $n \geq 4$ (and also for $n = 2$ and $n = 3$), an n-polytope is bounded by $(n-1)$-polytopes, and these are the **$(n-1)$-faces** of the n-polytope. Each of the n-polytope's $(n-1)$-faces is bounded by $(n-2)$-polytopes, and these are the **$(n-2)$-faces** of the n-polytope. The pattern continues on down until we have the 2-faces (which are polygons) bounded by the 1-faces (which are the edges of the n-polytope), and finally the 1-faces (edges) bounded by the 0-faces (which are the vertices of the n-polytope). A **flag** of an n-polytope is a sequence $F_n, F_{n-1}, \ldots, F_1, F_0$ where F_n is the n-polytope itself, and F_i is an i-face of F_{i+1} for $i = 0, 1, \ldots, n-1$.

An n-polytope is **regular** if its symmetry group acts transitively on its flags. There are six convex regular 4-polytopes, each of these is called an n-cell, where the "n" refers to the number of 3-faces. For example, the 8-cell has 8 3-faces, each of which is a (3-dimensional) cube.

1. **5-cell**

   The 5-cell is the 4-dimensional analogue of the tetrahedron. It has 5 vertices, 10 edges, 10 faces (2-faces) each of which is a regular 3-gon (equilateral triangle), and 5 tetrahedral 3-faces.

2. **16-cell**

   The 16-cell is the 4-dimensional analogue of the octahedron. It has 8 vertices, 24 edges, 32 triangular faces, and 16 tetrahedral 3-faces.

3. **8-cell**

   The 8-cell is the 4-dimensional analogue of the cube. It has 16 vertices, 32 edges, 24 square faces, and 8 cubic 3-faces.

4. **24-cell**

   The 24-cell has no direct 3-dimensional analogue. It has 24 vertices, 96 edges, 96 triangular faces, and 24 octahedral 3-faces.

5. **600-cell**

   The 600-cell is the 4-dimensional analogue of the icosahedron. It has 120 vertices, 720 edges, 1200 triangular faces, and 600 tetrahedral 3-faces.

6. **120-cell**

   The 120-cell is the 4-dimensional analogue of the dodecahedron. It has 600 vertices, 1200 edges, 720 pentagonal faces, and 120 dodecahedral 3-faces.

Theorem 2.3.2. A 4-polytope has Euler characteristic 0 and so satisfies

$$v - e + f - c = 0$$

where v is the number of vertices, e is the number of edges, and f is the number of faces, and c is the number of 3-faces.

The **dual** of an n-polytope is obtained by placing a vertex at the centre of each $(n-1)$-face, and joining two such vertices by an edge precisely when the corresponding $(n-1)$-faces share an edge. Taking the dual of an n-polytope interchanges i-faces with $(n-1-i)$-faces. The 5-cell and the 24-cell are self-dual, the 16-cell and the 8-cell are duals, and the 600-cell and the 120-cell are duals.

2.4 Sphere Packing

A **sphere packing** is an arrangement of spheres in some space such that the spheres do not overlap. A classical problem is to find the densest possible packing of non-overlapping equal-sized spheres in 3-dimensional Euclidean space. In a densest possible packing, the fraction of space filled by the spheres is $\frac{\pi}{\sqrt{18}}$, which is about 0.74. It has been known since ancient times how to pack spheres to achieve this density, but it was not proved to be the maximum until relatively recently. The proof was announced in 1998, but formal checking of the proof was not completed until 2014 [29].

There are several distinct ways of achieving a densest possible packing. Start by constructing a plane layer of spheres in which each sphere touches six other spheres – the sphere centres are positioned at the points of a regular triangular lattice. It is then possible to add another such layer of spheres on top (and below) but translated so that the spheres of the second layer fall into "holes" of the first layer. Only half the holes receive a sphere, and the second layer could instead be translated so that its spheres fall into the other half of the holes of the first layer. A maximum density packing is achieved by repeatedly adding layers in this manner.

In adding a third layer, which is to be the same as each of the first two layers, there are again two choices of holes in the second layer into which the spheres of the third layer can be placed. However, a distinction arises in the postitioning of the spheres of the third layer relative to the spheres of the first layer. The spheres of the third layer can be positioned either directly above the spheres of the first layer, or directly above the holes of the first layer that are not occupied by the spheres of the second layer. As more layers are added, more choices of this kind are available, and a multitude of distinct packings that achieve the maximum density arise.

The sphere packing problem can be generalised to other dimensions. In two dimensions, the optimal packing is a hexagonal arrangement where the centres of the spheres (circles) are on the points of a triangular/hexagonal lattice. The fraction of $\mathbb{R}^2$ covered by the circles is $\frac{\pi\sqrt{3}}{6}$, which is just over 90%.

The sphere packing problem can be generalised in many ways, including to higher dimensions, with spheres of differing sizes, and to non-Euclidean spaces. In $\mathbb{R}^n$ with $n \geq 4$, the optimal sphere packing density is known only for $n = 8$ and $n = 24$, where the spheres are centred on the points of **E_8 lattice** and the **Leech lattice** respectively. It was only in 2017, that these packings were proved to be optimal [57, 15]. The Ukrainian mathematician Maryna Viazovska was awarded the Fields Medal in 2022, predominantly for her work on sphere packings.

The E_8 lattice can be constructed from a Steiner system $S(3, 4, 8)$. The unique (up to isomorphism) $S(3, 4, 8)$ is given by

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

The following properties of the $S(3, 4, 8)$ are relavant.

(a) The complement of each block is a block.

(b) Any two blocks intersect in 0 or 2 points.

(c) The symmetric difference of any two distinct blocks is $\{1, 2 \ldots, 8\}$ or is a block.

These properties follow from the fact that if the point 8 is removed from the 7 blocks on the left, then the result is an $S(2, 3, 7)$ system, and the 7 blocks on the right form a 2-$(7, 4, 2)$-design.

For each block B_j, $j = 1, 2, \ldots, 14$, of the $S(3, 4, 8)$, let v_j be the vector of $\mathbb{Z}^8$ having a 1 in coordinate i if $i \in B_j$, and having a 0 in coordinate i if $i \notin B_j$. Thus, $\{v_j : j = 1, 2, \ldots, 14\}$ is a set of 14 vectors in $\mathbb{Z}^8$, each having four coordinates that are 1 and four coordinates that are 0. These 14 vectors together with $(0, 0, \ldots, 0)$ and $(1, 1, \ldots, 1)$ form a 4-dimensional vector subspace V of $\mathbb{Z}_2^8$. This is the $(8, 4, 4)$ **extended Hamming code**. Closure, and the fact that any two distinct vectors of V differ in at least four coordinates, follows from property (c) mentioned above.

The E_8 lattice is

$$\{x \in \mathbb{Z}^8 : x \equiv v \pmod 2, v \in V\}$$

where $x \equiv v \pmod 2$ means that if $x = (x_1, \ldots, x_8)$ and $v = (v_1, \ldots, v_8)$, then $x_i \equiv v_i \pmod 2$ for $i = 1, \ldots, 8$. Notice that if $x, y \in E_8$, then $x + y \in E_8$, and from this it follows that E_8 is a subgroup of $\mathbb{Z}^8$.

It can be seen that the minimum distance between distinct points of E_8 is 2. If points x and y are at distance d, then the points $x - y$ and 0 are also at distance d. So the minimum distance between distinct points of the lattice is equal to the minimum distance of a non-zero point from $(0, 0, \ldots, 0)$. This minimum is distance is 2, and is attained by points that have exactly four non-zero coordinates each equal to ± 1, and by points that have exactly one non-zero coordinate equal to ± 2.

The number of points at distance 2 from any given point is equal to the number of points at distance 2 from $(0, 0, \ldots, 0)$. This number is $14 \cdot 16 + 2 \cdot 8 = 240$ (there are 14 blocks in $S(3, 4, 8)$ and for each block there are $2^4 = 16$ ways of assigning ± 1 to the coordinates corresponding to the four points of the block, and there are $2 * 8 = 16$ vectors having one non-zero coordinate equal to ± 2).

The E_8 lattice is often defined as

$$E_8 = \{(x_1, x_2, \ldots, x_8) \in \mathbb{Z}^8 \cup (\mathbb{Z} + \tfrac{1}{2})^8 : x_1 + x_2 + \cdots + x_8 \equiv 0 \pmod 2\},$$

which has minimum distance of $\sqrt{2}$ between distinct points. This is attained, for example, by $(0, 0, 0, 0, 0, 0, 0, 0)$ and $(1, 1, 0, 0, 0, 0, 0, 0)$ and also by $(0, 0, 0, 0, 0, 0, 0, 0)$ and $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$. If we scale the lattice we constructed from $S(3, 4, 8)$ by a factor of $\frac{1}{\sqrt{2}}$, then we obtain this lattice, but the isomorphism is not obvious.

The Leech lattice can be constructed from the blocks of the Steiner system $S(5, 8, 24)$ as follows, see [17]. Let $\{1, 2, \ldots, 24\}$ be the point set of an $S(5, 8, 24)$ and let $\mathcal{B}$ be the set of blocks. For each block $B \in \mathcal{B}$ define v_B to be the vector in $\mathbb{Z}^{24}$ that has a 2 in coordinate i if $i \in B$, and a 0 in coordinate i if $i \notin B$. Let $w \in \mathbb{Z}^{24}$ be the vector $(1, 1, \ldots, 1, -3)$. Then the integer linear combinations of the vectors v_B, $B \in \mathcal{B}$, and w give us the points of the Leech lattice. Notice that $||w|| = \sqrt{32}$ and for each $B \in \mathcal{B}$ we have $||v_B|| = \sqrt{32}$. Also,

$$\min\{||v_B - w|| : B \in \mathcal{B}\} = \min\{||v_B - v_{B'}|| : B, B' \in \mathcal{B}\} = \sqrt{32}.$$

In the densest possible sphere packings in $\mathbb{R}^3$, described above, each sphere touches 12 other spheres – six in its own layer, three from the layer above, and three from the layer below. It turns out that, with all spheres the same size, this is the maximum number of non-overlapping spheres that touch a given sphere. It has been known for centuries that 12 spheres are possible, but a proof that no more than 12 is possible did not come until 1953 [48].

Generalising the problem described in the preceding paragraph to Euclidean space of any dimension, we have the following question, which is known as the **kissing number problem**.

In $\mathbb{R}^n$, how many non-overlapping unit spheres can touch a given unit sphere?

The question is trivial in $\mathbb{R}$, and the answer is easily seen to be 6 in $\mathbb{R}^2$. In fact, there is essentially only one way to arrange six non-overlapping unit circles so that they all touch a given unit circle – each of the outer circles touches its two neighbouring outer circles (as well as the inner circle). We have mentioned above that the answer is 12 in $\mathbb{R}^3$, and in that case the outer spheres can be arranged so that none of them touch each other. One way of arranging the 12 outer spheres is at the vertices of a regular icosahedron, with the given sphere at the centre of the icosahedron.

The situation in R^4 is similar to that of $\mathbb{R}^3$. In $\mathbb{R}^4$, it is possible to arrange 24 spheres at the vertices of the 24-cell (see Section 2.3), with the inner sphere at the centre of the 24-cell. Again, there is enough space that none of the outer spheres touch each other. The fact that 24 is the maximum number of spheres in $\mathbb{R}^4$ was proved in 2003 [44].

For $n > 4$, the maximum number of non-overlapping unit spheres that touch a given unit sphere in $\mathbb{R}^n$ is unknown, except that in $\mathbb{R}^8$ the maximum is 240, and in $\mathbb{R}^{24}$ the maximum is $196,560$. These solutions relate to the E_8 lattice and the Leech lattice. In each case the spheres are placed at all the lattice points of minimum distance from a given lattice point. Thus, in 3, 8 and 24 dimensions, the solutions to the kissing number problem occur in the solutions to the sphere packing problem, and are obtained by arranging the spheres at the points of special lattices which are highly symmetrical.

2.5 Projective and Affine Planes

Definition 2.5.1. An **incidence structure** is a triple (P, L, I) where P and L are disjoint sets and $I \subseteq P \times L$. The elements of P are called **points**, the elements of L are called **lines**, and I is called the **incidence relation**. The elements of I are called **flags** or **incidences**. If $(p, \ell) \in I$, then we say that p is **incident** with ℓ and ℓ is **incident** with p. We may also say that the point p lies on the line ℓ and that the line ℓ passes through point p.

It is often more convenient to think of an incident structure (P, L, I) as a set P of points together with a collection L of lines, or a pair (P, L), where each line $\ell \in L$ is a set consisting of the points that are incident (under I) with ℓ. That is, we think of the line ℓ as the set $\ell = \{p \in P : (p, \ell) \in I\}$.

Definition 2.5.2. A **projective plane** is an incidence structure satisfying the following three axioms.

(P1) For any two distinct points x and y, there is a unique line incident with both x and y.

(P2) For any two distinct lines P and Q, there is a unique point incident with both P and Q.

(P3) There exist four points, no three of which are collinear.

□

Example 2.5.3. The Euclidean plane $\mathbb{R}^2$ is not a projective plane because it has parallel lines, and so does not satisfy axiom P2. However a projective plane $\mathcal{P}$ can be constructed from $\mathbb{R}^2$ as follows.

- Each point of $\mathbb{R}^2$ is a point in $\mathcal{P}$.
- For each $m \in \mathbb{R} \cup \{\infty\}$, there is a point ∞_m in $\mathcal{P}$ (these are the "points at infinity").
- For each $m \in \mathbb{R} \cup \{\infty\}$ and for each line L of gradient m in $\mathbb{R}^2$, the points of $L \cup \{\infty_m\}$ form a line of $\mathcal{P}$ (the parallel lines of gradient m "meet at infinity", namely at the point ∞_m).
- The line $\{\infty_m : m \in \mathbb{R} \cup \{\infty\}\}$ is in $\mathcal{P}$ (this is the "the line at infinity").

It is easy to verify that $\mathcal{P}$ is a projective plane – the **real projective plane**.

The real projective plane can also be constructed as follows. Let V be the vector space of dimension 3 over $\mathbb{R}$. The 1-dimensional subspaces of V are the points of $\mathcal{P}$, and the 2-dimensional subspaces of V are the lines $\mathcal{P}$. By this, we mean that for each 2-dimensional subspace U of V, there is a line in $\mathcal{P}$ whose points are the 1-dimensional subspaces of U. □

We now turn our attention to finite projective planes.

Example 2.5.4. Let $P = \mathbb{Z}_2^3 \setminus \{0\}$ and let $L = \{x, y, z \in P : x + y + z = 0\}$. Then (P, L) is a projective plane, called the **Fano plane**.

Theorem 2.5.5. If $\mathcal{P}$ is a finite projective plane, then there is a constant $n \geq 2$ such that there are exactly $n + 1$ points on each line of $\mathcal{P}$, there are exactly $n + 1$ lines through each point of $\mathcal{P}$, the number of points in $\mathcal{P}$ is $n^2 + n + 1$, and the number of lines in $\mathcal{P}$ is $n^2 + n + 1$.

Proof First observe that if k is the number of lines through a point x, then the number of points on any line P that is not incident with x is also k (because any line through x intersects P in a unique point, distinct lines through x intersect P in distinct points, and there is a line through x and any point on P). Now let w, x, y and z be four distinct points with no three collinear, let P be the line through x and y, let Q be the line through x and z, and let R be the line through y and z. Note that P, Q and R are distinct and that w is on none of them.

Let k be the number of lines through w, and note that $k \geq 3$ because wx, wy and wz are distinct lines. By the observation made at the beginning of the proof, every line not through w has k points on it. This includes the lines P, Q and R. Since no point is on all of three of P, Q and R, it follows from the same observation that every point has k lines through it. Then from this it follows that every line has k points on it. Let $n = k - 1$. So $n \geq 2$. By considering the $n + 1$ lines through a point, we see that there are $(n + 1)n + 1 = n^2 + n + 1$ points in $\mathcal{P}$. If we sum over all points, the number of lines through each point, then we count each line $n + 1$ times. It follows that the number of lines in $\mathcal{P}$ is $(n^2 + n + 1)(n + 1)/(n + 1) = n^2 + n + 1$. □

The parameter n in Theorem 2.5.5 is called the **order** of the projective plane $\mathcal{P}$.

Definition 2.5.6. An **affine plane** is an incidence structure satisfying the following three axioms.

(A1) For any two distinct points x and y, there is a unique line incident with both x and y.

(A2) For any line P and any point x that is not on P, there is a unique line that is incident with x and incident with no point of P.

(A3) There exist four points, no three of which are collinear.

□

Example 2.5.7. The points and lines of $\mathbb{R}^2$ form an affine plane.

Theorem 2.5.8. If $\mathcal{A}$ is a finite affine plane, then there is a constant $n \geq 2$ such that there are exactly n points on each line of $\mathcal{A}$, there are exactly $n+1$ lines through each point of $\mathcal{A}$, the number of points in $\mathcal{A}$ is n^2, and the number of lines in $\mathcal{A}$ is $n^2 + n$.

Proof Let $\mathcal{A}$ be a finite affine plane. By Axiom A3, $\mathcal{A}$ has at least two distinct lines. Suppose first that all the points of $\mathcal{A}$ lie on two lines P and Q. We aim to show that in this case $\mathcal{A}$ satisfies the stated conditions with $n = 2$ (it will have four points and six lines, with each pair of distinct points being a line). By Axiom A3, there exist four points a, b, c and d, no three of which are collinear. This means that ab, ac, ad, bc, bd and cd are six distinct lines. Moreover, exactly two of a, b, c and d are on P and exactly two are on Q. Without loss of generality we can assume that P is the line ab and Q is the line cd.

Now, none of the lines ac, ad, bc nor bd has any other points, because any other point is on P or Q and this contradicts Axiom A1. Also, none of a, b, c nor d is a line (with one point) because this contradicts Axiom A2. We can now conclude that P is parallel to Q because otherwise there can be no line through a that is parallel to Q. If there is a point x on P which is neither a nor b, then c is not on xd, and so ac and bc are distinct lines through c that are parallel to xd. This contradicts Axiom A2 and we conclude that a and b are the only points on P. Similarly, we conclude that c and d are the only points on Q. Thus, $\mathcal{A}$ satisfies the stated conditions with $n = 2$.

We can now assume that no two lines of $\mathcal{A}$ contain all the points. Let P and Q be distinct lines, let x be a point which is on neither P nor Q, and let n be the number of points on P. The n points of P define n distinct lines through x (by Axiom A1). By Axiom A3, there is exactly one more line through x, and it is parallel to P.

Of the $n+1$ lines through x, exactly one is parallel to Q (by Axiom A2), and so the remaining n meet Q in n distinct points. These are all the points on Q (because each point on Q is also on a line through x). Since P and Q were chosen arbitrarily, we conclude that there are n points on each line. By considering an arbitrary point y, and a line R not through y, we see that there are $n+1$ lines through each point (each of the n points on R defines a line through y and there is exactly one line through y which is parallel to R). By considering the $n+1$ lines through a point, we see that there are $(n+1)(n-1)+1 = n^2$ points in $\mathcal{A}$. If we sum over all points, the number of lines through each point, then we count each line n times. It follows that the number of lines in $\mathcal{A}$ is $n^2(n+1)/n = n^2 + n$. □

The parameter n in Theorem 2.5.8 is called the **order** of the affine plane $\mathcal{A}$.

Theorem 2.5.9. The lines of an affine plane of order n can be partitioned into $n+1$ parallel classes, where each parallel class consists of a set of n pairwise parallel lines which collectively contain all the points.

Proof Let P be a line and suppose there are distinct lines Q and Q' which are both parallel to P. By Axiom A2, Q and Q' must be parallel to each other. Now, since there are n points on P and $n+1$ lines through each point of P, there are n^2+1 lines, including P itself, which intersect P. This leaves $n-1$ lines which are parallel to P, and we have already noted that these are pairwise parallel. The result follows. $\square$

Theorem 2.5.10. There exists a projective plane of order n if and only if there exists an affine plane of order n.

Proof An affine plane of order n can be obtained by from a projective plane of order n by deleting a line and deleting the points of that line from each of the remaining lines. Conversely, suppose that there exists an affine plane $(V, \mathcal{B})$ of order n. Let $\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_{n+1}$ be the $n+1$ resolution classes of $(V, \mathcal{B})$, which exists by Theorem 2.5.9. Let V' be the point set obtained by adding $n+1$ new points $x_1, x_2, \ldots, x_{n+1}$ to V. For $i = 1, 2, \ldots, n+1$, add the new point x_i to each line in R_i, and add a new line $\{x_1, x_2, \ldots, x_{n+1}\}$. It is routine to check that a projective plane of order n results. $\square$

The construction given in the proof of Theorem 2.5.10 is equivalent to the construction of the real projective plane from the affine plane $\mathbb{R}^2$, which was given in Example 2.5.3.

In Section 2.6 we will see that a projective plane of order q can be constructed from a finite field of order q. Thus, a projective plane of order q exists whenever q is a power of prime.

Theorem 2.5.11. If q is a power of a prime, then there exist projective and affine planes of order q.

All known finite projective planes have order a power of a prime, and although existence has been ruled out for infinitely many non-prime power orders, it also remains unresolved for infinitely many. The **Bruck-Ryser-Chowla Theorem** is an important theorem in design theory that rules out the existence of certain designs. It has the following consequence for the existence of projective planes (see [55]).

Theorem 2.5.12. If there exists a projective plane of order n with $n \equiv 1, 2 \pmod 4$ then for each prime $p \equiv 3 \pmod 4$ the largest α for which p^α divides n is even.

The smallest few values of n for which Theorem 2.5.12 rules out the existence of a projective plane of order n are $n = 6, 14, 21, 22$ and 30. We know that there exist projective planes for all prime power orders, so for every $n < 10$ the existence of a projective plane of order n is settled either by n being a prime power or by Theorem 2.5.12. The smallest unresolved case, the existence of a projective plane of order 10, was ruled out by Lam et al [41] in 1989, but the existence question remains open for infinitely many orders. The five smallest of these are $n = 12, 15, 18, 20$ and 24.

Some design theorists and geometers believe that finite projective planes of order n exist only when n is a prime power. Until the proof of the non-existence of a projective plane of order 10, some believed that they existed for all values of n not ruled out by the Bruck-Ryser-Chowla Theorem. Deciding whether or not projective planes of non-prime power order exist is probably the one of the most important open questions in finite geometry and design theory.

Although no projective planes of non-prime power order are known, projective planes of prime power order which are not isomorphic to those constructed from finite fields have been constructed. The projective planes arising from finite fields are known as **desarguesian** planes because they are the only ones in which **Desargues' Theorem** holds. Any other projective plane is known as a **nondesarguesian** plane.

In a projective plane, let x be a point and let $\{a_1, a_2, a_3\}$ and $\{b_1, b_2, b_3\}$ be two disjoint triangles (a triangle is a set of three non-collinear points) such that x, a_i, and b_i are collinear for $i = 1, 2, 3$. Also, let y_{12} be the point of intersection of the lines a_1a_2 and b_1b_2, let y_{13} be the point of intersection of the lines a_1a_3 and b_1b_3, and let y_{23} be the point of intersection of the lines a_2a_3 and b_2b_3. Desargues' Theorem states that the points y_{12}, y_{13} and y_{23} are collinear.

For $n \in \{2, 3, 4, 5, 7, 8\}$, the only projective plane of order n is the desarguesian plane arising from the finite field of order q. For infinitely many values of n given by the Bruck-Ryser-Chowla Theorem ($n = 6, 14, 21, 22, 30, \ldots$), there is no projective plane of order n, and there is no projective plane of order 10. There are exactly four non-isomorphic projective planes of order 9. For all other values of n, the number of non-isomorphic projective planes of order n is unknown. It is known that there are at least 22 non-isomorphic projective planes of order 16. The only known projective planes of prime order are desarguesian.

2.6 Projective and Affine Geometries $\mathrm{PG}(n, q)$ and $\mathrm{AG}(n, q)$

Projective and affine planes, and other incidence structures and designs, can be constructed from vector spaces over finite fields. In order to understand these methods, it is useful to be familiar with the *Gaussian binomial coefficients*, which are *q-analogues* of the ordinary binomial coefficients.

Definition 2.6.1. The **q-number** $[k]_q$ is defined by

$$[k]_q = \frac{1 - q^k}{1 - q} = 1 + q + q^2 + \cdots + q^{k-1},$$

the **q-factorial** $[k]_q!$ is defined by

$$[k]_q! = [k]_q[k-1]_q \cdots [1]_q,$$

and the Gaussian binomial coefficient $\binom{n}{r}_q$ is defined by

$$\binom{n}{r}_q = \frac{[n]_q!}{[r]_q![n-r]_q!} = \frac{[n]_q[n-1]_q \cdots [n-r+1]_q}{[r]_q[r-1]_q \cdots [1]_q} = \frac{(1-q^n)(1-q^{n-1}) \cdots (1-q^{n-r+1})}{(1-q^r)(1-q^{r-1}) \cdots (1-q)}$$

for $r \leq n$ and $\binom{n}{r}_q = 0$ for $r > n$. $\square$

Note the similarities between the Gaussian binomial coefficient $\binom{n}{r}_q$ and the ordinary binomial coefficient $\binom{n}{r}$. For example, it is easy to see that $\binom{n}{r}_q = \binom{n}{n-r}_q$.

Theorem 2.6.2. The number of r-dimensional subspaces of an n-dimensional vector space over a field of order q is given by the Gaussian binomial coefficient $\binom{n}{r}_q$.

Proof The number of ordered r-tuples of linearly independent vectors of an n-dimensional vector space over a field of order q is

$$(q^n-1)(q^n-q)\cdots(q^n-q^{r-1}).$$

To see this observe that there are q^n-1 ways of selecting the first vector (any vector other than the zero vector), and then q^n-q ways of selecting the second vector (any vector other than the q scalar multiples of the first vector), and then q^n-q^2 ways of selecting the third vector (any vector not in the 2-dimensional subspace generated by the first two vectors), and so on.

Since each r-tuple of linearly independent vectors generates an r-dimensional subspace, the number of r-dimensional subspaces is given by dividing $(q^n-1)(q^n-q)\cdots(q^n-q^{r-1})$ by the number of ordered r-tuples of linearly independent vectors in an r-dimensional subspace. Using the formula we derived above, this number is $(q^r-1)(q^r-q)\cdots(q^r-q^{r-1})$. Thus, the number of r-dimensional subspaces of an n-dimensional vector space over a field of order q is given by

$$\begin{aligned}\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{r-1})}{(q^r-1)(q^r-q)\cdots(q^r-q^{r-1})} &= \frac{(q^n-1)q(q^{n-1}-1)\cdots q^{r-1}(q^{n-r+1}-1)}{(q^r-1)q(q^{r-1}-1)\cdots q^{r-1}(q-1)}\\ &= \frac{(1-q^n)(1-q^{n-1})\cdots(1-q^{n-r+1})}{(1-q^r)(1-q^{r-1})\cdots(1-q)}\\ &= \binom{n}{r}_q.\end{aligned}$$

□

Definition 2.6.3. Let V be a vector space. The (additive) cosets in V of a d-dimensional subspace of V are called ***d*-flats**. The set of all d-flats, $0 \le d \le n-1$, of an n-dimensional vector space over a field of order q form the ***n*-dimensional affine geometry over $\mathbb{F}_q$**, which is denoted by AG(n,q). The 0-flats (vectors) are the **points** of AG(n,q), the 1-flats are the **lines**, and so on. The $(n-1)$-flats are the **hyperplanes** of AG(n,q). □

Theorem 2.6.4. Let q be a prime power, let $n \ge 2$, and let $1 \le d < n$. Each pair of distinct points of AG(n,q) occurs together in exactly $\binom{n-1}{d-1}_q$ d-flats.

Proof Let V be an n-dimensional vector space over $\mathbb{F}_q$ and let x and y be distinct vectors in V. So x and y are distinct points of AG(n,q). The number of d-flats containing both x and y is equal to the number of d-dimensional subspaces of V that contain the vector $z = x - y$. Let U be an

$(n-1)$-dimensional subspace of V such that $z \notin U$. The d-dimensional subspaces of V containing z are exactly the subspaces spanned by $W \cup \{z\}$ where W is a $(d-1)$-dimensional subspace of U. Since the number of such W is $\binom{n-1}{d-1}_q$, each pair of points occurs in exactly $\binom{n-1}{d-1}_q$ d-flats. □

Corollary 2.6.5. The points and lines of $\mathrm{AG}(2,q)$ form an affine plane of order q.

Proof We check the axioms for an affine plane. Putting $n = 2$ and $d = 1$ in Theorem 2.6.4 we see that there is exactly $\binom{1}{0}_q = 1$ line through each pair of distinct points. There are q^2 points and there are q points on each line. Thus, there are $(q^2-1)/(q-1) = q+1$ lines through each point, and there are $\binom{q^2}{2}/\binom{q}{2} = q(q+1)$ lines. The number of lines intersecting a given line is q^2+1 (including the line itself), which leaves $q(q+1) - (q^2+1) = q-1$ lines that are parallel to any given line.

If U is a 1-dimensional subspace of the underlying vector space V, then the cosets of U partition V. Thus, each line is contained in a parallel class of lines that partitions the points. Since we have seen that there are $q-1$ lines parallel to any given line, this means that the lines parallel to a given line are parallel to each other. Thus, for any given line and any given point not on the line, there is a unique line through the point and parallel to the given line.

Finally, no three of the four points $(0,0)$, $(1,0)$, $(0,1)$ and $(1,1)$ are collinear. □

Example 2.6.6. The 1-flats in $\mathrm{AG}(2,3)$, listed below, form an affine plane of order 3.

$$\begin{array}{cccc}
\{(0,0),(0,1),(0,2)\} & \{(0,0),(1,0),(2,0)\} & \{(0,0),(1,1),(2,2)\} & \{(0,0),(1,2),(2,1)\} \\
\{(1,0),(1,1),(1,2)\} & \{(0,1),(1,1),(2,1)\} & \{(0,1),(1,2),(2,0)\} & \{(0,1),(1,0),(2,2)\} \\
\{(2,0),(2,1),(2,2)\} & \{(0,2),(1,2),(2,2)\} & \{(0,2),(1,0),(2,1)\} & \{(0,2),(1,1),(2,0)\}
\end{array}$$

□

Definition 2.6.7. Let $n \geq 2$, let q be a prime power, and let V be the $(n+1)$-dimensional vector space over $\mathbb{F}_q$. The **projection** of any subspace U of V is defined to be $\{\langle x \rangle : x \in U\}$, where $\langle x \rangle$ denotes the 1-dimensional subspace of V generated by the vector x. The **projective geometry of dimension n over the field $\mathbb{F}_q$**, denoted $\mathrm{PG}(n,q)$, is the projection of V, and consists of the projections of all subspaces of V. The projections of the $(d+1)$-dimensional subspaces of V are the **d-dimensional subspaces** of $\mathrm{PG}(n,q)$. Thus, the projections of the 1-dimensional, 2-dimensional, and n-dimensional subspaces of V are the **points**, **lines** and **hyperplanes** respectively of $\mathrm{PG}(n,q)$.

Theorem 2.6.8. Let $n \geq 2$ and let q be a prime power. Each pair of distinct points of $\mathrm{PG}(n,q)$ occurs together in exactly $\binom{n-1}{d-1}_q$ d-dimensional subspaces of $\mathrm{PG}(n,q)$.

Proof Let $\mathrm{PG}(n,q)$ be the projection of V. Let x_1 and x_2 be distinct points of $\mathrm{PG}(n,q)$, let X_1 and X_2 be their corresponding 1-dimensional subspaces of V, and let $W = X_1 \oplus X_2$ (the notation $\oplus$ is used for the direct sum; that is, the subspace spanned by two subspaces having trivial intersection). Let W' be an $(n-1)$-dimensional subspace of V such that $W \oplus W' = V$. The $(d+1)$-dimensional subspaces of V containing both X_1 and X_2 are precisely the spaces $W \oplus Y$ where Y is a $(d-1)$-dimensional subspace of W'. Since the number of such Y is $\binom{n-1}{d-1}_q$, there are exactly $\binom{n-1}{d-1}_q$ $(d+1)$-dimensional subspaces of V containing both X_1 and X_2. That is, there are exactly $\binom{n-1}{d-1}_q$ d-dimensional subspaces of $\mathrm{PG}(n,q)$ that contain x_1 and x_2. □

Corollary 2.6.9. The points and lines of $\mathrm{PG}(2,q)$ form a projective plane of order q.

Proof We check the axioms for a projective plane. By Theorem 2.6.8, any two points of $\mathrm{PG}(2,q)$ are in exactly $\binom{1}{0}_q = 1$ line of $\mathrm{PG}(2,q)$. There are $\binom{3}{1}_q = q^2+q+1$ points and $\binom{3}{2}_q = q^2+q+1$ lines in $\mathrm{PG}(2,q)$, and there are $\binom{2}{1}_q = q+1$ points on any given line. Thus, there are $\frac{(q^2+q)}{q} = q+1$ lines through any given point, and so $(q+1)q+1 = q^2+q+1$ lines that intersect any given line (this includes the line itself). Since this is all the lines, any two lines intersect. We have already noted that any two points are in a unique line, so any two lines intersect in a unique point. Finally, no three of the four points $\langle(1,0,0)\rangle$, $\langle(0,1,0)\rangle$, $\langle(0,0,1)\rangle$, and $\langle(1,1,1)\rangle$ are collinear. □

It can be shown that if the construction given in the proof of Theorem 2.5.10 is applied to the affine plane arising from $\mathrm{AG}(2,q)$, then the resulting projective plane is the one arising from $\mathrm{PG}(2,q)$. Conversely, if we start with the projective plane arising from $\mathrm{PG}(2,q)$, delete a line and delete the points of that line from each of the remaining lines, then the resulting affine plane is the affine plane arising from $\mathrm{AG}(2,q)$.

Example 2.6.10. The points and hyperplanes of $\mathrm{PG}(2,3)$ form a projective plane of order 3. Let V be the 3-dimensional vector space over $\mathbb{F}_3$. The points are the 1-dimensional subspaces of V and the lines are the 2-dimensional subspaces of V. We shall use

$$001, 010, 011, 012, 100, 101, 102, 110, 111, 112, 120, 121, 122$$

to denote the 1-dimensional subspaces of V, where xyz denotes the 1-dimensional subspace generated by the vector (x,y,z).

For each 1-dimensional subspace of V, there is a corresponding orthogonal 2-dimensional subspace of V. Moreover, a 1-dimensional subspace $x'y'z'$ is contained in the 2-dimensional subspace that is orthogonal to the 1-dimensional subspace xyz if and only if $xx'+yy'+zz'=0$. Thus, the lines are as listed on the right below, with their corresponding orthogonal 1-dimensional subspaces listed on the left.

001	010, 100, 110, 120
010	001, 100, 101, 102
011	012, 100, 112, 121
012	011, 100, 111, 122
100	001, 010, 011, 012
101	010, 102, 112, 122
102	010, 101, 111, 121
110	001, 120, 121, 122
111	012, 102, 111, 120
112	011, 101, 112, 120
120	001, 110, 111, 112
121	011, 102, 110, 121
122	012, 101, 110, 122

□

2.7 Singer's Theorem

There is a natural correspondence between the non-zero vectors of an $(n+1)$-dimensional vector space V over $\mathbb{F}_q$ and the elements of the multiplicative group $\mathbb{F}^*_{q^{n+1}} = (\mathbb{F}_{q^{n+1}} \setminus \{0\}, \cdot)$; the vector $(a_0, a_1, \ldots, a_n) \in V$ corresponds with the polynomial $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{F}^*_{q^{n+1}}$. Of course, by the polynomial $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ we actually mean the equivalence class $[a_0 + a_1x + a_2x^2 + \cdots + a_nx^n]$ of $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ modulo some irreducible polynomial f of degree $n+1$ over $\mathbb{F}_q$. Moreover, this correspondence induces a correspondence between the points of $\mathrm{PG}(n,q)$ and elements of the factor group $\mathbb{F}^*_{q^{n+1}}/\mathbb{F}^*_q$ where $\mathbb{F}^*_q$ is the unique subgroup of order $q-1$ in $\mathbb{F}^*_{q^{n+1}}$ (consisting of the constant or degree 0 polynomials).

If we choose f to be an irreducible polynomial such that x is a primitive element of $F^*_{q^{n+1}}$ (such a polynomial is called a **primitive polynomial**, and these always exist), then the elements of $\mathbb{F}^*_{q^{n+1}}$ are (the equivalence classes of) $1, x, x^2, \ldots, x^{q^{n+1}-2}$. This means that we can take $1, x, \ldots, x^{q+q^2+\cdots+q^n}$ as (representatives for) the elements of $\mathbb{F}^*_{q^{n+1}}/\mathbb{F}^*_q$, and consider these as the points of $\mathrm{PG}(n,q)$. Singer's Theorem [50] uses the fact that the image of each hyperplane of $\mathrm{PG}(n,q)$ under the mapping $x^i \mapsto x^{i+1}$ is another hyperplane, to prove that the hyperplanes form a single orbit under the action of a cyclic group of order $\frac{q^{n+1}-1}{q-1}$.

Theorem 2.7.1. (**Singer's Theorem**, [50]) In $\mathrm{PG}(n,q)$, the points can be permuted in a single cycle π such that the induced action of $\langle\pi\rangle$ on the hyperplanes is regular.

Example 2.7.2. Construction of a projective plane of order 3 via the action of $\mathbb{Z}_{13}$. We work in $\mathbb{F}_{q^{n+1}}$ with $q=3$ and $n=2$. A primitive polynomial of degree $n+1=3$ over $\mathbb{F}_q = \mathbb{F}_3$ is $p(x) = x^3+2x+1$. Working modulo $p(x)$, we have $x^3 = -2x-1 = x+2$. It will also be convenient for subsequent calculations to note that $2x^3 = 2x+1$.

We now evaluate x^i for $i = 0, 1, 2, \ldots, 25$.

$$\begin{aligned}
x^0 &= 1 & x^{13} &= x^3 + 2x = 2\\
x^1 &= x & x^{14} &= 2x\\
x^2 &= x^2 & x^{15} &= 2x^2\\
x^3 &= x + 2 & x^{16} &= 2x + 1\\
x^4 &= x^2 + 2x & x^{17} &= 2x^2 + x\\
x^5 &= x^3 + 2x^2 = 2x^2 + x + 2 & x^{18} &= x^2 + 2x + 1\\
x^6 &= 2x^3 + x^2 + 2x = x^2 + x + 1 & x^{19} &= 2x^2 + 2x + 2\\
x^7 &= x^3 + x^2 + x = x^2 + 2x + 2 & x^{20} &= 2x^2 + x + 1\\
x^8 &= x^3 + 2x^2 + 2x = 2x^2 + 2 & x^{21} &= x^2 + 1\\
x^9 &= 2x^3 + 2x = x + 1 & x^{22} &= 2x + 2\\
x^{10} &= x^2 + x & x^{23} &= 2x^2 + 2x\\
x^{11} &= x^3 + x^2 = x^2 + x + 2 & x^{24} &= 2x^2 + 2x + 1\\
x^{12} &= x^3 + x^2 + 2x = x^2 + 2 & x^{25} &= 2x^2 + 1
\end{aligned}$$

As expected these are the 26 non-zero elements of $\mathbb{F}_{27}$. Note that $x^{13} = 2$ can be used to make calculations easier. For example, $x^{18} = x^{13} \cdot x^5 = 2(2x^2 + x + 2) = x^2 + 2x + 1$. However, we only need to calculate x^i for $i = 0, 1, \ldots, 12$ anyway.

Recalling the natural correspondence (noted above) between the points of $\mathrm{PG}(n, q)$ and the elements of the factor group $\mathbb{F}^*_{q^{n+1}}/\mathbb{F}^*_q$, we observe that those polynomials in the above list for which the coefficient of x^2 is zero form a line in $\mathrm{PG}(2, 3)$. Thus, since multiplication by x preserves lines, the orbit of $\{0, 1, 3, 9\}$ under $\mathbb{Z}_{13}$ forms a projective plane of order 3. $\square$

There is an affine analogue of Singer's Theorem which is described in a paper of Bose from 1946 [10]. For any non-zero element z of $\mathbb{F}_{q^n}$, define the permutation π_z on the points of $\mathrm{AG}(n, q)$ by $\pi_z(x) = zx$ for each $x \in \mathbb{F}_{q^n}$. Bose's result uses the observation that the image of any d-flat of $\mathrm{AG}(n, q)$ under the mapping π_z is another d-flat. If we take z to be a primitive element (generator of the multiplicative group $\mathbb{F}_{q^n} \setminus \{0\}$), then π_z fixes 0 and permutes the remaining points of $\mathrm{AG}(n, q)$ in a cycle of length $q^n - 1$. It follows from $\gcd(q^n - 1, q^d) = 1$ that the orbit under π_z of any d-flat not containing 0 has length $q^n - 1$ (when z is primitive).

Theorem 2.7.3. ([10]) In $\mathrm{AG}(n, q)$, there is a permuation π of the points such that π fixes 0 and permutes the remaining points in a single cycle, π preserves the d-flats, and the orbit under $\langle \pi \rangle$ of any d-flat not containing 0 has length $q^n - 1$.

Example 2.7.4. Construction of an affine plane of order 5 with an automorphism that fixes one point and permutes the remaining points in a cycle of length 24. We work in $\mathbb{F}_{q^n}$ with $q = 5$ and $n = 2$. A primitive polynomial of degree $n = 2$ over $\mathbb{F}_q = \mathbb{F}_5$ is $p(x) = x^2 + x + 2$. Working modulo $p(x)$, we have $x^2 = 4x + 3$. It will also be convenient for subsequent calculations to note that $2x^2 = 3x + 1$, $3x^2 = 2x + 4$ and $4x^2 = x + 2$.

We now evaluate x^i for $i = 0, 1, 2, \dots, 23$.

$$\begin{array}{lcl@{\qquad}lcl@{\qquad}lcl@{\qquad}lcl}
x^0 &=& 1 & x^6 &=& 2 & x^{12} &=& 4 & x^{18} &=& 3 \\
x^1 &=& x & x^7 &=& 2x & x^{13} &=& 4x & x^{19} &=& 3x \\
x^2 &=& 4x+3 & x^8 &=& 3x+1 & x^{14} &=& x+2 & x^{20} &=& 2x+4 \\
x^3 &=& 4x+2 & x^9 &=& 3x+4 & x^{15} &=& x+3 & x^{21} &=& 2x+1 \\
x^4 &=& 3x+2 & x^{10} &=& x+4 & x^{16} &=& 2x+3 & x^{22} &=& 4x+1 \\
x^5 &=& 4x+4 & x^{11} &=& 3x+3 & x^{17} &=& x+1 & x^{23} &=& 2x+2
\end{array}$$

As expected these are the 24 non-zero elements of $\mathbb{F}_{25}$. Note that $x^6 = 2$ can be used to make calculations easier. For example, $x^8 = x^6 \cdot x^2 = 2(4x+3) = 3x+1$.

We observe that

$$\{0,1,2,3,4\} = \{0, x^0, x^6, x^{12}, x^{18}\} \quad \text{and} \quad \{x, x+1, x+2, x+3, x+4\} = \{x^1, x^{10}, x^{14}, x^{15}, x^{17}\}$$

are two lines of $\mathrm{AG}(2,5)$ (one contains 0 and one does not). The orbits of these two lines under the permutation

$$(0)(x^0, x^1, x^2, \dots, x^{23})$$

form the lines of affine plane. Writing ∞ for 0 and i for x^i we obtain an affine plane with point set $\mathbb{Z}_{24} \cup \{\infty\}$ whose 30 lines are the columns of the following two arrays.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0
10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9
14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13
15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

0	1	2	3	4	5
6	7	8	9	10	11
12	13	14	15	16	17
18	19	20	21	22	23
∞	∞	∞	∞	∞	∞

$\square$

Chapter 3

Design Theory

Definition 3.0.1. A (combinatorial) **design** consists a set V and a collection $\mathcal{B}$ of subsets of V. The elements of V are the **points** of the design, and the subsets in $\mathcal{B}$ are called **blocks**. An **automorphism** of a design is a permutation of V that preserves the blocks. More precisely, a permutation π of V is an automorphism of a design $(V, \mathcal{B})$ if $\mathcal{B}\pi = \mathcal{B}$, where $\mathcal{B}\pi = \{B\pi : B \in \mathcal{B}\}$ and $B\pi = \{x\pi : x \in B\}$. A design with v points is **cyclic** if it has an automorphism that permutes its points in a single cycle of length v.

3.1 (v, k, λ)-designs

Definition 3.1.1. Let v, k and λ be positive integers with $k < v$. A **(v, k, λ)-design** is a design with v points where every block has k elements, and where every pair of points occurs in exactly λ blocks. □

Theorem 3.1.2. If there exists a (v, k, λ)-design, then the number of blocks is $b = \frac{\lambda v(v-1)}{k(k-1)}$, and each point occurs in $r = \frac{\lambda(v-1)}{(k-1)}$ blocks. Thus, $b = \frac{\lambda v(v-1)}{k(k-1)}$ and $r = \frac{\lambda(v-1)}{(k-1)}$ are integers.

Definition 3.1.3. The integer $r = \frac{\lambda(v-1)}{(k-1)}$ is called the **replication number** of the design. The notation b for number of blocks, and r for replication number is widely used. The conditions that $\frac{\lambda v(v-1)}{k(k-1)}$ and $\frac{\lambda(v-1)}{(k-1)}$ are integers are sometimes called **the obvious necessary conditions for the existence of a (v, k, λ)-design**. □

Example 3.1.4. Projective and affine planes may be thought of as 2-designs, with the points and lines of the plane being the points and blocks of the design. A projective plane of order n is an $(n^2 + n + 1, n + 1, 1)$-design, and an affine plane of order n is an $(n^2, n, 1)$-design. □

Example 3.1.5. A $(4n - 1, 2n - 1, n - 1)$-design is a **Hadamard design** of order n. Hadamard designs are (essentially) equivalent to **Hadamard matrices**. A famous unsolved problem in design theory is whether there exists a Hadamard design of order n for all $n \geq 2$.

The parameters for a Hadamard design of order n for $n = 2, 3, \ldots, 25$ are shown below.

$(7,3,1)$	$(11,5,2)$	$(15,7,3)$	$(19,9,4)$	$(23,11,5)$	$(27,13,6)$
$(31,15,7)$	$(35,17,8)$	$(39,19,9)$	$(43,21,10)$	$(47,23,11)$	$(51,25,12)$
$(55,27,13)$	$(59,29,14)$	$(63,31,15)$	$(67,33,16)$	$(71,35,17)$	$(75,37,18)$
$(79,39,19)$	$(83,41,20)$	$(87,43,21)$	$(91,45,22)$	$(95,47,23)$	$(99,49,24)$

The projective plane $\mathrm{PG}(2,2)$ is a Hadamard design of order 2, equivalently a $(7,3,1)$-design. A Hadamard design of order 3, equivalently a $(11,5,2)$-design, is given by the orbit of the block $\{1,3,4,5,9\}$ under the action of $\mathbb{Z}_{11}$. The points and blocks of a Hadamard design of order 4, equivalently a $(15,7,3)$-design are obtained from the points and hyperplanes of $\mathrm{PG}(3,2)$. If $q = p^\alpha$ is a prime power with $q \equiv 3 \pmod 4$, then the orbit of the quadratic residues of $\mathbb{F}_q$ under the action of $(\mathbb{F}_q, +)$ form a Hadamard design of order $n = \frac{q+1}{4}$.

From 1985 until 2005 the smallest unresolved case was the existence of a Hadamard design of order 107, or $(427,213,106)$-design. Such a design was constructed by Kharaghani and Tayfeh-Rezaie in 2005, see [38]. The smallest unresolved case is now the existence of a Hadamard design of order 167, or $(667,333,166)$-design. Various other cases have been resolved in the last few years. For example, a Hadamard design of order 191, or $(763,381,190)$-design, was constructed by Doković in 2008 [21]. □

Example 3.1.6. A $(\binom{n+2}{2} + 1, n+2, 2)$-design is a **biplane of order n**. A biplane resembles a projective plane, except that a biplane has two, instead of one, lines through any pair of distinct points, and in a biplane any pair of distinct lines intersects in exactly two, instead of one, points. A biplane has $\binom{n+2}{2} + 1$ lines and there are $n+2$ lines through each point.

The complements of the lines of a projective plane of order 2 form a biplane of order 2; namely a $(7,4,2)$-design. A biplane of order 3 is also a Hadamard design of order 3; namely a $(11,5,2)$-design. A biplane of order 4 is a $(16,6,2)$-design. One can be constructed as follows.

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/line 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 only known biplanes are of order $2,3,4,7,9$ and 11. There is no biplane of order $5,6,8,10$. It is unknown whether there are any biplanes of order $n > 11$. □

Definition 3.1.7. A (v,k,λ)-design that has v blocks is a **symmetric design**.

Theorem 3.1.8. *In a symmetric (v,k,λ)-design, we have $\lambda(v-1) = k(k-1)$, each point occurs in exactly k blocks, and any two blocks intersect in exactly λ points.*

Projective planes, Hadamard designs and biplanes are symmetric designs, but affine planes are not.

A very important result on the existence of (v, k, λ)-designs was proved by Wilson in 1975 [60]. 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 3.1.9. (Wilson's Theorem, [60]) 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 briefly mention some other facts concerning the existence of (v, k, λ)-designs.

Definition 3.1.10. 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 3.1.11. 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. □

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 [39]. 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 $\lambda \geq 2$ [33]. 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 $\lambda = 1$, the existence problem is not yet completely settled. The most recent new results were obtained in 2007 [1]. There remain 29 unresolved values of v (ranging from $v = 51$ to $v = 801$) and four cases where the obvious necessary conditions are satisfied but no design exists ($v = 16, 21, 36, 46$). For values of $k > 6$ less in known, especially for $k \geq 10$. A comprehensive summary of results is given in [2]. For $k \leq \frac{v}{2}$ (see Theorem 3.1.11), 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.

3.2 t-Designs

Definition 3.2.1. Let v, k, λ and t be positive integers such that $t \leq k < v$. A $t-(v, k, \lambda)$**-design** is a design with v points where every block has k elements, and where every t-set of points occurs in exactly λ blocks. □

In the broader context of t-designs, the (v, k, λ)-designs discussed in Section 3.1 are $2-(v, k, \lambda)$-designs. The term **t-design**, rather than $t-(v, k, \lambda)$-design, may be used if we do not wish to specify the values of v, k or λ.

Example 3.2.2. A $3-(8,4,1)$-design can be constructed as follows. The points are the elements of $\mathbb{Z}_2^3$ and the block set is $\mathcal{B}_1 \cup \mathcal{B}_2$ where

$$\mathcal{B}_1 = \{\{x, x + (0,0,1), x + (0,1,0), x + (1,0,0)\} : x \in \mathbb{Z}_2^3\}$$

and

$$\mathcal{B}_2 = \{\{x, y, x + (1,1,1), y + (1,1,1)\} : x, y \in \mathbb{Z}_2^3, x + y \in \{(0,0,1), (0,1,0), (1,0,0)\}\}.$$

This design can be thought of as having the vertices of a (3-dimensional) cube as its points, and having its block set made up of blocks of two types as follows. The blocks in $\mathcal{B}_1$ consist of a vertex and its three neighbouring vertices. The blocks in $\mathcal{B}_2$ consist of two adjacent vertices together with the two vertices opposite them.

The number of blocks in this design is clearly $8 + 6 = 14$. Since the number of triples covered by 14 blocks is $4 \times 14 = 56 = \binom{8}{3}$, to prove that the design is a $3-(8,4,1)$-design it suffices to show that every triple occurs in at least one block. Let $\{x, y, z\}$ be an arbitrary triple of points. If x and y are adjacent and x, y and z all lie on a face, then it is easy to see that $\{x, y, z\}$ occurs in a block of $\mathcal{B}_1$. If x and y are adjacent and x, y and z do not all lie on a face, then it is easy to see that $\{x, y, z\}$ occurs in a block of $\mathcal{B}_2$. By symmetry, we can thus assume that no two of x, y and z are adjacent. In this case it is easy to see that $\{x, y, z\}$ occurs in a block of $\mathcal{B}_1$. Thus, the design is indeed a $3-(8,4,1)$-design. □

Theorem 3.2.3. If $(V, \mathcal{B})$ is a $t-(v, k, \lambda)$-design and $S \subseteq V$ with $0 \leq |S| \leq t$, then the number of blocks of $\mathcal{B}$ that contain S is

$$\lambda_s = \frac{\lambda\binom{v-s}{t-s}}{\binom{k-s}{t-s}}$$

where $s = |S|$. In particular, if there exists a $t-(v, k, \lambda)$-design, then λ_s is an integer for $0 \leq s \leq t$.

Proof Define the set R by

$$R = \{(X, B) : X \subseteq V \setminus S, |X| = t - s, B \in \mathcal{B}, X \cup S \subseteq B\}.$$

The number of subsets of $V \setminus S$ having cardinality $t-s$ is $\binom{v-s}{t-s}$, and for each such set X, there are λ blocks of $\mathcal{B}$ that contain the t-set $X \cup S$. Thus $|R| = \lambda\binom{v-s}{t-s}$. On the other hand, if $\lambda(S)$ is the number of blocks of $\mathcal{B}$ that contain S, then $|R| = \lambda(S)\binom{k-s}{t-s}$, because for each block $B \in \mathcal{B}$ that contains S, there are $\binom{k-s}{t-s}$ ways to choose X from the points of $B \setminus S$. Combining the two expressions we have obtained for $|R|$, we see that $\lambda(S) = \frac{\lambda\binom{v-s}{t-s}}{\binom{k-s}{t-s}}$. □

It follows from Theorem 3.2.3 that any $t-(v,k,\lambda)$-design is also an $s-(v,k,\lambda_s)$-design for $0 \le s \le t$ where $\lambda_s = \frac{\lambda\binom{v-s}{t-s}}{\binom{k-s}{t-s}}$.

Definition 3.2.4. In the context of $t-(v,k,\lambda)$-designs, the parameters t, v, k, and λ are **admissible** if and only if

$$\lambda_s = \frac{\lambda\binom{v-s}{t-s}}{\binom{k-s}{t-s}}$$

is an integer for $0 \le s \le t$. These conditions are called **the obvious necessary conditions** for the existence of a $t-(v,k,\lambda)$-design. □

Notice that $\lambda_0 = \frac{\lambda\binom{v}{t}}{\binom{k}{t}}$ is the number b of blocks in a $t-(v,k,\lambda)$-design. The interpretation here is that the empty set is a subset of each block. We also have $\lambda_1 = \frac{\lambda\binom{v-1}{t-1}}{\binom{k-1}{t-1}}$, which is the replication number r of the design (the number of blocks in which each point occurs). And of course $\lambda_t = \lambda$. The preceding few sentences show that the obvious necessary conditions for the existence of a $t-(v,k,\lambda)$-design are equivalent to the obvious necessary conditions for the existence of a $2-(v,k,\lambda)$-design, see Definition 3.1.3.

In early 2014, Keevash [37] proved that the obvious necessary conditions for the existence of a $t-(v,k,\lambda)$-design are sufficient when v is large enough relative to t, k and λ. Prior to this result, only finitely many Steiner systems with $t \ge 4$ were known, and no Steiner systems with $t \ge 6$ were known.

Theorem 3.2.5. (Keevash, [37]) For all $t \ge 1$, $k \ge t$ and $\lambda \ge 1$, there is a constant $C(t,k,\lambda)$ such that for all $v \ge C(t,k,\lambda)$, there exists a $t-(v,k,\lambda)$-design if and only if $\binom{k-s}{t-s}$ divides $\lambda\binom{v-s}{t-s}$ for $0 \le s \le t$.

We have already noted that 2-designs are the familiar (v,k,λ)-designs. The following theorem gives simple necessary and sufficient conditions for the existence of a 1-design.

Theorem 3.2.6. There exists a $1-(v,k,\lambda)$-design if and only if k divides $v\lambda$.

Proof If there exists a $1-(v,k,\lambda)$-design, then the number of occurrences of points in blocks is $v\lambda$. Since each block contains k points, it follows that k divides $v\lambda$. Conversely, if k divides $v\lambda$, then $(\mathbb{Z}_v, \mathcal{B})$ is a $1-(v,k,\lambda)$-design where $\mathcal{B} = \{\{0,1,2,\ldots,k-1\} + ik : i = 0,1,\ldots,\frac{v\lambda}{k}-1\}$. □

3.3 Extensions and contractions

Definition 3.3.1. If $\mathcal{D} = (V,\mathcal{B})$ is a $t-(v,k,\lambda)$-design and $S \subseteq V$ such that $1 \le |S| < t$, then we define the **derivative** of $\mathcal{D}$ with respect to S to be the design

$$\mathcal{D}_S = (V \setminus S, \{B \setminus S : B \in \mathcal{B}, S \subset B\}).$$

When $S = \{x\}$, we write $\mathcal{D}_x$ rather than $\mathcal{D}_{\{x\}}$. □

Theorem 3.3.2. The derivative $\mathcal{D}_S$ of a $t-(v,k,\lambda)$-design is a $(t-s)-(v-s,k-s,\lambda)$-design where $s=|S|$.

Proof Let $\mathcal{D}=(V,\mathcal{B})$ be a $t-(v,k,\lambda)$-design and let $S \subseteq V$ such that $1 \le |S| < t$. Clearly, $\mathcal{D}_S$ has $v-s$ points, and each block of $\mathcal{D}_S$ has $k-s$ elements. If $X \subseteq V \setminus S$ with $|X| = t-s$, then $X \cup S$ is a t-subset of V and hence is contained in λ blocks of $\mathcal{D}$. It follows immediately that X is contained in λ blocks of $\mathcal{D}_S$. $\square$

Definition 3.3.3. If $\mathcal{D}$ is a $t-(v,k,\lambda)$-design and x is a point of $\mathcal{D}$, then $\mathcal{D}_x$ is a **contraction** of $\mathcal{D}$. $\square$

It is natural to ask for which designs can the reverse of the contraction process occur. That is, given a $t-(v,k,\lambda)$-design $\mathcal{D}'$, can we find a $(t+1)-(v+1,k+1,\lambda)$-design $\mathcal{D}$ such that $\mathcal{D}'$ is a contraction of $\mathcal{D}$.

Definition 3.3.4. If $\mathcal{D}$ is a $t-(v,k,\lambda)$-design and $\mathcal{D}'$ is a $(t-1)-(v-1,k-1,\lambda)$ such that $\mathcal{D}' \cong \mathcal{D}_x$ for some point x of $\mathcal{D}$, then $\mathcal{D}$ is an **extension** of $\mathcal{D}'$. A $t-(v,k,\lambda)$-design that has an extension is said to be **extendable**. $\square$

It is easy to demonstrate that not all $t-(v,k,\lambda)$-designs are extendable. Suppose $\mathcal{D}$ is an extendable $t-(v,k,\lambda)$-design. The number of blocks in $\mathcal{D}$ is $b = \lambda\frac{\binom{v}{t}}{\binom{k}{t}} = \lambda\frac{v!(k-t)!}{k!(v-t)!}$, and the number of blocks in its extension is $\lambda\frac{(v+1)!(k-t)!}{(k+1)!(v-t)!}$. Thus, the number of blocks in the extension is $\frac{b(v+1)}{k+1}$. Since this number is not always an integer, not all $t-(v,k,\lambda)$-designs are extendable. For example, any $(13,4,1)$-design is not extendable, as the number of blocks would be $\frac{13\cdot 14}{5}$. We have proven the following result.

Theorem 3.3.5. If b is the number of blocks in an extendable $t-(v,k,\lambda)$-design, then $\frac{b(v+1)}{k+1}$ is an integer and is the number of blocks in an extension.

On the other hand, we have the following theorem.

Theorem 3.3.6. Any $2-(2k+1,k,\lambda)$-design is extendable.

Proof Let $(V,\mathcal{B})$ be a $2-(2k+1,k,\lambda)$-design. The number of blocks is $b = \binom{2k+1}{2}\lambda/\binom{k}{2} = \frac{2(2k+1)\lambda}{k-1}$ and each point occurs in $r = \frac{2k\lambda}{k-1}$ blocks. Let ∞ be a new point ($\infty \notin V$) and consider the design $(V',\mathcal{B}')$ where $V' = V \cup \{\infty\}$ and $\mathcal{B}' = \{B \cup \{\infty\} : B \in \mathcal{B}\} \cup \{V \setminus B : B \in \mathcal{B}\}$. We claim that $(V',\mathcal{B}')$ is a $3-(2k+2,k+1,\lambda)$-design, and hence an extension of $(V,\mathcal{B})$.

Clearly $(V',\mathcal{B}')$ has $2k+2$ points and blocks of size $k+1$. So it remains only to check that each triple T of distinct points from V' occurs in exactly λ blocks of $\mathcal{B}'$. If $\infty \in T$, then this follows immediately from the fact that each pair of distinct elements of V occurs in exactly λ blocks of $\mathcal{B}$. Hence we may assume that $T = \{x,y,z\} \subseteq V$. Let c be the number of blocks of $\mathcal{B}$ that contain $\{x,y,z\}$. The number of blocks of $\mathcal{B}$ that contain exactly two elements from $\{x,y,z\}$ is $3(\lambda-c)$, and the number that contain exactly one element from $\{x,y,z\}$ is $3(r-2\lambda+c)$. It follows that the number of blocks of $\mathcal{B}$ that contain no elements of $\{x, y, z\}$ is $d = b-c-3(\lambda-c)-3(r-2\lambda+c) = b-c-3r+3\lambda$. Thus, the number of blocks of $\mathcal{B}'$ that contain $\{x, y, z\}$ is $\lambda' = c + d = b - 3r + 3\lambda$. It remains to show that $\lambda' = \lambda$, and this follows by substituting $b = \frac{2(2k+1)\lambda}{k-1}$ and $r = \frac{2k\lambda}{k-1}$ into $\lambda' = b - 3r + 3\lambda$ and simplifying. □

Example 3.3.7. We know that $(\mathbb{Z}_{11}, \mathcal{O}_{\mathbb{Z}_{11}}(\{1, 3, 4, 5, 9\}))$ is a $2-(11, 5, 2)$-design, and an extension of this design, a $3-(12, 6, 2)$-design, is given by the following blocks

1	3	4	5	9	∞	0	2	6	7	8	10
2	4	5	6	10	∞	1	3	7	8	9	0
3	5	6	7	0	∞	2	4	8	9	10	1
4	6	7	8	1	∞	3	5	9	10	0	2
5	7	8	9	2	∞	4	6	10	0	1	3
6	8	9	10	3	∞	5	7	0	1	2	4
7	9	10	0	4	∞	6	8	1	2	3	5
8	10	0	1	5	∞	7	9	2	3	4	6
9	0	1	2	6	∞	8	10	3	4	5	7
10	1	2	3	7	∞	9	0	4	5	6	8
0	2	3	4	8	∞	10	1	5	6	7	9

□

It is worth remarking that the 3-designs given by Theorem 3.3.6 are easily seen to be resolvable, having two blocks in each resolution class. One family of designs to which Theorem 3.3.6 applies is the Hadamard designs. Recall that a Hadamard design is a $2-(4n-1, 2n-1, n-1)$-design, which by Theorem 3.3.6 extends to a $3-(4n, 2n, n-1)$-design.

Corollary 3.3.8. Hadamard designs are extendable.

Having noted that all Hadamard designs are extendable, we now examine extendibility of projective planes. In Section 3.4 we will consider extensions of affine planes. The projective plane of order 2 is a $2-(7, 3, 1)$-design. It is unique up to isomorphism and is extendable by Theorem 3.3.6. The projective plane of order 3 is a $2-(13, 4, 1)$-design and we noted above that this design is not extendable (since $\frac{b(v+1)}{k+1} = \frac{13\cdot 14}{5}$ is not an integer, see Theorem 3.3.5). In the following example we construct a $3-(22, 6, 1)$-design, which shows that the unique (up to isomorphism) projective plane of order 4, a $2-(21, 5, 1)$-design, is extendable.

Example 3.3.9. Construction of a $3-(22, 6, 1)$-design from a $2-(11, 5, 2)$-design.

Suppose $(V, \mathcal{B})$ is a $2-(11, 5, 2)$-design. A set of three points from V will be called a *triangle* if it is not a subset of any block of $\mathcal{B}$. If T is a triangle and $x \in T$, then a block $B \in \mathcal{B}$ such that $B \cap T = \{x\}$ is called a *tangent* at x to T.

Let $T = \{x, y, z\}$ be a triangle. Of the five blocks containing x, there are exactly two containing $\{x, y\}$ and exactly two containing $\{x, z\}$. These four blocks are distinct and it follows that the fifth block containing x is a unique tangent at x to T. Hence, for each triangle T and each point $x \in T$, there is a unique tangent at x to T.

Before we construct our $3-(22,6,1)$-design, we prove some properties concerning the triangles of a $2-(11,5,2)$-design and their tangents. In particular, we shall show that for any pair $\{x,y\}$ of distinct points, there are exactly three triangles containing $\{x,y\}$, and we show that the nine tangents to these three triangles are precisely the nine blocks that do not contain $\{x,y\}$.

There are 8 points altogether in the two blocks that contain $\{x,y\}$, and for each remaining point z, $\{x,y,z\}$ is a triangle. Thus, for each pair $\{x,y\}$ of points, there are exactly three triangles containing $\{x,y\}$.

Let $\{x,y,z_1\}$, $\{x,y,z_2\}$ and $\{x,y,z_3\}$ be the three triangles containing $\{x,y\}$. We show that the nine tangents to these triangles are pairwise distinct. The two blocks containing $\{x,y\}$ are not tangents to these triangles, and so it suffices to show that each block not containing $\{x,y\}$ is a tangent to at least one of the triangles. Let B be a block not containing $\{x,y\}$.

If $B \cap \{x,y,z_1,z_2,z_3\} = \emptyset$, then each of the five points of B is in one of the two blocks that contains $\{x,y\}$, but is neither x nor y (because if a point $v \in B$ is not in one of the two blocks that contains $\{x,y\}$, then v together with x and y is a triangle). Hence one of the two blocks that contains $\{x,y\}$ also contains three points from B, and this contradicts the fact that any two blocks intersect in exactly two points. We conclude that $B \cap \{x,y,z_1,z_2,z_3\}$ is non-empty. Thus, B is either a tangent to one of the three triangles containing $\{x,y\}$, or it intersects each of them in at least two points. We show that the latter cannot be the case.

For a contradiction, suppose B intersects each of $\{x,y,z_1\}$, $\{x,y,z_2\}$ and $\{x,y,z_3\}$ in at least two points. Since B does not contain $\{x,y\}$, this means it contains $\{z_1,z_2,z_3\}$ and either x or y, but not both. Without loss of generality, suppose $\{z_1,z_2,z_3,x\} \subseteq B$. We know that B intersects each of the two blocks that contain $\{x,y\}$ in exactly two points. But since the six points other than x and y in these two blocks are distinct, and since none of them is in $\{z_1,z_1,z_3\}$, this is impossible. We conclude that B is a tangent to at least one of the triangles $\{x,y,z_1\}$, $\{x,y,z_2\}$ and $\{x,y,z_3\}$, and hence that the nine tangents to these triangles are distinct.

We are now ready to construct a $3-(22,6,1)$-design. The point set will be $V^* = V \cup \mathcal{B}$, and the block set $\mathcal{B}^*$ is defined as follows.

(1) For each point $x \in V$, the block $\{x\} \cup \{B : x \in B, B \in \mathcal{B}\}$ is in $\mathcal{B}^*$.

(2) For each block $B \in \mathcal{B}$, the block $\{B\} \cup B$ is in $\mathcal{B}^*$.

(3) For each triangle T, the block $T \cup \{B_x, B_y, B_z\}$ is in $\mathcal{B}^*$ where B_x, B_y and B_z are the three tangents to T.

We now check that $(V^*, \mathcal{B}^*)$ is a $3-(22,6,1)$-design. The number of triangles in a $2-(11,5,2)$-design is $\binom{11}{3} - 11 \cdot \binom{5}{3} = 55$, so there are 77 blocks in $\mathcal{B}^*$. Since $\binom{22}{3}/\binom{6}{3} = 77$, $\mathcal{B}^*$ has the correct number of blocks for a $3-(22,6,1)$-design. Thus, it suffices to show that any 3-element subset S of V^* is covered by at least one block of $\mathcal{B}^*$. This splits into cases depending on $|S \cap V|$.

First consider the case where $|S \cap V| = 3$; that is, $S \subset V$. If $S \subset B$ for some $B \in \mathcal{B}$, then S is covered by the block $\{B\} \cup B$ of $\mathcal{B}^*$. On the other hand, if S is not a subset of any block of $\mathcal{B}$, then S is a triangle and again S is covered.

Now consider the case where $|S \cap V| = 2$; that is $S = \{x, y, B\}$ where $x, y \in V$ and $B \in \mathcal{B}$. If $\{x, y\} \subseteq B$, then S is covered by $B \cup \{B\}$. Thus, we may assume that $\{x, y\}$ is not a subset of B. We have noted above that in this situation B is a tangent to some triangle containing $\{x, y\}$, so S is again covered.

For the remaining cases, namely $|S \cap V| \in \{0, 1\}$, we will use the fact that a $2-(11, 5, 2)$-design is symmetric, and exploit the symmetry between its points and its blocks. That is, the fact that if $(V, \mathcal{B})$ is a symmetric $2-(v, k, \lambda)$-design, and we define $B_x = \{B \in \mathcal{B} : x \in B\}$, then $(\mathcal{B}, \{B_x : x \in V\})$ is also a symmetric $2-(v, k, \lambda)$-design. This new design is called the *dual* of the original design. The points and blocks of the dual design are the blocks and the points respectively of the original design, with incidence of points and blocks preserved.

We will prove below that if T is a triangle in a $2-(11, 5, 2)$-design, then the three tangents to T form a triangle in its dual. That is, the tangents are three blocks with no mutually common point. Moreover, we will prove that if T is any triangle in the original design and T' is the corresponding triangle in the dual design, then in the dual design, the tangents to T' are the points of T. It follows that in $(V^*, \mathcal{B}^*)$, there is a symmetry between the points from V and the points from $\mathcal{B}$. This means that the cases $|S \cap V| = 0$ and $|S \cap V| = 1$ follow from the cases $|S \cap V| = 3$ and $|S \cap V| = 2$ respectively.

We now show the above-claimed results concerning triangles in the dual. Suppose $\{x, y, z\}$ is a triangle in our original $2-(11, 5, 2)$-design and let $X, Y, Z \in \mathcal{B}$ be the tangents at x, y and z respectively. For a contradiction to the claim $\{X, Y, Z\}$ is a triangle in the dual design, suppose that $a \in X \cap Y \cap Z$. Since there are two blocks in $\mathcal{B}$ that contain $\{x, y\}$, two that contain $\{x, z\}$, and two that contain $\{y, z\}$, and since these six blocks together with X, Y, and Z are all the blocks containing x, y or z, it is easy to see that we do not have each of the three pairs $\{a, x\}$, $\{a, y\}$ and $\{a, z\}$ occurring in exactly two blocks. We conclude that $X \cap Y \cap Z = \emptyset$, so that $\{X, Y, Z\}$ is a triangle in the dual design.

It remains to show that in the dual, the tangents to the triangle $\{X, Y, Z\}$ are x, y and z. Since any two blocks of $\mathcal{B}$ intersect in exactly two points, the blocks X, Y and Z are of the form $\{x, a, b, c, d\}$, $\{y, a, b, e, f\}$, and $\{z, c, d, e, f\}$. Hence in the dual design, x, y and z are the tangents to the triangle $\{X, Y, Z\}$. This completes the proof that $(V^*, \mathcal{B}^*)$ is a $3-(22, 6, 1)$-design. $\square$

Theorem 3.3.10. For $q \in \{1, 2, 4\}$ there is a unique up to isomorphism $2-(q^2+q+1, q+1, 1)$-design (or projective plane of order q), and it is extendable. For $q \notin \{1, 2, 4\}$, no $2-(q^2+q+1, q+1, 1)$-design is extendable.

Remark: For technical reasons, a $2-(3, 2, 1)$-design (the case $q = 1$) is not considered a projective plane.

Proof In the case $q = 1$, the set of all 3-subsets of a 4-set form the blocks a $3-(4, 3, 1)$-design, which is an extension of the unique (up to isomorphism) $2-(3, 2, 1)$-design. For $q = 2$ and $q = 4$, we have seen that the unique projective plane of order q is extendable, see Theorem 3.3.6 for the case $q = 2$ and Example 3.3.9 for the case $q = 4$.

Now suppose a $2-(q^2+q+1, q+1, 1)$-design has an extension. Since the number of blocks in a $2-(q^2+q+1, q+1, 1)$-design is q^2+q+1, by Theorem 3.3.5 we have $(q^2+q+1)(q^2+q+2) \equiv$

$0 \pmod{q+2}$. But $q^2+q+1 = (q+2)(q-1)+3$ and $q^2+q+2 = (q+2)(q-1)+4$, so $q+2$ divides 12. Thus, $q \in \{1, 2, 4, 10\}$. Since there is no projective plane of order 10, the theorem is proved. $\square$

3.4 Inversive Planes

We now turn to the question of extendibility of affine planes. To this end, we shall construct a family of designs, known as **inversive planes**, which are extensions of affine planes of order q where q is a prime power. To construct inversive planes we use permutation groups.

Let G be a permutation group acting on X and let $t \geq 1$ be an integer. Then G is **t-transitive** if for any $x_1, x_2, \ldots, x_t, y_1, y_2, \ldots, y_t \in X$ where $x_1, x_2, \ldots, x_t$ are distinct and $y_1, y_2, \ldots, y_t$ are distinct, there is a $g \in G$ such that $g(x_i) = y_i$ for $i = 1, 2, \ldots, t$. If there is a unique such $g \in G$, then G is **sharply** t-transitive. Recall that for a subset $Y \subseteq X$, the setwise stabilizer in G of Y is denoted by $G_{\{Y\}}$.

Example 3.4.1. The group $\mathrm{AGL}(1,q)$: a sharply 2-transitive permutation group of order $q(q-1)$ acting on $\mathbb{F}_q$. Let $\mathbb{F}_q$ be a field with q elements. For each $a \in \mathbb{F}_q \setminus \{0\}$ and each $b \in \mathbb{F}_q$, define a permutation $\pi_{ab} : \mathbb{F}_q \mapsto \mathbb{F}_q$ by $\pi_{ab}(x) = ax + b$ for all $x \in \mathbb{F}_q$. It is easy to see that π_{ab} is indeed a permutation, for if $\pi_{ab}(x) = \pi_{ab}(y)$, then $x = y$ (because $a \neq 0$). Let $G = \{\pi_{ab} : a \in \mathbb{F}_q \setminus \{0\}, b \in \mathbb{F}_q\}$. It is routine to check that G is a group. We show that G is sharply 2-transitive. Let $x_1, x_2, y_1, y_2 \in \mathbb{F}_q$ with $x_1 \neq x_2$ and $y_1 \neq y_2$. If we let $a = \frac{y_1 - y_2}{x_1 - x_2}$ (recall that $x_1 \neq x_2$ and $y_1 \neq y_2$, so a is well-defined and $a \neq 0$) and $b = y_1 - ax_1$, then we have $\pi_{ab}(x_1) = y_1$ and $\pi_{ab}(x_2) = y_2$. Thus, G is 2-transitive. Moreover, it is routine to check that if $\pi_{cd}(x_1) = y_1$ and $\pi_{cd}(x_2) = y_2$, then $c = a$ and $d = b$. Thus, G is sharply 2-transitive. The group G is called $\mathrm{AGL}(1, \mathrm{q})$. $\square$

Theorem 3.4.2. If G is a sharply t-transitive permutation group acting on a v-set V and K is a k-subset of V such that $t \leq k < v$, then $(V, \mathcal{O}_G(K))$ is a $t-(v,k,\lambda)$-design where $\lambda = \frac{k(k-1)\cdots(k-t+1)}{|G_{\{K\}}|}$.

Proof Let $G = \{g_1, g_2, \ldots, g_{|G|}\}$ and let $\{x_1, x_2, \ldots, x_t\}$ be an arbitrary t-set of points from V. Since G is sharply t-transitive, and since there are $k(k-1)\cdots(k-t+1)$ ordered t-tuples of distinct points in K, exactly $k(k-1)\cdots(k-t+1)$ of the sets $g_1(K), g_2(K), \ldots, g_{|G|}(K)$ contain $\{x_1, x_2, \ldots, x_t\}$. But each block from $\mathcal{O}_G(K)$ occurs $|G_{\{K\}}|$ times in $g_1(K), g_2(K), \ldots, g_{|G|}(K)$, and it follows that $\lambda = \frac{k(k-1)\cdots(k-t+1)}{|G_{\{K\}}|}$. $\square$

Example 3.4.3. We know from Example 3.4.1 that $G = \mathrm{AGL}(1, q^2)$ is a sharply 2-transitive permutation group acting on $\mathbb{F}_{q^2}$, where $q = p^n$ and p is prime. Consider the subset $\mathbb{F}_q$ of $\mathbb{F}_{q^2}$. By this we mean take $\mathbb{F}_q$ to be the unique subfield of order q in $\mathbb{F}_{q^2}$, which can be obtained via $\mathbb{F}_q = \{0\} \cup \mathbb{F}_q^*$ where $\mathbb{F}_q^*$ is the unique order $q-1$ subgroup of $\mathbb{F}_{q^2}^*$.

Since $\mathbb{F}_q$ is a subfield, $H = \{\pi_{ab} : a \in \mathbb{F}_q \setminus \{0\}, b \in \mathbb{F}_q\} \subseteq G_{\{\mathbb{F}_q\}}$. Suppose $\pi \in G_{\{\mathbb{F}_q\}}$ and let $x_1, x_2 \in \mathbb{F}_q$ with $x_1 \neq x_2$. Since $H \cong \mathrm{AGL}(1,q)$ acts 2-transitively on $\mathbb{F}_q$ and $\pi(x_1), \pi(x_2) \in \mathbb{F}_q$, there is an $h \in H$ such that $h(x_1) = \pi(x_1)$ and $h(x_2) = \pi(x_2)$. Since $\mathrm{AGL}(1, q^2)$ acts sharply 2-transitively on $\mathbb{F}_{q^2}$, this implies $\pi = h \in H$. Thus, $G_{\{\mathbb{F}_q\}} \subseteq H$ and so we have $G_{\{\mathbb{F}_q\}} = H$. In particular, $|G_{\{\mathbb{F}_q\}}| = q(q-1)$. Applying Theorem 3.4.2 with $G = \mathrm{AGL}(1, q^2)$, $V = \mathbb{F}_{q^2}$ and $K = \mathbb{F}_q$, we have that

$$(\mathbb{F}_{q^2}, \{\pi_{ab}(\mathbb{F}_q) : a \in \mathbb{F}_{q^2} \setminus \{0\}, b \in \mathbb{F}_{q^2}\})$$

is a $2-(q^2, q, 1)$-design. □

The $2-(q^2, q, 1)$-designs constructed in Example 3.4.3 are isomorphic to the $2-(q^2, q, 1)$-designs whose blocks are the 1-flats in $\mathrm{AG}(2, q)$ (see Theorem 2.6.4).

Example 3.4.4. The group $\mathrm{PGL}(2, q)$: a sharply 3-transitive permutation group of order $q^3 - q$ acting on the projective line $\mathrm{PG}(1, q)$.

Recall that the projective line $\mathrm{PG}(1, q)$ has as its points the 1-dimensional subspaces of the 2-dimensional vector space over $\mathbb{F}_q$. Denote by $\mathrm{GL}(2, q)$, the set of all 2 by 2 invertible matrices over $\mathbb{F}_q$. Define $\mathrm{PGL}(2, q)$ to be the quotient group $\mathrm{GL}(2, q)/Z$, where Z is the subgroup of scalar matrices in $\mathrm{GL}(2, q)$ (a scalar matrix has the form λI where I is the identity matrix, Z is the **centre** of $\mathrm{GL}(2, q)$).

It is routine to check that $\mathrm{PGL}(2, q)$ is a permutation group acting on $\mathrm{PG}(1, q)$; where for each $\langle x\rangle \in \mathrm{PG}(1, q)$ and each $[M] \in \mathrm{PGL}(2, q)$, $[M](\langle x\rangle) = \langle Mx\rangle$. To show that $|\mathrm{PGL}(2, q)| = q^3 - q$, it is sufficient to show that $|\mathrm{GL}(2, q)| = (q-1)(q^3-q)$, because there are $q-1$ scalar matrices in $\mathrm{GL}(2, q)$. But we have already seen in the proof of Theorem 2.6.2 that the number of ordered pairs of linearly independent vectors of a 2-dimensional vector space over $\mathbb{F}_q$ is $(q^2-1)(q^2-q) = (q-1)(q^3-q)$, and this is also the number of 2 by 2 invertible matrices over $\mathbb{F}_q$. Thus $|\mathrm{PGL}(2, q)| = q^3 - q$.

We now show that $\mathrm{PGL}(2, q)$ is sharply 3-transitive. Since $|\mathrm{PGL}(2, q)|$ equals the number of ordered triples of distinct elements of $\mathrm{PG}(1, q)$, namely $q^3 - q = (q+1)q(q-1)$, if $\mathrm{PGL}(2, q)$ is 3-transitive, then it is necessarily sharply 3-transitive. We shall show that for any triple $(\langle x\rangle, \langle y\rangle, \langle z\rangle)$ of distinct elements of $\mathrm{PG}(1, q)$, there is an $[M] \in \mathrm{PGL}(2, q)$ such that $[M](\langle\binom{1}{0}\rangle) = \langle x\rangle$, $[M](\langle\binom{0}{1}\rangle) = \langle y\rangle$, and $[M](\langle\binom{1}{1}\rangle) = \langle z\rangle$. This implies that $\mathrm{PGL}(2, q)$ is 3-transitive, because if we wish to map $(\langle x\rangle, \langle y\rangle, \langle z\rangle)$ to $(\langle x'\rangle, \langle y'\rangle, \langle z'\rangle)$, then we can use $[M'M^{-1}]$ where $[M]$ maps $(\langle\binom{1}{0}\rangle, \langle\binom{0}{1}\rangle, \langle\binom{1}{1}\rangle)$ to $(\langle x\rangle, \langle y\rangle, \langle z\rangle)$ and $[M']$ maps $(\langle\binom{1}{0}\rangle, \langle\binom{0}{1}\rangle, \langle\binom{1}{1}\rangle)$ to $(\langle x'\rangle, \langle y'\rangle, \langle z'\rangle)$.

Let $(\langle x\rangle, \langle y\rangle, \langle z\rangle)$ be a triple of distinct elements of $\mathrm{PG}(1, q)$, and let $x = \binom{x_1}{x_2}$, $y = \binom{y_1}{y_2}$, and $z = \binom{z_1}{z_2}$. Since $\langle x\rangle$, $\langle y\rangle$ and $\langle z\rangle$ are distinct, there is a unique solution $\binom{\mu}{\lambda}$ with $\mu \neq 0$ and $\lambda \neq 0$ to the following matrix equation.

$$\begin{pmatrix} z_1 & -y_1 \\ z_2 & -y_2 \end{pmatrix} \begin{pmatrix} \mu \\ \lambda \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

If we take

$$M = \begin{pmatrix} x_1 & \lambda y_1 \\ x_2 & \lambda y_2 \end{pmatrix},$$

then it is routine to check that $M\binom{1}{0} = \binom{x_1}{x_2}$, $M\binom{0}{1} = \lambda\binom{y_1}{y_2}$, and $M\binom{1}{1} = \mu\binom{z_1}{z_2}$. Since $\langle x\rangle$ and $\langle y\rangle$ are distinct, $\det(M) \neq 0$, and thus $[M]$ is the required element of $\mathrm{PGL}(2, q)$. This completes the proof that $\mathrm{PGL}(2, q)$ is sharply 3-transitive. □

Theorem 3.4.5. If q is a prime power, then there exists a $3-(q^2+1, q+1, 1)$-design.

Proof We know from Example 3.4.4 that $\mathrm{PGL}(2, q^2)$ is a sharply 3-transitive permutation group acting on $\mathrm{PG}(1, q^2)$. Define $B \subset \mathrm{PG}(1, q^2)$ by $B = \{\langle\binom{x}{y}\rangle \in \mathrm{PG}(1, q^2) : x, y \in \mathbb{F}_q\}$, where $\mathbb{F}_q$ is the subfield of order q in $\mathbb{F}_{q^2}$. It can be seen that $|B| = q+1$ (each subspace in B contains exactly $q-1$ non-zero vectors having both coordinates in $\mathbb{F}_q$, and the total number of such vectors is q^2-1).

Now let $G = \mathrm{PGL}(2, q^2)$ and consider the setwise stabilizer $G_{\{B\}}$ of B in G. It is easy to see that $H = \{[M] \in \mathrm{PGL}(2, q^2) : \text{each entry of } M \text{ is in } \mathbb{F}_q\}$ is a subgroup of $G_{\{B\}}$, and that $H \cong \mathrm{PGL}(2, q)$. It follows that H acts sharply 3-transitively on B. We now show that H is the whole of $G_{\{B\}}$. Suppose $[M] \in G_{\{B\}}$ and let $\langle x\rangle$, $\langle y\rangle$ and $\langle z\rangle$ be distinct elements of B. Since H acts 3-transitively on B, there is an $[M'] \in H$ such that $[M'](\langle x\rangle) = [M](\langle x\rangle)$, $[M'](\langle y\rangle) = [M](\langle y\rangle)$, and $[M'](\langle z\rangle) = [M](\langle z\rangle)$. Since G acts sharply 3-transitively on $\mathrm{PG}(1, q^2)$, this implies $[M] = [M']$. Thus, $[M] \in H$ and we have $H = G_{\{B\}}$. It follows that $|G_{\{B\}}| = q^3 - q$ and so by Theorem 3.4.2, $(\mathrm{PG}(1, q^2), \{[M](B) : [M] \in \mathrm{PGL}(2, q^2)\})$ is a $3-(q^2+1, q+1, 1)$-design. □

The $3-(q^2+1, q+1, 1)$-designs of Theorem 3.4.5 are known as **inversive planes**. It can be shown that these are extensions of the $2-(q^2, q, 1)$-designs constructed in Example 3.4.3, which as we noted earlier are isomorphic to the $2-(q^2, q, 1)$-designs whose blocks are the 1-flats in $\mathrm{AG}(2, q)$ (see Theorem 2.6.4).

3.5 Steiner Systems

Definition 3.5.1. A $t-(v, k, \lambda)$-design with $\lambda = 1$ is called a **Steiner system** and denoted $S(t, k, v)$.

Steiner systems with $t = 2$ where discussed in Section 3.1. Steiner systems with $k = t+1$ are of particular interest, and sometimes this condition is part of the definition of a Steiner system. However, we will use the broader definition given above.

An $S(2, 3, v)$ is a Steiner triple system of order v, and we noted in Section 3.1 that these exist for all $v \equiv 1, 3 \pmod 6$. The next smallest values of $t > 2$ and $k > t$ to consider are $t = 3$ and $k = 4$. Such designs are commonly known as **Steiner Quadruple systems**, and a $S(3, 4, v)$-design is known as a **Steiner Quadruple system of order** v. The existence Steiner Quadruple systems was settled by Hanani in 1960 [32].

Theorem 3.5.2. (Hanani, [32]) There exists a Steiner Quadruple system of order v if and only if $v = 1$ or $v \equiv 2$ or $4 \pmod 6$.

The necessity of $v \equiv 2$ or $4 \pmod 6$ (when $v > 1$) for the existence of a Steiner Quadruple system of order v follows from Theorem 3.2.3. A proof that a Steiner Quadruple system of order v exists whenever $v \equiv 2$ or $4 \pmod 6$ can be found in many textbooks on design theory, for example see [42].

For the case $t = 3$, we have also seen an $S(3, 6, 22)$ as an extension of a projective plane of order 4, and we saw that the only other extendable projective plane is the Steiner triple system $S(2, 3, 7)$, which extends to a Steiner quadruple system $S(3, 4, 8)$. The inversive planes give us an infinite family of Steiner systems with $t = 3$, namely $S(3, q+1, q^2+1)$ systems for each prime power q.

We now consider Steiner systems with $t \geq 4$. Although Keevash's Theorem, Theorem 1.3.2 [37], guarantees the existence of Steiner systems for all sufficiently large orders whenever the obvious necessary conditions are satisfied, only finitely many Steiner systems with $t \geq 4$ have been constructed. All known $S(4, k, v)$ systems extend to $S(5, k+1, v+1)$ systems. The parameters of known $S(5, k, v)$ systems are listed below.

$S(5,6,12)$	$S(5,6,24)$	$S(5,8,24)$	$S(5,7,28)$	$S(5,6,36)$
$S(5,6,48)$	$S(5,6,72)$	$S(5,6,84)$	$S(5,6,108)$	$S(5,6,132)$
$S(5,6,168)$	$S(5,6,244)$			

Below, we list parameter sets for non-trivial $S(2, k, v)$ systems with $v \leq 25$ that exist, together with their extensions. The symbol "X" indicates that the next system in the sequence does not exist, and the symbol "?" indicates that it is unknown whether the next system in the sequence exists [16, 45].

$$S(2,3,7) \to S(3,4,8) \to X$$
$$S(2,3,9) \to S(3,4,10) \to S(4,5,11) \to S(5,6,12) \to X$$
$$S(2,3,13) \to S(3,4,14) \to X$$
$$S(2,3,15) \to S(3,4,16) \to X$$
$$S(2,3,19) \to S(3,4,20) \to ?$$
$$S(2,3,21) \to S(3,4,22) \to S(4,5,23) \to S(5,6,24) \to X$$
$$S(2,3,25) \to S(3,4,26) \to ?$$
$$S(2,4,13) \to X$$
$$S(2,4,16) \to S(3,5,17) \to X$$
$$S(2,4,25) \to S(3,5,26) \to S(4,6,27) \to S(5,7,28) \to ?$$
$$S(2,5,21) \to S(3,6,22) \to S(4,7,23) \to S(5,8,24) \to X$$
$$S(2,5,25) \to S(3,6,26) \to X$$

We now turn our attention to the Steiner systems $S(5, 6, 12)$ and $S(5, 8, 24)$. We noted in Section 1.3 that each of these systems is unique up to isomorphism, and that their automorphism groups are the Mathieu groups M_{12} and M_{24} respectively. There are various methods for constructing $S(5,6,12)$ and $S(5,8,24)$. We briefly discuss just a couple.

In [17], the following constructions, with a very simple description, are given. If we let

$$x = (3\ 4)(6\ 7)(9\ 10)(11/12)$$

and

$$y = (1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9)(10\ 11\ 12),$$

then the group $G = \langle x, y\rangle$ is isomorphic to M_{12}. In Figure 3.1, the first of these two permutations corresponds with the four triangles, and the second permutation corresponds with the four additional edges in the figure. If we let $B = \{1,2,5,8,11,12\}$, indicated by the vertices marked with an asterisk in the figure, then the orbit of B under G forms an $S(5,6,12)$ system.

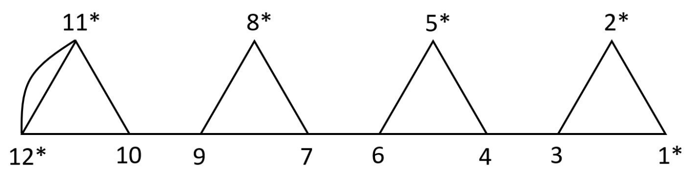

Figure 3.1: Generators for M_{12} and a block of $S(5,6,12)$

For M_{24} and $S(5,8,24)$ we have the following similar construction. If we let

$$x = (1\ 14)(4\ 5)(6\ 7)(8\ 9)(11\ 24)(16\ 17)(18\ 19)(20\ 21)$$

and

$$y = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)(9\ 10\ 1\ 12)(13\ 14\ 15\ 16)(17\ 18\ 19\ 20)(21\ 22\ 23\ 24),$$

then the group $G = \langle x, y\rangle$ is isomorphic to M_{24}. In Figure 3.2, the first of these two permutations corresponds with the six squares, and the second permutation corresponds with the eight additional edges in the figure. If we let $B = \{6,7,8,9,16,17,18,19\}$, indicated by the vertices marked with an asterisk in the figure, then the orbit of B under G forms an $S(5,8,24)$ system.

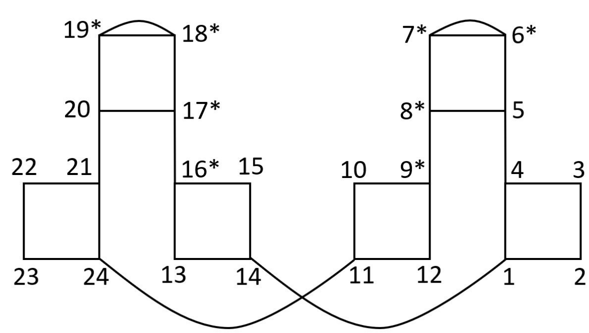

Figure 3.2: Generators for M_{24} and a block of $S(5,8,24)$

We now give a different construction of the Steiner system $S(5, 6, 12)$. First we need to briefly discuss the **projective special linear group** $\mathrm{PSL}(2, q)$. Recall from Section 3.4, that the projective linear group $\mathrm{PGL}(2, q)$ is the quotient group $\mathrm{GL}(2, q)/Z$ where $\mathrm{GL}(2, q)$ is the group of all 2 by 2 invertible matrices over $\mathbb{F}_q$ and Z is the subgroup of scalar matrices in $\mathrm{GL}(2, q)$.

A subgroup of $\mathrm{GL}(2, q)$ is the **special linear group** $\mathrm{SL}(2, q)$ which consists of all 2 by 2 matrices over $\mathbb{F}_q$ that have determinant 1. The **projective special linear group** $\mathrm{PSL}(2, q)$ is the quotient group $\mathrm{SL}(2, q)/SZ$ where SZ is the subgroup of scalar matrices with determinant 1.

Note that if $\lambda \in \mathbb{F}_q \setminus \{0\}$ and $M \in \mathrm{GL}(2, q)$, then $\det(\lambda M) = \lambda^2 \det(M)$. If q is even, then the only root of unity in $\mathbb{F}_q$ is 1, and $\{\lambda^2 : \lambda \in \mathbb{F}_q \setminus \{0\}\} = \mathbb{F}_q \setminus \{0\}$. If q is odd, then 1 and -1 are the only roots of unity in $\mathbb{F}_q$ and $\{\lambda^2 : \lambda \in \mathbb{F}_q \setminus \{0\}\}$ is the set of quadratic residues of $\mathbb{F}_q \setminus \{0\}$ and has cardinality $\frac{q-1}{2}$. It follows from these facts that when q is even, there is exactly one matrix $A \in \mathrm{SL}(2, q)$ in each $[M] \in \mathrm{PGL}(2, q)$. When q is odd, half of the $[M] \in \mathrm{PGL}(2, q)$ have two matrices $A, -A \in \mathrm{SL}(2, q)$, and the other half have no matrices in $\mathrm{SL}(2, q)$. Recall that the elements of $\mathrm{PGL}(2, q)$ are equivalence classes $[M]$ consisting of the non-zero scalar multiples of M.

In view of the remarks in the preceding paragraph, when q is even we have $\mathrm{SL}(2, q) \cong \mathrm{PSL}(2, q) \cong \mathrm{PGL}(2, q)$. When q is odd $\mathrm{PSL}(2, q)$ is a normal subgroup of index 2 in $\mathrm{PGL}(2, q)$. (When q is odd, $|\mathrm{SL}(2, q)| = |\mathrm{PGL}(2, q)| = 2|\mathrm{PSL}(2, q)|$, but $SL(2, q) \not\cong \mathrm{PGL}(2, q)$; $\mathrm{SL}(2, q)$ has $\mathrm{PSL}(2, q)$ as a quotient group, but not as a subgroup).

The automorphism group of $S(5, 6, 12)$ is the Mathieu group M_{12}, and M_{12} has a subgroup isomorphic to the projective special linear group $\mathrm{PSL}(2, 11)$. The orbit in $\mathrm{PSL}(2, 11)$ of the following block B yields the 132 blocks of $S(5, 6, 12)$.

$$B = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 1 \end{pmatrix}, \begin{pmatrix} 5 \\ 1 \end{pmatrix}, \begin{pmatrix} 9 \\ 1 \end{pmatrix} \right\}$$

A few comments on this:

- The group M_{12} is the full automorphism group of $S(5, 6, 12)$. It acts sharply 5-transitively on the points, and transitively on the blocks.

- Since $|M_{12}| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$, and the orbit of B under M_{12} has $\frac{\binom{12}{5}}{6} = 132$ blocks, the stabilizer in M_{12} of B has order $10 \cdot 9 \cdot 8 = 6!$. Thus, the stabilizer in M_{12} of B is the symmetric group S_6.

- The group $\mathrm{PSL}(2, 11)$ acts 2-transitively on the points of $S(5, 6, 12)$ and transitively on the blocks.

- The group $\mathrm{PSL}(2, 11)$ has order $\frac{12 \cdot 11 \cdot 10}{2} = 660$. The 5-subsets of points, which form a single orbit under M_{12}, split into six orbits under $\mathrm{PSL}(2, 11)$. Under $\mathrm{PSL}(2, 11)$, each 5-subset of points has stabilizer $\mathbb{Z}_5$ and an orbit of length $\frac{660}{5} = 132$. The six 5-subsets of B are from six distinct orbits of 5-subsets under $\mathrm{PSL}(2, 11)$.

3.6 Baranyai's Theorem

The set of all k-element subsets of a v-set form the blocks a t-$(v, k, 1)$-design with $t = k$. Conversely, if $t = k$, then the blocks of a t-$(v, k, 1)$-design are all the k-element subsets of a v-set. Although these designs are trivial, constructing resolvable k-$(v, k, 1)$-designs is an interesting problem.

In the case $k = 2$, a resolvable k-$(v, k, 1)$-design is equivalent to a 1-factorisation of K_v. We can think of a 1-factorisation of K_v as a partition of the 2-element subsets of a v-set V such that each part is partition of V. In general, one may ask for a partition of the k-element subsets of a v-set V such that each part is a partition of V. Baranyai's Theorem addresses this question.

In this section we prove Baranyai's Theorem. It is really a result about edge-colourings of complete hypergraphs, and is best presented in this setting. A **hypergraph** H consists of a vertex set $V(H)$, an edge set $E(H)$, and a function f which assigns a non-empty subset of V to each edge in $E(H)$. For each edge $e \in E(H)$, the vertices in $f(e)$ are called the **endpoints** of e, and a vertex x is said to be **incident** with an edge e if and only if x is an endpoint of e. Thus, an ordinary graph is a hypergraph in which each edge has exactly two endpoints (or one end-point in the case of a loop).

A hypergraph is **simple** if no two distinct edges have the same endpoints, and is k-*uniform* if $|f(e)| = k$ for each edge e. In a simple hypergraph, the endpoints of an edge uniquely identify the edge, and it is common to refer to the set of endpoints of an edge as the edge itself (for example, the edge $\{x, y\}$).

The **degree** $\deg(x)$ of a vertex x in a hypergraph is the number of edges having x as an endpoint. A hypergraph in which each vertex has degree d is said to be **d-regular** or **regular of degree d**. A d-regular spanning subhypergraph (a hypergraph H' is a subhypergraph of a hypergraph H if $V(H') \subseteq V(H)$ and $E(H') \subseteq E(H)$, and H' is **spanning** if $V(H') = V(H)$) is called a **d-factor**, and a decomposition into d-factors is called a **d-factorisation**. A hypergraph is **almost regular** if $|\deg(x) - \deg(y)| \leq 1$ for any two vertices x and y. The **complete k-uniform hypergraph of order v** has a vertex set V of cardinality v and each k-subset of V is an edge.

An **edge-colouring** of a hypergraph H is an assignment of colours to its edges. More formally, an **edge-colouring** of a hypergraph H is a function $\gamma : E(H) \mapsto S$ where S is some set, called the colour set. If $|S| = s$, then γ is an **s-edge-colouring** of H. An edge-colouring is **proper** if for each vertex x, the edges having x as an endpoint are assigned distinct colours. If γ is an s-edge-colouring of a hypergraph H with colours $c_1, c_2, \ldots, c_s$, then the **graph induced by colour class i** has vertex set $V(H)$ and edge set $\{e \in E(H) : \gamma(e) = c_i\}$, and is denoted by H_i. It is clear that a proper d-edge-colouring of a d-regular hypergraph H is equivalent to a 1-factorisation of H.

An edge-colouring of a hypergraph H is **almost regular** if the graph induced by each colour class is almost regular. Equivalently, an edge-colouring of a hypergraph H is almost regular if for any two vertices x and y, and any colour c, the number of edges of colour c incident with x differs from the number of edges of colour c incident with y by at most 1.

We are now ready to present Baranyai's Theorem.

Theorem 3.6.1. If $m_1 + m_2 + \cdots + m_t = \binom{v}{k}$, then there is an almost regular t-edge-colouring of the complete k-uniform hypergraph of order v with colours $c_1, c_2, \ldots, c_t$ such that for $i = 1, 2, \ldots, t$, the number of edges of colour c_i is m_i.

Proof Let K be a complete k-uniform hypergraph of order v, and let γ be an arbitrary assignment of colours $c_1, c_2, \ldots, c_t$ to the edges of K such that for $i = 1, 2, \ldots, t$, the number of edges assigned colour c_i is m_i. The edge-colouring γ exists because the number of edges is $\binom{v}{k}$ and $m_1 + m_2 + \cdots + m_t = \binom{v}{k}$. If γ is almost regular, then we are finished. Otherwise, there exists a colour c and vertices $\alpha, \beta \in V(K)$

such that the number of edges of colour c incident with α differs from the number of edges of colour c incident with β by at least 2.

We construct an auxiliary multigraph G, possibly containing loops, with vertex set $\{c_1, c_2, \ldots, c_t\}$ and edge set given by adding an edge $e_S = \{\gamma(S \cup \{\alpha\}), \gamma(S \cup \{\beta\})\}$ for each $(k-1)$-subset S of $V(K) \setminus \{\alpha, \beta\}$ (e_S is a loop if the edges $S \cup \{\alpha\}$ and $S \cup \{\beta\}$ are the same colour).

It is easily shown that the edges of any multigraph can be oriented such that $|\text{indeg}(x) - \text{outdeg}(x)| \leq 1$ for each vertex x. Give the edges of G such an orientation and define a new edge-colouring γ^* of K as follows.

- For each edge e of K containing neither α nor β, $\gamma^*(e) = \gamma(e)$.
- For each edge e of K containing both α and β, $\gamma^*(e) = \gamma(e)$.
- For each $(k-1)$-subset S of $V(K) \setminus \{\alpha, \beta\}$, there is an edge e_S in G and we define $\gamma^*(S \cup \{\alpha\}) = c_i$ and $\gamma^*(S \cup \{\beta\}) = c_j$ where c_i and c_j are the endpoints of e_S, and e_S is oriented from c_i to c_j.

Notice that the only difference between γ and γ^* is that for each $(k-1)$-subset S of $V(K) \setminus \{\alpha, \beta\}$, the colours of the two edges $S \cup \{\alpha\}$ and $S \cup \{\beta\}$ may have been interchanged. Thus, it is clear that for $i = 1, 2, \ldots, t$, the total number of edges assigned colour c_i is the same for γ and γ^*, and that for each vertex $x \in V(K) \setminus \{\alpha, \beta\}$, the number of edges incident with x and assigned colour c_i is the same for γ and γ^*.

However, for $i = 1, 2, \ldots, t$, in γ^* the number of edges of colour c_i incident with α equals $\text{outdeg}_G(c_i)$ plus the number of edges of colour c_i that have both α and β as endpoints, and the number of edges of colour c_i incident with β equals the $\text{indeg}(c_i)$ plus the number of edges of colour c_i that have both α and β as endpoints. Thus for $i = 1, 2, \ldots, t$, it follows from $|\text{indeg}(c_i) - \text{outdeg}(c_i)| \leq 1$ that in γ^* the number of edges of colour c_i incident with α differs from the number of edges of colour c_i incident with β by at most one. The required colouring can thus be obtained by repeating the above-described procedure. For each colour c_i, the procedure is applied for various pairs of vertices until the graph induced by colour class i is almost regular. □

The following result is an immediate consequence of Baranyai's Theorem.

Theorem 3.6.2. The set of all k-element subsets of a set V can be partitioned so that each part is a partition of V if and only if k divides $|V|$.

Proof The condition that k divides $|V|$ is obviously necessary. To prove that is it sufficient, let $v = |V|$ and apply Theorem 3.6.1 with $t = \binom{v-1}{k-1}$ and $m_i = \frac{v}{k}$ for $i = 1, 2, \ldots, t$. Note that $\frac{v}{k}\binom{v-1}{k-1} = \binom{v}{k}$. The colour classes of the resulting t-edge-colouring define the required partition of the k-element subsets of V. □

In the context of t-designs, Theorem 3.6.2 says that the complete design on v points with block size k is resolvable. It is a resolvable k-$(v, k, 1)$-design. In the language of hypergraphs, Theorem 3.6.2 says that the complete k-uniform hypergraph of order v has a 1-factorisation (or equivalently a proper $\binom{v-1}{k-1}$-edge-colouring) if and only if k divides v.

Chapter 4

Graph Symmetry

4.1 Vertex-Transitive and s-Arc-Transitive Graphs

Definition 4.1.1. Let X be a graph with vertex set $V(X)$ and edge set $E(X)$. An **automorphism** of X is a permutation f of $V(X)$ such that $uv \in E(X)$ if and only if $f(u)f(v) \in E(X)$. The set of all automorphisms of X is called the (full) **automorphism group** of X and is denoted by $\mathrm{Aut}(X)$. Any subgroup of $\mathrm{Aut}(X)$ is an automorphism group of X.

It is an easy exercise to verify that $\mathrm{Aut}(X)$ is indeed a group. When we talk about an automorphism group acting on a graph X, we are talking about $\mathrm{Aut}(X)$ as a permutation group acting on the vertex set $V(X)$. However, any automorphism group of a graph has a natural induced action on other elements/structures within the graph. For example, the induced action of $\mathrm{Aut}(X)$ on the set $E(X)$ of edges of X is given by

$$g(xy) = g(x)g(y)$$

for all $g \in \mathrm{Aut}(X)$ and all $xy \in E(X)$. It can be checked that this induced action is indeed a homomorphism from $\mathrm{Aut}(X)$ into $\mathrm{Sym}(E(X))$.

The induced action of $\mathrm{Aut}(X)$ on the subgraphs of X is given by defining $g(Y)$ to be the graph with vertex set

$$V(g(Y)) = g(V(Y)) = \{g(x) : x \in V(Y)\}$$

and edge set

$$E(g(Y)) = g(E(Y)) = \{g(x)g(y) : xy \in E(Y)\}$$

for each subgraph Y of X and each $g \in \mathrm{Aut}(X)$. It is clear that if Y is any subgraph of X and $g \in \mathrm{Aut}(X)$, then $Y \cong g(Y)$. So it makes sense to talk about the induced action of $\mathrm{Aut}(X)$ on the set of subgraphs of X that are isomorphic to a given subgraph, for example the set of 5-cycles of X.

Note that a graph is an incidence structure where the vertices are the points, the edges are the lines, and each edge/line contains exactly two points. For example, the 4-cycle (a, b, c, d) is an incidence structure with point set $P = \{1, 2, 3, 4\}$, line set $\{e_1, e_2, e_3, e_4\}$, and incidence relation $I = \{(a, e_1), (b, e_1), (b, e_2), (c, e_2), (c, e_3), (d, e_3), (d, e_4), (a, e_4)\}$.

Definition 4.1.2. A graph is **vertex-transitive** if it has a transitive automorphism group.

Definition 4.1.3. A graph X is **edge-transitive** if the induced action of $\mathrm{Aut}(X)$ on the edge set of X is transitive.

Definition 4.1.4. In a graph, an **s-arc** is a directed walk $v_0, v_1, \ldots, v_s$ such that v_i and v_{i+2} are distinct for $i = 0, 1, \ldots, s-2$.

Observe that for a graph X, there is a natural induced action of $\mathrm{Aut}(X)$ on the set of s-arcs of X. For each $g \in \mathrm{Aut}(X)$ and each s-arc $v_0, v_1, \ldots, v_s$ in X, we have $g(v_0, v_1, \ldots, v_s) = g(v_0), g(v_1), \ldots, g(v_s)$.

Definition 4.1.5. A graph X is **s-arc-transitive** if it contains at least one s-arc and $\mathrm{Aut}(X)$ acts transitively on the set of s-arcs of X. The term **arc-transitive** may be used instead of 1-arc-transitive.

The term 0-arc-transitive is equivalent to vertex-transitive. Observe that if X is s-arc-transitive, then it is not necessarily $(s-1)$-arc-transitive. For example, consider the 5-star $K_{1,5}$, which has one vertex of degree 5 that is joined to five vertices of degree 1. This graph is 2-arc-transitive, but not 1-arc-transitive. However, it can be shown that any s-arc-transitive graph that is not a tree is s'-arc-transitive for $0 \leq s' \leq s$.

Theorem 4.1.6. A connected graph X is arc-transitive if and only if X is vertex-transitive and for every vertex u in X, the stabilizer $\mathrm{Aut}(X)_u$ of u acts transitively on the neighbours of u.

Proof Suppose X is arc-transitive. If u and v are any two vertices of X, then, since X is connected, there exist arcs (u, u') and (v, v'), and, since X is arc-transitive, there exists $f \in \mathrm{Aut}(X)$ such that $f : (u, u') \mapsto (v, v')$. Thus, $f(u) = v$ and so X is vertex-transitive. Also, if u is any vertex of X and S is the set of neighbours of u, then for any $v, v' \in S$ there exists $f \in \mathrm{Aut}(X)$ such that $f : (u, v) \mapsto (u, v')$ (because X is arc transitive). So $f \in \mathrm{Aut}(X)_u$ and $f(v) = v'$. Thus, $\mathrm{Aut}(X)_u$ acts transitively on the neighbours of u.

Now suppose X is vertex-transitive and for every vertex u in X, $\mathrm{Aut}(X)_u$ acts transitively on the neighbours of u. Let (u, u') and (v, v') be two arcs of X. Since X is vertex-transitive, there exists $f \in \mathrm{Aut}(X)$ such that $f(u) = v$. Note that $f(u')$ is a neighbour of v. Since $\mathrm{Aut}(X)_v$ acts transitively on the neighbours of v, there exists $g \in \mathrm{Aut}(X)_v$ such that $g(f(u')) = v'$. Thus, $g \circ f \in \mathrm{Aut}(X)$ and $g \circ f : (u, u') \mapsto (v, v')$ and so X is arc-transitive. □

Recall that **girth** of a graph is the length of a shortest cycle, or infinity if the graph has no cycles.

Theorem 4.1.7. If X is s-arc-transitive and has degree at least 3, then X has girth at least $2s-2$.

Proof Let X be an s-arc-transitive graph of degree at least 3. If $s \in \{0, 1, 2\}$, then $2s - 2 \leq 2$ and so the result holds (because every graph has girth at least 3). So we assume $s \geq 3$. Also, since X has degree at least 3, X has at least one cycle. Let $\gamma \geq 3$ be the girth of X, and let $(u_1, u_2, \ldots, u_\gamma)$ be a γ-cycle in X. Since $(u_1, u_2, \ldots, u_\gamma)$ is a shortest cycle, and since X has degree at least 3, for each $i = 1, 2, \ldots, \gamma$ there exists a vertex v_i such that $v_i \sim u_i$ and $v_i \notin \{u_1, u_2, \ldots, u_\gamma\}$.

Since the γ-arc $u_1, u_2, \ldots, u_\gamma, v_\gamma$ cannot be mapped (by an automorphism of X) to the γ-arc $u_1, u_2, \ldots, u_\gamma, u_1$ (one is a path and the other is a cycle), X is not γ-arc-transitive. So $s < \gamma$. Consider the two s-arcs $u_1, u_2, \ldots, u_s, u_{s+1}$ and $u_1, u_2, \ldots, u_s, v_s$. Since X is s-arc-transitive, there exists $f \in \mathrm{Aut}(X)$ such that $f(u_i) = u_i$ for $i = 1, 2, \ldots, s$ and $f(u_{s+1}) = v_s$. Since $f(u_1) = u_1$ and $f(u_s) = u_s$, f maps the path $u_s, u_{s+1}, \ldots, u_\gamma, u_1$, which has length $\gamma - s + 1$, to another path of length $\gamma - s + 1$ from u_s to u_1. These two paths are not identical because $f(u_{s+1}) = v_s$ and $v_s \notin \{u_s, u_{s+1}, \ldots, u_\gamma, u_1\}$. Thus, the union of these two paths contains a cycle of length at most $2\gamma - 2s + 2$. So $2\gamma - 2s + 2 \geq \gamma$ and it follows that $\gamma \geq 2s - 2$. $\square$

Recall that in a graph X, an **x, y-path** is a sequence

$$x = x_0, e_1, x_1, e_2, x_2, \ldots, x_{t-1}, e_t, x_t = y$$

where $x_0, x_1, \ldots, x_t$ are distinct vertices of X, $e_1, e_2, \ldots, e_t$ are distinct edges of X, and e_i has endpoints x_{i-1} and x_i for $i = 1, 2, \ldots, t$. The **distance** between two vertices x and y, denoted $d(x, y)$, is the number of edges in a shortest x, y-path. The **diameter** of a graph X, denoted **diam(X)** is the largest distance between two vertices of X. That is, $\mathrm{diam}(X) = \max\{d(x, y) : x, y \in V(X)\}$.

Theorem 4.1.8. If X is a connected s-arc-transitive graph and has girth $2s-2$, then it has diameter $s - 1$.

Proof Let X be a connected s-arc-transitive graph that has girth $2s - 2$. Observe that for any two vertices u and v in a $(2s-2)$-cycle, a shortest path from u to v is in the cycle; otherwise, there would be a cycle of length less than $2s - 2$.

Thus, X has diameter at least $s - 1$ because opposite vertices in a $(2s - 2)$-cycle are at this distance. Suppose for a contradiction that the diameter of X is greater than $s - 1$. Then, since X is connected, there exist vertices u and v such that $d(u, v) = s$. Consider a path P of length s from u to v. Since P is an s-arc and X is s-arc-transitive, there is an automorphism mapping P to an s-arc in a $(2s - 2)$-cycle. Thus, P also lies in a $(2s - 2)$-cycle. But this implies that $d(u, v) \leq s - 1$, a contradiction. We conclude that X has diameter $s - 1$. $\square$

The following theorem was proved by Tutte in 1947 [56]. Recall that a **cubic** graph is a 3-regular graph.

Theorem 4.1.9. [Tutte, 1947 [56]] If a cubic graph is s-arc-transitive, then $s \leq 5$. Furthermore, for $0 \leq s \leq 5$ there exists a cubic graph that is s-arc-transitive but not $(s + 1)$-arc-transitive.

Examples for the second part of Tutte's theorem are:-

- The graph of the triangular prism ($\cong \mathrm{Cay}(\mathbb{Z}_6, \{2, 3, 4\})$) is 0-arc-transitive (vertex-transitive) but not 1-arc-transitive (arc-transitive).
- The graph known as F26A is 1-arc-transitive but not 2-arc-transitive.
- The graphs K_4, the graph of the 3-cube, and the graph of the dodecahedron are 2-arc-transitive but not 3-arc-transitive.

- The graphs $K_{3,3}$, the Petersen graph, the Pappus graph, the Desargues graph, and the Coxeter graph are 3-arc-transitive but not 4-arc transitive.
- The Heawood graph is 4-arc-transitive but not 5-arc-transitive.
- The Tutte-Coxeter graph is 5-arc-transitive but not 6-arc-transitive.

For graphs of arbitrary degree, we have the following theorem of Weiss from [59] (its proof depends on the classification of finite simple groups).

Theorem 4.1.10. [Weiss, 1961 [59]] If a graph of degree greater than 2 is s-arc-transitive, then $s \leq 7$.

The smallest known 7-arc-transitive graph of degree greater than 2 is a 4-regular graph with 728 vertices [18].

4.2 Cayley Graphs

Definition 4.2.1. Let G be a group and let S be a subset of G such that $1 \notin S$, and $s \in S$ if and only if $s^{-1} \in S$. The **Cayley graph on G with connection set S** has vertex set G, and edge set $\{gh : g, h \in G, g^{-1}h \in S\}$, and is denoted $\mathrm{Cay}(G; S)$.

Theorem 4.2.2. Let $\mathrm{Cay}(G; S)$ be a Cayley graph and let f_g denote left-multiplication by the element $g \in G$. Then f_g is an automorphism of $\mathrm{Cay}(G; S)$ and the group $G^* = \{f_g : g \in G\}$ has a regular action on $\mathrm{Cay}(G; S)$. Thus, $\mathrm{Cay}(G; S)$ is vertex-transitive.

Proof Let $g, h_1, h_2 \in G$. Since

$$h_1^{-1}h_2 = h_1^{-1}g^{-1}gh_2 = (gh_1)^{-1}(gh_2) = (f_g(h_1))^{-1}(f_g(h_2)),$$

we have $h_1^{-1}h_2 \in S$ if and only if $(f_g(h_1))^{-1}(f_g(h_2)) \in S$. That is, h_1h_2 is an edge of $\mathrm{Cay}(G; S)$ if and only if $f_g(h_1)f_g(h_2)$ is an edge of $\mathrm{Cay}(G; S)$. Thus, f_g is an automorphism of $\mathrm{Cay}(G; S)$.

For arbitrary $h_1, h_2 \in G$, if we let $g = h_2h_1^{-1}$, then we have $f_g(h_1) = gh_1 = h_2h_1^{-1}h_1 = h_2$. Thus, G^* acts transitively on $\mathrm{Cay}(G; S)$. Finally, if $f_g(h) = f_{g'}(h)$, then $gh = g'h$ which implies $g = g'$. So the action of G^* is regular. □

The following theorem was proved by Sabidussi [47].

Theorem 4.2.3. A graph X is a Cayley graph if and only if $\mathrm{Aut}(X)$ has a regular subgroup.

Proof The group G^* defined in Theorem 4.2.2 is a regular subgroup of the automorphism group of any Cayley graph on G. This establishes that if X is a Cayley graph, then $\mathrm{Aut}(X)$ has a regular subgroup.

Now let X be a graph and suppose $\mathrm{Aut}(X)$ has a regular subgroup G. Arbitrarily choose a fixed vertex u of X, and define a function $f : G \to V(X)$ by $f(g) = g(u)$ for each $g \in G$. Since G is regular, f is a bijection. Let $S = \{f^{-1}(v) : uv \text{ is an edge of } X\}$. We verify that f is an isomorphism from $\mathrm{Cay}(G;S)$ to X. We need to show that $g_1 \sim g_2$ in $\mathrm{Cay}(G;S)$ if and only if $f(g_1) \sim f(g_2)$ in X. We have

$$\begin{array}{rcll}
g_1 \sim g_2 \text{ in } \mathrm{Cay}(G;S) & \leftrightarrow & g_1^{-1}g_2 \in S & \text{(definition of Cayley graph)} \\
& \leftrightarrow & f^{-1}(f(g_1^{-1}g_2)) \in S & \\
& \leftrightarrow & u \sim f(g_1^{-1}g_2) \text{ in } X & \text{(definition of } S\text{)} \\
& \leftrightarrow & u \sim g_1^{-1}g_2(u) \text{ in } X & \text{(definition of } f\text{)} \\
& \leftrightarrow & g_1(u) \sim g_1(g_1^{-1}g_2(u)) \text{ in } X & \text{(since } g_1 \text{ is an automorphism)} \\
& \leftrightarrow & g_1(u) \sim g_2(u) \text{ in } X & \\
& \leftrightarrow & f(g_1) \sim f(g_2) \text{ in } X & \text{(definition of } f\text{)}
\end{array}$$

□

Cubes:

The k-dimensional vector space over $\mathbb{Z}_2$ is denoted by $\mathbb{Z}_2^k$. The **k-cube**, denoted Q_k, is the Cayley graph $\mathrm{Cay}(\mathbb{Z}_2^k; \{e_1, e_2, \ldots, e_k\})$ where for $i = 1, 2, \ldots, k$, e_i has 1 as its i-th coordinate and every other coordinate is 0. Thus, Q_k has vertex set $\mathbb{Z}_2^k$ and two vertices are adjacent if and only if they differ in exactly one coordinate.

Theorem 4.2.4. For each $v \in \mathbb{Z}_2^k$, define $f_v : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ by $f_v : x \mapsto x + v$ for each $x \in \mathbb{Z}_2^k$. Then $G = \{f_v : v \in \mathbb{Z}_2^k\} \leq \mathrm{Aut}(Q_k)$ and G has a regular action on Q_k. Furthermore, the stabilizer in $\mathrm{Aut}(Q_k)$ of each vertex is isomorphic to S_k and $|\mathrm{Aut}(Q_k)| = 2^k k!$.

Proof It is easy to see that f_v is an automorphism of Q_k because x and y have equal i-th coordinates if and only if $x + v$ and $y + v$ have equal i-th coordinates. For any two vertices x and y, we have $f_{x+y}(x) = x + x + y = y$. Thus, $G = \{f_v : v \in \mathbb{Z}_2^k\}$ acts transitively on Q_k, and since $|G| = |\mathbb{Z}_2^k|$ this action is regular.

For each $\theta \in \mathrm{Sym}(k)$ let θ' denote the permutation of $\mathbb{Z}_2^k$ obtained by applying θ to the coordinates of each vector. It is clear that each θ' is an automorphism of Q_k because x and y differ only in the i-th coordinate if and only if $\theta'(x)$ and $\theta'(y)$ differ only in the $\theta(i)$-th coordinate. Let $H = \{\theta' : \theta \in \mathrm{Sym}(k)\}$, so $H \cong S_k$. Since each $\theta' \in H$ fixes 0, H is a subgroup of the stabilizer $\mathrm{Aut}(Q_k)_0$ of 0. We now show that $H = \mathrm{Aut}(Q_k)_0$.

For $i = 0, 1, \ldots, k$, let V_i denote the set of vertices at distance i from 0, and let e_i denote the vertex of V_1 whose i-th coordinate is 1. Note that $u \in V_i$ if and only if the number of coordinates of u equal to 1 is i.

Below we show that the pointwise stabilizer of $V_0 \cup V_1$ is trivial. This implies that $H = \mathrm{Aut}(Q_k)_0$. To see this, let $f \in \mathrm{Aut}(Q_k)_0$. Then f induces a permutation of V_1. Thus, since $H \cong S_k$, there is an automorphism $h \in H$ such that $h \circ f$ fixes $V_0 \cup V_1$ pointwise. So if we show that the pointwise stabilizer of $V_0 \cup V_1$ is trivial, then $h \circ f$ is the identity, which implies that f is the inverse of h. This means that $f \in H$, and so $\mathrm{Aut}(Q_k)_0 = H$.

We now show that the pointwise stabilizer of $V_0 \cup V_1$ is trivial. Suppose $u \in V_t$ where $t \geq 2$. So u has at least two coordinates that are 1. Let coordinates i and j of u be 1 (where $i \neq j$). Then $u + e_i, u + e_j \in V_{t-1}$, $u + e_i + e_j \in V_{t-2}$ and $(u, u + e_i, u + e_i + e_j, u + e_j)$ is a 4-cycle in Q_k. Moreover,

u and $u+e_i+e_j$ are the only common neighbours of $u+e_i$ and $u+e_j$. Thus, any automorphism that fixes $V_{t-2} \cup V_{t-1}$ pointwise, also fixes V_t pointwise. It follows by induction on t that the pointwise stabilizer of $V_0 \cup V_1$ is trivial.

We have shown that $H = \mathrm{Aut}(Q_k)_0$. Thus, since Q_k is vertex transitive and $H \cong S_k$, the stabilizer of each vertex is isomorphic to S_k. Finally, since Q_k is vertex transitive with 2^k vertices, and the vertex stabilizer is S_k, it follows from the Orbit-Stabilizer Theorem that $|\mathrm{Aut}(Q_k)| = 2^k k!$. □

4.3 Kneser Graphs and the Erdös-Ko-Rado Theorem

Definition 4.3.1. The **Kneser graph** $\mathcal{K}(n,k)$ has vertices corresponding to the k-element subsets of an n-set, and two vertices are adjacent if and only if their corresponding subsets are disjoint.

Theorem 4.3.2. The Kneser graph $\mathcal{K}(n,k)$ is vertex-transitive.

Proof It is easy to see that if the underlying n-set is N, then the symmetric group $\mathrm{Sym}(N)$ acts transitively on the vertices of the graph. □

We shall show that for $k < n/2$, S_n is in fact the full automorphism group of $\mathcal{K}(n,k)$. To do this we use the *Erdös-Ko-Rado Theorem*, and we use the following result to prove it.

Recall that an **independent set** in a graph is a set of vertices, no two of which are adjacent, and that a **clique** is a set of vertices, any two of which are adjacent. An independent set of cardinality k is called an **independent k-set**, and a clique of cardinality k is called a **k-clique**.

Theorem 4.3.3. Let X be a vertex-transitive graph, let V be the vertex set of X, let $W \subseteq V$, and suppose that any independent set in X contains at most k vertices of W. Then any independent set in X has at most $k|V|/|W|$ vertices. Moreover, any independent set in X having $k|V|/|W|$ vertices contains exactly k vertices of W.

Proof Let G be the automorphism group of X and let S be an independent set in X. Let N be the number of ordered pairs (x,g) such that $x \in S$, $g \in G$, and $g(x) \in W$. We evaluate $|N|$ in two ways. First, for each vertex of $x \in S$, and each $y \in W$, there are $|G|/|V|$ automorphisms mapping x to y (see Theorems 1.2.7 and 1.2.8). Thus,

$$|N| = |S| \cdot |W| \cdot |G|/|V| \tag{4.1}$$

Second, for each $g \in G$, since $g(S)$ is an independent set, we have $|g(S) \cap W| \leq k$. So there are at most k points $x \in S$ such that $g(x) \in W$. This is because $x \in S$ and $g(x) \in W$ implies $x \in g^{-1}(g(S) \cap W)$. Thus,

$$|N| \leq k|G| \tag{4.2}$$

Combining (4.1) and (4.2) we have $|S| \leq k|V|/|W|$. It is clear that if $|S| = k|V|/|W|$, then we have $|g(S) \cap W| = k$ for each $g \in G$. In particular, $|S \cap W| = k$. □

Lemma 4.3.4. If $n \geq 2k$, then the largest clique in the Cayley graph $\mathrm{Cay}(\mathbb{Z}_n; \{\pm 1, \pm 2, \ldots, \pm(k-1)\})$ has cardinality k, and if $n > 2k$, then any k-clique is of the form $\{x, x+1, \ldots, x+k-1\}$.

Proof Let $n \geq 2k$. The set $\{0, 1, \ldots, k-1\}$ is a clique of cardinality k. To see that there is no larger clique, observe that the neighbours of 0 can be partitioned into non-adjacent pairs

$$\{1, -(k-1)\}, \{2, -(k-2)\}, \ldots, \{k-1, -1\}.$$

Since at most one vertex from each such pair can be in any clique containing 0, the largest clique containing 0 has cardinality at most k. Since the graph is vertex-transitive, this means that any clique has cardinality at most k.

For convenience in proving the second part of the lemma, we call cliques that are of the form $\{x, x+1, \ldots, x+k-1\}$ *consecutive*, and cliques that are not of this form *non-consecutive*.

Now let $n = 2k+1$ and let S be a k-clique. Thus, S is an independent k-set in the complement of our Cayley graph, namely $\mathrm{Cay}(\mathbb{Z}_n; \{\pm k\})$. But $\mathrm{Cay}(\mathbb{Z}_n; \{\pm k\})$ is a $(2k+1)$-cycle, and it is easy to see that any independent k-set in this $(2k+1)$-cycle is a consecutive k-clique in our Cayley graph. This completes the proof for the case $n = 2k+1$.

To prove the lemma for $n > 2k+1$, suppose for a contradiction that a counter-example exists, and let $n > 2k+1$ be the smallest integer such there exists a non-consecutive k-clique in $\mathrm{Cay}(\mathbb{Z}_n; \{\pm 1, \pm 2, \ldots, \pm(k-1)\})$. Since $n > 2k+1$, there exist vertices x and $x+1$ that are not in the k-clique. Thus, since $(0\,1\,\cdots\,n-1)$ is an automorphism of the graph, there exists a non-consecutive k-clique S in $\mathrm{Cay}(\mathbb{Z}_n; \{\pm 1, \pm 2, \ldots, \pm(k-1)\})$ which does not contain $n-2$ nor $n-1$.

Now delete the vertex $n-1$ (and all its adjacent edges) from the graph. The function f that maps the congruence class of x modulo n to the congruence class of x modulo $n-1$ for $x = 0, 1, \ldots, n-2$ is an isomorphism from the resulting graph to a subgraph of $\mathrm{Cay}(\mathbb{Z}_{n-1}; \{\pm 1, \pm 2, \ldots, \pm(k-1)\})$. Moreover, $f(S)$ is thus a non-consecutive k-clique in $\mathrm{Cay}(\mathbb{Z}_{n-1}; \{\pm 1, \pm 2, \ldots, \pm(k-1)\})$. This contradicts the minimality of n and the lemma is proved. $\square$

In a cyclically ordered n-tuple $(x_0, x_1, \ldots, x_{n-1})$, the set $\{x_i, x_{i+1}, \ldots, x_{i+k-1}\}$, where the subscripts are calculated in $\mathbb{Z}_n$, is called the **k-interval starting at x_i**. A set of k-intervals of $(x_1, x_2, \ldots, x_{n-1})$ is **consecutive** if the the subscripts of the starting points of the k-intervals are an interval of $(0, 1, \ldots, n-1)$. For example,

$$\{6, 7, 1\}, \{7, 1, 2\}, \{1, 2, 3\}, \{2, 3, 4\}$$

are consecutive 3-intervals of $(1, 2, 3, 4, 5, 6, 7)$.

Theorem 4.3.5. If $n \geq 2k$, then any independent set in the Kneser graph $\mathcal{K}(n, k)$ has cardinality at most $\binom{n-1}{k-1}$. Moreover, if $n > 2k$, then the vertices in any independent set of cardinality $\binom{n-1}{k-1}$ correspond to all the k-subsets containing a fixed element of the underlying n-set.

Proof Let the underlying n-set of $\mathcal{K}(n, k)$ be $\mathbb{Z}_n$, and let W be the set consisting of the k-intervals of the cyclically ordered n-tuple $(0, 1, \ldots, n-1)$. Observe that the k-intervals of $(0, 1, \ldots, n-1)$ starting at i and j intersect if and only if ij is an edge of the Cayley graph $\mathrm{Cay}(\mathbb{Z}_n; \{\pm 1, \pm 2, \ldots, \pm(k-1)\})$. Thus, by Lemma 4.3.4,

(a) the largest independent k-subset of W has cardinality k, and

(b) if $n > 2k$, then any k-subset of W corresponding to an independent set consists of k consecutive k-intervals of $(0, 1, \ldots, n)$.

By Theorem 4.3.3 and (a), any independent set of $\mathcal{K}(n,k)$ has at most $k\binom{n}{k}/n = \binom{n-1}{k-1}$ vertices.

Now suppose $n > 2k$ and let S be the set of k-subsets corresponding to an independent set of cardinality $\binom{n-1}{k-1}$ in $\mathcal{K}(n,k)$. By Theorem 4.3.3, S contains exactly k subsets from W, and by (b) these subsets are k consecutive k-intervals of $(0, 1, \ldots, n-1)$. The same result holds for any cyclically ordered n-tuple of the elements of $\mathbb{Z}_n$. That is, S contains k consecutive k-intervals from every cyclically ordered n-tuple of the elements of $\mathbb{Z}_n$.

If for every $A \in S$, every k-subset intersecting A in $k-1$ points is also in S, then it follows that every k-subset is in S, which is a contradiction. Thus, there exist k-subsets $A \in S$ and $B \notin S$ such that $|A \cap B| = k-1$. Let $A = \{a, x_1, x_2, \ldots, x_{k-1}\}$ and let $B = \{b, x_1, x_2, \ldots, x_{k-1}\}$. Since S contains k consecutive k-intervals from every cyclically ordered n-tuple of the elements of $\mathbb{Z}_n$, by considering the cyclically ordered n-tuples of the form $(\ldots, a, y_1, y_2, \ldots, y_{k-1}, b, \ldots)$ where $\{y_1, y_2, \ldots, y_{k-1}\} = \{x_1, x_2, \ldots, x_{k-1}\}$, we see that every k-subset containing a but not b is in S.

Let C be an arbitrary k-subset such that $a \notin C$. Since $n > 2k$, there exists a k-subset D such that $a \in D$, $b \notin D$, and $C \cap D = \emptyset$. But $a \in D$ and $b \notin D$ implies $D \in S$, and so $C \cap D = \emptyset$ implies $C \notin S$. Thus, every k-subset not containing a is not in S. Since $|S| = \binom{n-1}{k-1}$, this implies every k-subset containing a is in S. □

Theorem 4.3.5 is essentially the Erdös-Ko-Rado Theorem, proved in 1961 [23]. It is usually stated in the following form.

Theorem 4.3.6. [Erdös-Ko-Rado Theorem, 1961 [23]] If $n \geq 2k$, then the maximum number of distinct pairwise intersecting k-subsets of an n-set is $\binom{n-1}{k-1}$. Moreover, for $n > 2k$, any set of $\binom{n-1}{k-1}$ distinct pairwise intersecting k-subsets of an n-set consists of all the k-subsets containing a fixed element of the n-set.

Theorem 4.3.5 allows us to determine the full automorphism group of $\mathcal{K}(n,k)$ for $n > 2k$.

Theorem 4.3.7. For $n > 2k$, the full automorphism group of $\mathcal{K}(n,k)$ is S_n.

Proof Consider the induced action θ of S_n on the vertices of $\mathcal{K}(n,k)$. It is clear that the kernel of θ is the identity. That is, θ is faithful, which means that $S_n \cong \mathrm{Im}(\theta) \leq \mathrm{Aut}(\mathcal{K}(n,k))$. We need to show that there are no more automorphisms.

By Theorem 4.3.5, the maximum cardinality of an independent set in $\mathcal{K}(n,k)$ is $\binom{n-1}{k-1}$, and there are exactly n independent sets of cardinality $\binom{n-1}{k-1}$: namely $V_1, \ldots, V_n$ where V_i is the set of vertices corresponding to sets that contain i.

Any automorphism of $\mathcal{K}(n,k)$ permutes $V_1, \ldots, V_n$, so consider the induced action ϕ of $\mathrm{Aut}(\mathcal{K}(n,k))$ on $\{V_1, V_2, \ldots, V_n\}$. It is easy to see that $\mathrm{Im}(\phi) = \mathrm{Sym}(\{V_1, \ldots, V_n\})$, and it follows from the observation that there is exactly one vertex in the intersection of any k of the V_i, and that any vertex occurs in this manner, that $\ker\phi$ is the identity. Thus, by the First Isomorphism Theorem for groups, $\mathrm{Aut}(\mathcal{K}(n,k)) \cong \mathrm{Sym}(\{V_1, \ldots, V_n\}) \cong S_n$. □

4.4 Johnson Graphs

Definition 4.4.1. The **Johnson graph** $\mathcal{J}(n,k)$ has vertices corresponding to the k-subsets of an n-set, and two vertices are adjacent if and only if their corresponding k-subsets intersect in $k-1$ elements.

Theorem 4.4.2. The Johnson graph $\mathcal{J}(n,k)$ is vertex-transitive.

Proof It is easy to see that if the underlying n-set is N, then the symmetric group $\mathrm{Sym}(N)$ acts transitively on the vertices of the graph. □

Lemma 4.4.3. The graphs $\mathcal{J}(n,k)$ and $\mathcal{J}(n,n-k)$ are isomorphic.

Proof Let X be the underlying n-set. The function that maps each vertex of $\mathcal{J}(n,k)$ to its complement in X is an isomorphism. □

If S is a subset of the vertex set of a graph X, then the **induced subgraph on S** is the subgraph of X with vertex set S and with two vertices adjacent if and only if they are adjacent in X. Let X and Y be graphs with vertex sets $V(X)$ and $V(Y)$ and edge sets $E(X)$ and $E(Y)$. The **Cartesian product $X \square Y$** of X and Y is the graph with vertex $V(X) \times V(Y)$ and with (x_1, y_1) joined to (x_2, y_2) if and only if

- $x_1 = x_2$ and y_1 is joined to y_2 in Y; or
- $y_1 = y_2$ and x_1 is joined to x_2 in X.

Lemma 4.4.4. The induced subgraph on the neighbourhood of a vertex of $\mathcal{J}(n,k)$ is isomorphic to $K_{n-k} \times K_k$.

Proof Consider the neighbourhood of the vertex $\{1,2,\dots,k\}$. If we let $V_{i,j} = (\{1,2,\dots,k\} \setminus \{i\}) \cup \{j\}$ where $i \in \{1,2,\dots,k\}$ and $j \in \{k+1, k+2, \dots, n\}$, then the neighbourhood of $\{1,2,\dots,k\}$ is $\{V_{i,j} : i \in \{1,2,\dots,k\}, j \in \{k+1,, k+2, \dots, n\}\}$, the k copies of K_{n-k} have vertex sets

$$\{V_{i,k+1}, V_{i,k+2}, \dots, V_{i,n}\}$$

where $i = 1, 2, \dots, k$, and the $n-k$ copies of K_k have vertex sets

$$\{V_{1,j}, V_{2,j}, \dots, V_{k,j}\}$$

where $j = k+1, k+2, \dots, n$. So the result holds for the neighbourhood of the vertex $\{1,2,\dots,k\}$, and thus it holds for any vertex because $\mathcal{J}(n,k)$ is vertex-transitive. □

Theorem 4.4.5. Let $n \geq 3$ and $1 \leq k \leq n/2$. Then $\mathrm{Aut}(\mathcal{J}(n,k)) \cong \mathrm{Sym}(n)$ if $k < n/2$ and $\mathrm{Aut}(\mathcal{J}(n,k)) \cong \mathrm{Sym}(n) \times \mathbb{Z}_2$ if $k = n/2$.

Proof Let the underlying n-set of $\mathcal{J}(n,k)$ be $\{1,2,\ldots,n\}$. The proof is by induction on k. Since $\mathcal{J}(n,1) \cong K_n$ and $\mathrm{Aut}(K_n) \cong \mathrm{Sym}(n)$, the result holds for $k=1$. Now let $2 \le k \le n/2$. Consider the induced action θ of $\mathrm{Sym}(n)$ on the vertices of $\mathcal{J}(n,k)$. It is clear that the kernel of θ is the identity. That is, θ is faithful, which means that $S_n \cong \mathrm{Im}(\theta) \le \mathrm{Aut}(\mathcal{J}(n,k))$. Let X be the graph whose vertices are the $(n-k+1)$-cliques of $\mathcal{J}(n,k)$ with two $(n-k+1)$-cliques being adjacent if and only if they intersect in exactly one element.

For $k < n/2$, it follows from Lemma 4.4.4 that the $(n-k+1)$-cliques of $\mathcal{J}(n,k)$ are precisely the sets of vertices that contain a given $(k-1)$-subset of $\{1,2,\ldots,n\}$. Observe that the function which maps the clique consisting of sets of vertices containing a given $(k-1)$-set S to the vertex of $\mathcal{J}(n,k-1)$ corresponding to S is an isomorphism from X to $\mathcal{J}(n,k-1)$.

For $k = n/2$, we have the additional $(n-k+1)$-cliques of $\mathcal{J}(n,k)$ corresponding to k-subsets of a given $(k+1)$-subset. None of these $(n-k+1)$-cliques has a single point of intersection with any $(n-k+1)$-clique that is a set of vertices containing a given $(k-1)$-subset. Thus, in the case $k=n/2$, the graph X has a second component (in addition to a component isomorphic to $\mathcal{J}(n,k-1)$) whose vertices are cliques corresponding to k-subsets of a given $(k+1)$-subset. Observe that the function which maps the clique corresponding to the k-subsets of the $(k+1)$-subset S to the vertex of $\mathcal{J}(n,k+1)$ corresponding to S is an isomorphism from this second component of X to $\mathcal{J}(n,k+1)$. Note that for $k=n/2$ we have $\mathcal{J}(n,k+1) \cong \mathcal{J}(n,k-1)$, so X consists of two components, each isomorphic to $\mathcal{J}(n,k-1)$.

Now consider the induced action ϕ of $\mathrm{Aut}(\mathcal{J}(n,k))$ on X. By considering the intersections of $(n-k+1)$-cliques, and the fact that every vertex of $\mathcal{J}(n,k)$ occurs as the single point of intersection of two $(n-k+1)$-cliques, it can be seen that if an automorphism fixes all the vertices of X (that is, the $(n-k+1)$-cliques of $\mathcal{J}(n,k)$), then it fixes all the vertices of $\mathcal{J}(n,k)$. That is, the kernel of ϕ is the identity. Thus, $\mathrm{Aut}(\mathcal{J}(n,k)) \cong \mathrm{Im}(\phi) \le \mathrm{Aut}(X)$.

In the case $k < n/2$, we know that $X \cong \mathcal{J}(n,k-1)$, so by induction $\mathrm{Aut}(X) \cong S_n$, and we have $\mathrm{Aut}(\mathcal{J}(n,k)) \cong S_n$. This completes the proof for $k < n/2$.

Now suppose $k = n/2$. In this case, there is an automorphism ι of $\mathcal{J}(n,k)$ which maps each vertex to its complement. Thus, a subgroup of $\mathrm{Aut}(\mathcal{J}(n,k))$ is isomorphic to $S_n \times \mathbb{Z}_2$. The induced action on X of ι interchanges the two components of X. Thus, each vertex of X has a complementary vertex in the other component of X (the complement of each clique consists of the complements of the k-subsets in the clique).

Now, since the complement of each vertex V of $\mathcal{J}(n,k)$ is the unique vertex at distance k from V, automorphisms of $\mathcal{J}(n,k)$ preserve complements (map pairs of complementary vertices to pairs of complementary vertices). It follows that induced automorphisms of X also preserve complements. Thus, $\mathrm{Aut}(\mathcal{J}(n,k)) \cong \mathrm{Im}(\phi)$ is isomorphic to a subgroup of $\mathrm{Aut}(\mathcal{J}(n,k-1)) \times \mathbb{Z}_2$, and by induction $\mathrm{Aut}(\mathcal{J}(n,k-1)) \times \mathbb{Z}_2$ is isomorphic to $S_n \times \mathbb{Z}_2$. So we have $\mathrm{Aut}(\mathcal{J}(n,k)) \cong S_n \times \mathbb{Z}_2$. □

Overlaps between the families of Cayley, Kneser and Johnson Graphs:

We have seen three families of vertex-transitive graphs; Cayley graphs, Kneser graph and Johnson graphs. It is natural to ask how much overlaps there is between these families. The following two theorems characterise which Kneser graphs and which Johnson graphs are Cayley graphs. The result for Kneser graphs is due to Godsil [26], and the result for Johnson graphs is due to Dobson and Malnič [20].

Theorem 4.4.6. The Kneser graph $\mathcal{K}(n, k)$ is isomorphic to a Cayley graph if and only if

- $k = 1$;
- $k = 2$ and $n \equiv 3 \pmod 4$ is a prime-power;
- $k = 3$ and $n \in \{8, 32\}$; or
- $k \geq n/2$.

Theorem 4.4.7. Let $k \leq n/2$. The Johnson graph $\mathcal{J}(n, k)$ is isomorphic to a Cayley graph if and only if

- $k = 1$;
- $k = 2$ and $n = 4$ or $n \equiv 3 \pmod 4$ is a prime-power; or
- $k = 3$ and $n \in \{8, 32\}$.

This leaves the question of the overlap between Kneser graphs are Johnson graphs, and this is left as an exercise.

4.5 Distance-Transitive Graphs

Definition 4.5.1. A connected graph X is **distance-transitive** if for any vertices u, u', v, v' such that $d(u, u') = d(v, v')$, there exists $g \in \mathrm{Aut}(X)$ such that $g(u) = v$ and $g(u') = v'$. A subgroup $G \leq \mathrm{Aut}(X)$ **acts distance-transitively** on X if for any vertices u, u', v, v' such that $d(u, u') = d(v, v')$, there exists $g \in G$ such that $g(u) = v$ and $g(u') = v'$.

Examples of distance-transitive graphs are cycles, complete graphs, and regular complete bipartite graphs.

Proposition 4.5.2. The k-cube Q_k is distance-transitive.

Proof Suppose $d(u, u') = d(v, v')$. Then (since translation by u and translation by v are automorphisms) $d(0, u+u') = d(u, u') = d(v, v') = d(0, v+v')$. Thus, $u+u'$ and $v+v'$ have the same number of 1's and so there is an automorphism f, corresponding to a coordinate permutation, such that $f(0) = 0$ and $f(u+u') = v+v'$. Applying the automorphisms translation by u, then f, then translation by v, we map $u \mapsto 0 \mapsto 0 \mapsto v$ and $u' \mapsto u+u' \mapsto v+v' \mapsto v'$. Thus, Q_k is distance-transitive. $\square$

Proposition 4.5.3. The Johnson graph $\mathcal{J}(n, k)$ is distance-transitive.

Proof First observe that vertices u and v are at distance i if and only if the k-subsets corresponding to u and v intersect in $k-i$ elements. Thus, if $d(u,u') = d(v,v') = i$ and U, U', V, V' are the k-subsets corresponding to u, u', v, v' respectively, then $|U \cap U'| = |V \cap V'| = k-i$. Thus, there is permutation $f \in \mathrm{Sym}(n)$ such that $f(U \cap U') = V \cap V'$, $f(U \setminus U') = V \setminus V'$, and $f(U' \setminus U) = V' \setminus V$. It follows that $f(u) = v$ and $f(u') = v'$. $\square$

Proposition 4.5.4. Let X be a connected graph and let d be the diameter of X. A group G acts distance-transitively on X if and only if G acts transitively and for each vertex u, the stabilizer G_u has exactly $d+1$ orbits.

Proof Suppose G acts distance-transitively on X. Then G acts transitively. Let u be a vertex. Since the vertices at distinct distances from u are in distinct orbits of G_u, there are at least $d+1$ orbits of G_u. Let $d(u,x) = d(u,y)$. Then there exists $f \in G$ such that $f(u) = u$ and $f(x) = y$ (because G acts distance-transitively). Thus, any two vertices at equal distance from u are in the same orbit of G_u. This means that G_u has at most $d+1$ orbits. So G_u has exactly $d+1$ orbits.

Now suppose G acts transitively and for each vertex u, the stabilizer G_u has exactly $d+1$ orbits. This means that for any vertex u, any two vertices at equal distance from u are in the same orbit of G_u. Let $d(x,x') = d(y,y')$. Since G acts transitively, there exists $f \in G$ such that $f(x) = y$. Since automorphisms preserve distance, $d(y, f(x')) = d(f(x), f(x')) = d(x,x') = d(y,y')$. Thus, $f(x')$ and y' are at equal distance from y and so are in the same orbit of G_y. That is, there exists $g \in G_y$ such that $g(f(x')) = y'$. So we have $g(f(x)) = g(y) = y$ and $g(f(x')) = y'$. Thus, X is distance-transitive. $\square$

Proposition 4.5.5. A connected s-arc-transitive graph with girth $2s-2$ is distance-transitive.

Proof Let X be a connected s-arc-transitive graph with girth $2s-2$ and let $d(u,u') = d(v,v') = i$. There is a path of length i from u to u', and this is an i-arc. Similarly, there is an i-arc from v to v'. By Theorem 4.1.8, X has diameter $s-1$ and so $i \leq s-1$. Since X is s-arc-transitive and $i \leq s-1$, X is also i-arc-transitive. Thus, there is an automorphism mapping $u \mapsto v$ and $u' \mapsto v'$. $\square$

In 1971, Biggs and Smith [8] proved that there are exactly 12 cubic distance-transitive graphs, namely K_4, $K_{3,3}$, Q_3, the Petersen graph, the Heawood graph, the Pappus graph, the graph of the dodecahedron, the Desargues graph, the Coxeter graph, the Tutte-Coxeter graph, the Foster graph, the Biggs-Smith graph.

4.6 Hoffman-Singleton Theorem

Consider the problem of constructing a largest possible graph such that any two vertices are *close* to each other under the constraint that each vertex has a maximum number of neighbours. We need a few definitions in order to state this problem precisely.

Recall that, the diameter of a graph X, denoted $\mathrm{diam}(X)$, is the largest distance between two vertices of X. That is, $\mathrm{diam}(X) = \max\{d(x,y) : x, y \in V(X)\}$.

For given positive integers k and d, construct a graph with maximum degree k and diameter d with the largest possible number of vertices. Any graph with diameter $d = 1$ is complete. We will restrict our attention to the smallest non-trivial case, namely diameter $d = 2$. Thus, we wish to construct, for a given positive integer k, a graph with maximum degree k and diameter $d = 2$ having the maximum number of vertices.

It is an easy exercise to show that if X is a graph with maximum degree k and diameter 2, then the number of vertices in X is at most $1+k^2$, and that any such graph with $1+k^2$ vertices is k-regular. The bound of $1+k^2$ on the number of vertices is known as the **Moore bound** and any graph meeting this bound is known as a **Moore graph**. A similar bound exists for larger diameters and the terms Moore bound and Moore graph also apply. The Hoffman-Singleton Theorem (see Theorem 4.6.2) which was proved in 1960 [34], addresses the problem of the existence of Moore graphs of diameter 2. We first need the following result which will be used in its proof.

Theorem 4.6.1. The adjacency matrix of a connected k-regular graph has eigenvalue k with multiplicity 1.

Proof Let X be a connected k-regular graph, let $v_1, v_2, \ldots, v_n$ be the vertices of X, let A be the adjacency matrix of X, and let 1_n denote the n by 1 vector of 1s. Since each row and each column of A has exactly k 1s (and $n-k$ 0s), we have

$$A\begin{pmatrix}1\\1\\\vdots\\1\end{pmatrix} = k\begin{pmatrix}1\\1\\\vdots\\1\end{pmatrix}$$

and so 1_n is an eigenvector with corresponding eigenvalue k.

Now suppose that

$$x = \begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}$$

is another eigenvector of A with eigenvalue k, let $|x_j| = \max\{|x_1|, |x_2|, \ldots, |x_n|\}$, let $v_{i_1}, v_{i_2}, \ldots, v_{i_k}$ be the neighbours of v_j, and let $S = \{i_1, i_2, \ldots, i_k\}$. Thus, we have $x_{i_1} + x_{i_2} + \cdots + x_{i_k} = kx_j$ and it follows (using $|x_j| = \max\{|x_1|, |x_2|, \ldots, |x_n|\}$) that $x_{i_1} = x_{i_2} = \cdots = x_{i_k} = x_j$.

Applying the same argument for a neighbour $v_{j'}$ of v_j shows that if v_i is any neighbour of $v_{j'}$, then $x_i = x_{j'} = x_j$. Since the graph X is connected, repeating this argument shows that $x_1 = x_2 = \cdots = x_n$. Thus, the any eigenvector corresponding to the eigenvalue k is a scalar multiple of 1_n, which means that k has multiplicity 1. □

Theorem 4.6.2. [Hoffman-Singleton Theorem, 1960 [34]] If there exists a k-regular graph having $1+k^2$ vertices and diameter 2, then $k \in \{2, 3, 7, 57\}$.

Proof Let $n = 1+k^2$, and let X be a k-regular graph having n vertices and diameter 2. We observe some properties of X. Firstly, for any vertex v, the union of all paths of length 2 starting from v is a spanning tree of X. Thus, X has no 3-cycles and no 4-cycles – the shortest cycle in X is a 5-cycle. Also, adjacent vertices have no common neighbours, and any two non-adjacent vertices have exactly one common neighbour.

Let A be the adjacency matrix of X. So A is an n by n matrix where $A_{ij} = 1$ if $v_i \sim v_j$ and $A_{ij} = 0$ if $v_i \not\sim v_j$ for $1 \le i, j \le n$ with $i \ne j$, and $A_{ii} = 0$ for $1 \le i \le n$. Observe that A is symmetric and has exactly k 1's in each row and exactly k 1s in each column.

Now, consider the matrix A^2. Since adjacent vertices of X have no common neighbours, $A^2_{ij} = 0$ if $v_i \sim v_j$ for $1 \le i, j \le n$ with $i \ne j$. Since non-adjacent vertices of X have exactly one common neighbour, $A^2_{ij} = 1$ if $v_i \not\sim v_j$ for $1 \le i, j \le n$ with $i \ne j$. Since X is k-regular, $A^2_{ii} = k$ for $1 \le i \le n$.

Combining the observations from the preceding two paragraphs, we have

$$A^2 + A = \begin{pmatrix} k & 1 & 1 & \cdots & 1 \\ 1 & k & 1 & \cdots & 1 \\ 1 & 1 & k & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & 1 & \cdots & k \end{pmatrix}.$$

That is, $A^2 + A = J + (k-1)I$ where I is the n by n identity matrix and J is the n by n matrix of 1s. Thus,

$$A^2 + A - (k-1)I = J. \tag{4.3}$$

Also, since each row and each column of A has k 1s, we have

$$AJ = JA = kJ. \tag{4.4}$$

Now consider the eigenvalues and eigenvectors of A. We know from Theorem 4.6.1 (and its proof) that 1_n is an eigenvector of A with eigenvalue k. Let v be an eigenvector of A with eigenvalue $\lambda \ne k$. Then $Av = \lambda v$ which implies $JAv = J\lambda v$ and hence by (4.4) $kJv = \lambda Jv$. Since $k \ne \lambda$, this means

$$Jv = 0. \tag{4.5}$$

Starting from (4.3) we obtain

$$\begin{array}{rcll} A^2 + A - (k-1)I &=& J & \\ (A^2 + A - (k-1)I)v &=& Jv = 0 & \quad \text{(by (4.5))} \\ \lambda^2 v + \lambda v - (k-1)v &=& 0 & \\ (\lambda^2 + \lambda - (k-1))v &=& 0 & \\ \lambda^2 + \lambda - (k-1) &=& 0 & \end{array}$$

which means that the eigenvalues of A are k, $-\frac{1}{2} + \frac{1}{2}\sqrt{4k-3}$, and $-\frac{1}{2} - \frac{1}{2}\sqrt{4k-3}$.

Now, let a and b be the multiplicities of the eigenvalues $-\frac{1}{2} + \frac{1}{2}\sqrt{4k-3}$, and $-\frac{1}{2} - \frac{1}{2}\sqrt{4k-3}$ respectively. Since A has eigenvalue k with multiplicity 1 (by Theorem 4.6.1), and since the sum of the eigenvalues of A is the trace $\mathrm{tr}(A)$ of A, we have

$$1 + a + b = n = 1 + k^2 \tag{4.6}$$

and

$$k + a(-\tfrac{1}{2} + \tfrac{1}{2}\sqrt{4k-3}) + b(-\tfrac{1}{2} - \tfrac{1}{2}\sqrt{4k-3}) = 0. \tag{4.7}$$

rearranging (4.7) we obtain

$$k - \tfrac{1}{2}(a+b) + \tfrac{1}{2}(a-b)\sqrt{4k-3} = 0$$

and since (4.6) gives us $a + b = k^2$ and $a - b = 2a - k^2$ we have

$$k - \tfrac{1}{2}k^2 + \tfrac{1}{2}(2a - k^2)\sqrt{4k-3} = 0.$$

Multiplying through by 2 we obtain

$$2k - k^2 + (2a - k^2)\sqrt{4k-3} = 0 \tag{4.8}$$

and rearranging this we have

$$(2a - k^2)\sqrt{4k-3} = k(k-2).$$

Thus, since a and k are integers, we see that either $2a = k^2$ and $k = 2$ or $\sqrt{4k-3}$ is rational. So for $k > 2$, we have $4k-3 = s^2$ for some integer s, which means that $k = \frac{1}{4}(s^2+3)$ and $k^2 = \frac{1}{16}(s^4+6s^2+9)$. Substituting these values for k and k^2 into (4.8) we obtain

$$\tfrac{1}{2}(s^2+3) - \tfrac{1}{16}(s^4+6s^2+9) + 2as - \tfrac{1}{16}(s^4+6s^2+9)s = 0,$$

and it follows that

$$s^5 + s^4 + 6s^3 - 2s^2 + (9 - 32a)s = 15. \tag{4.9}$$

Thus, s divides 15, and so $s \in \{1, 3, 5, 15\}$. This implies (since $4k - 3 = s^2$) that $k \in \{1, 3, 7, 57\}$. Since there is no 1-regular graph of diameter 2, we conclude that $k \in \{2, 3, 7, 57\}$. $\square$

The 5-cycle is the unique Moore graph of diameter 2 and degree 2, the Petersen graph is the unique Moore graph of diameter 2 and degree 3, and the *Hoffman-Singleton graph*, see Section 4.7, is the unique Moore graph of diameter 2 and degree 7. It is unknown whether a Moore graph of diameter 2 and degree 57 exists. Higman (see [13]) has shown that there is no vertex-transitive Moore graph of diameter 2 and degree 57.

4.7 Some Special Graphs

Definition 4.7.1. The **incidence graph** (sometimes called the Levi graph) of an incidence structure (P, L, I) has vertex set $P \cup L$ and edge set given by joining $p \in P$ to $\ell \in L$ if and only if $p \in \ell$.

The Petersen Graph:

The Petersen graph has a vertex for each 2-subset of a 5-set, and two vertices are adjacent if and only if their corresponding 2-subsets are disjoint.

Let P denote the Petersen graph, let the underlying 5-set be $\{1, 2, 3, 4, 5\}$, and denote the vertex corresponding to the 2-subset $\{a, b\}$ by just ab. Clearly, P has 10 vertices and is 3-regular, because $\binom{5}{2} = 10$ and for any vertex ab, there are $\binom{3}{2} = 3$ 2-element subsets of $\{1, 2, 3, 4, 5\} \setminus \{a, b\}$.

Since there is no set of three pairwise disjoint 2-element subsets of $\{1,2,3,4,5\}$, P has no 3-cycles. Two non-adjacent vertices ab and bc of P have a unique common neighbour, namely the vertex corresponding to $\{1,2,3,4,5\} \setminus \{a,b,c\}$. Since non-adjacent vertices in a 4-cycle have two common neighbours, P has no 4-cycles. Since P has no 3-cycles nor 4-cycles, and since $(12, 34, 15, 23, 45)$ (for example) is a 5-cycle, P has girth 5 (recall that the girth of a graph is the length of a shortest cycle, or infinity if the graph has no cycles).

For a contradiction, suppose P has a Hamilton cycle $H = (x_1, x_2, \ldots, x_{10})$. Since H is a 2-regular spanning subgraph of P, the graph $P - E(H)$ is a 1-factor F of P. Since there are no 3-cycles nor 4-cycles in P, the edges in F join vertices that are at distance 4 or 5 in H. Since there are no 4-cycles in P, the five edges of F are not x_1x_6, x_2x_7, x_3x_8, x_4x_9 and x_5x_{10}. Thus, there is at least one edge of F that joins vertices that are at distance 4 in H. Without loss of generality, we can assume that $x_1x_5 \in E(F)$. But then it is not possible to choose the edge of F that is incident with x_6 without forming a 3-cycle or 4-cycle. Hence we conclude that there is no Hamilton cycle in P.

For a contradiction, suppose P has a proper 3-edge colouring. Each colour class is a 1-factor in P, and so the union of two colour classes is a 2-factor in which each cycle has even length. Since there are no 4-cycles and no Hamilton cycles, this is impossible. Thus, P has no proper 3-edge colouring.

The Heawood Graph:

The Heawood graph is the incidence graph of the Fano plane, which has points corresponding the elements of $\mathbb{Z}_7$ and a line $\ell_i = \{0+i, 1+i, 3+i\}$ for each $i \in \mathbb{Z}_7$ (all calculations done in $\mathbb{Z}_7$).

The Heawood graph has 14 vertices, is 3-regular, and has girth 6.

The Pappus Graph:

The Pappus graph is the incidence graph of the Pappus configuration, which has the elements of $\mathbb{Z}_3 \times \mathbb{Z}_3$ as its points, and the orbits under each of the three permutations $(x, y) \mapsto (x+1, y)$, $(x, y) \mapsto (x, y+1)$, $(x, y) \mapsto (x+1, y+1)$, form the lines (all calculations done in $\mathbb{Z}_3 \times \mathbb{Z}_3$).

The Desargues Graph:

The Desargues graph has a vertex for each 2-subset and each 3-subset of a 5-set. There are no edges joining pairs of vertices corresponding to 2-subsets, and no edges joining pairs of vertices corresponding to 3-subsets, and the vertex corresponding to the 2-subset S is joined to the vertex corresponding to the 3-subset T if and only if $S \subseteq T$.

The Graph F26A:

Consider the incidence structure where the points are the elements of $\mathbb{Z}_{13}$, and the lines are $\ell_i = \{0+i, 1+i, 4+i\}$ for each $i \in \mathbb{Z}_{13}$ (all calculations done in $\mathbb{Z}_{13}$). The graph F26A is the incidence graph of this incidence structure.

The Coxeter Graph:

The Coxeter graph can be obtained from the Kneser graph $\mathcal{K}(7,3)$ by deleting a set of 7 vertices whose corresponding 3-subsets form a Fano plane.

The Tutte-Coxeter Graph:

Let S be a 6-set. The vertex set of the Tutte-Coxeter Graph consists of all the 2-subsets of S, and all the partitions of S into 2-subsets. There are no edges joining pairs of 2-subsets, no edges joining pairs of partitions, and each 2-subset is joined to each partition that contains it.

The Hoffman-Singleton Graph:

The Hoffman-Singleton graph was constructed in 1960 [34] and is the unique Moore graph of diameter 2 and degree 7. There are various ways of constructing the Hoffman-Singleton graph. We shall use the following method which is based on the Fano Plane. Recall that the Fano Plane has 7 points and 7 lines, each line is incident with 3 points, each point is incident with 3 lines, for any two points there is a unique line incident with both, and for any two lines there is a unique point incident with both. The lines

$$124 \qquad 235 \qquad 346 \qquad 457 \qquad 561 \qquad 672 \qquad 713$$

form a Fano plane. The automorphism group of the Fano plane has order 168 (it is isomorphic to $\mathrm{PSL}(2,7) \cong \mathrm{PGL}(3,2) \cong \mathrm{PSL}(3,2) \cong \mathrm{GL}(3,2)$) and is a subgroup of A_7.

The 50 vertices of the Hoffman-Singleton graph correspond to the 35 3-subsets of $\{1,2,\ldots,7\}$, which we shall call *triads*, and the 15 copies of the Fano plane in its orbit under the action of A_7 ($\frac{7!/2}{168} = 15$). The edge set of the graph is given by joining vertices corresponding to disjoint triads, and joining a vertex corresponding to a triad to a vertex corresponding to a plane if and only if the triad is a line in the plane.

It can be shown that the Hoffman-Singleton graph has 50 vertices, is 7-regular, has girth 5, and has diameter 2. The Hoffman-Singleton graph is the unique graph with these properties. It is vertex transitive and its automorphism group has order $252,000 = 50 \times 7!$. The stabiliser of a vertex is S_7.

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 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.

[3] P. Adams, D. Bryant and M. Buchanan, Completing partial Latin squares with two filled rows and two filled columns, *Electron. J. Combin.*, **15(1)**, R56, (2008) 26pp.

[4] L. D. Andersen and A. J. W. Hilton, Thank Evans!, *Proc. London Math. Soc. (3)*, **47** (1983) 507–522.

[5] L. D. Andersen, A. J. W. Hilton and E. Mendelsohn, Embedding partial Steiner triple systems, *Proc. London Math. Soc. (3)*, **41** (1980) 557–576.

[6] I. Anderson, Combinatorial Designs: Construction Methods, Wiley, 1990.

[7] L. D. Baumert and D. M. Gordon, On the existence of cyclic difference sets with small parameters, *Fields Inst. Commun.*, **41** Amer. Math. Soc., Providence, RI (2004) 61–68.

[8] N. L. Biggs and D. H. Smith, On trivalent graphs, *Bulletin of the London Mathematical Society* **3** (1971), 155–158.

[9] 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.

[10] R. C. Bose, An affine analogue of Singer's theorem, *J. Indian Math. Soc. (N.S.)*, **6** (1942) 1–15.

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

[12] D. Bryant and B. Maenhaut, Almost regular edge colourings and regular decompositions of complete graphs, *J. Combin. Des.*, **16** (2008) 499–506.

[13] P. Cameron, Permutation Groups, Cambridge University Press, 1999.

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

[15] H. Cohn, A. Kumar, S. D. Miller, D. Radchenko and M. Viazovska, The sphere packing problem in dimension 24 *Annals of Mathematics* **185** (2017), 1017–1033

[16] C. J. Colbourn and R. Mathon, Steiner Systems, in *The CRC Handbook of Combinatorial Designs, 2nd edition* (Eds. C. J. Colbourn, J. H. Dinitz), CRC Press, Boca Raton (2007), 102–110.

[17] M. Conder, Generating the Mathieu groups and associated Steiner systems, *Discrete Math.* **112** (1993), 41–47.

[18] M. Conder, Group actions on graphs, maps and surfaces with maximum symmetry, invited paper in: Groups St Andrews 2001 in Oxford, *London Math. Soc. Lecture Note Series*, vol. **304**, Cambridge University Press, 2003, pp. 63-91.

[19] A. B. Cruse, On embedding incomplete symmetric Latin squares, *J. Combin. Theory Ser. A*, **16** (1974) 18–22.

[20] E. Dobson and A. Malnič, Groups that are transitive on all partitions of a given shape, *J. Algebraic Combin.* **42** (2015), 605–617.

[21] D. Ž. Doković, Hadamard matrices of order 764 exist, *Combinatorica*, **28** (2008) 487–489.

[22] J. Doyen and R. M. Wilson, Embeddings of Steiner triple systems, *Discrete Math.*, **5** (1973) 229–239.

[23] P. Erdös, C. Ko and R. Rado, Intersection theorems for systems of finite sets, *Quarterly Journal of Mathematics*, Oxford. Second Series, **12**, (1961) 313–320.

[24] T. Evans, Embedding incomplete latin squares, *Amer. Math. Monthly*, **67** (1960) 958–961.

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

[26] C. Godsil, More Odd Graph Theory, *Discrete Math.* **32** (1980), 205–207.

[27] D. M. Gordon, The prime power conjecture is true for $n < 2,000,000$, *Electron. J. Combin.*, **1** (1994) R6 7 pages.

[28] J. Hadamard, Résolution d'une question relative aux déterminants, *Bull. des Sciences Math.*, **17** (1893), 240–246.

[29] T. Hales, M. Adams, G. Bauer, D. T. Dang, J. Harrison, T. L. Hoang, C. Kaliszyk, V. Magron, S. McLaughlin, T. T. Nguyen, T. Q. Nguyen, T. Nipkow, S. Obua, J. Pleso, J. Rute, A. Solovyev, A. H. T. Ta, T. N. Tran, D. T. Trieu, J. Urban, K. K. Vu, and R. Zumkeller, A formal proof of the Kepler conjecture, it Forum Math. Pi **5** (2017), e2, 29 pp.

[30] M. Hall, An existence theorem for Latin squares, *Bull. Amer. Math. Soc.*, **51** (1945) 387–388.

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

[32] H. Hanani, On quadruple systems, *Canad. J. Math.*, 12 (1960) 145–157.

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

[34] A. J. Hoffman and R. R. Singleton, On Moore Graphs of Diameter Two and Three, *IBM J. Res. Develop.* **4** (1960), 497–504.

[35] 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.

[36] Y. J. Ionin and T. V. Trung, Symmetric Designs, in *The CRC Handbook of Combinatorial Designs, 2nd edition* (Eds. C. J. Colbourn, J. H. Dinitz), CRC Press, Boca Raton (2007), 110–124.

[37] P. Keevash, The existence of designs, `arXiv:1401.3665`, (2014), 56 pages.

[38] H. Kharaghani and B. Tayfeh-Rezaie, A Hadamard matrix of order 428. *J. Combin. Des.*, **13** (2005), 435–440.

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

[40] D. König, Über Graphen und ihre Anwendung auf Determinantentheorie und Mengenlehre, *Math. Ann.*, **77** (1916) 453–465.

[41] 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.

[42] C. C. Lindner and C. A. Rodger, Design theory. Second edition. Discrete Mathematics and its Applications (Boca Raton). CRC Press, Boca Raton, FL, 2009. xiv+264 pp.

[43] E. Mendelsohn and A. Rosa, Embedding maximal packings of triples, *Congr. Numer.*, **40** (1983) 235–247.

[44] O. R. Musin, The problem of the twenty-five spheres. (Russian) *Uspekhi Mat. Nauk* **58** (2003), no. 4 (352), 153–154; translation in *Russian Math. Surveys* **58** (2003), no. 4, 794–795.

[45] P. R. J. Östergård and O. Pottonen, There exists no Steiner system S(4,5,17), *J. Combin. Theory Series A* **115** (2008), 1570–1573.

[46] H. J. Ryser, A combinatorial theorem with an application to latin rectangles, *Proc. Amer. Math. Soc.*, **2** (1951) 550–552.

[47] G. Sabidussi, Vertex-transitive graphs, *Monatsh. Math.* **68** (1964), 426–438.

[48] K. Schütte and B. L. van der Waerden, Das Problem der dreizehn Kugeln. (German) *Math. Ann.* **125** (1953), 325–334.

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

[50] J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.*, **43** (1938), 377–385.

[51] N. M. Singhi and S. S. Shrikhande, Embedding of quasi-residual designs with $\lambda = 3$, *Utilitas Math.*, **4** (1973) 35–53.

[52] N. M. Singhi and S. S. Shrikhande, Embedding of quasi-residual designs, *Geometriae Dedicata.*, **2** (1974) 509–517.

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

[54] B. Smetaniuk, A new construction on Latin squares. I. A proof of the Evans conjecture, *Ars Combin.*, **11** (1981) 155–172.

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

[56] W. Tutte, A family of cubical graphs, *Proc. Cambridge Philos. Soc.* **43** (1947), 459–474.

[57] M. S. Viazovska, The sphere packing problem in dimension 8, *Ann. of Math.* **185** (2017), 991–1015.

[58] V. G. Vizing, On an estimate of the chromatic class of a p-graph, *Diskret. Analiz.*, **3** (1964) 25–30.

[59] R. Weiss, The nonexistence of 8-transitive graphs, *Combinatorica* **1** (1981), 309–311.

[60] 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.